



**INSTITUTO MEXICANO DEL SEGURO SOCIAL
DIRECCIÓN DE INNOVACIÓN Y DESARROLLO TECNOLÓGICO**

HOJA 1 DE 5

Formato SGMP F05
Apéndice MST

VERSIÓN 5.0

Apéndice “Seguridad Perimetral para el servicio de CCIMSS”

**INSTITUTO MEXICANO DEL SEGURO SOCIAL
DIRECCIÓN DE INNOVACIÓN Y DESARROLLO TECNOLÓGICO**

Apéndice

**“Seguridad Perimetral para el servicio de CCIMSS”
2018 – 2019**



Apéndice “Seguridad Perimetral para el servicio de CCIMSS”

Especificación Técnica Especificaciones del FW para la operación del Call Center.

Servicio de Protección Perimetral:

El “posible proveedor” deberá ofrecer en su solución, la infraestructura necesaria (hardware y software) que cumpla con las funcionalidades descritas de seguridad referida en el presente apéndice de seguridad perimetral, lo anterior será con lo que deberá contar el licitante en sus instalaciones, para el caso de las instalaciones del Instituto cada licitante deberá integrar en su proposición todo lo necesario para implementar la campaña de que se trate, incluyendo la infraestructura necesaria (equipo activo, ejemplo switches de telecomunicaciones, y pasivo de telecomunicaciones, ejemplo, elementos de cableado estructurado, fibra óptica, canalizaciones, ducterías, cross connection, es decir todo lo requerido para habilitar el servicio solicitado), debiendo al menos contar con las siguientes características

- Red perimetral con zonas DMZ para intercambio de información.
- Incluir interfaces de al menos 1 GigaEthernet
- 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.
- Incluir la facilidad 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.
- Soportar e incluir alta disponibilidad en modo Activo/Activo y Activo/Pasivo.
- 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.
- Integrar esquemas de autenticación que soporten servicios TACACS, RADIUS, LDAP, así como certificados digitales.
- Permitir e incluir la funcionalidad de almacenar una base de usuarios local que permita realizar autenticación, sin depender de un dispositivo externo.
- Capaz de establecer túneles VPN IPSEC/SSL con las siguientes características y especificaciones:
 - Deberá incluir lo necesario para soportar DES, 3DES y AES-256 para las fases I y II de IKE.
 - Deberá incluir lo necesario para 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 incluir lo necesario para soportar integridad de datos con md5, sha1 y sha2.
 - Deberá incluir lo necesario para soportar las topologías VPNs site-to-site: Meshed (todos a todos) y Star (Oficinas Remotas a Sitio Central).
 - Deberá incluir lo necesario para soportar VPNs client-to-site basadas en IPSEC.



Apéndice “Seguridad Perimetral para el servicio de CCIMSS”

- Deberá incluir lo necesario para establecer VPNs con gateways con direcciones IP dinámicas públicas.
- Deberá incluir lo necesario para crear una única asociación de seguridad (SA) por par de redes o subredes.
- Deberá incluir lo necesario para realizar VPNs SSL.
- Deberá incluir lo necesario para 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).
- Deberá incluir lo necesario para soportar la conexión de dispositivos móviles a través de un cliente de acceso remoto específico. Dicho cliente debe soportar al menos las siguientes plataformas: MAC OS X desde v10.4.10, iOS desde v4, Android desde v4.2, Windows desde v7, BlackBerry OS desde v5.0
- Incluir diferente modos de administración del sistema vía Web (HTTPS), por línea de comando (SSH), SNMPv3 y a través de una consola central de administración.
- Contar y operar al menos con una interface Gigabit Ethernet dedicada para administración.
- Incluir la funcionalidad de generación de logs de 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.
- Inspección de tráfico por medio del firewall en la capa de aplicación.
- 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, debe ser capaz de regresar a la configuración anterior, si es necesario o requerido.
- Debe incluir lo necesario para contar con la capacidad de asignar el control a diferentes administradores, como mínimo, en cuatro (4) niveles de acceso.

Redes Privadas Virtuales – VPN

- Capacidad para incluir un sistema operativo endurecido propietario del fabricante, que reciba actualizaciones y parches de software conforme sean publicadas.
- Capacidad para incluir la creación de 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.
- Soportar e incluir alta disponibilidad en modo Activo/Activo y Activo/Pasivo.
- Capacidad para integrar esquemas de autenticación que soporten servicios TACACS, RADIUS, LDAP y/o certificados digitales.
- Debe incluir lo necesario para almacenar una base de usuarios local que permita realizar autenticación, sin depender de un dispositivo externo.
- Debe incluir lo necesario para contar con la capacidad de crear hasta 5,000 túneles de VPN IPSec (sitio a sitio y cliente remoto)
- Deberá incluir lo necesario para soportar DES, 3DES y AES-256 para las fases I y II de IKE.



Apéndice “Seguridad Perimetral para el servicio de CCIMSS”

- Debe incluir lo necesario para Soportar al menos los siguientes grupos Diffie-Hellman: Grupo 1 (768 bit), Grupo 2 (1024 bit), Grupo 5 (1536 bit), Grupo 14 (2048 bit).
- Debe incluir lo necesario para soportar integridad de datos con md5, sha1 y sha2.
- Debe incluir lo necesario para soportar las topologías VPNs site-to-site: Meshed (todos a todos) y Star (Oficinas Remotas a Sitio Central).
- Debe incluir lo necesario para establecer VPNs con gateways con direcciones IP dinámicas públicas.
- Debe incluir lo necesario para crear una única asociación de seguridad (SA) por par de redes o subredes.
- Debe incluir lo necesario para contar con una capacidad para realizar VPNs SSL.
- Debe incluir lo necesario para contar una capacidad para 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).
- Deberá incluir lo necesario para soportar la conexión de dispositivos móviles a través de un cliente de acceso remoto específico. Dicho cliente debe soportar al menos las siguientes plataformas: MAC OS X desde v10.4.10, iOS desde v4, Android desde v4.2, Windows desde v7, BlackBerry OS desde v5.

Firman al calce las áreas responsables:

Area Técnica	Nombre	Firma
Coordinación de Sistemas de Infraestructura Tecnológica Institucional.	Ing.Eduardo Oropeza Ortiz Titular de la Coordinación de Sistemas de Infraestructura Tecnológica Institucional	
	Carlos Rincón Domínguez Titular de la Coordinación Técnica de Redes y Telecomunicaciones y encargado de la División de Telecomunicaciