



GOBIERNO DE
MÉXICO



DIRECCIÓN DE ADMINISTRACIÓN

Unidad de Adquisiciones

Coordinación de Adquisición de Bienes y Contratación de Servicios

Coordinación Técnica de Adquisición de Bienes de Inversión y Activos

División de Contratación de Activos y Logística

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Instituto Mexicano del Seguro Social

Dirección de Administración
Unidad de Adquisiciones

Coordinación de Adquisición de Bienes y Contratación de Servicios
Coordinación Técnica de Adquisición de Bienes de Inversión y Activos
División de Contratación de Activos y Logística.

Calle Durango número 291, Piso 5, Colonia Roma Norte, Demarcación Territorial Cuauhtémoc, Código Postal 06700, Ciudad de México, México.

Convocatoria Licitación Pública Nacional Electrónica Núm. LA-050GYR019-E182-2022

**Para la Contratación de los:
“Servicios Administrados de Seguridad Informática (SASI) 2022-2024”**



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Índice de la Convocatoria

ÍNDICE DE LA CONVOCATORIA.....	2
1. DATOS GENERALES O DE IDENTIFICACIÓN DE LA LICITACIÓN PÚBLICA.	11
1.1. DATOS DE IDENTIFICACIÓN.....	11
1.2. MEDIO QUE SE UTILIZARÁ PARA LA LICITACIÓN PÚBLICA Y CARÁCTER DE LA MISMA.	11
1.3. NÚMERO DE IDENTIFICACIÓN DE LA LICITACIÓN PÚBLICA ASIGNADO POR COMPRANET.....	12
1.4. INDICACIÓN DE LOS EJERCICIOS FISCALES PARA LA CONTRATACIÓN.	12
1.5. IDIOMA EN QUE SE DEBERÁN PRESENTAR LAS PROPOSICIONES, LOS FOLLETOS Y ANEXOS TÉCNICOS.	12
1.6. DISPONIBILIDAD PRESUPUESTARIA.....	12
1.7. PROCEDIMIENTO FINANCIADO CON CRÉDITOS EXTERNOS.....	12
2. OBJETO Y ALCANCE DE LA LICITACIÓN PÚBLICA.	12
2.1. OBJETO DE LA CONTRATACIÓN.....	12
2.2. AGRUPACIÓN DE PARTIDAS.....	13
2.3. PRECIOS MÁXIMOS DE REFERENCIA.....	13
2.4. NORMAS OFICIALES MEXICANAS, NORMAS ESTÁNDAR (ANTES MEXICANAS), INTERNACIONALES, REFERENCIA O ESPECIFICACIONES.	13
2.4.1. LICENCIAS, PERMISOS, REGISTROS, CERTIFICADOS O AUTORIZACIONES.	13
2.4.2. FOLLETOS, INSERTOS, CATÁLOGOS.	13
2.5. MÉTODO QUE SE UTILIZARÁ PARA REALIZAR LAS PRUEBAS QUE PERMITAN VERIFICAR EL CUMPLIMIENTO DE LAS ESPECIFICACIONES DE LOS SERVICIOS A CONTRATAR E INSTITUCIÓN PÚBLICA O PRIVADA QUE LO REALIZARÁ.	13
2.6. CANTIDADES A CONTRATAR.....	14
2.7. FORMA DE ADJUDICACIÓN.	14
2.8. MODELO DE CONTRATO.	15
3. FORMA Y TÉRMINOS QUE REGIRÁN LOS DIVERSOS ACTOS DE LA LICITACIÓN PÚBLICA NACIONAL ELECTRÓNICA.....	15
3.1. REDUCCIÓN DE PLAZOS.	15
3.2. FECHA, HORA Y LUGAR PARA LOS ACTOS DE LA LICITACIÓN PÚBLICA NACIONAL ELECTRÓNICA	15
3.3. VISITA A LAS INSTALACIONES.	16
3.4. JUNTA DE ACLARACIONES.....	16
3.5. RECEPCIÓN DE PROPOSICIONES.....	17
3.6. PROPOSICIONES CONJUNTAS.	19
3.7. PROPOSICIÓN ÚNICA.....	20
3.8. DOCUMENTACIÓN DISTINTA A LA PROPOSICIÓN.	20
3.9. ACREDITAMIENTO DE EXISTENCIA LEGAL Y PERSONALIDAD JURÍDICA DEL LICITANTE.	20
3.10. DOCUMENTACIÓN QUE SE RUBRICARÁ.	20



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

3.11. FALLO Y FIRMA DE CONTRATO.....	21
3.12. DOCUMENTOS QUE DE MANERA PREVIA A LA FIRMA DEL CONTRATO, DEBERÁ PRESENTAR EL LICITANTE ADJUDICADO	21
PERSONA MORAL	21
PERSONA FÍSICA.....	22
AMBOS	22
4. REQUISITOS QUE LOS LICITANTES DEBEN CUMPLIR Y QUE SU INCUMPLIMIENTO, AUSENCIA U OMISIÓN AFECTAN LA SOLVENCIA DE LA PROPOSICIÓN Y MOTIVARÁ SU DESECHAMIENTO.....	24
4.1. FIRMA ELECTRÓNICA.....	24
4.2. DOCUMENTACIÓN DISTINTA A LA PROPOSICIÓN (LEGAL-ADMINISTRATIVA).....	24
4.2.1. ESCRITO DE ACREDITACIÓN LEGAL Y PERSONALIDAD JURÍDICA DEL LICITANTE.....	25
4.2.2. ESCRITO DE NACIONALIDAD MEXICANA.....	25
4.2.3. ESCRITO DE CUMPLIMIENTO DE NORMAS.....	25
4.2.4. ESCRITO DE NO ENCONTRARSE EN LOS SUPUESTOS DE LOS ARTÍCULOS 50 Y 60 DE LA LAASSP.....	25
4.2.5. DECLARACIÓN DE INTEGRIDAD.....	25
4.2.6. ESCRITO DE ESTRATIFICACIÓN DE MIPYME.....	25
4.2.7. CONVENIO DE PARTICIPACIÓN CONJUNTA.....	25
4.2.8. ESCRITO DE ACEPTACIÓN DE LAS DISPOSICIONES DEL SISTEMA COMPRANET.....	26
4.3. PROPUESTA TÉCNICA.....	26
4.4. PROPUESTA ECONÓMICA.....	27
4.5 INDICACIONES.....	27
4.6. DOCUMENTOS QUE NO AFECTAN LA SOLVENCIA DE LA PROPOSICIÓN Y SU OMISIÓN NO SERÁ CAUSA DE DESECHAMIENTO:	27
A. ESCRITO PARA SOLICITAR LA CLASIFICACIÓN DE LA INFORMACIÓN ENTREGADA POR EL LICITANTE.....	27
B. DECLARACION DE No COLUSIÓN COMISIÓN FEDERAL DE COMPETENCIA ECONÓMICA.....	28
C. PROTOCOLO DE ACTUACIÓN EN MATERIA DE CONTRATACIONES PÚBLICAS Y OTORGAMIENTO Y PRÓRROGA DE LICENCIAS, PERMISOS, AUTORIZACIONES Y CONCESIONES.....	28
D. MANIFIESTO DE CONOCER Y REGISTRARSE EN EL MODULO DE FORMALIZACION DE INSTRUMENTOS JURÍDICOS	28
5. CAUSALES EXPRESAS DE DESECHAMIENTO.....	29
6. CRITERIOS ESPECÍFICOS CONFORME A LOS CUALES SE EVALUARÁN LAS PROPOSICIONES.....	32
6.1 EVALUACIÓN DE LA PROPUESTA TÉCNICA.....	32
6.1.1 Matriz de Puntos.....	33
6.2 EVALUACIÓN DE LA PROPUESTA ECONÓMICA.....	34
7. ADJUDICACIÓN DE CONTRATO.....	35
8. DECLARACIÓN DESIERTA DE LA LICITACIÓN.....	35



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

9. CANCELACIÓN DE LA LICITACIÓN, PARTIDA(S), O CONCEPTOS INCLUIDOS EN ÉSTA.....	35
10. INCONFORMIDADES	35
11. OPERACIÓN DE COMPRANET	36
12. FORMATOS QUE FACILITARÁN Y AGILIZARÁN LA PRESENTACIÓN Y RECEPCIÓN DE LAS PROPOSICIONES.....	37
13. INFORMACIÓN RESERVADA Y CONFIDENCIAL	37
14. PROTOCOLO DE ACTUACIÓN EN MATERIA DE CONTRATACIONES PÚBLICAS Y OTORGAMIENTO Y PRÓRROGA DE LICENCIAS, PERMISOS, AUTORIZACIONES Y CONCESIONES.....	38
15. NOTA INFORMATIVA OCDE.....	39
ANEXO 1.- ANEXO TÉCNICO	40
1. OBJETIVO DEL DOCUMENTO.....	40
1.1. OBJETIVO GENERAL	40
1.2. OBJETIVOS ESPECÍFICOS	40
2. ALCANCE	41
3. BENEFICIOS	41
4. ACTUALIZACIÓN TECNOLÓGICA	42
5. REQUERIMIENTOS DEL SERVICIO	43
6. REQUERIMIENTOS DEL SERVICIO - ESPECIFICACIONES TÉCNICAS	44
6.1. SERVICIOS DE SEGURIDAD – CONTINUIDAD OPERATIVA	45
6.1.1. SERVICIOS DE FIREWALL.....	45
6.1.2. SERVICIOS DE PREVENCIÓN DE INTRUSOS (IPS).....	47
6.1.3. SERVICIOS DE PROTECCIÓN CONTRA ATAQUES DENEGACIÓN DE SERVICIO (DDOS).....	49
6.1.4. SERVICIOS DE REDES PRIVADAS VIRTUALES (VPN).....	50
6.1.5. SERVICIOS DE FILTRADO DE CONTENIDO WEB	53
6.1.6. SERVICIOS DE FILTRADO DE CONTENIDO DE CORREO (ANTISPAM)	55
6.1.7. SERVICIOS DE FIREWALL ESPECIALIZADO EN SERVICIOS WEB (WAF)	57
6.1.8. SERVICIOS DE FIREWALL ESPECIALIZADO EN BASE DE DATOS (DBF).....	59



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

6.1.9. SERVICIOS DE GESTIÓN UNIFICADA DE AMENAZAS (UTM)	61
6.1.10. SERVICIO DE CORRELACIÓN DE EVENTOS	63
6.1.11. SERVICIO DE PROTECCIÓN DE AMENAZAS PERSISTENTES AVANZADAS (APT) ...	65
6.2. SERVICIOS DE SEGURIDAD – VERIFICACIÓN Y CALIDAD	66
6.2.1. SERVICIOS DE BORRADO SEGURO DE INFORMACIÓN	67
6.2.2. SERVICIO DE GESTIÓN DE DOMINIOS.....	68
6.2.3. SERVICIO DE CERTIFICADOS DIGITALES SSL.....	69
6.2.4. SERVICIOS DE CIBERINTELIGENCIA (CIBERSEGURIDAD)	69
6.2.5. SERVICIOS DE PROTECCIÓN EN REDES INALÁMBRICAS Y SEGURIDAD EN DISPOSITIVOS MÓVILES.	72
6.2.6. SERVICIOS DE GESTIÓN Y CONTROL DE ACCESO PARA USUARIOS PRIVILEGIADOS (AAA).....	73
6.2.7. SERVICIO DE ANTIVIRUS	75
6.2.8. SERVICIOS DE PREVENCIÓN DE PÉRDIDA DE INFORMACIÓN	76
6.2.9. SERVICIOS DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)	77
6.2.10. SERVICIOS CONTINUIDAD DE GESTIÓN DEL CAMBIO EN SEGURIDAD DE LA INFORMACIÓN.....	80
6.2.11. SERVICIOS DE ANÁLISIS DE VULNERABILIDADES DINÁMICO	81
6.2.12. SERVICIOS DE ANÁLISIS DE VULNERABILIDADES ESTÁTICO	82
6.2.13. SERVICIOS DE PRUEBAS DE PENETRACIÓN.....	84
6.2.14. SERVICIOS DE ANÁLISIS FORENSE.....	85
6.3. SERVICIOS DEL CENTRO DE OPERACIONES DE SEGURIDAD (SOC)	86
6.5. CONDICIONES PARA LA IMPLEMENTACIÓN DE LOS SERVICIOS	90
6.6. IMPLEMENTACIÓN DE LOS SERVICIOS.....	90
6.7. MESAS DE TRABAJO	91
6.8. PERFIL DEL PROVEEDOR	92
PARTIDA 2	94



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

7. CONDICIONES TÉCNICAS DE ACEPTACIÓN DE ENTREGABLES.....	95
7.1. ENTREGABLES GENERALES	95
7.2. ENTREGABLES BAJO DEMANDA	101
7.3. ENTREGABLES PERIÓDICOS.....	106
8. NIVELES DE SERVICIO QUE DEBERÁN CUMPLIRSE (SLA).....	109
8.1. PENAS CONVENCIONALES	109
9. DEDUCCIONES.....	109
10. CONVENIO DE CONFIDENCIALIDAD Y RESGUARDO DE LA INFORMACIÓN.....	110
11. NORMAS	110
12. NORMATIVIDAD APLICABLE	110
13. CUMPLIMIENTO DE POLÍTICAS.....	111
14. FINALIZACIÓN DEL CONTRATO.....	111
15. MODELO DE GOBIERNO	112
APÉNDICE “A”	114
APÉNDICE “B”	141
APÉNDICE “B-BIS”	144
ANEXO 2.- TÉRMINOS Y CONDICIONES.....	146
1. OBJETIVO DEL DOCUMENTO.....	146
2. PREMISA.....	146
3. NOMBRE DEL PROYECTO	146
4. OBJETIVOS DEL PROYECTO.....	146
5. NORMAS OFICIALES O CERTIFICACIONES	147
6. FOLLETOS, CATÁLOGOS, FOTOGRAFÍAS, MANUALES ENTRE OTROS	147
7. VISITAS A LAS INSTALACIONES	147
8. TIPO DE ABASTECIMIENTO REQUERIDO.....	147
9. GARANTÍAS.....	147
10. ACUERDOS DE NIVELES DE SERVICIO	148
10.1. PENAS CONVENCIONALES	149



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

10.2. SERVICIOS DE HABILITACIÓN, OPERACIÓN Y TRANSICIÓN	149
10.3. SERVICIOS DE SEGURIDAD – CONTINUIDAD OPERATIVA.....	149
10.4. SERVICIOS DE SEGURIDAD – VERIFICACIÓN/CALIDAD	150
10.5. SERVICIOS DEL CENTRO DE OPERACIONES DE SEGURIDAD (SOC).....	153
10.6. DEDUCCIONES	154
10.7. DISPONIBILIDAD	154
10.8. TIEMPO DE DETECCIÓN Y SOLUCIÓN DE FALLAS.....	156
10.9. TIEMPO DE DETECCIÓN Y MITIGACIÓN DE INCIDENTES.....	160
10.10. SOLICITUDES DE REQUERIMIENTOS Y CAMBIOS	163
10.11. SERVICIOS DE SEGURIDAD – CONTINUIDAD OPERATIVA.....	168
10.12. SERVICIOS DE SEGURIDAD – VERIFICACIÓN/CALIDAD	169
10.13. SERVICIOS DEL CENTRO DE OPERACIONES DE SEGURIDAD (SOC).....	181
11. CONDICIONES DE PAGO	186
12. ENTREGABLES	187
12.1. ENTREGABLES GENERALES.....	187
12.2. ENTREGABLES BAJO DEMANDA	193
12.3. ENTREGABLES PERIÓDICOS	198
13. CONDICIONES DE ACEPTACIÓN DE LOS SERVICIOS.....	201
14. LUGAR Y HORARIO PARA LA ENTREGA.....	201
15. CONVENIO DE CONFIDENCIALIDAD Y RESGUARDO DE LA INFORMACIÓN.....	201
16. PROPIEDAD INTELECTUAL.....	202
17. MÉTODO DE EVALUACIÓN DE PROPUESTAS	202
18. FUNCIONARIOS PÚBLICOS DE LA DIDT PARTICIPANTES EN EL PROCESO DE CONTRATACIÓN	202
19. VIGENCIA DEL CONTRATO	202
20. PLAZO DEL SERVICIO	203
21. ADMINISTRADOR DEL CONTRATO.....	203



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

22. MECANISMOS DE CONTROL PARA LA ADMINISTRACIÓN DEL CONTRATO.....	203
23. MECANISMOS REQUERIDOS AL PROVEEDOR PARA RESPONDER POR DEFECTOS O VICIOS OCULTOS DE LOS BIENES O DE LA CALIDAD DE LOS SERVICIOS	203
24. OTORGAMIENTO DE ANTICIPO.....	203
ANEXO 3.- ESCRITO DE ACREDITACIÓN LEGAL Y PERSONALIDAD JURÍDICA DEL LICITANTE	204
ANEXO 4.- ESCRITO DE NACIONALIDAD MEXICANA.....	206
ANEXO 5.- ESCRITO DE CUMPLIMIENTO DE NORMAS	207
ANEXO 6.- ESCRITO DE NO ENCONTRARSE EN LOS SUPUESTOS DE LOS ARTÍCULOS 50 Y 60 DE LA LAASSP	208
ANEXO 7.- DECLARACIÓN DE INTEGRIDAD	209
ANEXO 8.- ESCRITO DE ESTRATIFICACIÓN DE MIPYME.....	210
ANEXO 8 BIS.- INSTRUCTIVO DE LLENADO PARA EL ESCRITO DE ESTRATIFICACIÓN DE MICRO, PEQUEÑA O MEDIANA EMPRESA (MIPYMES)	211
ANEXO 9- PROPUESTA ECONÓMICA.....	212
ANEXO 10.- RELACIÓN DE DOCUMENTOS A PRESENTAR	216
ANEXO 11.- ESCRITO PARA SOLICITAR LA CLASIFICACIÓN DE LA INFORMACIÓN ENTREGADA POR EL LICITANTE	218
ANEXO 12.- ESCRITO DE MANIFESTACIÓN QUE NO DESEMPEÑA EMPLEO, CARGO O COMISIÓN EN EL SERVICIO PÚBLICO O, EN SU CASO, QUE A PESAR DE DESEMPEÑARLO, CON LA FORMALIZACIÓN DEL CONTRATO CORRESPONDIENTE NO SE ACTUALIZA UN CONFLICTO DE INTERÉS.....	219
ANEXO 13.- MANIFESTACIÓN DE INTERÉS EN PARTICIPAR	220
ANEXO 13.1- FORMATO DE SOLICITUD DE ACLARACIONES	221
ANEXO 14.- MODELO DE CONTRATO.....	222
ANEXO 15.- MODELO DE CONVENIO DE PROPOSICIÓN CONJUNTA	252
ANEXO 16.- NOTA INFORMATIVA PARA PARTICIPANTES DE PAÍSES MIEMBROS DE LA ORGANIZACIÓN PARA LA COOPERACIÓN Y EL DESARROLLO ECONÓMICO (OCDE)	257
ANEXO 17.- DECLARACION DE NO COLUSIÓN COMISIÓN FEDERAL DE COMPETENCIA ECONÓMICA	261
ANEXO 18.- MODELO DE FIANZA.....	263



GOBIERNO DE
MÉXICO



DIRECCIÓN DE ADMINISTRACIÓN

Unidad de Adquisiciones

Coordinación de Adquisición de Bienes y Contratación de Servicios

Coordinación Técnica de Adquisición de Bienes de Inversión y Activos

División de Contratación de Activos y Logística

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

ANEXO 19 CARTA DE AUTORIZACIÓN 32-D	267
ANEXO 20 MANIFESTACIÓN DE SERVICIOS ESPECIALIZADOS.....	268
ANEXO 21 ESCRITO DE ACEPTACIÓN DE LAS DISPOSICIONES DEL SISTEMA COMPRANET.	269
ANEXO 22 MANIFIESTO DE CONOCER Y REGISTRARSE EN EL MÓDULO DE FORMALIZACIÓN DE INSTRUMENTOS JURÍDICOS	270
GLOSARIO DE TÉRMINOS.....	272



GOBIERNO DE
MÉXICO



DIRECCIÓN DE ADMINISTRACIÓN

Unidad de Adquisiciones

Coordinación de Adquisición de Bienes y Contratación de Servicios

Coordinación Técnica de Adquisición de Bienes de Inversión y Activos

División de Contratación de Activos y Logística

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Convocatoria

El Instituto Mexicano del Seguro Social, en cumplimiento al artículo 134 de la Constitución Política de los Estados Unidos Mexicanos; el Título Primero “*Disposiciones Generales*”, Capítulo Único, artículos 3 fracción IX y 25 y Título Segundo “*De los Procedimientos de Contratación*”, Capítulo Primero “*Generalidades*”, Capítulo Segundo “*De la Licitación Pública*” y los artículos 26 fracción I, 26 Bis fracción II, 27, 28 fracción I, 29, 30 y 47 de la LAASSP; el “*Protocolo de actuación en materia de contrataciones públicas, otorgamiento y prórroga de licencias, permisos, autorizaciones y concesiones*” publicado en el DOF el 20 de agosto del 2015 y el “*Acuerdo por el que se modifica el diverso que expide el protocolo de actuación en materia de contrataciones públicas, otorgamiento y prórroga de licencias, permisos, autorizaciones y concesiones*”, publicado en el DOF el día 19 de febrero de 2016 y 28 de febrero de 2017; y los relativos y demás disposiciones vigentes aplicables en la materia, a través de la División de Contratación de Activos y Logística, se convoca a las personas físicas o morales de nacionalidad mexicana cuya actividad comercial esté relacionada con los servicios a contratar descritos en los **Anexos 1.- Anexo Técnico y 2.- Términos y Condiciones**, para participar en la licitación pública y, que **NO** se encuentren en alguno de los supuestos que se establecen en los artículos **50** y **60** de la LAASSP.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

1. DATOS GENERALES O DE IDENTIFICACIÓN DE LA LICITACIÓN PÚBLICA.

1.1. Datos de identificación.

Entidad convocante	Instituto Mexicano del Seguro Social.
Área contratante	Dirección de Administración. Unidad de Adquisiciones. Coordinación de Adquisición de Bienes y Contratación de Servicios. Coordinación Técnica de Adquisición de Bienes de Inversión y Activos División de Contratación de Activos y Logística.
Domicilio	Calle Durango número 291, Piso 5, Colonia Roma Norte, Código Postal 06700, Demarcación Territorial Cuauhtémoc, Ciudad de México, México.
Área requirente/técnica	Coordinación de Telecomunicaciones y Seguridad de la Información / División de Seguridad Informática Física.

Ninguna de las condiciones contenidas en la presente Convocatoria, así como en las proposiciones presentadas por los licitantes podrán ser negociadas, de conformidad con lo previsto en el séptimo párrafo del artículo 26 de la LAASSP.

1.2. Medio que se utilizará para la licitación pública y carácter de la misma.

La presente Licitación Pública Nacional conforme al medio utilizado es Electrónica. Por lo cual los licitantes deberán participar únicamente a través del Sistema Electrónico de Información Pública Gubernamental denominado "CompraNet", de conformidad con lo dispuesto en los artículos 26 Bis fracción II de la LAASSP, y en el **"Acuerdo por el que se establecen las disposiciones que deberán observar para la utilización del Sistema Electrónico de Información Pública Gubernamental, denominado CompraNet"**, publicado en el Diario Oficial de la Federación (DOF) el 28 de junio de 2011, en la cual exclusivamente se permitirá la participación de los licitantes a través de CompraNet y no se aceptarán proposiciones de manera presencial o a través de servicio postal o de mensajería.

Por lo anterior, las proposiciones remitidas a través de CompraNet deberán emplear los medios de identificación electrónica que establezca la Secretaría de Hacienda y Crédito Público (SHCP), los cuales producirán los mismos efectos que las leyes otorgan a los documentos correspondientes y, en consecuencia, tendrán el mismo valor probatorio; lo anterior conforme a lo establecido en los párrafos penúltimo y último del artículo 27 de la LAASSP y 50 de su Reglamento, así como los numerales 14 y 16 del "ACUERDO por el que se establecen las disposiciones que se deberán observar para la utilización del Sistema Electrónico de Información Pública Gubernamental denominado CompraNet", publicadas en el DOF el 28 de junio de 2011, y el Manual de Unidades Compradoras publicado por la SHCP.

Por lo anterior, aquellos interesados en participar en la presente licitación que requieran asesoría o presenten situaciones particulares sobre el manejo y uso de CompraNet, deberán dirigirse al personal que administra dicho sistema; los datos del contacto podrán ser localizados en la página web: <https://compranet.hacienda.gob.mx>.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

El carácter del presente procedimiento de contratación es **Nacional**.

1.3. Número de identificación de la Licitación Pública asignado por CompraNet.

LA-050GYR019-E182-2022.

1.4. Indicación de los ejercicios fiscales para la contratación.

La presente contratación abarcará los ejercicios fiscales **2022, 2023 y 2024**, autorizado por el H. Consejo Técnico mediante el Acuerdo ACDO.AS3.HCT.271021/266.P.DIDT.

1.5. Idioma en que se deberán presentar las proposiciones, los folletos y anexos técnicos.

Las proposiciones deberán presentarse en idioma español.

Los anexos técnicos, certificados, diplomas y folletos del servicio ofertado por el licitante podrán presentarse en el idioma del país de origen de los servicios que se oferta, acompañados de una traducción simple al español. Será motivo de desechar su propuesta si no acompaña la traducción de cualquier documento que presente en otro idioma que no sea el español, de conformidad con el artículo 29, fracción IV de la LAASSP.

1.6. Disponibilidad presupuestaria.

El monto del presupuesto para el ejercicio 2022 se encuentra aprobado de conformidad a los **Dictámenes de Disponibilidad Presupuestal Previos con folio 0000307831-2022 y 0000307839-2022** emitidos por la División de Control y Seguimiento al Presupuesto de Operación en Ámbito Central.

Clave CUCOP:

Núm.	CUCOP	Concepto
1	31900004	Servicios a centros de datos (hospedaje, electricidad, video vigilancia, monitoreo, aire acondicionado, servidores y otros).

1.7. Procedimiento financiado con créditos externos.

El presente procedimiento de contratación no será financiado con fondos provenientes de créditos externos otorgados al Gobierno Federal, ni con la garantía de Organismos Financieros Regionales o Multilaterales.

2. OBJETO Y ALCANCE DE LA LICITACIÓN PÚBLICA.

2.1. Objeto de la contratación.

El objeto es contar con los Servicios Administrados de Seguridad Informática del 2022 al 2024.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

La descripción amplia y detallada de los servicios a contratar se encuentra especificada en:

- a. Anexo 1.- Anexo Técnico.
- b. Anexo 2.- Términos y Condiciones.

2.2. Agrupación de Partidas.

La adjudicación del presente procedimiento de contratación se llevará a cabo mediante las siguientes partidas:

- Partida 1:**
1. Servicios de Seguridad - Continuidad Operativa
 2. Servicios de Seguridad – Verificación y Calidad
 3. Servicios del Centro de Operaciones de Seguridad (SOC)
- Partida 2:**
1. Análisis de Vulnerabilidades Estático
 2. Análisis de Vulnerabilidades Dinámico
 3. Servicios de Análisis Forense
 4. Servicios de Pruebas de Penetración

El licitante, **DEBERÁ** manifestar mediante un escrito libre que acompañará a su proposición la partida respecto de la cual es su voluntad participar.

2.3. Precios Máximos de Referencia.

En el presente procedimiento no se establecen Precios Máximos de Referencia.

2.4. Normas Oficiales Mexicanas, Normas Estándar (antes Mexicanas), Internacionales, Referencia o Especificaciones.

Para la presente contratación **no se requiere** el cumplimiento de alguna Norma Mexicana, Norma Oficial Mexicana o Norma Internacional o de referencia.

2.4.1. Licencias, permisos, registros, certificados o autorizaciones.

- Certificado ISO/IEC27001:2013
- Ceritificado ISO/IEC20000-1:2018

2.4.2. Folletos, insertos, catálogos.

No aplica.

2.5. Método que se utilizará para realizar las pruebas que permitan verificar el cumplimiento de las especificaciones de los servicios a contratar e institución pública o privada que lo realizará.

No aplica.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

2.6. Cantidades a contratar.

Con fundamento en los artículos 47, fracción I de la LAASSP y 85 del Reglamento, la adjudicación objeto de la presente Convocatoria será formalizada **mediante contrato abierto**, por no tener un número definido de servicios.

Los montos mínimos y máximos incluyendo el IVA de cada partida se describen a continuación:

Partida 1:

Importe Máximo \$346,248,400.00 (Trescientos cuarenta y seis millones, doscientos cuarenta y ocho mil, cuatrocientos pesos 00/100 M.N.)

Importe Mínimo \$138,499,360.00 (Ciento treinta y ocho millones, cuatrocientos noventa y nueve mil, trescientos sesenta pesos 00/100 M. N.)

Partida 2:

Importe Máximo \$45,481,645.01 (Cuarenta y cinco millones, cuatrocientos ochenta y un mil, sescientos cuarenta y cinco pesos 01/100 M.N.)

Importe Mínimo \$18,192,658.00 (Dieciocho millones, ciento noventa y dos mil, seiscientos cincuenta y ocho pesos 00/100 M.N.)

Los montos mínimos y máximos, incluyendo el IVA por ejercicio fiscal serán los siguientes:

PARTIDA 1				
MONTOS	AÑO			TOTAL
	2022	2023	2024	
MÁXIMO	\$43,281,050.00	\$173,124,200.00	\$129,843,150.00	\$346,248,400.00
MÍNIMO	\$17,312,420.00	\$69,249,680.00	\$51,937,260.00	\$138,499,360.00

PARTIDA 2				
MONTOS	AÑO			TOTAL
	2022	2023	2024	
MÁXIMO	\$5,685,205.63	\$22,740,822.50	\$17,055,616.88	\$45,481,645.01
MÍNIMO	\$2,274,082.25	\$9,096,329.00	\$6,822,246.75	\$18,192,658.00

2.7. Forma de adjudicación.

Se requiere una sola fuente de abastecimiento por cada partida.

Por la naturaleza técnica de los servicios del SASI 2022-2024, en el caso de las partidas 1 y 2, los licitantes únicamente podrán participar en una de las dos partidas, lo anterior para evitar conflicto de interés técnico en detrimento del IMSS.

En este sentido, se hace del conocimiento de los Licitantes que, derivado de la naturaleza de los servicios y por sus características técnicas, bajo ningún escenario se podrá adjudicar las partidas 1 y 2 a un mismo licitante al que se haya asignado una de las dos.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Se adjudicará al licitante que cumpla con todos y cada uno de los requisitos solicitados en la presente Convocatoria, con los **Anexos 1.- Anexo Técnico** y **2.- Términos y Condiciones** de la convocatoria y obtenga la mayor puntuación en la evaluación por puntos combinada, técnica y económica, de acuerdo a la matriz de evaluación prevista en el **numeral 6.1.1**, de conformidad con el artículo 36 Bis fracción I de la LAASSP.

2.8. Modelo de contrato.

Se adjunta como **Anexo 14** el modelo de contrato para formalizar los derechos y obligaciones que se deriven de la presente Licitación Pública Nacional Electrónica, al cual estará obligado el licitante que resulte adjudicado y atendiendo a lo establecido en el artículo 45 de la LAASSP y 81 de su Reglamento.

En caso de discrepancia entre el contenido del contrato y el de la presente convocatoria, prevalecerá lo estipulado en ésta última, así como el resultado de la Junta de Aclaraciones, de conformidad con lo señalado en el penúltimo párrafo del artículo 45 de la LAASSP.

3. FORMA Y TÉRMINOS QUE REGIRÁN LOS DIVERSOS ACTOS DE LA LICITACIÓN PÚBLICA NACIONAL ELECTRÓNICA.

3.1. Reducción de Plazos.

Para este procedimiento **NO APLICA** la reducción de plazos.

3.2. Fecha, hora y lugar para los actos de la Licitación Pública Nacional Electrónica

Acto	Fecha	Horario (Ciudad de México)	Lugar
Junta de Aclaraciones	13 de septiembre de 2022	11:00 horas	Los actos se realizarán de conformidad con lo establecido en el artículo 26 Bis, fracción II de la LAASSP, a través de CompraNet en la dirección electrónica https://compranet.hacienda.gob.mx/web/login.html
Presentación Apertura y de Proposiciones	27 de septiembre de 2022	11:00 horas	Al tratarse de una licitación pública electrónica, los licitantes únicamente podrán participar en los actos a través de ese medio.
Junta para la notificación del Fallo	3 de octubre de 2022	14:00 horas	

De cada junta se levantará acta, misma que se difundirá en CompraNet para efectos de notificación personal.

Asimismo, se hace del conocimiento de los interesados que los actos del procedimiento de esta licitación se llevarán a cabo en el domicilio de la convocante y, en su caso, con fundamento en el artículo 26 de la LAASSP, podrá asistir cualquier persona en calidad de observador, bajo la



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

condición de registrar su asistencia y abstenerse de intervenir en cualquier forma en los mismos. Una vez iniciado cualquiera de los distintos eventos en que participen los observadores, no se permitirá el ingreso a ningún otro.

Los observadores que ingresen a las instalaciones del Instituto deberán cumplir con las medidas de seguridad implementadas, además de aquellas medidas de prevención relacionadas con el virus SARS-CoV2; el no apegarse a su cumplimiento, les será denegado el acceso al inmueble o en su caso su desalojo.

3.3. Visita a las instalaciones.

No aplica.

3.4. Junta de aclaraciones.

La Junta de Aclaraciones se llevará a cabo en términos de los artículos 33 Bis de la LAASSP, 45 y 46 de su Reglamento, por lo que las personas que pretendan solicitar aclaraciones a la Convocatoria deberán presentar un escrito en término de los numerales citados y del artículo 48 fracción V del Reglamento, en el que expresen su interés en participar en la Licitación, por si o en representación de un tercero, de acuerdo con el **Anexo 13** que se adjunta para tal efecto, con el cual serán considerados licitantes y tendrán derecho a formular solicitudes de aclaración utilizando para tal caso el **Anexo 13.1** de la presente convocatoria.

Con el objeto de agilizar la junta de aclaraciones se solicita a los licitantes remitir el **Anexo 13.1** preferentemente en formato Word.

Los licitantes deberán enviar las solicitudes de aclaración y el escrito de interés, a través de CompraNet, en la sección "Mensajes Unidad Compradora/Licitantes" del "Procedimiento de Contratación", a más tardar **veinticuatro horas antes de la fecha y hora programada que se realice la Junta de Aclaraciones.**

Las solicitudes de aclaración deberán plantearse de manera concisa y estar directamente vinculadas con los puntos contenidos en la convocatoria, indicando el numeral o punto específico con el cual se relaciona.

El plazo para enviar dichas solicitudes será a partir de la publicación de esta convocatoria y hasta 24 horas de anticipación a la fecha programada para la Junta de Aclaraciones.

Cuando a razón de número de solicitudes de aclaración recibidas, o algún otro factor no imputable a la convocante y que sea acreditable, no sea posible otorgar respuestas el día en que inicia la Junta de Aclaraciones, el servidor público que presida la Junta, informará si éstas serán enviadas en ese momento **o si se suspenderá la sesión para reanudarla en hora o fecha posterior** a efecto de que las respuestas sean remitidas.

Con el envío de las respuestas a que se refiere el párrafo anterior, la convocante informará a los licitantes, atendiendo al número de solicitudes de aclaración contestadas, el plazo que estos tendrán para formular las preguntas que consideren necesarias en relación a las respuestas remitidas. Dicho plazo no podrá ser inferior a seis ni superior a cuarenta y ocho horas. Una vez



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

recibidas las preguntas a las respuestas otorgadas por la convocante, ésta informará a los licitantes el plazo máximo en el que enviará las contestaciones correspondientes, de conformidad con el artículo 46, fracción II del Reglamento.

De la Junta de Aclaraciones se levantará acta, misma que se difundirá en CompraNet para efectos de notificación personal.

Cuando el escrito de interés se presente fuera del plazo previsto en el artículo 33 Bis de la LAASSP, el licitante sólo tendrá derecho a formular preguntas sobre las respuestas que dé la convocante en la mencionada junta.

Asimismo, las solicitudes de aclaración que sean enviadas a través del sistema CompraNet con posterioridad al plazo previsto en el artículo 33 Bis de la LAASSP, no serán contestadas por la convocante por resultar extemporáneas, debiéndose integrar al expediente respectivo, salvo lo previsto en el artículo 46 fracción VI del Reglamento.

En cumplimiento a lo establecido en el artículo 33 penúltimo párrafo de la LAASSP, lo asentado en el acta que se derive del acto de Junta de Aclaraciones, formará parte de la Convocatoria a esta Licitación y deberá ser considerada por los licitantes para la elaboración de sus proposiciones ya que la evaluación de las mismas se realizará incluyendo lo establecido en dicha acta.

3.5. Recepción de proposiciones.

La presentación y apertura de proposiciones se llevará a cabo en términos de los artículos 34 y 35 de la LAASSP, así como 47, 48, 49, segundo párrafo y 50 del Reglamento, para lo cual podrán hacer uso de los formatos previstos en el numeral 12, de la presente convocatoria.

Para intervenir en el acto de presentación y apertura de proposiciones, bastará que los licitantes presenten un escrito en el que su firmante manifieste, bajo protesta de decir verdad, que cuenta con facultades suficientes para comprometerse por sí o por su representada, sin que resulte necesario acreditar su personalidad jurídica, para lo cual podrán hacer uso del **Anexo 3.- Escrito de acreditación legal y personalidad jurídica del licitante**.

Asimismo, se precisa que en la documentación técnica, legal y económica que integre la proposición remitida a través de CompraNet, se deberán emplear los medios de identificación electrónica en sustitución de la firma autógrafa, lo anterior de conformidad con lo señalado en la fracción II del artículo 26 Bis, el último párrafo del artículo 27 de la LAASSP y el primer párrafo del artículo 50 del Reglamento.

Sólo serán consideradas las proposiciones que se reciban por medio de CompraNet en respuesta al requerimiento técnico y económico. El licitante deberá firmar electrónicamente la proposición; para que se considere que se envió firmada, deberán descargarse los archivos PDF generados por CompraNet y que contienen los datos capturados en la propuesta, sólo esos archivos deberán firmarse utilizando el módulo de firma electrónica de documentos y cargarse en el área correspondiente.

Se procederá a la apertura de los sobres generados mediante el sistema, en el supuesto de que



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

durante el acto de presentación y apertura de proposiciones, por causas ajenas a la voluntad de la Convocante, no sea posible abrir los sobres que contengan las propuestas enviadas por CompraNet, el acto se reanudará a partir de que se restablezcan las condiciones que dieron origen a la interrupción, salvo lo previsto en el numeral 29 del "ACUERDO por el que se establecen las disposiciones que se deberán observar para la utilización del Sistema electrónico de Información Pública Gubernamental denominado CompraNet" el cual contempla lo siguiente:

"29.- Las dependencias y entidades, a través de la Unidad Compradora, recabarán de los licitantes su aceptación de que se tendrán como no presentadas sus proposiciones y, en su caso, la documentación requerida por la Unidad Compradora, cuando el archivo electrónico en el que se contengan las proposiciones y/o demás información no pueda abrirse por tener algún virus informático o por cualquier otra causa ajena a la dependencia o entidad."

Una vez alcanzada la fecha y hora de inicio del evento de apertura de proposiciones, el licitante no podrá enviar su proposición o modificación de la misma.

Una vez recibidas las proposiciones en la fecha, hora y lugar establecidos, éstas no podrán retirarse o dejarse sin efecto, por lo que deberán considerarse vigentes dentro del procedimiento de contratación hasta su conclusión.

Recibidas las proposiciones que hayan sido enviadas a través de CompraNet, se procederá a la apertura de todas y cada una de ellas, haciéndose constar la documentación presentada, sin que ello implique la evaluación de su contenido, por lo que, en el caso de que algún licitante omita la presentación de algún documento o requisito, no serán desechadas en ese momento, haciéndose constar ello en el formato de recepción de los documentos que integran la propuesta conforme al **Anexo 10** Relación de documentos a presentar, lo anterior de conformidad con lo establecido el artículo 47 del Reglamento.

De acuerdo a lo dispuesto en el artículo 50 del Reglamento, el licitante deberá foliar cada uno de los documentos que integren la proposición y aquéllos distintos a ésta, en todas y cada una de las hojas que los integren. Al efecto, se deberán numerar de manera individual la propuesta técnica y económica, así como el resto de los documentos que entregue el licitante, y por ser una licitación electrónica, podrá enviarse en varios archivos electrónicos. Sólo la falta absoluta de folio será causa de desechamiento, siempre y cuando esta circunstancia impide llevar a cabo su evaluación y por tanto, afecte la solvencia de la proposición.

El Instituto conforme al artículo 35 fracción III de la LAASSP, levantará el acta correspondiente que servirá de constancia de la celebración del acto de presentación y apertura de proposiciones, se hará constar el importe total de cada una de las partidas, en su caso de las proposiciones presentadas, asimismo se señalará lugar, fecha y hora en que se dará a conocer el fallo de la Licitación. El acta será firmada por los asistentes, a los cuales se les entregará copia simple de la misma.

El acta correspondiente al acto de presentación y apertura de proposiciones se difundirá a través de CompraNet al concluir el mismo, para efectos de su notificación en términos de lo dispuesto



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

en el último párrafo del artículo 37 Bis de la LAASSP.

3.6. Proposiciones conjuntas.

Conforme al artículo 34 de la LAASSP, los interesados podrán presentar propuestas conjuntas, siempre y cuando éstas cumplan con lo establecido en el artículo 44 y 48, fracción VIII, segundo párrafo del Reglamento.

Las personas interesadas podrán agruparse para presentar una propuesta, para tal efecto deberán cubrir los siguientes requisitos:

- a)** Uno de los integrantes podrá presentar el escrito mediante el cual se manifieste el interés en participar en la junta de aclaraciones y en el procedimiento de contratación.
- b)** Los integrantes deberán celebrar en términos de la legislación aplicable un convenio, en el cual se establezcan con precisión los siguientes aspectos, de conformidad con el **Anexo 15** de la presente convocatoria, o en cualquier instrumento siempre que cumpla con los requisitos establecidos en los artículos 34 de la LAASSP y 44 del Reglamento:
 - I.** Nombre, Domicilio y RFC de las personas integrantes, señalando, en su caso, los datos de los instrumentos públicos con los que se acredita la existencia legal de las personas morales y, de haberlas, sus reformas y modificaciones, así como el nombre de los socios que aparezcan en éstas,
 - II.** Nombre y domicilio de los representantes de cada una de las personas agrupadas, señalando, en su caso, los datos de las escrituras públicas con las que acrediten las facultades de representación, así como la designación de un domicilio común para todos los efectos que deriven del Convenio.
 - III.** Designación de un representante común, otorgándole poder amplio y suficiente, para atender todo lo relacionado con la propuesta y con el procedimiento de licitación pública nacional electrónica,
 - IV.** Descripción de las partes objeto del contrato que corresponderá cumplir a cada persona integrante, así como la manera en que se exigirá el cumplimiento de las obligaciones, y
 - V.** Estipulación expresa de que cada uno de los firmantes quedará obligado junto con los demás integrantes ya sea en forma solidaria o mancomunada para efectos del procedimiento de contratación y del contrato, en caso de que se les adjudique el mismo.

En el acto de presentación y apertura de proposiciones el representante común de la agrupación deberá señalar que la propuesta se presenta en forma conjunta. El convenio a que hace referencia el inciso b), se presentará con la propuesta y, en caso de que a los licitantes que la hubieren presentado se les adjudique el contrato, dicho convenio, formará parte integrante del mismo como uno de sus anexos.

En el supuesto de que se adjudique el contrato a los licitantes que presentaron una propuesta conjunta, el convenio indicado en el inciso b) y las facultades del apoderado legal de la



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

agrupación que formalizará el contrato respectivo, deberán constar en escritura pública, salvo que el contrato sea firmado por todas las personas que integran la agrupación que formula la propuesta conjunta o por sus representantes legales, quienes en lo individual, deberán acreditar su respectiva personalidad, o por el apoderado legal de la nueva sociedad que se constituya por las personas que integran la agrupación que formuló la propuesta conjunta, antes de la fecha fijada para la firma del contrato. Esto deberá comunicarse mediante escrito a la convocante por dichas personas o por su apoderado legal, al momento de darse a conocer el fallo o a más tardar en las veinticuatro horas siguientes.

En caso de que se presente proposición conjunta, y no se presente el convenio de participación conjunta o el presentado no cumpla con los requisitos legales y reglamentarios, afecta la solvencia de la propuesta y motivará su desechamiento.

- c) De conformidad con lo establecido en el artículo 48, fracción VIII, segundo párrafo del Reglamento de la LAASSP los integrantes deberán presentar en forma individual los escritos siguientes: **Escrito de no encontrarse en los supuestos de los artículos 50 y 60 de la LAASSP, Declaración de integridad, Escrito de nacionalidad mexicana y Escrito de estratificación de MIPYME**, conforme a los Anexos señalados en el numeral **4.2 Documentación distinta a la proposición (legal-administrativa)**.

La proposición deberá ser enviada por CompraNet y firmada electrónicamente por el representante común que para ese acto haya sido designado por el grupo de personas.

3.7. Proposición única.

Los licitantes sólo podrán presentar una proposición por la partida en que pretendan participar en el presente procedimiento de contratación.

3.8. Documentación distinta a la proposición.

El licitante podrá presentar la documentación distinta a la que conforma las propuestas técnica y económica, misma que forma parte de su proposición.

3.9. Acreditamiento de existencia legal y personalidad jurídica del licitante.

El licitante deberá acreditar su existencia legal y, en su caso, la personalidad jurídica de su representante, para efectos de la suscripción de la proposición, en el acto de presentación y apertura de proposiciones, para lo cual podrá hacer uso del **Anexo 3** de la convocatoria, o en formato libre siempre que cumpla con los requisitos del artículo 48, fracción V del Reglamento.

3.10. Documentación que se rubricará.

Serán rubricadas por los servidores públicos que asistan al acto de presentación y apertura de proposiciones, las Propuestas Económicas (**Anexo 9**) y la Relación de documentos a presentar (**Anexo 10**).

En todo caso, la totalidad de los archivos se almacenarán en medios ópticos de almacenamiento, uno para ser entregado al área técnica y/o requirente y otro para que obre en el expediente.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

3.11. Fallo y firma de contrato.

a) Fallo:

El fallo se emitirá de conformidad con el artículo 37 de la LAASSP en la fecha y hora establecida en el numeral 3.2 de la presente Convocatoria; en caso de que en la fecha prevista no se pueda emitir, el mismo podrá ser diferido hasta por veinte días naturales contados a partir de la fecha prevista originalmente y su contenido se difundirá a través de CompraNet el mismo día en que se emita, en el entendido de que este procedimiento sustituye a la notificación personal.

Así también el fallo podrá ser consultado en el portal de compras del IMSS en el apartado "Transparencia" (<http://compras.imss.gob.mx/>), o bien en el mural de comunicación ubicado en el piso 5 del inmueble en la Calle Durango número 291, Colonia Roma Norte, Código Postal 06700, Demarcación Territorial Cuauhtémoc, Ciudad de México, México; en donde se fijará copia de un ejemplar del acta por un término no menor de cinco días hábiles.

b) Firma del contrato:

El licitante adjudicado deberá firmar los contratos, dentro de los 15 días naturales siguientes al de la notificación del fallo, sin perjuicio de que con la citada notificación se realice la requisición de los servicios objeto de la presente licitación.

Para tal efecto, deberá hacerlo a través de CompraNet, en términos del **Manual de Operación** que contiene las directrices que se deberán observar en el Sistema Electrónico de Información Pública Gubernamental sobre Adquisiciones, Arrendamientos, Servicios, Obras Públicas y Servicios relacionados con las Mismas denominado CompraNet, para la utilización del **Módulo de Formalización de Instrumentos Jurídicos**, derivados de los procedimientos de contratación al amparo de la Ley y de la Ley de Obras Públicas y Servicios Relacionados con las Mismas, en este sentido, se informa que previo a llevar a cabo la formalización de los contratos, el licitante que resulte adjudicado deberá presentar en la División de Contratos, ubicada en Calle Durango número 291, piso 10, Colonia Roma Norte, C.P. 06700, Demarcación Territorial Cuauhtémoc, Ciudad de México, los documentos que se indican en el anexo adjunto a la Convocatoria denominado **Documentación Legal Solicitada para la Elaboración de Contratos**; precisando que el Acta Constitutiva que se integre a dicha documentación, deberá contener sello de recepción de la División de Contratación de Activos y Logística.

Adicionalmente, el licitante adjudicado deberá actualizar sus datos en el registro interno de proveedores del IMSS, a cargo de la División de Investigación de Mercados de Arrendamientos y Servicios, ubicada en Calle Durango 291, Piso 7, ala Sinaloa, Colonia Roma Norte, Demarcación Territorial Cuauhtémoc, C.P. 06700, en la Ciudad de México.

3.12. Documentos que de manera previa a la firma del contrato, deberá presentar el licitante adjudicado

Persona moral

- Acta constitutiva y, en su caso, sus respectivas modificaciones.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- b. Poder notarial del representante legal que firmará el contrato.

Persona física

- a. Acta de nacimiento o carta de naturalización.

Ambos

- a) Identificación oficial vigente y con fotografía del representante legal (cartilla del servicio militar nacional, pasaporte, credencial para votar ó cédula profesional), tratándose de personas físicas, y en el caso de personas morales, de la persona que firme la propuesta.
- b) Cédula de Registro Federal de Contribuyentes.
- c) Comprobante de domicilio con vigencia no mayor a 3 meses.
- d) En su caso, escrito de estratificación de empresa en términos del artículo 3 de la Ley para el Desarrollo de la Competitividad de la Micro, Pequeña y Mediana Empresa.
- e) Escrito en términos del artículo 50 y 60 de la LASSPP.
- f) Opinión positiva de cumplimiento de obligaciones fiscales emitida por el SAT, vigente a la firma del contrato, en términos del artículo 32-D del Código Fiscal de la Federación.
- g) Opinión positiva de cumplimiento de obligaciones fiscales en materia de seguridad social vigente a la firma del contrato emitida por el Instituto Mexicano del Seguro Social (IMSS), en términos del artículo 32-D del Código Fiscal de la Federación y del Acuerdo ACDO.AS1.HCT.260220/64.P.DIR dictado por el H. Consejo Técnico de "EL INSTITUTO" publicado en el Diario Oficial de la Federación el 30 de marzo de 2020.
- h) Escrito bajo protesta de decir verdad que no desempeña empleo, cargo o comisión en el servicio público o, en su caso, que a pesar de desempeñarlo, con la formalización del contrato correspondiente no se actualiza un conflicto de interés. (Artículo 49 fracción IX de la Ley General de Responsabilidades Administrativas DOF 18-07-2016). **(Anexo 12)**
- i) Constancia de situación fiscal vigente, emitida por el Instituto del Fondo Nacional de la Vivienda para los Trabajadores (INFONAVIT) en los términos establecidos por las "Reglas para la obtención de la constancia de situación fiscal en materia de aportaciones patronales y entero de amortizaciones" publicadas en el Diario Oficial de la Federación (DOF) el 28 de junio del 2017.

El licitante autoriza al IMSS consultar en tiempo real y en línea, la opinión de cumplimiento en materia de contribuciones de seguridad social, a través de los sistemas electrónicos que para tales efectos dispone la Dirección de Incorporación y Recaudación del IMSS. Para tal efecto, el licitante deberá utilizar el **Anexo 19**, que se adjunta a la presente Convocatoria.

En caso de que el licitante adjudicado haya participado en proposición conjunta, los documentos señalados deberán presentarse por cada uno de los integrantes del consorcio.

En caso de que el licitante:

- I. No se encuentre registrado ante este instituto o;
- II. Cuente con Registro Patronal pero se encuentre dado de baja o;
- III. No tenga personal que sea sujeto de aseguramiento obligatorio, de conformidad con lo dispuesto por el artículo 12 de la LSS.

No podrá obtener la citada Opinión, por lo cual dicho licitante podrá dar cumplimiento a tal requerimiento presentando lo siguiente:



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- i. Documento emitido por este Instituto (resultado de la consulta en el sistema para obtener la Opinión), en el que se haga constar que no se puede emitir la Opinión de cumplimiento, de conformidad con la Regla Quinta del Anexo único del ACDO.AS1.HCT.260220/64.P.DIR dictado por el H. Consejo Técnico de "EL INSTITUTO" publicado en el Diario Oficial de la Federación el 30 de marzo de 2020;
- ii. Escrito libre, bajo protesta de decir verdad, que no le es posible obtener la multicitada Opinión, justificando el motivo y anexando el documento en el que conste que no se puede emitir la misma y;

En el caso de que el licitante manifieste que presta sus servicios a través de trabajadores subcontratados con un tercero, deberá de presentar en tal caso, junto con la documentación citada en los dos párrafos anteriores, la Opinión de cumplimiento de obligaciones del subcontratante, desde luego, vigente y positiva (lo anterior en términos del artículo 15-A de la LSS).

En caso de que el participante forme parte de un grupo comercial y uno de los entes que forma parte del grupo se encarga de administrar la plantilla laboral de todas las empresas que lo conforman, será necesario que exhiba el documento que acredite la subcontratación para situarse en el supuesto del párrafo anterior.

En caso de que el licitante no cuente con trabajadores debido a que celebró contrato de prestación de servicios con otra empresa que es la que tiene contratados a los trabajadores (outsourcing), deberá presentar dicho contrato, así como escrito libre en el que manifieste que no se encuentra obligado debido a tal situación y opinión positiva vigente de cumplimiento de obligaciones en materia de seguridad social de la empresa subcontratada emitida por el IMSS.

En caso de que el licitante no cuente con trabajadores, deberá presentar escrito libre en el que manifieste que no se encuentra obligado a inscribirse ante el IMSS, por lo que no puede obtener la opinión de cumplimiento de obligaciones en materia de seguridad social.

Para los casos de contratos que se formalicen con personas físicas que presten sus servicios por sí mismos y por lo tanto no cuentan con un Registro Patronal ni tengan trabajadores registrados en el Instituto, el particular deberá de manifestar mediante escrito libre, bajo protesta de decir verdad, que no le es posible obtener la multicitada Opinión, justificando el motivo y anexando el documento (resultado de la solicitud de Opinión que le da el Sistema Institucional) en el que conste que no se puede emitir la misma.

En el caso de aquellos patrones (proveedores o contratistas y sus subcontratados) que tengan más de un Registro Patronal ante el Instituto y alguno o más de uno de estos Registros no se encuentre al corriente en el cumplimiento de las multicitadas obligaciones, no se podrá considerar que se encuentra al corriente en el cumplimiento de dichas obligaciones, aun cuando el registro patronal que haya utilizado para el contrato que se trate si se encuentre al corriente en sus pagos, por lo que deberá regularizar todos sus Registros a efecto de poder obtener la Opinión positiva.

En caso de que el participante cuente con trabajadores contratados bajo el régimen de



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

honorarios asimilados a salarios, deberá presentar el(las) contrato(s) con los que acredite el régimen de contratación, así como escrito libre en el que manifieste que no se encuentra obligado a inscribirse ante el IMSS debido a tal situación, por lo que no puede obtener la opinión de cumplimiento de obligaciones en materia de seguridad social.

Para efectos de lo anterior, el licitante deberá presentar un escrito en el que manifieste bajo protesta de decir verdad si se encuentra o no subcontratando algún servicio u obra especializada para llevar a cabo sus operaciones cotidianas, en el cumplimiento de su objeto social o para la prestación de servicios y/o enajenación de bienes que pretende realizar en favor del IMSS, utilizando el **Anexo 20** que se adjunta a la presente Convocatoria.

En caso de que el licitante se encuentre inscrito en el Registro Único de Proveedores y Contratistas de CompraNet, deberá remitir únicamente la documentación referida en los incisos: f), g), h) i).

En caso de proposición conjunta, los documentos a que se hace referencia en párrafos anteriores, deberán presentarlos por cada uno de los integrantes del consorcio a quien se le haya adjudicado el contrato.

Los licitantes podrán presentar como parte de su propuesta, los documentos que se indican en el numeral 3.12, apartado de "Ambos", sin que su incumplimiento u omisión afecten la solvencia de su proposición, a excepción de los documentos marcados en los incisos d) y e), dado que éstos documentos se incluyen en el numeral 4 de la Convocatoria.

4. REQUISITOS QUE LOS LICITANTES DEBEN CUMPLIR Y QUE SU INCUMPLIMIENTO, AUSENCIA U OMISIÓN AFECTAN LA SOLVENCIA DE LA PROPOSICIÓN Y MOTIVARÁ SU DESECHAMIENTO.

4.1. Firma electrónica.

Con fundamento en los artículos 26 Bis fracción II y 34 de la LAASSP, el licitante deberá remitir a través del sistema CompraNet, la documentación legal, las propuestas técnica y económica firmadas con la firma electrónica avanzada del licitante que emite el SAT para el cumplimiento de sus obligaciones fiscales.

La falta de firma electrónica en su proposición será motivo de desechamiento, pues afecta la solvencia de la misma. En caso de propuestas conjuntas, la proposición deberá ser firmada electrónicamente por aquel consorciado designado en el convenio como representante común.

La revisión de la firma electrónica corresponde al área contratante.

4.2. Documentación distinta a la proposición (legal-administrativa).

El licitante deberá presentar los siguientes documentos, para lo cual podrá hacer uso de los anexos que se le proporcionan y que se indican a continuación:



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

4.2.1. Escrito de acreditación legal y personalidad jurídica del licitante.

Escrito **bajo protesta de decir verdad** que cuenta con facultades suficientes para comprometerse por sí o por su representada, de acuerdo con el **Anexo 3** de la presente convocatoria que se adjunta para tal efecto, o en escrito libre siempre que cumpla con los requisitos del artículo 48, fracción V del Reglamento. (La cual podrán acompañar de una copia simple por ambos lados de su identificación oficial vigente con fotografía (cartilla del servicio militar nacional, pasaporte, credencial para votar o cédula profesional, tratándose de personas físicas, y en el caso de personas morales, de la persona que firme la propuesta).

4.2.2. Escrito de nacionalidad mexicana.

Escrito **bajo protesta de decir verdad**, que el licitante es de nacionalidad mexicana, de acuerdo con el **Anexo 4** de la presente convocatoria que se adjunta para tal efecto.

4.2.3. Escrito de Cumplimiento de normas.

No aplica.

4.2.4. Escrito de no encontrarse en los supuestos de los artículos 50 y 60 de la LAASSP.

Escrito **bajo protesta de decir verdad**, que no se ubica en los supuestos establecidos en los artículos 50 y 60 de la LAASSP, de acuerdo con el **Anexo 6** de la presente convocatoria que se adjunta para tal efecto.

4.2.5. Declaración de integridad.

Escrito en el que el licitante manifieste, **bajo protesta de decir verdad** que se abstendrán de adoptar conductas, por si o a través de interpósita persona, para que los servidores públicos del IMSS induzcan o alteren las evaluaciones de las propuestas, el resultado del procedimiento u otros aspectos que otorguen condiciones más ventajosas con relación a los demás participantes, de acuerdo con el **Anexo 7** de la presente convocatoria que se adjunta para tal efecto.

4.2.6. Escrito de estratificación de MIPYME.

En su caso, escrito **bajo protesta de decir verdad** que el licitante cuenta con estratificación como micro, pequeña o mediana empresa, de acuerdo con el **Anexo 8** de la presente convocatoria que se adjunta para tal efecto.

En caso de no clasificarse en dicha estratificación, los licitantes no están obligados a presentar el formato citado, o bien, a presentar un escrito libre en el que manifieste que no se ubica en la misma.

4.2.7. Convenio de participación conjunta.

En caso de presentar propuesta conjunta, cada una de las personas agrupadas deberá



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

presentar en forma individual los siguientes documentos: Escrito de acreditación legal y personalidad jurídica (**Anexo 3**), Manifestación de Nacionalidad Mexicana (**Anexo 4**), Escrito de no encontrarse en los supuestos de los artículos 50 y 60 de la LAASSP (**Anexo 6**), Declaración de Integridad (**Anexo 7**) y en su caso el Escrito de Estratificación de las micro, pequeñas y medianas empresas (**Anexo 8**).

En caso de que se presente proposición conjunta, y no se presente el convenio de participación conjunta o el presentado no cumpla con las disposiciones legales y reglamentarias, afecta la solvencia de la propuesta y motivará su desechamiento.

En caso de que el licitante no se ubique dentro de este supuesto, no será necesario integrar a su proposición el **citado escrito**, ni incluir escrito en el cual manifieste tal condición, lo cual no será considerado como causal de desechamiento.

4.2.8. Escrito de aceptación de las disposiciones del sistema CompraNet.

Escrito libre en el que manifieste su aceptación de que se tendrán como no presentadas sus proposiciones y, en su caso, la documentación requerida, cuando el archivo electrónico en el que se contengan las proposiciones y/o demás información no pueda abrirse por tener algún virus informático o por cualquier otra causa ajena al IMSS, en términos de lo dispuesto por el numeral 29 del “Acuerdo por el que se establecen las disposiciones que deberán observar para la utilización del sistema electrónico de información pública gubernamental, denominado CompraNet”.

La evaluación de la documentación legal-administrativa será realizada por el Área Contratante, de conformidad con el numeral 4.39 primer párrafo de las POBALINES, así como el numeral 4.2.2.1.15 del Manual, verificando que la documentación presentada por el licitante cumpla con los requisitos solicitados, así como los que se deriven del acto de la Junta de Aclaraciones.

En caso de que se presente proposición conjunta, se verificará que el convenio presentado, cumpla con la información señalada en los artículos 34 de la LAASSP y 44 del RLAASP. El área contratante evaluará los términos legales del convenio, y el área técnica, la descripción de las partes objeto del contrato que corresponderá cumplir a cada integrante, en términos del numeral 4.2.2.1.15 del Manual.

4.3. Propuesta técnica.

La evaluación técnica será realizada por el Área técnica y/o requirente, de conformidad con el artículo 2, fracciones II y III del Reglamento, así como de los numerales 4.25, inciso e) y 4.39 primer párrafo de las POBALINES, así como del numeral 4.2.2.1.16 del Manual.

La propuesta técnica deberá incluir la **descripción amplia y detallada del servicio**, para lo cual el licitante deberá cumplir con las especificaciones contenidas en el **Anexo 1.- Anexo Técnico**, así como con el **Anexo 2.- Términos y Condiciones** de la presente convocatoria, y anexar a su propuesta los documentos solicitados en dichos anexos, considerando el resultado de la Junta de Aclaraciones.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Los licitantes, para la presentación de su propuesta técnica, deberán ajustarse estrictamente a los requisitos y especificaciones previstos en el **Anexo 1.- Anexo Técnico**, describiendo en forma amplia y detallada el servicio que esté ofertando, así como lo señalado por el **Anexo 2.- Términos y Condiciones**, lo anterior para que sus proposiciones se declaren solventes técnicamente.

Deberá estar foliada y con firma electrónica avanzada del licitante, que emite el SAT para el cumplimiento de sus obligaciones fiscales.

La falta de presentación de la documentación o su incumplimiento afecta la solvencia de la propuesta y motivará su desechamiento.

Sólo después de haber cumplido con estos requisitos, se proceda a la asignación de puntos de acuerdo a la Matriz de puntos establecida en el **numeral 6.1.1** de la convocatoria.

4.4. Propuesta económica.

El licitante deberá presentar su propuesta económica debidamente requisitada, considerando el resultado de la Junta de Aclaraciones, para lo cual podrá hacer uso del **Anexo 9** de la presente convocatoria; en caso de no hacer uso del citado anexo, el documento que se remita, deberá contener los mismos datos solicitados en el referido anexo, la cual deberá estar foliada y con firma electrónica avanzada del licitante, que emite el SAT para el cumplimiento de sus obligaciones fiscales.

Los servicios objeto de esta licitación deberán cotizarse en pesos mexicanos.

La falta de presentación de la documentación o su incumplimiento afecta la solvencia de la propuesta y motivará su desechamiento.

La información capturada en el sistema CompraNet no será objeto de evaluación.

La evaluación económica será realizada por el Área Contratante, con el apoyo en su caso, del área técnica/requirente, de conformidad con los numerales 4.39, primero y segundo párrafos de las POBALINES y 4.2.2.1.17 del Manual, considerando el resultado de la Junta de Aclaraciones.

4.5 Indicaciones.

El IMSS podrá verificar la autenticidad o veracidad de los documentos solicitados, para asegurarse del cumplimiento de los requisitos establecidos y, que la descripción de los servicios ofertados sean acordes a lo solicitado en las especificaciones técnicas de acuerdo al **Anexo 1.- Anexo Técnico** de la presente Convocatoria, así como que los licitantes no estén impedidos para participar en esta Licitación.

4.6. Documentos que no afectan la solvencia de la proposición y su omisión no será causa de desechamiento:

a. Escrito para solicitar la clasificación de la información entregada por el licitante.

Escrito mediante el cual el licitante deberá indicar si en los documentos que proporciona



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

al IMSS se contiene información de carácter confidencial o comercial reservada, señalando los documentos o las secciones de éstos que la contengan, así como el fundamento y motivación por los cuales considera que tengan ese carácter, conforme al numeral 13 de la presente convocatoria y **Anexo 11** Información Reservada y Confidencial. Cabe señalar que de no clasificarse la información por parte del Licitante en los términos señalados, o no señalar motivo y fundamento de la clasificación, la información presentada como parte de su proposición técnica, legal y económica tendrá tratamiento de información de carácter público de conformidad con el artículo 113, fracción III de la Ley Federal de Transparencia y Acceso a la Información Pública así como el numeral Cuadragésimo del “ACUERDO del Consejo Nacional del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, por el que se aprueban los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas” publicado en el Diario Oficial de la Federación el día 15 de abril del 2016.

b. Declaración de No Colusión Comisión Federal de Competencia Económica.

Escrito mediante el cual el licitante manifieste una declaración de integridad que conoce la Ley Federal de Competencia Económica. **Anexo 17**.

Este escrito es a sugerencia de la Comisión Federal de Competencia Económica, siendo optativo al licitante la presentación del mismo.

c. Protocolo de actuación en materia de contrataciones públicas y otorgamiento y prórroga de licencias, permisos, autorizaciones y concesiones.

A fin de fomentar las mejores prácticas en la prevención de conflictos de interés, los particulares podrán formular el manifiesto señalado en los numerales 2 y 3 del Anexo Segundo del Acuerdo por el que se expide el “Protocolo de Actuación en materia de Contrataciones Públicas y Otorgamiento y Prórroga de Licencias, Permisos, Autorizaciones y Concesiones”, para personas físicas o, en su caso, para personas morales, el cual podrá realizarse a través de la dirección electrónica www.gob.mx/sfp, siendo este medio electrónico de comunicación el único para presentarlo. El Sistema generará un acuse de presentación del manifiesto, mismo que será necesario presentar como parte de su proposición, de conformidad con la Guía de Operación del Sistema del Manifiesto de los Particulares, disponible en la misma dirección electrónica, lo anterior en términos del numeral 14 de la presente Convocatoria.

d. Manifiesto de conocer y registrarse en el módulo de formalización de instrumentos jurídicos

Declaración escrita en papel membretado por parte del licitante respecto a que conoce y se estará a lo establecido en los artículos tercero, cuarto y demás aplicables del ACUERDO por el que se incorpora como un módulo de CompraNet la aplicación denominada Formalización de Instrumentos Jurídicos y se emiten las Disposiciones de carácter general que regulan su funcionamiento, publicado en el Diario Oficial de la Federación el pasado 18 de septiembre de 2020, donde se determina que todo instrumento jurídico que derive de algún procedimiento de contratación realizado por las Dependencias y Entidades, se



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

deberá utilizar la firma electrónica avanzada (e.firma) que emite el Servicio de Administración Tributaria como medio de identificación. (**Anexo 22**).

5. CAUSALES EXPRESAS DE DESECHAMIENTO.

De conformidad con el artículo 29, fracción XV de la LAASSP, a continuación, se enlistan las causas expresas de desechamiento:

- 5.1** El incumplimiento de alguno de los requisitos establecidos en la convocatoria a la Licitación Pública Nacional Electrónica contenidos en los numerales **4.1, 4.2, 4.3 y 4.4**, que con motivo de dicho incumplimiento se afecte la solvencia de la proposición.
- 5.2** Cuando el licitante incurra en cualquier violación a las disposiciones de la LAASSP, a su Reglamento o a cualquier ordenamiento legal o normativo **vinculado a este procedimiento**.
- 5.3** Si se comprueba que algún licitante ha acordado con otro u otros elevar el costo de las partidas objeto de la presente convocatoria, o cualquier otro acuerdo que tenga como fin obtener una ventaja sobre los demás licitantes.
- 5.4** La falta de presentación o incumplimiento de los escritos o manifestaciones bajo protesta de decir verdad, previstos en la LAASSP o el Reglamento que se soliciten como requisito de participación en la presente convocatoria será motivo de desechamiento, por incumplir las disposiciones jurídicas que los establecen, conforme al artículo 39 penúltimo párrafo del Reglamento.
- 5.5** Cuando la información proporcionada en cumplimiento del numeral 4.2, discrepe o no corresponda, resulte incompleta o incongruente a la proporcionada en el **Anexo 3**. (Acreditación legal y personalidad jurídica del licitante).
- 5.6** En caso de que el licitante no cotice la totalidad de la partida conforme a las condiciones y características solicitadas en la presente convocatoria.
- 5.7** Que el licitante presente más de una propuesta técnica y/o económica para la misma partida.
- 5.8** En caso de que la propuesta técnica y/o económica no cuente con la firma electrónica, establecida por la Secretaría de la Función Pública como medio de identificación electrónica, es decir, la firma electrónica avanzada que emite el SAT para el cumplimiento de obligaciones fiscales del licitante. Se tendrá como no firmada la proposición cuando en alguno de los campos de CompraNet denominados "Anexo Requerimiento técnico Firmado Digitalmente" y/o "Anexo Requerimiento Económico Firmado Digitalmente" se aprecie el mensaje: "*sin archivo adjunto*".
- 5.9** Cuando la firma electrónica de la proposición técnica y/o económica no sea válida. Se considerará como no valida la firma electrónica cuando en el campo "Resultado de la verificación de firma electrónica" del Informe sobre la firma digital generado por



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

CompraNet se aprecie la leyenda “Archivo con Firma Digital No Valido”.

- 5.10** Cuando la firma electrónica de la propuesta sea de una persona diversa al licitante. Se considerará que la firma electrónica de la propuesta es de persona diversa al licitante cuando en el campo “Titular del certificado de firma electrónica” del Informe sobre la firma digital generado por CompraNet aparezca una razón social o un nombre de persona física distinto al del licitante que envía la proposición por CompraNet.
- 5.11** Tratándose de propuestas conjuntas, cuando la proposición no sea firmada electrónicamente por el integrante del consorcio designado como representante común. Se considerará que la propuesta no se encuentra firmada electrónicamente por el representante común del consorcio cuando el nombre (personas físicas) o la razón social (personas morales) del consorciado designado como representante común en el convenio señalado en el numeral 3.6 de la presente convocatoria no sea el que aparezca en el campo “Titular del certificado de firma electrónica” del Informe sobre la firma digital generado por CompraNet.
- 5.12** En caso de que las empresas se encuentren dentro de alguno de los supuestos de los artículos 50 y 60 de la LAASSP.
- 5.13** Cuando sólo se presente la propuesta técnica y no se presente la propuesta económica que oferte, o viceversa.
- 5.14** En caso de que los documentos que envíen los licitantes a través de la plataforma CompraNet no sean legibles, imposibilitando el análisis integral de la proposición, y esto conlleve a un faltante o carencia de información que afecte la solvencia de la proposición.
- 5.15** En caso de que la propuesta económica mejor evaluada de la partida de que se trate supere el presupuesto autorizado y no haya la posibilidad de reducir las cantidades de servicios materia de la licitación hasta por un 10%, o para no reasignar recursos a fin de cubrir el faltante, cuando así se determine, en términos del artículo 56 del Reglamento.
- 5.16** Cuando la proposición conjunta incumpla con lo indicado en los numerales 3.6 y/o 4.2.7 de esta convocatoria, debiendo cumplir con lo establecido en los artículos 44 y 48, fracción VIII, del Reglamento.
- 5.17** En el caso de proposiciones conjuntas, no presentar el convenio correspondiente, o éste no cumpla con lo establecido en el artículo 34 de la LAASSP y 44 del Reglamento.
- 5.18** Que la propuesta técnica no alcance el mínimo de 45 puntos de los 60 puntos disponibles en la evaluación técnica.
- 5.19** Cuando no cumplan con alguno de los requisitos y/o anexos de la Convocatoria, así como los que se deriven de la Junta de Aclaraciones, y que con motivo de dicho incumplimiento se afecte directamente la solvencia de la propuesta, conforme a lo previsto en el último párrafo del Artículo 36 de la LAASSP.
- 5.20** Cuando exista discrepancia entre lo ofertado en la propuesta técnica con lo ofertado en la



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

propuesta económica, en lo referente a la descripción del servicio o en cualquiera de sus características.

- 5.21** Cuando la propuesta económica presente precios escalonados o condicionados.
- 5.22** Cuando se presente la omisión en la presentación de alguna de las cartas compromisos requeridas que afecten la solvencia.
- 5.23** Si el licitante envía su proposición en fecha u hora posterior a la señalada o por medio distinto a CompraNet.
- 5.24** Que no se puedan abrir los archivos del licitante, por contener virus informáticos o por cualquier causa técnica imputable a estos, en términos del numeral 29 del "ACUERDO por el que se establecen las disposiciones que se deberán observar para la utilización del Sistema Electrónico de Información Pública Gubernamental denominado CompraNet".
- 5.25** No manifestar la partida respecto de la cual es su voluntad participar.
- 5.26** La falta absoluta de folio en los documentos que integran la proposición, cuando se constate que no mantienen continuidad en las hojas que integran la proposición y ello implique no contar con la información suficiente que le permita a la convocante evaluarla y determinar la solvencia de la proposición.
- 5.27** Si las propuestas no se presentan el idioma español, así como los anexos técnicos, certificados, diplomas y folletos del servicio ofertado por el licitante que se presenten en el idioma del país de origen de los servicios que se oferta y no acompañen la traducción simple al español.
- 5.28** Cuando no exista correspondencia, resulten incompletos o incongruentes los datos asentados en su propuesta económica **Anexo 9**.
- 5.29** Cuando presenten la propuesta económica en moneda extranjera, sin que lo haya permitido la Convocatoria.

Para estos casos se incluirán las observaciones que correspondan en el acta respectiva al acto de fallo.

Nota: De conformidad con el artículo 36 de la LAASSP, quedan comprendidos entre los requisitos cuyo incumplimiento por sí mismos no afecten la solvencia de la propuesta los siguientes: proponer un plazo de entrega menor al solicitado en cuyo caso prevalecerá el estipulado en la convocatoria; omitir aspectos que puedan ser cubiertos con información contenida en la propia propuesta técnica o económica; no observar los formatos establecidos si se proporciona de manera clara la información requerida y no observar requisitos que carezcan de fundamento legal o cualquier otro que no tenga por objeto determinar objetivamente la solvencia de la propuesta presentada. En ningún caso podrán suplirse las deficiencias sustanciales de las propuestas presentadas.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

6. CRITERIOS ESPECÍFICOS CONFORME A LOS CUALES SE EVALUARÁN LAS PROPOSICIONES.

6.1 Evaluación de la propuesta técnica.

Con fundamento en lo dispuesto por el artículo 36 Bis fracción I de la LAASSP y 52 del Reglamento; el Capítulo Segundo, Sección Cuarta en su Décimo Lineamiento, del Acuerdo por el que se emiten diversos Lineamientos en Materia de Adquisiciones, Arrendamientos y Servicios y de Obras Públicas y Servicios Relacionados con las Mismas, publicado en el Diario Oficial de la Federación el 9 de septiembre de 2010; el Criterio TU-01/2012 emitido por la Secretaría de la Función Pública el 9 de enero de 2012; **el criterio de evaluación que se utilizará será el de PUNTOS**, considerando exclusivamente los requisitos y condiciones establecidos en la Convocatoria y en el numeral **6.1.1 “Matriz de Puntos”**, considerando el resultado de la Junta de Aclaraciones, a efecto de que se garantice satisfactoriamente el cumplimiento de las obligaciones respectivas.

El puntaje mínimo para considerar que una propuesta técnica es solvente es de al menos 45 puntos de los 60 puntos máximos que se pueden obtener en esta evaluación, de lo contrario, serán desecharadas.

El detalle de los documentos con los que se acreditarán los rubros y subrubros, están contenidos en el numeral 6.1.1 “Matriz de Puntos” de esta convocatoria.

La evaluación técnica será realizada por el Área técnica y/o requirente, de conformidad con el artículo 2, fracciones II y III del Reglamento, así como de los numerales 4.25, inciso e) y 4.39 primer párrafo de las POBALINES, así como del numeral 4.2.2.1.16 del Manual.

- En primer término, se verificará si las proposiciones fueron debidamente firmadas electrónicamente, tal como se exige en el Apartado 4. Requisitos que los licitantes deben cumplir y que su incumplimiento, ausencia u omisión afectan la solvencia de la proposición y motivará su desechamiento, numeral 4.1 Firma electrónica, de esta Convocatoria.
- Sólo después de constatar que el o los licitantes firmaron adecuadamente sus proposiciones, se procederá a la evaluación de la documentación distinta a la proposición (legal-administrativa) a que se refiere el Apartado 4. Requisitos que los licitantes deben cumplir y que su incumplimiento, ausencia u omisión afectan la solvencia de la proposición y motivará su desechamiento, numeral 4.2. de la convocatoria.
- Una vez que los licitantes cumplen con el requerimiento anterior, se procederá a la evaluación de los requisitos indispensables, de conformidad con lo previsto en los **Anexos 1.- Anexo Técnico y 2.- Términos y Condiciones**, de esta Convocatoria, considerando el resultado de la Junta de Aclaraciones respectiva.
- Sólo después de advertirse el cumplimiento de los requisitos indispensables establecidos en esta Convocatoria, con base en la puntuación que corresponde a la propuesta técnica de cada licitante, se determinará si resulta solvente, para lo cual deberá obtener una puntuación mínima de 45 puntos de los 60 puntos que se pueden obtener en esta Evaluación.
- En caso de que se presente proposición conjunta, el Área técnica verificará que el convenio



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

presentado contenga la descripción de las partes objeto del contrato que corresponderá cumplir a cada integrante, en términos del numeral 4.2.2.1.15 del Manual, incluyendo dentro de su Dictamen técnico el resultado de dicha revisión.

- Finalmente, de advertirse que las propuestas técnicas evaluadas obtuvieron una calificación igual o superior a 45 puntos, se procederá a realizar la evaluación de las propuestas económicas, de conformidad con lo establecido en el Numeral 6.1.1 Matriz de puntos de esta Convocatoria.

La evaluación final será, la que resulte de sumar los puntos obtenidos en la evaluación técnica y la evaluación económica.

6.1.1 Matriz de Puntos

RUBRO / SUBRUBROS	VALOR EN PUNTOS
I.- CAPACIDAD DEL LICITANTE	24
I a). - Capacidad de los recursos humanos	12.5
I a) 1.- Experiencia: en asuntos relacionados con la materia del servicio objeto del procedimiento de contratación	3.3
I a) 2.- Competencia o habilidad en el trabajo de acuerdo con sus conocimientos académicos o profesionales	7.1
I a) 3.- Dominio de herramientas relacionadas con el servicio	2.1
I b). - Capacidad de los recursos económicos y de equipamiento	10
I b) 1- Capacidad de los recursos económicos	6
I b) 2- Solución de centro de operaciones de seguridad (SOC)	2
I b) 3- Capacidad del SOC del licitante	2
I c). - Participación de discapacitados o empresas que cuenten con trabajadores con discapacidad	0.5
I d). - Participación de MIPYMES	0.5
I e). - Igualdad de género	0.5
II.- EXPERIENCIA Y ESPECIALIDAD DEL LICITANTE	18
II a). - Experiencia: en la prestación de servicios similares a los requeridos en el procedimiento de contratación	9
II b). - Especialidad: Contratos similares a los que se solicitan	9
III.- PROPUESTA DE TRABAJO	12
III a). - Metodología para la prestación del servicio	4
III b). - Plan de trabajo propuesto por el licitante	4
III c). -Esquema estructural de la organización de los recursos humanos <ul style="list-style-type: none"> • Esquema Estructural y Organigrama • Matriz de Escalación 	4
IV.- CUMPLIMIENTO DE CONTRATOS	6
IV a). - Demostración documental de contratos cumplidos satisfactoriamente	6
TOTAL	60



Matriz de Puntos y
Porcentajes SASI 2022



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

6.2 Evaluación de la propuesta económica.

La convocante sólo procederá a realizar la evaluación de las propuestas económicas de aquéllas propuestas cuya oferta técnica resulte solvente por haber obtenido por lo menos 45 puntos.

Para la elaboración de la propuesta económica se adjunta el **Anexo 9** a la presente Convocatoria.

El cálculo de la puntuación económica tendrá un valor máximo de 40 puntos, de tal manera que aquella propuesta técnicamente solvente que oferte en su propuesta económica el precio más bajo, obtendrá 40 puntos y al resto de los licitantes se hará el reparto proporcional.

Cuando se detecte un error de cálculo en alguna propuesta, se podrá llevar a cabo su rectificación cuando la corrección no implique la modificación del precio unitario.

En caso de discrepancia entre las cantidades escritas con letra y número, prevalecerá la primera, asimismo, de presentarse errores en las cantidades o volúmenes solicitados, estos podrán corregirse, en apego al artículo 55 del Reglamento.

No se considerarán las proposiciones, cuando no cotice la totalidad de la partida requerida.

Para determinar la puntuación que corresponda a la oferta económica de cada participante, se aplicará la siguiente fórmula:

$$PPE = MPemb \times 40 / MPI.$$

Donde:

PPE = Puntuación que corresponden a la oferta económica;

MPemb = Monto de la oferta económica más baja, y

MPI = Monto de la i-ésima oferta económica;

Calificación final

Para calcular la calificación final se aplicará la siguiente fórmula:

$$PTj = TPT + PPE \text{ Para toda } j = 1, 2, \dots, n$$

Donde:

PTj = Puntuación total de la propuesta;

TPT = Total de puntuación asignada a la oferta técnica;

PPE = Puntuación asignada a la oferta económica, y

El subíndice "j" representa a las demás propuestas determinadas como solventes como resultado de la evaluación.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

La suma de todos los rubros con sus correspondientes subrubros en la evaluación técnica representa 60 puntos, a la Propuesta Económica le corresponden los restantes 40 puntos.

La evaluación económica será realizada por el Área Contratante, con el apoyo en su caso, del área técnica/requirente, de conformidad con los numerales 4.39, segundo párrafo de las POBALINES y 4.2.2.1.17 del Manual, considerando el resultado de la Junta de Aclaraciones.

7. ADJUDICACIÓN DE CONTRATO.

El contrato será adjudicado al licitante cuya oferta resulte solvente porque cumple con los requisitos legales, técnicos y económicos de la presente convocatoria y obtenga el mayor número de puntos combinado de la propuesta técnica y la económica, de conformidad con el artículo 36 Bis fracción I de la LAASSP.

En caso de existir empate en dos o más proposiciones, se dará preferencia en primer término a las micro empresas, a continuación se considerará a las pequeñas empresas y en caso de no contarse con alguna de las anteriores empresas, la adjudicación se efectuará a favor del licitante que tenga el carácter de mediana empresa.

De no actualizarse el supuesto anterior se realizará la adjudicación del contrato a favor del licitante que resulte ganador del sorteo por insaculación que realice la convocante, en presencia del representante del OIC, conforme el artículo 54 del Reglamento.

8. DECLARACIÓN DESIERTA DE LA LICITACIÓN.

La convocante procederá a declarar desierta, de conformidad con lo establecido en los artículos 38 de la LAASSP y 58 del Reglamento a la Licitación cuando:

- La totalidad de las proposiciones presentadas no reúnan los requisitos solicitados;
- No se presenten proposiciones en el Acto de Presentación y Apertura.

9. CANCELACIÓN DE LA LICITACIÓN, PARTIDA(S), O CONCEPTOS INCLUIDOS EN ÉSTA.

Con fundamento en el artículo 38 de la LAASSP, la Convocante podrá cancelar la presente licitación, o partida(s) o concepto, incluidos en ésta, por caso fortuito o fuerza mayor; de igual manera se podrá cancelar cuando existan circunstancias debidamente justificadas que provoquen la extinción de la necesidad, o que de continuarse con el procedimiento de contratación se pudiera ocasionar un daño o perjuicio al IMSS, previo a la comunicación del fallo por parte del Área requirente/técnica.

10. INCONFORMIDADES.

De acuerdo con lo dispuesto en artículo 66 de la LAASSP, los licitantes podrán interponer inconformidad en las oficinas de la SFP ubicadas en Avenida de los Insurgentes Sur número 1735, Colonia Guadalupe Inn, Código Postal 01020, Demarcación Territorial Álvaro Obregón, en la Ciudad de México, México.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

O bien ante el OIC en el IMSS ubicado en. Avenida Revolución número 1586, Colonia San Ángel, Demarcación Territorial Álvaro Obregón, Código Postal 01000, en la Ciudad de México, México.

Asimismo, se señala que tales inconformidades podrán presentarse mediante el sistema CompraNet en la dirección electrónica www.compranet.hacienda.gob.mx. (cnet@hacienda.gob.mx) Lo anterior, contra actos del procedimiento de contratación que contravengan las disposiciones que rigen las materias objeto del mencionado ordenamiento.

11. OPERACIÓN DE COMPRANET.

Para aclarar dudas con relación a la operación de CompraNet (Presentación de solicitudes de aclaración, envío y firma electrónica de proposiciones, consulta de actas y documentos publicados por la Unidad Compradora, etc.), los licitantes podrán dirigirse al correo rupc@hacienda.gob.mx o al Centro de Atención Telefónico (CAT): 5536881977 de lunes a viernes de 9:00 AM a 6:00 PM (Ciudad de México).



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

12. FORMATOS QUE FACILITARÁN Y AGILIZARÁN LA PRESENTACIÓN Y RECEPCIÓN DE LAS PROPOSICIONES.

Número	Descripción
Anexo 1	Anexo Técnico
Anexo 2	Términos y Condiciones.
Anexo 3	Escrito de acreditación legal y personalidad jurídica del licitante.
Anexo 4	Escrito de nacionalidad mexicana.
Anexo 5	Escrito de cumplimiento de Normas NO APLICA
Anexo 6	Escrito de no encontrarse en los supuestos de los artículos 50 y 60 de la LAASSP.
Anexo 7	Declaración de integridad.
Anexo 8	Escrito de estratificación de MIPYME.
Anexo 8 Bis	Instructivo de llenado Estratificación de micro, pequeña o mediana empresa (MIPYMES).
Anexo 9	Propuesta Económica
Anexo 10	Relación de documentos a presentar.
Anexo 11	Escrito para solicitar la clasificación de la información entregada por el licitante.
Anexo 12	Escrito de manifestación que no desempeña empleo, cargo o comisión en el servicio público o, en su caso, que a pesar de desempeñarlo, con la formalización del contrato correspondiente no se actualiza un conflicto de interés.
Anexo 13	Manifestación de Interés en participar
Anexo 13.1	Formato de solicitud de aclaraciones.
Anexo 14	Modelo de Contrato.
Anexo 15	Modelo de convenio de proposición conjunta.
Anexo 16	Nota informativa para participantes de países miembros de la Organización para la Cooperación y el Desarrollo Económico (OCDE).
Anexo 17	Declaración de No Colusión Comisión Federal de Competencia Económica.
Anexo 18	Modelo de fianza
Anexo 19	Carta de autorización 32-D
Anexo 20	Manifestación de servicios especializados
Anexo 21	Escrito de aceptación de las disposiciones del sistema CompraNet
Anexo 22	Manifiesto de conocer y registrarse en el Módulo de Formalización de Instrumentos Jurídicos

13. INFORMACIÓN RESERVADA Y CONFIDENCIAL.

Se hace del conocimiento del licitante, que en términos de lo dispuesto por los artículos 97, 98, 110 fracción XIII, 111 y 113 de la Ley Federal de Transparencia y Acceso a la Información Pública, deberá indicar si en los documentos que proporcionan al IMSS contiene información de carácter confidencial o comercial reservada, señalando los documentos o las secciones de éstos que la contengan, así como el fundamento por el cual considera que tengan ese carácter, para lo cual se anexa el formato **Anexo 11**.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

14. PROTOCOLO DE ACTUACIÓN EN MATERIA DE CONTRATACIONES PÚBLICAS Y OTORGAMIENTO Y PRÓRROGA DE LICENCIAS, PERMISOS, AUTORIZACIONES Y CONCESIONES.

Se hace del conocimiento de los licitantes que en el presente procedimiento se observará el Protocolo de Actuación en materia de Contrataciones Públicas y Otorgamiento y Prórroga de Licencias, Permisos, Autorizaciones y Concesiones contenido en el Acuerdo por el que se expidió el mismo, publicado en el Diario Oficial de la Federación el 20 de agosto de 2015, modificado mediante los similares de fecha 19 de febrero de 2016 y 28 de febrero de 2017, mismo que puede ser consultado en la sección de la Secretaría de la Función Pública, en el portal de la Ventanilla Única Nacional (gob.mx) a través de la liga www.gob.mx/sfp. En ese sentido se informa que los datos personales que se recaben con motivo del contacto con particulares serán protegidos y tratados conforme las disposiciones jurídicas aplicables.

Asimismo, de conformidad con el numeral 2 del Anexo Segundo del referido Acuerdo se hace de conocimiento a los interesados en participar en el presente procedimiento que, tratándose de personas físicas, podrán formular un manifiesto en el que afirmen o nieguen los vínculos o relaciones de negocios, laborales, profesionales, personales o de parentesco por consanguinidad o afinidad hasta el cuarto grado que tenga la propia persona con el o los servidores públicos siguientes:

I. Presidente de la República; II. Secretarios de Estado; III. Jefe de la Oficina de la Presidencia de la República; IV. Consejero Jurídico del Ejecutivo Federal; V. Procurador General de la República; VI. Titulares de entidades; VII. Titulares de órganos reguladores coordinados; VIII. Subprocuradores o Titulares de Fiscalías Especializadas; IX. Comisionados adscritos a órganos reguladores coordinados; X. Subsecretarios, oficiales mayores, consejeros adjuntos, titulares de órganos administrativos desconcentrados, titulares de unidad y directores generales en las dependencias; XI. Directores generales, gerentes, subgerentes, directores o integrantes de los órganos de gobierno o de los comités técnicos de las entidades, y XII. Personal que interviene en contrataciones públicas, en el otorgamiento y prórroga de licencias, permisos, autorizaciones y concesiones, incluidos en el Registro que lleva la Secretaría de la Función Pública.

Los particulares personas morales, podrán formular por medio de sus representantes legales un manifiesto en el que afirmen o nieguen los vínculos o relaciones de negocios, laborales, profesionales, personales o de parentesco por consanguinidad o afinidad hasta el cuarto grado que tengan las personas que a continuación se señalan, con el o los servidores públicos señalados en el párrafo que antecede:

- a) Integrantes del consejo de administración o administradores;
- b) Director general, gerente general, o equivalentes;
- c) Representantes legales, y
- d) Personas físicas que posean directa o indirectamente cuando menos el diez por ciento de los títulos representativos del capital social de la persona moral.

En ambos casos, los particulares formularán el manifiesto a través de la dirección electrónica www.gob.mx/sfp siendo este medio electrónico de comunicación el único para presentarlo. El Sistema generará un acuse de presentación del manifiesto, mismo que será necesario presentar como parte de su proposición, de conformidad con la Guía de Operación del Sistema del



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Manifiesto de los Particulares, disponible en la misma dirección electrónica. A través de dicho medio electrónico los particulares podrán también denunciar presuntos conflictos de interés de los que tengan conocimiento, enunciando las pruebas con las que en su caso cuenten.

Por otra parte, se informa que de conformidad con el numeral 10 de dicho Anexo Segundo, los licitantes podrán presentar una declaración de integridad en la que manifiesten, bajo protesta de decir verdad, que por sí mismos o a través de interpósoita persona, se abstendrán de realizar conductas contrarias a las disposiciones jurídicas aplicables.

Finalmente, se informa que los particulares tienen derecho a presentar queja o denuncia por el incumplimiento de las obligaciones que adviertan en el contacto con los servidores públicos, ante el Órgano Interno de Control en el IMSS, o bien, a través del Sistema Integral de Quejas y Denuncias Ciudadanas, establecido mediante el Acuerdo publicado en el Diario Oficial de la Federación el día 9 de diciembre de 2015.

15. NOTA INFORMATIVA OCDE.

Nota informativa para participantes de países miembros de la Organización para la Cooperación y el Desarrollo Económico (OCDE) y firmantes de la Convención para Combatir el Cohecho de Servidores Públicos Extranjeros en Transacciones Comerciales Internacionales.

Esta nota es de carácter informativo por lo que no deberá incluirse en la proposición y no será causal de desechamiento la no presentación de la misma. **Anexo 16.**

Mtra. Elia Sandra Varas Galeana

Titular de la División de Contratación de Activos y Logística

Área contratante

Con fundamento en el numeral 5.3.8, inciso a) de las Políticas, Bases y Lineamientos en Materia de Adquisiciones, Arrendamientos y Servicios del IMSS



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Anexo 1.- Anexo Técnico

1. Objetivo del Documento

Elaborar el documento que contenga los requerimientos y las especificaciones técnicas y de calidad, así como el alcance de la adquisición, arrendamiento o servicio de TIC y SI que se pretenda contratar.

Clasificador Único de las Contrataciones Públicas (CUCOP): 31900004 Servicios a centros de datos (hospedaje, electricidad, video vigilancia, monitoreo, aire acondicionado, servidores y otros).

1.1. Objetivo General

Contar, de manera integrada y unificada, con los servicios administrados mediante dos partidas que garanticen la continuidad operativa, de negocio y de seguridad de la información del IMSS mediante: (1) Toma en operación y transición, (2) servicios de infraestructura que operen, den soporte y mantenimiento a la infraestructura instalada, y que, implementen y gestionen infraestructura para los centros de datos y den la atención a los servicios y aplicaciones con las que cuenta el instituto, (3) servicios que brinden protección a servidores, aplicaciones y bases de datos mediante una solución integral, (4) servicios de seguridad de la información, en materias específicas relacionadas con las tecnologías de la información, comunicaciones y seguridad de la información, incluyendo servicios especializados.

1.2. Objetivos Específicos

- Asegurar y proteger la información Institucional.
- Garantizar la continuidad operativa, de negocio y de la seguridad de la información de la Institución, durante la vigencia del presente contrato, especialmente durante la toma de operación y transición del contrato anterior a los servicios propios de SASI 2022-2024.
- Fortalecer la seguridad de la información de la Institución contra amenazas, disminuyendo el riesgo de sufrir incidentes de seguridad, mediante el uso de tecnología de punta para el monitoreo, detección, aseguramiento, contención y respuesta ante ataques que puedan presentarse en la infraestructura de cómputo, sistemas y aplicaciones del IMSS.
- Contar con servicios de infraestructura regulados por niveles de servicio, que: implementen (instalen, migren, habiliten y pongan a punto) los componentes necesarios en los centros de datos y servicios propios del IMSS y que de forma complementaria gestionen (operen, monitorean, den soporte y mantenimiento preventivo y correctivo) a la correspondiente infraestructura con el propósito de satisfacer las necesidades de: conectividad, comunicación, protección, control y filtrado de la propia Institución, manteniendo la plataforma tecnológica en condiciones óptimas de operación.
- Contar con los servicios de protección de forma unificada e integrada, incluyendo prevención de pérdida de información, protección de computo físico o virtual, protección de correo electrónico externo e interno, herramientas de colaboración y trazabilidad, filtrado e inspección de acceso a internet e intranet, mediante una solución integral que permita una gestión consolidada de las funcionalidades, características y servicios, con el propósito de mantener, asegurar y robustecer el esquema de seguridad del IMSS.
- Contar con servicios de seguridad de la información, que complementen el esquema de seguridad institucional de forma consistente y robusta, con el control, aseguramiento, diagnóstico, pruebas, metodologías, de distintos rubros como el de acceso a cuentas privilegiadas, base de datos, aplicaciones, fuentes múltiples de información para correlación y trazabilidad de eventos, vulnerabilidades, investigación forense y de procesos de seguridad, así como con otros servicios especializados en materia de seguridad y tecnologías de la información.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- Contar con servicios para la gestión del cambio y de soporte extendido que tienen como objetivo coadyuvar en la prestación del resto de los servicios SASI 2022-2024.

2. Alcance

El alcance del SASI 2022-2024 incluye:

- Un esquema de servicios de implementación, gestión y monitoreo de la infraestructura física, de seguridad necesaria para integrar los centros de datos mediante una arquitectura flexible y que responda a las necesidades de migración. Este esquema incluye la operación, soporte y mantenimiento de la infraestructura instalada, así como su potencial substitución, con el fin de mantener una plataforma moderna, y uniforme tecnológicamente, que garantice la continuidad operativa, del negocio y de la seguridad de la información del IMSS.
- Un esquema de servicios de protección con una solución integral que incluya: protección de servicios de colaboración internos, correo externo y navegación web, detecte y proteja contra amenazas avanzadas, prevenga la fuga de información y mediante una gestión consolidada.
- Un esquema de servicios de seguridad que complementen el esquema de protección, mediante servicios orientados a: Firewalls, IPS, Filtrado de Contenido, Anti DDoS, Antispam, WAF, DBF, VPN, así como la implementación y administración de nuevos servicios que requiera el instituto, como son análisis de vulnerabilidades, análisis forense, pruebas de penetración, borrado seguro de información, aseguramiento de aplicaciones, ciberinteligencia (ciberseguridad), servicios de protección en redes inalámbricas y seguridad en dispositivos móviles, servicios de gestión y control de acceso para usuarios privilegiados (AAA), servicio de correlación de eventos, servicio de protección de amenazas persistentes avanzadas (APT), servicios de gestión de procesos de seguridad y servicios especializados en materia de seguridad de la información, de este modo, se tiene un esquema de seguridad completo.

3. Beneficios

Los beneficios que se esperan alcanzar con la prestación de los servicios SASI 2022-2024 se dirigen a garantizar la continuidad de la operación, del negocio y de la seguridad de la información de la propia Institución, fortaleciendo su esquema de infraestructura, comunicaciones, servicios de protección y en servicios especializados en materia de seguridad de la información, contribuyendo al cumplimiento de los objetivos del IMSS; extendiéndose a toda la institución en términos técnicos, protección y servicios especializados como son:

- Contar con una infraestructura física, de seguridad, flexible y escalable; basada en una arquitectura que se adapte oportunamente a las necesidades de migración y a las exigencias para la prestación de los servicios que demanda el IMSS.
- Proporcionar una plataforma tecnológicamente moderna y estandarizada que se mantenga actualizada y en buenas condiciones, para el despliegue oportuno de los servicios que garanticen la continuidad operativa, de negocios y de seguridad de la información del IMSS.
- Contar con un esquema completo de servicios especializados en materia de tecnologías de la información que dé protección tanto a la infraestructura, a los servicios y a los usuarios finales tanto como a aspectos normativos, de procesos, de calidad y de ingeniería entorno a la seguridad de la información.
- Proporcionar los servicios de protección para los usuarios, a través de un esquema desde la red interna y desde la red externa ante los elementos de riesgo y perniciosos que pueden presentarse.
- Garantizar la calidad en la entrega de los servicios de SASI 2022-2024 mediante Acuerdos de Niveles de Servicio elaborados considerando el impacto que genera su no disponibilidad o la no



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

entrega de esos servicios en el esquema de seguridad completo de SASI 2022-2024.

4. Actualización Tecnológica

Como parte de su proceso de evolución tecnológica, el IMSS se reserva el derecho de actualizar las especificaciones de infraestructura, de software y hardware que mantienen los servicios de SASI 2022-2024, toda vez que los activos de infraestructura son susceptibles de integrar mejoras en hardware o software, lo que permite proveer mecanismos de protección adicional conforme la evolución de funcionalidades en materia de seguridad o para aquellos que requieran de una sustitución (por falla) o un reajuste. Por lo tanto, el "LICITANTE" conoce y acepta que el IMSS está en continua evolución tecnológica, por lo que se debe apegar a ella en todo momento.

Como parte de su proceso de evolución tecnológica, el IMSS se reserva el derecho de actualizar las especificaciones de infraestructura, de software y hardware que mantienen los servicios de SASI 2022-2024, con el objetivo de proteger a la Institución de la obsolescencia, conforme a la misma evolución del mercado observando el mapa de ruta de actualización de los componentes, para los servicios SASI 2022-2024, solicitados o para aquellos que requieran de una sustitución (por falla) o un reajuste. Por lo tanto, el "LICITANTE" conoce y acepta que el IMSS está en continua evolución tecnológica, por lo que se debe apegar a ella en todo momento.

El "LICITANTE", tomando en consideración las características del servicio, deberá cumplir con los mecanismos de seguridad de la información o controles que le establezca la Coordinación de Telecomunicaciones y Seguridad de la Información, con la finalidad de garantizar la conservación, integridad, confiabilidad y disponibilidad de los datos que se encuentran en los sistemas tecnológicos del IMSS una vez que haya iniciado la prestación del servicio, en caso de incumplimiento, el "LICITANTE" deberá considerar lo establecido en el apartado de "Penas Convencionales y Deducciones".

El "LICITANTE" efectuará la actualización de cualquier tipo de licencia, componente, dispositivo, parche, arquitectura, etc. siempre y cuando el fabricante de dicho componente haya liberado una versión que lo reemplace por aspectos de seguridad, compatibilidad, fin de soporte, capacidad, error o falla detectada, o similar; con la finalidad de mantener estable y segura la operación de los servicios SASI 2022-2024. Toda actualización o mejora deberá ser consultada y aprobada por el IMSS. Estos mecanismos le garantizarán a la institución que, durante toda la vigencia del contrato, dispondrá de los componentes del servicio que incorporan la versión más avanzada de la tecnología validada, probada y liberada por los fabricantes, para satisfacción de las necesidades del servicio SASI 2022-2024.

Los plazos para llevar a cabo las actualizaciones tecnológicas de nuevas versiones (software) de los componentes relacionados con los servicios de SASI 2022-2024 serán de, por lo menos, seis meses después de su última versión liberada por el fabricante, siempre que el IMSS considere que dicha actualización es conveniente para alcanzar los objetivos de SASI 2022-2024 y del propio IMSS, durante la vigencia del contrato, buscando reducir el riesgo e impacto a la operación, al ejecutar estas actualizaciones siempre se deberá contar con un documento de recomendaciones y riesgos generado por los ingenieros del fabricante al igual se deberá contar con apoyo del centro de asistencia técnica del fabricante durante las ventanas de ejecución de cambios.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

5. Requerimientos del servicio

Los Servicios requeridos y que deberán ser parte de la solución propuesta, se desagregan por partida, mismos que deberán incluir al menos lo siguiente:

Partida 1

1. Servicios de Seguridad - Continuidad Operativa

(Firewalls, IPS, AntiDDoS, Filtrado Web, Filtrado de correo, Firewall de Aplicaciones WEB, Firewall de base de datos, cifrado de información, Control de Accesos, entre otros.), servicios que deberán cumplir con los niveles de servicio establecidos para que de manera inmediata y en donde lo requiera el Instituto se continue con la operación. Estos servicios serán bajo demanda a petición expresa del instituto, así como los tiempos de entrega serán conforme al sitio y dependiendo del tipo de tecnología en una modalidad de alta disponibilidad (HA), así como los niveles de servicios requeridos tanto para la implementación, como la operación, incluyendo los temas de soporte y resolución de problemas e incidentes.

2. Servicios de Seguridad – Verificación y Calidad

Consiste en los requerimientos necesarios para que los servicios de calidad de la Seguridad de la Información se continúen, como son, aseguramiento de aplicaciones, cumplimiento normativo, herramientas de seguridad, ciberinteligencia, protección de datos, protección de redes inalámbricas, seguridad de dispositivos móviles y de escritorio, control de acceso a la red, aseguramiento de cuentas privilegiadas, gestión de dominios, administración de certificados digitales, así como los niveles de servicio requeridos en la operación, incluyendo el soporte y resolución de problemas e incidentes.

3. Servicios del Centro de Operaciones de Seguridad (SOC)

El Instituto requiere que el proveedor del servicio cuente con un Centro de Operaciones de Seguridad (SOC), que se encuentre físicamente en las instalaciones del proveedor. El objetivo de este centro deberá de ser la continuidad de la gestión de la seguridad y responsable de la administración, operación, monitoreo, soporte y atención a fallas de los componentes de las soluciones de seguridad, la ejecución de actividades de revisiones de seguridad, correlación de eventos, monitoreo de servicios, administración de bitácoras, atención y respuesta a incidentes, análisis forense, análisis de ciberamenazas avanzadas, auditoría de reglas de acceso, notificación de alertas y vulnerabilidades, así como el establecimiento de acciones de mejora sustentable, la gestión del centro de operaciones de seguridad, parches y actualizaciones de las firmas de las soluciones de seguridad, que opere 7x24x365. El SOC deberá acreditarse con presentación de la copia simple del certificado ISO/IEC27001:2013 e ISO/IEC20000-1:2018 vigentes a nombre del licitante.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Partida 2

1. Análisis de Vulnerabilidades Estático

El instituto requiere la continuidad de servicios de análisis de vulnerabilidades estáticos (aseguramiento de aplicaciones) que permitan atender a la protección de vulnerabilidades nuevas o conocidas, que representen una riesgo, en lo que a seguridad de la información se refiere, en el desarrollo de aplicaciones en sus diferentes etapas de construcción.

2. Análisis de Vulnerabilidades Dinámico

El instituto requiere la continuidad de servicios de análisis de vulnerabilidades dinámicos que permitan atender a la protección de vulnerabilidades nuevas o conocidas, que representen un riesgo, en lo que a seguridad de la información se refiere, en todos aquellos activos de infraestructura que dan soporte a las aplicaciones y sistemas informáticos.

3. Servicios de Análisis Forense

El Instituto requiere la continuidad de un servicio de análisis de incidentes de seguridad para determinar y documentar a través de la integración de registros o bitácoras las evidencias o indicios de eventos y su relación en el tiempo que identifiquen cuando ocurrió, que infraestructura, servicios tecnológicos o sistema de información fueron comprometidos, como fue realizado, y quien o que, estuvo relacionado con el incidente y el impacto del evento.

4. Servicios de Pruebas de Penetración

El Instituto requiere la continuidad de un servicio que permita realizar un proceso sistemático para comprobar las vulnerabilidades de las aplicaciones y la infraestructura que la soportan, con el propósito de buscar huecos o fallas en la seguridad.

Los servicios objeto de esta contratación se adjudicarán por **partida** a un solo licitante, cuya proposición cumpla con la totalidad de los requisitos de cumplimiento obligatorio; y haya obtenido la mayor puntuación en la evaluación combinada de puntos o porcentajes conforme a lo siguiente:

Por la naturaleza técnica de los servicios del SASI 2022-2024, en el caso de las partidas 1 y 2, los licitantes únicamente podrán participar en una de las dos partidas, lo anterior para evitar conflicto de interés técnico en detrimento del IMSS.

En este sentido, se hace del conocimiento de los Licitantes que, derivado de la naturaleza de los servicios y por sus características técnicas, bajo ningún escenario se podrá adjudicar las partidas 1 y 2 a un mismo licitante al que se haya asignado una de las 2.

6. Requerimientos del Servicio - Especificaciones Técnicas

Partida 1.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

6.1. Servicios de Seguridad – Continuidad Operativa

6.1.1. Servicios de Firewall

Descripción del servicio: El instituto requiere de la continuidad operativa del servicio que proporciona la seguridad y protección de control de acceso, filtrado y bloqueo contra ataques dirigidos a las aplicaciones e inspección sobre los paquetes a nivel de aplicación para identificar patrones de tráfico anómalo, por lo que el proveedor deberá cumplir con las siguientes especificaciones funcionales mínimas.

- Proporcionar la continuidad operativa de los activos de infraestructura con los que cuenta hoy en día el Instituto o lo que sea necesario implementar, incluyendo el soporte técnico, licenciamiento o lo que se requiera que garantice esta continuidad operativa, así como los niveles de servicio requeridos para este servicio, conforme a lo establecido en el Apéndice B.
- Integrar activos de infraestructura de propósito específico (*Appliances*) con capacidad de expansión bajo demanda, para la continuidad operativa del Instituto, conforme lo dispuesto en el Apéndice A.
- Definir en conjunto con el Instituto la estrategia de habilitación para la continuidad operativa de los activos de infraestructura actuales o aquellos que se requieran como parte de las necesidades operativas de este, conforme lo dispuesto en el Apéndice A y B.
- Llevar a cabo las tareas necesarias para la instalación del equipo en los Centro de Datos correspondientes, o en su caso, aquella otra localidad donde le sea solicitado por el Instituto.
- Acordar con el personal del Instituto, ya sea a través del administrador del contrato o del modelo de gobierno designado para este propósito, las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de *hardware* o *software* que integran el servicio sin un control de cambios autorizado por este último.
- Continuar con la integración de cada activo de infraestructura hacia su respectiva consola de administración centralizada pudiendo ser en modo *stand alone* para la administración de todos los dispositivos, así como garantizar que la bitácora del cada activo quede integrada en la solución de correlación de eventos del proyecto u otra que el Instituto designe para este propósito.
- Garantizar que los activos de infraestructura cuenten con actualización tecnológica, estable y validada, del sistema operativo, aplicación (*firmware*) u otro componente necesario con el que cuente el servicio correspondiente, conforme lo dispuesto en el Apéndice A y B.
- Permitir únicamente el tráfico interno y externo definido por el Instituto entre el punto de conexión central, hacia y desde los diferentes puntos de interconexión con otras redes.
- Continuar con el acceso a servicios ubicados en la capa de servidores de los centros de datos (DMZ), realizando la gestión de acuerdo con el esquema de seguridad y respetando la segmentación definida entre las diversas zonas de seguridad.
- Prevenir la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del Instituto.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- Atender todos los requerimientos de cambio, atención de incidentes/fallas y solicitudes de información que el Instituto genere, apegado a los Niveles de Servicio definidos para dicho propósito.
- Monitorear todos los eventos registrados en la solución, así como emitir alertas de incidentes generados por los activos de infraestructura que compongan el servicio, cumpliendo al menos:
 - Notificar aquellas actividades sospechosas relacionadas con la violación de las políticas, así como aquellas que sean identificadas a través de las funcionalidades habilitadas en la solución.
 - Notificar sobre fallas relacionadas con el *hardware* de los activos de infraestructura provisto a través del servicio.
- Integrar el licenciamiento del *software* que permita continuar con los servicios y activos de infraestructura correspondientes, así como todas aquellas renovaciones necesarias durante la vigencia de los servicios, conforme a lo establecido en el Apéndice B.
- Realizar evaluaciones operativas a los servicios (herramienta de *software* y activos de infraestructura) así como los análisis de vulnerabilidades, que permitan identificar, entre otros, mejoras en el desempeño de los activos, mejoras en la gestión de configuraciones, detección de nuevas funcionalidades operativas derivadas de actualizaciones en versiones de *hardware* y/o *software*; Dichas evaluaciones deberán ejecutarse cada 6 meses, desde el inicio de operaciones de los servicios y hasta 6 meses antes del término de los mismos.
- Realizar las integraciones de conectividad física y lógica que permitan habilitar los servicios descritos en el presente Anexo Técnico tales como, componentes habilitadores de comunicaciones entre redes, cableado eléctrico y de datos, montaje en racks, entre otros.
- Proporcionar al Instituto cuentas de acceso a las consolas de administración del correspondiente servicio, así como herramientas en *software* que permitan acceder a las mismas (aplicaciones cliente-servidor, portales web u otro que se encuentre disponible), las cuales deberán ser de solo lectura, y cuyos atributos de consulta se definirán en las mesas que para este propósito se integren.
- Proporcionar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas para dicha solución, donde se pueda consultar información sobre los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimientos vigentes, licenciamiento adquirido para cada servicio proporcionado, y otras que sirva para la toma de decisión respecto al uso del presente servicio.
- Incluir un servicio de auditoría de reglas de acceso en los diferentes dispositivos firewall para el análisis, depuración de las mismas y mejor control de acceso y seguridad, dicha solución deberá estar implementada en las instalaciones del centro de datos primario sin generar costo adicional para el instituto.
- Cumplir con las especificaciones técnicas y operativas descrita en el Apéndice A.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

6.1.2. Servicios de Prevención de Intrusos (IPS)

Descripción del servicio: El Instituto requiere de la continuidad operativa del servicio que brinda la protección perimetral basado en firmas y que identifica vulnerabilidades, para contener los intentos de obtener acceso a los recursos o servicios publicados en Internet o Intranet que pudieran afectar la operación de la organización, detectar accesos no autorizados y prevenir fugas de información, por lo que el proveedor deberá cumplir con las siguientes especificaciones funcionales mínimas.

- Proporcionar la continuidad operativa de los activos de infraestructura con los que cuenta hoy en día el Instituto o lo que sea necesario implementar, incluyendo el soporte técnico, licenciamiento o lo que se requiera que garantice esta continuidad operativa, así como los niveles de servicio requeridos para este servicio, conforme a lo establecido en el Apéndice B.
- Integrar activos de infraestructura de propósito específico (*Appliances*) con capacidad de expansión bajo demanda, para la continuidad operativa del Instituto, conforme lo dispuesto en el Apéndice A.
- Definir en conjunto con el Instituto la estrategia de habilitación para la continuidad operativa de los activos de infraestructura actuales o aquellos que se requieran como parte de las necesidades operativas de este, conforme lo dispuesto en el Apéndice A y B.
- Acordar con el personal del Instituto, ya sea a través del administrador del contrato o del modelo de gobierno designado para este propósito, las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de *hardware/software* que integran el servicio sin un control de cambios autorizado por este último.
- Continuar con la integración de cada activo de infraestructura hacia su respectiva consola de administración centralizada pudiendo ser en modo stand alone para la administración de todos los dispositivos, así como asegurar que la bitácora del cada activo quede integrada en la solución de correlación de eventos del proyecto u otra que el Instituto designe para este propósito.
- Garantizar que los activos de infraestructura cuenten con actualización tecnológica, estable y validada, del sistema operativo, aplicación (*firmware*) u otro componente necesario con el que cuente el servicio correspondiente, conforme lo dispuesto en el Apéndice A y B.
- Garantizar que los activos de infraestructura cuenten con actualización tecnológica, estable y validada, del sistema operativo, aplicación (*firmware*) u otro componente necesario con el que cuente el servicio correspondiente.
- Permitir únicamente el tráfico (interno y externo) definido por el Instituto entre el punto de conexión central, hacia y desde los diferentes puntos de interconexión con otras redes.
- Prevenir la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del Instituto.
- Atender todos los requerimientos de cambio, atención de incidentes/fallas y solicitudes de información que el Instituto genere, apegado a los Niveles de Servicio definidos para dicho propósito.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- Monitorear todos los eventos registrados en la solución, así como emitir alertas de incidentes generados por los activos de infraestructura que compongan el servicio, cumpliendo al menos:
- Notificar aquellas actividades sospechosas relacionadas con la violación de las políticas, así como aquellas que sean identificadas a través de las funcionalidades habilitadas en la solución.
- Notificar sobre fallas relacionadas con el hardware de los activos de infraestructura provisto a través del servicio.
- Integrar el licenciamiento del *software* que permita continuar con los servicios y activos de infraestructura correspondientes, así como todas aquellas renovaciones necesarias durante la vigencia de los servicios, conforme a lo establecido en el Apéndice B.
- Realizar evaluaciones operativas a los servicios (herramienta de *software* y activos de infraestructura) así como los análisis de vulnerabilidades, que permitan identificar, entre otros, mejoras en el desempeño de los activos, mejoras en la gestión de configuraciones, detección de nuevas funcionalidades operativas derivadas de actualizaciones en versiones de *hardware* y/o *software*; Dichas evaluaciones deberán ejecutarse cada 6 meses, desde el inicio de operaciones de los servicios y hasta 6 meses antes del término de los mismos.
- Realizar las integraciones de conectividad física y lógica que permitan habilitar los servicios descritos en el presente Anexo Técnico tales como, componentes habilitadores de comunicaciones entre redes, cableado eléctrico y de datos, montaje en racks, entre otros.
- Realizar las integraciones de conectividad física y lógica que permitan habilitar los servicios descritos en el presente Anexo Técnico tales como, componentes habilitadores de comunicaciones entre redes, cableado eléctrico y de datos, montaje en racks, entre otros.
- Proporcionar al Instituto cuentas de acceso a las consolas de administración del correspondiente servicio, así como herramientas en *software* que permitan acceder a las mismas (aplicaciones cliente-servidor, portales *web* u otro que se encuentre disponible), las cuales deberán ser de solo lectura, y cuyos atributos de consulta se definirán en las mesas que para este propósito se integren.
- Proporcionar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas para dicha solución, donde se pueda consultar información sobre los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimientos vigentes, licenciamiento adquirido para cada servicio proporcionado, y otras que sirva para la toma de decisión respecto al uso del presente servicio.
- Incluir un servicio de auditoría de reglas de acceso en los diferentes dispositivos IPS para el análisis, depuración de las mismas y mejor control de acceso y seguridad, dicha solución deberá estar implementada en las instalaciones del centro de datos primario sin generar costo adicional para el instituto
- Cumplir, de forma mínima, con las especificaciones técnicas y operativas descrita en el Apéndice A.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

6.1.3. Servicios de Protección contra Ataques Denegación de Servicio (DDoS)

Descripción del servicio: El Instituto requiere la continuidad operativa del servicio que protege contra los ataques de denegación de servicio distribuido que se encuentre basado en firmas y volúmenes de conexión altos, por lo que el proveedor deberá cumplir con las siguientes especificaciones funcionales mínimas.

- Proporcionar la continuidad operativa de los activos de infraestructura con los que cuenta hoy en día el Instituto o lo que sea necesario implementar, incluyendo el soporte técnico, licenciamiento o lo que se requiera que garantice esta continuidad operativa, así como los niveles de servicio requeridos para este servicio, conforme a lo establecido en el Apéndice B.
- Integrar activos de infraestructura de propósito específico (*Appliances*) con capacidad de expansión bajo demanda, para la continuidad operativa del Instituto, conforme lo dispuesto en el Apéndice A.
- Definir en conjunto con el Instituto la estrategia de habilitación para la continuidad operativa de los activos de infraestructura actuales o aquellos que se requieran como parte de las necesidades operativas de este, conforme lo dispuesto en el Apéndice A y B.
- Llevar a cabo las tareas necesarias para la instalación del equipo en los Centro de Datos correspondientes, o en su caso, aquella otra localidad donde le sea solicitado por el Instituto.
- Acordar con el personal del Instituto, ya sea a través del administrador del contrato o del modelo de gobierno designado para este propósito, las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de hardware o software que integran el servicio sin un control de cambios autorizado por este último.
- Continuar con la integración de cada activo de infraestructura hacia su respectiva consola de administración centralizada pudiendo ser en modo stand alone para la administración de todos los dispositivos, así como garantizar que la bitácora del cada activo quede integrada en la solución de correlación de eventos del proyecto u otra que el Instituto designe para este propósito.
- Garantizar que los activos de infraestructura cuenten con actualización tecnológica, estable y validada, del sistema operativo, aplicación (firmware) u otro componente necesario con el que cuente el servicio correspondiente, conforme lo dispuesto en el Apéndice A y B.
- Permitir únicamente el tráfico interno y externo definido por el Instituto entre el punto de conexión central, hacia y desde los diferentes puntos de interconexión con otras redes.
- Continuar con el acceso a servicios ubicados en la capa de servidores de los centros de datos (DMZ), realizando la gestión de acuerdo con el esquema de seguridad y respetando la segmentación definida entre las diversas zonas de seguridad.
- Prevenir la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del Instituto.
- Atender todos los requerimientos de cambio, atención de incidentes/fallas y solicitudes de



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

información que el Instituto genere, apegado a los Niveles de Servicio definidos para dicho propósito.

- Monitorear todos los eventos registrados en la solución, así como emitir alertas de incidentes generados por los activos de infraestructura que compongan el servicio, cumpliendo al menos:
 - Notificar aquellas actividades sospechosas relacionadas con la violación de las políticas, así como aquellas que sean identificadas a través de las funcionalidades habilitadas en la solución.
 - Notificar sobre fallas relacionadas con el hardware de los activos de infraestructura provisto a través del servicio.
- Integrar el licenciamiento del software que permita continuar con los servicios y activos de infraestructura correspondientes, así como todas aquellas renovaciones necesarias durante la vigencia de los servicios, conforme a lo establecido en el Apéndice B.
- Realizar evaluaciones operativas a los servicios (herramienta de software y activos de infraestructura) así como los análisis de vulnerabilidades, que permitan identificar, entre otros, mejoras en el desempeño de los activos, mejoras en la gestión de configuraciones, detección de nuevas funcionalidades operativas derivadas de actualizaciones en versiones de hardware y/o software; Dichas evaluaciones deberán ejecutarse cada 6 meses, desde el inicio de operaciones de los servicios y hasta 6 meses antes del término de los mismos.
- Realizar las integraciones de conectividad física y lógica que permitan habilitar los servicios descritos en el presente Anexo Técnico tales como, componentes habilitadores de comunicaciones entre redes, cableado eléctrico y de datos, montaje en racks, entre otros.
- Proporcionar al Instituto cuentas de acceso a las consolas de administración del correspondiente servicio, así como herramientas en software que permitan acceder a las mismas (aplicaciones cliente-servidor, portales web u otro que se encuentre disponible), las cuales deberán ser de solo lectura, y cuyos atributos de consulta se definirán en las mesas que para este propósito se integren.
 - Proporcionar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas para dicha solución, donde se pueda consultar información sobre los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimientos vigentes, licenciamiento adquirido para cada servicio proporcionado, y otras que sirva para la toma de decisión respecto al uso del presente servicio.
 - Incluir un servicio de auditoría de reglas de acceso en los diferentes dispositivos DDoS para el análisis, depuración de las mismas y mejor control de acceso y seguridad, dicha solución deberá estar implementada en las instalaciones del centro de datos primario sin generar costo adicional para el instituto.
 - Cumplir con las especificaciones técnicas y operativas descrita en el Apéndice A.

6.1.4. Servicios de Redes Privadas Virtuales (VPN)



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Descripción del servicio. El Instituto requiere la continuidad operativa del servicio de interconexión a través de Internet que permita establecer la comunicación desde localidades remotas para la transferencia de información a través de un canal cifrado, por lo que el proveedor deberá cumplir con las siguientes especificaciones funcionales mínimas.

- Proporcionar la continuidad operativa de los activos de infraestructura con los que cuenta hoy en día el Instituto o lo que sea necesario implementar, incluyendo el soporte técnico, licenciamiento o lo que se requiera que garantice esta continuidad operativa, así como los niveles de servicio requeridos para este servicio, conforme a lo establecido en el Apéndice B.
- Integrar activos de infraestructura de propósito específico (Appliances) con capacidad de expansión bajo demanda, para la continuidad operativa del Instituto, conforme lo dispuesto en el Apéndice A.
- Definir en conjunto con el Instituto la estrategia de habilitación para la continuidad operativa de los activos de infraestructura actuales o aquellos que se requieran como parte de las necesidades operativas de este, conforme lo dispuesto en el Apéndice A y B.
- Llevar a cabo las tareas necesarias para la instalación del equipo en los Centro de Datos correspondiente, o en su caso, aquella otra localidad donde le sea requerido por el Instituto.
- Acordar con el personal del Instituto, ya sea a través del administrador del contrato o del modelo de gobierno designado para este propósito, las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de *hardware* o *software* que integran el servicio sin un control de cambios autorizado por este último.
- Continuar con la integración de cada activo de infraestructura hacia su respectiva consola de administración centralizada pudiendo ser en modo independiente (*stand alone*) para la administración de los dispositivos, así como garantizar que la bitácora del cada activo quede integrada en la solución de correlación de eventos del proyecto u otra que el Instituto designe para este propósito.
- Garantizar que los activos de infraestructura cuenten con actualización tecnológica, estable y validada, del sistema operativo, aplicación (*firmware*) u otro componente necesario con el que cuente el servicio correspondiente.
- Garantizar que los activos de infraestructura cuenten con actualización tecnológica, estable y validada, del sistema operativo, aplicación (*firmware*) u otro componente necesario con el que cuente el servicio correspondiente, conforme lo dispuesto en el Apéndice A y B.
- Permitir únicamente el tráfico interno y externo definido por el Instituto entre el punto de conexión central, hacia y desde los diferentes puntos de interconexión con otras redes.
- Continuar con el acceso a servicios ubicados en la capa de servidores de los centros de datos (DMZ), realizando la gestión de acuerdo con el esquema de seguridad y respetando la segmentación definida entre las diversas zonas de seguridad.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- Prevenir la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del Instituto.
- Atender todos los requerimientos de cambio, atención de incidentes/fallas y solicitudes de información que el Instituto genere, apegado a los Niveles de Servicio definidos para dicho propósito.
- Monitorear todos los eventos registrados en la solución, así como emitir alertas de incidentes generados por los activos de infraestructura que compongan el servicio, cumpliendo al menos:
 - Notificar aquellas actividades sospechosas relacionadas con la violación de las políticas, así como aquellas que sean identificadas a través de las funcionalidades habilitadas en la solución.
 - Notificar sobre fallas relacionadas con el hardware de los activos de infraestructura provisto a través del servicio.
- Integrar el licenciamiento del software que permita continuar con los servicios y activos de infraestructura correspondientes, así como todas aquellas renovaciones necesarias durante la vigencia de los servicios, conforme a lo establecido en el Apéndice B.
- Realizar evaluaciones operativas a los servicios (herramienta de software y activos de infraestructura) así como los análisis de vulnerabilidades, que permitan identificar, entre otros, mejoras en el desempeño de los activos, mejoras en la gestión de configuraciones, detección de nuevas funcionalidades operativas derivadas de actualizaciones en versiones de hardware y/o software. Dichas evaluaciones deberán ejecutarse cada 6 meses, desde el inicio de operaciones de los servicios y hasta 6 meses antes del término de los mismos.
- Realizar las integraciones de conectividad física y lógica que permitan habilitar los servicios descritos en el presente Anexo Técnico tales como, componentes habilitadores de comunicaciones entre redes, cableado eléctrico y de datos, montaje en racks, entre otros.
- Proporcionar al Instituto cuentas de acceso a las consolas de administración del correspondiente servicio, así como herramientas en software que permitan acceder a las mismas (aplicaciones cliente-servidor, portales web u otro que se encuentre disponible), las cuales deberán ser de solo lectura, y cuyos atributos de consulta se definirán en las mesas que para este propósito se integren.
- Proporcionar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas para dicha solución, donde se pueda consultar información sobre los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimientos vigentes, licenciamiento adquirido para cada servicio proporcionado, y otras que sirva para la toma de decisión respecto al uso del presente servicio.
- Incluir un servicio de auditoría de reglas de acceso en los diferentes dispositivos VPN para el análisis, depuración de las mismas y mejor control de acceso y seguridad, dicha solución deberá estar implementada en las instalaciones del centro de datos primario sin generar costo adicional para el instituto.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- Cumplir con las especificaciones técnicas y operativas descrita en el Apéndice A.

6.1.5. Servicios de Filtrado de Contenido Web

Descripción del servicio. El Instituto requiere la continuidad operativa del servicio de filtrado de contenido Web mediante políticas de acceso que permite controlar y filtrar la utilización del servicio de acceso a Internet, en función de roles y perfiles, por lo que el proveedor deberá cumplir con las siguientes especificaciones funcionales mínimas.

- Proporcionar la continuidad operativa de los activos de infraestructura con los que cuenta hoy en día el Instituto o lo que sea necesario implementar, incluyendo el soporte técnico, licenciamiento o lo que se requiera que garantice esta continuidad operativa, así como los niveles de servicio requeridos para este servicio, conforme a lo establecido en el Apéndice B.
- Integrar activos de infraestructura de propósito específico (Appliances) con capacidad de expansión bajo demanda, para la continuidad operativa del Instituto, conforme lo dispuesto en el Apéndice A.
- Definir en conjunto con el Instituto la estrategia de habilitación para la continuidad operativa de los activos de infraestructura actuales o aquellos que se requieran como parte de las necesidades operativas de este, conforme lo dispuesto en el Apéndice A y B.
- Llevar a cabo las tareas necesarias para la instalación del equipo en los Centro de Datos correspondiente, o en su caso, aquella otra localidad donde le sea solicitado por el Instituto.
- Acordar con el personal del Instituto, ya sea a través del administrador del contrato o del cuerpo de gobierno designado para este propósito, las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de *hardware* o *software* que integran el servicio sin un control de cambios autorizado por este último.
- Continuar con la integración de cada activo de infraestructura hacia su respectiva consola de administración centralizada pudiendo ser en modo stand alone para la administración de todos los dispositivos, así como garantizar que la bitácora del cada activo quede integrada en la solución de correlación de eventos del proyecto u otra que el Instituto designe para este propósito.
- Garantizar que los activos de infraestructura cuenten con actualización tecnológica, estable y validada, del sistema operativo, aplicación (firmware) u otro componente necesario con el que cuente el servicio correspondiente, conforme lo dispuesto en el Apéndice A y B.
- Permitir únicamente el tráfico interno y externo definido por el Instituto entre el punto de conexión central, hacia y desde los diferentes puntos de interconexión con otras redes.
- Continuar con el acceso a servicios ubicados en la capa de servidores de los centros de datos (DMZ), realizando la gestión de acuerdo con el esquema de seguridad y respetando la segmentación definida entre las diversas zonas de seguridad.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- Prevenir la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del Instituto.
- Atender todos los requerimientos de cambio, atención de incidentes/fallas y solicitudes de información que el Instituto genere, apegado a los Niveles de Servicio definidos para dicho propósito.
- Monitorear todos los eventos registrados en la solución, así como emitir alertas de incidentes generados por los activos de infraestructura que compongan el servicio, cumpliendo al menos:
 - Notificar aquellas actividades sospechosas relacionadas con la violación de las políticas, así como aquellas que sean identificadas a través de las funcionalidades habilitadas en la solución.
 - Notificar sobre fallas relacionadas con el hardware de los activos de infraestructura provisto a través del servicio.
- Integrar el licenciamiento del software que permita continuar con los servicios y activos de infraestructura correspondientes, así como todas aquellas renovaciones necesarias durante la vigencia de los servicios, conforme a lo establecido en el Apéndice B.
- Realizar evaluaciones operativas a los servicios (herramienta de software y activos de infraestructura) así como los análisis de vulnerabilidades, que permitan identificar, entre otros, mejoras en el desempeño de los activos, mejoras en la gestión de configuraciones, detección de nuevas funcionalidades operativas derivadas de actualizaciones en versiones de hardware y/o software. Dichas evaluaciones deberán ejecutarse cada 6 meses, desde el inicio de operaciones de los servicios y hasta 6 meses antes del término de los mismos.
- Realizar las integraciones de conectividad física y lógica que permitan habilitar los servicios descritos en el presente Anexo Técnico tales como, componentes habilitadores de comunicaciones entre redes, cableado eléctrico y de datos, montaje en racks, entre otros.
- Proporcionar al Instituto cuentas de acceso a las consolas de administración del correspondiente servicio, así como herramientas en software que permitan acceder a las mismas (aplicaciones cliente-servidor, portales web u otro que se encuentre disponible), las cuales deberán ser de solo lectura, y cuyos atributos de consulta se definirán en las mesas que para este propósito se integren.
- Proporcionar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas para dicha solución, donde se pueda consultar información sobre los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimientos vigentes, licenciamiento adquirido para cada servicio proporcionado, y otras que sirva para la toma de decisión respecto al uso del presente servicio.
- Incluir un servicio de auditoría de reglas de acceso en los diferentes dispositivos de Filtrado de Contenido Web para el análisis, depuración de las mismas y mejor control de acceso y seguridad, dicha solución deberá estar implementada en las instalaciones del centro de



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

datos primario sin generar costo adicional para el instituto.

- Cumplir con las especificaciones técnicas y operativas descrita en el Apéndice A.

6.1.6. Servicios de Filtrado de Contenido de Correo (Antispam)

Descripción del servicio. El Instituto requiere la continuidad operativa de un servicio para analizar correos electrónicos de entrada y salida con el objetivo de bloquear aquellos que sean clasificados como spam, malware, phishing y con contenido malicioso, entre otros, por lo que el proveedor deberá cumplir con las siguientes especificaciones funcionales mínimas.

- Proporcionar la continuidad operativa de los activos de infraestructura con los que cuenta hoy en día el Instituto o lo que sea necesario implementar, incluyendo el soporte técnico, licenciamiento o lo que se requiera que garantice esta continuidad operativa, así como los niveles de servicio requeridos para este servicio, conforme a lo establecido en el Apéndice B.
- Integrar activos de infraestructura de propósito específico (*Appliances*) con capacidad de expansión bajo demanda, para la continuidad operativa del Instituto, conforme lo dispuesto en el Apéndice A.
- Definir en conjunto con el Instituto la estrategia de habilitación para la continuidad operativa de los activos de infraestructura actuales o aquellos que se requieran como parte de las necesidades operativas de este, conforme lo dispuesto en el Apéndice A y B.
- Llevar a cabo las tareas necesarias para la instalación del equipo en los Centro de Datos correspondiente, o en su caso, aquella otra localidad donde le sea solicitado por el Instituto.
- Proteger el correo electrónico de entrada y salida, así como la reputación del direccionamiento IP que se utiliza para generar esta comunicación en Internet, para lo cual deberá incluir, un servicio de protección a través de los activos de infraestructura existente así como un mecanismo de sanitización en la nube de Internet que prevea una doble capa de verificación sobre correos anómalos o no deseados (spam), con virus o malware.
- Acordar con el personal del Instituto, ya sea a través del administrador del contrato o del modelo de gobierno designado para este propósito, las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de *hardware* o *software* que integran el servicio sin un control de cambios autorizado por este último.
- Continuar con la integración de cada activo de infraestructura hacia su respectiva consola de administración centralizada pudiendo ser en modo stand alone para la administración de todos los dispositivos, así como garantizar que la bitácora del cada activo quede integrada en la solución de correlación de eventos del proyecto u otra que el Instituto designe para este propósito.
- Garantizar que los activos de infraestructura cuenten con actualización tecnológica, estable y validada, del sistema operativo, aplicación (firmware) u otro componente necesario con el que cuente el servicio correspondiente, conforme lo dispuesto en el Apéndice A y B.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- Permitir únicamente el tráfico interno y externo definido por el Instituto entre el punto de conexión central, hacia y desde los diferentes puntos de interconexión con otras redes.
- Continuar con el acceso a servicios ubicados en la capa de servidores de los centros de datos (DMZ), realizando la gestión de acuerdo con el esquema de seguridad y respetando la segmentación definida entre las diversas zonas de seguridad.
- Prevenir la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del Instituto.
- Atender todos los requerimientos de cambio, atención de incidentes/fallas y solicitudes de información que el Instituto genere, apegado a los Niveles de Servicio definidos para dicho propósito.
- Monitorear todos los eventos registrados en la solución, así como emitir alertas de incidentes generados por los activos de infraestructura que compongan el servicio, cumpliendo al menos:
 - Notificar aquellas actividades sospechosas relacionadas con la violación de las políticas, así como aquellas que sean identificadas a través de las funcionalidades habilitadas en la solución.
 - Notificar sobre fallas relacionadas con el hardware de los activos de infraestructura provisto a través del servicio.
- Integrar el licenciamiento del *software* que permita continuar con los servicios y activos de infraestructura correspondientes, así como todas aquellas renovaciones necesarias durante la vigencia de los servicios, conforme a lo establecido en el Apéndice B.
- Realizar evaluaciones operativas a los servicios (herramienta de *software* y activos de infraestructura) así como los análisis de vulnerabilidades, que permitan identificar, entre otros, mejoras en el desempeño de los activos, mejoras en la gestión de configuraciones, detección de nuevas funcionalidades operativas derivadas de actualizaciones en versiones de *hardware* y/o *software*. Dichas evaluaciones deberán ejecutarse cada 6 meses, desde el inicio de operaciones de los servicios y hasta 6 meses antes del término de los mismos.
- Realizar las integraciones de conectividad física y lógica que permitan habilitar los servicios descritos en el presente Anexo Técnico tales como, componentes habilitadores de comunicaciones entre redes, cableado eléctrico y de datos, montaje en racks, entre otros.
- Proporcionar al Instituto cuentas de acceso a las consolas de administración del correspondiente servicio, así como herramientas en *software* que permitan acceder a las mismas (aplicaciones cliente-servidor, portales web u otro que se encuentre disponible), las cuales deberán ser de solo lectura, y cuyos atributos de consulta se definirán en las mesas que para este propósito se integren.
- Proporcionar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas para dicha solución, donde se pueda consultar información sobre los casos de



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

soporte generados, documentación técnica de los servicios, pólizas de mantenimientos vigentes, licenciamiento adquirido para cada servicio proporcionado, y otras que sirva para la toma de decisión respecto al uso del presente servicio.

- Incluir un servicio de auditoría de reglas de acceso en los diferentes dispositivos Antispam para el análisis, depuración de las mismas y mejor control de acceso y seguridad, dicha solución deberá estar implementada en las instalaciones del centro de datos primario sin generar costo adicional para el instituto.
- Cumplir con las especificaciones técnicas y operativas descrita en el Apéndice A.

6.1.7. Servicios de Firewall Especializado en Servicios Web (WAF)

Descripción del servicio. El Instituto requiere la continuidad del servicio de protección, prevención y control de ataques para aplicativos web expuestos en Internet/Intranet, por lo que el proveedor deberá cumplir con las siguientes especificaciones funcionales mínimas.

- Proporcionar la continuidad operativa de los activos de infraestructura con los que cuenta hoy en día el Instituto o lo que sea necesario implementar, incluyendo el soporte técnico, licenciamiento o lo que se requiera que garantice esta continuidad operativa, así como los niveles de servicio requeridos para este servicio, conforme a lo establecido en el Apéndice B.
- Integrar activos de infraestructura de propósito específico (Appliances) con capacidad de expansión bajo demanda, para la continuidad operativa del Instituto, conforme lo dispuesto en el Apéndice A.
- Definir en conjunto con el Instituto la estrategia de habilitación para la continuidad operativa de los activos de infraestructura actuales o aquellos que se requieran como parte de las necesidades operativas de este, conforme lo dispuesto en el Apéndice A y B.
- Llevar a cabo las tareas necesarias para la instalación del equipo en los Centro de Datos correspondiente, o en su caso, aquella otra localidad donde le sea solicitado por el Instituto.
- Acordar con el personal del Instituto, ya sea a través del administrador del contrato o del modelo de gobierno designado para este propósito, las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de *hardware* o *software* que integran el servicio sin un control de cambios autorizado por este último.
- Continuar con la integración de cada activo de infraestructura hacia su respectiva consola de administración centralizada pudiendo ser en modo stand alone para la administración de todos los dispositivos, así como garantizar que la bitácora del cada activo quede integrada en la solución de correlación de eventos del proyecto u otra que el Instituto designe para este propósito.
- Garantizar que los activos de infraestructura cuenten con actualización tecnológica, estable y validada, del sistema operativo, aplicación (*firmware*) u otro componente necesario con el que cuente el servicio correspondiente, conforme lo dispuesto en el Apéndice A y B.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- Permitir únicamente el tráfico interno y externo definido por el Instituto entre el punto de conexión central, hacia y desde los diferentes puntos de interconexión con otras redes.
- Continuar con el acceso a servicios ubicados en la capa de servidores de los centros de datos (DMZ), realizando la gestión de acuerdo con el esquema de seguridad y respetando la segmentación definida entre las diversas zonas de seguridad.
- Prevenir la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del Instituto.
- Atender los requerimientos de cambio, atención de incidentes/fallas y solicitudes de información que el Instituto genere, apegado a los Niveles de Servicio definidos para dicho propósito.
- Monitorear todos los eventos registrados en la solución, así como emitir alertas de incidentes generados por los activos de infraestructura que compongan el servicio, cumpliendo al menos:
 - Notificar aquellas actividades sospechosas relacionadas con la violación de las políticas, así como aquellas que sean identificadas a través de las funcionalidades habilitadas en la solución.
 - Notificar sobre fallas relacionadas con el hardware de los activos de infraestructura provisto a través del servicio.
- Integrar el licenciamiento del software que permita continuar con los servicios y activos de infraestructura correspondientes, así como todas aquellas renovaciones necesarias durante la vigencia de los servicios, conforme a lo establecido en el Apéndice B.
- Realizar evaluaciones operativas a los servicios (herramienta de *software* y activos de infraestructura) así como los análisis de vulnerabilidades, que permitan identificar, entre otros, mejoras en el desempeño de los activos, mejoras en la gestión de configuraciones, detección de nuevas funcionalidades operativas derivadas de actualizaciones en versiones de *hardware* y/o *software*. Dichas evaluaciones deberán ejecutarse cada 6 meses, desde el inicio de operaciones de los servicios y hasta 6 meses antes del término de los mismos.
- Realizar las integraciones de conectividad física y lógica que permitan habilitar los servicios descritos en el presente Anexo Técnico tales como, componentes habilitadores de comunicaciones entre redes, cableado eléctrico y de datos, montaje en racks, entre otros.
- Proporcionar al Instituto cuentas de acceso a las consolas de administración del correspondiente servicio, así como herramientas en *software* que permitan acceder a las mismas (aplicaciones cliente-servidor, portales web u otro que se encuentre disponible), las cuales deberán ser de solo lectura, y cuyos atributos de consulta se definirán en las mesas que para este propósito se integren.
- Proporcionar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas para dicha solución, donde se pueda consultar información sobre los casos de



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

soporte generados, documentación técnica de los servicios, pólizas de mantenimientos vigentes, licenciamiento adquirido para cada servicio proporcionado, y otras que sirva para la toma de decisión respecto al uso del presente servicio.

- Incluir un servicio de auditoría de reglas de acceso en los diferentes dispositivos WAF para el análisis, depuración de las mismas y mejor control de acceso y seguridad, dicha solución deberá estar implementada en las instalaciones del centro de datos primario sin generar costo adicional para el instituto.
- Cumplir con las especificaciones técnicas y operativas descrita en el Apéndice A.

6.1.8. Servicios de Firewall especializado en Base de Datos (DBF)

Descripción del servicio. El Instituto requiere la continuidad operativa del servicio de protección a las instancias de bases de datos en tiempo real, así como el monitoreo del tráfico de base de datos con la finalidad de realizar la detección de ataques avanzados, por lo que el proveedor deberá cumplir con las siguientes especificaciones funcionales mínimas.

- Proporcionar la continuidad operativa de los activos de infraestructura con los que cuenta hoy en día el Instituto o lo que sea necesario implementar, incluyendo el soporte técnico, licenciamiento o lo que se requiera que garantice esta continuidad operativa, así como los niveles de servicio requeridos para este servicio, conforme a lo establecido en el Apéndice B.
- Integrar activos de infraestructura de propósito específico (Appliances) con capacidad de expansión bajo demanda, para la continuidad operativa del Instituto, conforme lo dispuesto en el Apéndice A.
- Definir en conjunto con el Instituto la estrategia de habilitación para la continuidad operativa de los activos de infraestructura actuales o aquellos que se requieran como parte de las necesidades operativas de este, conforme lo dispuesto en el Apéndice A y B.
- Llevar a cabo las tareas necesarias para la instalación del equipo en los Centro de Datos correspondiente, o en su caso, aquella otra localidad donde le sea solicitado por el Instituto.
- Acordar con el personal del Instituto, ya sea a través del administrador del contrato o del modelo de gobierno designado para este propósito, las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de *hardware* o *software* que integran el servicio sin un control de cambios autorizado por este último.
- Continuar con la integración de cada activo de infraestructura hacia su respectiva consola de administración centralizada pudiendo ser en modo stand alone para la administración de todos los dispositivos, así como garantizar que la bitácora del cada activo quede integrada en la solución de correlación de eventos del proyecto u otra que el Instituto designe para este propósito.
- Garantizar que los activos de infraestructura cuenten con actualización tecnológica, estable y validada, del sistema operativo, aplicación (firmware) u otro componente necesario con el



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

que cuente el servicio correspondiente, conforme lo dispuesto en el Apéndice A y B.

- Permitir únicamente el tráfico interno y externo definido por el Instituto entre el punto de conexión central, hacia y desde los diferentes puntos de interconexión con otras redes.
- Continuar con el acceso a servicios ubicados en la capa de servidores de los centros de datos (Base de datos), realizando la gestión de acuerdo con el esquema de seguridad y respetando la segmentación definida entre las zonas de servidores.
- Prevenir la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del Instituto.
- Atender todos los requerimientos de cambio, atención de incidentes/fallas y solicitudes de información que el Instituto genere, apegado a los Niveles de Servicio definidos para dicho propósito.
- Monitorear todos los eventos registrados en la solución, así como emitir alertas de incidentes generados por los activos de infraestructura que compongan el servicio, cumpliendo al menos:
 - Notificar aquellas actividades sospechosas relacionadas con la violación de las políticas, así como aquellas que sean identificadas a través de las funcionalidades habilitadas en la solución.
 - Notificar sobre fallas relacionadas con el hardware de los activos de infraestructura provisto a través del servicio.
- Integrar el licenciamiento del *software* que permita continuar con los servicios y activos de infraestructura correspondientes, así como todas aquellas renovaciones necesarias durante la vigencia de los servicios, conforme a lo establecido en el Apéndice B.
- Realizar evaluaciones operativas a los servicios (herramienta de *software* y activos de infraestructura) así como los análisis de vulnerabilidades, que permitan identificar, entre otros, mejoras en el desempeño de los activos, mejoras en la gestión de configuraciones, detección de nuevas funcionalidades operativas derivadas de actualizaciones en versiones de *hardware* y/o *software*. Dichas evaluaciones deberán ejecutarse cada 6 meses, desde el inicio de operaciones de los servicios y hasta 6 meses antes del término de los mismos.
- Realizar las integraciones de conectividad física y lógica que permitan habilitar los servicios descritos en el presente Anexo Técnico tales como, componentes habilitadores de comunicaciones entre redes, cableado eléctrico y de datos, montaje en racks, entre otros.
- Proporcionar al Instituto cuentas de acceso a las consolas de administración del correspondiente servicio, así como herramientas en *software* que permitan acceder a las mismas (aplicaciones cliente-servidor, portales web u otro que se encuentre disponible), las cuales deberán ser de solo lectura, y cuyos atributos de consulta se definirán en las mesas que para este propósito se integren.
- Proporcionar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

integradas para dicha solución, donde se pueda consultar información sobre los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimientos vigentes, licenciamiento adquirido para cada servicio proporcionado, y otras que sirva para la toma de decisión respecto al uso del presente servicio.

- Incluir un servicio de auditoría de reglas de acceso en los diferentes dispositivos DBF para el análisis, depuración de las mismas y mejor control de acceso y seguridad, dicha solución deberá estar implementada en las instalaciones del centro de datos primario sin generar costo adicional para el instituto.
- Cumplir con las especificaciones técnicas y operativas descrita en el Apéndice A.

6.1.9. Servicios de Gestión Unificada de Amenazas (UTM)

Descripción del servicio. El Instituto requiere la continuidad operativa del servicio de protección perimetral especializada en control de acceso, prevención de intrusos, filtrado de contenido Web y VPN, para control de tráfico y detección de actividad anómala, por lo que el proveedor deberá cumplir con las siguientes especificaciones funcionales mínimas.

- Proporcionar la continuidad operativa de los activos de infraestructura con los que cuenta hoy en día el Instituto o lo que sea necesario implementar, incluyendo el soporte técnico, licenciamiento o lo que se requiera que garantice esta continuidad operativa, así como los niveles de servicio requeridos para este servicio, conforme a lo establecido en el Apéndice B.
- Integrar activos de infraestructura de propósito específico (*Appliances*) con capacidad de expansión bajo demanda, para la continuidad operativa del Instituto, conforme lo dispuesto en el Apéndice A.
- Definir en conjunto con el Instituto la estrategia de habilitación para la continuidad operativa de los activos de infraestructura actuales o aquellos que se requieran como parte de las necesidades operativas de este, conforme lo dispuesto en el Apéndice A y B.
- Llevar a cabo las tareas necesarias para la instalación del equipo en los Centro de Datos correspondiente, o en su caso, aquella otra localidad donde le sea solicitado por el Instituto.
- Acordar con el personal del Instituto, ya sea a través del administrador del contrato o del modelo de gobierno designado para este propósito, las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de *hardware* o *software* que integran el servicio sin un control de cambios autorizado por este último.
- Continuar con la integración de cada activo de infraestructura hacia su respectiva consola de administración centralizada pudiendo ser en modo stand alone para la administración de todos los dispositivos, así como garantizar que la bitácora del cada activo quede integrada en la solución de correlación de eventos del proyecto u otra que el Instituto designe para este propósito.
- Garantizar que los activos de infraestructura cuenten con actualización tecnológica, estable



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

y validada, del sistema operativo, aplicación (*firmware*) u otro componente necesario con el que cuente el servicio correspondiente, conforme lo dispuesto en el Apéndice A y B.

- Permitir únicamente el tráfico interno y externo definido por el Instituto entre el punto de conexión central, hacia y desde los diferentes puntos de interconexión con otras redes.
- Prevenir la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del Instituto.
- Atender todos los requerimientos de cambio, atención de incidentes/fallas y solicitudes de información que el Instituto genere, apegado a los Niveles de Servicio definidos para dicho propósito.
- Monitorear todos los eventos registrados en la solución, así como emitir alertas de incidentes generados por los activos de infraestructura que compongan el servicio, cumpliendo al menos:
 - Notificar aquellas actividades sospechosas relacionadas con la violación de las políticas, así como aquellas que sean identificadas a través de las funcionalidades habilitadas en la solución.
 - Notificar sobre fallas relacionadas con el hardware de los activos de infraestructura provisto a través del servicio.
- Integrar el licenciamiento del *software* que permita continuar con los servicios y activos de infraestructura correspondientes, así como todas aquellas renovaciones necesarias durante la vigencia de los servicios, conforme a lo establecido en el Apéndice B.
- Realizar evaluaciones operativas a los servicios (herramienta de *software* y activos de infraestructura) así como los análisis de vulnerabilidades, que permitan identificar, entre otros, mejoras en el desempeño de los activos, mejoras en la gestión de configuraciones, detección de nuevas funcionalidades operativas derivadas de actualizaciones en versiones de *hardware* y/o *software*. Dichas evaluaciones deberán ejecutarse cada 6 meses, desde el inicio de operaciones de los servicios y hasta 6 meses antes del término de los mismos.
- Realizar las integraciones de conectividad física y lógica que permitan habilitar los servicios descritos en el presente Anexo Técnico tales como, componentes habilitadores de comunicaciones entre redes, cableado eléctrico y de datos, montaje en racks, entre otros.
- Proporcionar al Instituto cuentas de acceso a las consolas de administración del correspondiente servicio, así como herramientas en *software* que permitan acceder a las mismas (aplicaciones cliente-servidor, portales web u otro que se encuentre disponible), las cuales deberán ser de solo lectura, y cuyos atributos de consulta se definirán en las mesas que para este propósito se integren.
- Proporcionar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas para dicha solución, donde se pueda consultar información sobre los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimientos vigentes, licenciamiento adquirido para cada servicio proporcionado, y otras que sirva para



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

la toma de decisión respecto al uso del presente servicio.

- Incluir un servicio de auditoría de reglas de acceso en los diferentes dispositivos UTM para el análisis, depuración de las mismas y mejor control de acceso y seguridad, dicha solución deberá estar implementada en las instalaciones del centro de datos primario sin generar costo adicional para el instituto.
- Cumplir con las especificaciones técnicas y operativas descrita en el Apéndice A.

6.1.10. Servicio de Correlación de Eventos

Descripción del servicio. El Instituto requiere de un servicio de seguridad que administre, analice, explote, emplee y aproveche las bitácoras de los dispositivos de seguridad con la finalidad de conocer exactamente qué pasa en distintos puntos de la red de forma centralizada y eliminar falsos positivos generados, por lo que el proveedor deberá cumplir con las siguientes especificaciones funcionales mínimas.

- Proporcionar activos de infraestructura nuevos de última generación y dedicados exclusivamente para las necesidades del Instituto.
- Habilitar los activos de infraestructura requeridos en esquemas de Alta Disponibilidad (HA por sus siglas en inglés).
- Integrar activos de infraestructura de propósito específico (*appliances* o servidores físicos) con capacidades de expansión bajo demanda conforme lo dispuesto en el Apéndice A.
- Definir en conjunto con el Instituto la estrategia de habilitación de los nuevos activos de infraestructura para correlación de eventos en la arquitectura de seguridad y comunicaciones.
- Ejecutar todas las tareas necesarias para la instalación del equipo en los Centro de Datos correspondientes, o en su caso, aquella otra localidad donde le sea requerido por el Instituto.
- Acordar con el personal del Instituto, ya sea a través del administrador del contrato o del modelo de gobierno designado para este propósito, todas las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de hardware/software que integran el servicio sin un control de cambios autorizado por este último.
- Integrar cada activo de infraestructura hacia su respectiva consola de administración centralizada pudiendo ser en modo independiente (*stand alone*) para la administración de todos los dispositivos, así como asegurar que la bitácora de cada activo quede integrada en la solución de correlación de eventos del proyecto u otra que el Instituto designe para este propósito.
- Asegurar que los activos de infraestructura propuestos cuenten con la última versión liberada, estable y validada, del sistema operativo, aplicación (*firmware*) u otro componente necesario con el que cuente el servicio correspondiente.
- Permitir únicamente la correlación definida por el Instituto entre el punto de conexión central, hacia y desde los diferentes puntos de interconexión vía syslog con otras redes o nubes.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- Atender los requerimientos de cambio, atención de fallas y solicitudes de información que el Instituto genere, apegado a los Niveles de Servicio definidos para dicho propósito.
- Monitorear los eventos registrado en la solución, así como emitir alertas de incidentes generados por los activos de infraestructura que compongan el servicio, cumpliendo al menos:
- Notificar aquellas actividades sospechosas relacionadas con la violación de las políticas, así como aquellas que sean identificadas a través de las funcionalidades habilitadas en la solución.
- Notificar sobre fallas relacionadas con el *hardware* de los activos de infraestructura provisto a través del servicio.
- En caso de que el desempeño de la tecnología que soporta el servicio propuesto no sea el adecuado, el proveedor del servicio deberá presentar la propuesta de mejora de los activos afectados, así como realizar la sustitución de los componentes tecnológicos por otros de igual o mejores características/funcionalidades, esto último con la autorización previa por parte del Instituto.
- Integrar el licenciamiento del *software* que permita habilitar los servicios y activos de infraestructura correspondientes, así como todas aquellas renovaciones necesarias durante la vigencia de los servicios.
- Realizar evaluaciones operativas a los servicios (herramienta de *software* y activos de infraestructura) que permitan identificar, entre otros: mejoras en el desempeño de los activos, mejoras en la gestión de configuraciones, detección de nuevas funcionalidades operativas derivadas de actualizaciones en versiones de hardware y/o software. Dichas evaluaciones deberán ejecutarse cada 6 meses, desde el inicio de operaciones de los servicios y hasta 6 meses antes del término de los mismos.
- Proporcionar al Instituto cuentas de acceso a las consolas de administración del correspondiente servicio, así como herramientas en *software* que permitan acceder a las mismas (*aplicaciones cliente-servidor, portales web u otro que se encuentre disponible*), las cuales deberán ser de solo lectura, y cuyos atributos de consulta se definirán en las mesas que para este propósito se integren.
- Proporcionar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas para dicha solución, donde se pueda consultar información sobre los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimientos vigentes, licenciamiento adquirido para cada servicio proporcionado, y otras que sirva para la toma de decisión respecto al uso del presente servicio.
- Incluir un servicio de auditoría de reglas de acceso en los diferentes dispositivos del Correlacionador de Eventos para el análisis, depuración de las mismas y mejor control de acceso y seguridad, dicha solución deberá estar implementada en las instalaciones del centro de datos primario sin generar costo adicional para el instituto.
- Cumplir, de forma mínima, con las especificaciones técnicas y operativas descrita en el Apéndice A.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

6.1.11. Servicio de Protección de Amenazas Persistentes Avanzadas (APT)

Descripción del servicio. El Instituto requiere la habilitación de un servicio que le permita tener la capacidad de protegerse de amenazas avanzadas que se encuentren activas en la organización y que hayan podido sobrepasar los controles de seguridad existentes, por lo que el proveedor deberá cumplir con las siguientes especificaciones funcionales mínimas.

- Proporcionar activos de infraestructura nuevos de última generación y dedicados exclusivamente para las necesidades del Instituto.
- Habilitar los activos de infraestructura requeridos en esquemas de Alta Disponibilidad (HA por sus siglas en inglés).
- Integrar activos de infraestructura de propósito específico (*appliances*) con capacidades de expansión bajo demanda, pudiendo ser estas últimas instancias virtuales, conforme lo dispuesto en el Apéndice A.
- Definir en conjunto con el Instituto la estrategia de habilitación de los nuevos activos de infraestructura para Amenazas Persistentes Avanzadas en la arquitectura de seguridad y comunicaciones.
- Ejecutar las tareas necesarias para la instalación del equipo en los Centro de Datos correspondiente, o en su caso, aquella otra localidad donde le sea solicitado por el Instituto.
- Acordar con el personal del Instituto, ya sea a través del administrador del contrato o del cuerpo de gobierno designado para este propósito, todas las ventanas de mantenimiento necesarias para la correcta operación del servicio, y en ningún momento podrá realizar cambios a los componentes de *hardware/software* que integran el servicio sin un control de cambios autorizado por este último.
- Integrar cada activo de infraestructura hacia su respectiva consola de administración centralizada pudiendo ser en modo stand alone para la administración de todos los dispositivos, así como asegurar que la bitácora de cada activo quede integrada en la solución de correlación de eventos del proyecto u otra que el Instituto designe para este propósito.
- Asegurar que los activos de infraestructura propuestos cuenten con la última versión liberada, estable y validada, del sistema operativo, aplicación (*firmware*) u otro componente necesario con el que cuente el servicio correspondiente.
- Permitir únicamente el tráfico definido por el Instituto entre el punto de conexión central, hacia y desde los diferentes puntos de interconexión con otras redes o nubes.
- Prevenir la explotación de vulnerabilidades y la entrada de tráfico malicioso a las redes del Instituto.
- Atender los requerimientos de cambio, atención de incidentes/fallas y solicitudes de información que el Instituto genere, apegado a los Niveles de Servicio definidos para dicho propósito.
- Monitorear los eventos registrado en la solución, así como emitir alertas de incidentes generados



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

por los activos de infraestructura que compongan el servicio, cumpliendo al menos:

- Notificar aquellas actividades sospechosas relacionadas con la violación de las políticas, así como aquellas que sean identificadas a través de las funcionalidades habilitadas en la solución.
- Notificar sobre fallas relacionadas con el *hardware* de los activos de infraestructura provisto a través del servicio.
- En caso de que el desempeño de la tecnología que soporta el servicio propuesto no sea el adecuado, el proveedor del servicio deberá presentar la propuesta de mejora de los activos afectados, así como realizar la sustitución de los componentes tecnológicos por otros de igual o mejores características/funcionalidades, esto último con la autorización previa por parte del Instituto.
- Integrar el licenciamiento del *software* que permita habilitar los servicios y activos de infraestructura correspondientes, así como todas aquellas renovaciones necesarias durante la vigencia de los servicios.
- Realizar evaluaciones operativas a los servicios (herramienta de *software* y activos de infraestructura) que permitan identificar, entre otros: mejoras en el desempeño de los activos, mejoras en la gestión de configuraciones, detección de nuevas funcionalidades operativas derivadas de actualizaciones en versiones de hardware y/o software. Dichas evaluaciones deberán ejecutarse cada 6 meses, desde el inicio de operaciones de los servicios y hasta 6 meses antes del término de los mismos.
- Proporcionar al Instituto cuentas de acceso a las consolas de administración del correspondiente servicio, así como herramientas en *software* que permitan acceder a las mismas (aplicaciones cliente-servidor, portales web u otro que se encuentre disponible), las cuales deberán ser de solo lectura, y cuyos atributos de consulta se definirán en las mesas que para este propósito se integren.
- Proporcionar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas para dicha solución, donde se pueda consultar información sobre los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimientos vigentes, licenciamiento adquirido para cada servicio proporcionado, y otras que sirva para la toma de decisión respecto al uso del presente servicio.
- Incluir un servicio de auditoría de reglas de acceso en los diferentes dispositivos del servicio de Amenazas Persistentes Avanzadas para el análisis, depuración de las mismas y mejor control de acceso y seguridad, dicha solución deberá estar implementada en las instalaciones del centro de datos primario sin generar costo adicional para el instituto.
- Cumplir, de forma mínima, con las especificaciones técnicas y operativas descrita en el Apéndice A.

6.2. Servicios de Seguridad – verificación y calidad

El Instituto requiere continuar con la prestación de servicios bajo demanda durante la vigencia del contrato y que a través de este se definan, identifiquen, clasifiquen y prioricen las debilidades de las aplicaciones



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

que proporcionan una evaluación de las amenazas previsibles, que permitan reaccionar de manera apropiada, así como robustecer la confidencialidad, integridad y disponibilidad de la información, atendiendo a las necesidades operativas del IMSS.

6.2.1. Servicios de Borrado Seguro de Información

Descripción del servicio. Se requiere dar continuidad a la solución de borrado seguro de información, para los dispositivos tales como computadoras personales, laptops, servidores, unidades de almacenamiento fijas, removibles, externos y cualquier otro que el Instituto determine, con el fin de evitar la pérdida y dispersión de información propiedad de este; lo anterior aplicará cuando sean retirados dichos dispositivos por motivos de conclusión de contrato, obsolescencia, falla, baja y/o reasignación, entre otros. Para tal efecto se requiere la renovación del derecho de uso y soporte técnico de los productos de software de borrado seguro, así como, la actualización de dicho licenciamiento, actualizaciones (*updates* y *upgrades*) que permitan garantizar la confidencialidad de la información propiedad del Instituto, cumpliendo con lo establecido en la legislación vigente y aplicable relacionada con los derechos de autor.

Los servicios proporcionados por el proveedor, así como las entregas de información requeridas en el presente documento, deberán apegarse a la normativa vigente aplicable para dichos servicios y soluciones, por lo que el proveedor deberá cumplir con las siguientes especificaciones funcionales mínimas.

- Integrar todas aquellas renovaciones que sean necesarias durante la vigencia de los servicios.
- Garantizar que las herramientas de borrado seguro cuenten con la última versión liberada, estable y validada, por parte del fabricante, así como para otros componentes necesarios del servicio correspondiente.
- Deberá permitir realizar borrados completos en medios de almacenamiento dispuestos en activos de infraestructura como: equipos de cómputo (de escritorio y portátil), equipos de propósito específico (*appliance*), servidores físicos o virtuales, derivado de la sustitución, migraciones o retiro por finalización del contrato.
- Deberá asegurar que los datos no puedan ser recuperados, basándose en al menos los siguientes estándares internacionales.
 - HMG Infosec Standard 5 (baseline and enhanced)
 - Opnavinst 5239.1A
 - Extended NIST 800-88
 - DoD 5220.22-M
 - ISO-IEC 15408
 - ECE y BSI/VSITR
- Borrado de Discos duros IDE/ATA, SCSI, SAS, USB, SATA, SSD, Fiber Channel y FireWire, de estado sólido y mecánicos de cualquier tamaño.
- Deberá brindar la destrucción local y/o remota en múltiples dispositivos de almacenamiento.
- Deberá posibilitar el desmontaje RAID (SCSI).



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- Deberá permitir el borrado y detección de zonas bloqueadas / ocultas (DCO, HPA).
- Deberá generar certificados de borrado infalsificables que ofrezcan protección ante cualquier instancia legal, en donde se incluya el resultado del proceso de borrado, fecha, hora, los datos del equipo, el detalle del dispositivo de almacenamiento borrado.
- Deberá emitir una firma electrónica para la autenticación de la integridad del reporte de sanitización emitido por el software de borrado.
- La solución deberá ejecutarse sin importar de que sistema operativo se trate.
- El reporte que generé la solución deberá ser exportado a un medio de almacenamiento como USB o disco duro.
- El servicio de borrado seguro esta provisto mediante un proceso o flujo operativo, el cual deberá contemplar entre otros, los siguientes puntos:
 - Solicitud de borrado.
 - Identificación del medio de borrado.
 - Definición de fecha de borrado.
 - Flujos operativos para la autorización de borrado o destrucción.
 - Como referencia, se muestran los insumos a ser atendidos

DISPOSITIVOS
Derecho Uso de Licencias y Soporte Técnico
PC y Laptops
Servidores
Máquinas Virtuales y Unidades Lógicas
Archivos, carpetas, bases de datos
Console Management
Servicio de Soporte Técnico Especializado
Disco Duro, PC, Laptops, Disco Duro Servidor y Disco Duro Storage
Borrado de Bases de Datos, LUN's y Contenedores
Borrado de Máquinas Virtuales
Degaussing Discos Duros, SSD y Cintas LTO

- La continuidad del servicio deberá considerar que los usuarios puedan acceder a las consolas de administración de la solución para la gestión, administración, supervisión y operación, todo ello con el fin de habilitar las funcionalidades operativas para realizar el borrado seguro de manera descentralizada (en oficinas remotas).

6.2.2. Servicio de Gestión de Dominios

Descripción del servicio. Continuidad operativa del servicio que permita registrar ante las instancias certificadas por el NIC, los dominios que requiera el Instituto y su correcta gestión, por lo que el proveedor deberá cumplir con las siguientes especificaciones funcionales mínimas.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- Registro – Llevar a cabo el seguimiento correspondiente ante las instancias certificadoras
 - Revisar y dar seguimiento a el nombre de domino acordado con el personal designado por el Instituto
 - Revisar que no se encuentre duplicado o usado por ningún tercero
- Alojamiento – Dar seguimiento al alojamiento de dicho dominio
 - Actualización de las directivas de seguridad.
 - Continuidad al mantenimiento requerido

El proveedor de servicios deberá continuar con la gestión y los pagos que correspondan derivados del registro, cambio de dominio o proveedor sin costo adicional para el Instituto.

6.2.3. Servicio de Certificados Digitales SSL

Descripción del Servicio. Se requiere la continuidad del servicio que permite contar con certificados SSL para la protección de las páginas web del Instituto, durante la vigencia del contrato, por lo que el proveedor deberá cumplir con las siguientes especificaciones funcionales mínimas.

- Validación de dominios
- Cifrado SSL de al menos 256 bits
- No debe de ser auto firmado, sino emitido por una instancia certificadora válida (tercero confiable)
- El tiempo de emisión deberá cumplir con los niveles de servicios establecidos para hacerlo llegar al personal del Instituto vía correo electrónico
- El proveedor deberá hacerse cargo de la gestión en cuanto a pagos de derecho y cualquier cargo derivado de contar con el o los certificados.
- Los certificados deberán ser al menos de los siguientes tipos:
 - Certificados SSL con validación de dominio (DV SSL)
 - Certificado para un solo dominio
 - Certificado para múltiples dominios (SAN)
 - Certificados comodines (wildcard)

6.2.4. Servicios de Ciberinteligencia (Ciberseguridad)

Descripción del servicio. El Instituto requiere de un servicio con inteligencia accionable que le permita actuar oportunamente para protegerse y minimizar amenazas o ataques informáticos detectados a través de campañas y operaciones identificadas, al mismo tiempo que pueda ordenar investigaciones de acuerdo a sus necesidades, por lo que el proveedor deberá cumplir con las siguientes especificaciones funcionales mínimas.

- Detectar posible venta de información confidencial del Instituto en mercados negros.
- Dar seguimiento a grupos hacktivistas y del cibercrimen nacionales y extranjeros que puedan representar una amenaza para el Instituto.
- Poder infiltrarse en canales de IRC donde se perpetren y difundan campañas de ataques informáticos que puedan afectar al Instituto.
- Monitorear foros y comunidades tanto de redes abiertas como de la Red Onion/TOR donde se perpetren y difundan campañas de ataques informáticos que pudieran representar un riesgo para el Instituto.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- Poder monitorear las noticias tanto nacionales como extranjeras tanto en la red abierta como en la Deep Web para la colección de inteligencia táctica, que permita al Instituto tomar acciones preventivas adicionales para la protección de infraestructura susceptible de un ataque informático.
- Colectar, a través de un cuestionario especializado, los elementos que provean la información necesaria para realizar el análisis de la situación global del Instituto, así como generar los perfiles de investigación a ser utilizados para los servicios permanentes.
- A través de un cuestionario en esta etapa se deberá recopilar la siguiente información:
 - Páginas publicadas.
 - Historial de amenazas de seguridad experimentadas por el Instituto.
 - Sistemas críticos consultados por usuarios externos.
 - Lista de activos críticos y su atracción o valor para el ciber-crimen.
 - Contactos para la elaboración de la matriz de escalación.
 - Datos para la elaboración de la declaración de trabajo (SOW por sus siglas en inglés).
- Realizar un análisis de la situación global del instituto, una vez teniendo el contexto de su entorno e identificando el tipo de exposición y amenazas que podrían impactarle de acuerdo al acontecer local y las amenazas globales del sector en el que se desenvuelve.
- Generación de perfiles de investigación con la información recabada. Dicho perfil de investigación deberá ser utilizado durante la vigilancia de Ciberinteligencia, el cual incluye lo siguiente:
 - Perfiles virtuales a emplear.
 - Definición de fuentes asociadas a los perfiles virtuales utilizados en el monitoreo.
- Determinar los umbrales para los eventos que dispararán las alertas que se deberán de notificar hacia la matriz de notificación definida en conjunto con el Instituto para los servicios como "Vigilancia Permanente de Ciberinteligencia".
- Mantener supervisión de los correos/sitios de phishing y direcciones IP dudosas que le comparta el instituto con el fin de realizar un análisis de los mismos. De manera adicional deberá realizar vigilancia en el ciberespacio las 24 horas del día los 365 días del año, sobre redes sociales, Darknet, buscadores de internet de las cosas, entre otras fuentes, para ello se deberá colectar inteligencia empleando técnicas de OSINT (Open Source Intelligence) como líneas de tiempo y mapas de conexiones, Virtual HUMINT donde se emplean la infiltración de perfiles virtuales.
- Identificar campañas para ataques específicos, venta de información, infraestructura vulnerable expuesta a través de internet, relaciones entre perfiles, grupos privados de facebook, entre otros.
- Realizar esta evaluación en cualquiera de los siguientes casos:
 - Durante la vigilancia de Ciberinteligencia, al encontrarse algún hallazgo que represente realmente una amenaza para el Instituto, se deberá realizar una notificación inicial con la finalidad de que el Instituto pueda tomar las líneas de acción necesarias para mitigar la amenaza descubierta.
 - Cuando se solicite el análisis de sitios dedicados al phishing, correos que contengan phishing o direcciones IP.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- Durante la elaboración del análisis del comportamiento de los grupos hacktivistas.
- Durante el análisis de las direcciones IP, producto de ataques de denegación de servicios que haya experimentado el Instituto.
- Realizar un análisis correlacionando toda la información recolectada por las herramientas y la situación general alrededor del evento, a partir de este análisis deberá emitir un dictamen hacia el instituto con inteligencia accionable, táctica u operativa según corresponda, en un plazo no mayor a 24 horas después de la detección de cualquiera de los siguientes eventos:
 - Declaración de posibles ataques de denegación de servicio por parte de grupos hacktivistas o del cibercrimen.
 - Defacements.
 - Fuga de información confidencial del Instituto hacia sitios públicos.
 - Malware dirigido.
 - Phishing detectado en parking domains.
 - Indicios de amenazas o ataques informáticos sobre el Instituto.
 - Existencia de campañas (conjunto de acciones para perpetrar un ataque informático) en contra del Instituto.
 - Venta o publicación de información sensible del Instituto en la Darknet.
 - Publicación de información confidencial de personal del Instituto como usuarios y contraseñas.
 - Nuevos esquemas de fraude detectados en otros organismos del sector.
- Para cualquier otro tipo de evento distinto a los listados solo deberá realizarse la notificación inicial.
- Deberá generarse el proceso de inteligencia accionable en cualquiera de los siguientes casos:
 - Cuando se detecte que un ataque ya sucedió y tuvo un impacto en el Instituto, para lo cual se emitirán recomendaciones hacia el Instituto.
 - En los casos donde se realice el análisis a petición del Instituto de sitios o correos relacionados con phishing así como direcciones IP, se deberá generar a partir de los hallazgos identificados inteligencia accionable donde deberán incluirse detalles sobre los sitios, direcciones IP, artefactos maliciosos, entre otros, al igual que sobre los reportes generados como parte de los servicios.
- Realizar el análisis de hasta 50 direcciones IP que el Instituto considere dudosas por mes, con el objetivo de analizarlas en búsqueda de información relacionada con ataques, además de determinar si éstas han realizado intrusiones a otros organismos de similares características a las del Instituto, si forman parte de una botnet, han sufrido un defacement, o bien forman parte de alguna campaña en particular.
- Analizar el comportamiento del hacktivismo en México y su relación con otros grupos, incluyendo el detalle de las operaciones del mes en curso, sus objetivos y el impacto de las mismas, así como recomendaciones para protegerse ante las nuevas operaciones esperadas.
- Analizar hasta 3 correos electrónicos o sitios al mes, con los cuales se realizarán entre otras las siguientes acciones:
 - Identificación de los encabezados y análisis del malware en el contenido.
 - Extracción de datos como dominios y direcciones IP, mismas que deberán ser analizadas



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

en una plataforma de “Inteligencia sobre Amenazas” para determinar el riesgo que representa el Phishing para el Instituto.

6.2.5. Servicios de Protección en Redes Inalámbricas y Seguridad en Dispositivos Móviles.

Descripción del servicio. El Instituto requiere un servicio de protección en redes inalámbricas específicas que permitan colocar controles que garanticen y protejan la información producida internamente y recibida a través de los recursos de redes inalámbricas (WLAN), contra ataques generales que buscan aprovechar esta modalidad para infiltrarse en la red de comunicaciones del Instituto, así mismo se requiere un servicio de protección de dispositivos móviles, que prevenga el robo o sustracción de información considerando para lo anterior, la administración de políticas y el cumplimiento de operación en los dispositivos móviles, por lo que el proveedor deberá cumplir con las siguientes especificaciones funcionales mínimas.

- Garantizar que las herramientas propuestas para el servicio cuenten con la última versión liberada, estable y validada, por parte del fabricante, así como para otros componentes necesarios con el que cuente el servicio correspondiente.
- Integrar el licenciamiento del software que permita habilitar los servicios y activos de infraestructura correspondientes, así como todas aquellas renovaciones necesarias durante la vigencia de los servicios.
- Proteger contra ataques informáticos comunes a la red inalámbrica (WLAN).
- Actualizar y mejorar los procesos que permitan la autenticación de usuarios internos.
- Cifrado TKIP y AES basado en *hardware*.
- Tener la funcionalidad de WIPS en tiempo real (prevención de intrusiones inalámbricas).
- Integrado en un tercer radio de banda doble específico (sin afectar el rendimiento del punto de acceso).
- Permitir aplicar políticas de control sobre las aplicaciones que los dispositivos
- Permitir la instalación de aplicaciones y ejecutar actualizaciones en múltiples dispositivos a la vez de manera remota y controlando el tipo de conexión y la fecha de ejecución
- Permitir realizar modificaciones de cambio de contraseña de bloqueo, y también se puede configurar la longitud, el tipo de contraseña, si es alfanumérica o numérica, el número de intentos, entre otros.
- Permitir a los administradores del sistema mantener y controlar estos dispositivos de forma centralizada.
- Analizar los dispositivos para asegurarse de que cumplen con la política del Instituto.
- Recuperar toda la información sobre los dispositivos, incluidos los detalles del dispositivo, certificados, aplicaciones instaladas, entre otros.
- Regular el acceso a las cuentas Institucionales tales como cuentas de correo electrónico, Wi-Fi y



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

VPN.

- Bloquear los dispositivos de forma remota para evitar robados o perdida de información.
- Deberá soportar la conexión desde dispositivos móviles y de escritorio a través de un cliente de acceso remoto. Dicho cliente debe soportar al menos las siguientes plataformas operativas: MAC OS X, iOS, Android, Windows desde v7.
- Alarmas.

6.2.6. Servicios de Gestión y Control de Acceso para Usuarios Privilegiados (AAA).

Descripción del Servicio. El Instituto requiere un servicio de control de acceso para usuarios privilegiados con la intención de entregar en los servidores las funcionalidades de control y monitoreo de las cuentas de usuarios privilegiados existentes en cada uno de ellos, así como un mecanismo de Autenticación, Autorización y Contabilización (AAA por sus siglas en inglés, Authentication, Authorization and Accounting), por lo que el proveedor deberá cumplir con las siguientes especificaciones funcionales mínimas.

- Contar con una solución tecnológica que controle de manera granular el acceso a los activos de infraestructura que soportan las aplicaciones, a través de la administración del ciclo de vida de identidades.
- Integrar procesos que identifique los roles y perfiles de cada usuario por aplicación, así como la trazabilidad de los accesos realizados.
- Considerar, de manera enunciativa más no limitativa, las siguientes plataformas operativas:
 - Microsoft Windows
 - Unix
 - Linux
- Revisar y validar en conjunto con el Instituto los requerimientos de protección de las claves privilegiadas en los servidores en que se vaya a habilitar para el servicio.
- Implementar los agentes propiciados por la solución en sistemas operativos soportados por los fabricantes correspondientes.
- El proveedor deberá llevar a cabo todas las tareas necesarias para la instalación del equipo en la zona de los Centro de Datos donde le sea solicitado.
- El proveedor deberá acordar con el personal del Gobierno de Contrato las ventanas de mantenimiento necesarias según el tiempo de implementación del que se trate.
- El proveedor deberá integrar el dispositivo hacia la consola de administración de la solución, y asegurarse que la bitácora del dispositivo quede integrada a la solución de Correlación del proyecto.
- Servicios de autenticación, autorización y registro (AAA) para habilitar el control de acceso e



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

identidad hacia la red del Instituto.

- Habilitar los activos de infraestructura requeridos en esquemas de Alta Disponibilidad (HA por sus siglas en inglés).
- Uso de RADIUS la autenticación de acceso a la red.
- Uso de TACACS+ para la autenticación para accesos administrativos a la infraestructura del Centro de Datos.
- Deberá ser capaz de soportar la administración de al menos 5,000 dispositivos de red.
- Administración centralizada para políticas de acceso de gestión y VPN.
- Capacidad de generar políticas basadas en reglas y atributos.
- Capacidad de generación de políticas con asignación de VLANs.
- Integración con bases de datos externas tales como Active Directory y LDAP.
- Capacidad de integrarse a un dominio de Directorio Activo.
- Integración con soluciones de contraseña únicas.
- Integración con los dispositivos de red para asegurar la aplicación de políticas de seguridad basadas en identidad.
- Uso de los siguientes protocolos de autenticación:
 - CHAP/MSCHAP
 - PAP
 - PEAP
 - EAP-TLS
 - MS-CHAP
 - EAP-MD5
- Generación de políticas de restricciones por dispositivo y hora del día.
- Uso de listas de acceso descargables.
- Capacidad de operar en esquemas conglomerados (clúster) con más de 3 dispositivos operando como un solo sistema.
- Capacidad de operar en esquemas de procesamiento físico (appliance) o virtualizados
- Interface de administración gráfica basada en web
- Interface de programación para actualizar, crear, leer y borrar operaciones de dispositivos, terminales y usuarios de la base de datos interna.
- Funciones de reporteo y auditoría



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- Capacidades de monitoreo y diagnóstico de problemas
- Administración de mensajes de eventos (logs) exportables.

6.2.7. Servicio de Antivirus

Descripción del servicio. El proveedor deberá proporcionar el licenciamiento, instalación, habilitación, configuración, puesta a punto, gestión, monitoreo, soporte y mantenimiento de una solución, que pueda poner en riesgo su funcionalidad, comprometiendo la seguridad en la actividad de los usuarios.

La protección de antivirus deberá realizarse a través de un agente, el cual deberá ser distribuido a los activos de infraestructura que el Instituto solicite, siendo responsabilidad del proveedor garantizar la entrega de dicho agente a los activos de infraestructura indicados por el Instituto, la distribución y administración puede ejecutarse onpremise o nube.

El proveedor deberá considerar que las actividades de remediación en infecciones de virus, serán su responsabilidad, por lo que deberá brindar el apoyo correspondiente a través de la explotación de las funcionalidades de la solución del antivirus propuesta como parte del presente servicio. El proveedor deberá notificar al personal que Instituto designe sobre los hallazgos de actividad sospechosa vía correo electrónico, u otro mecanismo que ambas partes determinen. El proveedor deberá atender los incidentes de *malware* que puedan presentarse; conforme se determine en los Acuerdos de Nivel de Servicio, o en su caso, a los Acuerdos de Nivel Operativos.

Cuando la necesidad de instalación del Instituto sea de más de 200 agentes, el proveedor, en conjunto con el Instituto, deberán definir una estrategia que permita el despliegue del agente de Antivirus, así como adecuar la estrategia de entrega de actualizaciones de Antivirus en cada uno de los activos de infraestructura solicitados, sin afectar la operación del Instituto, considerando que dichos activos y consolas de administración se encontrarán distribuidos en las diferentes localidades del Instituto.

El proveedor deberá configurar en la solución de Antivirus propuesta, las políticas base de seguridad definidas en conjunto con el Instituto, como parte de las reglas que regirá el presente servicio, para los activos de infraestructura a los cuales les sea provisto, la cual deberá ser desplegada a los mismos a través de la consola de administración de la solución. A su vez, el proveedor deberá realizar la puesta a punto de las políticas definidas en la solución de antivirus propuesta, con fundamento en el monitoreo continuo de la misma y los requerimientos del Instituto.

El proveedor deberá definir una estrategia en conjunto con el Instituto que permita el despliegue para la entrega de actualizaciones de Antivirus en cada uno de los activos de infraestructura sin afectar las operaciones de los servicios internos, los cuales se encuentran distribuidos en las diferentes localidades de la CDMX. Será responsabilidad del proveedor mantener actualizados en todo momento los activos de infraestructura con la última versión o actualización de antivirus liberada por el fabricante.

El proveedor, en conjunto con el Instituto, definirá la cantidad de activos de infraestructura que constituirá la línea base para el primer año de prestación del servicio. Posteriormente, un mes antes de cumplir cada año de servicio se realizará una redefinición de la línea base para la prestación del servicio del próximo año.

El proveedor deberá entregar al personal del Instituto la última versión del agente de antivirus, para que este sea integrado dentro de la imagen de software de los Puestos de Servicio.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Como parte de la operación del presente servicio, el proveedor deberá:

- Emitir alertas de incidentes y monitorear los eventos generados por los elementos tecnológicos de la solución de Antivirus.
- Monitorear el cumplimiento de las políticas de uso de información implantadas en la solución.
- Notificar sobre las actividades sospechosas relacionadas con la infección de activos de infraestructura.
- Notificar sobre todas aquellas actividades sospechosas que sean identificadas a través de las funcionalidades de la Solución de Antivirus, efectuando la contención de las mismas a través de la solución propuesta.
- Resolver las solicitudes de soporte técnico especializado, a fin de evitar y prevenir infecciones en los activos de infraestructura donde se encuentre instalada la solución de Antivirus.
- Recolectar e integrar, al menos la información de eventos de seguridad o logs generada por la solución de Antivirus, hacia la solución de correlación de eventos, cuyo detalle de información a integrar será definido entre el Instituto y el proveedor.
- Desarrollar la afinación de la solución con base en el resultado del monitoreo continuo, además de gestionar las reglas antivirus en los activos de infraestructura, con base en las necesidades del Instituto y en el resultado del monitoreo día a día.

6.2.8. Servicios de Prevención de Pérdida de Información

Descripción del servicio. El Instituto requiere una solución que permita detectar y evitar la fuga y/o pérdida de información sensible en los activos de infraestructura del IMSS instalados en los Centros de Datos, misma que debe estar integrada a los activos de infraestructura, servicio de correo electrónico externo, correo electrónico interno, navegación web y portales de colaboración, para una completa visualización y prevención en distintas capas de seguridad.

Dicho módulo debe tener la capacidad de generar políticas a través de palabras clave o expresiones regulares con la información sensible, bloqueando su transmisión a través de diversos canales de comunicación.

El servicio deberá enfocarse en prevenir fuga de información sensible desde los puestos de servicio.

El proveedor deberá configurar en la solución propuesta las políticas base de seguridad definidas en conjunto con el Instituto, para los activos de infraestructura, desarrollando los perfiles correspondientes.

Dichas políticas deberán ser desplegadas a través de la consola de administración de la solución, y el proveedor deberá realizar la puesta a punto de las mismas, con fundamento en su monitoreo continuo y los requerimientos del Instituto, para lo cual, el Instituto requiere que se tomen en consideración, como mínimo, las siguientes premisas:

- Tipos de documentos.
Se refiere a las formas en las cuales se pueden estructurar los activos de información que son relevantes para los procesos del Instituto: reportes, estudios, oficios, correspondencia, acuerdos, directivas, planes estratégicos, contratos, convenios, anotaciones, memorandos, estadísticas, procedimientos, políticas, reglamentos, informes, solicitudes, encuestas, históricos, entre otros.
- Medios de almacenamiento de la información.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Se refiere a los distintos medios en los cuales pueden resguardarse los activos de información para su posterior manipulación

El proveedor deberá asegurar que las funcionalidades de la Solución de Prevención de Pérdida de Información deberán cumplirse aun cuando el activo de infraestructura no se encuentre firmado a ningún Directorio Activo, o bien, a la red del Instituto.

Como parte de la operación del servicio, el proveedor deberá:

- Emitir alertas de incidentes y monitorear los eventos generados por los elementos tecnológicos de la solución de Prevención de Pérdida de Información.
- Monitorear el cumplimiento de las políticas de uso de información implantadas en la solución.
- Notificar al Instituto sobre actividades sospechosas relacionadas con la violación de las políticas sobre fuga de información configuradas en los activos de infraestructura.
- Efectuar la contención de actividades sospechosas.
- Atender a las solicitudes de soporte técnico especializado, a fin de evitar fugas de información en los equipos en los que se encuentre habilitada la solución.
- Recolectar e integrar, al menos la información de eventos de seguridad o logs generada por la solución de Prevención de Pérdida de Información, hacia la solución de correlación de eventos, cuyo detalle de la información a integrar será definido entre el Instituto y el proveedor.
- Administrar los elementos tecnológicos a través de procesos de gestión de cambios, configuraciones y versiones de acuerdo con los requerimientos del Instituto.

La solución propuesta por el proveedor deberá contar con las siguientes funcionalidades:

- Presente un log de auditoría de todas las actividades de los usuarios.
- Proporcione reportes predefinidos y personalizados que puedan ser programados o de una sola vez.
- Proporcione un mecanismo de alertas y notificaciones.
- Tecnología de Detección.
 - Capacidad para extraer textos de diferentes tipos de documentos para ejecutar escaneos de contenido.
 - Capacidad de realizar detecciones basadas en palabras (keywords) personalizadas o frases (key phrases) personalizadas, con la habilidad de poner diferentes palabras en una sola regla de detección.
- Debe de ser capaz de ejecutar escaneos de contenido en diversos canales de información (Correo, https/http, ftp, entre otros)

6.2.9. Servicios de Sistema de Gestión de Seguridad de la Información (SGSI)

Descripción del servicio. Garantizar la continuidad operativa del Sistema de Gestión de Seguridad de la Información (SGSI), que deberá estar basado en el estándar ISO/IEC 27001:2013, mediante el cual se emitirán las directivas en materia de seguridad de la información a las áreas de TI y a los terceros que soportan la operación de TI, mismo que deberá considerar las actualizaciones que correspondan.

El proveedor del servicio deberá garantizar la continuidad operativa de este servicio y deberá cumplir con al menos las siguientes funcionalidades operativas:

Planear



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- Capacitación de seguimiento – Curso “Inducción a la norma ISO/IEC 27001:2013 o vigente, que permita:
 - Conocer la estructura de la norma ISO/IEC27001:2013
 - Interpretar los requisitos solicitados para el cumplimiento de la norma
 - Conocer las etapas para la implementación de un SGSI
 - Se deberán considerar al menos 8 participantes, con un tiempo mínimo de 8 horas y máximo de 40 horas.
- Seguimiento y actualización en la aplicación de las directivas en materia de seguridad. Manual de políticas de seguridad de la información, que deberá apegarse a lo siguiente:
 - Dominios que establece la norma ISO/IEC 27001:2013
 - Procesos de seguridad aplicables en la normativa vigente.
 - Enfocarse a las áreas de TI y a los terceros que proveen servicios de TI al Instituto, considerando como alcance el catálogo de infraestructuras críticas del Instituto (al menos 20 directivas).
- Identificación y evaluación de activos (relacionado al catálogo de infraestructuras críticas) del proceso involucrado en el Sistema de Gestión de Seguridad de la Información. La metodología deberá considerar los siguientes temas:
 - Identificación de los activos del proceso.
 - Valoración de los activos del proceso.
 - Identificación de requerimientos de seguridad.
 - Identificación de los controles de seguridad existentes.
- Generación de la declaración de aplicabilidad. (SoA: Statement of Applicability). La metodología deberá considerar los siguientes temas:
 - Identificación y aplicabilidad de los requerimientos internos y externos
 - Selección de los objetivos de control y controles para el tratamiento de los riesgos
 - Verificación de requerimientos contractuales y legales
 - Identificación de los requerimientos internos y externos
 - Validación de aplicabilidad de los requerimientos
 - Formato de Autorización para implantar y operar el Sistema de Gestión de Seguridad de la Información
 - Preparación de la declaración de aplicabilidad
 - Documentar los objetivos de control y los controles elegidos y la justificación de su elección
 - Documentar los controles actualmente implementados
 - Documentar la exclusión de controles y la justificación de su exclusión
- Operación el Sistema de Gestión de Seguridad de la Información
 - Análisis de Riesgos de Seguridad de la Información
 - Análisis de riesgo con base en lo definido en el servicio de gestión de riesgos de seguridad
 - Generación de la actualización del plan de tratamiento de riesgos
La metodología deberá considerar los siguientes temas:
 - Identificación de las acciones a realizar por parte de la institución y su administración
 - Identificación de los recursos necesarios y prioridades
 - Identificación de las responsabilidades para administrar los riesgos de seguridad de la



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

información

- Aplicación del seguimiento al plan de tratamiento de riesgos.
La metodología deberá considerar los siguientes temas:
 - Asignación de los roles y responsabilidades en el seguimiento de los controles relativos a personas, procesos y tecnología involucrados en la mitigación de los riesgos.
 - Actualización de documentación, alineada a los requisitos establecidos en la normativa vigente
- Detalle y actualización de políticas y procedimientos de seguridad existentes
- Definición del proceso de reporte y atención de incidentes de seguridad
- Propuestas de implementación de los controles seleccionados.
La metodología deberá considerar los siguientes temas:
 - Control de accesos
 - Monitoreo de cuentas
 - Definición del proceso de Continuidad del negocio
 - Implantación de los Roles y responsabilidades definidas para el Sistema de Gestión de Seguridad de la Información
 - Controles de seguridad en la infraestructura tecnológica de acuerdo con lo definido en el alcance.
- Administración del cambio cultural.
La metodología deberá considerar los siguientes temas:
 - Actualización del Programa de concientización con usuarios y operadores del Sistema de Gestión de Seguridad de la Información
 - Seguimiento y apoyo a las necesidades de capacitación para el personal que administra el Sistema de Gestión de Seguridad de la Información y seguridad de la información
 - Manual de Gestión de Seguridad de la Información.
Se deberá documentar un manual que contenga las referencias generadas en esta fase para dar trazabilidad al de las cláusulas de la norma.
- Monitorear y Revisar el Sistema de Gestión de Seguridad de la Información
Revisiones gerenciales.
La metodología deberá considerar los siguientes temas:
 - Los dueños del proceso deberán hacer una revisión y actualización al Sistema de Gestión de Seguridad de la Información con la finalidad de verificar que los objetivos del Sistema de Gestión de Seguridad de la Información están alineados a los objetivos de negocio en materia de seguridad de la información y que garantizan el adecuado manejo de los riesgos existentes.
 - El proveedor deberá actualizar el procedimiento de revisiones gerenciales.
 - El proveedor actualizará los formatos requeridos para llevar a cabo las revisiones gerenciales
- Auditorías internas.
La metodología deberá considerar lo siguiente:
 - Seguimiento y apoyo en la generación del plan de auditorías internas a las áreas de TI y a los terceros que proveen servicios de TI al Instituto.
 - Actualización o en su caso definición de los formatos requeridos para llevar a cabo las



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- auditorías
- Aplicación de una auditoría interna al Sistema de Gestión de Seguridad de la Información para verificar el cumplimiento con el estándar ISO/IEC 27001:2013 o vigente y a los procesos establecidos en la normativa vigente aplicable.
- Actualización del Sistema de Gestión de Seguridad de la Información
Implementación de mejoras
Deberá considerar los siguientes temas:
 - Priorización de las acciones correctivas y no conformidades identificadas en las revisiones gerenciales, revisiones independientes, auditorías internas y revisiones técnicas
 - Identificación de los responsables de llevar a cabo las mejoras.
 - El Instituto definirá las fechas compromiso para la terminación de las mejoras, únicamente para seguimiento interno.
- Acciones correctivas y no conformidades.
Deberá considerar lo siguiente:
 - Apoyo en la definición y seguimiento del procedimiento para realizar acciones correctivas y no conformidades derivadas de las auditorias.
 - Actualización del formato para llenado de acciones correctivas y no conformidades.
 - Coordinación de la ejecución de las acciones correctivas ya definidas y en su caso las no conformidades que se identifiquen.
- Comunicar los resultados de las acciones tomadas.
Se deberá considerar lo siguiente:
 - o Apoyo en la programación de reuniones de seguimiento al Sistema de Gestión de Seguridad de la Información para dar a conocer el alcance de las acciones correctivas y no conformidades realizadas y verificar su apego a los requerimientos de los dueños de la información y a los involucrados en los procesos del Instituto.

6.2.10. Servicios Continuidad de Gestión del Cambio en Seguridad de la Información

Descripción del servicio. El Instituto requiere de la integración de un programa de gestión del cambio para la protección de la información, alineado a los requerimientos del estándar ISO/IEC27001:2013, siguiendo una estrategia cultural.

Este servicio deberá contar con un plan de transferencia de conocimiento al personal del Instituto en los principales temas de seguridad de la información considerando al menos los siguientes rubros:

- Regulación vigente en materia de seguridad de la información.
- Políticas de seguridad del Instituto.
- Procesos de seguridad del Instituto.
- Controles de seguridad implementados en el Instituto.

El servicio se describe en las etapas que a continuación se indican:

Etapa 1. Definición de la estrategia de gestión del cambio

- Contextualización del Instituto. El proveedor deberá tener el contexto cultural del Instituto en



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

materia de seguridad de la información

- Diagnóstico del estado actual. El proveedor deberá llevar a cabo un diagnóstico del nivel de conocimiento en materia de seguridad de la información que presente la brecha entre la situación actual y la situación requerida por el Instituto
- Preparación de la estrategia. El proveedor, con base en los resultados obtenidos en el diagnóstico, deberá proponer una estrategia de gestión del cambio en seguridad de la información con el fin de hacer una adecuada transferencia del conocimiento.

Etapa 2. Diseño del programa de gestión del cambio

- Preparación del programa. El proveedor deberá generar un plan de trabajo detallado con los temas que forman parte de la transferencia del conocimiento, el número de personal involucrado y las fechas en las cuales se llevará a cabo.
- Preparación de contenidos. El proveedor deberá desarrollar los materiales en formato Power Point, u otros que el Instituto defina, que serán utilizados para la transferencia del conocimiento en seguridad de la información.
- Generación del modelo de evaluación. El proveedor deberá presentar un modelo de evaluación con el fin de identificar el grado de efectividad de la transferencia de conocimiento de seguridad de la información.
- Preparación del grupo de trainees. El proveedor deberá identificar y preparar a un grupo de 5 trainees con el fin de que puedan replicar la transferencia del conocimiento a otras áreas sustantivas dentro del Instituto.

Etapa 3. Comunicación del programa de gestión del cambio

- Despliegue de la transferencia. El proveedor deberá llevar a cabo el despliegue de la transferencia del conocimiento al personal de TI del Instituto y de las áreas sustantivas definidas por este dentro de la Ciudad de México.

Etapa 4. Medición del programa de gestión del cambio

- Aplicación de evaluaciones. El proveedor habilitará una herramienta tecnológica con el fin de aplicar evaluaciones en línea a los participantes de la transferencia del conocimiento.
- Análisis de datos obtenidos. El proveedor deberá revisar la información obtenida con el fin de organizar los resultados obtenidos.
- Presentación de resultados generales. El proveedor deberá llevar a cabo una presentación ejecutiva con los resultados obtenidos al personal de TI del Instituto.

Partida 2

6.2.11. Servicios de Análisis de Vulnerabilidades Dinámico

Descripción del servicio. El Instituto requiere la continuidad operativa de un servicio que permita ejecutar análisis técnicos especializados sobre los activos de infraestructura de procesamiento, redes, sistemas y aplicaciones, con la finalidad de identificar vulnerabilidades nuevas o conocidas, por lo que el proveedor deberá cumplir con las siguientes especificaciones funcionales mínimas.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- Integrar las tareas necesarias para la ejecución de los análisis de vulnerabilidades en los centros de datos que el instituto indique, o en su caso, en aquellas otras localidades donde le sea requerido.
- Dar seguimiento a los reportes a través de las herramientas con las que se cuentan, que permiten complementar los análisis de vulnerabilidades llevados a cabo.
- Renovación del licenciamiento del software que permite continuar con los servicios y activos de infraestructura que correspondan.
- Garantizar que las herramientas de análisis de vulnerabilidades cuenten con la última versión liberada, estable y validada, por parte del fabricante, así como para otros componentes necesarios con el que cuenta el servicio.
- Identificar los servicios a analizar, incluyendo el número de equipos involucrados y la versión de las plataformas de los sistemas.
- Identificación de vulnerabilidades documentadas en organismos internacionales como el CVE (Common Vulnerability Exposures).
- Identificación de configuraciones por omisión.
- Capacidad para determinar el grado de vulnerabilidad ante técnicas de ataque como:
 - SQL injection
 - Cross Site Scripting
 - Cross Site Request Forgery
 - Sensitive Data Exposure
 - Security Misconfiguration
 - Broken Authentication and Session Management
- Elaborar un reporte ejecutivo y técnico, por cada requerimiento atendido, en el que se describan los detalles de los riesgos asociados a cada vulnerabilidad identificada utilizando la metodología de cálculo de riesgos de OWASP llamada “OWASP Risk Rating Methodology”, detallando recomendaciones y/o acciones específicas para remediar las vulnerabilidades descubiertas.
- Integrar un proceso y/o procedimiento para la continuidad de las medidas de remediación y recomendaciones descubiertas en cada revisión ejecutada.
- El proveedor de servicios deberá integrar el mecanismo operativo necesario para llevar a cabo el proceso de remediación conforme las vulnerabilidades reportadas, contemplando personal especializado para las plataformas operativas y herramientas en software descubiertas.

6.2.12. Servicios de Análisis de Vulnerabilidades Estático

Descripción del servicio. El Instituto requiere identificar el nivel inicial de madurez de las prácticas de seguridad en el software con las que cuenta el Instituto, por lo que el proveedor deberá cumplir con las siguientes especificaciones funcionales mínimas.

- Implementar una solución tecnológica que permita realizar pruebas dinámicas y estáticas de una



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

manera centralizada y con soporte al menos a los siguientes lenguajes de programación: HTML, Java, .Net, C#, PHP.

- Integrar el licenciamiento del software que permita habilitar los servicios y activos de infraestructura correspondientes, así como todas aquellas renovaciones necesarias durante la vigencia de los servicios.
- Garantizar que las herramientas propuestas para el servicio cuenten con la última versión liberada, estable y validada, por parte del fabricante, así como para otros componentes necesarios con el que cuente el servicio correspondiente.
- Integrar un proceso de evaluación de las prácticas existentes de seguridad de software en el Instituto.
- Construir un programa de evaluación de seguridad de software con iteraciones definidas en conjunto con el Instituto.
- Actualizar y crear procesos en las diferentes etapas del ciclo de vida de desarrollo de software para asegurar el mismo.
- Ayudar en el cumplimiento del software basado en estándares y/o marcos normativos previamente definidos en conjunto con el Instituto.
- Identificar el nivel inicial de madurez de las prácticas de seguridad en el software con las que cuenta el Instituto.
- Identificar y entender el entorno del Instituto, personal relacionado, normatividad y tecnologías que cubran el alcance de la entrega del servicio para identificar el modelo de operación, flujos de interacción, entre otros, de las diferentes entidades que deben ser incluidas en el proceso.
- Integrar las mejores prácticas de seguridad en el software mencionadas en el modelo de madurez propuesto y alineado a OpenSAMM.
- Realizará la transferencia de las prácticas de seguridad en el software implementadas al personal que el Instituto designe para dicho propósito.
- Operar el modelo de madurez establecido, pudiendo certificar en 3 diferentes etapas el nivel de cumplimiento el software evaluado, las cuales podrán ser:
 - Al inicio del desarrollo de una aplicativo.
 - Durante el desarrollo de un aplicativo.
 - Posterior al desarrollo de un aplicativo.
- Preservar la integridad y confidencialidad de la información recibida durante la ejecución de las pruebas dinámicas y/o estáticas correspondientes (cadena de custodia).
- Elaborar un reporte ejecutivo y técnico, por cada requerimiento atendido, donde se describa los detalles de los riesgos asociados a cada hallazgo o vulnerabilidad identificada, detallando recomendaciones y/o acciones específicas para remediar las vulnerabilidades descubiertas.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

6.2.13. Servicios de Pruebas de Penetración

Descripción del servicio. El Instituto requiere la continuidad de un servicio que permita realizar un proceso sistemático para comprobar las vulnerabilidades de las aplicaciones y la infraestructura que la soportan, con el propósito de buscar huecos o fallas en la seguridad, por lo que el proveedor deberá cumplir con las siguientes especificaciones funcionales mínimas.

- Integrar todas las tareas necesarias para la ejecución de las pruebas de penetración en los centros de datos que el instituto indique, o en su caso, en aquellas otras localidades donde le sea requerido.
- Dar seguimiento a los servicios o activos de información que deberán ser analizados, incluyendo el número de equipos involucrados, y la versión de las plataformas de los sistemas analizados.
- Identificación de vulnerabilidades y malas configuraciones.
- Explotación de acceso a los sistemas mediante el aprovechamiento de los huecos de seguridad detectados y/o vulnerabilidades detectadas.
- Evaluación de vulnerabilidades de al menos los siguientes rubros:
 - Autenticación y Autorización
 - Intentos ilimitados de inicio de sesión
 - Insuficiente autenticación
 - Insuficiente autorización
 - Gestión de sesión
 - Predicción de sesión
 - Secuestro de sesión
 - Reproducir sesión
 - Expiración de sesión insuficiente
 - Inyección de código
 - Inyección comando de Sistema Operativo
 - Inyección SQL
 - Cross-site Scripting
 - Inyección LDAP
 - Inyección HTML
 - Parameters Tampering
 - Cookie Poisoning
 - Hidden Field Manipulation
 - Criptografía
 - Fortaleza del algoritmo
 - Gestión de llaves
 - Ataques Lógicos
 - Abuso de funcionalidades



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- Input Field Validation Checking
- Protección de Datos
 - Transporte
 - Almacenamiento
- Divulgación de Información
 - Indexado de directorio
 - Path Traversal
 - Manejo inseguro de errores
 - Comentarios HTML
- Realizar un reporte ejecutivo y técnico, por cada requerimiento atendido, en el que se describan los detalles de los riesgos asociados a cada vulnerabilidad identificada utilizando la metodología de cálculo de riesgos de OWASP llamada “OWASP Risk Rating Methodology”, detallando recomendaciones y/o acciones específicas para remediar las vulnerabilidades descubiertas.
- Integrar un proceso y/o procedimiento para la continuidad de las medidas de remediación y recomendaciones descubiertas en cada revisión ejecutada.
- El proveedor de servicios deberá integrar el mecanismo operativo necesario para llevar a cabo el proceso de remediación conforme las vulnerabilidades reportadas, contemplando personal especializado para las plataformas operativas y herramientas en software descubiertas.

6.2.14. Servicios de Análisis Forense

Descripción del servicio. El Instituto requiere la continuidad de un servicio de análisis de incidentes de seguridad para determinar y documentar a través de la integración de registros o bitácoras las evidencias o indicios de eventos y su relación en el tiempo que identifiquen cuando ocurrió, que infraestructura, servicios tecnológicos o sistema de información fueron comprometidos, como fue realizado, y quien o que, estuvo relacionado con el incidente y el impacto del evento, por lo que el proveedor deberá cumplir con las siguientes especificaciones funcionales mínimas.

- Integrar las tareas necesarias para la ejecución de los análisis forenses en los centros de datos que el instituto indique, o en su caso, en aquellas otras localidades donde le sea requerido.
- Continuar con la definición del objetivo parámetros y cuestionario que resulten de interés para la investigación solicitada.
- Dar continuidad y seguimiento a los casos solicitados, así como, el registro de los indicadores correspondientes.
- Preservar la integridad de la información recibida durante la ejecución del proceso de análisis forense (cadena de custodia).
- Participar en entrevistas con los principales involucrados con la finalidad de obtener el contexto necesario en las investigaciones digitales que deban realizarse.
- Obtener información de fuentes públicas en la red en caso de que estas pudieran llegar a ser



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

relevantes para la investigación realizada.

- Realizar las evaluaciones de información en los equipos de cómputo, servidores físicos, servidores virtuales, dispositivos móviles, equipo de comunicaciones, entre otros, para la identificación de indicios de compromiso y su evidencia correspondiente.
- Llevar a cabo un proceso de recuperación de información que haya sido borrada previamente.
- Dar seguimiento a la herramienta colaborativa que tiene por objeto facilitar la visualización de hallazgos a los usuarios finales, así como generar reportes de hallazgos en caso de ser requerido.
- Elaborar un dictamen técnico, por cada requerimiento atendido, con la información identificada en el o los procesos de análisis forense, considerando la generación y firma de los documentos que expresen los resultados de la investigación en forma clara y concisa, de manera que puedan ser comprendidos por aquellos que no conocen o dominen el lenguaje técnico.

6.3. Servicios del Centro de Operaciones de Seguridad (SOC)

El Instituto requiere que el proveedor del servicio cuente con un Centro de Operaciones de Seguridad (SOC), que se encuentre físicamente en las instalaciones del proveedor. El objetivo de este centro deberá ser la continuidad operativa a la gestión de la seguridad, así como el responsable de la administración, operación, monitoreo, soporte y atención a fallas de los componentes de las soluciones de seguridad, que ejecute actividades de revisiones de seguridad, correlación de eventos, monitoreo de servicios, administración de bitácoras, atención y respuesta a incidentes, así como el establecimiento de acciones de mejora sustentable.

El servicio del Security Operation Center (SOC) que soportará la operación y prestación del servicio requerido por el Instituto, deberá proporcionar un control continuo, una mayor eficiencia y oportunidad de mejora, para lo anterior el licitante deberá proporcionar servicios de tecnología de la información fiables en lo referente a la gestión de servicios de TI, mismos que deberá acreditar con las certificaciones ISO/IEC27001:2013 e ISO/IEC 20000-1:2018 vigentes y a nombre del Licitante.

El Licitante, deberá considerar que el servicio de SOC se refiere a las soluciones propuestas e implementadas hoy en día por el instituto, así mismo deberá considerar que la correlación de bitácoras se deberá basar en un servicio de correlación de eventos e incidentes de seguridad en el que los casos de uso deberán ser ilimitados, así como las respuestas ante un incidente alineadas a tiempo de los niveles de servicio (SLA) establecidos para este servicio.

- Ubicarse dentro de territorio nacional, mismo que podrá acreditar con la copia simple a nombre del SOC del licitante del ISO/IEC27001:2013 e ISO/IEC20000-1:2018.
- Operación continua las 24 horas del día, los 7 días de la semana y durante los 365 días del año (7x24x365), esto último conforme la vigencia del contrato.
- Contar con personal para la atención del servicio en sitio y de forma remota, el cual deberá ser personal calificado con base en las credenciales requeridas para la administración y monitoreo de los componentes que integran la solución.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- Operación en un centro de datos alterno ubicado dentro de territorio nacional.
- Mantenimiento de las suscripciones a sitios y listas de empresas, fabricantes y medios especializados en seguridad de la información, que permitan alertar sobre nuevas vulnerabilidades.
- Infraestructura dedicada para la administración, operación y monitoreo de los componentes hardware y software que componen los servicios de seguridad.
- Realizar evaluaciones operativas a los servicios (herramienta de software y activos de infraestructura) que permitan identificar, entre otros, mejoras en el desempeño de los activos, mejoras en la gestión de configuraciones, detección de nuevas funcionalidades operativas derivadas de actualizaciones en versiones de hardware y/o software. Dichas evaluaciones deberán ejecutarse cada 3 meses, desde el inicio de operaciones de los servicios y hasta 3 meses antes del término de estos.
- Realizar acciones correctivas y preventivas para asegurar la confidencialidad, integridad y disponibilidad de la información que se maneja en las diferentes soluciones de seguridad.
- Notificaciones y alertas personalizadas, en caso de desviaciones, anomalías o brechas de seguridad, para cada una de las soluciones de seguridad.
- Revisiones continuas a la operación del SOC, que permitan establecer mejora en los procesos, procedimientos y controles de seguridad.
- Analizar los eventos de seguridad y administración de bitácoras que se integran en los servicios de correlación de información, a fin de establecer acciones preventivas a través de modificaciones a las configuraciones de las soluciones de seguridad.
- Integrar un Equipo de Atención y Respuesta a Incidentes de Seguridad.
- Soporte y Atención a fallas a los componentes hardware y software que integran la solución, conforme los estipulado en los acuerdos de niveles de servicio
- Monitorear la disponibilidad de los componentes hardware y software que integran la solución ofertada. La solución de monitoreo debe tener la capacidad de generar alertas y notificaciones en caso de fallas, degradación del desempeño de procesamiento de información, intermitencia y/o pérdida de disponibilidad.
- Realizar mantenimiento preventivo y correctivo a las soluciones de seguridad habilitadas, así como a los activos de infraestructura que soportan cada servicio.
- Ejecutar procesos operativos para al menos los siguientes rubros:
 - Gestión de Riesgos
 - Gestión de Continuidad
 - Monitoreo y Detección
 - Gestión de Seguridad de la información
 - Administración de Dispositivos
 - Gestión de solicitudes de servicio



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- Administración de Cambios Operacionales
 - Administración de Configuraciones
 - Administración de Vulnerabilidades
 - Gestión de Incidentes
 - Gestión de Problemas
- Integración de una Mesa de servicio apegada a ITIL v4, la cual debe integrarse con la Mesa de Servicios Tecnológicos del Instituto, considerando todas las actividades de puesta a punto, desarrollo de piezas de software, configuraciones, entre otros, que permitan establecer la comunicación para la generación de requerimientos, cambios, incidentes, y otros procesos que determine el Instituto.
 - El servicio de requerimientos, cambios, incidentes, entre otros, deberá permitir la generación de eventos (tickets), mediante los mecanismos que se establezcan en las mesas de trabajo correspondiente, que, de manera enunciativa más no limitativa, podrán ser:
 - Un número telefónico directo en las instalaciones del SOC.
 - Un número telefónico a diez dígitos.
 - Correo Electrónico
 - Portal Web
 - El personal del proveedor del servicio, que atenderá las operaciones de los servicios de seguridad, deberá contar con experiencia probada en las áreas de tecnología y de seguridad de la información previamente mencionadas, para lo cual, deberá integrarse el currículum vitae de todo el personal que participe en el servicio, indicando al menos:
 - Experiencia profesional: bajo este rubro, se considerarán todos los puestos que cada integrante haya desempeñado, con fecha, nombre de los empleadores, nombre de los puestos que ha ejercido y el tipo de funciones bajo su responsabilidad, y deberá contar con experiencia comprobable al menos 3 años.
 - Experiencia en proyectos de su especialidad en Seguridad de la Información: bajo este rubro se citarán y describirán todos los proyectos en que se ha participado, y deberá contar con experiencia comprobable de al menos 3 años.
 - Estudios: bajo este rubro se anotarán todos los estudios en materia de seguridad de la información, así como las certificaciones que en su caso haya logrado y que se encuentren vigentes a la fecha de presentación de la propuesta técnica. Las certificaciones son de tecnología y/o de seguridad de tipo “vendor-neutral”.
 - Incluir la estructura del grupo de trabajo, indicando por cada perfil las responsabilidades y competencias
 - El Instituto podrá solicitar la revisión de la infraestructura de seguridad por un tercero en cualquier momento, durante la vigencia del contrato, con la finalidad de dar certeza de la entrega del servicio.
 - Seguimiento a la Base de Datos de la Gestión de la Configuración (CMDB por sus siglas en inglés) que contenga los detalles relevantes de cada elemento de configuración (CI) y de la relación entre ellos, incluyendo el equipo físico, software y la relación entre incidencias, problemas, cambios y otros datos del servicio de seguridad.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- Generar los reportes de Inteligencia de Negocio y Analítica de Información que permitan tener estadísticas del uso y desempeño de los servicios de seguridad, esto último con el objetivo de coadyuvar a la toma de decisión estratégica y operativa de los servicios, así como para determinar el plan de capacidad de cada tecnología implementada. Dichos reportes podrán considerar, de manera enunciativa más no limitativa, la siguiente información:
 - Estadísticas de uso de procesamiento por tecnología
 - Estadísticas de desempeño por tecnología (throughput)
 - Estadísticas de ataques informáticos bloqueados.
 - Estadísticas de comportamientos tipo esperado de uso por tecnología (líneas base)
 - Estadísticas de usuarios concurrentes por servicio.
 - Estadísticas de crecimiento diario, mensual y anual por cada servicio.
- Proporcionar al Instituto cuentas de acceso a las consolas de administración de los servicios de seguridad, así como herramientas en software que permitan acceder a las mismas (aplicaciones cliente-servidor, portales web u otro que se encuentre disponible), las cuales deberán ser de solo lectura, y cuyos atributos de consulta se definirán en las mesas que para este propósito se integren.
- Las consolas de administración provistas para los servicios de seguridad deberán permitir visualizar al menos:
 - Políticas: Control de Acceso
 - Configuraciones: Listas de Control de Acceso (Listas Blancas, Listas negras), Líneas base de seguridad.
 - Objetos: Usuarios, Grupos, Direcciones IP
 - Bitácoras.
 - Estadísticas en tiempo real: Desempeño, procesamiento, usuarios conectados, conexiones por segundo, ancho de banda utilizado.
- Proporcionar al Instituto cuentas de acceso a las bases de conocimiento de las tecnologías integradas para cada solución o servicio, donde se pueda consultar información sobre los casos de soporte generados, documentación técnica de los servicios, pólizas de mantenimientos vigentes, licenciamiento adquirido para cada servicio proporcionado, y otras que sirva para la toma de decisión respecto al uso de los servicios de seguridad.
- Integrar un Tablero de Estadísticas de Servicios de Seguridad a través de un portal único de administración de los servicios de seguridad de forma independiente a las consolas de administración de los servicios de seguridad, así como de las herramientas de monitoreo que contenga información estratégica sobre el uso de los servicios en tiempo real y de manera histórica, y que permita al Instituto tener el contexto general sobre el desempeño de las soluciones, su estado de salud, incidentes registrados, reportes de actividades sospechosas relevantes a nivel mundial, u otra información relevante que permita tomar decisiones sobre las condiciones de operación de los servicios, el licitante ganador debe incluir en su oferta económica los costos asociados al desarrollo para el cumplimiento de éste requerimiento.
- Permitir al personal que designe el administrador del contrato, generar reportes explotando todas las variables y funcionalidades de la herramienta de monitoreo, con la opción de parametrizar dichos reportes y consultarlos vía web.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

6.5. Condiciones para la implementación de los servicios

El proveedor del servicio de SASI 2022-2024, será responsable de llevar a cabo la implementación de los servicios solicitados conforme a los plazos descritos en el presente documento, lo cual incluye las renovaciones o migraciones de tecnología que el cumplimiento de SASI 2022-2024, implique para la prestación puntual de dichos servicios.

En todos los casos, los servicios se aceptarán siempre y cuando la totalidad de los componentes habilitadores, y sus funcionalidades requeridas, hayan sido correctamente entregadas y aceptadas por el Administrador del Contrato y las áreas del Instituto que deban involucrarse, dependiendo de la naturaleza del servicio.

El proveedor del servicio de SASI 2022-2024, deberá considerar que el Instituto proveerá los servicios de energía eléctrica y hosting en los centros de datos y localidades donde residirán los componentes habilitadores requeridos para soportar cada uno de los servicios de SASI 2022-2024. Los insumos necesarios para la instalación, energización y todos los componentes de *hardware* y *software* necesarios para la incorporación de las soluciones propuestas por el licitante ganador a la red del Instituto, será a cargo del licitante adjudicado.

Para la instalación, configuración y habilitación de cada una de las soluciones de los servicios, el proveedor de SASI 2022-2024, deberá considerar el apego a los procesos y procedimientos de control de cambios del Instituto para la integración de la infraestructura los Centros de Datos del Instituto. El detalle de estos procesos y procedimientos se proporcionarán en las Mesas de Trabajo entre el licitante ganador de SASI 2022-2024, y el Instituto.

Es importante señalar que, el licitante adjudicado deberá contar con un proceso para la gestión de solicitudes que impliquen cualquier tipo de modificación o cambio en los componentes habilitadores requeridos en la descripción particular de cada uno de los servicios; para tal efecto, el licitante ganador deberá entender el control de cambios como la función de agregar, remover o modificar debidamente los componentes habilitadores y/o las configuraciones que lo necesiten, con la finalidad de ejecutar algún cambio orientado a satisfacer las necesidades del Instituto, sin afectar la continuidad de la operación, del negocio o de la seguridad de la información.

6.6. Implementación de los servicios

Las obligaciones contractuales mínimas del proveedor adjudicado, sin menoscabo de realizar aquellas que no estén incluidas en este apartado y que sean necesarias para cumplir con los requerimientos de servicio de SASI 2022-2024, son las siguientes:

- **Implementación de Servicios:** corresponde a la provisión, entrega, montaje e instalación física y lógica de todos los componentes de hardware, software, así como y puesta en marcha de todas las funcionalidades requeridas para cada uno de los servicios. Esto incluye conexiones a la red eléctrica e integración a la Red, así como asegurar la interoperabilidad con el resto de los componentes del Centro o los Centro de Datos del Instituto y ejecución de pruebas a nivel red y aplicativo, los componentes, equipos, accesorios, herramientas y todo lo necesario para el cumplimiento del presente apartado, debe quedar incluido en la propuesta del licitante ganador.
- **Migración de servicios Seguridad:** Corresponde a la responsabilidad de entregar un plan de



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

migración, así como las correspondientes actividades en las que involucra migración de flujos de seguridad que se deben brindar en los componentes habilitadores que el proveedor de SASI 2022-2024, proveerá al Instituto. Estas actividades involucra a las tecnologías de conmutación, enrutamiento, centro de datos, seguridad, sin menoscabo de migrar aquellos flujos que no estén incluidas en este apartado y que sean necesarias para la entrega correcta del plan de migración requeridas en este proyecto, siendo los proveedores salientes quienes entreguen los flujos de comunicación y seguridad necesarios al proveedor de SASI 2022-2024, en forma documental al gobierno de contrato y áreas de tecnología involucradas del Instituto antes de comenzar las labores de implantación para su validación.

- **Operación estable del proyecto:** Pruebas integrales de todas las funcionalidades de los Componentes Habilitadores y la conectividad e interoperabilidad con el resto de los Componentes del Centro de Datos. El proveedor adjudicado llevará a cabo la integración y pruebas de la infraestructura de Comunicaciones, Seguridad, software y de las herramientas asociadas que aseguren que toda la infraestructura y componentes que conforman, se encuentren operando correctamente como un solo sistema integral (pruebas de conectividad, reglas de flujos de comunicaciones, políticas de seguridad, funcionalidades, seguridad, monitoreo y gestión).

6.7. Mesas de Trabajo

El proveedor adjudicado será responsable de integrar al servicio de SASI 2022-2024, una mesa de trabajo para la atención de los diferentes requerimientos que puedan surgir durante la vigencia del contrato.

Este servicio deberá estar disponible a lo largo de la vigencia del presente contrato. De este modo, el licitante adjudicado será el responsable de asignar personal con experiencia y expertos para conformar las mesa de trabajo. En caso de que el personal asignado sea retirado del servicio de SASI 2022-2024, será responsabilidad del licitante adjudicado notificar al Instituto con anticipación el motivo y fecha de su remoción de manera oficial. Así también será responsable de notificar de qué manera se llevará a cabo la sustitución del recurso en un esquema que garantice siempre la continuidad y calidad de los servicios requeridos.

El proveedor adjudicado será responsable de instrumentar las mesas de trabajo tanto para las funcionalidades que utilice la infraestructura, así como también aquellas que impliquen una reingeniería de la misma, en las que se desarrollarán reportes de evaluación de postura de redes y seguridad del servicio, se documentarán conclusiones y recomendaciones de modificación de la infraestructura de la red y seguridad como mejora u optimización de la disponibilidad, capacidad y desempeño de los recursos y seguridad de las aplicaciones que viven en los centros de datos del Instituto.

El Instituto podrá en cualquier momento de la vigencia del contrato de SASI 2022-2024, solicitar al proveedor adjudicado del servicio de diseño para cambios relevantes que se planeen efectuar en la infraestructura de red y seguridad que conforman el presente proyecto.

A continuación, se enlistan las responsabilidades mínimas que tendrá que llevar a cabo el licitante adjudicado, sin menoscabo de realizar aquellas que no estén incluidas en este apartado y que sean necesarias para cumplir con los requerimientos solicitados.

- Generar reportes de estado de salud y proponer mejoras y/o soluciones arquitectónicas de la infraestructura de red y seguridad.
- Análisis de impacto de nuevos requerimientos que requieran el uso de la Infraestructura de red y



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

seguridad existente en el contrato de SASI 2022-2024.

- Desarrollo de recomendaciones de optimización de anchos de banda, mejores rutas, optimización de la infraestructura.
- Diseño de mejoras sobre la infraestructura y recomendaciones que brinden el más alto desempeño y nivel de servicio.
- Entrega de reportes proactivos de recomendaciones de actualizaciones de software de los componentes habilitadores que conforman el contrato SASI 2022-2024.
- Entrega de reporte de análisis detallado del comportamiento de la red de comunicaciones y elementos de seguridad que conforman el contrato SASI 2022-2024.
- Todas las propuestas de configuración avanzada o configuración de nuevas funcionalidades propuestas por el licitante ganador de SASI 2022-2024 deben de estar validadas por personal certificado y con experiencia del proveedor del servicio de SASI 2022-2024.
- Consultoría y recomendaciones de arquitectura de Centro de Datos en base a sus mejores prácticas, dimensionamiento, uso adecuado de recursos.
- Revisión de los requerimientos de diseño, prioridades y objetivos de acuerdo a lo especificado por el administrador del contrato.
- Revisión de la arquitectura y topología de la infraestructura de la red.
- Revisión de la configuración de protocolos.
- Revisión de la configuración de características de los servicios.
- Revisión de las mejores prácticas en materia de seguridad informática.
- Recomendación y diseños que permitan incrementar de manera notable las funcionalidades y que conforman la infraestructura tecnológica del Instituto.

6.8. Perfil del Proveedor

El proveedor deberá contar con la capacidad, flexibilidad, solvencia económica y competencia técnica certificada que permita implementar y operar las soluciones de seguridad y sus mecanismos con todo lo necesario para su correcto funcionamiento, en los sitios en donde “EL INSTITUTO” lo requiera conforme a las características y especificaciones mencionadas en el presente Anexo Técnico.

El personal del proveedor del servicio, que atenderá las operaciones de los servicios de seguridad, deberá contar con experiencia probada en las áreas de tecnología y de seguridad de la información previamente mencionadas, para lo cual, deberá integrarse el currículum vitae de todo el personal que participe en el servicio, indicando al menos:

- Experiencia profesional: bajo este rubro, se considerarán todos los puestos que cada integrante haya desempeñado, con fecha, nombre de los empleadores, nombre de los puestos que ha ejercido y el tipo de funciones bajo su responsabilidad, y deberá contar con experiencia comprobable al menos 3 años.
- Experiencia en proyectos de su especialidad en Seguridad de la Información: bajo este rubro se citarán y describirán todos los proyectos en que se ha participado, y deberá contar con experiencia comprobable de al menos 3 años.
- Estudios: bajo este rubro se anotarán todos los estudios en materia de seguridad de la información, así como las certificaciones que en su caso haya logrado y que se encuentren vigentes a la fecha de presentación de la propuesta técnica. Las certificaciones son de tecnología y/o de seguridad de tipo “vendor-neutral”.
- Incluir la estructura del grupo de trabajo, indicando por cada perfil las responsabilidades y competencias.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

El currículo vitae de todo el personal que participe en el servicio, se acreditará siempre y cuando contenga todas y cada una de las características requeridas, por lo que el incumplimiento de la presentación de este, afectaría la solvencia de la propuesta.

Se deberá acreditar al menos la licenciatura o ingeniería en informática, telecomunicaciones, computación o carrera a fin, en los términos que establece la Ley Reglamentaria del Art. 5 Constitucional, la acreditación será con el título y cédula profesional y para el caso de estudios en el extranjero, estos deberán estar avalados por las instancias oficiales correspondientes, así como estar debidamente apostillados.

A continuación, se listan las credenciales y capacidades que deberán cubrir los recursos asignados al proyecto:

Partida 1

Perfil	Certificaciones a demostrar	Experiencia a desmostrar	Función	Número de recursos
Administrador del Centro de Operaciones de Seguridad (SOC)	Se deberá presentar alguna las siguientes certificaciones vigentes: CISM (Certified Information Security Manager) CISSP (Certified Information Systems Security Professional) CRISC (Certified in Risk and Information Systems Control)	3 años de experiencia en participación de proyectos de seguridad de la información.	Responsable de la administración, monitoreo, operación de los servicios proporcionados por el SOC, así como del soporte, atención a fallas e incidentes de seguridad	Al menos 1
Administración y Operación de soluciones y herramientas tecnológicas	Consultor especializado en cada una de las soluciones de seguridad integradas. Se aceptan como documentos comprobables el certificado vigente que haya tomado directamente del fabricante o de un centro de entrenamiento autorizado por el fabricante.	3 años de experiencia en participación de proyectos de seguridad de la información.	Operar administrar y monitorear las soluciones de seguridad propuestas.	Al menos 3
Líder de proyecto	Se deberá presentar alguna las siguientes certificaciones vigentes: PMP (Project Manager Professional) Certificado por PMI ITIL v4 (Expert o Master) EC-Council Project Management In IT Security (PMITS)	3 años de experiencia en participación de proyectos de seguridad de la información.	Es la persona encargada de administrar y coordinar el proyecto	Al menos 1



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Perfil	Certificaciones a demostrar	Experiencia a desmostrar	Función	Número de recursos
Operador de la mesa de servicio SOC	Se deberá presentar la siguiente certificación vigente: ITIL v4 Foundation Certification	3 años de experiencia en participación de proyectos de seguridad de la información.	Personal encargado de las operaciones de soporte de primer nivel, el monitoreo de los servicios, así como del registro y seguimiento de solicitudes de ventanas de mantenimiento, reportes de fallas y requerimientos	Al menos 4
Arquitecto Especializado en Redes y Seguridad	Se deberá presentar alguna las siguientes certificaciones vigentes: CCNP (Cisco Certified Network Professional) CCIE Enterprise Infrastructure (Cisco Certified Internetwork Expert) CCIE Security (Cisco Certified Internetwork Expert)	3 años de experiencia en participación de proyectos de redes y seguridad de la información.	Responsable de la administración, monitoreo, operación de los servicios proporcionados por el SOC, en lo que a servicios de interconexión de red se refiere, así como del soporte, atención a fallas e incidentes que se presenten en la interoperabilidad con otros proveedores y/o fabricantes	Al menos 1

Partida 2

Perfil	Certificaciones a demostrar	Experiencia a desmostrar	Función	Número de recursos
Líder de proyecto	Se deberá presentar alguna las siguientes certificaciones vigentes: PMP (Project Manager Professional) Certificado por PMI ITIL v4 (Expert o Master) EC-Council Project Management In IT Security (PMITS)	3 años de experiencia en participación de proyectos de seguridad de la información.	Es la persona encargada de administrar y coordinar el proyecto	Al menos 1
Analista de Seguridad	Se deberá presentar la siguiente certificación vigente: CEH (Certified Ethical Hacker)	3 años de experiencia en participación de proyectos de seguridad de la información.	Responsable de ejecutar las revisiones de seguridad sobre las aplicaciones y la infraestructura, así como prever, detectar, analizar, contener, erradicar, documentar incidente de seguridad	Al menos 2



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Perfil	Certificaciones a demostrar	Experiencia a desmostrar	Función	Número de recursos
Consultor de Penetración	Se deberá presentar alguna las siguientes certificaciones vigentes: GPEN (GIAC Certified Penetration Tester) CEH (Certified Ethical Hacker)	3 años de experiencia en participación de proyectos de seguridad de la información.	Realizar simulacros de ataque a la red de la infraestructura o las aplicaciones para determinar lo que los atacantes pueden acceder y qué problemas pueden causar Evaluar la seguridad de la infraestructura de red y aplicaciones utilizando herramientas y técnicas que un atacante podría utilizar	Al menos 1
Consultor Forense de Cómputo	Se deberá presentar alguna las siguientes certificaciones vigentes: EnCE (EnCase Certified Examiner) CHFI (Certified Hacker Forensics Investigator)	3 años de experiencia en participación de proyectos de seguridad de la información.	Analizar, en el supuesto de un ataque y penetración exitoso a la infraestructura, la metodología de ataque para determinar cómo se logró, cuál fue el alcance del daño, logrando así determinar las medidas preventivas a implementar. Debe tener la capacidad de ejecutar investigaciones forenses en caso de ser necesario	Al menos 1

7. Condiciones técnicas de aceptación de entregables

Durante la habilitación, transición y operación de los servicios de seguridad, el Instituto requiere recibir distintos tipos de documentos, reportes, artefactos, dictámenes o esquemas que favorezcan el desempeño y la continuidad del servicio, y que den certidumbre a las actividades diarias que el proveedor efectuará bajo la supervisión de los funcionarios designados por este último para tales efectos.

7.1. Entregables Generales

Durante la habilitación, transición y operación de los servicios de seguridad, el Instituto requiere recibir distintos tipos de documentos, reportes, artefactos, dictámenes o esquemas que favorezcan el desempeño y la continuidad del servicio, y que den certidumbre a las actividades diarias que el proveedor efectuará bajo la supervisión de los funcionarios designados por este último para tales efectos.

Partida 1

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
----------	------------	--------------	---------



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
Servicios de Habilitación, Operación y Transición	Plan de Trabajo Detallado de los servicios del proyecto	Única Vez	15 días naturales posteriores a la emisión del fallo
	Documento Compromiso de suscripción del acuerdo de niveles operacional (<i>Operational Level Agreement, OLA</i>)	Única Vez	15 días naturales posteriores a la emisión del fallo
	Matriz de Escalación	Única Vez	15 días naturales posteriores a la emisión del fallo
	Escrito por parte del proveedor, firmado por el representante legal, donde declare sus habilidades, competencias y capacidades para soportar la prestación de los servicios	Única Vez	15 días naturales posteriores a la emisión del fallo
Servicios de Seguridad – Continuidad Operativa	Documento con el diseño de Alto Nivel de las Soluciones de Seguridad a implementar en los centros de datos o donde lo indique el Instituto	Única Vez	5 días hábiles posteriores a la integración de las mesas de trabajo por cada servicio que se pretenda habilitar
	Documento con el diseño de Bajo Nivel de las Soluciones de Seguridad a implementar en los centros de datos o donde lo indique el Instituto	Única Vez	10 días hábiles posteriores a la integración de las mesas de trabajo por cada servicio que se pretenda habilitar



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
Servicios de Seguridad – Verificación/Calidad	Memorias Técnicas Iniciales de las Soluciones de Seguridad Implementadas	Única Vez	10 días hábiles posteriores al término de la habilitación de todos los componentes en los Centro de Datos o donde lo indique el Instituto, conforme cada solución integrada y posterior a la integración de las mesas de trabajo
	Memorias Técnicas Actualizadas de las Servicios de Seguridad	Única Vez	20 días hábiles previo al término del contrato para aquellos servicios que se encuentren habilitados
Servicios de Seguridad – Verificación/Calidad	Documento con el diseño de Alto Nivel de los servicios de Seguridad a implementar en los centros de datos o donde lo indique el Instituto, que requieran integrar activos de infraestructura para su habilitación	Única Vez	5 días hábiles posteriores a la integración de las mesas de trabajo por cada servicio que se pretenda habilitar
	Documento con el diseño de Bajo Nivel de las Soluciones de Seguridad a implementar en los centros de datos o donde lo indique el Instituto	Única Vez	10 días hábiles posteriores a la integración de las mesas de trabajo por cada servicio que se pretenda habilitar



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
	Memorias Técnicas Iniciales de las Soluciones de Seguridad Implementadas, que requieran integrar activos de infraestructura para su habilitación	Única Vez	10 días hábiles posteriores al término de la habilitación de todos los componentes en los Centro de Datos o donde lo indique el Instituto, conforme cada solución integrada y posterior a la integración de las mesas de trabajo
	Memorias Técnicas Actualizadas de las Servicios de Seguridad, que requieran integrar activos de infraestructura para su habilitación	Única Vez	20 días hábiles previo al término del contrato para aquellos servicios que se encuentren habilitados
Servicios de Borrado Seguro de Información	Procedimientos de Operación del servicio	Única Vez	10 días hábiles posteriores a la integración de las mesas de trabajo
Servicio de Gestión de Dominios	Procedimientos de Operación del servicio	Única Vez	10 días hábiles posteriores a la integración de las mesas de trabajo
Servicio de Certificados Digitales SSL	Procedimientos de Operación del servicio	Única Vez	10 días hábiles posteriores a la integración de las mesas de trabajo
Servicios de Sistema de Gestión de Seguridad de la Información (SGSI)	Metodología para la continuidad de los servicios	Única Vez	10 días hábiles posteriores a la integración de las mesas de trabajo



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
Servicios de Gestión del Cambio en Seguridad de la Información	Metodología para la implementación de los servicios	Única Vez	10 días hábiles posteriores a la integración de las mesas de trabajo
Servicios del Centro de Operaciones de Seguridad (SOC)	Procesos de operación implementados: • Requerimientos • Cambios • Configuraciones • Incidentes • Problemas • Monitoreo	Única Vez	15 días naturales posteriores a la emisión del fallo
	Matriz de Escalación Técnica y Organizacional	Única Vez	15 días naturales posteriores a la emisión del fallo
	Procedimiento de operación de la Mesa de Servicios: • Requerimientos • Cambios • Configuraciones • Incidentes • Problemas • Monitoreo	Única Vez	15 días naturales posteriores a la emisión del fallo
	Expedientes Curriculares del personal del SOC	Única Vez	15 días naturales posteriores a la emisión del fallo
Tablero de Estadísticas de Servicios de Seguridad (Portal Único)	Creación de cuentas de acceso en portal único de las soluciones de seguridad	Única Vez	10 días hábiles posteriores al término de la habilitación de los componentes en los Centro de Datos o donde lo indique el Instituto, conforme cada solución integrada y posterior a la integración de las mesas de trabajo



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Partida 2.

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
Servicios de Habilitación, Operación y Transición	Plan de Trabajo Detallado de los servicios del proyecto	Única Vez	15 días naturales posteriores a la emisión del fallo
	Documento Compromiso de suscripción del acuerdo de niveles operacional (<i>Operational Level Agreement</i> , OLA)	Única Vez	15 días naturales posteriores a la emisión del fallo
	Matriz de Escalación	Única Vez	15 días naturales posteriores a la emisión del fallo
	Escrito por parte del proveedor, firmado por el representante	Única Vez	15 días naturales posteriores a la emisión del fallo
	legal, donde declare sus habilidades, competencias y capacidades para soportar la prestación de los servicios	Única Vez	
Servicios de Análisis de Vulnerabilidades Dinámico	Procedimientos de Operación del servicio	Única Vez	10 días hábiles posteriores a la integración de las mesas de trabajo
Servicios de Pruebas de Penetración	Procedimientos de Operación del servicio	Única Vez	10 días hábiles posteriores a la integración de las mesas de trabajo
Servicios de Análisis Forense	Procedimientos de Operación del servicio	Única Vez	10 días hábiles posteriores a la integración de las mesas de trabajo





Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Servicios de Análisis de Vulnerabilidades Estático	Procedimientos de Operación del servicio	Única Vez	10 días hábiles posteriores a la integración de las mesas de trabajo
--	--	-----------	--

7.2. Entregables bajo demanda

El proveedor, de manera enunciativa más no limitativa, deberá generar entregables para los servicios de seguridad, que incluya al menos los siguientes conceptos:

Partida 1.

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
Servicios de Borrado Seguro de Información	Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las actividades de borrado seguro ejecutadas por cada activo o grupo de activos de infraestructura procesados, donde se integre el o los certificados de borrado por cada medio de almacenamiento analizado y que incluya al menos: fecha, hora, datos del activo de infraestructura, dispositivos de almacenamiento borrado.	Evento	5 días hábiles posteriores a la solicitud generada por parte del Instituto
Servicio de Gestión de Dominios	Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de los dominios que se hayan renovados adquiridos.	Evento	5 días hábiles posteriores a la solicitud generada por parte del Instituto



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
Servicio de Certificados Digitales SSL	Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de los certificados que se hayan renovado o adquiridos (incluyendo archivo electrónico comprado con la llave pública relacionada con los requerimientos)	Evento	1 día hábil posteriores a la solicitud generada por parte del Instituto
Servicios de Sistema de Gestión de Seguridad de la Información	Plan de Trabajo de continuidad y operación de los servicios conforme al alcance definido en las mesas de trabajo	Evento	10 días hábiles posteriores a la solicitud generada por parte del Instituto
Servicios de Gestión del Cambio en Seguridad de la Información	Plan de Trabajo de continuidad y operación de los servicios conforme al alcance definido en las mesas de trabajo	Evento	10 días hábiles posteriores a la solicitud generada por parte del Instituto
Servicios del Centro de Operaciones de Seguridad (SOC)	Creación de cuentas de acceso en las consolas de administración de las soluciones de seguridad	Evento	5 días hábiles posteriores al término de la implementación de cualquier solución de seguridad o conforme a cada solicitud generada por el Instituto
	Creación de cuentas de acceso en la base de conocimientos de las soluciones de seguridad	Evento	5 días hábiles posteriores al término de la implementación de cualquier solución de seguridad o conforme cada solicitud generada por el Instituto
	Actualización de la matriz de escalación	Evento	5 días hábiles posteriores a la incorporación o sustitución de nuevo personal del Centro de Operaciones de Seguridad y Red



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
	Reportes Técnicos de las ventanas de mantenimiento ejecutadas en las soluciones de seguridad y red	Evento	5 días hábiles posteriores a la ejecución de la ventana mantenimiento
	Reporte con Estadísticas de uso y desempeño (información analítica) de las soluciones de seguridad y red	Evento	5 días hábiles posteriores a la solicitud generada por parte del Instituto
	Reporte Técnico de las configuraciones de las soluciones de seguridad y red	Evento	5 días hábiles posterior a la solicitud generada por parte del Instituto
	Reporte Técnico de los incidentes presentados en las soluciones de seguridad y red	Evento	5 días hábiles posteriores a la solicitud generada por parte del Instituto
	Reporte Técnico de los requerimientos registrados en la mesa de servicios	Evento	5 días hábiles posteriores a la solicitud generada por parte del Instituto
	Reporte Técnico del inventario de los activos de infraestructura integrados en las soluciones de seguridad y red, así como su diagrama de interrelación conforme fueron registrados en la CMDB	Evento	5 días hábiles posteriores a la solicitud generada por parte del Instituto
	Diagramas de Arquitectura de las soluciones de seguridad y red	Evento	2 días hábiles posteriores a la solicitud generada por parte del Instituto

Partida 2

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
----------	------------	--------------	---------



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
Servicios de Análisis de Vulnerabilidades Dinámico	Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las vulnerabilidades detectadas por cada activo o grupo de activos de infraestructura escaneados indicando al menos: Activo(s) de infraestructura o aplicativo relacionado, fecha de escaneo, direccionamiento IP, vulnerabilidades detectadas (Alta, Media, Baja), recomendaciones para remediación de hallazgos y que incluya los archivos electrónicos fuente de las herramientas tecnológicas utilizadas para el proceso de análisis	Evento	7 días hábiles posteriores a la solicitud generada por parte del Instituto



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
Servicios de Prueba de Penetración	Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las vulnerabilidades detectadas por cada activo o grupo de activos de infraestructura escaneados indicando al menos: Activo(s) de infraestructura o aplicativo relacionado, fecha de escaneo, direccionamiento IP, vulnerabilidades detectadas (Alta, Media, Baja), recomendaciones para remediación de hallazgos y que incluya los archivos electrónicos fuente de las herramientas tecnológicas utilizadas para el proceso de análisis	Evento	10 días hábiles posteriores a la solicitud generada por parte del Instituto
Servicios de Análisis Forense	Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de los hallazgos detectadas por cada activo o grupo de activos de infraestructura verificados	Evento	15 días hábiles posteriores a la solicitud generada por parte del Instituto



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
Servicios de Análisis de Vulnerabilidades Estático	Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las vulnerabilidades detectadas por cada pieza de software (codigo) analizados indicando al menos: aplicativo relacionado, fecha de análisis, código fuente analizado, vulnerabilidades detectadas (Alta, Media, Baja), recomendaciones para remediación de hallazgos y que incluya los archivos electrónicos fuente de las herramientas tecnológicas utilizadas para el proceso de análisis	Evento	10 días hábiles posteriores a la solicitud generada por parte del Instituto

7.3. Entregables Periódicos

El proveedor, de manera enunciativa más no limitativa, deberá generar entregables para los servicios de seguridad, que incluya al menos los siguientes conceptos:

Partida 1

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
----------	------------	--------------	---------



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
Servicios de Seguridad – Continuidad Operativa	Reportes Técnicos de los activos de infraestructura que contemplen: <ul style="list-style-type: none">• Disponibilidad• Controles de Cambios• Requerimientos• Incidentes/Fallas• Actividad Sospechosa• Estadísticas de uso de los servicios (conforme la definición en las mesas de trabajo)	Mensual	5 días hábiles posteriores al cumplimiento del mes vencido
Servicios de Seguridad – Verificación/Calidad	Reportes Técnicos de los activos de infraestructura que contemplen: <ul style="list-style-type: none">• Disponibilidad• Controles de Cambios• Requerimientos• Incidentes/Fallas• Actividad Sospechosa• Estadísticas de uso de los servicios (conforme la definición en las mesas de trabajo)	Mensual	5 días hábiles posteriores al cumplimiento del mes vencido
Servicios del Centro de Operaciones de Seguridad (SOC)	Reporte Técnico de los requerimientos generados a través de la Mesa de Servicios para los servicios de seguridad implementados	Mensual	5 días hábiles posteriores al cumplimiento del mes vencido
	Reporte Técnico de los controles de cambios generados para los servicios de seguridad implementados	Mensual	5 días hábiles posteriores al cumplimiento del mes vencido
	Reporte Técnico de los incidentes presentados en los servicios de seguridad implementados	Mensual	5 días hábiles posteriores al cumplimiento del mes vencido
	Reporte Técnico de los eventos de actividad sospechosa presentados en los servicios de seguridad implementados	Mensual	5 días hábiles posteriores al cumplimiento del mes vencido



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
	Reporte de las estadísticas de uso y desempeño, así como de la analítica de información de los servicios de seguridad implementados, conforme las definiciones realizadas en las mesas de trabajo	Mensual	5 días hábiles posteriores al cumplimiento del mes vencido
	Reporte de las evaluaciones operativas a los servicios de seguridad implementados	Trimestral	5 días hábiles posteriores al cumplimiento de cada trimestre calendario
	Reporte que integre el calendario de actualizaciones de versionamiento en software de cada servicio implementados	Trimestral	5 días hábiles posteriores al cumplimiento de cada trimestre calendario

Partida 2

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
Servicios de Análisis de Vulnerabilidades Dinámico	Reporte Técnico de los requerimientos generados a través de la Mesa de Servicios para los servicios de seguridad implementados	Mensual	5 días hábiles posteriores al cumplimiento del mes vencido
	Reporte Técnico de los controles de cambios generados para los servicios de seguridad implementados	Mensual	5 días hábiles posteriores al cumplimiento del mes vencido
	Reporte de las evaluaciones operativas a los servicios de seguridad implementados	Trimestral	5 días hábiles posteriores al cumplimiento de cada trimestre calendario
	Reporte que integre el calendario de actualizaciones de versionamiento en software de cada servicio implementados	Trimestral	5 días hábiles posteriores al cumplimiento de cada trimestre calendario



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Los entregables requeridos durante la vigencia del contrato, deberán ser entregados en formato electrónico (MS Word, MS Excel, PDF) conforme los periodos estipulados por el Instituto.

De igual manera, el proveedor deberá establecer un repositorio digital, que, de manera alterna, servirá para alojar los entregables antes señalados, mismos que estarán disponibles para su consulta durante la vigencia del contrato, teniendo en cuenta que el Instituto definirá en las mesas de trabajo los permisos de acceso correspondientes para el administrador del contrato, cuerpo de gobierno que se conforme para este propósito u otros funcionarios que sean designados por el primero mencionado.

8. Niveles de servicio que deberán cumplirse (SLA)

El objetivo de los Niveles de Servicio consiste en proporcionar al Instituto un mecanismo que permita:

- Medir de forma efectiva el desempeño de los servicios proporcionados por el proveedor.
- Procurar que los servicios de sean proporcionados con la calidad prevista.

Los Niveles de Servicio son métricas definidas por el "IMSS" que serán cumplidas por el proveedor de SASI 2022-2024, con objeto de cumplir con la calidad requerida en la prestación del servicio.

Con relación a lo establecido en los artículos 45, fracción XIX, 53 y 53 BIS de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, 86, segundo párrafo, 95, 96 y 97 de su Reglamento; se aplicarán las Penas Convencionales y Deducciones correspondientes, por atraso en el cumplimiento de las fechas pactadas de entrega o de la prestación del servicio y, con motivo del incumplimiento parcial o deficiente en que pudiera incurrir el "Proveedor" de SASI 2022-2024, respecto de los servicios prestados.

Los niveles de servicios se aplicarán conforme a lo estipulado en el documento de "Términos y Condiciones".

8.1. Penas Convencionales

Durante la vigencia del contrato, se aplicarán penas convencionales a todos aquellos servicios que no sean entregados conforme lo establecido en los niveles de servicios definidos por el instituto.

Las penas convencionales se aplicarán conforme a lo estipulado en el documento de "Términos y Condiciones".

9. Deducciones

Durante la vigencia del contrato, al presentarse una falla, incidente, atención de requerimientos, ventana de mantenimiento, entre otras, cuya causa raíz haya sido derivada por un tercero, la deductiva correspondiente al servicio asociado no será aplicada al proveedor de SASI 2022-2024, siempre y cuando demuestre con evidencias fehacientes que el servicio correspondiente se presentó bajo las especificaciones del anexo técnico y sus apéndices.

Con base en lo anterior, y cuando las fallas, incidentes, atención de requerimientos, ventanas de mantenimiento, entre otras, sean atribuibles a la entrega de los servicios de seguridad por parte del Proveedor se aplicara una deductiva conforme los niveles de servicios establecidos,



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Las deducciones se aplicarán conforme a lo estipulado en el documento de “Términos y Condiciones”.

10. Convenio de Confidencialidad y Resguardo de la Información

El “Licitante” deberá suscribir el Convenio de Confidencialidad y Resguardo de Información correspondiente. En complemento, el “Licitante” deberá considerar al menos los siguientes mecanismos de control de acceso a la información del IMSS:

- a. Se deberán establecer controles de acceso y privilegios restringidos al personal del “Licitante”, a fin de acotar su acceso para tareas y funciones específicas cuando requieran estar dentro de las instalaciones del IMSS.
- b. El “Licitante” deberá implantar y aceptar en todo momento el uso de controles que permitan establecer “Pistas de Auditoría” para los accesos/copias de datos, incluyendo bitácoras individuales de usuario.
- c. Los empleados del “Licitante” con acceso a la información sensible del IMSS, deberán firmar acuerdos de confidencialidad con este.
- d. El almacenamiento de datos y acceso, incluyendo acceso remoto, serán en los sitios específicos señalados por el instituto de los servicios de SASI 2022- 2024 observando los requisitos de seguridad y resguardo de la información.
- e. El “Licitante” deberá permitir el acceso a información relacionada con el servicio prestado al IMSS para la realización de auditorías.
- f. El “Licitante” no deberá hacer uso indebido de la documentación, información, ni activos de TIC a los que tengan acceso o que se generen con motivo de la prestación del servicio.

11. Normas

No aplica

12. Normatividad Aplicable

El Proveedor de servicios deberá sujetarse a las políticas internas vigentes del Instituto y a cualquier modificación o inclusión de nuevas políticas que se realicen durante la vigencia del contrato. Las políticas aplicables se le darán a conocer durante las mesas de trabajo, sin embargo, se deberán considerar las que se enlistan a continuación, de manera enunciativa más no limitativa:

- Marco normativo de aplicación general y obligatoria en la Administración Pública Federal.
- Artículo 8, segundo y tercer párrafo, fracción I de la Ley Orgánica de la Administración Pública Federal.
- Acuerdo por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la Información y comunicación, y la seguridad de la información en la Administración Pública Federal.
- Políticas de Seguridad con base en el Sistema de Gestión de Seguridad de la Información (SGSI) del Instituto.
- Certificados ISO/IEC27001:2013 e ISO/IEC20000-1:2018 vigentes a nombre del licitante



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

participante.

13. Cumplimiento de Políticas

El Proveedor de servicios deberá respetar las políticas de seguridad vigentes en el Instituto y bajo ninguna circunstancia permitirá que se infrinjan los lineamientos vigentes. Si alguno de los lineamientos de seguridad implantados en el Instituto llegase a cambiar durante la vigencia del contrato establecido con dicho proveedor, éste deberá asegurarse de modificar su infraestructura y procesos de tal forma que cumpla con los nuevos requerimientos.

Todos los equipos de cómputo personal propiedad del proveedor de servicios, que estén involucrados en la prestación de los servicios, deberán estar protegidos con sistemas de detección de intrusos, control de infecciones virales, detección y eliminación de programas tipo "back door" o "Troyanos". Esta regla aplica tanto para los equipos de cómputo móviles (laptops, handheld, smartphones, tablet PC, etc.) como para los equipos de escritorio (desktop, deskside, etc.) usados por los recursos designados para las diversas tareas de administración y gestión.

Si dichos equipos requieren de la instalación de sistemas operativos, aplicaciones, sistemas antivirus, sistemas de seguridad y demás herramientas que el proveedor considere necesario para la correcta operación de su personal, así como de la adquisición, instalación, mantenimiento y licenciamiento de estos, el costo será absorbido por el proveedor.

14. Finalización del Contrato

En el caso de terminación anticipada del contrato o a la finalización de la vigencia del mismo, el "Licitante" será responsable de iniciar el proceso de respaldo de la información, el proceso de baja, de realizar los movimientos de resguardo, traslado y empaquetado de todo el equipo ubicado en las instalaciones del IMSS que forma parte de los servicios y que no constituya parte de las modificaciones, adecuaciones y/o activos que hayan sido realizados como permanentes, o aquellos que de común acuerdo con el IMSS hayan sido sustituidos como parte del servicio.

Una vez terminada la vigencia del servicio, la infraestructura, los componentes habilitadores y los demás elementos utilizados por el proveedor para la prestación de los servicios se transferirán al IMSS para la continuidad operativa. Este acto se llevará a cabo mediante un acta de entrega recepción, en la que dichos componentes se transmitirán al IMSS, a título gratuito, libres de toda limitación de dominio, gravamen y responsabilidad de cualquier naturaleza, conforme a la normativa aplicable al Instituto.

El "Licitante" deberá entregar al IMSS, a más tardar 2 meses antes de la finalización del contrato, un plan de trabajo detallado para lograr una transición efectiva de los servicios de seguridad, en el que se incluyan todos aquellos elementos para efectuarlo. Dicho plan deberá permitir una completa y correcta transición de los servicios, incluyendo la conformación y actualización de la documentación necesaria del proyecto, así como las mesas de trabajo necesarias para dicha transición con el o los proveedores que den continuidad operativa al proyecto.

La documentación deberá incluir información que se generó durante la vigencia del contrato, documentación de los procesos internos de aprovisionamiento, configuración y tareas de operación, soporte y mantenimiento debidamente actualizadas, tomando en consideración los eventos de administración de cambios y configuración, incidentes y problemas, además de un inventario actualizado a la fecha de entrega de todos los componentes habilitadores e infraestructura auxiliar que el IMSS solicite



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

se mantengan para la transición de un nuevo contrato de servicios, para que pueda continuarse prestando el mantenimiento preventivo y correctivo a todos los componentes de la solución y diseñar el mecanismo para la renovación tecnológica del resto, procurando afectar de forma mínima la operación.

La fecha límite para la entrega de la documentación final actualizada que se mencionó anteriormente será de 2 meses antes de la finalización del contrato SASI 2022-2024. Asimismo, el “Licitante” deberá implementar un esquema de respaldo de la información en cada uno de los componentes que integran los servicios incluyendo los relacionados con los Centros de Datos del IMSS, el respaldo de la información deberá ser almacenada en cada punto táctico para ser entregada al cuerpo de gobierno del contrato para su resguardo. Una vez contando con la autorización del cuerpo de gobierno de SASI 2022-2024.

Asimismo, al término del contrato, garantizará los niveles de servicio durante el período de transferencia de servicios al nuevo proveedor.

Dicho período de transición estará sujeto al plan de trabajo que el “Licitante” haya presentado previamente, y que el IMSS hubiera aprobado. No obstante, durante dicho periodo, el “Licitante” deberá proporcionar la orientación tecnológica adecuada al personal del IMSS para garantizar la continuidad de los servicios requeridos, poniendo a disposición del IMSS o de un tercero la transferencia.

15. Modelo de Gobierno

El Modelo de Gobierno establece la forma como se trabajará en relación con este proyecto, los lineamientos operacionales para el proveedor y la manera como se medirá el grado de desempeño. El Modelo de Gobierno surge de la necesidad de diseñar una estructura operativa orientada a procesos para administrar los “Servicios Administrados de Seguridad Informática SASI 2022-2024”, el cual facilitará la relación entre todos los involucrados para su adecuada implantación y operación.

El Modelo de Gobierno comprende los principales aspectos a considerar para asegurar y controlar la operación del proyecto.

Dicho modelo establece la organización y los roles que participarán por parte del Instituto dentro del proyecto.

El Modelo de Gobierno establece esquemas operativos y procesos, con la finalidad de que cada una de las etapas del servicio, el administrador del contrato y los líderes del proyecto, con apoyo por parte del proveedor del servicio (SOC), garanticen los niveles de servicios establecidos para la operación.



La estructura organizacional que ejecutar para el proyecto de “Servicios Administrados de Seguridad



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Informática (SASI 2022-2024)", busca que los responsables trabajen de manera efectiva, definiendo roles y responsabilidades en cada nivel, para lo cual se muestra en la siguiente tabla de manera enunciativa mas no limitativa a los responsables y sus roles correspondientes.

NIVELES ORGANIZACIONALES	RESPONSABLES	DESCRIPCIÓN
Supervisión y Administración de los Servicios	• Administración de Contrato	Determinar los incumplimientos respecto a las penas convencionales y/o deductivas descritas en Anexo Técnico, Términos y Condiciones en el apartado "Acuerdos de Niveles de Servicio de SASIC" Elaborar el dictamen de servicios, el cual deberá contener los servicios prestados a mes vencido, así como la identificación de los incumplimientos de los mismos.
Líder de Proyecto Proveedor (SOC)	• Líder del proyecto del proveedor	Entregar al administrador del contrato la documentación relativa a los servicios bajo su responsabilidad ("Reporte de Servicios Consolidado" y "Reportes de Niveles de Servicios" correspondientes).
Líder de Proyecto Operación	• Líderes de los Servicios del proyecto SASIC	Mantener la operación de los servicios de acuerdo a los niveles de servicio establecidos en descritas en Anexo Técnico, Términos y Condiciones en el apartado "Acuerdos de Niveles de Servicio de SASIC".



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Apéndice "A"

Servicios Administrados de Seguridad Informática (SASI) 2022-2024

1. Objetivo del Documento

Elaborar el documento que contenga los requerimientos y las especificaciones técnicas y de calidad, así como el alcance de la adquisición, arrendamiento o servicio de TIC y SI que se pretenda contratar.

2. Servicio de Firewall

Especificaciones Técnicas:

- Cumplir con el desempeño y capacidades considerando al menos las siguientes especificaciones:

	Tipo 1	Tipo 2	Tipo 3	Tipo 4
Desempeño	5 Gbps	10 Gbps	20 Gbps	240 Gbps
Conexiones simultáneas por seg.	1,000,000	2,000,000	4,000,000	32,000,000
Conexiones nuevas por seg.	50,000	125,000	200,000	1,000,000
Paquetes por seg.	1,000,000	3,000,000	5,000,000	30,000,000
Interfaces 10GbE	8	8	12	12

Se requieren mínimo 2 y máximo 4 equipos tipo 4 para el centro de datos principal, ubicado en Morelia Michoacán (configuración en HA)

- El licitante deberá considerar en su propuesta económica que las características de conexiones simultáneas por segundo se refiere a conexiones concurrentes por segundo.
- Incluir un sistema operativo propietario del fabricante, que reciba actualizaciones y parches de software conforme sean publicadas.
- Basado en la tecnología conocida como "Stateful Inspection", el cual realiza un análisis granular de los estados de las comunicaciones y aplicaciones, para controlar el flujo del tráfico pasando a través del "gateway", y de esta manera abrir dinámicamente y de una forma segura, puertos y un gran rango de protocolos.
- Certificado por organismos de la industria como Common Criteria o ICSA Labs.
- Incluir la posibilidad de crear NATs dinámicos y estáticos, permitiendo trasladar direcciones IP y puertos origen y destino, en un mismo paquete.
- Permitir implementar reglas aplicadas a intervalos de tiempo específicos.
- Integrar listas de control de acceso basadas en dirección origen, dirección destino, protocolos, interfaces de red, puertos, URL destino, identidad, rangos de tiempo o periodo.
- Capacidad de agrupar objetos tales como direcciones IP, protocolos y puertos para la simplificación de configuración de políticas de seguridad.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- Capacidad de establecer límites máximos de conexiones TCP, UDP, conexiones incompletas, conexiones por cliente y conexiones con tiempo de espera agotado (timeout).
- Capacidad de implementar mecanismos de calidad de servicio tales como la asignación de ancho de banda a cada tipo de flujo, encolamiento prioritario y moldeado de tráfico (traffic shaping).
- Capacidad de inspeccionar tráfico FTP, HTTP, HTTPS, DNS, ICMP, RADIUS, SMTP y SNMP, H.323, SIP, RSTP, SNMP, entre otros.
- Capacidad para realizar bloqueos de tráfico basado en ubicación geográfica (geolocalización).
- Soportar alta disponibilidad en modo Activo/Activo y Activo/Pasivo.
- Capacidad de segmentar lógicamente el o los activos de infraestructura en dispositivos virtuales (firewalls virtuales); en el que cada instancia virtual es un dispositivo independiente con sus propias políticas de seguridad, interfaces y usuarios administrativos.
- Capacidad de crear hasta 100 instancias de dispositivos virtuales (firewalls virtuales) que deberán ser soportadas en cada uno de los diferentes tipos de firewalls.
- Deberá soportar Interfaces de Programación de Aplicaciones (APIs por sus siglas en inglés) para la integración con una plataforma de software libre y de código abierto, así como para la integración de una solución de cómputo en la nube (cloud computing).
- Capacidad para ser integrado con servicios de correlación de eventos de seguridad.
- Soportar y operar bajo protocolos de ruteo BGP y OSPF.
- Soportar y operar mediante rutas estáticas.
- Realizar inspección en capa 3 y 4.
- Soporte y operación con al menos 1,000 VLANs
- Integrar esquemas de autenticación que soporten servicios TACACS, RADIUS, LDAP y/o certificados digitales.
- Permitir almacenar una base de usuarios local que permita realizar autenticación, sin depender de un dispositivo externo.
- Contar y operar al menos con una interface Gigabit Ethernet dedicada para administración.
- Generación de bitácoras de eventos (logs) con múltiples niveles de criticidad.
- Incluir una consola centralizada de gestión con las siguientes características:
 - Configuración, de manera centralizada, de políticas en todos los firewalls de la infraestructura.
 - Identificación de qué reglas corresponden a fuentes, destinos y tipos de tráfico.
 - Ejecución de operaciones para grupos o bloques de dispositivos de frontera de seguridad.
 - Capacidad de ofrecer diferentes vistas durante el monitoreo de dispositivos, topologías o políticas.
 - Agrupación de parámetros de configuración para su posterior implementación.
- Durante una actualización de configuración, deberá ser capaz de regresar a la configuración anterior, si es necesario o requerido.
- Auditoria de todas las actividades realizadas por los usuarios con privilegios administrativos, monitoreo, respaldo, entre otros, de la solución, y que incluya al menos: inicio de sesión de usuarios, cambios realizados en los activos de infraestructura (altas, bajas o cambios de políticas, configuraciones, activos afectados, entre otros) y tareas administrativas de respaldo de configuración, mismo que deberá incluir fecha y hora de cada actividad realizada.

3. Servicio de Prevención de Intrusos (IPS)

Especificaciones Técnicas:



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- Cumplir con el desempeño y capacidades considerando al menos las siguientes funcionalidades operativas:

	Tipo 1	Tipo 2	Tipo 3
Desempeño	15 Gbps	20 Gbps	24 Gbps
Conexiones simultaneas / concurrentes por seg.	15,000,000	25,000,000	30,000,000
Conexiones nuevas por seg.	120,000	160,000	200,000
Interfaces 10GbE	4	8	8

Se requieren mínimo 2 y máximo 4 equipos tipo 3 para el centro de datos Principal ubicado en Morelia Michoacán (configuración en HA)

- Incluir un sistema operativo propietario del fabricante, que reciba actualizaciones y parches de software conforme sean publicadas.
- Latencia máxima de 0.5 milisegundos.
- Las interfaces de Inspección deberán operar en la capa 2 del modelo de OSI, por lo que las interfaces de inspección no requerirán de una dirección IP ni MAC.
- Capaz de soportar un despliegue en modo L3, permitiendo definir características de switching y routing sobre el tráfico inspeccionado.
- Capacidad de detección en línea sin bloquear tráfico (Modo transparente o supervisión). El sistema sólo alertará que eventos serían bloqueados.
- Capacidad de configuración del modo transparente o supervisión para todo el tráfico o sólo para los paquetes especificados por dirección IP, protocolo, VLAN ID, entre otros.
- Capacidad de crear reglas y filtros de acceso que soporte y opere por dispositivo, puerto, VLAN, IP o rango de IP.
- Soporte de funcionamiento pasivo como un IDS (sistema de detección de intrusos), con alertas de ataque, tráfico malicioso o no deseado, sin interferir con el tráfico.
- Soporte de la combinación de las modalidades IDS (pasivo) e IPS (en línea) dentro de un mismo equipo.
- La solución de IPS deberá contemplar que el flujo de información esté asegurado ante una falla en el IPS, pudiendo comutar el tráfico por hardware, es decir, sin necesidad de un dispositivo exterior que pudiera representar otro punto de falla en la red.
- Soporte de funcionalidades de alta disponibilidad y configuraciones del tipo activo/activo y activo/failover. Esto deberá ser soportado sin degradar el desempeño del IPS y manteniendo las tasas de transmisión requerida.
- Soporte de actualizaciones automáticas de seguridad del archivo de firmas de cuando menos una vez por mes.
- Soporte de análisis de tráfico de voz sobre IP.
- Soporte de monitoreo de VLANs, incluyendo tramas 802.1q
- Soporte de monitoreo de IPv6.
- Soporte de monitoreo con inspección profunda de paquete y monitoreo de paquete en escenarios de alta disponibilidad y con handshake TCP incompleto.
- Reconocimiento de Tunelado de Protocolos que permita la identificación de protocolos aun cuando estos estén encapsulados.
- Detección de escaneo de puertos.
- Detección de re-ensamblaje de paquetes fragmentados.
- Captura de tráfico para el análisis de evidencia en formato soportado por TCPDUMP y de manera opcional en formato. ENC (estándar para el software de análisis de protocolos), dicho archivo podrá



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- ser usado para hacer reconstrucción o análisis forense del ataque.
- Integración de Listas Blanca (IP whitelist) mediante una lista de direcciones IP “confiables” que el sistema no bloqueará.
 - Integración de firmas definidas por el Instituto mediante el uso de expresiones regulares.
 - Capacidad para realizar bloqueos de tráfico basado en ubicación geográfica (geolocalización).
 - Capacidad de crear perfiles de tráfico con reglas específicas para supervisar la transferencia de datos entre dos hosts de la red y crear una alarma cuando cierto umbral sea rebasado.
 - Capacidad de integración con el directorio de usuarios (Active Directory y/o LDAP).
 - Capacidad para ser integrado con servicios de correlación de eventos de seguridad.
 - Administración de seguridad centralizada que incluya las políticas, actualización, respuestas (bloquear, notificar, ignorar, etc.) y opciones de auditoría.
 - Consola centralizada que administre los IPS y la integración de usuarios que realice las configuraciones necesarias para remediación de incidentes de seguridad.
 - Consola remota con interfaz gráfica o Web cifrada (HTTPS) para el uso en modo de consulta, con diferentes perfiles de usuarios.
 - Auditoria de todas las actividades realizadas por los usuarios administrativos, monitoreo, respaldo, entre otros, de la solución, y que incluya al menos: inicio de sesión de usuarios, cambios realizados en los activos de infraestructura (altas, bajas o cambios de políticas, configuraciones, activos afectados, entre otros) y tareas administrativas de respaldo de configuración, mismo que deberá incluir fecha y hora de cada actividad realizada.
 - Deberá soportar Interfaces de Programación de Aplicaciones (APIs por sus siglas en inglés) para la integración con una plataforma de software libre y de código abierto, así como para la integración de una solución de cómputo en la nube (cloud computing).
 - Capacidad de segmentar lógicamente el o los activos de infraestructura en dispositivos virtuales (IPS virtuales); en el que cada instancia virtual es un dispositivo independiente con sus propias políticas de seguridad, interfaces y usuarios administrativos.
 - El licitante deberá considerar en su propuesta económica la capacidad de crear hasta 100 instancias de dispositivos virtuales (IPS virtuales) en todos los equipos ofertados.
 - Para los equipos en el centro de datos principal se requiere una consola de Administración.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

4. Servicios de Protección contra Denegación (DDoS)

	Tipo 1	Tipo 2
Desempeño	20 Gbps	120 Gbps
Conexiones simultaneas por seg.	25,000,000	120,000,000
Conexiones nuevas por seg.	160,000	600,000
Interfaces 10GbE	8	8

Se requieren mínimo 2 y máximo 4 equipos tipo 2 para el Centro de Datos Principal ubicado en Morelia Michoacán (configuración en HA)

Especificaciones Técnicas:

Cumplir con el desempeño y capacidades considerando al menos las siguientes funcionalidades operativas:

- Incluir un sistema operativo propietario del fabricante, que reciba actualizaciones y parches de software conforme sean publicadas.
- El licitante deberá considerar en su propuesta que la cantidad de tráfico máximo a inspeccionar por los equipos y un ancho de banda de los enlaces de internet que estarán recibiendo los equipos, de 1 Gbps para ambos casos.
- Deberá garantizar el paso transaccional de datos legítimos, privilegiando la eliminación de tráfico anómalo dentro de los canales de comunicación del Instituto (Clean Pipes).
- Detección del tráfico basado en el lenguaje TCPDUMP (con información definida en las capas 3 y 4)
- Deberá tener la capacidad de advertir anticipadamente algún posible ataque, analizando tendencias de tráfico malicioso en tiempo real.
- Deberá de tener capacidad de monitoreo en tiempo real de los circuitos dedicados que entregan la conectividad a Internet/Intranet para detectar el comportamiento anormal del tráfico que pueda estar dirigido a atacar las interfaces de los enrutadores implicados en los enlaces.
- Deberá de tener la capacidad de monitoreo en tiempo real las subredes pública que conectan los enlaces, para que permita la detección de tráfico anormal que pueda significar un ataque dirigido a ella.
- Detección de ataques basado en la línea de base contra los recursos definidos, con opciones configurables por recursos que permitan filtrar la sensibilidad de la anomalía y disparar un evento de tipo alerta, en paquetes por segundo y bytes por segundo.
- Soportar alta disponibilidad en modo Activo/Activo y Activo/Pasivo.
- Capacidad de agrupar objetos tales como direcciones IP, protocolos y puertos para la simplificación de configuración de políticas de seguridad.
- Capacidad de establecer límites máximos de conexiones TCP, UDP, conexiones incompletas, conexiones por cliente y conexiones con tiempo de espera agotado (timeout).
- Deberá monitorear, de manera enunciativa más no limitativa, las siguientes variables en tiempo real:
 - Para el protocolo IP:
 - ICMP
 - Paquetes IP fragmentados
 - Paquetes IP NULL
 - Paquetes IP con direcciones privadas



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- Para el protocolo TCP:
 - Segmentos TCP NULL
 - Segmentos TCP RST
 - Segmentos SYN
 - Tráfico total
- Deberá como mínimo detectar los siguientes tipos de ataques DoS/DDoS sobre las interfaces, subredes y activos de infraestructura:
 - ACK Flood
 - SYN Flood
 - Hogging CPU
 - Chargen (Character generator)
 - FIN Flood
 - ToS Flood
 - DNS Malformed
 - HTTP Flood
 - ICMP Flood
 - UDP Flood
 - Non- UDP/TCP/ICMP Protocol Flood
 - PPS Flood Attack
 - Zombie attack
 - Land Attack
- Deberá de permitir la personalización de los niveles de alarma o umbrales que sirvan para la detección de ataques, a una granularidad por objeto monitoreado.
- Deberá monitorear actividad sospechosa que pueda significar algún ataque de gusanos, virus, entre otros.
- Deberá monitorear actividad “Dark IP”.
- Detección de anomalías DDoS y amenazas de día cero antes de que impacten en los servicios.
- Detección de zombis (con selecciones de umbrales en bytes por segundos y paquetes por segundos) para clasificar una IP como zombis y con la opción de conocer una lista de zombis activos detectados.
- Protección contra amenazas conocidas
 - Ping de la muerte
 - Ataque por inundación SYN
 - Fragmentacion de paquetes y reensamblaje
 - Broadcast de correo electrónico
 - Saturadores de CPU
 - Scripts generadores de trafico
 - Generadores de caracteres
 - Ataques fuera de banda (WinNuke)
 - Ataque Smurf (generador de gran cantidad de paquetes ICMP)
- Auditoria de todas las actividades realizadas por los usuarios administrativos, monitoreo, respaldo, entre otros, de la solución, y que incluya al menos: inicio de sesión de usuarios, cambios realizados en los activos de infraestructura (altas, bajas o cambios de políticas, configuraciones, activos afectados, entre otros) y tareas administrativas de respaldo de configuración, mismo que deberá incluir fecha y hora de cada actividad realizada.
- Capacidad para realizar bloqueos de tráfico basado en ubicación geográfica (geolocalización).



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

5. Redes Privadas Virtuales – VPN (C2S – S2S)

Se requieren mínimo 1 y máximo 2 equipos para el centro de datos principal ubicado en Morelia Michoacán (configuración en HA)

Especificaciones Técnicas:

Cumplir con el desempeño y capacidades considerando al menos las siguientes funcionalidades operativas:

- Incluir un sistema operativo propietario del fabricante, que reciba actualizaciones y parches de software conforme sean publicadas.
- Deberá incluir al menos 4 interfaces 10/100/1000 Gb, expandibles a interfaces 10Gb de ser necesario.
- Deberá tener un desempeño de al menos 2Gbps y 1,000,000 conexiones concurrentes
- Capacidad de permitir 50,000 nuevas conexiones por segundo.
- Deberá incluir la posibilidad de crear NATs dinámicos y estáticos, permitiendo trasladar direcciones IP y puertos origen y destino, en un mismo paquete.
- Deberá permitir implementar reglas aplicadas a intervalos de tiempo específicos.
- Deberá soportar alta disponibilidad en modo Activo/Activo y Activo/Pasivo.
- Deberá integrar esquemas de autenticación que soporten servicios TACACS, RADIUS, LDAP y/o certificados digitales.
- Deberá permitir la creación de grupos de usuarios.
- Deberá permitir delimitar la cantidad de conexiones por usuarios.
- Deberá permitir almacenar una base de usuarios local que permita realizar autenticación, sin depender de un servicio de autenticación externo.
- Capacidad de crear hasta 5,000 túneles de VPN IPsec (sitio a sitio y cliente remoto)
- Deberá soportar DES, 3DES y AES-256 para las fases I y II de IKEv1 e IKEv2.
- Deberá soportar al menos los siguientes grupos Diffie-Hellman: Grupo 1 (768 bit), Grupo 2 (1024 bit), Grupo 5 (1536 bit), Grupo 14 (2048 bit).
- Deberá soportar integridad de datos con md5, sha1 y sha2.
- Deberá soportar las topologías VPNs site-to-site: Meshed (todos a todos) y Star (Oficinas Remotas a Sitio Central).
- Deberá establecer VPNs con gateways con direcciones IP dinámicas públicas.
- Deberá crear una única asociación de seguridad (SA) por par de redes o subredes.
- Deberá realizar VPNs SSL.
- Deberá soportar la conexión desde dispositivos móviles y de escritorio a través de un cliente de acceso remoto. Dicho cliente debe soportar al menos las siguientes plataformas operativas: MAC OS X desde v10.4.10, iOS desde v4, Android desde v4.2, Windows desde v7.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

6. Filtrado de Contenido Web

Cumplir con el desempeño y capacidades considerando al menos las siguientes funcionalidades operativas:

- Incluir un sistema operativo propietario del fabricante, que reciba actualizaciones y parches de software conforme sean publicadas.
- Soportar de forma mínima 120,000 usuarios de forma simultánea.
- Integrar esquema de alta disponibilidad (Activo/Activo o Activo/Pasivo).
- Permitir operar en modo de proxy explícito y/o proxy transparente.
- Mecanismos de autenticación tales como: archivos locales de contraseña NTLM, LDAP, RADIUS, Active Directory y certificados.
- Control de autenticaciones simultáneas con una misma cuenta de usuario.
- Cifrado de datos (usuario/contraseña) en el proceso de autenticación.
- Controlar e inspeccionar al menos los protocolos: HTTP, HTTPS (SSL), FTP, CIFS, MAPI, DNS, P2P, SOCKS (v4/v5), IM (AOL, MSN, Yahoo Messengers), TCP-Tunnel, MMS, RTSP.
- Catalogar las páginas por dominio (o subdominio), URL o IP.
- Bloqueo de las amenazas emergentes más comunes como: pop-ups, banners, spyware, adware, compartición de archivos punto a punto (P2P file sharing).
- Clasificación en tiempo real de sitios en internet (on-the-fly) que aún no han sido asignados a alguna categoría (servicio automático de validación en línea del sitio para determinar si es malicioso en caso de no tenerlo asignado en alguna categoría).
- Monitoreo y bloqueo de aplicaciones P2P tales como: BitTorrent, eDonkey, Gnutella, Fasttrack.
- Permitir personalización detallada de políticas de control de acceso a través de parámetros como: direcciones IP, grupos de subredes, protocolos, URLs, grupos y usuarios de directorio activo, entre otros.
- Permitir la clasificación de URL (dominio o subdominio) o IP en una sola categoría.
- Permitir el uso de expresiones regulares.
- Permitir la creación de categorías de filtrado personalizadas, así como la creación de listas blancas y negras de filtrado URL.
- Capacidad de evitar la ejecución de códigos maliciosos.
- Bloqueo y filtrado de HTTP, en tipos de archivos específicos, tales como .mp3, .exe, .zip, entre otros.
- Actualización de la base de datos para el filtrado de contenido en tiempo real y de manera automática (de forma diaria).
- Permitir la recopilación (caching) de páginas web en disco duro y memoria RAM, con el fin de hacer más eficiente el uso de los recursos del equipo.
- Proporcionar capacidades de administración y reporteo centralizado incluyendo control de acceso discrecional, control de versiones, auditoria de usuario, sistema y utilerías de restauración de configuración.
- Deberá proporcionar soporte de administración multisesión (múltiples administradores utilizando el servicio de administración centralizado), a través de una interfaz gráfica vía Web cifrada (HTTPS).
- Auditoria de todas las actividades realizadas por los usuarios administrativos, monitoreo, respaldo, entre otros, de la solución, y que incluya al menos: inicio de sesión de usuarios, cambios realizados en los activos de infraestructura (altas, bajas o cambios de políticas, configuraciones, activos afectados, entre otros) y tareas administrativas de respaldo de configuración, mismo que deberá incluir fecha y



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

hora de cada actividad realizada.

7. Servicios de Filtrado de Contenido de Correo (Antispam)

Cumplir con el desempeño y capacidades considerando al menos las siguientes funcionalidades operativas:

- Incluir un sistema operativo propietario del fabricante, que reciba actualizaciones y parches de software conforme sean publicadas.
- Capacidad de hasta 1.5M de correos por hora
- Con una capacidad de por lo menos 120,000 usuarios
- 12 TB por equipo, en HA por lo menos 24 TB.
- Integrar esquema de alta disponibilidad (Activo/Activo o Activo/Pasivo).
- Capacidad de revisar tanto el correo entrante como el saliente.
- Deberá escanear y analizar el asunto, encabezados y el cuerpo de los correos recibidos y enviados.
- Contar con un filtro de contenido para buscar palabras clave en el cuerpo del mensaje, en los encabezados From, To, CC, Subject y en X-Headers. Así mismo, deberá poder detectar estas palabras en archivos adjuntos.
- Capacidad para poder configurar el tamaño máximo del mensaje y el número de destinatarios del correo tanto a nivel de conexión SMTP, como en políticas cuando el correo ya ha sido recibido.
- Contar con mecanismos para clasificar los remitentes por su origen y tomar decisiones de flujo y volumen en consecuencia. Además, se debe contar con la facilidad de designar ciertas fuentes de correo en grupos como listas negras, listas blancas o cualquier otro grupo al que deba aplicársele una política específica.
- Capacidad para ofrecer el análisis de archivos comprimidos en los formatos más populares, incluyendo aquellos con 7 capas de compresión.
- Capacidad de detectar el verdadero formato de un archivo y permitir aplicar políticas basadas en este rubro.
- Capacidad para detectar enlaces maliciosos dentro de los correos recibidos en base a la reputación de la URL, utilizando la tecnología de reputación del fabricante, permitiendo la configuración de umbrales para esta detección.
- Contar con un módulo de bloqueo de correo electrónico no deseado con base en la reputación de cuentas de correo, dominios y direcciones IP.
- Capacidad para soportar la revisión de firmas DKIM en los encabezados de correos entrantes.
- Contar con actualizaciones para sus patrones y motores de detección de spam (heurística), phising y código malicioso.
- Capacidades de colaboración con los centros de investigación de amenazas del fabricante, con la finalidad de reportar de manera automática cualquier comportamiento sospechoso relacionado con el tráfico de correo electrónico.
- Capaz de recibir tráfico con conexiones seguras (TLS) y poder hacer conexiones con otros servidores bajo el mismo protocolo.
- Contar con mecanismos que permitan evitar la recepción de correos de notificaciones dirigidas a cuentas de usuarios no válidos o que no existen en el dominio destino (correos de rebote o Bounced Mails).
- Bloqueo automático de IP debido a alta cantidad de envío de spam, ataque tipo DHA (Directory Harvest Attack), Bounced Mails o código malicioso, totalmente parametrizable al número de mensajes



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- recibidos en un intervalo de tiempo determinado a discreción.
- Capacidad para Integrar excepciones, tanto en hosts remitentes como en destinatarios, así como para cuentas de usuarios o dominios específicos.
 - Permitir la creación de cuarentenas o carpetas de auditoría de correo, la cuarentena debe poder ser almacenada por la solución como mínimo 30 días.
 - Cuando se encuentre contenido malicioso en cuerpo del correo y archivos adjuntos, podrá realizar cualquiera de las siguientes acciones:
 - Reemplazar texto del mensaje afectado.
 - Poner en cuarentena el mensaje completo.
 - Eliminar el mensaje completo.
 - Hacer copia de seguridad (copia del mensaje), para reportarlo con los centros de investigación de amenazas del fabricante.
 - Detectar correos masivos con virus y removerlos además de los archivos adjuntos, incluyendo la característica de archivos adjuntos Zero-byte.
 - Proporcionar la facilidad de enviar notificaciones a los usuarios (cuentas de correo electrónico) cuando algún evento sospechoso sea detectado.
 - Capacidad de integrar agentes que realicen la función de escaneo y detección de spam en activos de infraestructura o servicios de correo electrónico bajo plataformas operativas Linux y/o Windows.
 - Auditoria de todas las actividades realizadas por los usuarios administrativos, monitoreo, respaldo, entre otros, de la solución, y que incluya al menos: inicio de sesión de usuarios, cambios realizados en los activos de infraestructura (altas, bajas o cambios de políticas, configuraciones, activos afectados, entre otros) y tareas administrativas de respaldo de configuración, mismo que deberá incluir fecha y hora de cada actividad realizada. Capacidad para realizar bloqueos de tráfico basado en ubicación geográfica (geolocalización).



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

8. Firewall Especializado en Servicios Web (WAF)

Se requieren mínimo 1 y máximo 2 equipos para el centro de datos principal ubicado en Morelia Michoacán (configuración en HA)

Especificaciones Técnicas:

Cumplir con el desempeño y capacidades considerando al menos las siguientes funcionalidades operativas:

- Incluir un sistema operativo propietario del fabricante, que reciba actualizaciones y parches de software conforme sean publicadas.
- Integrar esquema de alta disponibilidad (Activo/Activo o Activo/Pasivo).
- Inspección y análisis de perfiles de comportamiento normal de usuarios para detectar y mitigar el uso anormal de aplicativos Web.
- Soportar un throughput de 5 Gbps en capa 7.
- Soportar 100,000 Transacciones por Segundo (TPS).
- El licitante ganador debe considerar en su propuesta en términos de transacciones por segundo de tráfico HTTPS requiriendo PFS/DH (Perfect Forward Secrecy/ Diffie-Hellman) al menos 60,000 tps
- Servicio de reputación para identificar y bloquear ataques automatizados y/o usuarios maliciosos.
- Detección de ataques por clientes automatizados y robots.
- Detección de URL rewriting u ofuscación del URL.
- Manejo de errores y reescritura de errores para aplicativos Web.
- Capacidad para soportar inspección del protocolo XML.
- Certificado por organismos de la industria como ICSA Labs o PCI.
- Actualización automática de firmas de prevención contra código malicioso.
- parcheo sobre aplicativos Web contra vulnerabilidades nuevas o conocidas (parcheo virtual).
- Protección contra ataques/vulnerabilidades conocidas (OWASP), de manera enunciativa más no limitativa:
 - SQL injection
 - Cross Site Scripting
 - Cross Site Request Forgery
 - Sensitive Data Exposure
 - Security Misconfiguration
 - Broken Authentication and Session Management
 - Otras nuevas identificadas por OWASP
- Soportar formatos de mensaje:
 - Web 2.0
 - HTML
 - XHTML
 - HTML5
 - XML
 - JSON
 - AJAX
 - FLASH



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- JavaScript.
- Soportar Protocolos: TCP v4 y v6, HTTP, HTTPS, SSL/TLS.
- Soportar mitigación de amenazas:
 - HTML Content Aware
 - Intrusion Detection and Prevention (URI patterns)
 - URI rate-based heuristics
 - Vendor Vulnerabilities
 - URL cloaking / rewrite
 - Parameter Inspection
 - Learning mode
- Integridad de transacciones:
 - Session Tracking Cookies, Source/Destination IPs
 - HTTP RFC conformance
 - HTML Form parameter checking
 - Cross-Site Scripting
 - Cookie Signing
- Auditoria de todas las actividades realizadas por los usuarios administrativos, monitoreo, respaldo, entre otros, de la solución, y que incluya al menos: inicio de sesión de usuarios, cambios realizados en los activos de infraestructura (altas, bajas o cambios de políticas, configuraciones, activos afectados, entre otros) y tareas administrativas de respaldo de configuración, mismo que deberá incluir fecha y hora de cada actividad realizada.
- Capacidad para realizar bloqueos de tráfico basado en ubicación geográfica (geolocalización).
- Debe soportar Interfaces de Programación de Aplicaciones (APIs por sus siglas en inglés) para la integración con una plataforma de software libre y de código abierto, así como para la integración de una solución de cómputo en la nube (cloud computing).
- El licitante deberá considerar en su propuesta al menos 200 sitios/portales a proteger.

9. Servicios de Gestión Unificada de Amenazas (UTM)

Especificaciones Técnicas:

Cumplir con el desempeño y capacidades considerando al menos las siguientes funcionalidades operativas:

	Tipo 1	Tipo 2	Tipo 3	Tipo 4
Desempeño	1 Gbps	2 Gbps	5 Gbps	10 Gbps
Conexiones simultáneas por seg.	10,000	20,000	50,000	100,000
Conexiones nuevas por seg.	150,000	500,000	1,000,000	2,000,000
Interfaces 10/100/1000 Mbps.	4	4	8	8

Se requieren mínimo 1 y máximo 2 equipos para el centro de datos principal ubicado en Morelia Michoacán (configuración en HA)

El licitante deberá considerar en su propuesta que funcionalidad de alta disponibilidad modo Activo/activo y/o Activo/Pasivo.

El licitante deberá considerar en su propuesta que la característica de conexiones simultáneas por



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

segundo" y "conexiones nuevas por segundo, se refiera a conexiones concurrentes por segundo, así así como considerar que la suma de las sesiones concurrentes refiere a el servicio UTM por cada tipo y las sesiones concurrentes de la tabla de UTM.

Generales

- Deberá incluir un sistema operativo endurecido propietario del fabricante, que reciba actualizaciones y parches de software conforme sean publicadas.
- Soportar alta disponibilidad en modo Activo/Activo y Activo/Pasivo.

Funcionalidad Firewall

- Deberá estar basado en la tecnología conocida como "Stateful Inspection", el cual realiza un análisis granular de los estados de las comunicaciones y aplicaciones, para controlar el flujo del tráfico pasando a través del "gateway", y de esta manera abrir dinámicamente y de una forma segura, puertos y un gran rango de protocolos.
- Deberá incluir la posibilidad de crear NATs dinámicos y estáticos, permitiendo trasladar direcciones IP y puertos origen y destino, en un mismo paquete.
- Deberá permitir implementar reglas aplicadas a intervalos de tiempo específicos.
- Deberá soportar y operar bajo protocolos de ruteo BGP y OSPF.
- Deberá soporte y operar mediante rutas estáticas.
- Deberá realizar inspección en capa 3 y 4.

Funcionalidad IPS e IDS

- Soporte de al menos: 1,000,000 conexiones simultáneas por cada Gigabit de inspección.
- Latencia máxima de 0.5 milisegundos.
- Las interfaces de Inspección deberán operar en la capa 2 del modelo de OSI, por lo que las interfaces de inspección no requerirán de una dirección IP ni MAC.
- El equipo deberá ser capaz de soportar un despliegue en modo L3, permitiendo definir características de switching y routing sobre el tráfico inspeccionado
- Capacidad de detección en línea sin bloquear tráfico (Modo transparente). El sistema sólo alertará que eventos serían bloqueados.
- Capacidad de crear reglas y filtros de acceso que soporte y opere por dispositivo, puerto, VLAN, IP o rango de IP.
- Soporte de funcionamiento pasivo como un IDS (sistema de detección de intrusos), con alertas de ataque, tráfico malicioso o no deseado, sin interferir con el tráfico.
- Soporte de la combinación de las modalidades IDS (pasivo) e IPS (en línea) dentro de un mismo equipo.
- La solución de IPS deberá contemplar que el flujo de información esté asegurado ante una falla en el IPS, pudiendo comutar el tráfico por hardware, es decir, sin necesidad de un dispositivo exterior que pudiera representar otro punto de falla en la red.
- Reconocimiento de tunelado de protocolos que permita la identificación de protocolos aun cuando estos estén encapsulados.
- Detección de re-ensamblaje de paquetes fragmentados.
- Integración de listas blanca (IP whitelist) mediante una lista de direcciones IP "confiables" que el sistema no bloqueará.
- Capacidad de crear perfiles de tráfico con reglas específicas para supervisar la transferencia de datos entre dos hosts de la red y crear una alarma cuando cierto umbral sea rebasado.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Filtrado de Contenido Web

- Deberá permitir operar en modo de proxy explícito y/o proxy transparente.
- Controlar e inspeccionar al menos los protocolos: HTTP, HTTPS (SSL).
- Catalogar las páginas por Dominio (o subdominio), URL o IP.
- Permitir personalización detallada de políticas de control de acceso a través de parámetros como: direcciones IP, grupos de subredes, protocolos, URLs, grupos y usuarios de directorio activo, entre otros.
- Permitir la creación de categorías de filtrado personalizadas, así como la creación de listas blancas y negras de filtrado URL.
- Capacidad de evitar la ejecución de códigos maliciosos.
- Permitir el bloqueo y filtrado de HTTP, en tipos de archivos específicos, tales como .mp3, .exe, .zip, entre otros.
- Actualización de la base de datos para el filtrado de contenido en tiempo real y de manera automática (de forma diaria).

Funcionalidad VPN

- Deberá incluir la posibilidad de crear NATs dinámicos y estáticos, permitiendo trasladar direcciones IP y puertos origen y destino, en un mismo paquete.
- Deberá permitir almacenar una base de usuarios local que permita realizar autenticación, sin depender de un dispositivo externo.
- Capacidad de crear hasta 5,000 túneles de VPN IPSec (sitio a sitio y cliente remoto)
- Deberá soportar DES, 3DES y AES-256 para las fases I y II de IKEv1 e IKE v2.
- Deberá soportar al menos los siguientes grupos Diffie-Hellman: Grupo 1 (768 bit), Grupo 2 (1024 bit), Grupo 5 (1536 bit), Grupo 14 (2048 bit).
- Deberá soportar integridad de datos con md5, sha1 y sha2.
- Deberá soportar las topologías VPNs site-to-site: Meshed (todos a todos) y Star (Oficinas Remotas a Sitio Central).
- Deberá establecer VPNs con gateways con direcciones IP dinámicas públicas.
- Deberá crear una única asociación de seguridad (SA) por par de redes o subredes.
- Deberá soportar Secure Sockets Layer (SSL) versión 3, con al menos los siguientes algoritmos de cifrado simétrico y longitud de llaves: RC4 (128 bits) y 3DES (192bits).



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

10. Firewall Especializado en Base de Datos (DBF)

Se requieren mínimo 1 y máximo 2 equipos para el centro de datos principal ubicado en Morelia Michoacán (configuraciones en HA)

Especificaciones Técnicas:

- Tecnología de autoaprendizaje con mínima intervención humana, el proceso deberá ser constante y deberá aprender estructura de bases de datos, incluyendo schemas, objetos, tablas; sistemas, aplicaciones, campos, directorios, así como el comportamiento de cada usuario.
- Deberá operar a nivel local y en la capa de red
- Deberá soportar al menos los siguientes motores de Bases de Datos:
 - Microsoft SQL Server
 - Oracle
 - Sybase
 - Informix
 - MySQL
 - Progress
 - PostgreSQL
- Proporcionar protección por medio de bloqueos y alertas contra violaciones de seguridad por ataques conocidos, actividad sospechosa o cualquier actividad específica a definir.
- En caso de ser necesario la utilización de agentes, estos deberán soportar al menos los siguientes Sistemas Operativos:
 - AIX
 - HP-UX
 - Solaris
 - RHEL
 - SuSE
 - OEL
 - Windows 32/64 bits
- Capacidad para funcionar independiente a la activación de la auditoría nativa de la base de datos.
- Transparente para la base de datos y/o las aplicaciones que accedan a ella, es decir, no requerirá que se realicen cambios en la programación, configuración u operación (triggers, stored procedures, etc.) de ninguna de ellas.
- Se requiere un repositorio para el registro de la actividad, el cual no deberá ser accesible por ningún otro mecanismo que no sea la interacción mediante la GUI (interfaz gráfica) proporcionada por el fabricante o por medios administrativos debidamente asegurados.
- Capaz de descubrir servidores de bases de datos y realizar análisis de vulnerabilidades sobre el software de manejo de la base de datos, el protocolo de comunicación, y configuración de seguridad, sin importar el sistema operativo sobre el que se encuentren instaladas.
- Capacidad para poder realizar descubrimientos automatizados en la red para identificar nuevas bases de datos siendo habilitadas, ya sea a nivel de servidor o puertos habilitados en servidores conocidos.
- Capacidad de analizar y clasificar los tipos de dato dentro de las Bases de Datos de acuerdo a las políticas de negocio. Las definiciones de tipo de dato deberán poder crearse de manera flexible y granular.
- Capacidad para proveer un servicio de protección del software de base de datos mediante la aplicación de parches virtuales que impidan atacar las vulnerabilidades encontradas en dicho software, independientemente de la liberación de la corrección o actualización del fabricante.
- Deberá apoyar en los esfuerzos de análisis de vulnerabilidades, configuración de seguridad,



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- comportamiento/performance de aplicativos y Control de cambios.
- Deberá monitorear toda la actividad de las bases de datos, y deberá almacenar los comandos SQL tal cual fueron escritos por el usuario o aplicación, incluyendo comandos DDL, DML y DCL.
 - Deberá monitorear e interactuar con la actividad de la base de datos sin importar el punto de entrada, ya sean conexiones directas, servidores de aplicaciones, acceso directo a la base de datos, ligas, stored procedures, entre otros.
 - Deberá hacer análisis y auditoría sobre todo el tráfico en tiempo real, sin importar el volumen de tráfico, sin necesidad de crear un archivo log primero para su análisis posterior.
 - Capacidad de monitorear el tráfico encriptado hacia las Bases de Datos.
 - Capacidad para proveer detalles sobre alertas ya sean falsos positivos o negativos y deberá tener la facilidad de cambiar una política desde la alerta.
 - Deberá manejar reglas y políticas tan amplias o granulares como se requieran y deberán poder ser construidas automáticamente o manualmente y deberán poder ser actualizadas, igualmente, de forma manual o automática.
 - Las políticas granulares para control de acceso o generación de alertas deberán de contar con los siguientes criterios para la validación de la actividad en la aplicación de Base de Datos. Los criterios deberán de poder usarse en cualquier número y cualquier combinación:
 - Número de registros a regresar por la consulta (SQL Query)
 - Número de registros afectados
 - Tipo de datos accesado (financiero, recursos humanos, inventarios, o cualquier definición personalizada)
 - Acceso a datos marcados como sensibles
 - Base de Datos, Schema, Instancia, Tabla y Columna accesada
 - Estado de autenticación de la sesión
 - Usuario y/o Grupo de Usuarios de Base de Datos conectado
 - Usuario conectado en la capa aplicativa, a diferencia del usuario conectado a la DB
 - Por búsqueda en diccionarios de datos (tarjetas de crédito, datos privados, o cualquier customización por expresiones regulares)
 - Logins, Logouts, Queries
 - IPs de origen y destino
 - Nombre de Host origen, Usuario firmado en el Host origen
 - Aplicación usada para la conexión a la base de datos
 - Tiempo de respuesta/procesamiento del query
 - Errores en el manejador de SQL
 - Número de ocurrencias en intervalos de tiempo definidos
 - Por operaciones básicas (Select, Insert, Update, Delete)
 - Por operaciones privilegiadas (Create, Alter, Drop, Grant, Revoke, Truncate, Export)
 - Por Stored Procedure o Function utilizada
 - Si existe ticket asignado de cambios
 - Hora del Día
 - Deberá posibilitar los análisis en tiempo real e histórico bajo demanda, es decir, sin necesidad de pasar por un proceso batch previo.
 - Deberá proteger contra ataques SQL y no-SQL.
 - Contar con un mecanismo de actualización de la inteligencia interna de seguridad, que incluye las pruebas de las evaluaciones de vulnerabilidad, las firmas contra ataques, la granularidad de las políticas de seguridad y defensas contra comportamientos conocidos.
 - Considerar de emergencia, para potenciales violaciones de la información que incluyan, enunciativa más no limitativamente:
 - Altos volúmenes de acceso a datos sensibles más allá de lo habitual.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- Acceso a datos inusual para cierta hora del día.
- Acceso a datos desde una ubicación (física) desconocida.
- Acceso a datos utilizando aplicaciones/herramientas no autorizadas.
- Debe manejar una auditoría sobre sí misma, manteniendo un control de cambios sobre las políticas autorizadas y configuraciones realizadas.
- Debe tener facilidades de Archivado de la información histórica y de auditoría, con flexibilidad de opciones de protocolo o medio (como SAN o por medio de FTP, HTTP, NFS, SCP)
- Deberá tener la capacidad de exportar datos y eventos, tales como alertas, eventos de sistema y base de datos, información de seguridad/administración, entre otras, hacia otras herramientas de administración por medio de protocolos SNMP y Syslog.
- Deberá contar con un servicio de investigación sobre vulnerabilidades y amenazas informáticas, para lo cual deberá presentar la documentación respectiva en el descubrimiento de las mismas.
- Deberá soportar y aplicar simultáneamente un modelo de seguridad positivo y negativo.
- El modelo negativo de seguridad define explícitamente las firmas de ataques conocidos, por lo que deberá además cumplir con las siguientes especificaciones:
 - Deberá bloquear las transacciones que tengan contenido que coincida con firmas de ataque conocidos.
 - Deberá incluir una lista pre-configurada y detallada de las firmas de ataque.
 - Deberá permitir la modificación o adición de firmas por el administrador.
 - Deberá permitir la actualización automática de la base de datos de firmas, asegurando una completa protección contra las amenazas de aplicación más recientes.
 - Deberá detectar ataques conocidos a nivel base de datos
- Capacidad para realizar bloqueos de tráfico basado en ubicación geográfica (geolocalización).
- Debe soportar Interfaces de Programación de Aplicaciones (APIs por sus siglas en inglés) para la integración con una plataforma de software libre y de código abierto, así como para la integración de una solución de cómputo en la nube (cloud computing).

11. Servicio de Correlación de Eventos

Se requieren mínimo 2 y máximo 4 equipos para el centro de datos principal ubicado en Morelia Michoacán (configuraciones en HA)

Especificaciones Técnicas:

- Capacidad para recolectar datos de toda aplicación o dispositivo que tenga una fuente de eventos necesaria para la organización, siendo esto a través de desarrollos predefinidos del fabricante, o con desarrollos personalizados ejecutados por el proveedor del servicio.
- Capacidad para almacenar la información tal y como fue recibida del dispositivo o aplicaciones (eventos en crudo), para efectos de auditoría y análisis forense. La solución deberá generar una firma o "checksum" de los eventos recibidos para garantizar la integridad y mantener la cadena de custodia.
- Permitir la detección automática de fuentes de eventos recolectados a través del protocolo syslog, el cual puede ser enviado vía UDP, TCP o SSL/TLS.
- Capacidad de permitir filtrar eventos por cualquier campo del registro, que son los atributos donde se almacena la información recolectada por la herramienta de las fuentes de eventos.
- Contar con lógica de taxonomía a nivel de la recolección de los eventos, y que permita definir y modificar la misma con base en los eventos auditados.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- Capacidad para detectar automáticamente la desconexión de un conector de integración a través del envío de señales de comunicación para el aseguramiento de la continuidad operativa (“Keep Alive”).
- Capacidad para integrarse con los sistemas de detección y prevención de intrusos y los de administración de vulnerabilidades (VM)
- Contar con la capacidad de emitir notificaciones a partir de eventos y datos recopilados a través de mecanismos como SMTP, SNMP y SYSLOG.
- Correlacionar eventos en tiempo real, es decir, que la información de los eventos sobre los que se está basando deberá venir del flujo del bus de mensajes.
- Capacidad para definir reglas de correlación con distintos niveles de complejidad, partiendo de las basadas en patrones, hasta reglas basadas en periodos de tiempo, anidadas, causa/efecto y secuenciales.
- El módulo de creación de reglas de correlación deberá tener la capacidad de seleccionar eventos para hacer las reglas, así como el seleccionar campos del mismo para ser incluidos en la regla a través de mecanismos como “Drag-and-Drop”.
- Contar con la capacidad de probar las reglas antes de ser implementadas en el motor de correlación.
- Deberá comprimir los datos almacenados al menos con una relación de 10 a 1.
- Contar con mecanismos de monitoreo de la integridad de la información local y archivada.
- Capacidad para soportar de forma nativa la integración con soluciones de almacenamiento en red como SAN, NAS, NFS o CIFS.
- Contar con una suscripción de boletines de seguridad más importantes del mercado para así identificar las vulnerabilidades conocidas, correlacionando la información de herramientas de administración de vulnerabilidades con los eventos recolectados, lo que permitirá automatizar su detección.

12. Servicio de Protección de Amenazas Persistentes Avanzadas (APT)

Se requieren mínimo 2 y máximo 4 equipos para el centro de datos principal ubicado en Morelia Michoacán (configuraciones en HA)

Especificaciones Técnicas:

- Detectar cuando un equipo intenta hacer comunicación con un servidor de comando y control en Internet.
- Detectar cuando una amenaza intenta ingresar en la organización mediante internet.
- Detectar e interactuar cuando un atacante o código maliciosos está realizando actividades de movimientos laterales en la organización.
- Detectar ataques del tipo “zero day” que puedan intentar comprometer activos de la organización.
- Tener las capacidades de detección de anomalías en los puntos de la red designados, dicha detección no debe basarse en firmas ni heurística.
- Tener la capacidad de actuar no solo por la generación de alertas de los componentes tecnológicos implementados, si no capacidades de caza de amenazas.
- Contar con las capacidades de análisis y perfilamiento de los actores detrás de un ataque sobre el Instituto.
- Apoyará al Instituto en la detección y prevención de ataques avanzados, así como el manejo de



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

los incidentes que deriven de ello.

- Elevar el nivel de visibilidad respecto a detección de amenazas avanzadas persistentes.
- Elevar el nivel de capacidades de actuación ante una amenaza avanzada persistente.
- Permitir contar con la información suficiente para identificar el impacto real de una amenaza.
- Permitir proteger diversos segmentos de la red del Instituto con diferentes niveles de protección de acuerdo con la criticidad de los usuarios de cada segmento.
- Permitir tener arquitectura modular y escalable de protección y viabilidad.
- Contar con un servicio especializado que permita apoyar al Instituto en la actuación y respuesta ante un ataque desarrollado con amenazas avanzadas.
- Acortar los tiempos de detección y actuación ante una amenaza avanzada.
- Integrar las capacidades de identificar una amenaza cuando tiene comunicación al exterior mediante el servicio de internet del Instituto o movimiento laterales en las diversas localidades, estas capacidades de detección deberán tener la capacidad de perfilar el comportamiento de los usuarios y sus dispositivos con el propósito de detectar cualquier anomalía que puede representar un impacto o riesgo para la Institución
- Disponer de una capa de inteligencia provista por los fabricantes de los componentes tecnológicos y fortalecida por la capa de inteligencia propia del Proveedor; dichas capas deben incluir al menos las siguientes características:
 - IP, URL Maliciosos
 - Hashes de archivos maliciosos
 - Tácticas, técnicas y procedimientos de los atacantes de la región en organizaciones similares al Instituto.
- Proporcionar las capacidades de realizar investigaciones en profundidad para detectar intrusiones que han pasado desapercibidas para los controles de seguridad implementados, esta investigación debe permitir al menos las siguientes capacidades:
 - Caza de amenazas que han estado activas, pero por su comportamiento no han podido ser detectadas.
 - Interacción con el código malicioso y ataques mediante la implementación de trampas en la red y la emulación de servicios.
 - Engaño de los atacantes mediante la implementación de información que pueda rastrear el origen de un ataque.
 - Análisis dinámico de los artefactos detectados.
 - Análisis de indicadores de compromiso en la red de cómputo del Instituto.
- Generar inteligencia accionable con la cual se puedan alimentar los controles preventivos para evitar que una amenaza conocida pueda volver a presentarse o la detección y contención sea temprana.

13. Antivirus

Se requieren servicios para el centro de datos principal ubicado en Morelia Michoacán en HA

Especificaciones Técnicas:

La solución propuesta por el proveedor deberá contar con las siguientes funcionalidades:

- La solución antivirus debe proteger a los siguientes sistemas operativos, en las plataformas Intel y AMD (Windows Server 2012 y posteriores).
- La solución antivirus deberá integrar agentes para la detección de virus, malware, entre otros en



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- las plataformas de correo electrónico institucional (Exchange Server 2010 y superiores)
- Reputación Web
 - La solución de antivirus deberá contar con un sistema basado en la reputación de sitios web que permitan de manera proactiva evitar que los usuarios cuando naveguen descarguen componentes maliciosos e infecten sus estaciones de trabajo.
 - El sistema de reputación de archivos debe estar integrado o desagregado de la consola de antimalware.
 - Niveles de seguridad para evitar la navegación Web a sitios maliciosos cuando los usuarios se encuentran dentro o fuera de la red corporativa.
 - Permitir reclasificar sitios web.
 - El sistema de protección Web no deberá depender de ningún explorador en específico.
 - Permitir editar la lista de URL permitidas a nivel general, grupos o personal.
- Ataques de día Zero
 - Cuando es publicada o descubierta una vulnerabilidad en sistema operativo o en alguna aplicación, el Antimalware deberá ser capaz de detener un ataque causado por un malware que aprovecha la vulnerabilidad descubierta.
- Protección Antimalware
 - Detectar, analizar y eliminar programas maliciosos, como virus, spyware, gusanos, troyanos, keyloggers, programas publicitarios, rootkits, phishing, entre otros.
 - Detectar, analizar y eliminar, de forma automática y en tiempo real, los programas maliciosos en:
 - Procesos que se ejecutan en la memoria principal (RAM);
 - Archivos creados, copiar, renombrar, mover o modificados, incluyendo períodos de sesiones en la línea de comandos (DOS o shell) abiertos por el usuario;
 - Archivos comprimidos de forma automática, al menos en los siguientes formatos: ZIP, EXE, ARJ, MIME / UU, CAB de Microsoft, Microsoft Comprimir.
 - Archivos recibidos a través de software de comunicación instantánea (Whatsapp, MSN Messenger, Yahoo Messenger, Google Talk, ICQ, entre otros).
 - Detectar y proteger a la estación de trabajo contra acciones maliciosas que se ejecutan en navegadores Web mediante secuencias de comandos en lenguajes tales como JavaScript, VBScript / ActiveX, etc.
 - La detección heurística de virus desconocidos.
- Control de dispositivos
 - Proporcionar o restringir el acceso a dispositivos USB, Floppy, CD's y Carpetas compartidas.
 - La solución Antimalware deberá evitar una infección provocada por la ejecución del archivo Autorun.inf contenido en un dispositivo de USB al momento de ser conectado en la estación de trabajo.
 - Para los dispositivos USBs, Floppy, CD's y Carpetas compartidas, el antimalware deberá permitir al usuario hacer modificaciones, control total, solo lectura y ejecución, solo lectura en el contenido del dispositivo. Siendo esta configuración independiente para cada uno de los dispositivos a proteger.
- Protección por comportamiento
 - Para aquellos programas que no están permitidos ser ejecutados en la estación de trabajo, deberán ser agregados a una lista de bloqueo de programas específicos.
 - Evitar o monitorear que un programa con comportamiento sospechoso pueda realizar lo siguiente:
 - Duplicar o injectar archivos de sistema similares.
 - Modificar el archivo de HOST.
 - Incrustar elementos "plugins" en el navegador de Internet Explorer.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- Instalar librería del programa malicioso.
- Instale nuevos servicios.
- Modifique archivos de sistema.
- Instale servicios o programas para iniciarse al arrancar la estación de trabajo.
- Reporte de amenazas a los laboratorios
 - Capacidad de reportar eventos de amenazas aún no identificadas, de manera automática a través del comportamiento, a los laboratorios de antimalware para el análisis e identificación de la fuente y generación de una protección proactiva.
 - Capacidad de limitar los recursos utilizados para la notificación a los laboratorios, respetando la confidencialidad de la información.
 - Lanzar una política de seguridad en caso de epidemias.
- Métodos de Actualización, Instalación y desinstalación
 - Instalación de cliente antivirus mediante la URL de la Consola de la solución.
 - Instalación de cliente antivirus mediante línea de comandos o script.
 - Lanzamiento de instalación vía navegación de los grupos de trabajo de Windows.
 - Lanzamiento de instalación vía integración con el dominio de Active Directory.
 - Lanzamiento de instalación vía escaneo de equipos dentro de un segmento de Red.
 - Desinstalación del cliente desde el administrador de programas de Windows o el acceso directo a Uninstall.exe del menú inicio.
 - Desinstalación del cliente de forma remota desde la consola de administración.
 - Configuración de Actualizaciones automáticas, así como la fuente de actualización.
 - Distribución de actualizaciones a los clientes de manera Automática y Manual.
 - Actualización de sistema de firmas para clientes sin conectividad al servidor.
 - Actualización de grupo de usuarios por Agentes de Actualización o repositorios.
- Configuración de escaneos
 - Personalización de opciones de escaneo y Acción para una detección en los modos: Manual, en Tiempo Real y Programado.
- Privilegios de los usuarios
 - Personalizar los permisos de los clientes para realizar acciones en el software local.
 - Inhabilitación de los servicios y/o componentes del Cliente antivirus por medio de contraseña.
 - Habilitar o deshabilitar opciones para el cliente que frecuentemente entra/sale de la red local.

14. Servicios de Prevención de Perdida de Información

Se requieren servicios para el centro de datos principal ubicado en Morelia Michoacán en HA

Especificaciones Técnicas:

La solución propuesta por el proveedor deberá contar con las siguientes funcionalidades:

- Presente un Log de auditoría de todas las actividades de los usuarios.
- Proporcione Reportes predefinidos y personalizados que puedan ser programados o de una sola vez.
- Proporcione un mecanismo de alertas y notificaciones.
- Que sea capaz de proporcionar administración basada en roles múltiples con las siguientes opciones:



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- Capacidad para definir roles de usuarios tales como Administrador, administrador de la seguridad o administrador de cuentas.
- Capacidad para agregar y modificar roles personalizados.
- Capacidad de configurar cuentas de usuario y asignar un rol particular a cada usuario.
- Tecnología de Detección.
 - Capacidad para extraer textos de diferentes tipos de documentos para ejecutar escaneos de contenido.
 - Capacidad de realizar detecciones basadas en palabras (keywords) personalizadas o frases (key phrases) personalizadas, con la habilidad de poner diferentes palabras en una sola regla de detección.
 - Capacidad de detección basada en expresiones regulares.
 - Capacidad de detección basada en atributos de archivos tales como tipo de archivo y tamaño de archivo.
 - Capacidad de utilizar validación de reglas de expresión.
 - Capaz de extraer y ejecutar escaneo de contenido de documentos dentro de archivos comprimidos tales como archivos zip y rar.
 - Capaz de controlar la cantidad de capas de compresión que va a descomprimir en archivos comprimidos.
 - Capaz de soportar texto en diferentes idiomas (al menos español e inglés).
 - Que sea capaz de definir identificadores de datos a través de palabras, expresiones o atributos de archivos.
 - Proporcione identificadores de datos predefinidos.
 - Capaz de duplicar y personalizar identificadores de datos predefinidos y personalizados.
 - Capaz de crear identificadores de datos múltiples.
 - Que sea capaz de combinar palabras, expresiones y atributos de archivos dentro de plantillas para identificar información sensible.
 - Proporcione plantillas predefinidas.
 - Con capacidad para importar y exportar plantillas.
 - Capacidad para crear diversas plantillas personalizadas.
 - Capaz de combinar diversas plantillas dentro de una política.
 - Capacidad de crear diversas políticas.
 - Capacidad de crear políticas desde la consola de administración centralizada.
 - Capaz de soportar diversas acciones para una política simple.
 - Capaz de definir un set diferente de acciones basado en la condición de la máquina si está dentro o fuera de la red.
 - Capaz de soportar las siguientes acciones cuando haya fuga de información sensible:
 - Sólo registro del evento (Log violation only).
 - Bloqueo de la transferencia de datos (Block data transfer).
 - Alertas en el equipo del cliente (Client-side alerts).
 - Alertas en el servidor de DLP (Server-side alerting).
 - Almacenamiento de información para análisis forense (Forensic data-capture)
- Debe de ser capaz de ejecutar escaneos de contenido en los siguientes canales de información:
 - Correo electrónico
 - HTTP/HTTPS
 - FTP
 - Dispositivos removibles
 - Copia de información a CD/DVD
 - Mensajería instantánea
 - Comando de impresión
 - P2P



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- Portapapeles
- Correo web
- Capaz de restringir acceso a los siguientes dispositivos:
 - Unidades extraíbles
 - Unidades ópticas
 - IEEE 1394
 - Impresión de pantalla
 - Bluetooth
 - Tarjetas PCMCIA
 - Carpetas compartidas
- Capaz de especificar excepciones de dispositivos
 - Capaz de definir diversas excepciones.
 - Capaz de utilizar comodines cuando se defina una excepción de dispositivos.
 - La configuración de control de dispositivos se debe de realizar de forma centralizada, desde la consola de administración.
 - Capaz de enviar un mensaje de notificación en la computadora del cliente.
 - Capaz de guardar en el log los eventos de control de dispositivos.

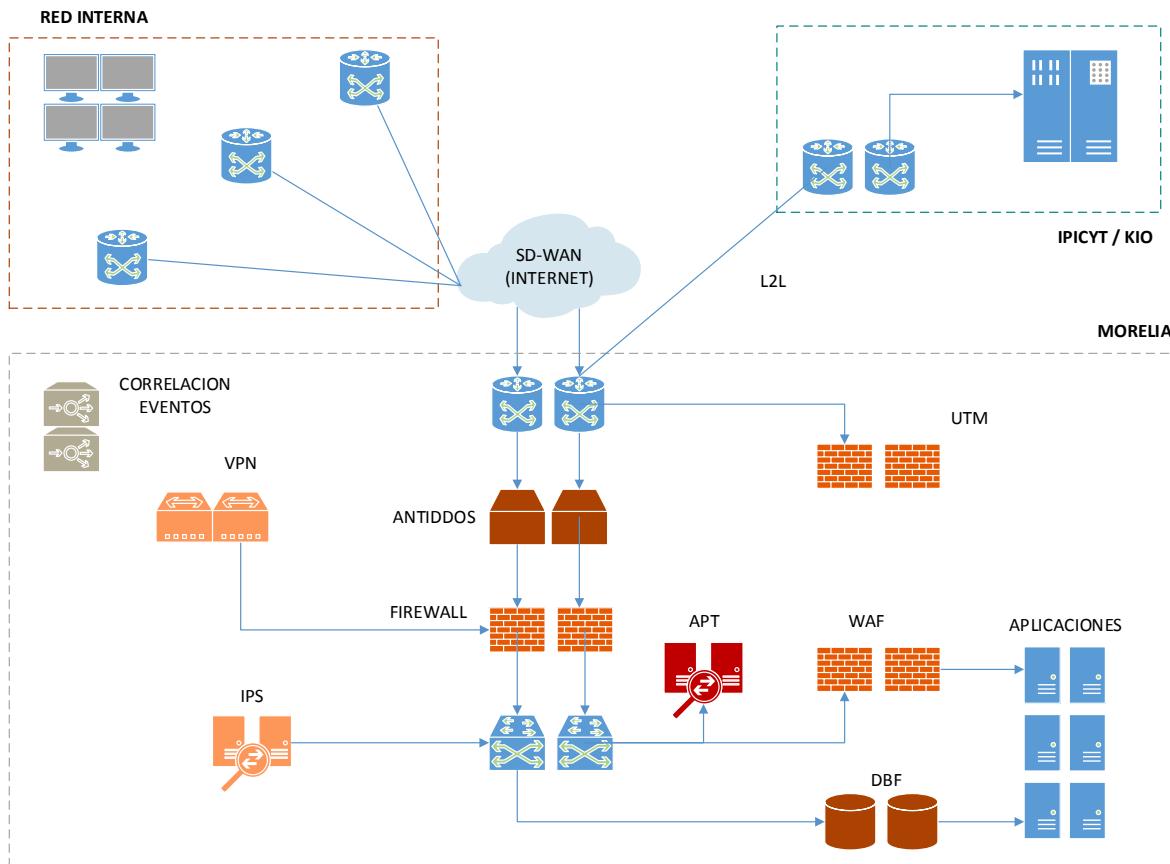
15. Generales para todas las soluciones

- Todas las soluciones deben de cumplir como mínimo con estas especificaciones y capacidades, lo cual son enunciativas más no limitativas.
- Las propuestas deberán considerar todos los componentes necesarios para su correcta operación (Equipo activo de Telecomunicaciones, cableado, módulos, etc.)
- Las propuestas Técnicas, deberán ser acompañadas de las hojas de especificaciones, trípticos y demás información que permita verificar el cumplimiento de las mismas.
- Los proveedores podrán realizar propuestas de mejora de cada una de las soluciones y/o diseño de la red con forme a sus propuestas. (Ver el diagrama 01 propuesta mínima esperada de las soluciones).
- De las propuestas de solución, podrán proponer arreglos tipo cluster.

DIAGRAMA 01. PROPUESTA MÍNIMA ESPERADA DE LAS SOLUCIONES



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022



16. Especificaciones físicas y estándares de conexión para los insumos que conforman los Servicios Administrados de Seguridad Informática 2022-2024

- Especificación y requerimientos de energía eléctrica

El Instituto proporcionará las facilidades dentro de los centro de datos para la alimentación eléctrica (contactos regulados), para el funcionamiento y operación del equipamiento propuesto por el licitante, el proveedor deberá considerar en su propuesta técnica la característica, cantidad, ubicación y los tipos de contactos requeridos para el aprovisionamiento inicial.

- Especificación y requerimientos de espacio físico y ambiental

El Instituto proporcionará la información específica respecto al espacio físico asignado para que el proveedor adjudicado instale la infraestructura de redes y seguridad en los centro de datos correspondientes. Para tal efecto el licitante deberá incluir en su propuesta técnica un apartado indicando la cantidad de espacio físico mínimo indispensable que se requerirá para la instalación de la infraestructura de seguridad.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

También se deberá contar con las facilidades para su instalación y se deberá apegar al reglamento y políticas internas para la instalación dentro de cada Centro de Datos. Así también deberá indicar las condiciones ambientales adecuadas para el funcionamiento del equipo a instalar para dar el servicio.

- Especificación y requerimiento para el montaje de hardware

Debido a que el requerimiento del Instituto es un servicio administrado, será responsabilidad del proveedor adjudicado el montaje de los equipos propuestos, racks, gabinetes, rack de panel de parcheo (Parch panel rack), distribuidores fibra óptica, y todo lo necesario para la correcta operación de la solución propuesta, por lo que, en su propuesta económica debe considerar todo lo necesario con la finalidad de proveer lo necesario.

- Especificación para racks

El proveedor adjudicado deberá cumplir con las especificaciones de los racks y gabinetes, incluyendo sus dimensiones físicas, para cada uno de los centros de datos donde el Instituto indique para implementar los Servicios SASI 2022-2024, y en apego a las normas y estándares de la industria y los que se acuerden o indiquen durante las mesas de trabajo con el Instituto.

- Políticas de cableado estructurado en centro de datos

El proveedor adjudicado deberá cumplir con los requerimientos para cada uno de los Centros de Datos donde el Instituto indique implementar los Servicios SASI 2022-2024, y en apego a las normas y estándares de la industria y los que se acuerden o indiquen durante las mesas de trabajo con el Instituto, así mismo el proveedor adjudicado deberá suministrar los elementos para la interconectividad necesarios, por lo que deberá: proporcionar e implementar los distribuidores de fibras, las canaletas, los jumpers, y cualquier otro elemento que sea necesario para la correcta interconexión de los racks o puntos de interconexión bajo los estándares de cableado estructurado.

- Especificación de cableado para racks

El licitante deberá contemplar dentro de su propuesta (tanto para el aprovisionamiento inicial, como durante la operación y vigencia del contrato), todo el cableado, jumpers y patch cords necesarios para lograr la interconexión propuesta de todos y cada uno de los módulos y elementos del sistema.

- Especificaciones y requerimientos técnicos de cableado y conectores

Todos los componentes del sistema de cableado, así como troncales de cobre y/o fibra –excepto los correspondientes a los servidores- necesarios para la interconexión de todos los módulos de hardware solicitados para suministrar el servicio de SASI 2022-2024 en el Centro de Datos deberán incluirse como parte de la propuesta de los Licitantes y deberán ser sin costo extra para el IMSS. Asimismo, en el caso de incrementos en los servicios deberán estar incluidos.

- Especificaciones y requerimientos técnicos de equipo de comunicaciones de red

Todos los componentes de interconexión (comunicaciones o balanceo de cargas) que apoyen la operación y administración que se lleve a cabo entre las soluciones de seguridad y red, que por su naturaleza sean requeridos para la puesta en operación del servicio de SASI 2022-2024 en el Centro de Datos, deberán incluirse como parte de la propuesta de los Licitantes y deberán ser sin costo extra para el IMSS. Asimismo, en el caso de incrementos en los servicios deberán estar incluidos.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- Políticas de seguridad de acceso físico a externos

El proveedor adjudicado deberá cumplir las políticas de seguridad de acceso físico a externos en los centros de datos donde el instituto determine para la provisión de los Servicios correspondientes SASI 2022-2024.

- Especificación y requerimientos de sistema de canalización.

El proveedor adjudicado deberá salvaguardar la integridad física del cableado para evitar fallas potenciales en la operación. De este modo, para salvaguardar la correcta operación del sistema de cableado de fibra óptica y cableado UTP, el licitante ganador utilizará la infraestructura existente en los Centros de Datos y, en general, cumplirá con las norma y políticas de canalización en los mencionados Centros de Datos.

17. Condiciones para los servicios de mantenimiento

El proveedor adjudicado será responsable de realizar las tareas de mantenimiento preventivo y correctivo para la totalidad de la infraestructura dentro del alcance de los servicios de SASI 2022-2024, a través de las labores que considere necesarias y de acuerdo con la estrategia de entrega y soporte de los servicios correspondientes. Enseguida se detallan las condiciones específicas para este servicio.

18. Condiciones para los servicios de mantenimiento preventivo

Como parte del Servicio de Mantenimiento el proveedor adjudicado deberá realizar al menos un mantenimiento preventivo al año a toda la infraestructura que forme parte del contrato de SASI 2022-2024. Para lo cual deberá integrar un Plan de Mantenimiento Preventivo, en el cual debe tomar en cuenta para la proyección de mantenimientos, las ventanas de mantenimiento necesarias, con el fin de ser programadas e informadas con anticipación al administrador del contrato, con objeto de minimizar el impacto a la operación.

En la correspondiente propuesta técnica el licitante, deberá incluir un Plan de Mantenimiento Preventivo, el cual deberá incluir como mínimo:

- La descripción de los procesos asociados.
- Los Recursos Humanos y Materiales involucrados.
- Los alcances técnicos del mantenimiento y los protocolos de prueba.
- Las rutas de escalamiento correspondientes.

Esta información debe agruparse por tipo de equipo o infraestructura. Para cada caso, el proveedor adjudicado deberá contemplar el calendario de los servicios de mantenimiento preventivo, el cual será validado y autorizado por administrador del contrato, quien revisará que no afecte períodos críticos de la operación del Instituto.

El calendario final de mantenimientos preventivos, fundamentado en el Plan de Mantenimiento Preventivo que se entregará durante las Mesas de Trabajo, será elaborado por El licitante ganador y autorizado por el Instituto, acotando los inmuebles, fechas y actividades a realizar con el máximo detalle, a efectos de coordinar todas las labores necesarias para su correcta ejecución.

19. Condiciones para los servicios de mantenimiento correctivo



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

El proveedor adjudicado será responsable de realizar el mantenimiento correctivo para los servicios correspondientes de SASI 2021-2024, para lo cual, previamente deberá integrar a su propuesta los procedimientos para reportar un incidente que requiera mantenimiento correctivo, y un ejemplo de matriz de escalamiento con los niveles y tiempos establecidos entre cada nivel.

Como parte de las Mesas de Trabajo, El licitante ganador deberá proporcionar la Matriz de Escalamiento con los nombres de contactos y responsables.

El licitante ganador efectuará el servicio de Mantenimiento Correctivo cuantas veces sea necesario durante la vigencia del servicio, de acuerdo con las especificaciones técnicas del fabricante y consistirá en la reparación o remplazo de las partes dañadas del equipo, cuando ocurra una falla que así lo requiera.

Si el equipo en cuestión no puede ser reparado, deberá sustituirse por otro equipo de características técnicas iguales o superiores, sin que esto implique la degradación del nivel de servicio requerido para dicho equipo. El tiempo para el reemplazo de partes no deberá exceder los 30 días naturales, durante los cuales El licitante ganador deberá proporcionar un equipo provisional para mantener la operación. El tiempo para el reemplazo de equipos no deberá exceder los 45 días naturales, durante los cuales el licitante ganador deberá proporcionar un equipo provisional para mantener la operación.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Apéndice “B”

Servicios Administrados de Seguridad Informática (SASI) 2022-2024

Objetivo del Documento

Elaborar el documento que contenga los requerimientos y las especificaciones técnicas y de calidad, así como el alcance de la adquisición, arrendamiento o servicio de TIC y SI que se pretenda contratar.

2. Inventario de Activos de Infraestructura – Servicios de Continuidad

CONCEPTO	Sitio	Marca	Modelo	Número Serie
I. Servicios de Seguridad - Continuidad Operativa				
1. Arquitectura de Firewall.				
Tipo 1	IPICYT	Fortinet	FG-1100E	FG10E0TB21900070
Tipo 2	CENATI MONTERREY	Fortinet	FG-1100E	FG10E0TB21900374
	CENATI MONTERREY	Fortinet	FG-1100E	FG10E0TB20903342
Tipo 3	CENATI MÉXICO	Fortinet	FG-1800F	FG180FTK20900846
	CENATI MÉXICO	Fortinet	FG-1800F	FG180FTK20901096
	JALISCO	Fortinet	FG-1800F	FG180FTK20900666
	JALISCO	Fortinet	FG-1800F	FG180FTK20900667
Tipo 4	IPICYT	Fortinet	FG-4200F	FG420FTK20900121
	IPICYT	Fortinet	FG-4200F	FG420FTK20900136
2. Prevención de Intrusiones (IPS)				
Tipo 1	CENATI MÉXICO	Fortinet	FG-1800F-BDL-950-12	FG180FTK20901206
Tipo 2	CENATI MONTERREY	Fortinet	FG-2200E-BDL-950-12	FG2K2ET920900397
Tipo 3	CENATI MÉXICO	Fortinet	FG-3300E-BDL-950-12	FG3K3ET919900293
	CENATI MÉXICO	Fortinet	FG-3300E-BDL-950-12	FG3K3ET919900310
Tipo 4	IPICYT	Fortinet	FG-3300E-BDL-950-12	FG3K3ET919900331
	IPICYT	Fortinet	FG-3300E-BDL-950-12	FG3K3ET919900323
3. Anti-denegación de servicios DDoS				
Tipo 1	CENATI MONTERREY	Fortinet	FDD-1500F	FI1K5FTE20000010
	CENATI MONTERREY	Fortinet	FDD-1500F	FI1K5FTE20000039
Tipo 2	IPICYT	Fortinet	FDD-1500F	FI1K5FTE20000009



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

	IPICYT	Fortinet	FDD-1500F	FI1K5FTE20000045
4. Redes Privadas Virtuales (VPN)				
	IPICYT	Fortinet	FG-1100E	FG10E0TB21900305
	IPICYT	Fortinet	FG-1100E	FG10E0TB20903417
	IPICYT	Fortinet	FG-1100E	FG10E0TB20903544
	IPICYT	Fortinet	FG-1100E	FG10E0TB21900273
5. Filtrado de contenido web (WEBFILTERING)				
	IPICYT	Fortinet	FG-1801F-BDL-950-12	FG181FTK20900649
	IPICYT	Fortinet	FG-1801F-BDL-950-12	FG181FTK20900909
	IPICYT	Fortinet	FG-1801F-BDL-950-12	FG181FTK20901026
	IPICYT	Fortinet	FG-1801F-BDL-950-12	FG181FTK20901059
6. Antispam				
	IPICYT	Fortinet	FML-3200E-BDL-641-12	FE3K2ET319000024
	IPICYT	Fortinet	FML-3200E-BDL-641-12	FE3K2ET319000028
	IPICYT	Fortinet	FML-3200E-BDL-641-12	FE3K2ET319000029
	IPICYT	Fortinet	FML-3200E-BDL-641-12	FE3K2ET319000035
7. Firewall Especializado en Servicios Web (WAF)				
	IPICYT	IMPERVA	X10K2	2030BA3322
	IPICYT	IMPERVA	X10K2	2030BA3319
	CENATI MONTERREY	IMPERVA	X10K2	2030BA4461
	CENATI MONTERREY	IMPERVA	X10K2	2030BA4457
8. Firewall de Base de Datos (DBF)				
	IPICYT	IMPERVA	X6520	2030BA3391
	IPICYT	IMPERVA	X6520	2030BA3392
	CENATI MONTERREY	IMPERVA	X6520	2113BA0235
	CENATI MONTERREY	IMPERVA	X6520	2113BA0238
9. Gestión Unificada de Amenazas (UTM)				
Tipo 1	ATLIXCO	Fortinet	FG-100F-BDL-950-12	FG100FTK21003654
Tipo 2	OAXTEPEC	Fortinet	FG-400E-BDL-950-12	FG4H0ETB20902009
Tipo 3	CENATI MONTERREY	Fortinet	FG-600E-BDL-950-12	FG6H0ETB21901099



GOBIERNO DE
MÉXICO



DIRECCIÓN DE ADMINISTRACIÓN

Unidad de Adquisiciones

Coordinación de Adquisición de Bienes y Contratación de Servicios

Coordinación Técnica de Adquisición de Bienes de Inversión y Activos

División de Contratación de Activos y Logística

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Tipo 4	CENATI MÉXICO	Fortinet	FG-1800F-BDL-950-12	FG180FTK20901163
--------	---------------	----------	---------------------	------------------

143

Durango No. 291, 5to. piso. Col. Roma Norte. Alcaldía Cuauhtémoc. C. P. 06700. CDMX.

www.imss.aob.mx



Ricardo
2022 Flores
Año de
Magón

PRECURSOR DE LA REVOLUCIÓN MEXICANA



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Apéndice "B-bis" Servicios Administrados de Seguridad Informática (SASI) 2022-2024

1. Objetivo del Documento

Elaborar el documento que contenga los requerimientos y las especificaciones técnicas y de calidad, así como el alcance de la adquisición, arrendamiento o servicio de TIC y SI que se pretenda contratar.

2. Inventario de Activos de Infraestructura – Servicios de Continuidad

No.	Descripción del servicio	Unidad de medida	Cantidad referencial mínima	Cantidad referencial máxima
1	Licenciamiento Firewall (Tipo 1) - Renovacion	Servicio	1	1
2	Licenciamiento Firewall (Tipo 2) - Renovación	Servicio	2	2
3	Licenciamiento Firewall (Tipo 3) - Renovación	Servicio	4	4
4	Licenciamiento Firewall (Tipo 4) - Renovación	Servicio	2	2
5	Licenciamiento IPS (Tipo 1) - Renovación	Servicio	1	1
6	Licenciamiento IPS (Tipo 2) - Renovación	Servicio	1	1
7	Licenciamiento IPS (Tipo 3) - Renovación	Servicio	2	2
8	Licenciamiento IPS (Tipo 4) - Renovación	Servicio	2	2
9	Licenciamiento Anti-denegación de servicios DDoS (Tipo 1) - Renovación	Servicio	2	2
10	Licenciamiento Anti-denegación de servicios DDoS (Tipo 2) - Renovación	Servicio	2	2
11	Licenciamiento Redes Privadas Virtuales - Renovación	Servicio	4	4
12	Licenciamiento Filtrado de Contenido Web - Renovación	Servicio	4	4
13	Licenciamiento Filtrado de Contenido de Correo (Antispam) - Renovación	Servicio	4	4
14	Licenciamiento Firewall Especializado en Servicios Web (WAF) - Renovación	Servicio	4	4
15	Licenciamiento Firewall Especializado en Base de Datos (DBF) - Renovación	Servicio	4	4
16	Licenciamiento Gestión Unificada de Amenazas (UTM) (Tipo 1) - Renovación	Servicio	1	1
17	Licenciamiento Gestión Unificada de Amenazas (UTM) (Tipo 2) - Renovación	Servicio	1	1
18	Licenciamiento Gestión Unificada de Amenazas (UTM) (Tipo 3) - Renovación	Servicio	1	1



GOBIERNO DE
MÉXICO



DIRECCIÓN DE ADMINISTRACIÓN

Unidad de Adquisiciones

Coordinación de Adquisición de Bienes y Contratación de Servicios

Coordinación Técnica de Adquisición de Bienes de Inversión y Activos

División de Contratación de Activos y Logística

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

19	Licenciamiento Gestión Unificada de Servicio	1	1
	Amenazas (UTM) (Tipo 4) - Renovación		

145

Durango No. 291. 5to. piso. Col. Roma Norte. Alcaldía Cuauhtémoc. C. P. 06700. CDMX.

www.imss.aob.mx



Ricardo
2022 Flores
Año de
Magón

PRECURSOR DE LA REVOLUCIÓN MEXICANA



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Anexo 2.- Términos y Condiciones

1. Objetivo del documento

Establecer las necesidades y condiciones de entrega de los “Servicios Administrados de Seguridad Informática 2022-2024”.

2. Premisa

Las bases de datos, aplicaciones y cualquier otro tipo de información utilizadas en el suministro de los servicios o a la que se tenga acceso derivado de la naturaleza de los servicios, que sean propiedad exclusiva del Instituto Mexicano del Seguro Social (“El Instituto”) continuarán siendo propiedad exclusiva del mismo. En ese sentido, el proveedor se obliga a utilizarlas exclusivamente para cubrir los servicios requeridos.

El proveedor deberá presentar como parte de su propuesta técnica escrito firmado por su representante legal respecto de las obligaciones de confidencialidad, las cuales estarán sujetas a lo dispuesto por la Ley Federal de Transparencia y Acceso a la Información Pública o por la Ley correlativa aplicable al Instituto.

3. Nombre del proyecto

“Servicios Administrados de Seguridad Informática 2022 – 2024”

4. Objetivos del proyecto

El Instituto Mexicano del Seguro Social (IMSS), a través de la Dirección de Innovación y Desarrollo Tecnológico (DIDT) requiere contar de manera integrada y unificada, con los servicios administrados que brinden la continuidad operativa, de negocio y de seguridad de la información del Instituto que:

- Asegure y proteger la información Institucional.
- Garantice la continuidad operativa, de negocio y de la seguridad de la información de la Institución, durante la vigencia del presente contrato, especialmente durante la toma de operación y transición del contrato anterior a los servicios propios de SASI 2022-2024.
- Fortalezca la seguridad de la información de la Institución contra amenazas, disminuyendo el riesgo de sufrir incidentes de seguridad, mediante el uso de tecnología de punta para el monitoreo, detección, aseguramiento, contención y respuesta ante ataques que puedan presentarse en la infraestructura de cómputo, sistemas y aplicaciones del IMSS.
- Cuente con servicios de infraestructura regulados por niveles de servicio, que: implementen (instalen, migren, habiliten y pongan a punto) los componentes necesarios en los centros de datos y servicios propios del IMSS y que de forma complementaria gestionen (operen, monitorean, den soporte y mantenimiento preventivo y correctivo) a la correspondiente infraestructura con el propósito de satisfacer las necesidades de: conectividad, comunicación, protección, control y filtrado de la propia Institución, manteniendo la plataforma tecnológica en condiciones óptimas de operación.
- Cuente con los servicios de protección de forma unificada e integrada, incluyendo prevención de pérdida de información, protección de cómputo físico o virtual, correo electrónico externo e interno, herramientas de colaboración, acceso a internet e intranet, filtrado; mediante una solución integral



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

que permita una gestión consolidada de las funcionalidades, características y servicios, con el propósito de mantener, asegurar y robustecer el esquema de seguridad del IMSS.

- Cuente con servicios de seguridad de la información, que complementen el esquema de seguridad institucional de forma consistente y robusta, con el control, aseguramiento, diagnóstico, pruebas, metodologías, de distintos rubros como el de acceso a cuentas privilegiadas, base de datos, aplicaciones, fuentes múltiples, vulnerabilidades, investigación forense y de procesos de seguridad, así como con otros servicios especializados en materia de seguridad y tecnologías de la información.
- Cuente con servicios para la capacitación y de soporte extendido que tienen como objetivo coadyuvar en la prestación del resto de los servicios SASI 2022-2024.

5. Normas oficiales o certificaciones

- Certificado ISO/IEC27001:2013
- Certificado ISO/IEC20000-1:2018

Ambos vigentes a nombre del licitante participante.

6. Folletos, catálogos, fotografías, manuales entre otros

No aplica

7. Visitas a las instalaciones

No se requiere.

8. Tipo de abastecimiento requerido

El tipo de abastecimiento será mediante dos partidas.

9. Garantías

El proveedor, se obliga a constituir en la forma y términos previstos por los artículos 48 y 49 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público; 103 de su Reglamento y numerales 4.30 y 4.30.3 de las Políticas, Bases y Lineamientos en materia de Adquisiciones, Arrendamientos y Servicios del Instituto Mexicano del Seguro Social, la garantía de cumplimiento divisible correspondiente.

En cualquier momento, el instituto podrá hacer válida la póliza de garantía del contrato en caso de que el proveedor no cumpla con los tiempos y plazos de entrega establecidos en los presentes Términos y Condiciones.

Las modificaciones a las fianzas deberán formalizarse con la participación que corresponda a la afianzadora, en términos de las disposiciones aplicables.

La garantía permanecerá vigente a partir de la fecha de adjudicación del contrato respectivo, y hasta que se cumplan plenamente todas y cada una de las obligaciones del contrato, así como durante la substancialización de todos los recursos legales o juicios que, en su caso, sean interpuestos por cualquiera de las partes y hasta que se dicte la resolución definitiva por autoridad competente.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Para garantizar el cumplimiento de todas y cada una de las obligaciones estipuladas en el contrato Adjudicado, el proveedor se compromete a entregar, dentro de los 10 (diez) días naturales posteriores a la firma del contrato correspondiente, de conformidad con el artículo 103 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, por el 10% del monto máximo por el que se adjudica el contrato, a favor de el instituto, el cual será un contrato abierto y la garantía será divisible.

El proveedor, se obliga a entregar a el Instituto la póliza de fianza antes señalada, en la división de contratos, ubicada en calle Durango número 291, piso 10, Colonia Roma Norte, Alcaldía Cuauhtémoc, apegándose al formato que para tal efecto se entregará en la referida División.

a) Devolución de garantías

La liberación de garantías relativas al cumplimiento del Contrato podrán realizarse una vez que haya transcurrido el plazo de garantía indicado, a solicitud expresa por el proveedor por escrito en papel membretado de su empresa, dicha solicitud debe dirigirse a la Coordinación de Adquisición de Bienes y Contratación de Servicios, quien autorizará la devolución o cancelación de la póliza de garantía (fianza) correspondiente, dicha autorización se entregará al proveedor, siempre que demuestre haber cumplido con la totalidad de las obligaciones adquiridas por virtud del presente Contrato.

La garantía de cumplimiento a las obligaciones del contrato únicamente podrá ser liberada mediante autorización expresa y por escrito otorgado por la División de Seguridad Informática Física.

b) Ejecución de la garantía

Se hará efectiva la garantía relativa al cumplimiento del contrato cuando:

- El proveedor incumpla con cualquiera de las obligaciones establecidas en el contrato que se celebre.
- Se rescinda administrativamente el contrato.
- La ejecución de la garantía será con independencia de la aplicación de las penas convencionales que procedan y de la rescisión administrativa del contrato.
- La ejecución de la garantía de cumplimiento del contrato será proporcional al monto de las obligaciones incumplidas.
- Además de las sanciones anteriormente mencionadas, serán aplicables las que estipulen las disposiciones legales vigentes en la materia.

10. Acuerdos de Niveles de Servicio

El objetivo de los niveles de servicio consiste en proporcionar al Instituto un mecanismo que permita:

- Medir de forma efectiva el desempeño de los servicios proporcionados por el proveedor.
- Procurar que los servicios le sean proporcionados con la calidad prevista.

De conformidad con lo establecido en el artículo 53 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, el Instituto aplicará penas convencionales por el atraso en el cumplimiento de las fechas pactadas de entrega o de la prestación del servicio, las que no excederán del monto de la garantía de cumplimiento del contrato, y serán determinadas en función de los bienes o servicios no entregados o prestados oportunamente.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

10.1. Penas Convencionales

Se aplicarán penas convencionales por incumplimiento en el plazo de prestación de los servicios por parte del proveedor adjudicado del 0.2% por cada día natural de atraso en el inicio de la prestación del servicio, respecto del valor máximo total del contrato.

10.2. Servicios de Habilitación, Operación y Transición

Partida 1 y 2

DESCRIPCIÓN DEL NIVEL DE SERVICIO	FECHA DE ENTREGA	PENA CONVENCIONAL MENSUAL	FÓRMULA DE CÁLCULO
Plan de trabajo detallado de los servicios del proyecto	15 días naturales posteriores a la emisión del fallo	1% por cada día natural de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Documento Compromiso de suscripción de OLAs	15 días naturales posteriores a la emisión del fallo	1% por cada día natural de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Matriz de Escalación	15 días naturales posteriores a la emisión del fallo	1% por cada día natural de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Escrito por parte del proveedor, firmado por el representante legal, donde declare sus habilidades, competencias y capacidades para soportar la prestación de los servicios	15 días naturales posteriores a la emisión del fallo	1% por cada día natural de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

10.3. Servicios de Seguridad – Continuidad Operativa

Partida 1



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

DESCRIPCIÓN DEL NIVEL DE SERVICIO	FECHA DE ENTREGA	PENA CONVENCIONAL MENSUAL	FÓRMULA DE CÁLCULO
Documento con el diseño de alto nivel de las soluciones de seguridad a implementar en los centros de datos o donde lo indique el Instituto	5 días hábiles posteriores a la integración de las mesas de trabajo por cada servicio que se pretenda habilitar	2% por cada día hábil de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Documento con el diseño de bajo nivel de las soluciones de seguridad a implementar en los centros de datos o donde lo indique el Instituto	10 días hábiles posteriores a la integración de las mesas de trabajo por cada servicio que se pretenda habilitar	2% por cada día hábil de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Memorias técnicas iniciales de las soluciones de seguridad implementadas	10 días hábiles posteriores al término de la habilitación de todos los componentes en los Centro de Datos o donde lo indique el Instituto, conforme cada solución integrada y posterior a la integración de las mesas de trabajo	2% por cada día hábil de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Memorias técnicas actualizadas de los servicios de seguridad	20 días hábiles previo al término del contrato para aquellos servicios que se encuentren habilitados	2% por cada día hábil de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

10.4. Servicios de Seguridad – Verificación/Calidad

Partida 1



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

DESCRIPCIÓN DEL NIVEL DE SERVICIO	FECHA DE ENTREGA	PENA CONVENCIONAL MENSUAL	FÓRMULA DE CÁLCULO
Documento con el diseño de Alto Nivel de los servicios de Seguridad a implementar en los centros de datos o donde lo indique el Instituto, que requieran integrar activos de infraestructura para su habilitación	5 días hábiles posteriores a la integración de las mesas de trabajo por cada servicio que se pretenda habilitar	2% por cada día hábil de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Documento con el diseño de Bajo Nivel de las Soluciones de Seguridad a implementar en los centros de datos o donde lo indique el Instituto	10 días hábiles posteriores a la integración de las mesas de trabajo por cada servicio que se pretenda habilitar	2% por cada día hábil de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Memorias Técnicas Iniciales de las Soluciones de Seguridad Implementadas, que requieran integrar activos de infraestructura para su habilitación	10 días hábiles posteriores al término de la habilitación de todos los componentes en los Centro de Datos o donde lo indique el Instituto, conforme cada solución integrada y posterior a la integración de las mesas de trabajo	2% por cada día hábil de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

DESCRIPCIÓN DEL NIVEL DE SERVICIO	FECHA DE ENTREGA	PENA CONVENCIONAL MENSUAL	FÓRMULA DE CÁLCULO
Memorias Técnicas Actualizadas de las Servicios de Seguridad que requieran integrar activos de infraestructura para su habilitación	20 días hábiles previo al término del contrato para aquellos servicios que se encuentren habilitados	2% por cada día hábil de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
<u>Procedimientos de Operación del servicio</u> <ul style="list-style-type: none"> • Servicios de Borrado Seguro de Información • Servicio de Gestión de Dominios • Servicio de Certificados Digitales SSL • Servicios de Ciberinteligencia • Servicios de Protección en Redes Inalámbricas y Seguridad en Dispositivos móviles • Servicios de Antivirus • Servicios de Prevención de Perdida de Información 	10 días hábiles posteriores a la integración de las mesas de trabajo	2% por cada día hábil de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

DESCRIPCIÓN DEL NIVEL DE SERVICIO	FECHA DE ENTREGA	PENA CONVENCIONAL MENSUAL	FÓRMULA DE CÁLCULO
<p>Metodología de implementación de los servicios.</p> <ul style="list-style-type: none"> • Servicios de Sistema de Gestión de Seguridad de la Información (SGSI) • Servicios de Gestión del Cambio en Seguridad de la Información 	10 días hábiles posteriores a la integración de las mesas de trabajo	2% por cada día hábil de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

Partida 2

DESCRIPCIÓN DEL NIVEL DE SERVICIO	FECHA DE ENTREGA	PENA CONVENCIONAL MENSUAL	FÓRMULA DE CÁLCULO
<u>Procedimientos de Operación del servicio</u> <ul style="list-style-type: none"> • Servicio de Análisis de Vulnerabilidades Estático • Servicio de Análisis de Vulnerabilidades Dinámico • Servicios de Análisis Forense • Servicio de Pruebas de Penetración 	10 días hábiles posteriores a la integración de las mesas de trabajo	2% por cada día hábil de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

10.5. Servicios del Centro de Operaciones de Seguridad (SOC)

Partida 1



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

DESCRIPCIÓN DEL NIVEL DE SERVICIO	FECHA DE ENTREGA	PENA CONVENCIONAL MENSUAL	FÓRMULA DE CÁLCULO
Procesos de operación implementados: • Requerimientos • Cambios • Configuraciones • Incidentes • Problemas • Monitoreo	15 días naturales posteriores a la emisión del fallo	2% por cada día natural de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Matriz de Escalación Técnica y Organizacional	15 días naturales posteriores a la emisión del fallo	2% por cada día natural de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
<u>Procedimiento de operación de la Mesa de Servicios:</u> • Requerimientos • Cambios • Configuraciones • Incidentes • Problemas • Monitoreo	15 días naturales posteriores a la emisión del fallo	2% por cada día natural de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Expedientes Curriculares personal del SOC	15 días naturales posterior a la emisión del fallo	2% por cada día natural de atraso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

10.6. Deducciones

Durante la vigencia del contrato, al presentarse una falla, incidente, atención de requerimientos, ventana de mantenimiento, entre otras, cuya causa raíz haya sido derivada por un tercero, la deductiva correspondiente al servicio asociado no será aplicada al proveedor de SASI 2022-2024, siempre y cuando demuestre con evidencias fehacientes que el servicio correspondiente se presentó bajo las especificaciones del anexo técnico, términos y condiciones y los apéndices A y B.

Con base en lo anterior, y cuando las fallas, incidentes, atención de requerimientos, ventanas de mantenimiento, entre otras, sean atribuibles a la entrega de los servicios de seguridad por parte del Proveedor, se aplicarán deductivas conforme lo siguiente rubros:

10.7. Disponibilidad



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Partida 1

La disponibilidad se define como la medida del porcentaje de tiempo, en que el sistema que brinda el servicio de seguridad de SASI 2022-2024, (o un componente del sistema) realiza la función que le es propia. Es decir; disponibilidad es la proporción de tiempo en que el sistema cumple con la función para la cual está dispuesto, en relación con el tiempo en que debería haber estado disponible.

Las mediciones de disponibilidad deberán ser realizadas por el Proveedor de SASI 2022-2024, usando su correspondiente herramienta de monitoreo del servicio y herramienta de gestión de incidentes, con el afán de obtener mediciones precisas con respecto a los tiempos operacionales y los no operacionales y sus atribuibles.

Deberán realizarse mediciones de disponibilidad desde el inicio del período operacional de los servicios de infraestructura SASI 2022-2024, para todos los módulos o posiciones de servicio contratados.

El Proveedor de SASI 2022-2024, comprometerá la disponibilidad en base a los siguientes factores:

Incluye todos los componentes WAN, LAN, dispositivos de seguridad, y demás dispositivos que soportan al servicio de seguridad, así como su equivalente de configuración lógica.

El origen de medición será por una correlación de los poleos y/o muestras recolectadas cada 5 minutos por el sistema de monitoreo y los períodos de indisponibilidad extraídos de los incidentes abiertos en el sistema de administrador de incidencias del proveedor de SASI 2022-2024, restándosele aquellos períodos de indisponibilidad cuya responsabilidad no sea atribuible al Proveedor de SASI 2022-2024. La forma de medición en específico se describirá de la siguiente manera.

- Calculada en base a 30 días por mes
- Calculada a partir del inicio de la falla
- Se considera indisponible cuando el protocolo de la interfaz se encuentra caído (Down) o por caída de tráfico imputable a infraestructura del proveedor.
- Solo es calculada en base a fallas imputables al Proveedor de SASI 2022-2024.

Disponibilidad por sitio y por posición de servicio

Las caídas originadas por falla de energía responsabilidad del Instituto no serán tomadas en cuenta para la disponibilidad.

$$\text{Disponibilidad_del_Servicio} = \left[\frac{\text{Tiempo_Total} - (\text{Tiempo_Indisponible} - \text{Tiempo_Instituto})}{\text{Tiempo_Total}} \right] \times 100$$

Dónde:

Tiempo Total: Tiempo total de disponibilidad para el mes de medición.

Tiempo Indisponible: Tiempo indisponible según plataforma de monitoreo.

Tiempo Instituto: Tiempos atribuibles al Instituto extraídos del sistema de administración de incidentes.

Objetivos por métrica:

Disponibilidad Servicio	% Disponibilidad
Servicios de Seguridad – Continuidad Operativa	99.99%



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Servicios de Seguridad – Verificación y Calidad	99.97%
Servicios del Centro de Operaciones de Seguridad (SOC)	99.99%

Deductiva por incumplimiento

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
Cuando no se cumplen con los objetivos de servicio, para los diferentes niveles de disponibilidad, conforme al esquema de medición propuesto	% Disponibilidad conforme la tabla de objetivos	Minuto	0.5% por cada minuto de indisponibilidad	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

10.8. Tiempo de detección y solución de fallas

Partida 1

La métrica de tiempo de solución a fallas es independiente de la métrica de disponibilidad, dado que se refiere al tiempo en el cual será devuelta a la normalidad (restitución de la operación estable) uno o varios servicios al presentarse una falla. Las mediciones de Tiempo de Solución de Fallas deberán ser realizadas por el Proveedor de SASI 2022-2024, usando su correspondiente herramienta de gestión y monitoreo del servicio. El Proveedor deberá realizar esta medición en un periodo mensual considerando el promedio del tiempo de solución para cada tipo de severidad. La metodología que se realice, las herramientas y los responsables sobre las mediciones, quedarán definidos en las mesas de trabajo.

El Tiempo de Solución a Fallas se divide en tres casos, en función de la severidad, causa e impacto de los mismos:

Severidad Crítica: Representa un incidente de alto impacto dado el riesgo que representa. Este tipo de incidente puede, potencialmente, ocasionar afectación y daño en activos y servicios del cliente. Eventos de afectación total al servicio, pérdida total del sistema de comunicaciones y/o seguridad, degradación de los recursos del Instituto o bien mediante el descubrimiento de vulnerabilidad en la infraestructura protegida. La alarma relativa en el sistema de gestión se mantiene por más de 10 minutos.

Severidad Alta: Representa un incidente serio en el que hay una degradación más no una afectación de negocio a los servicios e infraestructura que es protegida mediante los dispositivos de alta disponibilidad o de seguridad. El incidente se manifiesta mediante el bloqueo o bajo desempeño al acceder a ciertos servicios de red que requieren el uso de los dispositivos de comunicaciones y/o seguridad, así como la



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

pérdida parcial de alguna funcionalidad en el equipo de comunicaciones y/o seguridad. Eventos de afectación que ocasionan degradación en el servicio sin llegar a ocasionar caída del mismo.

Severidad Media: Representa un incidente menor que no trae consecuencias de impacto de negocio a los servicios e infraestructura protegida por los dispositivos de seguridad. El incidente se da mediante fallas en visualización de bitácoras o problemas para comunicación de servicios internos del Instituto y hacia un grupo reducido de usuarios. Eventos de afectación al servicio por períodos de tiempo menores a 10 minutos ocasionando intermitencia en la disponibilidad del servicio.

Severidad Baja: Son casos considerados como preventivos para fines de mejora u optimización de cualquier servicio de seguridad. Estos casos de severidad deben ser atendidos por ingenieros del proveedor de servicios en sitio con la colaboración del fabricante vía un centro de asistencia técnica personalizada. El tiempo de resolución de este tipo de falla será definido por el Instituto y el Proveedor de SASI 2022-2024, al momento de presentar el caso.

La severidad de un incidente es determinada por la convocante. Conforme la operación y criticidad de un servicio, se define la severidad, así como su nivel de escalación, con base en lo siguiente:

SEVERIDAD	AFFECTACIÓN	TIEMPO MÁXIMO DE REGISTRO	TIEMPO MÁXIMO DE SOLUCIÓN
Critica	Representa una falla de alto impacto que impide la operación total de un servicio, mismo que soporta una función de negocio del Instituto a nivel nacional.	10 minutos posteriores a la detección de la falla	2 horas posteriores al registro y notificación de la falla
Alta	Representa una falla en la que hay una degradación que impide la operación de un servicio, mismo que soporta una función de negocio del Instituto pero que no tiene un impacto a nivel nacional.	20 minutos posterior a la detección de la falla	4 horas posterior al registro y notificación de la falla
Media	Representa una falla menor que impide la operación de un servicio, mismo que afecta a un grupo de usuarios reducido del Instituto.	120 minutos posterior a la detección de la falla	48 horas posterior al registro y notificación de la falla



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Baja	Son casos considerados como preventivos para fines de mejora u optimización de cualquier servicio de seguridad, tienen un bajo impacto en la operación del negocio y su atención y/o solución puede ser calendarizada.	5 días hábiles posterior a la detección de la falla	Se define entre el Instituto y el Proveedor de SASI 2022-2024 conforme las mesas de trabajo que se establezcan para este propósito.
-------------	--	---	---

Deductivas por incumplimiento

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
Tiempo máximo de registro y notificación conforme al nivel de severidad crítica	10 minutos posteriores al registro y notificación de la falla	Minuto	0.2% por cada minuto de atraso en el registro y notificación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de solución conforme al nivel de severidad crítica	2 horas posteriores al registro y notificación de la falla	Hora	0.5% por cada hora o fracción de atraso en la solución de la falla	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de registro y notificación conforme al nivel de severidad alta	20 minutos posteriores al registro y notificación de la falla	Minuto	0.2% por cada minuto de atraso en el registro y notificación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
Tiempo máximo de solución conforme al nivel de severidad alta	4 horas posteriores a la registro y notificación de la falla	Hora	0.5% por cada hora o fracción de atraso en la solución de la falla	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de registro y notificación conforme al nivel de severidad media	120 minutos posteriores al registro y notificación de la falla	Minuto	0.2% por cada minuto de atraso en el registro y notificación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de solución conforme al nivel de severidad media	48 horas posteriores al registro y notificación de la falla	Hora	0.5% por cada hora o fracción de atraso en la solución de la falla	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de registro y notificación conforme al nivel de severidad baja	5 días hábiles posteriores al registro y notificación de la falla	Día	0.2% por cada día hábil de atraso en el registro y notificación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de solución conforme al nivel de severidad baja	Se define entre el Instituto y el Proveedor de SASI 2022-2024 conforme las mesas de trabajo que se establezcan para este propósito.	Día	0.5% por cada día de atraso en la solución de la falla conforme la fecha establecida en las mesas de trabajo	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

10.9. Tiempo de detección y mitigación de incidentes

Partida 1

Una actividad sospechosa son acciones que pudieran estar encaminadas a comprometer la seguridad de la red y de los activos de información, es la etapa previa a la materialización de un incidente de seguridad. Un incidente de seguridad es el registro de una violación a las políticas de seguridad informática o al uso aceptable de políticas o de prácticas de seguridad estandarizado; es la evidencia inequívoca de que la confidencialidad, integridad y disponibilidad de la información ha sido vulnerada.

Las métricas de tiempo para la actividad sospechosa se refieren al tiempo de notificación y envío de dictamen que el proveedor SASI 2022-2024 deberá realizar ante el Instituto al momento de detectar una actividad sospechosa. Ante una actividad sospechosa, el proveedor del SASI 2022-2024 deberá registrar y notificar al personal del Instituto en máximo 30 minutos. Posterior a su detección y registro, se deberá emitir un dictamen de actividad sospechosa con recomendaciones para erradicarla, este dictamen será enviado al personal del Instituto en máximo 90 minutos.

Las métricas para el tiempo de registro y notificación se refieren al tiempo en que proveedor SASI 2022-2024 avisa al Instituto cuando ha confirmado un incidente de seguridad, ésta métrica deberá realizarse en los tiempos definidos según la prioridad a partir de que se apertura algún registro relacionado con un incidente de seguridad. La métrica de tiempo de contención se refiere a que, tras la detección del incidente, el Proveedor de SASI 2022-2024 deberá detener y aislar el mismo según los tiempos definidos para cada prioridad.

Las mediciones deberán ser realizadas por el proveedor de SASI 2022-2024, usando su correspondiente herramienta de gestión y monitoreo del servicio. El proveedor deberá realizar esta medición en un periodo mensual según el nivel de servicio para cada tipo de métrica y/o prioridad.

Objetivos de la métrica

SEVERIDAD	AFFECTACIÓN	TIEMPO MÁXIMO DE REGISTRO	TIEMPO MÁXIMO DE SOLUCIÓN
Critica	Representa un incidente de alto impacto que impide la operación total de un servicio, mismo que soporta una función de negocio del Instituto a nivel nacional.	10 minutos posteriores a la detección del incidente	60 minutos posteriores al registro y notificación del incidente



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

SEVERIDAD	AFFECTACIÓN	TIEMPO MÁXIMO DE REGISTRO	TIEMPO MÁXIMO DE SOLUCIÓN
Alta	Representa un incidente en el que hay una degradación que impide la operación de un servicio, mismo que soporta una función de negocio del Instituto pero que no tiene un impacto a nivel nacional.	20 minutos posterior a la detección del incidente	240 minutos posteriores al registro y notificación del incidente
Media	Representa un incidente menor que impide la operación de un servicio, mismo que afecta a un grupo de usuarios reducido del Instituto.	30 minutos posterior a la detección del incidente	60 minutos posteriores al registro y notificación del incidente
Baja	Son casos considerados como preventivos para fines de mejora u optimización de cualquier servicio de seguridad, tienen un bajo impacto en la operación del negocio y su atención y/o solución puede ser calendarizada.	60 minutos posterior a la detección del incidente	2,880 minutos posteriores al registro y notificación del incidente

Deductiva por incumplimiento

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
---	----------------------	------------------------	-----------	-----------------------



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Registro y notificación de Actividad Sospechosa	30 minutos posteriores a la detección actividad sospechosa	Minuto	0.5% por cada minuto de atraso en el registro y notificación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Envío de Dictamen de Actividad Sospechosa	90 minutos posteriores al registro y notificación de actividad sospechosa	Minuto	1% por cada minuto de atraso en la elaboración del dictamen	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
Tiempo máximo de registro y notificación conforme al nivel de severidad crítica	10 minutos posteriores al registro y notificación del incidente	Minuto	0.5% por cada minuto de atraso en el registro y notificación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de solución conforme al nivel de severidad crítica	60 minutos posteriores al registro y notificación del incidente	Minuto	1% por cada minuto de atraso en la solución del incidente	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de registro y notificación conforme al nivel de severidad alta	20 minutos posteriores al registro y notificación del incidente	Minuto	0.5% por cada minuto de atraso en el registro y notificación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
Tiempo máximo de solución conforme al nivel de severidad alta	240 minutos posteriores al registro y notificación del incidente	Minuto	1% por cada minuto de atraso en la solución del incidente	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de registro y notificación conforme al nivel de severidad media	30 minutos posteriores al registro y notificación del incidente	Minuto	0.5% por cada minuto de atraso en el registro y notificación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de solución conforme al nivel de severidad media	1,440 minutos posteriores al registro y notificación del incidente	Minuto	1% por cada minuto de atraso en la solución del incidente	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de registro y notificación conforme al nivel de severidad baja	60 minutos posteriores al registro y notificación del incidente	Minuto	0.5% por cada minuto de atraso en el registro y notificación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de solución conforme al nivel de severidad baja	2,880 minutos posteriores al registro y notificación del incidente	Minuto	1% por cada minuto de atraso en la solución del incidente	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

10.10. Solicitudes de requerimientos y cambios



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Partida 1

Es el tiempo que tarda el Proveedor de SASI 2022-2024, en realizar una alta, cambio o baja sobre la infraestructura del servicio en seguridad, basada en el menú de configuraciones comunes preestablecidas durante las mesas de trabajo correspondientes. Estas configuraciones deberán ser acorde a las necesidades de conectividad y flujos de información de las aplicaciones del Instituto, entendiendo que la complicación para su atención es menor dado que se tiene la experiencia y el conocimiento de las mismas configuraciones de los módulos de los servicios de seguridad en operación.

Objetivos de la métrica:

PRIORIDAD	DESCRIPCIÓN	TIEMPO MÁXIMO DE REGISTRO	TIEMPO MÁXIMO DE EJECUCIÓN
Alta	Requerimiento generado por parte del Instituto a fin de atender a necesidades de operación emergentes.	10 minutos posteriores a la solicitud formal por parte del Instituto	60 minutos posteriores al registro realizado por el Instituto
Media	Requerimiento generado por parte del Instituto a fin de atender a necesidades de operación comunes.	30 minutos posteriores a la solicitud formal por parte del Instituto	480 minutos posteriores al registro realizado por el Instituto
Baja	Requerimiento generado por parte del Instituto a fin de atender a necesidades de operación programadas.	60 minutos posteriores a la solicitud formal por parte del Instituto	1,440 minutos posteriores al registro realizado por el Instituto

Cambios

PRIORIDAD	DESCRIPCIÓN	TIEMPO MÁXIMO DE REGISTRO	TIEMPO MÁXIMO DE EJECUCIÓN
-----------	-------------	---------------------------	----------------------------



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

PRIORIDAD	DESCRIPCIÓN	TIEMPO MÁXIMO DE REGISTRO	TIEMPO MÁXIMO DE EJECUCIÓN
Emergente	Cambios requeridos como resultado de una pérdida repentina del servicio, falla en un activo de infraestructura o a petición del Instituto.	1 hora posteriores a la solicitud formal por parte del Instituto	Conforme al plan de trabajo definido entre el Instituto y el Proveedor
Normal	Cambios solicitados para mejorar o restaurar un servicio o ampliar un activo de infraestructura, que no están considerados en el catálogo de cambios estándar, mismos que deben ser analizados y aprobados por el Instituto.	1 hora posteriores a la solicitud formal por parte del Instituto	Conforme al plan de trabajo definido entre el Instituto y el Proveedor
Estándar	Cambios en los servicios y/o activos de infraestructura que se realiza en línea y sigue una trayectoria establecida, mismos que representan una solución aceptada a un requerimiento o conjunto de requerimientos específicos.	1 hora posteriores a la solicitud formal por parte del Instituto	24 horas posterior al registro realizado por el Instituto

Cualquier cambio ejecutado por el Proveedor, mismo que no se encuentre autorizado por el Instituto, derive o no en alguna falla de los servicios de seguridad, será catalogado como un incidente de seguridad, mismo que será clasificado con base en las afectaciones o riesgos que pudieron generar.

Deductiva por incumplimiento:



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
Tiempo máximo de registro y notificación conforme al nivel de prioridad Alta	10 minutos posteriores al registro y notificación del requerimiento	Minuto	0.2% por cada minuto de atraso en el registro y notificación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de ejecución conforme al nivel de prioridad Alta	60 minutos posteriores al registro y notificación del requerimiento	Minuto	0.5% por cada minuto de atraso en la ejecución del requerimiento	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de registro y notificación conforme al nivel de prioridad Media	30 minutos posteriores al registro y notificación del requerimiento	Minuto	0.2% por cada minuto de atraso en el registro y notificación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de solución conforme al nivel de prioridad Media	8 horas posteriores al registro y notificación del requerimiento	Hora	0.5% por cada hora o fracción de atraso en la ejecución del requerimiento	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de registro y notificación conforme al nivel de prioridad Baja	60 minutos posteriores al registro y notificación del requerimiento	Minuto	0.2% por cada minuto de atraso en el registro y notificación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
Tiempo máximo de solución conforme al nivel de prioridad Baja	24 horas posteriores al registro y notificación del requerimiento	Hora	0.5% por cada hora o fracción de atraso en la ejecución del requerimiento	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

Cambios

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
Tiempo máximo de registro y notificación conforme al nivel de prioridad Emergente	60 minutos posteriores al registro y notificación del cambio	Minuto	0.2% por cada minuto de atraso en el registro y notificación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de ejecución conforme al nivel de prioridad Emergente	Conforme al plan de trabajo definido entre el Instituto y el Proveedor	Hora	1% por cada hora o fracción de atraso en la ejecución del cambio	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de registro y notificación conforme al nivel de prioridad Normal	60 minutos posteriores al registro y notificación del cambio	Minuto	0.2% por cada minuto de atraso en el registro y notificación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
Tiempo máximo de solución conforme al nivel de prioridad Normal	Conforme al plan de trabajo definido entre el Instituto y el Proveedor	Hora	1% por cada hora o fracción de atraso en la ejecución del cambio	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de registro y notificación conforme al nivel de prioridad Estándar	60 minutos posteriores al registro y notificación del cambio	Minuto	0.2% por cada minuto de atraso en el registro y notificación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tiempo máximo de solución conforme al nivel de prioridad Estándar	24 horas posteriores al registro y notificación del cambio	Hora	1% por cada hora o fracción de atraso en la ejecución del cambio	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

10.11. Servicios de Seguridad – Continuidad Operativa

Partida 1

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
---	------------------------------	---------------------------------	------------------	-------------------------------



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
<p>Reportes Técnicos de los activos de infraestructura que contemplen:</p> <ul style="list-style-type: none"> • Disponibilidad • Controles de Cambios • Requerimientos • Incidentes/Fallas • Actividad Sospechosa • Estadísticas de uso de los servicios (conforme la definición en las mesas de trabajo) 	5 días hábiles posteriores al cumplimiento del mes vencido	Día	1% por cada día hábil de atraso en la entrega de los reportes técnicos	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

10.12. Servicios de Seguridad – Verificación/Calidad

Partida 1

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
---	------------------------------	---------------------------------	------------------	-------------------------------



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
Reportes Técnicos de los activos de infraestructura que contemplen: <ul style="list-style-type: none">• Disponibilidad• Controles de Cambios• Requerimientos• Incidentes/Falla• Actividad Sospechosa• Estadísticas de uso de los servicios (conforme la definición en las mesas de trabajo)	5 días hábiles posteriores al cumplimiento del mes vencido	Día	1% por cada día hábil de atraso en la entrega de los reportes técnicos	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
Servicios de Borrado Seguro de Información: Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las actividades de borrado seguro ejecutadas por cada activo o grupo de activos de infraestructura procesados, donde se integre el o los certificados de borrado por cada medio de almacenamiento analizado y que incluya al menos: fecha, hora, datos del activo de infraestructura, dispositivos de almacenamiento borrado.	5 días hábiles posteriores a la solicitud generada por parte del Instituto	Día	1% por cada día hábil de atraso en la entrega de los reportes técnicos/ejecutivos	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
Servicio de Gestión de Dominios: Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de los dominios que se hayan renovados adquiridos.	5 días hábiles posteriores a la solicitud generada por parte del Instituto	Día	1% por cada día hábil de atraso en la entrega de los reportes técnicos/ejecutivos	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Servicio de Certificados Digitales SSL: Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de los certificados que se hayan renovado o adquiridos (incluyendo archivo electrónico compreso con la llave publica relacionado con los requerimientos)	1 día hábil posterior a la solicitud generada por parte del Instituto	Día	1% por cada día hábil de atraso en la entrega de los reportes técnicos/ejecutivos	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
Servicios de Ciberinteligencia: Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de amenazas y ataques potenciales a los que se encuentra expuesto el Instituto que incluya: Situación general del evento, hallazgos detectados, mecanismos de inteligencia accionable, táctica u operativa recomendados para prevención y/o contención	1 día hábil posterior a la solicitud generada por parte del Instituto	Día	1% por cada día hábil de atraso en la entrega de los reportes técnicos/ejecutivos	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Servicios de Sistema de Gestión de Seguridad de la Información: Plan de Trabajo de implementación y operación de los servicios conforme al alcance definido en las mesas de trabajo	10 días hábiles posteriores a la solicitud generada por parte del Instituto	Día	1% por cada día hábil de atraso en la entrega del plan de trabajo	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
Servicios de Sistema de Gestión de Seguridad de la Información: Reporte de actividades relacionadas con las solicitudes de Implementación, Evaluación y/o Mejora del Sistemas De Gestión de Seguridad de la Información (SGSI)	Conforme a la fecha estipulada en el plan de trabajo acordado entre el Instituto y el Proveedor	Día	1% por cada día hábil de atraso en la entrega de los reportes de actividades, por periodo, evento	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Servicios de Gestión del Cambio en Seguridad de la Información: Plan de Trabajo de implementación y operación de los servicios conforme al alcance definido en las mesas de trabajo	10 días hábiles posteriores a la solicitud generada por parte del Instituto	Día	1% por cada día hábil de atraso en la entrega del plan de trabajo	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
Servicios de Gestión del Cambio en Seguridad de la Información: Reporte de actividades relacionadas con las solicitudes de Implementación, Evaluación y/o Mejora de la Gestión del Cambio en Seguridad de la Información	Conforme a la fecha estipulada en el plan de trabajo acordado entre el Instituto y el Proveedor	Día	1% por cada día hábil de atraso en la entrega de los reportes de actividades, periodo, evento	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

Partida 2

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
---	------------------------------	---------------------------------	------------------	-------------------------------



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
<p><u>Servicio de Análisis de Vulnerabilidades Estático</u> Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las vulnerabilidades detectadas por cada pieza de software (código) escaneados indicando al menos: Activo(s) de infraestructura o aplicativo relacionado, fecha de escaneo, direccionamiento IP, vulnerabilidades detectadas (Alta, Media, Baja), recomendaciones para remediación de hallazgos y que incluya los archivos electrónicos fuente de las herramientas tecnológicas utilizadas para el proceso de</p>	7 días hábiles posteriores a la solicitud generada por parte del Instituto	Día	1% por cada día hábil de atraso en la entrega de los reportes técnicos/ejecutivos	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento



GOBIERNO DE
MÉXICO



DIRECCIÓN DE ADMINISTRACIÓN

Unidad de Adquisiciones

Coordinación de Adquisición de Bienes y Contratación de Servicios

Coordinación Técnica de Adquisición de Bienes de Inversión y Activos

División de Contratación de Activos y Logística

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
análisis				

177

Durango No. 291. 5to. piso. Col. Roma Norte. Alcaldía Cuauhtémoc. C. P. 06700. CDMX.

www.imss.aob.mx





Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
<u>Servicio de Análisis de Vulnerabilidades Dinámico</u> Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las vulnerabilidades detectadas por cada activo o grupo de activos de infraestructura escaneados indicando al menos: Activo(s) de infraestructura o aplicativo relacionado, fecha de escaneo, direccionamiento IP, vulnerabilidades detectadas (Alta, Media, Baja), recomendaciones para remediación de hallazgos y que incluya los archivos electrónicos fuente de las herramientas tecnológicas utilizadas para el	7 días hábiles posteriores a la solicitud generada por parte del Instituto	Día	1% por cada día hábil de atraso en la entrega de los reportes técnicos/ejecutivos	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento



GOBIERNO DE
MÉXICO



DIRECCIÓN DE ADMINISTRACIÓN

Unidad de Adquisiciones

Coordinación de Adquisición de Bienes y Contratación de Servicios

Coordinación Técnica de Adquisición de Bienes de Inversión y Activos

División de Contratación de Activos y Logística

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
proceso de análisis				

179

Durango No. 291. 5to. piso. Col. Roma Norte. Alcaldía Cuauhtémoc. C. P. 06700. CDMX.

www.imss.aob.mx





Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
<u>Servicios de Pruebas de Penetración:</u> Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las vulnerabilidades detectadas por cada activo o grupo de activos de infraestructura escaneados indicando al menos: Activo(s) de infraestructura o aplicativo relacionado, fecha de escaneo, direccionamiento IP, vulnerabilidades detectadas (Alta, Media, Baja), recomendaciones para remediación de hallazgos y que incluya los archivos electrónicos fuente de las herramientas tecnológicas utilizadas para el	10 días hábiles posteriores a la solicitud generada por parte del Instituto	Día	1% por cada día hábil de atraso en la entrega de los reportes técnicos/ejecutivos	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
proceso de análisis				
<u>Servicios de Análisis Forense:</u> Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de los hallazgos detectadas por cada activo o grupo de activos de infraestructura verificados	15 días hábiles posteriores a la solicitud generada por parte del Instituto	Día	1% por cada día hábil de atraso en la entrega de los reportes técnicos/ejecutivos	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

10.13. Servicios del Centro de Operaciones de Seguridad (SOC)

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
Reporte Técnico de los requerimientos generados a través de la Mesa de Servicios para los servicios de seguridad implementados	5 días hábiles posteriores al cumplimiento del mes vencido	Día	1% por cada día hábil de atraso en la entrega de los reportes técnicos	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
Reporte Técnico de los controles de cambios generados para los servicios de seguridad implementados	5 días hábiles posteriores al cumplimiento del mes vencido	Día	1% por cada día hábil de atraso en la entrega de los reportes técnicos	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Reporte Técnico de los incidentes presentados en los servicios de seguridad implementados	5 días hábiles posteriores al cumplimiento del mes vencido	Día	1% por cada día hábil de atraso en la entrega de los reportes técnicos	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Reporte Técnico de los eventos de actividad sospechosa presentados en los servicios de seguridad implementados	5 días hábiles posteriores al cumplimiento del mes vencido	Día	1% por cada día hábil de atraso en la entrega de los reportes técnicos	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Reporte de las estadísticas de uso y desempeño, así como de la analítica de información de los servicios de seguridad implementados, conforme las definiciones realizadas en las mesas de trabajo	5 días hábiles posteriores al cumplimiento del mes vencido	Día	1% por cada día hábil de atraso en la entrega de los reportes de estadísticas	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
Reporte de las evaluaciones operativas a los servicios de seguridad implementados	5 días hábiles posteriores al cumplimiento de cada trimestre vencido	Día	1% por cada día hábil de atraso en la entrega de los reportes de estadísticas	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Reporte que integre el calendario de actualizaciones de versionamiento en software de cada servicio implementados	5 días hábiles posteriores al cumplimiento de cada trimestre vencido	Día	1% por cada día hábil de atraso en la entrega de los reportes de estadísticas	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Creación de cuentas de acceso en las consolas de administración de los servicios de seguridad	5 días hábiles posteriores al término de la implementación de cualquier solución de seguridad o conforme a cada solicitud generada por el Instituto	Día	1% por cada día hábil de atraso en la entrega de las cuentas de acceso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
Creación de cuentas de acceso en la base de conocimientos de las soluciones de seguridad	5 días hábiles posteriores al término de la implementación de cualquier solución de seguridad o conforme a cada solicitud generada por el Instituto	Día	1% por cada día hábil de atraso en la entrega de las cuentas de acceso	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Actualización de la matriz de escalación	5 días hábiles posteriores a la incorporación o sustitución de nuevo personal del Centro de Operaciones de Seguridad	Día	1% por cada día hábil de atraso en la entrega de la matriz de escalación	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Reportes Técnicos de las ventanas de mantenimiento ejecutadas en las soluciones de seguridad	5 días hábiles posteriores a la ejecución de la ventana mantenimiento	Día	1% por cada día hábil de atraso en la entrega de los reportes técnicos	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Reporte con Estadísticas de uso y desempeño (información analítica) de las soluciones de seguridad	5 días hábiles posteriores a la solicitud generada por parte del Instituto	Día	1% por cada día hábil de atraso en la entrega del reporte	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
Reporte Técnico de las configuraciones de las soluciones de seguridad	5 días hábiles posteriores a la solicitud generada por parte del Instituto	Día	1% por cada día hábil de atraso en la entrega del reporte técnico	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Reporte Técnico de los incidentes presentados en las soluciones de seguridad	5 días hábiles posteriores a la solicitud generada por parte del Instituto	Día	1% por cada día hábil de atraso en la entrega del reporte técnico	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Reporte Técnico de los requerimientos registrados en la mesa de servicios	5 días hábiles posteriores a la solicitud generada por parte del Instituto	Día	1% por cada día hábil de atraso en la entrega del reporte técnico	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Reporte Técnico del inventario de los activos de infraestructura integrados en las soluciones de seguridad y su diagrama de interrelación conforme fueron registrados en la CMDB	5 días hábiles posteriores a la solicitud generada por parte del Instituto	Día	1% por cada día hábil de atraso en la entrega del reporte técnico	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

CONCEPTO (DESCRIPCIÓN DEL NIVEL DE SERVICIO)	NIVEL DE SERVICIO	UNIDAD DE MEDIDA	DEDUCTIVA	FÓRMULA DE CÁLCULO
Diagramas de Arquitectura de las soluciones de seguridad	2 días hábiles posteriores a la solicitud generada por parte del Instituto	Día	1% por cada día hábil de atraso en la entrega del reporte técnico	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento
Tablero de Estadísticas de Servicios de Seguridad (Portal Único)	10 días hábiles posteriores al término de la habilitación de los componentes en los Centro de Datos o donde lo indique el Instituto, conforme cada solución integrada y posterior a la integración de las mesas de trabajo	Día	1% por cada día hábil de atraso en la entrega de los reportes de actividades, por periodo, por evento	Valor unitario de la facturación mensual del servicio relacionado con el incumplimiento

Cualquier cambio ejecutado por el SOC, mismo que no se encuentre autorizado por el Instituto, derive o no en alguna falla de los servicios de seguridad, será catalogado como un incidente de seguridad, mismo que será clasificado con base en las afectaciones o riesgos que pudieron generar.

11. Condiciones de Pago

Como se establece en el presente documento, el administrador de contrato será el servidor público responsable de supervisar que se cumplan en tiempo y forma los compromisos contenidos en el contrato que para tal efecto se celebre.

Los pagos se realizarán previa validación y aceptación de los servicios por parte del Administrador del Contrato, es decir, el Titular de la División de Seguridad Informática Física, que reciba cada uno de los servicios y que será responsable de realizar los trámites de pago en estricto apego al procedimiento administrativo vigente en el instituto.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Para proceder a la liberación de pago, el Titular de la División de Seguridad Informática Física o el Servidor Público que para tal efecto haya designado el Titular de la Coordinación de Telecomunicaciones y Seguridad de la Información, será responsable de la supervisión y administración de todas las obligaciones a cargo del proveedor.

Así como de la ejecución, validación, técnica y administrativamente de todos y cada uno de los documentos que acreditan que los servicios proporcionados por el proveedor se cumplieron en tiempo, forma y cantidad con las características, especificaciones y condiciones contractualmente pactadas para el proyecto, procederá de conformidad con lo establecido en el artículo 51 de la LAASSP, la forma de pago al proveedor será la estipulada en los contratos y quedará sujeta a las condiciones que establezcan las mismas; sin embargo, no podrá exceder de veinte días naturales contados a partir de la entrega de la factura respectiva, previa entrega de certificado de licencia o de la prestación de los servicios en los términos del contrato.

El proveedor deberá entregar en la División de Trámite de Erogaciones, situada en la calle de Gobernador Tiburcio Montiel No. 15, PB, Col. San Miguel Chapultepec, Código Postal 11850, Delegación Miguel Hidalgo, México, D.F., en días y horas hábiles, los siguientes documentos:

- Original y copia de la factura que expida el Proveedor, a nombre del Instituto Mexicano del Seguro Social, con dirección en Av. Paseo de la Reforma N° 476, Col. Juárez, Delegación Cuauhtémoc, C.P. 06600, México, D.F., y R.F.C. IMS-421231-I45; que reúna los requisitos fiscales, en la que se indiquen los servicios proporcionados y el número de contrato que ampara dichos servicios,
- Original y Copia de la documentación que avale la entrega de los servicios a satisfacción de el instituto (Acta Entrega-Recepción de los Servicios).
- Carta firmada por el representante legal, en la cual haga del conocimiento de el instituto la cuenta bancaria a la que se efectuará la transferencia electrónica bancaria correspondiente.
- Nota de crédito (en caso de que aplique) a favor del Instituto Mexicano del Seguro Social por el importe de la sanción en caso de entrega extemporánea de los servicios contratados.
- Presentará Orden de Ingreso (Nota de Crédito) (en caso de que aplique para Soporte Técnico dentro de los primeros 10 días hábiles después de la fecha del Acta Entrega-Recepción de los Servicios del trimestre firmada, a favor del Instituto Mexicano del Seguro Social por el importe de la sanción en caso de entrega extemporánea de los servicios contratados, en caso de no entregar la Orden de ingreso (Nota de Crédito) correspondiente al plazo citado en este punto, se aplicara la ejecución de garantía.

En caso de que el proveedor presente sus facturas con errores o deficiencias, estos se le harán saber por parte de el instituto dentro del término estipulado para ello, y el plazo de pago se ajustará, debiendo presentar nuevamente toda la documentación mencionada anteriormente (en original y/o copia, según corresponda).

El Pago se realizará en pesos mexicanos, en pagos pagos progresivos a mes vencido conforme a las entregas programadas.

12. Entregables

El proveedor deberá entregar al Titular de la División de Seguridad Informática Física dependiente de la Coordinación de Telecomunicaciones y Seguridad de la Información los siguientes:

12.1. Entregables Generales



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Partida 1

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
Servicios de Habilitación, Operación y Transición	Plan de Trabajo Detallado de los servicios del proyecto	Única Vez	15 días naturales posteriores a la emisión del fallo
	Documento Compromiso de suscripción del acuerdo de niveles operacional (<i>Operational Level Agreement, OLA</i>)	Única Vez	15 días naturales posteriores a la emisión del fallo
	Matriz de Escalación	Única Vez	15 días naturales posteriores a la emisión del fallo
	Escrito por parte del proveedor, firmado por el representante legal, donde declare sus habilidades, competencias y capacidades para soportar la prestación de los servicios	Única Vez	15 días naturales posteriores a la emisión del fallo
Servicios de Seguridad – Continuidad Operativa	Documento con el diseño de Alto Nivel de las Soluciones de Seguridad a implementar en los centros de datos o donde lo indique el Instituto	Única Vez	5 días hábiles posteriores a la integración de las mesas de trabajo por cada servicio que se pretenda habilitar
	Documento con el diseño de Bajo Nivel de las Soluciones de Seguridad a implementar en los centros de datos o donde lo indique el Instituto	Única Vez	10 días hábiles posteriores a la integración de las mesas de trabajo por cada servicio que se pretenda habilitar



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
Servicios de Seguridad – Verificación/Calidad	Memorias Técnicas Iniciales de las Soluciones de Seguridad Implementadas	Única Vez	10 días hábiles posteriores al término de la habilitación de todos los componentes en los Centro de Datos o donde lo indique el Instituto, conforme cada solución integrada y posterior a la integración de las mesas de trabajo
	Memorias Técnicas Actualizadas de las Servicios de Seguridad	Única Vez	20 días hábiles previo al término del contrato para aquellos servicios que se encuentren habilitados
Servicios de Seguridad – Verificación/Calidad	Documento con el diseño de Alto Nivel de los servicios de Seguridad a implementar en los centros de datos o donde lo indique el Instituto, que requieran integrar activos de infraestructura para su habilitación	Única Vez	5 días hábiles posteriores a la integración de las mesas de trabajo por cada servicio que se pretenda habilitar
	Documento con el diseño de Bajo Nivel de las Soluciones de Seguridad a implementar en los centros de datos o donde lo indique el Instituto	Única Vez	10 días hábiles posteriores a la integración de las mesas de trabajo por cada servicio que se pretenda habilitar



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
	Memorias Técnicas Iniciales de las Soluciones de Seguridad Implementadas, que requieran integrar activos de infraestructura para su habilitación	Única Vez	10 días hábiles posteriores al término de la habilitación de todos los componentes en los Centro de Datos o donde lo indique el Instituto, conforme cada solución integrada y posterior a la integración de las mesas de trabajo
	Memorias Técnicas Actualizadas de las Servicios de Seguridad, que requieran integrar activos de infraestructura para su habilitación	Única Vez	20 días hábiles previo al término del contrato para aquellos servicios que se encuentren habilitados
Servicios de Borrado Seguro de Información	Procedimientos de Operación del servicio	Única Vez	10 días hábiles posteriores a la integración de las mesas de trabajo
Servicio de Gestión de Dominios	Procedimientos de Operación del servicio	Única Vez	10 días hábiles posteriores a la integración de las mesas de trabajo
Servicio de Certificados Digitales SSL	Procedimientos de Operación del servicio	Única Vez	10 días hábiles posteriores a la integración de las mesas de trabajo
Servicios de Sistema de Gestión de Seguridad de la Información (SGSI)	Metodología para la continuidad de los servicios	Única Vez	10 días hábiles posteriores a la integración de las mesas de trabajo



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
Servicios de Gestión del Cambio en Seguridad de la Información	Metodología para la implementación de los servicios	Única Vez	10 días hábiles posteriores a la integración de las mesas de trabajo
Servicios del Centro de Operaciones de Seguridad (SOC)	Procesos de operación implementados: <ul style="list-style-type: none"> • Requerimientos • Cambios • Configuraciones • Incidentes • Problemas • Monitoreo 	Única Vez	15 días naturales posteriores a la emisión del fallo
	Matriz de Escalación Técnica y Organizacional	Única Vez	15 días naturales posteriores a la emisión del fallo
	Procedimiento de operación de la Mesa de Servicios: <ul style="list-style-type: none"> • Requerimientos • Cambios • Configuraciones • Incidentes • Problemas • Monitoreo 	Única Vez	15 días naturales posteriores a la emisión del fallo
	Expedientes Curriculares del personal del SOC	Única Vez	15 días naturales posteriores a la emisión del fallo
Tablero de Estadísticas de Servicios de Seguridad (Portal Único)	Creación de cuentas de acceso en portal único de las soluciones de seguridad	Única Vez	10 días hábiles posteriores al término de la habilitación de los componentes en los Centro de Datos o donde lo indique el Instituto, conforme cada solución integrada y posterior a la integración de las mesas de trabajo



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Partida 2.

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
Servicios de Habilitación, Operación y Transición	Plan de Trabajo Detallado de los servicios del proyecto	Única Vez	15 días naturales posteriores a la emisión del fallo
	Documento Compromiso de suscripción del acuerdo de niveles operacional (<i>Operational Level Agreement, OLA</i>)	Única Vez	15 días naturales posteriores a la emisión del fallo
	Matriz de Escalación	Única Vez	15 días naturales posteriores a la emisión del fallo
	Escrito por parte del proveedor, firmado por el representante legal, donde declare sus habilidades, competencias y capacidades para soportar la prestación de los servicios	Única Vez	15 días naturales posteriores a la emisión del fallo
Servicios de Análisis de Vulnerabilidades Dinámico	Procedimientos de Operación del servicio	Única Vez	10 días hábiles posteriores a la integración de las mesas de trabajo
Servicios de Pruebas de Penetración	Procedimientos de Operación del servicio	Única Vez	10 días hábiles posteriores a la integración de las mesas de trabajo
Servicios de Análisis Forense	Procedimientos de Operación del servicio	Única Vez	10 días hábiles posteriores a la integración de las mesas de trabajo



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Servicios de Análisis de Vulnerabilidades Estático	Procedimientos de Operación del servicio	Única Vez	10 días hábiles posteriores a la integración de las mesas de trabajo
--	--	-----------	--

12.2. Entregables bajo demanda

El proveedor, de manera enunciativa más no limitativa, deberá generar entregables para los servicios de seguridad, que incluya al menos los siguientes conceptos:

Partida 1

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
Servicios de Borrado Seguro de Información	Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las actividades de borrado seguro ejecutadas por cada activo o grupo de activos de infraestructura procesados, donde se integre el o los certificados de borrado por cada medio de almacenamiento analizado y que incluya al menos: fecha, hora, datos del activo de infraestructura, dispositivos de almacenamiento borrado.	Evento	5 días hábiles posteriores a la solicitud generada por parte del Instituto
Servicio de Gestión de Dominios	Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de los dominios que se hayan renovados adquiridos.	Evento	5 días hábiles posteriores a la solicitud generada por parte del Instituto



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
Servicio de Certificados Digitales SSL	Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de los certificados que se hayan renovado o adquiridos (incluyendo archivo electrónico compreso con la llave pública relacionada con los requerimientos)	Evento	1 día hábil posteriores a la solicitud generada por parte del Instituto
Servicios de Sistema de Gestión de Seguridad de la Información	Plan de Trabajo de continuidad y operación de los servicios conforme al alcance definido en las mesas de trabajo	Evento	10 días hábiles posteriores a la solicitud generada por parte del Instituto
Servicios de Gestión del Cambio en Seguridad de la Información	Plan de Trabajo de continuidad y operación de los servicios conforme al alcance definido en las mesas de trabajo	Evento	10 días hábiles posteriores a la solicitud generada por parte del Instituto
Servicios del Centro de Operaciones de Seguridad (SOC)	Creación de cuentas de acceso en las consolas de administración de las soluciones de seguridad	Evento	5 días hábiles posteriores al término de la implementación de cualquier solución de seguridad o conforme a cada solicitud generada por el Instituto
	Creación de cuentas de acceso en la base de conocimientos de las soluciones de seguridad	Evento	5 días hábiles posteriores al término de la implementación de cualquier solución de seguridad o conforme cada solicitud generada por el Instituto
	Actualización de la matriz de escalación	Evento	5 días hábiles posteriores a la incorporación o sustitución de nuevo personal del Centro de Operaciones de Seguridad y Red



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
	Reportes Técnicos de las ventanas de mantenimiento ejecutadas en las soluciones de seguridad y red	Evento	5 días hábiles posteriores a la ejecución de la ventana mantenimiento
	Reporte con Estadísticas de uso y desempeño (información analítica) de las soluciones de seguridad y red	Evento	5 días hábiles posteriores a la solicitud generada por parte del Instituto
	Reporte Técnico de las configuraciones de las soluciones de seguridad y red	Evento	5 días hábiles posterior a la solicitud generada por parte del Instituto
	Reporte Técnico de los incidentes presentados en las soluciones de seguridad y red	Evento	5 días hábiles posteriores a la solicitud generada por parte del Instituto
	Reporte Técnico de los requerimientos registrados en la mesa de servicios	Evento	5 días hábiles posteriores a la solicitud generada por parte del Instituto
	Reporte Técnico del inventario de los activos de infraestructura integrados en las soluciones de seguridad y red, así como su diagrama de interrelación conforme fueron registrados en la CMDB	Evento	5 días hábiles posteriores a la solicitud generada por parte del Instituto
	Diagramas de Arquitectura de las soluciones de seguridad y red	Evento	2 días hábiles posteriores a la solicitud generada por parte del Instituto

Partida 2

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
----------	------------	--------------	---------



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
Servicios de Análisis de Vulnerabilidades Dinámico	Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las vulnerabilidades detectadas por cada activo o grupo de activos de infraestructura escaneados indicando al menos: Activo(s) de infraestructura o aplicativo relacionado, fecha de escaneo, direccionamiento IP, vulnerabilidades detectadas (Alta, Media, Baja), recomendaciones para remediación de hallazgos y que incluya los archivos electrónicos fuente de las herramientas tecnológicas utilizadas para el proceso de análisis	Evento	7 días hábiles posteriores a la solicitud generada por parte del Instituto



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
Servicios de Prueba de Penetración	Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las vulnerabilidades detectadas por cada activo o grupo de activos de infraestructura escaneados indicando al menos: Activo(s) de infraestructura o aplicativo relacionado, fecha de escaneo, direccionamiento IP, vulnerabilidades detectadas (Alta, Media, Baja), recomendaciones para remediación de hallazgos y que incluya los archivos electrónicos fuente de las herramientas tecnológicas utilizadas para el proceso de análisis	Evento	10 días hábiles posteriores a la solicitud generada por parte del Instituto
Servicios de Análisis Forense	Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de los hallazgos detectadas por cada activo o grupo de activos de infraestructura verificados	Evento	15 días hábiles posteriores a la solicitud generada por parte del Instituto



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
Servicios de Análisis de Vulnerabilidades Estático	Reporte Técnico y Ejecutivo en formato electrónico (MS Word, PDF) con el detalle de las vulnerabilidades detectadas por cada pieza de software (codigo) analizados indicando al menos: aplicativo relacionado, fecha de análisis, código fuente analizado, vulnerabilidades detectadas (Alta, Media, Baja), recomendaciones para remediación de hallazgos y que incluya los archivos electrónicos fuente de las herramientas tecnológicas utilizadas para el proceso de análisis	Evento	10 días hábiles posteriores a la solicitud generada por parte del Instituto

12.3. Entregables Periódicos

El proveedor, de manera enunciativa más no limitativa, deberá generar entregables para los servicios de seguridad, que incluya al menos los siguientes conceptos:

Partida 1

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
----------	------------	--------------	---------



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
Servicios de Seguridad – Continuidad Operativa	Reportes Técnicos de los activos de infraestructura que contemplen: <ul style="list-style-type: none">• Disponibilidad• Controles de Cambios• Requerimientos• Incidentes/Fallas• Actividad Sospechosa• Estadísticas de uso de los servicios (conforme la definición en las mesas de trabajo)	Mensual	5 días hábiles posteriores al cumplimiento del mes vencido
Servicios de Seguridad – Verificación/Calidad	Reportes Técnicos de los activos de infraestructura que contemplen: <ul style="list-style-type: none">• Disponibilidad• Controles de Cambios• Requerimientos• Incidentes/Fallas• Actividad Sospechosa• Estadísticas de uso de los servicios (conforme la definición en las mesas de trabajo)	Mensual	5 días hábiles posteriores al cumplimiento del mes vencido
Servicios del Centro de Operaciones de Seguridad (SOC)	Reporte Técnico de los requerimientos generados a través de la Mesa de Servicios para los servicios de seguridad implementados	Mensual	5 días hábiles posteriores al cumplimiento del mes vencido
	Reporte Técnico de los controles de cambios generados para los servicios de seguridad implementados	Mensual	5 días hábiles posteriores al cumplimiento del mes vencido
	Reporte Técnico de los incidentes presentados en los servicios de seguridad implementados	Mensual	5 días hábiles posteriores al cumplimiento del mes vencido
	Reporte Técnico de los eventos de actividad sospechosa presentados en los servicios de seguridad implementados	Mensual	5 días hábiles posteriores al cumplimiento del mes vencido



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
	Reporte de las estadísticas de uso y desempeño, así como de la analítica de información de los servicios de seguridad implementados, conforme las definiciones realizadas en las mesas de trabajo	Mensual	5 días hábiles posteriores al cumplimiento del mes vencido
	Reporte de las evaluaciones operativas a los servicios de seguridad implementados	Trimestral	5 días hábiles posteriores al cumplimiento de cada trimestre calendario
	Reporte que integre el calendario de actualizaciones de versionamiento en software de cada servicio implementados	Trimestral	5 días hábiles posteriores al cumplimiento de cada trimestre calendario

Partida 2

SERVICIO	ENTREGABLE	PERIODICIDAD	ENTREGA
Servicios de Análisis de Vulnerabilidades Dinámico	Reporte Técnico de los requerimientos generados a través de la Mesa de Servicios para los servicios de seguridad implementados	Mensual	5 días hábiles posteriores al cumplimiento del mes vencido
Servicios de Análisis de Vulnerabilidades Estático	Reporte Técnico de los controles de cambios generados para los servicios de seguridad implementados	Mensual	5 días hábiles posteriores al cumplimiento del mes vencido
Servicios de Pruebas de Penetración	Reporte de las evaluaciones operativas a los servicios de seguridad implementados	Trimestral	5 días hábiles posteriores al cumplimiento de cada trimestre calendario
Servicios de Análisis Forense	Reporte que integre el calendario de actualizaciones de versionamiento en software de cada servicio implementados	Trimestral	5 días hábiles posteriores al cumplimiento de cada trimestre calendario



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Los entregables requeridos durante la vigencia del contrato, deberán ser entregados en formato electrónico (MS Word, MS Excel, PDF) conforme los periodos estipulados por el Instituto.

De igual manera, el proveedor deberá establecer un repositorio digital, que, de manera alterna, servirá para alojar los entregables antes señalados, mismos que estarán disponibles para su consulta durante la vigencia del contrato, teniendo en cuenta que el Instituto definirá en las mesas de trabajo los permisos de acceso correspondientes para el administrador del contrato, cuerpo de gobierno que se conforme para este propósito u otros funcionarios que sean designados por el primero mencionado.

13. Condiciones de aceptación de los servicios

1. Se deberán formalizar los entregables descritos en el numeral anterior a efecto de dar por recibido los servicios requeridos.
2. Todos los documentos deben ser entregados en papel membretado de la empresa de manera impresa y en electrónico.
3. Se entregará a la División de Seguridad Informática Física perteneciente a la Coordinación de Telecomunicaciones y Seguridad de la Información.

14. Lugar y horario para la entrega

- La entrega se realizará en las instalaciones de el Instituto ubicadas en la calle de Avenida Paseo de la Reforma 476, Anexo de Telecomunicaciones Planta Alta, Colonia Juárez, Delegación Cuauhtémoc, Ciudad de México, C.P. 06600.
- El horario para la entrega será de las 9:00 horas a las 17:00 horas
- En caso de contingencia podrá solicitarse la entrega de las cartas requeridas en el presente documento en cualquiera de los inmuebles que formen parte de las Oficinas Centrales de el instituto, ubicadas en la Colonia Juárez, Delegación Cuauhtémoc, C.P. 06600 en la Ciudad de México.

15. Convenio de Confidencialidad y Resguardo de la Información

El “Licitante” deberá suscribir el Convenio de Confidencialidad y Resguardo de Información Correspondiente con la persona designada como Administradora de Contrato. En complemento, el “Licitante” deberá considerar al menos los siguientes mecanismos de control de acceso a la información del IMSS:

- a. Se deberán establecer controles de acceso y privilegios restringidos al personal del “Licitante”, a fin de acotar su acceso para tareas y funciones específicas cuando requieran estar dentro de las instalaciones del IMSS.
- b. El “Licitante” deberá implantar y aceptar en todo momento el uso de controles que permitan “Pistas de Auditoría” para los accesos/copias de datos, incluyendo bitácoras individuales de usuario.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- c. La seguridad lógica deberá estar protegida mediante el uso de "Firewalls", mecanismos de encriptación y seguridad física entre las redes del "Licitante" y las del IMSS.
- d. El "Licitante" deberá contar con sistemas que contengan una administración estricta de registros y políticas de retención de la información del IMSS.
- e. Los empleados del "Licitante" con acceso a la información sensible del IMSS, deberán firmar acuerdos de confidencialidad con este.
- f. El almacenamiento de datos y acceso, incluyendo acceso remoto, serán en los sitios específicos señalados por el "Licitante" de los servicios de SASI 2022- 2024 observando los requisitos de seguridad y resguardo de la información.
- g. El uso de *hardware* que podría ser utilizado para copiar datos y extraer información, como son dispositivos removibles, quemado de CD y dispositivos de memoria "Flash-USB", entre otros, por parte del personal del "Licitante" serán restringidos y deberán observar las políticas de seguridad del IMSS al respecto.
- h. El "Licitante" deberá permitir el acceso a información relacionada con el servicio prestado al IMSS para la realización de auditorías.
- i. El "Licitante" no deberá hacer uso indebido de la documentación, información, ni activos de TIC a los que tengan acceso o que se generen con motivo de la prestación del servicio.

16. Propiedad Intelectual

El proveedor se obliga durante la garantía de las licencias a liberar a el Instituto de toda responsabilidad de carácter civil, mercantil, penal o administrativa que, en su caso, se ocasione con motivo de la infracción de derechos de autor, patentes, marcas u otros derechos de propiedad industrial o intelectual a nivel Nacional o Internacional.

17. Método de evaluación de propuestas

Se evaluará mediante el procedimiento de puntos y porcentajes, conforme a las características que presenten los proveedores en cuanto a funcionalidades requeridas en el Anexo Técnico, de acuerdo con la ponderación establecida en la matriz de evaluación correspondiente.

18. Funcionarios públicos de la DIDT participantes en el proceso de contratación

- a) C. Florencio Fernando González Velázquez, Titular de la Coordinación de Telecomunicaciones y Seguridad de la Información.
- b) C. Abraham Gutiérrez Castillo, Titular de la División de Seguridad Informática Física.
- c) C. Cynthia Osmara Verdin Villegas, Jefe Área Nivel Central.

19. Vigencia del Contrato

La vigencia del contrato será a partir del día hábil siguiente a la notificación del fallo y hasta el 30 de septiembre de 2024.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

20. Plazo del servicio

La prestación de los servicios iniciará a partir del día hábil siguiente a la notificación del fallo y hasta el 30 de septiembre de 2024.

21. Administrador del Contrato

Conforme a las Políticas, Bases y Lineamientos en Materia de Adquisiciones, Arrendamientos y Servicios del Instituto, el Administrador del Contrato, será el responsable de supervisar que se cumplan en tiempo y forma los compromisos contenidos en el contrato que para tal efecto se celebre, por lo que:

- a) **Administrador del Contrato y Responsable Técnico;** Titular de la División de Seguridad Informática Física.
- b) **Supervisor del Contrato;** Titular de la Coordinación de Telecomunicaciones y Seguridad de la Información.

Los servicios a cargo del proveedor estarán bajo la administración y supervisión del responsable designado que para tal efecto.

22. Mecanismos de control para la administración del contrato

El Administrador del Contrato en conjunto con el proveedor deberá generar el acta de entrega-recepción conforme a lo establecido en el Anexo Técnico.

23. Mecanismos requeridos al proveedor para responder por defectos o vicios ocultos de los bienes o de la calidad de los servicios

No aplica

24. Otorgamiento de anticipo

No aplica



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Anexo 3.- Escrito de acreditación legal y personalidad jurídica del licitante

Ciudad de México, a _____ de _____ de 20____.

_____ (Nombre)_____, manifiesto **bajo protesta de decir verdad**, que los datos aquí asentados son ciertos y han sido verificados, así como que cuento con facultades suficientes para **comprometerme por mí o por mi representada y suscribir las propuestas** en la presente Licitación Pública Nacional Electrónica Núm. _____, a nombre y representación de.__(Persona Física o Moral) ____.

Datos Personas Morales y Físicas.

Registro Federal de Contribuyentes.		
Domicilio.		
Calle y Número.		
Colonia.	Demarcación Territorial o Municipio.	
Código Postal.	Entidad Federativa.	
Teléfono Fijo.	Teléfono Móvil.	
Correo Electrónico.		
Número de la Escritura Pública en la que consta su Acta Constitutiva.		Fecha.
Nombre, número y circunscripción del Notario Público (ante el cual se dio fe de la misma).		
Fecha y Datos de su Inscripción en el Registro Público de Comercio.		
Descripción del Objeto Social.		
Relación de Accionistas.		
Apellido Paterno	Apellido Materno	Nombre(s)
Reformas al Acta Constitutiva que incidan con el objeto del procedimiento (Señalar Nombre, Número y Circunscripción del Notario o Fedatario Público que las protocolizó, así como la Fecha y los datos de su Inscripción en el Registro Público de la Propiedad).		

Apoderado Legal o Representante. (Nombre y Domicilio)
Documento para Acreditar Personalidad y Facultades. (Escritura Pública y Modificaciones, Fecha, nombre y circunscripción del Notario Público)

Asimismo, manifiesto que los cambios o modificaciones que se realicen en cualquier momento a los datos o documentos contenidos en el presente documento y durante la vigencia del contrato que, en su caso, sea suscrito con el Instituto, deberán ser comunicados a éste, dentro de los cinco días hábiles siguientes a la fecha en que se generen.

Protesto lo necesario

(Nombre y Firma del Apoderado o Representante Legal del Licitante)



GOBIERNO DE
MÉXICO



DIRECCIÓN DE ADMINISTRACIÓN

Unidad de Adquisiciones

Coordinación de Adquisición de Bienes y Contratación de Servicios

Coordinación Técnica de Adquisición de Bienes de Inversión y Activos

División de Contratación de Activos y Logística

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

205

Durango No. 291. 5to. piso. Col. Roma Norte. Alcaldía Cuauhtémoc. C. P. 06700. CDMX.

www.imss.aob.mx





Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Anexo 4.- Escrito de nacionalidad mexicana

Ciudad de México, a _____ de _____ de 20____

Instituto Mexicano del Seguro Social

Dirección de Administración

Unidad de Adquisiciones

Coordinación de Adquisición de Bienes y Contratación de Servicios

Coordinación Técnica de Adquisición de Bienes de Inversión y Activos

División de Contratación de Activos y Logística

Presente

Me refiero al procedimiento _____ (*Licitación Pública Nacional Electrónica*) _____ No._____ (*Número de Procedimiento*) ____ en el que mi representada, la empresa _____ (*nombre o razón social del licitante*) _____ participa a través de la presente propuesta.

Sobre el particular, y en los términos de lo previsto en numeral 4.2, Documentación distinta a la proposición (legal-administrativa), de las bases de la convocatoria de la Licitación Pública Nacional Electrónica citada en el párrafo anterior, manifiesto **bajo protesta de decir verdad** lo siguiente:

- Conforme al artículo 35 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, que mi representada es de nacionalidad mexicana, para participar en el procedimiento de Licitación Pública Nacional Electrónica.
- Conforme al artículo 39, fracción VIII del Reglamento de la citada Ley que el origen de los servicios que oferto, serán de origen nacional.

Protesto lo necesario

(Nombre y Firma del Apoderado o Representante Legal del Licitante)



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Anexo 5.- Escrito de cumplimiento de normas

Ciudad de México, a _____ de _____ de 20____

Instituto Mexicano del Seguro Social
Dirección de Administración
Unidad de Adquisiciones
Coordinación de Adquisición de Bienes y Contratación de Servicios
Coordinación Técnica de Adquisición de Bienes de Inversión y Activos
División de Contratación de Activos y Logística
Presente

Me refiero al procedimiento _____ (*Licitación Pública Nacional Electrónica*) _____.
No.____ (Número de Procedimiento) ____ en el que mi representada, la empresa
_____ (nombre o razón social del licitante) _____ participa a través de la
presente propuesta.

Sobre el particular, y en los términos de lo previsto en numeral 4.2, Documentación distinta a la proposición (legal-administrativa), de las bases de la convocatoria de la Licitación Pública Nacional Electrónica citada en el párrafo anterior, manifiesto lo siguiente:

Que en caso de resultar adjudicado, los servicios propuestos cumplirán con las normas solicitadas en la presente convocatoria, de acuerdo con el Anexo [***] que se adjunta para tal efecto.

Por esto lo necesario

(Nombre y Firma del Poderoso o Representante Legal del Licitante)

Anexo [*].- El licitante debe indicar el nombre y/o numero de anexo en que se encuentra dentro de su propuesta técnica.**



GOBIERNO DE
MÉXICO



DIRECCIÓN DE ADMINISTRACIÓN

Unidad de Adquisiciones

Coordinación de Adquisición de Bienes y Contratación de Servicios

Coordinación Técnica de Adquisición de Bienes de Inversión y Activos

División de Contratación de Activos y Logística

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Anexo 6.- Escrito de no encontrarse en los supuestos de los artículos 50 y 60 de la LAASSP

Ciudad de México, a ____ de _____ de 20____.

Instituto Mexicano del Seguro Social
Dirección de Administración
Unidad de Adquisiciones
Coordinación de Adquisición de Bienes y Contratación de Servicios
Coordinación Técnica de Adquisición de Bienes de Inversión y Activos
División de Contratación de Activos y Logística
Presente

____Nombre _____, en mi carácter de representante legal de la (Persona Física o Moral)
manifiesto **bajo protesta de decir verdad** lo siguiente:

Que la empresa que represento, el suscrito, los socios o accionistas y las personas que forman parte de la sociedad, no se encuentran en alguno de los supuestos señalados en los artículos 50 y 60 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, lo que manifiesto para los efectos correspondientes con relación a la Licitación Pública Nacional Electrónica número. _____.

Protesto lo necesario

(Nombre y Firma del Apoderado o Representante Legal del Licitante)

Nota. En caso de que el licitante sea persona física, adecuar el formato



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Anexo 7.- Declaración de integridad

Ciudad de México, a _____ de _____ de 20____

Instituto Mexicano del Seguro Social
Dirección de Administración
Unidad de Adquisiciones
Coordinación de Adquisición de Bienes y Contratación de Servicios
Coordinación Técnica de Adquisición de Bienes de Inversión y Activos
División de Contratación de Activos y Logística
Presente

____Nombre _____, en mi carácter de representante legal de la (Persona Física o Moral) _____, y en términos de la convocatoria de la Licitación Pública Nacional Electrónica número _____, manifiesto **bajo protesta de decir verdad** lo siguiente:

Que mi representada se abstendrá por si misma o a través de interpósita persona, de adoptar conductas para que los servidores públicos del Instituto, induzcan o alteren las evaluaciones de las proposiciones, el resultado del procedimiento, u otros aspectos que le otorguen condiciones más ventajosas con relación a los demás participantes.

(EN CASO DE SER PERSONA FÍSICA, DEBERÁ SUSTITUIR EL PÁRRAFO ANTERIOR POR LO SIGUIENTE: "Me permito manifestar BAJO PROTESTA DE DECIR VERDAD que me abstendré por sí mismo o a través de interpósita persona, de adoptar conductas que induzcan o alteren las evaluaciones de las proposiciones, el resultado del procedimiento, u otros aspectos que le otorguen condiciones más ventajosas con relación a los demás participantes; asimismo me abstendré por sí mismo o por interpósito persona, de llevar a cabo cualquier acto que implique trasgresión a las disposiciones de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y su Reglamento; así como a lo dispuesto en general por la Ley Federal de Competencia Económica.") **EN CASO DE NO SER PERSONA FÍSICA PODRÁ ELIMINAR ESTE PÁRRAFO.**

Que en caso de resultar adjudicado, me obligo a liberar al Instituto de toda responsabilidad de carácter civil, mercantil, penal o administrativa que, en su caso, se ocasione con motivo de la infracción de derechos de autor, patentes, marcas u otros derechos de propiedad industrial o intelectual a nivel nacional o internacional.

Protesto lo necesario

(Nombre y Firma del Apoderado o Representante Legal del Licitante)



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Anexo 8.- Escrito de estratificación de MIPYME

Ciudad de México, a _____ de _____ de 20____

Instituto Mexicano del Seguro Social

Dirección de Administración

Unidad de Adquisiciones

Coordinación de Adquisición de Bienes y Contratación de Servicios

Coordinación Técnica de Adquisición de Bienes de Inversión y Activos

División de Contratación de Activos y Logística

Presente

Me refiero al procedimiento de _____ (3) _____ Núm. _____ (4) _____ en el que mí representada, la empresa_____ (5) _____, participa a través de la presente propuesta.

Al respecto y de conformidad con lo dispuesto por el artículo 34 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, manifiesto **bajo protesta de decir verdad** que mi representada está constituida conforme a las leyes mexicanas, con Registro Federal de Contribuyentes _____ (6) _____, y asimismo que considerando los criterios (sector, número total de trabajadores y ventas anuales) establecidos en el Acuerdo por el que se establece la estratificación de las micro, pequeñas y medianas empresas, publicado en el Diario Oficial de la Federación el 30 de junio de 2009, mi representada tiene un Tope Máximo Combinado de _____ (7) _____, con base en lo cual se estatifica como una empresa _____ (8) _____.

De igual forma, declaro que la presente manifestación la hago teniendo pleno conocimiento de que la omisión, simulación o presentación de información falsa, son infracciones previstas por los artículos 69 y 81, ambos de la Ley General de Responsabilidades Administrativas, y demás disposiciones aplicables.

Protesto lo necesario

(Nombre y Firma del Apoderado o Representante Legal del Licitante)



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Anexo 8 Bis.- Instructivo de llenado para el escrito de estratificación de micro, pequeña o mediana empresa (MIPYMES)

Descripción.

Formato para que los licitantes manifiesten, bajo protesta de decir verdad, la estratificación que les corresponde como MIPYMES, de conformidad con el Acuerdo de Estratificación de las MIPYMES, publicado en el Diario Oficial de la Federación el 30 de junio de 2009.

Instructivo de llenado.

Llenar los campos conforme aplique tomando en cuenta los rangos previstos en el Acuerdo antes mencionado.

1. Señalar la fecha de suscripción del documento.
2. Anotar el nombre de la convocante.
3. Precisar el procedimiento de contratación de que se trate (Licitación Pública Nacional Electrónica).
4. Indicar el número de procedimiento de contratación asignado por CompraNet.
5. Anotar el nombre, razón social o denominación del licitante.
6. Indicar el Registro Federal de Contribuyentes del licitante.
7. Señalar el número que resulte de la aplicación de la expresión. Tope Máximo Combinado = (Trabajadores) x 10% + (Ventas anuales en millones de pesos) x 90%.

Para tales efectos puede utilizar la calculadora MIPYMES disponible en la página <http://www.comprasdegobierNúm.gob.mx/calculadora>

Para el concepto “Trabajadores”, utilizar el total de los trabajadores con los que cuenta la empresa a la fecha de la emisión de la manifestación.

Para el concepto “ventas anuales”, utilizar los datos conforme al reporte de su ejercicio fiscal correspondiente a la última declaración anual de impuestos federales, expresados en millones de pesos.

8. Señalar el tamaño de la empresa (Micro, Pequeña o Mediana), conforme al resultado de la operación señalada en el numeral anterior.
9. Anotar el nombre y firma del apoderado o representante legal del licitante.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Anexo 9- Propuesta Económica

Instituto Mexicano del Seguro Social
Dirección de Administración
Unidad de Adquisiciones
Coordinación de Adquisición de Bienes y Contratación de Servicios
Coordinación Técnica de Adquisición de Bienes de Inversión y Activos
División de Contratación de Activos y Logística
Presente

PARTIDA 1

No.	Descripción de Servicio	Unidad de Medida	Precio Unitario
1	Firewall (Tipo 4)	Servicio	
2	Licenciamiento Firewall (Tipo 4) - Implementación	Servicio	
3	Licenciamiento Firewall (Tipo 1) - Renovacion	Servicio	
4	Licenciamiento Firewall (Tipo 2) - Renovación	Servicio	
5	Licenciamiento Firewall (Tipo 3) - Renovación	Servicio	
6	Licenciamiento Firewall (Tipo 4) - Renovación	Servicio	
7	IPS (Tipo 3)	Servicio	
8	Licienciamiento IPS (Tipo 4) - Implementación	Servicio	
9	Licenciamiento IPS (Tipo 1) - Renovación	Servicio	
10	Licenciamiento IPS (Tipo 2) - Renovación	Servicio	
11	Licenciamiento IPS (Tipo 3) - Renovación	Servicio	
12	Licenciamiento IPS (Tipo 4) - Renovación	Servicio	
13	Anti-denegación de servicios DDoS (Tipo 2)	Servicio	
14	Licenciamiento Anti-denegación de servicios DDoS (Tipo 2) - Implementación	Servicio	
15	Licenciamiento Anti-denegación de servicios DDoS (Tipo 1) - Renovación	Servicio	
16	Licenciamiento Anti-denegación de servicios DDoS (Tipo 2) - Renovación	Servicio	
17	Redes Privadas Virtuales	Servicio	
18	Licenciamiento Redes Privadas Virtuales - Implementación	Servicio	



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

19	Licenciamiento Redes Privadas Virtuales - Renovación	Servicio	
20	Licenciamiento Filtrado de Contenido Web - Renovación	Servicio	
21	Licenciamiento Filtrado de Contenido de Correo (Antispam) - Renovación	Servicio	
22	Firewall Especializado en Servicios Web (WAF)	Servicio	
23	Licenciamiento Firewall Especializado en Servicios Web (WAF) - Implementación	Servicio	
24	Licenciamiento Firewall Especializado en Servicios Web (WAF) - Renovación	Servicio	
25	Firewall Especializado en Base de Datos (DBF)	Servicio	
26	Licenciamiento Firewall Especializado en Base de Datos (DBF) - Implementación	Servicio	
27	Licenciamiento Firewall Especializado en Base de Datos (DBF) - Renovación	Servicio	
28	Gestión Unificada de Amenazas (UTM) (Tipo 4)	Servicio	
29	Licenciamiento Gestión Unificada de Amenazas (UTM) (Tipo 4) - Implementación	Servicio	
30	Licenciamiento Gestión Unificada de Amenazas (UTM) (Tipo 1) - Renovación	Servicio	
31	Licenciamiento Gestión Unificada de Amenazas (UTM) (Tipo 2) - Renovación	Servicio	
32	Licenciamiento Gestión Unificada de Amenazas (UTM) (Tipo 3) - Renovación	Servicio	
33	Licenciamiento Gestión Unificada de Amenazas (UTM) (Tipo 4) - Renovación	Servicio	
34	Correlación de Eventos	Servicio	
35	Licenciamiento Correlación de Eventos - Implementación	Servicio	
36	Protección de Amenazas Persistentes Avanzadas (APT)	Servicio	
37	Licenciamiento Protección de Amenazas Persistentes Avanzadas (APT) - Implementación	Servicio	
38	Borrado Seguro de Información	Servicio	
39	Ciberinteligencia	Servicio	
40	Protección de Redes Inalámbricas y Seguridad en dispositivos Móviles	Servicio	
41	Gestión de control de acceso para usuarios privilegiados (AAA)	Servicio	
42	Sistema de Gestión de Seguridad de la Información (SGSI)	Servicio	
43	Gestión de Dominios	Servicio	



GOBIERNO DE
MÉXICO



DIRECCIÓN DE ADMINISTRACIÓN

Unidad de Adquisiciones

Coordinación de Adquisición de Bienes y Contratación de Servicios

Coordinación Técnica de Adquisición de Bienes de Inversión y Activos

División de Contratación de Activos y Logística

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

44	Certificados Digitales SSL	Servicio	
45	Servicios de Prevención de Perdida de Información	Servicio	
46	Servicio de Antivirus	Servicio	
47	Servicios de Gestión del Cambio en Seguridad de la Información	Servicio	
48	Servicios del Centro de Operaciones de Seguridad (SOC)	Servicio	
Suma de Precios Unitarios:			

Monto en letra sin IVA (00/100 M.N.)

- Precios serán fijos durante la vigencia del contrato

Razón Social.- _____ (Del Licitante)

RFC.- _____ (Del Licitante)

Lugar y fecha.- _____

Representante Legal del Licitante (Nombre y Firma)_____



GOBIERNO DE
MÉXICO



DIRECCIÓN DE ADMINISTRACIÓN

Unidad de Adquisiciones

Coordinación de Adquisición de Bienes y Contratación de Servicios

Coordinación Técnica de Adquisición de Bienes de Inversión y Activos

División de Contratación de Activos y Logística

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Instituto Mexicano del Seguro Social
Dirección de Administración
Unidad de Adquisiciones
Coordinación de Adquisición de Bienes y Contratación de Servicios
Coordinación Técnica de Adquisición de Bienes de Inversión y Activos
División de Contratación de Activos y Logística
Presente

PARTIDA 2

No.	Descripción de Servicio	Unidad de Medida	Precio Unitario
49	Análisis de Vulnerabilidades Estático	Servicio	
50	Análisis de Vulnerabilidades Dinámico	Servicio	
51	Pruebas de Penetración	Servicio	
52	Análisis Forense	Servicio	
Suma de Precios Unitarios:			

Monto en letra sin IVA (00/100 M.N.)

- Precios serán fijos durante la vigencia del contrato

Razón Social.- _____ (Del Licitante)

RFC.- _____ (Del Licitante)

Lugar y fecha.- _____

Representante Legal del Licitante (Nombre y Firma) _____



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Anexo 10.- Relación de documentos a presentar

Fecha	
Licitación Pública Nacional Electrónica (Número)	
Denominación o Razón Social y Dirección Completa	
Teléfonos y Correo Electrónico	
Nombre del Representante	

Referencia	Documento legal-administrativo	Presentado	
		Si	No
Numeral 4.2.1 Anexo 3	Escrito bajo protesta de decir verdad que cuenta con facultades suficientes para comprometerse por sí o por su representada.		
Numeral 4.2.2 Anexo 4	Escrito bajo protesta de decir verdad, que el licitante es de nacionalidad mexicana.		
Numeral 4.2.4 Anexo 6	Escrito bajo protesta de decir verdad, que no se ubica en los supuestos establecidos en los artículos 50 y 60 de la LAASSP.		
Numeral 4.2.5 Anexo 7	Declaración de integridad, en la que el licitante manifieste, bajo protesta de decir verdad que se abstendrán de adoptar conductas, por si o a través de interpósita persona, para que los servidores públicos del IMSS induzcan o alteren las evaluaciones de las propuestas, el resultado del procedimiento u otros aspectos que otorguen condiciones más ventajosas con relación a los demás participantes.		
Numeral 4.2.6 Anexo 8	En su caso, escrito bajo protesta de decir verdad que el licitante cuenta con estratificación como micro, pequeña o mediana empresa.		
Anexo 11	Escrito para solicitar la clasificación de la información entregada por el licitante.		
Anexo 12	Escrito de manifestación que no desempeña empleo, cargo o comisión en el servicio público o, en su caso, que a pesar de desempeñarlo, con la formalización del contrato correspondiente no se actualiza un conflicto de interés.		
Anexo 15	Convenio de participación conjunta, cuando aplique.		
Anexo 16	Nota informativa para participantes de países miembros de la Organización para la Cooperación y el Desarrollo Económico (OCDE).		
Anexo 17	Escrito de Integridad de Comisión Federal de Competencia Económica.		
Anexo 19	Carta de autorización 32-D		
Anexo 20	Manifestación de servicios especializados		



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Referencia	Documento legal-administrativo	Presentado	
		Si	No
Anexo 21	Escrito libre en el que manifieste su aceptación de que se tendrán como no presentadas sus proposiciones y, en su caso, la documentación requerida, cuando el archivo electrónico en el que se contengan las proposiciones y/o demás información no pueda abrirse por tener algún virus informático o por cualquier otra causa ajena al IMSS, en términos de lo dispuesto por el numeral 29 del "Acuerdo por el que se establecen las disposiciones que deberán observar para la utilización del sistema electrónico de información pública gubernamental, denominado CompraNet".		
Anexo 22	Manifiesto de conocer el modulo de formalizacion de instrumentos juridicos.		
Numeral 4.3	Documentación de la propuesta técnica enviada por el CompraNet		
Numeral 6	Documentación proporcionada para la evaluación por puntos.		
Numeral 4.4 Anexo 9	Formato de propuesta Económica.		



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Anexo 11.- Escrito para solicitar la clasificación de la información entregada por el licitante

Ciudad de México, a ____ de _____ de 20__.

Instituto Mexicano del Seguro Social
Dirección de Administración
Unidad de Adquisiciones
Coordinación de Adquisición de Bienes y Contratación de Servicios
Coordinación Técnica de Adquisición de Bienes de Inversión y Activos
División de Contratación de Activos y Logística
Presente

____ (Nombre) _____, en mi carácter de _____, de la ____ (Persona Física o Moral) ___, manifiesto por medio de la presente que los documentos contenidos en mi propuesta y remitida a la convocante para la Licitación Pública Nacional Electrónica Núm. _____ que contiene a su vez información de carácter Reservada y Confidencial con fundamento en términos de lo dispuesto por los artículos 97, 98, 110 fracción XIII, 111 y 113 de la Ley Federal de Transparencia y Acceso a la Información Pública, deberá indicar si en los documentos que proporcionan al IMSS se contiene información de carácter confidencial o comercial reservada, señalando los documentos o las secciones de éstos que la contengan, así como el fundamento por el cual considera que tengan ese carácter.

(El licitante deberá señalar y fundamentar los numerales de su proposición administrativa-legal y/o técnica que considere información confidencial y/o comercial reservada.). Cabe señalar que de no clasificarse la información por parte del licitante en los términos señalados, la información presentada como parte de su proposición técnica - legal - económica tendrá tratamiento de información de carácter público.

Relación de documentos:

Ejemplos:

Protesto lo necesario

(Nombre y Firma del Apoderado o Representante Legal del Licitante)



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Anexo 12.- Escrito de manifestación que no desempeña empleo, cargo o comisión en el servicio público o, en su caso, que a pesar de desempeñarlo, con la formalización del contrato correspondiente no se actualiza un conflicto de interés

Ciudad de México, a _____ de _____ de 2022.

Instituto Mexicano del Seguro Social

Dirección de Administración

Unidad de Adquisiciones

Coordinación de Adquisición de Bienes y Contratación de Servicios

Coordinación Técnica de Adquisición de Bienes de Inversión y Activos

División de Contratación de Activos y Logística

Presente

PROCEDIMIENTO No. _____

PARA PERSONAS MORALES:

_____, en mi carácter de _____, de la __ (Persona Moral) __, manifiesto bajo protesta de decir verdad que los siguientes socios o accionistas

- 1.
- 2.
- 3.

No desempeñan empleo, cargo o comisión en el servicio público y no se actualiza un Conflicto de Interés.

(En caso de algún socio o accionista desempeñe empleo, cargo o comisión en el servicio público, se deberá indicar el nombre del socio o accionista)

- 1.
- 2.
- 3.

Independientemente de desempeñar empleo, cargo o comisión en el servicio público, con la formalización del contrato correspondiente, no se actualiza un Conflicto de Interés.

PARA PERSONA FÍSICAS:

_____, manifiesto bajo protesta de decir verdad que no desempeño empleo, cargo o comisión en el servicio público y no se actualiza un Conflicto de Interés.

O

_____, manifiesto bajo protesta de decir verdad que a pesar de desempeñar empleo, cargo o comisión en el servicio público y no se actualiza un Conflicto de Interés.

(Nombre y firma del licitante o representante legal de la persona moral)



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Anexo 13.- Manifestación de Interés en participar

Ciudad de México, a _____ de _____ de 20____

____ (Nombre) ____, en términos del artículo 33 Bis de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, en relación con el 48 fracción V de su Reglamento, expreso el interés de mi representada en participar en la presente Licitación Pública Nacional Electrónica Núm. _____ y en su caso **solicitar aclaraciones** a los aspectos contenidos en la convocatoria, por si o a nombre y representación de ____ (Persona Física o Moral) ___, y manifiesto **bajo protesta de decir verdad** que los datos aquí asentados son ciertos y han sido verificados, los siguientes datos:

Datos Personas Morales y Físicas.

Registro Federal de Contribuyentes.		
Domicilio.		
Calle y Número.		
Colonia.	Demarcación Territorial o Municipio.	
Código Postal.	Entidad Federativa.	
Teléfono Fijo.	Teléfono Móvil.	
Correo Electrónico.		
Número de la Escritura Pública en la que consta su Acta Constitutiva.		Fecha.
Nombre, Número y Circunscripción del Notario Público (ante el cual se dio fe de la misma).		
Fecha y Datos de su Inscripción en el Registro Público de Comercio.		
Descripción del Objeto Social.		
Relación de Accionistas.		
Apellido Paterno	Apellido Materno	Nombre(s)
Reformas al Acta Constitutiva que incidan con el objeto del procedimiento (Señalar Nombre, Número y Circunscripción del Notario o Fedatario Públicos que las protocolizó, así como la Fecha y los datos de su Inscripción en el Registro Público de la Propiedad)		

Apoderado o Representante Legal. (Nombre y Domicilio)	
Documento para Acreditar Personalidad y Facultades. (Escritura Pública y Modificaciones, Fecha, nombre, número y circunscripción del Notario Público ante el cual se otorgó)	

Protesto lo necesario

(Nombre y firma del apoderado o representante legal del licitante)

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Anexo 13.1- Formato de solicitud de aclaraciones

Procedimiento:		Fecha:	
Nombre o Razón Social del Licitante			
Domicilio			
RFC.			
Teléfono			
Correo Electrónico			

1.- Numerales de la convocatoria

Instructivo de llenado

Concepto	Descripción
(1) No. de pregunta y/o aclaración.	Se refiere al número consecutivo de la pregunta o aclaración formulada por el licitante.
(2) Numeral de la convocatoria.	Los licitantes deberán indicar el numeral específico de la convocatoria sobre el cual deseen formular preguntas o solicitar aclaraciones. En caso de requerir más renglones, deberán copiar la celda que contiene la “Lista Desplegable” y pegarla en la correspondiente celda.
(3) Pregunta y/o aclaración	Las preguntas o solicitudes de aclaración versarán exclusivamente sobre el contenido de la convocatoria.

Representante Legal del Licitante

Nombre y firma





Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Anexo 14.- Modelo de contrato

CONTRATO **(ABIERTO O CERRADO)** PARA LA PRESTACIÓN DEL SERVICIO DE **(\$DESCRIPCIÓN CATEGORÍA)**, QUE CELEBRAN, POR UNA PARTE, EL **(NOMBRE DE LA ENTIDAD)**, REPRESENTADA POR **(NOMBRE DEL REPRESENTANTE DE LA ENTIDAD)**, EN SU CARÁCTER DE **(SEÑALAR CARGO DEL REPRESENTANTE)**, EN ADELANTE “**EL INSTITUTO**” Y, POR LA OTRA, **(RAZÓN SOCIAL DE LA PERSONA FÍSICA O MORAL)**, EN LO SUCESIVO “**EL PROVEEDOR**”, **Solo si el proveedor es persona moral** REPRESENTADA POR **NOMBRE DEL REPRESENTANTE DE LA PERSONA MORAL**, EN SU CARÁCTER DE EL REPRESENTANTE LEGAL, A QUIENES DE MANERA CONJUNTA SE LES DENOMINARÁ “**LAS PARTES**”, AL TENOR DE LOS ANTECEDENTES, DECLARACIONES Y CLÁUSULAS SIGUIENTES:

CONTRATO **(ABIERTO O CERRADO)** PARA LA PRESTACIÓN DEL SERVICIO DE **(\$DESCRIPCIÓN CATEGORÍA)**, QUE CELEBRAN, POR UNA PARTE, EL **(NOMBRE DE LA ENTIDAD)**, REPRESENTADA POR **(NOMBRE DEL REPRESENTANTE DE LA ENTIDAD)**, EN SU CARÁCTER DE **(SEÑALAR CARGO DEL REPRESENTANTE)**, EN ADELANTE “**EL INSTITUTO**” Y, POR LA OTRA, **(RAZÓN SOCIAL DE LA PERSONA FÍSICA O MORAL)**, REPRESENTADA POR _____ EN SU CARÁCTER DE REPRESENTANTE LEGAL, EN PARTICIPACIÓN CONJUNTA CON _____, REPRESENTADA POR EL _____, EN SU CARÁCTER DE _____, A QUIENES EN FORMA CONJUNTA O INDIVIDUALMENTE DE LES DENOMINARÁ EN LO SUCESIVO “**EL PROVEEDOR**” Y EN FORMA CONJUNTA CON “**EL INSTITUTO**” SE LES DENOMINARÁ “**LAS PARTES**”, AL TENOR DE LOS ANTECEDENTES, DECLARACIONES Y CLÁUSULAS SIGUIENTES:

ANTECEDENTES

(Es la parte del contrato que se refiere a los hechos, sucesos, programas, mandatos, entre otros que dan origen a la prestación de los servicios y que para fines de cumplimiento de las funciones sustantivas deben atender las entidades, **(enumerar tantas como sean necesarias)**.

Que para dar cumplimiento a lo señalado en el artículo _____ de los Lineamiento que regulan la operación del Programa _____ “**EL INSTITUTO**” deberá _____.

Mediante oficio N° _____, el Titular de “**EL INSTITUTO**”, instruyó _____.

DECLARACIONES

I. “**EL INSTITUTO**” declara, a través de su Apoderada Legal, que:

I.1 Es un Organismo Descentralizado de la Administración Pública Federal con personalidad



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

jurídica y patrimonio propios, que tiene a su cargo la organización y administración del Seguro Social, como un servicio público de carácter nacional, en términos de los artículos 4º y 5º de la Ley del Seguro Social.

- I.2 Conforme a lo dispuesto por el artículo 268 A de la Ley de Seguro Social, y acredita su personalidad mediante el testimonio de la Escritura Pública número _____ de fecha _____, otorgada ante la fe del Licenciado _____, Titular de la Notaría Pública Número _____ del _____, e inscrita en el Registro Público de Organismos Descentralizados bajo el folio número _____, de fecha _____; manifiesta bajo protesta de decir verdad que las facultades que le fueron conferidas no le han sido revocadas, modificadas, ni restringidas en forma alguna en cumplimiento a los artículos 24 y 25 de la Ley Federal de las Entidades Paraestatales, el C. (NOMBRE DEL REPRESENTANTE DE LA ENTIDAD), (SEÑALAR CARGO DEL REPRESENTANTE), con R.F.C **(Colocar RFC)** es el servidor público que tiene conferidas las facultades legales para celebrar el presente contrato, quien podrá ser sustituido en cualquier momento en su cargo o funciones, sin que ello implique la necesidad de elaborar convenio modificadorio.
- I.3 De conformidad con el artículo 84, penúltimo párrafo del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, suscribe el presente instrumento el C. (NOMBRE DEL ADMINISTRADOR DEL PRESENTE CONTRATO), (SEÑALAR CARGO DEL ADMINISTRADOR DEL PRESENTE CONTRATO), con R.F.C **(Colocar RFC)**, facultado para administrar el cumplimiento de las obligaciones que deriven del objeto del presente contrato, quien podrá ser sustituido en cualquier momento en su cargo o funciones, bastando para tales efectos un comunicado por escrito y firmado por el servidor público facultado para ello, dirigido al representante de “**EL PROVEEDOR**” para los efectos del presente contrato, encargados del cumplimiento de las obligaciones contraídas en el presente instrumento jurídico.
- El (NOMBRE DEL ADMINISTRADOR DEL PRESENTE CONTRATO), (SEÑALAR CARGO DEL ADMINISTRADOR DEL PRESENTE CONTRATO), con R.F.C **(Colocar RFC)**, fungie como área consolidadora y representante de los administradores del presente contrato, quien será responsable de las designaciones de los administradores de este contrato, por lo que en su expediente deberán obrar las designaciones individuales de estos, los cuales serán encargados de dar seguimiento y verificar el cumplimiento de los derechos y obligaciones establecidos en este instrumento jurídico, de conformidad con lo dispuesto en el artículo 84, penúltimo párrafo del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.
- I.4 La adjudicación del presente contrato se realizó mediante el procedimiento de (TIPO DE PROCEDIMIENTO) (COLOCAR MEDIO DEL PROCEDIMIENTO) de carácter **(COLOCAR EL CARÁCTER DEL PROCEDIMIENTO)**, realizado al amparo de lo establecido en los artículos 134 de la Constitución Política de los Estados Unidos Mexicanos y en los artículos (FUNDAMENTO) de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y los correlativos de su Reglamento.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Cuando la proposición ganadora haya sido presentada en forma conjunta por varias personas (física o moral), se estará a lo dispuesto por el artículo 44 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

- I.5 “**EL INSTITUTO**” cuenta con recursos suficientes y con autorización para ejercerlos en el cumplimiento de sus obligaciones derivadas del presente contrato, como se desprende del Dictamen / Certificado de Disponibilidad Presupuestal Previo con cuenta número **(NUMERO DE SUFICIENCIA PRESUPUESTARIA)** con folio de autorización **(FOLIO AUTORIZACIÓN SP)**, de fecha _____ de _____ de _____, emitido por la _____ que se agrega al presente contrato en el **Anexo** _____ ()

“**EL INSTITUTO**” cuenta con recursos suficientes y con autorización para ejercerlos en el cumplimiento de sus obligaciones derivadas del presente contrato, como se desprende del Oficio de Liberación de Inversión (OLI) número **(NUMERO DE SUFICIENCIA PRESUPUESTARIA)** con folio de autorización **(FOLIO AUTORIZACIÓN SP)**, de fecha _____ de _____ de _____, emitido por la _____ que se agrega al presente contrato en el **Anexo** _____ ()

- I.6 Para efectos fiscales las Autoridades Hacendarias le han asignado el Registro Federal de Contribuyentes N° **(RFC ENTIDAD)**.
- I.7 Tiene establecido su domicilio en Calle Durango número 291, Colonia Roma Norte, Demarcación Territorial Cuauhtémoc, Código Postal 06700, en la Ciudad de México, mismo que señala para los fines y efectos legales del presente contrato.

II. “**EL PROVEEDOR**” declara que:

- II.1 Es una persona **(MORAL)** legalmente constituida según consta en la Escritura Pública número _____ de fecha _____, pasada ante la fe del (la) Licenciado (a) _____, Titular de la Notaría Pública número _____ de _____, e inscrita en el Registro Público de la Propiedad y de Comercio de _____, con el folio mercantil electrónico número _____, denominada **(NOMBRE O RAZÓN SOCIAL)**, cuyo objeto social es, entre otros, **(OBJETO SOCIAL)**.

Es una persona **(FISICA)** que acredita su personalidad para la firma de este contrato, mediante copia certificada de su acta de nacimiento, folio número _____, expedida por la _____ del _____, de fecha _____ e identificación oficial consistente en _____ expedida por _____, con código de identificación _____, con vigencia al año _____, denominada **(NOMBRE O RAZÓN SOCIAL)**, cuyas actividades consistentes, entre otras, en **(OBJETO SOCIAL)**, _____, inscrita en el Régimen de _____.

- II.2 La o el C. **(NOMBRE DEL REPRESENTANTE LEGAL)**, en su carácter de **representante legal**, cuenta con facultades suficientes para suscribir el presente contrato y obligar a su representada en los términos, lo cual acredita mediante la Escritura Pública número _____ de _____.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

fecha _____, pasada ante la fe del (la) Licenciado (a) _____, Titular de la Notaría Pública número _____ de _____, e inscrita en el Registro Público de la Propiedad y de Comercio de _____, con el folio mercantil electrónico número _____, mismo que bajo protesta de decir verdad manifiesta que no le han sido limitado ni revocado en forma alguna.

II.3 Reúne las condiciones de organización, experiencia, personal capacitado y demás recursos técnicos, humanos y económicos necesarios, así como con la capacidad legal suficiente para cumplir con las obligaciones que contrae en el presente contrato.

II.4 Manifiesta bajo protesta de decir verdad, no encontrarse en los supuestos de los artículos 50 y 60 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

En caso de que “**EL PROVEEDOR**” se encuentre en los supuestos señalados anteriormente, el contrato será nulo previa determinación de la autoridad competente de conformidad con lo establecido en el artículo 15 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

Asimismo, manifiesta que ni él ni ninguno de los socios o accionistas desempeñan un empleo, cargo o comisión en el servicio público, ni se encuentran inhabilitados para ello, o en su caso que, a pesar de desempeñarlo, con la formalización del presente contrato no se actualiza un conflicto de interés, en términos del artículo 49, fracción IX de la Ley General de Responsabilidades Administrativas.

II.5 Bajo protesta de decir verdad, declara que conoce y se obliga a cumplir con el Convenio 138 de la Organización Internacional del Trabajo en materia de erradicación del Trabajo Infantil, del artículo 123 Constitucional, apartado A) en todas sus fracciones y de la Ley Federal del Trabajo en su artículo 22, manifestando que ni en sus registros, ni en su nómina tiene empleados menores de quince años y que en caso de llegar a tener a menores de dieciocho años que se encuentren dentro de los supuestos de edad permitida para laborar le serán respetados todos los derechos que se establecen en el marco normativo transrito.

II.6 Cuenta con su Registro Federal de Contribuyentes (RFC PROVEEDOR).

II.7 Cuenta, al igual que su subcontratante con el documento vigente expedido por el Servicio de Administración Tributaria (SAT), de opinión de cumplimiento de obligaciones fiscales en sentido positivo, de conformidad con el artículo 32 D del Código Fiscal de la Federación, así como a lo dispuesto por las Reglas 2.1.29 y 2.1.37 de la Resolución Miscelánea Fiscal para 2022, publicada el 27 de diciembre de 2021 en el Diario Oficial de la Federación, del cual (de los cuales) presenta copia a “**EL INSTITUTO**” para efectos de la suscripción del presente contrato.(Lo resaltado en amarillo solo se debe incluir cuando exista subcontratación).

II.8.- Sus trabajadores se encuentran inscritos en el régimen obligatorio del Seguro Social, y al



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

corriente en el pago de las cuotas obrero patronales a que haya lugar, conforme a lo dispuesto en la Ley del Seguro Social, cuyas constancias correspondientes debidamente emitidas por “**EL INSTITUTO**” exhibe para efectos de la suscripción del presente instrumento jurídico. (EN CASO DE APLICAR)

II.9.- Cuenta, al igual que su subcontratante, con el documento correspondiente vigente, expedido

por “**EL INSTITUTO**” sobre el cumplimiento de sus obligaciones fiscales en materia de seguridad social, conforme al Acuerdo ACDO.SA1.HCT.101214/281.P.DIR dictado por el H. Consejo Técnico de “**EL INSTITUTO**” en la sesión ordinaria celebrada el 10 de diciembre de 2014, publicado en el Diario Oficial de la Federación el 27 de febrero de 2015 y su modificación publicada en el mismo de fecha 3 de abril de 2015, del cual (de los cuales) presenta copia a “**EL INSTITUTO**” para efectos de la suscripción del presente contrato.

En caso de incumplimiento en sus obligaciones en materia de seguridad social, solicita se apliquen los recursos derivados del presente contrato, contra los adeudos que, en su caso, tuviera a favor de “**EL INSTITUTO**”. (En caso de aplicar)

II.10.- Cuenta, al igual que su subcontratante, con el documento correspondiente vigente, expedido por el INFONAVIT en los términos del Acuerdo del H. Consejo de Administración del Instituto del Fondo Nacional de la Vivienda para los Trabajadores por el que se emiten las Reglas para la obtención de la constancia de situación fiscal en materia de aportaciones patronales y entero de descuentos, publicado en el Diario Oficial de la Federación el 28 de junio de 2017, del cual (de los cuales) presenta copia a “**EL INSTITUTO**” para efectos de la suscripción del presente contrato.

II.11.- Señala como su domicilio para todos los efectos legales el ubicado en **(DOMICILIO FISCAL PROVEEDOR)**, para oír y recibir toda clase de notificaciones y documentos, el ubicado en _____ número _____, Colonia _____, Demarcación Territorial _____, Código Postal _____, en la Ciudad de México, teléfonos: (55) _____ o (01 ____) _____, correos electrónicos: _____.

II.12 Conforme a lo previsto en los artículos 57 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 107 de su Reglamento, “**EL PROVEEDOR**”, en caso de auditorías, visitas o inspecciones que practique la Secretaría de la Función Pública y el Órgano Interno de Control en “**EL INSTITUTO**” y cualquier otra entidad fiscalizadora, deberá proporcionar la información relativa al presente contrato que en su momento se requiera, generada desde el procedimiento de adjudicación hasta la conclusión de la vigencia, a efecto de ser sujetos a fiscalización de los recursos de carácter federal.

EN CASO DE QUE SE HAYA ADJUDICADO A UN PROVEEDOR EN PARTICIPACIÓN CONJUNTA, SE INCLUIRÁ EL SIGUIENTE TEXTO:

III.- “EL PROVEEDOR”, declara conjuntamente que:



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

III.1.- Han celebrado convenio de participación conjunta, cuyas obligaciones deberán cumplirse en términos del mismo, el cual se integra al presente instrumento jurídico como **Anexo _____**.

III.2.- Conocen el contenido y los requisitos que establece la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y su Reglamento, la Convocatoria y sus Anexos.

III. De “LAS PARTES”:

III.1 Que es su voluntad celebrar el presente contrato y sujetarse a sus términos y condiciones, para lo cual se reconocen ampliamente las facultades y capacidades necesarias, mismas que no les han sido revocadas o limitadas en forma alguna, por lo que de común acuerdo se obligan de conformidad con las siguientes:

Hechos los antecedentes y declaraciones anteriores, “**LAS PARTES**” convienen en otorgar el presente contrato, de conformidad con las siguientes:

CLÁUSULAS

PRIMERA. OBJETO DEL CONTRATO.

“**EL PROVEEDOR**” acepta y se obliga a proporcionar a “**EL INSTITUTO**” el servicio de (**OBJETO DEL CONTRATO SELECCIONADO**), al amparo del procedimiento de contratación señalado en el punto I.4 de las declaraciones de este instrumento jurídico.

Los **Anexos** que forman parte integrante del presente contrato, se enuncian a continuación:

Anexo 1 (uno) “Dictamen/Certificado de Disponibilidad Presupuestal Previo y/o OLI”

Anexo 2 (dos) “Anexo Técnico, Términos y Condiciones, Programa Calendarizado (EN CASO DE APLICAR)”

Anexo 3 (tres) “Propuesta Técnica y Económica de “**EL PROVEEDOR**” y Acta de Fallo/Oficio de Adjudicación”

Anexo 4 (cuatro) “Junta de Aclaraciones, la cual se encuentra disponible para su consulta en CompraNet” (EN CASO DE APLICAR)

Anexo 5 (cinco) “Convenio de Participación Conjunta” (EN CASO DE APLICAR)

SEGUNDA. DE LOS MONTOS Y PRECIOS.

(EN CASO DE SER CERRADO): (en caso que en detalle de \$Categoría a contratar haya



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

seleccionado NO, no se muestra esta línea y la tabla El(los) precio(s) unitario(s) del presente contrato, expresado(s) en moneda nacional es (son):

(COLOCAR TABLA PRECIO UNITARIO)

El monto total del mismo es por la cantidad de (MONTO TOTAL DEL CONTRATO sin impuestos) en moneda nacional antes de impuestos y (MONTO TOTAL DEL CONTRATO con impuestos) en moneda nacional después de impuestos.

El precio unitario es considerado fijo y en moneda nacional (pesos mexicanos) hasta que concluya la relación contractual que se formaliza, incluyendo “**EL PROVEEDOR**” todos los conceptos y costos involucrados en la prestación del servicio (**OBJETO DEL CONTRATO SELECCIONADO**), por lo que “**EL PROVEEDOR**” no podrá agregar ningún costo extra y los precios serán inalterables durante la vigencia del presente contrato.

(EN CASO DE PLURIANUAL) De acuerdo a la plurianualidad del presente contrato, se pagará a “**EL PROVEEDOR**” los siguientes montos en cada ejercicio fiscal.

Ejercicio Fiscal	EJERCICIO FISCAL	Porcentaje (%) CORRESPONDIENTE AL FISCAL	Monto (MONTO TOTAL CONTRATO con impuestos * % CORRESPONDIENTE AL EJERCICIO FISCAL)
------------------	------------------	--	--

Se agregarán tantos se
hayan programado

(EN CASO DE SER ABIERTO): (en caso que se haya seleccionado monto total o en detalle de \$Categoría a contratar haya seleccionado NO, no se muestra esta línea y la tabla El(los) precio(s) unitario(s) del presente contrato, expresado(s) en moneda nacional es (son):

(COLOCAR TABLA PRECIO UNITARIO)_

El(los) precio(s) unitario(s) del presente contrato es por la cantidad de (PRECIO UNITARIO) en moneda nacional antes de impuestos, el monto total mínimo del mismo es por la cantidad de (MONTO MÍNIMO TOTAL DEL CONTRATO) en moneda nacional antes de impuestos y el monto total máximo del mismo es por la cantidad de (MONTO MÁXIMO TOTAL DEL CONTRATO) en moneda nacional antes de impuestos.

El precio unitario es considerado fijo y en moneda nacional (pesos mexicanos) hasta que concluya la relación contractual que se formaliza, incluyendo “**EL PROVEEDOR**” todos los conceptos y costos involucrados en la prestación del servicio (**OBJETO DEL CONTRATO**



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

SELECCIONADO), por lo que “EL PROVEEDOR” no podrá agregar ningún costo extra y los precios serán inalterables durante la vigencia del presente contrato.

(EN CASO DE PLURIANUAL) De acuerdo a la plurianualidad del presente contrato, se considerarán los montos mínimos y máximos a pagar a “EL PROVEEDOR” en cada ejercicio fiscal.

Ejercicio Fiscal	Porcentaje	Monto mínimo	Monto máximo
(COLOCAR EJERCICIO FISCAL)	(% CORRESPONDIENTE AL FISCAL)	(MONTO MÍNIMO * % CORRESPONDIENTE AL FISCAL)	(MONTO MÁXIMO * % CORRESPONDIENTE AL FISCAL)

Se agregarán
tantos se
hayan
programado

TERCERA. FORMA Y LUGAR DE PAGO.

Se efectuarán pagos _____ a “EL PROVEEDOR” una vez prestados los servicios, de conformidad con lo dispuesto en los artículos 51 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 93 de su Reglamento, así como por lo establecido en los Términos y Condiciones que se agregan al presente contrato en el Anexo _____.(_____.)

El CFDI o factura electrónica deberá ser presentada (señalar la forma y el medio mediante el cual se presentará)

El pago se realizará en pesos mexicanos, o en su caso se especificará la moneda extranjera, en los plazos normados por la Dirección de Finanzas, de acuerdo al “Procedimiento para la recepción, glosa y aprobación de documentos presentados para trámite de pago y la constitución, modificación, cancelación, operación y control de fondos fijos” sin que éstos rebasen los 20 (veinte) días naturales posteriores a aquel en que “EL PROVEEDOR” presente en forma impresa el Comprobante Fiscal Digital por Internet (CFDI), siempre y cuando se cuente con la suficiencia presupuestal, así como con la documentación comprobatoria que acredite la entrega de los servicios, conforme a los numerales cuarto y sexto del capítulo quinto, intitulado, de los Lineamientos para promover la agilización de pago a los proveedores contenidos en el “Acuerdo por el que se emiten diversos lineamientos en materia de adquisiciones, arrendamientos y servicios y de obras públicas y servicios relacionados con las



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

mismas”, concordante con los artículos 65 y 66 del Reglamento de la Ley Federal de Presupuesto y Responsabilidad Hacendaria, conforme a lo siguiente: (EN CASO DE APLICAR)

Considerar párrafos adicionales conforme a lo señalado en el Anexo Técnico y Términos y Condiciones.

En caso de aplicar, el contrato y su Dictamen de Disponibilidad Presupuestal (DDP) deberán estar registrados en el Sistema PREI Millenium.

El CFDI deberá presentarse ante la División de Trámite de Erogaciones de la Coordinación de Contabilidad y Trámite de Erogaciones en Órganos Normativos, la Oficina de Control de Trámite de Erogaciones en los Órganos de Operación Administrativa Desconcentrada (OOAD), la Oficina de Trámite de Erogaciones de la Unidad Médica de Alta Especialidad (UMAE), según corresponda, para proceder a su glosa, revisión y, en su caso, aprobación. Dicho CFDI deberá contener el nombre, cargo y firma de autorización del administrador del presente contrato, de quien suscribió la orden de compra. Asimismo, en dicho CFDI se deberán indicar: número de alta en SAI o número de identificación de pedido-recepción en PREI-Millenium (cuando sea aplicable), número de proveedor, número de contrato, número de garantía de cumplimiento que se haya aceptado, denominación social de la institución que otorga la garantía de cumplimiento y la indicación de que “**EL PROVEEDOR**” cuenta con opiniones positivas y vigentes en materia de aportaciones de seguridad social ante el IMSS e INFONAVIT así como de obligaciones fiscales ante el SAT. (EN CASO DE APLICAR)

En caso de que el devengo por la entrega-recepción no genere número de alta en SAI o número de pedido-recepción en PREI-Millenium, en su caso, se deberá adjuntar acta de entrega-recepción.

El personal de la División de Trámite de Erogaciones de la Coordinación de Contabilidad y Trámite de Erogaciones no podrá devolver el CFDI presentado por errores que no afecten la validez fiscal del documento o por causas imputables a “**EL INSTITUTO**”.

Para los casos en que no se formalice el presente contrato, el fallo o notificación de la adjudicación será el documento con el cual procederá el pago respectivo de los servicios proporcionados, únicamente para el periodo comprendido entre el fallo y la fecha en que debió formalizarse el contrato.

Para efectos de lo anterior, la División de Contratos deberá informar al administrador del presente contrato o Área Consolidadora, en su caso, en un plazo no mayor a 24 (veinticuatro) horas posteriores al vencimiento del plazo para formalización del instrumento legal, de la falta de formalización del mismo, a efecto de que se realicen las gestiones que correspondan para no recibir los servicios materia del presente contrato.

El pago en moneda extranjera se considerará, siempre en dólares EE.UU.A., y en caso de que se cubra la obligación de pago en territorio nacional, se liquidará al tipo de cambio publicado en el Diario Oficial de la Federación (DOF) o en el Tipo de cambio para solventar obligaciones



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

denominadas en dólares de los EE. UU. A., pagaderas en la República Mexicana, publicado por el Banco de México (FIX) que determina el Banco de México; así se expresará en el apartado “monto” de la convocatoria, invitación a cuando menos tres personas y/o contrato de conformidad a lo dispuesto en los artículos 45 fracción XIII de la Ley de Adquisiciones, Arrendamientos y Servicios de Sector Público en concordancia con el 8 de la Ley Monetaria de los Estados Unidos Mexicanos. (EN CASO DE APLICAR)

“**EL PROVEEDOR**” deberá expedir sus CFDI en el esquema de facturación electrónica, con las especificaciones normadas en los artículos 29 y 29-A del Código Fiscal de la Federación (CFF), así como las que emita el Servicio de Administración Tributaria (SAT) a nombre de “**EL INSTITUTO**”, con Registro Federal de Contribuyentes IMS421231I45 y en caso de ser necesario como dato adicional, el domicilio en Avenida Paseo de la Reforma Núm. 476 en la Colonia Juárez, C.P. 06600, Demarcación Territorial Cuauhtémoc, Ciudad de México.

Para la validación de dichos comprobantes “**EL PROVEEDOR**” deberá cargar en Internet, a través del Portal de Servicios a Proveedores de la página de “**EL INSTITUTO**” archivo en formato XML. La validez de los mismos, será determinada durante la carga y únicamente los comprobantes válidos serán procedentes para pago.

El pago se realizará mediante transferencia electrónica de fondos y en la fecha, a través del esquema electrónico interbancario que “**EL INSTITUTO**” tiene en operación, para tal efecto “**EL PROVEEDOR**” deberá proporcionar la documentación requerida por la Coordinación de Tesorería, para dar de alta en el Sistema de “**EL INSTITUTO**”, la cuenta bancaria, (no deberá ser referenciada ni concentradora), CLABE, Banco y Sucursal a menos que éste acredite en forma fehaciente la imposibilidad para ello.

El pago se depositará a “**EL PROVEEDOR**” en la fecha programada, a través del Sistema de Pagos Electrónicos Interbancarios.

El administrador del presente contrato será quien dará la autorización para que la Dirección de Finanzas proceda a su pago de acuerdo a lo normado en el anexo “Normatividad de pago de las Cuentas Contables” del “Procedimiento para la recepción, glosa y aprobación de documentos presentados para trámite de pago y la constitución, modificación, cancelación, operación y control de fondos fijos”.

En ningún caso, se deberá autorizar el pago de los servicios, si no se ha determinado, calculado y notificado a “**EL PROVEEDOR**” las penas convencionales o deducciones pactadas en el presente contrato, así como su registro y validación en el Sistema PREI Millenium.

“**EL PROVEEDOR**” podrá optar por cobrar a través de factoraje financiero conforme al Programa de Cadenas Productivas de Nacional Financiera, S.N.C., Institución de Banca de Desarrollo con “**EL INSTITUTO**”.

En caso de que “**EL PROVEEDOR**” reciba pagos en exceso deberá reintegrar las cantidades pagadas en exceso más los intereses correspondientes, conforme a la tasa que establezca la



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Ley de Ingresos de la Federación, en los casos de prórroga para el pago de créditos fiscales. Los intereses se calcularán sobre las cantidades en exceso y se computarán por días naturales desde la fecha de su entrega hasta la fecha en que se pongan efectivamente las cantidades a disposición de “**EL INSTITUTO**”.

En caso de que “**EL PROVEEDOR**” presente su CFDI con errores o deficiencias, conforme a lo previsto en los artículos 89 y 90 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, “**EL INSTITUTO**” dentro de los 3 (tres) días hábiles siguientes a la recepción de la misma, indicará por escrito a “**EL PROVEEDOR**” las deficiencias o errores que deberá corregir. El periodo que transcurra a partir de la entrega del citado escrito y hasta que “**EL PROVEEDOR**” presente las correcciones no se computará dentro del plazo estipulado para el pago.

“**EL PROVEEDOR**”, para cada uno de los pagos que efectivamente reciba, de acuerdo con esta cláusula, deberá de expedir a nombre de “**EL INSTITUTO**”, el “CFDI con complemento para la recepción de pagos”, también denominado “recibo electrónico de pago”, el cual elaborará dentro de los plazos establecidos por las disposiciones fiscales vigentes y lo cargará en el portal de servicios a proveedores de la página de “**EL INSTITUTO**”.

“**EL PROVEEDOR**” se obliga a no cancelar ante el SAT los CFDI a favor de “**EL INSTITUTO**” previamente validados en el portal de servicios a proveedores, salvo justificación y comunicación por parte del mismo al administrador del presente contrato para su autorización expresa, debiendo éste informar a las áreas de trámite de erogaciones de dicha justificación y reposición del CFDI en su caso.

El administrador del presente contrato llevará a cabo la valoración de la procedencia del pago por concepto de gastos no recuperables conforme a lo previsto en los artículos 101 y 102 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, en relación con los artículos 38, 46, 54 Bis y 55 Bis, segundo párrafo de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, previa solicitud por escrito a “**EL PROVEEDOR**”, acompañada de los documentos siguientes:

- Copia de la identificación oficial vigente con fotografía y firma de la persona que haya realizado los trámites relacionados con el procedimiento de contratación.
- El CFDI que reúna los requisitos de los artículos 29 y 29-A del CFF, 37 al 40 del Reglamento del Código Fiscal de la Federación (RCFF) y, en su caso, la Resolución de la Miscelánea Fiscal del Ejercicio que corresponda.
- La solicitud la realizará al administrador del presente contrato para la determinación de la procedencia del pago y, en su caso, elaborar el finiquito y remitirlo para el pago respectivo a la Coordinación de Contabilidad y Trámite de Erogaciones, dependiente de la Dirección de Finanzas, o ante la Jefatura de Servicios de Finanzas o de la Unidad Médica de Alta Especialidad (UMAE) o ante los Órganos de Operación Administrativa Desconcentrada (OOAD), según corresponda.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Al notificar a “**EL PROVEEDOR**” la aplicación de una pena convencional, el administrador del presente contrato deberá solicitar a las áreas de contabilidad (en Órganos Normativos, OOAD o en UMAE) la emisión del CFDI de ingreso por dicho concepto y entregarlo a “**EL PROVEEDOR**” para que se compense contra los adeudos que tenga “**EL INSTITUTO**” para con “**EL PROVEEDOR**” o, para que en su defecto, éste proceda a pagar a “**EL INSTITUTO**” la pena convencional.

El pago de los servicios quedará condicionado proporcionalmente al pago que “**EL PROVEEDOR**” deba efectuar por conceptos de penas convencionales y/o deducciones. En ambos casos, “**EL INSTITUTO**” realizará las retenciones correspondientes sobre el CFDI que se presente para pago. En el entendido de que en el supuesto de que sea rescindido el presente contrato, no procederá el cobro de dichas penalizaciones, ni la contabilización de las mismas para hacer efectiva la garantía de cumplimiento, de conformidad con lo establecido por el artículo 95 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

Las Unidades Responsables del Gasto (URG) deberán registrar los contratos, convenios y su DDP en el Sistema PREI Millenium para el trámite de pago correspondiente.

Los servicios cuya recepción no genere alta a través del SAI o el PREI Millenium de manera electrónica, deberán contener la firma de recepción y de autorización para el trámite de pago de acuerdo a lo establecido en el “Procedimiento para la recepción, glosa y aprobación de documentos presentados para trámite de pago y la constitución, modificación, cancelación, operación y control de fondos fijos” vigente, así como el Acta de Entrega-Recepción, según corresponda.

Para que “**EL PROVEEDOR**” pueda celebrar un contrato de cesión de derechos de cobro, mismo que deberá notificarlo por escrito a “**EL INSTITUTO**” con un mínimo de 5 (cinco) días naturales anteriores a la fecha de pago programada, el administrador del presente contrato, o en su caso, el Titular del Área Requirente, deberá entregar los documentos sustantivos de dicha cesión al área responsable de autorizar ésta, conforme al “Procedimiento para la recepción, glosa y aprobación de documentos presentados para trámite de pago y la constitución, modificación, cancelación, operación y control de fondos fijos”.

En caso de aplicar, en lo referente a los pagos por suscripciones, seguros u otros servicios, que sean de trato sucesivo, su pago será autorizado previa solicitud del Área Requirente de que se trate.

PARRAFO PARA EN CASO DE QUE EXISTA PARTICIPACIÓN CONJUNTA.

Para efectos del cobro de sus CFDI, deberá presentarse por “**EL PROVEEDOR**” que se haya establecido en el convenio de participación conjunta, en el entendido de que “**EL INSTITUTO**” no será responsable de la manera en que hayan acordado la distribución del pago.

El CFDI o factura electrónica se deberá presentar desglosando el IVA cuando aplique.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

“EL PROVEEDOR” manifiesta su conformidad de que hasta en tanto no se cumpla con la verificación, supervisión y aceptación de los servicios, no se tendrán como recibidos o aceptados por el administrador del presente contrato mencionado en la Declaración I.3.

Para efectos de trámite de pago, **“EL PROVEEDOR”** deberá ser titular de una cuenta de cheques vigente y para tal efecto proporciona la CLABE _____, del banco _____, a nombre de “_____”, en la que se efectuará la transferencia electrónica de pago.

El pago de los servicios proporcionados, quedará condicionado proporcionalmente al pago que **“EL PROVEEDOR”** deba efectuar por concepto de penas convencionales.

(EN CASO DE EXISTIR ANTICIPOS) Se otorgarán a **“EL PROVEEDOR”** los siguientes anticipos, con la previa autorización del (SERVIDOR PÚBLICO CON FACTULTADES PARA AUTORIZAR ANTICIPO) de conformidad con el ____(ordenamiento jurídico en los que se regulen sus facultades)____.

ANTICIPO (PORCENTAJE DEL MONTO FECHA A OTORGAR ANTICIPO
TOAL)

(COLOCAR EL % DE ANTICIPO) (FECHA EN QUE SE PAGARÁ ANTICIPO)

Se agregarán tantos se hayan programado

Asimismo se estipula que la amortización de los anticipos atrás descritos se llevará a cabo
(señalar la forma en que se llevará a cabo su amortización.)

CUARTA. VIGENCIA.

El contrato comprenderá una vigencia considerada a partir de **COLOCAR FECHA DE INICIO**) y hasta el (**COLOCAR FECHA DE TERMINO DEL CONTRATO**) sin perjuicio de su posible terminación anticipada, en los términos establecidos en su clausulado.

QUINTA. MODIFICACIONES DEL PRESENTE CONTRATO.

De conformidad con lo establecido en el artículo 52 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, **“EL INSTITUTO”** podrá celebrar por escrito Convenio



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Modificatorio, al presente contrato dentro de la vigencia del mismo. Para tal efecto, “**EL PROVEEDOR**” se obliga a entregar, en su caso, la modificación de la garantía, en términos del artículo 103, fracción II del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

PRÓRROGAS.- Asimismo, se podrán acordar prórrogas al plazo originalmente pactado por caso fortuito, fuerza mayor o por causas atribuibles a “**EL INSTITUTO**”, lo cual deberá estar debidamente acreditado en el expediente de contratación respectivo. “**EL PROVEEDOR**” puede solicitar la modificación del plazo originalmente pactado cuando se actualicen y se acrediten los supuestos de caso fortuito o de fuerza mayor.

Cualquier modificación a los derechos y obligaciones estipuladas por “**LAS PARTES**” en el presente contrato, deberá formalizarse mediante convenio y por escrito, mismo que será suscrito por los servidores públicos que lo hayan hecho en el contrato, quienes los sustituyan o estén facultados para ello.

SEXTA. GARANTÍA DEL SERVICIO.

“**EL PROVEEDOR**” se obliga a otorgar a “**EL INSTITUTO**”, las siguientes garantías:

(EN CASO SELECCIONAR GARANTÍA SOBRE SERVICIOS)

- Garantía del servicio.**- “**EL PROVEEDOR**” se obliga con “**EL INSTITUTO**” a entregar _____ (CONFORME LO SEÑALE EL ANEXO TÉCNICO Y/O TERMINOS Y CONDICIONES)

(EN CASO SELECCIONAR GARANTÍA DE ANTICIPO)

- Garantía de los anticipos recibidos.** - “**EL PROVEEDOR**” entregará a “**EL INSTITUTO**”, a más tardar el (**COLOCAR FECHA DE ENTREGA DE GARANTÍA DE ANTICIPOS**) previamente a la entrega del anticipo una garantía constituida por la totalidad del monto de los anticipos recibidos.

El otorgamiento de anticipos, deberá garantizarse en los términos del artículo 48 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y primer párrafo del artículo 81 de su Reglamento. Si las disposiciones jurídicas aplicables lo permitan, la entrega de la garantía de anticipos se realice de manera electrónica

La póliza de garantía de anticipo será devuelta a “**EL PROVEEDOR**” una vez que el “**EL INSTITUTO**” entregue a “**EL PROVEEDOR**”, autorización por escrito de que demuestre haber cumplido con la totalidad de las obligaciones adquiridas en el presente contrato, para lo cual “**EL PROVEEDOR**”, deberá solicitar por escrito a “**EL INSTITUTO**” una vez concluida la verificación de cumplimiento o terminación del presente contrato la liberación de la fianza a efecto de que “**EL PROVEEDOR**” pueda solicitar a la afianzadora la cancelación o liberación de la fianza.

En caso de que “**EL INSTITUTO**” requiera hacer efectivo un importe parcial de la póliza de



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

garantía de fianza de anticipo, “**EL PROVEEDOR**” se obliga a presentar a “**EL INSTITUTO**” otra póliza nueva de fianza o un endoso a la misma, amparando el importe restante de la obligación total requerida.

SÉPTIMA. GARANTÍA DE CUMPLIMIENTO DEL PRESENTE CONTRATO.

(EN CASO NO SELECCIONAR GARANTÍA DE CUMPLIMIENTO DEL CONTRATO)

Ingresar excepción de la garantía de cumplimiento

(EN CASO SI SELECCIONAR GARANTÍA DE CUMPLIMIENTO DEL CONTRATO)

DE CUMPLIMIENTO DEL CONTRATO.- “**EL PROVEEDOR**” se obliga a entregar a más tardar dentro de los 10 (diez) días naturales posteriores a la firma de este instrumento jurídico (**VERIFICAR PLAZO DE ENTREGA EN LOS TÉRMINOS Y CONDICIONES**), en términos de la fracción II del artículo 48 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, una garantía de cumplimiento de todas y cada una de las obligaciones a su cargo derivadas del presente contrato, mediante fianza expedida por compañía autorizada en los términos del artículo 81, fracción VI del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y de la Ley de Instituciones de Seguros y de Fianzas a favor del “Instituto Mexicano del Seguro Social” por un monto equivalente al 10% (diez por ciento) sobre el importe total ó máximo que se indica en la Cláusula Segunda del presente contrato, sin considerar el Impuesto al Valor Agregado (I.V.A.), en Moneda Nacional.

“**EL PROVEEDOR**” queda obligado a entregar a “**EL INSTITUTO**” la póliza de fianza antes señalada, en la División de Contratos, ubicada en Calle Durango número 291, 10º piso, Colonia Roma Norte, Demarcación Territorial Cuauhtémoc, Código Postal 06700, en la Ciudad de México, apegándose al formato que para tal efecto se entregará en la referida División.

VERIFICAR VIGENCIA DE LA GARANTÍA EN LOS TÉRMINOS Y CONDICIONES.

Dicha póliza de garantía de cumplimiento del contrato se liberará de forma inmediata a “**EL PROVEEDOR**” una vez que “**EL INSTITUTO**” le otorgue autorización por escrito, para que éste pueda solicitar a la afianzadora correspondiente la cancelación de la fianza, autorización que se entregará a “**EL PROVEEDOR**” siempre que demuestre haber cumplido con la totalidad de las obligaciones adquiridas por virtud del presente contrato; para lo anterior deberá presentar mediante escrito la solicitud de liberación de la fianza en la División de Contratos, misma que llevará a cabo el procedimiento para su liberación y entrega.

ENDOSO DE LA GARANTÍA DE CUMPLIMIENTO.- En el supuesto de que “**EL INSTITUTO**” y por así convenir a sus intereses, decidiera modificar en cualquiera de sus partes el presente contrato, “**EL PROVEEDOR**” se obliga a otorgar el endoso de la póliza de garantía originalmente entregada, en el que conste las modificaciones o cambios en la respectiva fianza, observándose los mismos términos y condiciones señalados en la presente cláusula para la entrega de la garantía de cumplimiento, debiéndola entregar “**EL PROVEEDOR**” a más tardar



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

dentro de los 10 (diez) días naturales posteriores a la firma del convenio respectivo.

(EN EL CASO DE APLICAR DE ACUERDO AL MONTO)

No obstante lo anterior, y toda vez que el monto del presente contrato es menor a 900 (novecientos) días de Unidad de Medida y Actualización (UMA), “**EL PROVEEDOR**” podrá presentar la garantía de cumplimiento de las obligaciones estipuladas, mediante cheque certificado, por un importe equivalente al 10% (diez por ciento) del monto total, sin considerar el Impuesto al Valor Agregado, en favor de “**EL INSTITUTO**”, siendo necesario considerar lo siguiente:

- a) El cheque debe expedirse a nombre del "Instituto Mexicano del Seguro Social".
- b) Dicho cheque deberá ser resguardado, a título de garantía, por “**EL INSTITUTO**” en la División de Contratos.
- c) El cheque será devuelto a solicitud, por escrito de “**EL PROVEEDOR**” el segundo día hábil posterior a que “**EL INSTITUTO**” constate el cumplimiento del presente instrumento, previa validación del administrador del presente contrato.

EJECUCIÓN DE LA GARANTÍA DE CUMPLIMIENTO DE ESTE CONTRATO.- “**EL INSTITUTO**” llevará a cabo la ejecución de la garantía de cumplimiento de contrato en los casos siguientes:

- a) Se rescinda administrativamente el presente contrato.
- b) Si “**EL PROVEEDOR**” no puede realizar el cambio físico del producto, en términos de lo que dispone las Cláusulas _____ del presente contrato.
- c) Cuando en el supuesto de que se realicen modificaciones al contrato, “**EL PROVEEDOR**” no entregue en el plazo pactado el endoso o la nueva garantía, que ampare el porcentaje establecido para garantizar el cumplimiento del presente instrumento, de conformidad con la Cláusula Décima Cuarta, inciso b). (VERIFICAR)
- d) Por cualquier otro incumplimiento de las obligaciones contraídas en este contrato.

De conformidad con el artículo 81, fracción II del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, la aplicación de la garantía de cumplimiento se hará efectiva de manera proporcional al monto de las obligaciones incumplidas. por el monto total de las obligaciones garantizadas.
(Dependiendo del caso concreto)

OCTAVA. OBLIGACIONES DE “EL PROVEEDOR”.

- a) Proporcionar los servicios en las fechas o plazos y lugares específicos conforme a lo requerido en el presente contrato y anexos respectivos.
- b) Correrá bajo su cargo los costos de flete, transporte, seguro y de cualquier otro derecho que se genere, hasta el lugar de la prestación de los servicios, así como el



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

- costo de su traslado de regreso al término del presente contrato, en caso de aplicar.
- c) Cumplir con las especificaciones técnicas y de calidad y demás condiciones establecidas en el presente contrato y respectivos anexos, así como la cotización y el requerimiento asociado a ésta;
 - d) Asumir su responsabilidad ante cualquier situación que pudiera generarse con motivo del presente contrato.
 - e) No difundir a terceros sin autorización expresa de “**EL INSTITUTO**” la información que le sea proporcionada, inclusive después de la rescisión o terminación del presente instrumento, sin perjuicio de las sanciones administrativas, civiles y penales a que haya lugar.
 - f) Proporcionar la información que le sea requerida por parte de la Secretaría de la Función Pública y el Órgano Interno de Control en “**EL INSTITUTO**”, de conformidad con el artículo 107 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

“**LAS PARTES**” que suscriben el presente contrato en su carácter de “**EL PROVEEDOR**”, asumen las obligaciones materia de este instrumento jurídico en forma mancomunada o solidaria conforme a lo estipulado en el convenio de participación conjunta.

NOVENA. OBLIGACIONES DE “EL INSTITUTO”.

- a) Otorgar todas las facilidades necesarias, a efecto de que “**EL PROVEEDOR**” lleve a cabo el objeto del presente contrato en los términos convenidos.
- b) Sufragar el pago correspondiente en tiempo y forma, por la prestación de los servicios.
- c) Extender a “**EL PROVEEDOR**”, en caso de que lo requiera, por conducto del administrador del presente contrato, la constancia de cumplimiento de obligaciones contractuales inmediatamente que se cumplan éstas a satisfacción expresa de dicho servidor público para que se dé trámite a la cancelación de la garantía de cumplimiento del presente contrato.

DÉCIMA. LUGAR, PLAZOS Y CONDICIONES DE LA PRESTACIÓN DEL SERVICIO.

“**EL PROVEEDOR**” se obliga a prestar a “**EL INSTITUTO**” el servicio que se menciona en la Cláusula Primera del presente instrumento jurídico, conforme a lo establecido en el Anexo Técnico y en los Términos y Condiciones integrados en el **Anexo ___ ()** de este instrumento jurídico, apegándose a las condiciones, alcances y características detalladas en la convocatoria, junta de aclaraciones (en su caso) y acta de _____ del procedimiento del cual deriva el presente contrato, disponibles para su consulta en el Portal de Compras Gubernamentales CompraNet.,

Se podrán acordar prórrogas al plazo originalmente pactado por caso fortuito, fuerza mayor o por causas atribuibles a “**EL INSTITUTO**”, lo cual deberá estar debidamente acreditado en el expediente de contratación respectivo. “**EL PROVEEDOR**” puede solicitar la modificación del plazo originalmente pactado cuando se actualicen y se acrediten los supuestos de caso fortuito o de fuerza mayor .



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

EN CASO DE EXISTA PARTICIPACIÓN CONJUNTA

“**EL PROVEEDOR**” convino en conjuntar sus recursos técnicos, legales, administrativos, económicos y financieros por lo que se obliga a prestar el servicio objeto del presente contrato en términos del convenio de participación conjunta.

“**EL PROVEEDOR**” conviene que en el supuesto de que cualquiera se declare en quiebra o suspensión de pagos, no los libera de cumplir con sus obligaciones, por lo que cualquiera de ellas que subsista, acepta y se obliga expresamente a responder solidariamente/mancomunada de las obligaciones contractuales a que hubiere lugar.

DÉCIMA PRIMERA. NORMAS, LICENCIAS, AUTORIZACIONES Y PERMISOS.

Los servicios, que de acuerdo al objeto del presente contrato se adquieran o contraten, deberán cumplir con las Normas Oficiales Mexicanas y con las Normas Mexicanas, según proceda, y a falta de éstas, con las Normas Internacionales, de conformidad con lo dispuesto en la Ley de Infraestructura de la Calidad; en su caso, con las normas de referencia o especificaciones técnicas y cumplir con las características y especificaciones requeridas en el Anexo Técnico y los Términos y Condiciones, que se agregan al presente contrato en el **Anexo _ ()**.

DÉCIMA SEGUNDA. SEGUROS.

En caso de aplicar, “**EL PROVEEDOR**” deberá entregar las pólizas de seguros y/o responsabilidad civil requeridas y cumpliendo con los requisitos señalados en el Anexo Técnico, Términos y Condiciones, que se agregan al presente contrato en el **Anexo _ ()**, y, en su caso, Junta de Aclaraciones, que se agrega al presente contrato en el **Anexo _ ()**.

DÉCIMA TERCERA. DEFECTOS Y VICIOS OCULTOS.

“**EL PROVEEDOR**” queda obligado ante “**EL INSTITUTO**” a responder de los defectos y vicios ocultos derivados de las obligaciones del presente contrato, así como de cualquier otra responsabilidad en que hubiere incurrido, en los términos señalados en este instrumento jurídico y sus respectivos anexos, así como la cotización y el requerimiento asociado a ésta, y/o en la legislación aplicable en la materia.

Para los efectos de la presente cláusula, se entiende por vicios ocultos los defectos que existan en los servicios que los hagan impropios para los usos a que se le destine o que disminuyan de tal modo este uso, que de haberlo conocido “**EL INSTITUTO**” no lo hubiere adquirido o los hubiere adquirido a un precio menor.

DÉCIMA CUARTA. RESPONSABILIDAD.

“**EL PROVEEDOR**” se obliga a responder por su cuenta y riesgo de los daños y/o perjuicios que por inobservancia o negligencia de su parte lleguen a causar a “**EL INSTITUTO**”, con



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

motivo de las obligaciones pactadas, o bien por los defectos o vicios ocultos en los servicios prestados, de conformidad con lo establecido en el artículo 53 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

DÉCIMA QUINTA. IMPUESTOS Y DERECHOS.

Los impuestos y/o derechos que procedan con motivo de los servicios objeto del presente contrato, serán pagados por “**EL PROVEEDOR**” conforme a la legislación aplicable en la materia.

“**EL INSTITUTO**” sólo cubrirá el Impuesto al Valor Agregado (I.V.A.), de acuerdo con lo establecido en las disposiciones fiscales vigentes en la materia, en caso de aplicar.

“**EL PROVEEDOR**”, en su caso, cumplirá con la inscripción de sus trabajadores en el régimen obligatorio del Seguro Social, así como con el pago de las cuotas obrero-patronales a que haya lugar, conforme a lo dispuesto en la Ley del Seguro Social. “**EL INSTITUTO**”, a través del Área fiscalizadora competente, podrá verificar en cualquier momento el cumplimiento de dicha obligación.

“**EL PROVEEDOR**” que tenga cuentas líquidas y exigibles a su cargo por concepto de cuotas obrero patronales, conforme a lo previsto en el artículo 40 B de la Ley del Seguro Social, acepta que “**EL INSTITUTO**” las compense con el o los pagos que tenga que hacerle por concepto de contraprestación por la prestación del servicio objeto de este contrato.

DÉCIMA SEXTA. PROHIBICIÓN DE CESIÓN DE DERECHOS Y OBLIGACIONES.

“**EL PROVEEDOR**” no podrá ceder total o parcialmente los derechos y obligaciones derivados del presente contrato, a favor de cualquier otra persona física o moral, con excepción de los derechos de cobro, en cuyo caso se deberá contar con la conformidad previa y por escrito de “**EL INSTITUTO**” deslindando a ésta de toda responsabilidad.

DÉCIMA SÉPTIMA. DERECHOS DE AUTOR, PATENTES Y/O MARCAS.

“**EL PROVEEDOR**” se obliga para con “**EL INSTITUTO**”, a responder por los daños y/o perjuicios que pudiera causar a “**EL INSTITUTO**” y/o a terceros, si con motivo de la prestación del servicio se violan derechos de autor, de patentes y/o marcas u otro derecho reservado a nivel Nacional o Internacional.

Por lo anterior, “**EL PROVEEDOR**” manifiesta en este acto bajo protesta de decir verdad, no encontrarse en ninguno de los supuestos de infracción a la Ley Federal del Derecho de Autor, ni a la Ley Federal de Protección a la Propiedad Industrial.

En caso de que sobreviniera alguna reclamación en contra de “**EL INSTITUTO**” por cualquiera de las causas antes mencionadas, la única obligación de éste será la de dar aviso en el



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

domicilio previsto en este instrumento jurídico a “**EL PROVEEDOR**”, para que éste lleve a cabo las acciones necesarias que garanticen la liberación de “**EL INSTITUTO**” de cualquier controversia o responsabilidad de carácter civil, mercantil, penal o administrativa que, en su caso, se ocasione.

Lo anterior de conformidad a lo establecido en el artículo 45, fracción XX de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

DÉCIMA OCTAVA. CONFIDENCIALIDAD.

“**LAS PARTES**” están conformes en que la información que se derive de la celebración del presente instrumento jurídico, así como toda aquella información que “**EL INSTITUTO**” entregue a “**EL PROVEEDOR**” tendrá el carácter de confidencial, por lo que este se compromete, de forma directa o a través de interpósita persona, a no proporcionarla o divulgarla por escrito, verbalmente o por cualquier otro medio a terceros, inclusive después de la terminación de este contrato.

La información contenida en el presente contrato es pública, de conformidad con lo dispuesto en los artículos 70 fracción XXVIII de la Ley General de Transparencia y Acceso a la Información Pública y 68 de la Ley Federal de Transparencia y Acceso a la Información Pública; sin embargo, la información que proporcione “**EL INSTITUTO**” a “**EL PROVEEDOR**” para el cumplimiento del objeto materia del mismo, será considerada como confidencial en términos de los artículos 116 y 113, respectivamente, de los citados ordenamientos jurídicos, por lo que “**EL PROVEEDOR**” se compromete a recibir, proteger y guardar la información confidencial proporcionada por “**EL INSTITUTO**” con el mismo empeño y cuidado que tiene respecto de su propia información confidencial, así como hacer cumplir a todos y cada uno de los usuarios autorizados a los que les entregue o permita acceso a la información confidencial, en los términos de este instrumento.

“**EL PROVEEDOR**” se compromete a que la información considerada como confidencial no será utilizada para fines diversos a los autorizados con el presente contrato; asimismo, dicha información no podrá ser copiada o duplicada total o parcialmente en ninguna forma o por ningún medio, ni podrá ser divulgada a terceros que no sean usuarios autorizados. De esta forma, “**EL PROVEEDOR**” se obliga a no divulgar o publicar informes, datos y resultados obtenidos objeto del presente instrumento, toda vez que son propiedad de “**EL INSTITUTO**”.

Cuando de las causas descritas en las cláusulas de **CAUSALES DE RESCISIÓN ADMINISTRATIVA DEL CONTRATO Y PROCEDIMIENTO DE RESCISIÓN** y **TERMINACIÓN ANTICIPADA**, del presente contrato, concluya la vigencia del mismo, subsistirá la obligación de confidencialidad sobre el servicio establecido en este instrumento legal.

En caso de incumplimiento a lo establecido en esta cláusula, “**EL PROVEEDOR**” tiene conocimiento en que “**EL INSTITUTO**” podrá ejecutar o tramitar las sanciones establecidas en la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y su Reglamento, así como presentar las denuncias correspondientes de conformidad con lo dispuesto por el Libro



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Segundo, Título Noveno, Capítulos I y II del Código Penal Federal y demás normatividad aplicable.

De igual forma, “**EL PROVEEDOR**” se compromete a no alterar la información confidencial, a llevar un control de su personal y hacer de su conocimiento las sanciones que se aplicarán en caso de incumplir con lo dispuesto en esta cláusula, por lo que, en su caso, se obliga a notificar a “**EL INSTITUTO**” cuando se realicen actos que se consideren como ilícitos, debiendo dar inicio a las acciones legales correspondientes y sacar en paz y a salvo a “**EL INSTITUTO**” de cualquier proceso legal.

“**EL PROVEEDOR**” se obliga a poner en conocimiento de “**EL INSTITUTO**” cualquier hecho o circunstancia que en razón del servicio prestados sea de su conocimiento y que pueda beneficiar o evitar un perjuicio a la misma.

Asimismo, “**EL PROVEEDOR**” no podrá, con motivo del servicio que preste a “**EL INSTITUTO**”, utilizar la información a que tenga acceso, para asesorar, patrocinar o constituirse en consultor de cualquier persona que tenga relaciones directas o indirectas con el objeto de las actividades que lleve a cabo.

DÉCIMA NOVENA. ADMINISTRACIÓN, VERIFICACIÓN, SUPERVISIÓN Y ACEPTACIÓN DEL SERVICIO.

“**EL INSTITUTO**” designa como responsable de administrar y vigilar el cumplimiento del presente contrato al C. (COLOCAR NOMBRE DEL ADMINISTRADOR DEL PRESENTE CONTRATO), (COLOCAR CARGO DEL ADMINISTRADOR DEL PRESENTE CONTRATO), con el objeto de verificar el óptimo cumplimiento del mismo, por lo que indicará a “**EL PROVEEDOR**” las observaciones que se estimen pertinentes, quedando éste obligado a corregir las anomalías que le sean indicadas, así como deficiencias en la prestación del servicio, de conformidad con lo establecido en el documento de designación de administrador del presente contrato que se agrega al presente y el artículo 84 penúltimo párrafo del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

En el caso de que se lleve a cabo un relevo institucional temporal o permanente con dicho servidor público de “**EL INSTITUTO**” tendrá carácter de ADMINISTRADOR DEL PRESENTE CONTRATO la persona que sustituya al servidor público en el cargo, conforme a la designación correspondiente.

Asimismo, “**EL INSTITUTO**” sólo aceptará el servicio materia del presente contrato y autorizará el pago de los mismos previa verificación de las especificaciones requeridas, de conformidad con lo especificado en el presente contrato y sus correspondientes anexos, así como la cotización y el requerimiento asociado a ésta.

El servicio será recibido previa revisión del administrador del presente contrato; la inspección del servicio consistirá en la verificación del cumplimiento de las especificaciones técnicas establecidas en el contrato y en su caso en los anexos respectivos, así como la cotización y el



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

requerimiento asociado a ésta.

En tal virtud, “**EL PROVEEDOR**” manifiesta expresamente su conformidad de que hasta en tanto no se cumpla de conformidad con lo establecido en el párrafo anterior, el servicio no se tendrá por aceptado por parte de “**EL INSTITUTO**”.

“**EL INSTITUTO**”, a través administrador del presente contrato o a través del personal que para tal efecto designe, podrá rechazar el servicio si no reúnen las especificaciones y alcances establecidos en este contrato, en su Anexo técnico y en los Términos y Condiciones, que se agregan al presente contrato en el **Anexo** (), obligándose “**EL PROVEEDOR**” en este supuesto a entregarlos nuevamente bajo su exclusiva responsabilidad y sin costo adicional para “**EL INSTITUTO**”

VIGÉSIMA. DEDUCCIONES.

Con fundamento en lo dispuesto en los artículos 53 Bis de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y 97 de su Reglamento, “**EL PROVEEDOR**”, por la entrega parcial o deficiente en la prestación del servicio, se hará acreedor a una sanción equivalente al (COLOCAR PORCENTAJE DE DEDUCTIVA) % del valor de lo incumplido, conforme a los conceptos señalados en el Anexo Técnico, los Términos y Condiciones, que se agregan al presente contrato en el **Anexo** (), y Junta de Aclaraciones, que se agrega al presente contrato en el **Anexo** (), en caso de aplicar.

El administrador del presente contrato será responsable del cálculo, aplicación y seguimiento de las deducciones. El monto máximo de aplicación de las deducciones no podrán ser mayor al que resulte de aplicar el porcentaje de la garantía de cumplimiento del presente contrato.

En caso de que se exceda se podrá proceder a la rescisión del presente contrato.

VIGÉSIMA PRIMERA. PENAS CONVENCIONALES.

De conformidad con lo establecido en los artículos 45, fracción XIX, 53 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, 95 y 96 de su Reglamento, la pena convencional aplicable a “**EL PROVEEDOR**”, por atraso en la prestación del servicio será (COLOCAR PORCENTAJE DE PENA CONVENCIONAL) %, (colocar periodicidad de pena), sin considerar el I.V.A., y se calculará conforme a lo señalado en los Términos y Condiciones, que se agregan al presente contrato en el **Anexo** () y, en su caso, la Junta de Aclaraciones, que se agrega al presente contrato en el **Anexo** ().

El administrador del presente contrato será el responsable de determinar, calcular y aplicar las penas convencionales, vigilando los correspondientes registro o captura y validación en el sistema PREI Millenium, así como de notificarlas a “**EL PROVEEDOR**” personalmente,



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

mediante oficio o por medios de comunicación electrónica.

“EL INSTITUTO” descontará las cantidades que resulten de aplicar la pena convencional, sobre los pagos que deba cubrir a **“EL PROVEEDOR”**. Por lo tanto, **“EL PROVEEDOR”** autoriza a descontar las cantidades que resulten de aplicar las sanciones señaladas en párrafos anteriores, sobre los pagos que éste deba cubrirle a **“EL INSTITUTO”** durante el período en que incurra y/o se mantenga en atraso con motivo de la prestación del servicio.

Para autorizar el pago de la prestación del servicio, previamente **“EL PROVEEDOR”** tiene que haber cubierto las penas convencionales aplicadas conforme a lo dispuesto en el presente contrato. El administrador del presente contrato será el responsable de verificar que se cumpla esta obligación, dentro de los 5 (cinco) días hábiles siguientes a la conclusión del atraso.

VIGÉSIMA SEGUNDA. SANCIONES ADMINISTRATIVAS.

Cuando **“EL PROVEEDOR”** incumpla con sus obligaciones contractuales por causas imputables a éste, y como consecuencia, cause daños y/o perjuicios graves a **“EL INSTITUTO”**, o bien, proporcione información falsa, actúe con dolo o mala fe en la celebración del presente contrato o durante la vigencia del mismo, por determinación de la Secretaría de la Función Pública, se podrá hacer acreedor a las sanciones establecidas en la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, en los términos de los artículos 59, 60 y 61 de dicho ordenamiento legal y 109 al 115 de su Reglamento.

VIGÉSIMA TERCERA. SANCIONES APLICABLES Y TERMINACIÓN DE LA RELACIÓN CONTRACTUAL

“EL INSTITUTO”, de conformidad con lo establecido en los artículos 53, 53 Bis, 54 y 54 Bis de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, y 86 segundo párrafo, 95 al 100 y 102 de su Reglamento, aplicará sanciones, o en su caso, llevará a cabo la cancelación de partidas total o parcialmente o la rescisión administrativa del presente contrato.

VIGÉSIMA CUARTA. RELACIÓN LABORAL.

“LAS PARTES” convienen en que **“EL INSTITUTO”** no adquiere ninguna obligación de carácter laboral para con **“EL PROVEEDOR”** ni para con los trabajadores que el mismo contrate para la realización del objeto del presente instrumento jurídico, toda vez que dicho personal depende exclusivamente de **“EL PROVEEDOR”**.

Por lo anterior, no se le considerará a **“EL INSTITUTO”** como patrón, ni aún substituto, y **“EL PROVEEDOR”** expresamente lo exime de cualquier responsabilidad de carácter civil, fiscal, de seguridad social, laboral o de otra especie, que en su caso pudiera llegar a generarse.

“EL PROVEEDOR” se obliga a liberar a **“EL INSTITUTO”** de cualquier reclamación de índole laboral o de seguridad social que sea presentada por parte de sus trabajadores, ante las autoridades competentes.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

VIGÉSIMA QUINTA. EXCLUSIÓN LABORAL.

“LAS PARTES” convienen en que **“EL INSTITUTO”** no adquiere ninguna obligación de carácter laboral con **“EL PROVEEDOR”** ni con los elementos que éste utilicen para la prestación del servicio objeto del presente contrato, por lo cual no se le podrá considerar como patrón ni como un sustituto. En particular el personal se entenderá relacionado exclusivamente con la o las personas que lo emplearon y por ende cada una de ellas asumirá su responsabilidad por dicho concepto.

Igualmente, y para este efecto y cualquiera no previsto, **“EL PROVEEDOR”** exime expresamente a **“EL INSTITUTO”** de cualquier responsabilidad laboral, civil, penal, de seguridad social o de otra especie que, en su caso, pudiera llegar a generarse; sin embargo, si **“EL INSTITUTO”** tuviera que realizar alguna erogación por alguno de los conceptos que anteceden, **“EL PROVEEDOR”** se obliga a realizar el reembolso e indemnización correspondiente.

Por lo anterior, **“LAS PARTES”** reconocen expresamente en este acto que **“EL INSTITUTO”** no tiene nexo laboral alguno con **“EL PROVEEDOR”**, por lo que éste último libera a **“EL INSTITUTO”** de toda responsabilidad relativa a cualquier accidente o enfermedad que pudiera sufrir o contraer cualquiera de sus trabajadores durante el desarrollo de sus labores o como consecuencia de ellos, así como de cualquier responsabilidad que resulte de la aplicación de la Ley Federal del Trabajo, de la Ley del Seguro Social, de la Ley del Instituto del Fondo Nacional de la Vivienda para los Trabajadores y/o cualquier otra aplicable, derivada de la prestación del servicio materia de este contrato.

VIGÉSIMA SEXTA. SUSPENSIÓN DE LA PRESTACIÓN DEL SERVICIO.

Cuando en la prestación del servicio, se presente caso fortuito o de fuerza mayor, **“EL INSTITUTO”** bajo su responsabilidad, podrá de resultar aplicable conforme a la normatividad en la materia, suspender el servicio, en cuyo caso únicamente se pagarán aquellos que hubiesen sido efectivamente recibidos por **“EL INSTITUTO”**.

Cuando la suspensión obedezca a causas imputables a **“EL INSTITUTO”**, a solicitud escrita de **“EL PROVEEDOR”**, cubrirá los gastos no recuperables, durante el tiempo que dure esta suspensión, para lo cual **“EL PROVEEDOR”** deberá presentar dentro de los 30 (treinta) días naturales siguientes de la notificación del término de la suspensión, la factura y documentación de los gastos no recuperables en que haya incurrido, siempre que estos sean razonables, estén debidamente comprobados y se relacionen directamente con el presente contrato.

“EL INSTITUTO -” pagará los gastos no recuperables, en moneda nacional (pesos mexicanos), dentro de los 45 (cuarenta y cinco) días naturales posteriores a la presentación de la solicitud debidamente fundada y documentada de **“EL PROVEEDOR”**, así como del CFDI o factura electrónica respectiva y documentación soporte.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

En caso de que “**EL PROVEEDOR**” no presente en tiempo y forma la documentación requerida para el trámite de pago, la fecha de pago se recorrerá el mismo número de días que dure el retraso.

El plazo de suspensión será fijado por “**EL INSTITUTO**”, a cuyo término en su caso, podrá iniciarse la terminación anticipada del presente contrato, o bien, podrá continuar produciendo todos los efectos legales, una vez que hayan desaparecido las causas que motivaron dicha suspensión.

VIGÉSIMA SÉPTIMA. CAUSALES DE RESCISIÓN ADMINISTRATIVA DEL PRESENTE CONTRATO Y PROCEDIMIENTO DE RESCISIÓN.

“**EL INSTITUTO**” podrá rescindir administrativamente este contrato sin más responsabilidad para el mismo y sin necesidad de resolución judicial, cuando “**EL PROVEEDOR**” incurra en cualquiera de las causales que se señalan en el Anexo Técnico, Términos y Condiciones, que se agregan al presente contrato en el **Anexo _ ()**, y las que se señalan a continuación:

1. Cuando no entregue la garantía de cumplimiento del presente contrato, a más tardar dentro de los 10 (diez) días naturales posteriores a la firma del mismo.
2. Cuando incurra en falta de veracidad total o parcial respecto a la información proporcionada para la celebración del presente contrato.
3. Cuando se compruebe que “**EL PROVEEDOR**” haya prestado el servicio con descripciones y características distintas a las pactadas en este contrato o cuando no los entregue conforme a las normas y/o calidad solicitadas por “**EL INSTITUTO**”.
4. Cuando se transmitan total o parcialmente, bajo cualquier título y a favor de otra persona física o moral, los derechos y obligaciones a que se refiere el presente documento, con excepción de los derechos de cobro, previa autorización de “**EL INSTITUTO**”.
5. Si la autoridad competente declara el concurso mercantil o cualquier situación análoga o equivalente que afecte el patrimonio de “**EL PROVEEDOR**”.
6. Cuando de manera reiterativa y constante, “**EL PROVEEDOR**” sea sancionado por parte de “**EL INSTITUTO**” con penalizaciones y/o deducciones sobre el mismo concepto de los servicios proporcionados, o por ubicarse en los límites de incumplimientos previstos en la cláusula de penas convencionales y/o deducciones del presente instrumento.
7. Cuando se incumplan o contravengan las disposiciones de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, su reglamento y los demás lineamientos que rigen en la materia.
8. En el supuesto de que la Comisión Federal de Competencia Económica, de acuerdo con sus facultades, notifique a “**EL INSTITUTO**” la sanción impuesta a “**EL PROVEEDOR**” con motivo de la colusión de precios en que hubiese incurrido durante el procedimiento de contratación, en contravención a lo dispuesto en la Ley Federal de Competencia Económica y artículo 34 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, en caso de aplicar.
9. Si “**EL PROVEEDOR**” no permite a “**EL INSTITUTO**” la administración y verificación a



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

que se refiere la cláusula correspondiente señalada en el presente contrato.

- 10.** Cuando incumpla, total o parcialmente, con cualesquiera de las obligaciones establecidas en el presente contrato y sus anexos.

“**EL INSTITUTO**”, en términos de lo dispuesto en el artículo 54 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, podrá rescindir administrativamente el presente contrato en cualquier momento, cuando “**EL PROVEEDOR**” incurra en incumplimiento de cualquiera de las obligaciones a su cargo, de conformidad con el procedimiento siguiente:

- a) Si “**EL INSTITUTO**” considera que “**EL PROVEEDOR**” ha incurrido en alguna de las causales de rescisión que se consignan en la Cláusula que antecede, lo hará saber a “**EL PROVEEDOR**” de forma indubitable por escrito, a efecto de que éste exponga lo que a su derecho convenga y aporte, en su caso, las pruebas que estime pertinentes, en un término de 5 (cinco) días hábiles, a partir de la notificación de la comunicación de referencia.
- b) Transcurrido el término a que se refiere el inciso anterior, se resolverá considerando los argumentos y pruebas que hubiere hecho valer.
- c) La determinación de dar o no por rescindido administrativamente el presente contrato, deberá ser debidamente fundada, motivada y comunicada por escrito a “**EL PROVEEDOR**” dentro de los 15 (quince) días hábiles siguientes, al vencimiento del plazo señalado en el inciso a), de esta Cláusula.

En el supuesto de que se rescinda este contrato, “**EL INSTITUTO**” no aplicarán las penas convencionales, ni su contabilización para hacer efectiva la garantía de cumplimiento de este instrumento jurídico.

En caso de que “**EL INSTITUTO**” determine dar por rescindido el presente contrato, se deberá formular y notificar un finiquito dentro de los 20 (veinte) días naturales siguientes a la fecha en que se notifique la rescisión, de conformidad con el artículo 99 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, en el que se hagan constar los pagos que, en su caso, deba efectuar “**EL INSTITUTO**” por concepto de la prestación del servicio por “**EL PROVEEDOR**” hasta el momento en que se determine la rescisión administrativa del presente contrato.

Iniciado un procedimiento de conciliación “**EL INSTITUTO**”, bajo su responsabilidad, podrá suspender el trámite del procedimiento de rescisión.

Si previamente a la determinación de dar por rescindido este contrato, “**EL PROVEEDOR**” proporciona el servicio, el procedimiento iniciado quedará sin efectos, previa aceptación y verificación de “**EL INSTITUTO**” por escrito, de que continúa vigente la necesidad de contar con el servicio y aplicando, en su caso, las penas convencionales correspondientes.

“**EL INSTITUTO**” podrá determinar no dar por rescindido este contrato, cuando durante el



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

procedimiento advierta que dicha rescisión pudiera ocasionar algún daño o afectación a las funciones que tiene encomendadas. En este supuesto, “**EL INSTITUTO**” elaborará un dictamen en el cual justifique que los impactos económicos o de operación que se occasionarían con la rescisión del contrato resultarían más inconvenientes.

De no darse por rescindido este contrato, “**EL INSTITUTO**” establecerá, con “**EL PROVEEDOR**”, un nuevo plazo para el cumplimiento de aquellas obligaciones que se hubiesen dejado de cumplir, a efecto de que “**EL PROVEEDOR**” subsane el incumplimiento que hubiere motivado el inicio del procedimiento de rescisión. Lo anterior se llevará a cabo a través de un convenio modificatorio en el que se atenderá a las condiciones previstas en los dos últimos párrafos del artículo 52 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

VIGÉSIMA OCTAVA. TERMINACIÓN ANTICIPADA.

De conformidad con lo establecido en el artículo 54 Bis de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, y 102 de su Reglamento, “**EL INSTITUTO**” podrá dar por terminado anticipadamente el presente contrato sin responsabilidad para éste y sin necesidad de que medie resolución judicial alguna, cuando concurran razones de interés general o bien cuando por causas justificadas se extinga la necesidad de requerir el servicio objeto del presente contrato, y se demuestre que de continuar con el cumplimiento de las obligaciones pactadas se occasionaría algún daño o perjuicio a “**EL INSTITUTO**” o se determine la nulidad de los actos que dieron origen al presente instrumento jurídico, con motivo de la resolución de una inconformidad o intervención de oficio emitida por la Secretaría de la Función Pública.

La terminación anticipada del presente contrato se sustentará mediante dictamen que precise las razones o las causas justificadas que den origen a la misma. Los gastos no recuperables por la terminación anticipada serán pagados siempre que éstos sean razonables, estén comprobados y se relacionen directamente con el presente instrumento jurídico.

VIGÉSIMA NOVENA. DISCREPANCIAS.

“**LAS PARTES**” convienen que, en caso de discrepancia entre la Convocatoria y/o solicitud de cotización, la propuesta económica de “**EL PROVEEDOR**” y el presente contrato, prevalecerá lo establecido en la Convocatoria y/o solicitud de cotización, junta de aclaraciones respectiva, en caso de aplicar, de conformidad con lo dispuesto por el artículo 81 fracción IV, del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

TRIGÉSIMA. CONCILIACIÓN.

“**LAS PARTES**” acuerdan que para el caso de que se presenten desavenencias derivadas de la ejecución y cumplimiento del presente contrato se someterán al procedimiento de conciliación establecido en los artículos 77, 78, 79 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, y 126 al 136 de su Reglamento y al Decreto por el que se



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

establecen las acciones administrativas que deberá implementar la Administración Pública Federal para llevar a cabo la conciliación o la celebración de convenios o acuerdos previstos en las leyes respectivas como medios alternativos de solución de controversias, publicado en el Diario Oficial de la Federación el 29 de abril de 2016.

La solicitud de conciliación se presentará mediante escrito, el cual contendrá los requisitos contenidos en el artículo 15 de la Ley Federal de Procedimiento Administrativo, además, hará referencia al número de contrato, al servidor público encargado de su administración, objeto, vigencia y monto del contrato, señalando, en su caso, sobre la existencia de convenios modificatorios, debiendo adjuntar copia de los instrumentos consensuales debidamente suscritos.

TRIGÉSIMA PRIMERA. DOMICILIOS.

“LAS PARTES” señalan como sus domicilios legales para todos los efectos a que haya lugar y que se relacionan en el presente contrato, los que se indican en el apartado de Declaraciones, por lo que cualquier notificación judicial o extrajudicial, emplazamiento, requerimiento o diligencia que en dichos domicilios se practique, será enteramente válida, al tenor de lo dispuesto en el Título Tercero del Código Civil Federal y sus correlativos en los Estados de la República Mexicana.

TRIGÉSIMA SEGUNDA. LEGISLACIÓN APLICABLE.

“LAS PARTES” se obligan a sujetarse estrictamente para la prestación del servicio objeto del presente contrato a todas y cada una de las cláusulas que lo integran, así como la cotización y el requerimiento asociado a ésta, a la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, su Reglamento; al Código Civil Federal; la Ley Federal de Procedimiento Administrativo; al Código Federal de Procedimientos Civiles; a la Ley Federal de Presupuesto y Responsabilidad Hacendaria y su Reglamento, el Acuerdo por el que se expide el protocolo de actuación en materia de contrataciones públicas, otorgamiento y prórroga de licencias, permisos, autorizaciones y concesiones y a las demás disposiciones jurídicas aplicables.

TRIGÉSIMA TERCERA. JURISDICCIÓN.

“LAS PARTES” convienen que, para la interpretación y cumplimiento de este contrato, así como para lo no previsto en el mismo, se someterán a la jurisdicción y competencia de los Tribunales Federales en la Ciudad de México, renunciando expresamente al fuero que pudiera corresponderles en razón de su domicilio actual o futuro.

FIRMANTES O SUSCRIPCIÓN.

Previa lectura y debidamente enteradas **“LAS PARTES”** del contenido, alcance y fuerza legal del presente contrato, en virtud de que se ajusta a la expresión de su libre voluntad y que su consentimiento no se encuentra afectado por dolo, error, mala fe, ni otros vicios de la voluntad,



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Lo firman y ratifican en todas sus partes, por triplicado, en la Ciudad de México, el _____, quedando un ejemplar en poder de “**EL PROVEEDOR**” y los restantes en poder de “**EL INSTITUTO**”.

Por lo anteriormente expuesto, tanto “**EL INSTITUTO**” como “**EL PROVEEDOR**”, declaran estar conformes y bien enterados de las consecuencias, valor y alcance legal de todas y cada una de las estipulaciones que el presente instrumento jurídico contiene, por lo que lo ratifican y firman electrónicamente en las fechas especificadas en cada firma electrónica.

POR:
“**EL INSTITUTO**”

NOMBRE	CARGO	R.F.C.
<u>(NOMBRE DEL REPRESENTANTE LEGAL DE “EL INSTITUTO”)</u>	<u>(CARGO DEL REPRESENTANTE LEGAL DE “EL INSTITUTO”)</u>	<u>(R.F.C. DEL REPRESENTANTE LEGAL DE “EL INSTITUTO”)</u>
<u>(NOMBRE DEL ADMINISTRADOR DEL PRESENTE CONTRATO)</u>	<u>(CARGO DEL ADMINISTRADOR DEL PRESENTE CONTRATO)</u>	<u>(R.F.C. DEL ADMINISTRADOR DEL PRESENTE CONTRATO)</u>

POR:
“**EL PROVEEDOR**”



GOBIERNO DE
MÉXICO



DIRECCIÓN DE ADMINISTRACIÓN
Unidad de Adquisiciones

Coordinación de Adquisición de Bienes y Contratación de Servicios
Coordinación Técnica de Adquisición de Bienes de Inversión y Activos
División de Contratación de Activos y Logística

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

NOMBRE

R.F.C.

(RAZÓN SOCIAL DE LA PERSONA FÍSICA (R.F.C. DE LA PERSONA FÍSICA O MORAL)
O MORAL)



DOCUMENTACION
LEGAL para firma de



**Ricardo
Flores
Magón**
Año de
PRECURSOR DE LA REVOLUCIÓN MEXICANA



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Anexo 15.- Modelo de convenio de proposición conjunta

CONVENIO DE PROPOSICIÓN CONJUNTA QUE CELEBRAN POR UNA PARTE _____, REPRESENTADA POR _____ EN SU CARÁCTER DE _____, A QUIEN EN LO SUCESIVO SE LE DENOMINARÁ “EL PARTICIPANTE A”, Y POR OTRA _____, REPRESENTADA POR _____, EN SU CARÁCTER DE _____, A QUIEN EN LO SUCESIVO SE LE DENOMINARÁ “EL PARTICIPANTE B”, Y CUANDO SE HAGA REFERENCIA A LOS QUE INTERVIENEN SE DENOMINARÁN “Las Partes”, AL TENOR DE LAS SIGUIENTES DECLARACIONES Y CLÁUSULAS.

1.1. “EL PARTICIPANTE A”, DECLARA QUE.:

1.1.1 ES UNA SOCIEDAD LEGALMENTE CONSTITUIDA, DE CONFORMIDAD CON LAS LEYES MEXICANAS, SEGÚN CONSTA EN EL TESTIMONIO DE LA ESCRITURA PÚBLICA (PÓLIZA) NÚMERO ___, DE FECHA ___, OTORGADA ANTE LA FE DEL LIC. ___ NOTARIO (CORREDOR) PÚBLICO NÚMERO ___, DEL ___, E INSCRITA EN EL REGISTRO PÚBLICO DE LA PROPIEDAD Y DE COMERCIO DE ___, EN EL FOLIO MERCANTIL ___ DE FECHA _____.

EL ACTA CONSTITUTIVA DE LA SOCIEDAD ___ (SI/NO) HA TENIDO REFORMAS Y MODIFICACIONES.

Nota. En su caso, se deberán relacionar las escrituras en que consten las reformas o modificaciones de la sociedad.

LOS NOMBRES DE SUS SOCIOS SON:

_____ CON REGISTRO FEDERAL DE CONTRIBUYENTES _____.

1.1.2 TIENE LOS SIGUIENTES REGISTROS OFICIALES. REGISTRO FEDERAL DE CONTRIBUYENTES NÚMERO ___ Y REGISTRO PATRONAL ANTE EL INSTITUTO MEXICANO DEL SEGURO SOCIAL NÚMERO ___.

1.1.3 SU REPRESENTANTE LEGAL CON EL CARÁCTER YA MENCIONADO, CUENTA CON LAS FACULTADES NECESARIAS PARA SUSCRIBIR EL PRESENTE CONVENIO, DE CONFORMIDAD CON EL CONTENIDO DEL TESTIMONIO DE LA ESCRITURA PÚBLICA NÚMERO ___ DE FECHA ___, OTORGADA ANTE LA FE DEL LIC. ___ NOTARIO PÚBLICO NÚMERO ___, DEL ___ E INSCRITA EN EL REGISTRO PÚBLICO DE LA PROPIEDAD Y DE COMERCIO, EN EL FOLIO MERCANTIL NÚMERO ___ DE FECHA ___, MANIFESTANDO “BAJO PROTESTA DE DECIR VERDAD”, QUE DICHAS FACULTADES NO LE HAN SIDO REVOCADAS, NI LIMITADAS O MODIFICADAS EN FORMA ALGUNA, A LA FECHA EN QUE SE SUSCRIBE EL PRESENTE INSTRUMENTO JURÍDICO.

EL DOMICILIO DEL REPRESENTANTE LEGAL ES EL UBICADO EN: _____.

1.1.4 SU OBJETO SOCIAL, ENTRE OTROS CORRESPONDE A. _____; POR LO QUE CUENTA CON LOS RECURSOS FINANCIEROS, TÉCNICOS, ADMINISTRATIVOS Y HUMANOS PARA OBLIGARSE, EN LOS TÉRMINOS Y CONDICIONES QUE SE ESTIPULAN EN EL



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

PRESENTE CONVENIO.

2.1 “EL PARTICIPANTE B”, DECLARA QUE:

2.1.1 ES UNA SOCIEDAD LEGALMENTE CONSTITUIDA DE CONFORMIDAD CON LAS LEYES DE LOS ESTADOS UNIDOS MEXICANOS, SEGÚN CONSTA EL TESTIMONIO (PÓLIZA) DE LA ESCRITURA PÚBLICA NÚMERO ___, DE FECHA ___, PASADA ANTE LA FE DEL LIC. ___ NOTARIO (CORREDOR) PÚBLICO NÚMERO ___, DEL ___, E INSCRITA EN EL REGISTRO PÚBLICO DE LA PROPIEDAD Y DEL COMERCIO, EN EL FOLIO MERCANTIL NÚMERO ___ DE FECHA ____.

EL ACTA CONSTITUTIVA DE LA SOCIEDAD ___ (SI/NO) HA TENIDO REFORMAS Y MODIFICACIONES.

Nota. En su caso, se deberán relacionar las escrituras en que consten las reformas o modificaciones de la sociedad.

LOS NOMBRES DE SUS SOCIOS SON:

_____ CON REGISTRO FEDERAL DE CONTRIBUYENTES _____.

2.1.2 TIENE LOS SIGUIENTES REGISTROS OFICIALES. REGISTRO FEDERAL DE CONTRIBUYENTES NÚMERO _____ Y REGISTRO PATRONAL ANTE EL INSTITUTO MEXICANO DEL SEGURO SOCIAL NÚMERO _____.

2.1.3 SU REPRESENTANTE LEGAL, CON EL CARÁCTER YA MENCIONADO, CUENTA CON LAS FACULTADES NECESARIAS PARA SUSCRIBIR EL PRESENTE CONVENIO, DE CONFORMIDAD CON EL CONTENIDO DEL TESTIMONIO DE LA ESCRITURA PÚBLICA NÚMERO ___ DE FECHA ___, PASADA ANTE LA FE DEL LIC. ___ NOTARIO PÚBLICO NÚMERO ___, DEL ___ E INSCRITA EN EL REGISTRO PÚBLICO DE LA PROPIEDAD Y DEL COMERCIO, EN EL FOLIO MERCANTIL NÚMERO ___ DE FECHA ___, MANIFESTANDO “BAJO PROTESTA DE DECIR VERDAD” QUE DICHAS FACULTADES NO LE HAN SIDO REVOCADAS, NI LIMITADAS O MODIFICADAS EN FORMA ALGUNA, A LA FECHA EN QUE SE SUSCRIBE EL PRESENTE INSTRUMENTO JURÍDICO.

EL DOMICILIO DE SU REPRESENTANTE LEGAL ES EL UBICADO EN _____.

2.1.4 SU OBJETO SOCIAL, ENTRE OTROS CORRESPONDE A. _____; POR LO QUE CUENTA CON LOS RECURSOS FINANCIEROS, TÉCNICOS, ADMINISTRATIVOS Y HUMANOS PARA OBLIGARSE, EN LOS TÉRMINOS Y CONDICIONES QUE SE ESTIPULAN EN EL PRESENTE CONVENIO.

3.1. “Las Partes” DECLARAN QUE:

3.1.1. CONOCEN LOS REQUISITOS Y CONDICIONES ESTIPULADAS EN LA CONVOCATORIA A



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

LA LICITACIÓN PÚBLICA NACIONAL _____.

3.1.2. MANIFIESTAN SU CONFORMIDAD EN FORMALIZAR EL PRESENTE CONVENIO, CON EL OBJETO DE PARTICIPAR CONJUNTAMENTE EN LA LICITACIÓN, PRESENTANDO PROPUESTA TÉCNICA Y ECONÓMICA, CUMPLIENDO CON LO ESTABLECIDO EN LA CONVOCATORIA DE LA LICITACIÓN Y CON LO DISPUESTO EN LOS ARTÍCULOS 34, DE LA LEY DE ADQUISICIONES, ARRENDAMIENTOS Y SERVICIOS DEL SECTOR PÚBLICO Y 44 DE SU REGLAMENTO.

3.1.3. SEÑALAN COMO DOMICILIO LEGAL PARA TODOS LOS EFECTOS QUE DERIVEN DEL PRESENTE CONVENIO, EL UBICADO EN _____. (MENTIONAR E IDENTIFICAR A CUÁNTOS INTEGRANTES CONFORMAN LA PROPOSICIÓN CONJUNTA PARA LA PRESENTACIÓN DE PROPUESTAS).

EXPUESTO LO ANTERIOR, LAS PARTES OTORGAN LAS SIGUIENTES.

CLÁUSULAS

PRIMERA.- OBJETO: “PROPOSICIÓN CONJUNTA”.

“Las Partes” CONVIENEN, EN CONJUNTAR SUS RECURSOS TÉCNICOS, LEGALES, ADMINISTRATIVOS, ECONÓMICOS Y FINANCIEROS PARA PRESENTAR PROPUESTA TÉCNICA Y ECONÓMICA EN LA LICITACIÓN PÚBLICA NACIONAL NÚMERO _____ Y EN CASO DE SER ADJUDICATARIO DEL CONTRATO, SE OBLIGAN A OTORGAR EL SERVICIO CONTRATADO OBJETO DEL CONVENIO, CON LA PARTICIPACIÓN SIGUIENTE.

PARTICIPANTE “A”. (DESCRIBIR LA PARTE QUE SE OBLIGA A SUMINISTRAR).

(CADA UNO DE LOS INTEGRANTES QUE CONFORMAN LA PROPOSICIÓN CONJUNTA PARA LA PRESENTACIÓN DE PROPUESTAS DEBERÁ DESCRIBIR LA PARTE QUE SE OBLIGA A ENTREGAR).

SEGUNDA.-REPRESENTANTE COMÚN Y OBLIGADO SOLIDARIO.

“Las Partes” ACEPTAN EXPRESAMENTE EN DESIGNAR COMO REPRESENTANTE COMÚN AL _____, A TRAVÉS DEL PRESENTE INSTRUMENTO, OTORGÁNDOLE PODER AMPLIO Y SUFFICIENTE, PARA ATENDER TODO LO RELACIONADO CON LAS PROPUESTAS TÉCNICA Y ECONÓMICA EN EL PROCEDIMIENTO DE LICITACIÓN, ASÍ COMO PARA SUSCRIBIR DICHAS PROPUESTAS.

ASIMISMO, CONVIENEN ENTRE SI EN CONSTITUIRSE EN FORMA CONJUNTA Y SOLIDARIA PARA COMPROMETERSE POR CUALQUIER RESPONSABILIDAD DERIVADA DEL CUMPLIMIENTO DE LAS OBLIGACIONES ESTABLECIDAS EN EL PRESENTE CONVENIO, CON RELACIÓN AL CONTRATO QUE SUS REPRESENTANTES LEGALES FIRMAN CON EL INSTITUTO MEXICANO DEL SEGURO SOCIAL (IMSS), DERIVADO DEL PROCEDIMIENTO DE CONTRATACIÓN _____, ACEPTANDO EXPRESAMENTE EN RESPONDER ANTE EL



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

IMSS POR LAS PROPUESTAS QUE SE PRESENTEN Y, EN SU CASO, DE LAS OBLIGACIONES QUE DERIVEN DE LA ADJUDICACIÓN DEL CONTRATO RESPECTIVO.

TERCERA.- DEL COBRO DE LAS FACTURAS.

"Las Partes" CONVIENEN EXPRESAMENTE, QUE "EL PARTICIPANTE¹⁷⁵ (LOS PARTICIPANTES, DEBERÁN INDICAR CUÁL DE ELLOS ESTARÁ FACULTADO PARA REALIZAR EL COBRO), PARA EFECTUAR EL COBRO DE LAS FACTURAS RELATIVAS AL SERVICIO QUE SE PROPORCIONE AL IMSS, CON MOTIVO DEL CONTRATO QUE SE DERIVE DE LA LICITACIÓN PÚBLICA NACIONAL NÚMERO _____.

CUARTA.- VIGENCIA.

"Las Partes" CONVIENEN, EN QUE LA VIGENCIA DEL PRESENTE CONVENIO SERÁ EL DEL PERÍODO DURANTE EL CUAL SE DESARROLLE EL PROCEDIMIENTO DE LA LICITACIÓN PÚBLICA NACIONAL NÚMERO _____, INCLUYENDO, EN SU CASO, DE RESULTAR ADJUDICADOS DEL CONTRATO, EL PLAZO QUE SE ESTIPULE EN ÉSTE Y EL QUE PUDIERA RESULTAR DE CONVENIOS DE MODIFICACIÓN.

QUINTA.-OBLIGACIONES.

"Las Partes" CONVIENEN EN QUE EN EL SUPUESTO DE QUE CUALQUIERA DE ELLAS QUE SE DECLARE EN QUIEBRA O EN SUSPENSIÓN DE PAGOS, NO LAS LIBERA DE CUMPLIR CON SUS OBLIGACIONES, POR LO QUE CUALQUIERA DE ELLAS QUE SUBSISTA, ACEPTE Y SE OBLIGA EXPRESAMENTE A RESPONDER SOLIDARIAMENTE DE LAS OBLIGACIONES CONTRACTUALES A QUE HUBIERE LUGAR.

"Las Partes" ACEPTAN Y SE OBLIGAN A PROTOCOLIZAR ANTE NOTARIO PÚBLICO EL PRESENTE CONVENIO, EN CASO DE RESULTAR ADJUDICADOS DEL CONTRATO QUE SE DERIVE DEL FALLO EMITIDO EN LA LICITACIÓN PÚBLICA NACIONAL NÚMERO _____ EN QUE PARTICIPAN Y, QUE EL PRESENTE INSTRUMENTO, DEBIDAMENTE PROTOCOLIZADO, FORMARÁ PARTE INTEGRANTE DEL CONTRATO QUE SUSCRIBAN LOS REPRESENTANTES LEGALES DE CADA INTEGRANTE Y EL IMSS.

LEÍDO QUE FUE EL PRESENTE CONVENIO POR "Las Partes" Y ENTERADOS DE SU ALCANCE Y EFECTOS LEGALES, ACEPTANDO QUE NO EXISTIÓ ERROR, DOLO, VIOLENCIA O MALA FE, LO RATIFICAN Y FIRMAN, DE CONFORMIDAD EN LA CIUDAD DE MÉXICO, EL DÍA _____ DE _____ DE 20____.

"EL PARTICIPANTE A"

NOMBRE Y CARGO
DEL APODERADO LEGAL

"EL PARTICIPANTE B"

NOMBRE Y CARGO
DEL APODERADO LEGAL



GOBIERNO DE
MÉXICO



DIRECCIÓN DE ADMINISTRACIÓN
Unidad de Adquisiciones

Coordinación de Adquisición de Bienes y Contratación de Servicios
Coordinación Técnica de Adquisición de Bienes de Inversión y Activos
División de Contratación de Activos y Logística

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

256

Durango No. 291. 5to. piso. Col. Roma Norte. Alcaldía Cuauhtémoc. C. P. 06700. CDMX.

www.imss.aob.mx





Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Anexo 16.- Nota informativa para participantes de países miembros de la Organización para la Cooperación y el Desarrollo Económico (OCDE)

El compromiso de México en el combate a la corrupción ha trascendido nuestras fronteras y el ámbito de acción del gobierno federal. En el plano internacional y como miembro de la Organización para la Cooperación y el Desarrollo Económico (OCDE) y firmante de la **Convención para combatir el cohecho de servidores públicos extranjeros en transacciones comerciales internacionales**, hemos adquirido responsabilidades que involucran a los sectores público y privado.

Esta Convención busca establecer medidas para prevenir y penalizar a las personas y a las empresas que prometan o den gratificaciones a funcionarios públicos extranjeros que participan en transacciones comerciales internacionales. Su objetivo es eliminar la competencia desleal y crear igualdad de oportunidades para las empresas que compiten por las contrataciones gubernamentales.

La OCDE ha establecido mecanismos muy claros para que los países firmantes de la Convención cumplan con las recomendaciones emitidas por ésta y en caso de México, iniciará en **noviembre de 2003** una segunda fase de **evaluación** – la primera ya fue aprobada- en donde un grupo de expertos verificará, entre otros:

- La compatibilidad de nuestro marco jurídico con las disposiciones de la Convención.
- El conocimiento que tengan los sectores público y privado de las recomendaciones de la Convención.

El resultado de esta evaluación **impactará** el grado de inversión otorgado a México por las agencias calificadores y la atracción de inversión extranjera.

Las **responsabilidades del sector público** se centran en:

- Profundizar las reformas legales que inició en 1999.
- Difundir las recomendaciones de la Convención y las obligaciones de cada uno de los actores comprometidos en su cumplimiento.
- Presentar casos de cohecho en proceso y concluidos (incluyendo aquellos relacionados con lavado de dinero y extradición).

Las **responsabilidades** del sector privado contemplan:

- **Las empresas:** adoptar esquemas preventivos como el establecimiento de códigos de conducta, de mejores prácticas corporativas (controles internos, monitoreo, información financiera pública, auditorías externas) y de mecanismos que prevengan el ofrecimiento y otorgamiento de recursos o bienes a servidores públicos, para obtener beneficios particulares o para la empresa.
- **Los contadores públicos:** realizar auditorías: no encubrir actividades ilícitas (doble contabilidad y transacciones indebidas, como asientos contables falsificados, informes





Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

financieros fraudulentos, transferencias sin autorización, acceso a los activos sin consentimiento de la gerencia); utilizar registros contables precisos; informar a los directivos sobre conductas ilegales.

• **Los abogados:** promover el cumplimiento y revisión de la Convención (imprimir el carácter vinculatorio entre ésta y la legislación nacional); impulsar los esquemas preventivos que deben adoptar las empresas.

Las **sanciones** impuestas a las personas físicas o morales (privados) y a los servidores públicos que incumplan las recomendaciones de la Convención, implican entre otras, privación de la libertad, extradición, decomiso y/o embargo de dinero o bienes.

Asimismo, es importante conocer que el pago realizado a servidores públicos extranjeros es perseguido y castigado independientemente de que el funcionario sea acusado o no. Las investigaciones pueden iniciarse por denuncia, pero también por otros medios, como la revisión de la situación patrimonial de los servidores públicos o la identificación de transacciones ilícitas, en el caso de las empresas.

El culpable puede ser perseguido en cualquier país firmante de la Convención, independientemente del lugar donde el acto de cohecho haya sido cometido.

En la medida que estos lineamientos sean conocidos por las empresas y los servidores públicos del país, estaremos contribuyendo a construir estructuras preventivas que impidan el incumplimiento de las recomendaciones de la convención y por tanto la comisión de actos de corrupción.

Por otra parte, es de señalar que el Código Penal Federal sanciona el cohecho en los siguientes términos:

Artículo 222.- Cometan el delito de cohecho:

I.- El servidor público que por sí, o por interpósito persona solicite o reciba ilícitamente para sí o para otro, dinero o cualquier beneficio, o acepte una promesa, para hacer o dejar de realizar un acto propio de sus funciones inherentes a su empleo, cargo o comisión;

II.- El que dé, prometa o entregue cualquier beneficio a alguna de las personas que se mencionan en el artículo 212 de este Código, para que haga u omita un acto relacionado con sus funciones, a su empleo, cargo o comisión, y

III.- El legislador federal que, en el ejercicio de sus funciones o atribuciones, y en el marco del proceso de aprobación del presupuesto de egresos respectivo, gestione o solicite:

a) La asignación de recursos a favor de un ente público, exigiendo u obteniendo, para sí o para un tercero, una comisión, dádiva o contraprestación, en dinero o en especie, distinta a la que le corresponde por el ejercicio de su encargo;

b) El otorgamiento de contratos de obra pública o de servicios a favor de determinadas



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

personas físicas o morales.

Se aplicará la misma pena a cualquier persona que gestione, solicite a nombre o en representación del legislador federal las asignaciones de recursos u otorgamiento de contratos a que se refieren los incisos a) y b) de este artículo.

Al que comete el delito de cohecho se le impondrán las siguientes sanciones:

Cuando la cantidad o el valor de la dádiva, de los bienes o la promesa no exceda del equivalente de quinientas veces el valor diario de la Unidad de Medida y Actualización en el momento de cometerse el delito, o no sea valuable, se impondrán de tres meses a dos años de prisión y de treinta a cien días multa.

Cuando la cantidad o el valor de la dádiva, los bienes, promesa o prestación excede de quinientas veces el valor diario de la Unidad de Medida y Actualización en el momento de cometerse el delito, se impondrán de dos a catorce años de prisión y de cien a ciento cincuenta días multa.

En ningún caso se devolverá a los responsables del delito de cohecho, el dinero o dádivas entregadas, las mismas se aplicarán en beneficio del Estado.

Capítulo XI Cohecho a servidores públicos extranjeros

Artículo 222 bis.- Se impondrán las penas previstas en el artículo anterior al que con el propósito de obtener o retener para sí o para otra persona ventajas indebidas en el desarrollo o conducción de transacciones comerciales internacionales, ofrezca, prometa o dé, por sí o por interpósita persona, dinero o cualquiera otra dádiva, ya sea en bienes o servicios:

I. A un servidor público extranjero, en su beneficio o el de un tercero, para que dicho servidor público gestione o se abstenga de gestionar la tramitación o resolución de asuntos relacionados con las funciones inherentes a su empleo, cargo o comisión;

II. A un servidor público extranjero, en su beneficio o el de un tercero, para que dicho servidor público gestione la tramitación o resolución de cualquier asunto que se encuentre fuera del ámbito de las funciones inherentes a su empleo, cargo o comisión, o

III. A cualquier persona para que acuda ante un servidor público extranjero y le requiera o le proponga llevar a cabo la tramitación o resolución de cualquier asunto relacionado con las funciones inherentes al empleo, cargo o comisión de este último.

Para los efectos de este artículo se entiende por servidor público extranjero, toda persona que desempeñe un empleo, cargo o comisión en el poder legislativo, ejecutivo o judicial o en un órgano público autónomo en cualquier orden o nivel de gobierno de un Estado extranjero, sea designado o electo; cualquier persona en ejercicio de una función para una autoridad, organismo o empresa pública o de participación estatal de un país extranjero; y cualquier funcionario o agente de un organismo u organización pública internacional.

Cuando alguno de los delitos comprendidos en este artículo se cometa en los supuestos a





GOBIERNO DE
MÉXICO



DIRECCIÓN DE ADMINISTRACIÓN

Unidad de Adquisiciones

Coordinación de Adquisición de Bienes y Contratación de Servicios

Coordinación Técnica de Adquisición de Bienes de Inversión y Activos

División de Contratación de Activos y Logística

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

que se refiere el artículo 11 de este Código, el juez impondrá a la persona moral hasta mil días multa y podrá decretar su suspensión o disolución, tomando en consideración el grado de conocimiento de los órganos de administración respecto del cohecho en la transacción internacional y el daño causado o el beneficio obtenido por la persona moral.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Anexo 17.- Declaracion de No Colusión Comisión Federal de Competencia Económica

(ESTE ESCRITO ES A SUGERENCIA DE LA COMISIÓN FEDERAL DE COMPETENCIA, SIENDO OPTATIVO AL LICITANTE LA PRESENTACIÓN DEL MISMO, NO SIENDO CAUSAL DE DESECHAMIENTO LA NO PRESENTACIÓN)

[Nombre del representante o representante común de ser éste el caso], en representación de [Nombre de la persona física o moral] (en adelante, e indistintamente, el “Oferente” o “Licitante”), presento la oferta adjunta (en adelante, la “Oferta”):

Para:

[Nombre y Clave del proceso en que participa]

Convocado por:

[Nombre de la Convocante] (en adelante, la Autoridad Convocante"),

Vengo a presentar por mí y en representación del Oferente, la siguiente declaración de integridad (en adelante, la “declaración de Integridad”):

1. He leído y entiendo los términos de la presente declaración de Integridad;

2. Comprendo que la Oferta que se acompaña será desechada si la declaración de Integridad no es verídica y no se ajusta al contenido referido;

3. Comprendo que si la declaración de Integridad no es verídica me expongo a incurrir personalmente y a comprometer la responsabilidad de mi representada, en ilícitos de carácter civil, penal y administrativo, y en especial de las penas en que incurre quien declara con falsedad ante autoridad distinta a la judicial, en términos del artículo 247 fracción I del Código Penal Federal. Lo anterior, sin perjuicio de las sanciones que en términos de las legislaciones aplicables a este procedimiento se contemplan;

4. Conozco la Ley Federal de Competencia Económica, en particular lo previsto en los artículos 9° y 35 fracciones I, IV, IX y X, así como el artículo 254 bis del Código Penal Federal;

5. Cada persona cuya firma aparece en la Oferta que se acompaña ha sido autorizada por el Oferente para definir los términos y condiciones de la Oferta y para firmarla, en su representación;

6. Para los propósitos de la presente declaración de Integridad y de la Oferta que se acompaña, entiendo que la palabra “Competidor” comprenderá cualquier persona física o moral, además del Oferente, afiliado o no con el Oferente, que:

- (a) Haya presentado o pueda presentar una Oferta en el presente proceso;
- (b) Podría potencialmente presentar una Oferta en el mismo proceso;



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

7. El Oferente declara que (maque con una X uno de los Siguientes cuadros):

- (a) [] se ha presentado a este proceso en forma independiente si mediar consulta, comunicación, acuerdo, arreglo, combinación o convenio con Competidor alguno;
- (b) [] sí ha entablado consultas, comunicaciones, arreglos, combinaciones, acuerdos o convenios con uno o más competidores respecto de esta convocatoria. En el documento(s) adjunto(s) declara toda información detallada, incluyendo los nombres de los Competidores y la naturaleza y razones de tales consultas, comunicaciones, acuerdos o convenios. [La información es especialmente relevante cuando la Oferta involucre propuestas conjuntas o esquemas de subcontratación. En este supuesto, se deberán incluir los términos y condiciones en que participarán las personas involucradas];

8. En particular y sin limitar la generalidad de los párrafos 7 (a) o 7 (b), no ha habido consulta, comunicación, acuerdo, arreglo, combinación o convenio con Competidor alguno en relación a:

- (a)** Precios;
- (b)** Métodos, factores o fórmulas empleadas para la determinación de precios;
- (c)** La intención o decisión de presentar o no una Oferta; o bien
- (d)** La presentación de una oferta que no cumple con las especificaciones del presente proceso; a excepción de lo expresamente estipulado en el párrafo 7 (b) anterior;

9. Además, no ha existido consulta, comunicación, acuerdo o convenio con Competidor alguno en cuanto a calidad, cantidad, especificaciones o detalles de envío de los productos o servicios referidos en este proceso, a excepción de lo expresamente autoriza la Autoridad Convocante o conforme a los hechos relevados en concordancia con el párrafo 7 (b) anterior;

10. Los términos de la Oferta que se adjunta no han sido ni serán revelados por el Oferente, para conocimiento de algún Competidor, en forma directa o indirecta con el objeto o efecto de manipular, fijar, o concentrar precios; manipular, establecer o concertar métodos, factores o fórmulas empleadas para la determinación de precios; afectar o inducir la intención o decisión de presentar o no una Oferta; o bien la presentación de una oferta que no cumple con las especificaciones del presente proceso.

Además, los términos de la oferta que se adjunta no han sido ni serán revelados por el Oferente, para conocimiento de algún Competidor, en forma directa o indirecta con el objeto o efecto de manipular, fijar, o concertar la calidad, cantidad, especificaciones o detalles de envío de los productos o servicios referidos en este proceso o conforme a lo expuesto en el párrafo 7 (b) anterior.

(Nombre y Firma)
(Fecha)



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Anexo 18.- Modelo de Fianza

FORMATO. FIANZA DE CUMPLIMIENTO DE CONTRATO

(Afianzadora)

Denominación social: _____ en lo sucesivo la "Afianzadora".

Domicilio: _____.

Autorización del Gobierno Federal para operar: _____. (especificar si fue Procedimiento de Licitación Pública, Invitación a Cuando Menos Tres Personas o Adjudicación Directa, y el número de éste)

Beneficiaria:

_____ (Nombre de la Entidad paraestatal), en lo sucesivo "la Beneficiaria".

Domicilio: _____.

El medio electrónico, por el cual se pueda enviar la fianza a "la Beneficiaria": _____.

Fiado (s): _____. (En caso de proposición conjunta, el nombre y datos de cada uno de ellos)

Nombre o denominación social: _____.

RFC: _____.

Domicilio: _____. (El mismo que aparezca en el contrato principal)

Datos de la póliza:

Número: _____. (Número asignado por la "Afianzadora")

Monto Afianzado: _____. (Con letra y número, sin incluir el Impuesto al Valor Agregado).

Moneda: _____.

Fecha de expedición: _____.

Obligación garantizada: El cumplimiento de las obligaciones estipuladas en el contrato en los términos de la Cláusula PRIMERA de la presente póliza de fianza.

Naturaleza de las Obligaciones: (Divisible o Indivisible, de conformidad con lo estipulado en el contrato).

Si es **Divisible** aplicará el siguiente texto: La obligación garantizada será divisible, por lo que, en caso de presentarse algún incumplimiento, se hará efectiva solo en la proporción correspondiente al incumplimiento de la obligación principal.

Si es **Indivisible** aplicará el siguiente texto: La obligación garantizada será indivisible y en caso de presentarse algún incumplimiento se hará efectiva por el monto total de las obligaciones garantizadas.

Datos del contrato, en lo sucesivo el "Contrato":

Número asignado por "la Contratante": _____.

Objeto: _____.

Monto del Contrato: _____. (Con número y letra, sin el Impuesto al Valor Agregado)



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Moneda: _____.

Fecha de suscripción: _____.

Tipo: Adquisiciones, Arrendamientos y Servicios.

Obligación contractual para la garantía de cumplimiento: (Divisible o Indivisible, de conformidad con lo estipulado en el contrato)

Procedimiento al que se sujetará la presente póliza de fianza para hacerla efectiva: El previsto en el artículo 279 de la Ley de Instituciones de Seguros y de Fianzas.

Competencia y Jurisdicción: Para todo lo relacionado con la presente póliza, el fiado, el fiador y cualesquier otro obligado, así como "la Beneficiaria", se someterán a la jurisdicción y competencia de los tribunales federales de _____ (precisar el lugar), renunciando al fuero que pudiera corresponderle en razón de su domicilio o por cualquier otra causa.

La presente fianza se expide de conformidad con lo dispuesto por los artículos 48, fracción II y último párrafo, y artículo 49, fracción II, de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, y 103 de su Reglamento.

Validación de la fianza en el portal de internet, dirección electrónica www.amig.org.mx

CLÁUSULAS GENERALES A QUE SE SUJETARÁ LA PRESENTE PÓLIZA DE FIANZA PARA

GARANTIZAR EL CUMPLIMIENTO DEL CONTRATO EN MATERIA DE
ADQUISICIONES, ARRENDAMIENTOS Y SERVICIOS.

PRIMERA. - OBLIGACIÓN GARANTIZADA.

Esta póliza de fianza garantiza el cumplimiento de las obligaciones estipuladas en el "Contrato" a que se refiere esta póliza y en sus convenios modificatorios que se hayan realizado o a los anexos del mismo, cuando no rebasen el porcentaje de ampliación indicado en la cláusula siguiente, aún y cuando parte de las obligaciones se subcontraten.

SEGUNDA. - MONTO AFIANZADO.

La "Afianzadora", se compromete a pagar a "la Beneficiaria", hasta el monto de esta póliza, que es _____ (con número y letra sin incluir el Impuesto al Valor Agregado) que representa el ____ % (señalar el porcentaje con letra) del valor del "Contrato".

La "Afianzadora" reconoce que el monto garantizado por la fianza de cumplimiento se puede modificar en el caso de que se formalice uno o varios convenios modificatorios de ampliación del monto del "Contrato" indicado en la carátula de esta póliza, siempre y cuando no se rebase el ____ % de dicho monto. Previa notificación del fiado y cumplimiento de los requisitos legales, la "Afianzadora" emitirá el documento modificatorio correspondiente o endoso para el solo efecto de hacer constar la referida ampliación, sin que se entienda que la obligación sea novada.

En el supuesto de que el porcentaje de aumento al "Contrato" en monto fuera superior a los indicados, la "Afianzadora" se reserva el derecho de emitir los endosos subsecuentes, por la diferencia entre ambos montos, sin embargo, previa solicitud del fiado, la "Afianzadora" podrá garantizar dicha diferencia y emitirá el documento modificatorio correspondiente.

La "Afianzadora" acepta expresamente que, en caso de requerimiento, se compromete a pagar el monto total afianzado, siempre y cuando en el "Contrato" se haya estipulado que la obligación garantizada es indivisible; de estipularse que es divisible, la "Afianzadora" pagará de forma



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

proporcional el monto de la o las obligaciones incumplidas.

TERCERA. - INDEMNIZACIÓN POR MORA.

La "Afianzadora", se obliga a pagar la indemnización por mora que en su caso proceda de conformidad con el artículo 283 de la Ley de Instituciones de Seguros y de Fianzas.

CUARTA. - VIGENCIA.

La fianza permanecerá vigente hasta que se dé cumplimiento a la o las obligaciones que garantice en los términos del "Contrato" y continuará vigente en caso de que "la Contratante" otorgue prórroga o espera al cumplimiento del "Contrato", en los términos de la siguiente cláusula.

Asimismo, esta fianza permanecerá vigente durante la substanciación de todos los recursos legales, arbitrajes o juicios que se interpongan con origen en la obligación garantizada hasta que se pronuncie resolución definitiva de autoridad o tribunal competente que haya causado ejecutoria.

De esta forma la vigencia de la fianza no podrá acotarse en razón del plazo establecido para cumplir la o las obligaciones contractuales.

QUINTA. - PRÓRROGAS, ESPERAS O AMPLIACIÓN AL PLAZO DEL CONTRATO.

En caso de que se prorrogue el plazo originalmente señalado o conceder esperas o convenios de ampliación de plazo para el cumplimiento del "Contrato" garantizado y sus anexos, el fiado dará aviso a la "Afianzadora", la cual deberá emitir los documentos modificatorios o endosos correspondientes.

La "Afianzadora" acepta expresamente garantizar la obligación a que esta póliza se refiere, aún en el caso de que se otorgue prórroga, espera o ampliación al fiado por parte de la "Contratante" para el cumplimiento total de las obligaciones que se garantizan, por lo que no se actualiza el supuesto de extinción de fianza previsto en el artículo 179 de la Ley de Instituciones de Seguros y de Fianzas, sin que se entienda novada la obligación.

SEXTA. - SUPUESTOS DE SUSPENSIÓN.

Para garantizar el cumplimiento del "Contrato", cuando concurren los supuestos de suspensión en los términos de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, su Reglamento y demás disposiciones aplicables, "la Contratante" deberá emitir el o las actas circunstanciadas y, en su caso, las constancias a que haya lugar. En estos supuestos, a petición del fiado, la "Afianzadora" otorgará el o los endosos conducentes, conforme a lo estatuido en el artículo 166 de la Ley de Instituciones de Seguros y de Fianzas, para lo cual bastará que el fiado exhiba a la "Afianzadora" dichos documentos expedidos por "la Contratante".

El aplazamiento derivado de la interposición de recursos administrativos y medios de defensa legales, no modifica o altera el plazo de ejecución inicialmente pactado, por lo que subsistirán inalterados los términos y condiciones originalmente previstos, entendiendo que los endosos que emita la "Afianzadora" por cualquiera de los supuestos referidos, formarán parte en su conjunto, solidaria e inseparable de la póliza inicial.

SÉPTIMA. - SUBJUDICIDAD.

La "Afianzadora" realizará el pago de la cantidad reclamada, bajo los términos estipulados en esta póliza de fianza, y, en su caso, la indemnización por mora de acuerdo a lo establecido en el artículo 283 de la Ley de Instituciones de Seguros y de Fianzas, aun cuando la obligación se encuentre subjúdice, en virtud de procedimiento ante autoridad judicial, administrativa o



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

tribunal arbitral, salvo que el fiado obtenga la suspensión de su ejecución, ante dichas instancias.

La "Afianzadora" deberá comunicar a "la Beneficiaria" de la garantía, el otorgamiento de la suspensión al fiado, acompañándole las constancias respectivas que así lo acrediten, a fin de que se encuentre en la posibilidad de abstenerse del cobro de la fianza hasta en tanto se dicte sentencia firme.

OCTAVA. - COAFIANZAMIENTO O YUXTAPOSICIÓN DE GARANTÍAS.

El coafianzamiento o yuxtaposición de garantías, no implicará novación de las obligaciones asumidas por la "Afianzadora" por lo que subsistirá su responsabilidad exclusivamente en la medida y condiciones en que la asumió en la presente póliza de fianza y en sus documentos modificatorios.

NOVENA. - CANCELACIÓN DE LA FIANZA.

La "Afianzadora" quedará liberada de su obligación fiadora siempre y cuando "la Contratante" le comunique por escrito, por conducto del servidor público facultado para ello, su conformidad para cancelar la presente garantía.

El fiado podrá solicitar la cancelación de la fianza para lo cual deberá presentar a la "Afianzadora" la constancia de cumplimiento total de las obligaciones contractuales. Cuando el fiado solicite dicha cancelación derivado del pago realizado por saldos a su cargo o por el incumplimiento de obligaciones, deberá presentar el recibo de pago correspondiente.

Esta fianza se cancelará cuando habiéndose cumplido la totalidad de las obligaciones estipuladas en el "Contrato", "la Contratante" haya calificado o revisado y aceptado la garantía exhibida por el fiado para responder por los defectos, vicios ocultos de los bienes entregados y por el correcto funcionamiento de los mismos o por la calidad de los servicios prestados por el fiado, respecto del "Contrato" especificado en la carátula de la presente póliza y sus respectivos convenios modificatorios.

DÉCIMA. - PROCEDIMIENTOS.

La "Afianzadora" acepta expresamente someterse al procedimiento previsto en el artículo 279 de la Ley de Instituciones de Seguros y de Fianzas para hacer efectiva la fianza.

DÉCIMA PRIMERA. -RECLAMACIÓN

"La Beneficiaria" podrá presentar la reclamación a que se refiere el artículo 279 de Ley de Instituciones de Seguros y de Fianzas en cualquier oficina, o sucursal de la Institución y ante cualquier apoderado o representante de la misma.

DÉCIMA SEGUNDA. - DISPOSICIONES APLICABLES.

Será aplicable a esta póliza, en lo no previsto por la Ley de Instituciones de Seguros y de Fianzas la legislación mercantil y a falta de disposición expresa el Código Civil Federal.

----- FIN DE TEXTO -----



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Anexo 19 Carta de autorización 32-D

Ciudad de México, a ____ de _____ de ____.

Instituto Mexicano del Seguro Social
Presente.

Quien al calce suscribe en mi carácter de (marque solo uno):

- Persona Física
- Representante Legal de Persona Moral
- Persona física, que presenta su propuesta en forma conjunta con las personas físicas y/o morales siguientes:

- Representante Legal de Persona Moral, que presenta su propuesta en forma conjunta con las personas físicas y/o morales siguientes:

Y con relación al procedimiento de contratación número _____, AUTORIZO que los funcionarios adscritos a la División de Contratos puedan acceder mediante los sistemas electrónicos que para tales efectos disponga la Dirección de Incorporación y Recaudación del Instituto Mexicano del Seguro Social, a la consulta en tiempo real y en línea de opinión de cumplimiento en materia de contribuciones se seguridad social del Instituto Mexicano del Seguro Social. Lo anterior, respecto del de la voz, de mi representada y/o mis representadas según corresponda.

En el entendido de que, de existir discrepancia entre la información consultada por los servidores públicos de la División de Contratos y la(s) opinión(es) de cumplimiento presentada(s) por el de la voz al momento de formalizar el instrumento jurídico respectivo, y aplicando el principio *pro homine*, prevalecerá(n) la(s) que favorezca(n) al de la voz, a mi representada y/o mis representadas según corresponda.

Atentamente

(nombre y firma)



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Anexo 20 Manifestación de servicios especializados

Instituto Mexicano del Seguro Social

Presente.

Quien al calce suscribe en mi carácter de (marque solo uno):

- Persona Física
- Representante Legal de Persona Moral
- Persona física, que presenta su propuesta en forma conjunta con las personas físicas y/o morales siguientes:

-
- Representante Legal de Persona Moral, que presenta su propuesta en forma conjunta con las personas físicas y/o morales siguientes:
-
-

Manifiesto, con relación al procedimiento de contratación número _____, lo siguiente (marque uno):

- A la fecha, **NO** me(nos) encuentro(encontramos) subcontratando algún servicio u obra especializada para llevar a cabo mis(nuestras) operaciones cotidianas, en el cumplimiento de mi(nuestro) objeto social, o para la prestación de servicios y/o enajenación de bienes que pretendo(pretendemos) realizar a favor de ese Instituto Mexicano del Seguro Social.
- A la fecha, **SI** me(nos) encuentro(encontramos) subcontratando algún servicio u obra especializada para llevar a cabo mis(nuestras) operaciones cotidianas, en el cumplimiento de mi(nuestro) objeto social, o para la prestación de servicios y/o enajenación de bienes que pretendo(pretendemos) realizar a favor de ese Instituto Mexicano del Seguro Social, con las siguientes personas físicas y/o morales:

Nombre o Razón Social	RFC	Número de Folio del Aviso presentado ante el Registro de Prestadoras de Servicios Especializados u Obras Especializadas

Atentamente

(nombre y firma)



GOBIERNO DE
MÉXICO



DIRECCIÓN DE ADMINISTRACIÓN

Unidad de Adquisiciones

Coordinación de Adquisición de Bienes y Contratación de Servicios

Coordinación Técnica de Adquisición de Bienes de Inversión y Activos

División de Contratación de Activos y Logística

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Anexo 21 Escrito de aceptación de las disposiciones del sistema CompraNet.

Ciudad de México, a ____ de _____ de 2022.

Instituto Mexicano del Seguro Social
Dirección de Administración
Unidad de Adquisiciones
Coordinación de Adquisición de Bienes y Contratación de Servicios
Coordinación Técnica de Adquisición de Bienes de Inversión y Activos
División de Contratación de Activos y Logística
Presente

Escrito en el que manifieste su aceptación de que se tendrán como no presentadas sus proposiciones y, en su caso, la documentación requerida, cuando el archivo electrónico en el que se contengan las proposiciones y/o demás información no pueda abrirse por tener algún virus informático o por cualquier otra causa ajena al IMSS, en términos de lo dispuesto por el numeral 29 del "Acuerdo por el que se establecen las disposiciones que deberán observar para la utilización del sistema electrónico de información pública gubernamental, denominado CompraNet".

Protesto lo necesario

(Nombre y Firma del Apoderado o Representante Legal del Licitante)



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Anexo 22 Manifiesto de conocer y registrarse en el Módulo de Formalización de Instrumentos Jurídicos

Para personas morales:

Instituto Mexicano del Seguro Social

Dirección de Administración

Unidad de Adquisiciones

Coordinación de Adquisición de Bienes y Contratación de Servicios

Coordinación Técnica de Adquisición de Bienes de Inversión y Activos

División de Contratación de Activos y Logística

Procedimiento Número: XX-050GYR019-EXX-2022

_____, en mi carácter de _____, de la ___(persona moral)___, conozco y estaré a lo establecido en los artículos tercero, cuarto y demás aplicables del ACUERDO por el que se incorpora como un módulo de CompraNet la aplicación denominada Formalización de Instrumentos Jurídicos y se emiten las Disposiciones de carácter general que regulan su funcionamiento, publicado en el Diario Oficial de la Federación el pasado 18 de septiembre de 2020, donde se determina que todo instrumento jurídico que derive de algún procedimiento de contratación realizado por las Dependencias y Entidades, se deberá utilizar la firma electrónica avanzada (e.firma) que emite el Servicio de Administración Tributaria como medio de identificación.

En consecuencia, en caso de resultar adjudicado, manifiesto mi compromiso para registrarme en el Módulo de Formalización de Instrumentos Jurídicos.

Asimismo, es de mi conocimiento que se puede consultar el material de apoyo para el registro en el citado módulo, en la liga electrónica:
<https://www.gob.mx/compranet/documentos/modulo-de-formalizacion-de-instrumentos-juridicos>

(Nombre y firma del licitante o representante legal de la persona moral)



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

Para persona físicas:

Instituto Mexicano del Seguro Social
Dirección de Administración
Unidad de Adquisiciones
Coordinación de Adquisición de Bienes y Contratación de Servicios
Coordinación Técnica de Adquisición de Bienes de Inversión y Activos
División de Contratación de Activos y Logística

Procedimiento Número: XX-050GYR019-EXX-2022

Conozco y estaré a lo establecido en los artículos tercero, cuarto y demás aplicables del ACUERDO por el que se incorpora como un módulo de CompraNet la aplicación denominada Formalización de Instrumentos Jurídicos y se emiten las Disposiciones de carácter general que regulan su funcionamiento, publicado en el Diario Oficial de la Federación el pasado 18 de septiembre de 2020, donde se determina que todo instrumento jurídico que derive de algún procedimiento de contratación realizado por las Dependencias y Entidades, se deberá utilizar la firma electrónica avanzada (e.firma) que emite el Servicio de Administración Tributaria como medio de identificación.

En consecuencia, en caso de resultar adjudicado el respectivo instrumento jurídico se suscribirá en el Módulo de Formalización de Instrumentos Jurídicos, por lo que se deberá estar registrado.

Asimismo, es de mi conocimiento que se puede consultar el material de apoyo para el registro en el citado módulo, en la liga electrónica:
<https://www.gob.mx/compranet/documentos/modulo-de-formalizacion-de-instrumentos-juridicos>

(Nombre y firma del licitante)



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

GLOSARIO DE TÉRMINOS

Para efectos de ésta convocatoria, se entenderá por:

Administrador del contrato: Servidor(es) público(s) en quien recae la responsabilidad de administrar y verificar el cumplimiento de los derechos y obligaciones establecidas en el contrato.

ALSC: Administración Local de Servicios al Contribuyente.

Área contratante: La facultada en el IMSS para llevar a cabo los procedimientos de contratación a efecto de adquirir o arrendar bienes, así como para pactar la prestación de servicios.

Área requirente: La que en el IMSS, solicite o requiera formalmente la adquisición o arrendamiento de bienes o la prestación de servicios, o bien aquella que los utilizará, en términos de lo que establece la fracción II del artículo 2 del Reglamento.

Área técnica: La responsable de elaborar las especificaciones técnicas que se deberán incluir en el procedimiento de contratación, de responder las preguntas que sobre estos aspectos técnicos realicen los licitantes; así como de realizar la evaluación de las propuestas técnicas. El Área Técnica, podrá tener también el carácter de Área Requirente; para el presente procedimiento de contratación, en términos de lo que establece la fracción III del artículo 2 del Reglamento.

CABCS: Coordinación de Adquisición de Bienes y Contratación de Servicios.

CECOBAN: Centro de Compensación Bancaria.

COMPRANET: El Sistema Electrónico de información pública gubernamental sobre adquisiciones, arrendamientos, servicios, obras públicas y servicios relacionados con las mismas con dirección electrónica en Internet: <http://compranet.funcionpublica.gob.mx>.

Contrato: Documento a través del cual se formalizan los derechos y obligaciones derivados del Fallo del procedimiento de contratación de la adquisición o arrendamiento de bienes o la prestación de los servicios.

Convocatoria: El documento que contiene los requisitos de carácter legal, técnico y económico con respecto de los servicios objeto de la contratación y las personas interesadas en proveerlos o prestarlos, así como los términos a que se sujetará el procedimiento de contratación respectivo y los derechos y obligaciones de las partes, de conformidad al MAAGMAASSP.

CUCOP: Clasificador Único de Contrataciones Públicas

DOF: Diario Oficial de la Federación.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

EMA (Entidad Mexicana de Acreditación): Entidad de gestión privada en nuestro país, que tiene como objetivo acreditar a los Organismos de la Evaluación de la Conformidad que son los laboratorios de ensayo, laboratorios de calibración, laboratorios clínicos, unidades de verificación (organismos de inspección) y organismos de certificación.

Entidad Convocante: Instituto Mexicano del Seguro Social (IMSS).

Escrito Libre: Documento que deberá cumplir como mínimo con los datos requeridos en la Convocatoria, sin importar el orden y/o ubicación del contenido.

IMSS o Instituto: Instituto Mexicano del Seguro Social.

INFONAVIT: Instituto del Fondo Nacional de la Vivienda para los Trabajadores.

Investigación de mercado: La verificación de la existencia de bienes, arrendamientos o servicios, de proveedores a nivel nacional o internacional y del precio estimado basado en la información que se obtenga en la propia dependencia o entidad, de organismos públicos o privados, de fabricantes de bienes o prestadores del servicio, o una combinación de dichas fuentes de información.

IVA: Impuesto al Valor Agregado.

ISR: Impuesto Sobre la Renta

LAASSP: Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

LFCE: Ley Federal de Competencia Económica.

Licitante: La persona que participa en los procedimientos de Licitación Pública.

LIC: Ley de Infraestructura de la Calidad.

Manual o MAAGMAASSP: Manual Administrativo de Aplicación General en Materia de Adquisiciones, Arrendamientos y Servicios del Sector Público.

Medio de Identificación Electrónica: Conjunto de datos electrónicos asociados con documentos que son utilizados para reconocer a su autor, y que legitiman el consentimiento de éste para obligarlo a las manifestaciones que en él se contienen, de conformidad con el artículo 27 de la LAASSP.

Medios remotos de comunicación electrónica: Los dispositivos tecnológicos para efectuar transmisión de datos e información a través de computadoras, líneas telefónicas, enlaces dedicados, microondas y similares.

MIPYMES: Las micro, pequeñas y medianas empresas de nacionalidad mexicana a que hace referencia la Ley para el Desarrollo de la Competitividad de la Micro, Pequeña y Mediana Empresa.



Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

NOM: Norma Oficial Mexicana.

Normas: Las Normas Oficiales Mexicanas, las Normas Estándar (antes Mexicana), según proceda, y a falta de éstas, las Normas Internacionales, de conformidad con lo dispuesto por los artículos 64 y 84 de la Ley de Infraestructura de la Calidad en su caso, las normas de referencia o especificaciones a que se refiere el artículo 67 de la Ley antes citada.

OIC: Órgano Interno de Control en el IMSS.

Partida o concepto.- La división o desglose de los bienes a adquirir y/o arrendar o de los servicios a contratar, contenidos en un procedimiento de contratación o en un contrato, para diferenciarlos unos de otros, clasificarlos o agruparlos.

Penas Convencionales: Son aquellas que se derivan por atraso en el cumplimiento de las fechas pactadas para la entrega de los bienes y/o servicios, misma que no excederá del monto de la garantía del contrato, y será determinada en función de los bienes y/o servicios no entregados oportunamente.

POBALINES.- Las políticas, bases y lineamientos a que se refieren el párrafo séptimo del artículo 1 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

PMR: Precio Máximo de Referencia.

Proveedor: La persona física o moral que celebre contratos de adquisiciones, arrendamientos o servicios.

Reglamento: Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

Resolución miscelánea fiscal: Publicación anual en el DOF que agrupa disposiciones de carácter general, aplicables a impuestos, productos, aprovechamientos, contribuciones de mejoras y derechos federales, excepto a los relacionados con el comercio exterior.

RFC.- Registro Federal de Contribuyentes.

SAT: Servicio de Administración Tributaria.

SE: Secretaría de Economía.

SFP: Secretaría de la Función Pública.

SHCP: Secretaría de Hacienda y Crédito Público.

SSA: Secretaría de Salud.

Sobre cerrado: Cualquier medio que contenga la proposición del licitante, cuyo contenido solo puede ser conocido en el Acto de Presentación y Apertura de Proposiciones, en términos



GOBIERNO DE
MÉXICO



DIRECCIÓN DE ADMINISTRACIÓN
Unidad de Adquisiciones

Coordinación de Adquisición de Bienes y Contratación de Servicios
Coordinación Técnica de Adquisición de Bienes de Inversión y Activos
División de Contratación de Activos y Logística

Licitación Pública Nacional Electrónica Número LA-050GYR019-E182-2022

de la Ley.

Testigo Social: Mecanismo de participación ciudadana en la gestión de las contrataciones públicas, con un diseño institucional que favorece la incidencia de la sociedad civil en la adecuada construcción de la acción pública en la materia.

UMAE's: Unidades Médicas de Alta Especialidad, **son órganos de operación administrativa desconcentrada** del Instituto Mexicano del Seguro Social, en términos de lo establecido en el artículo 2 fracción IV del Reglamento Interior del Instituto Mexicano del Seguro Social.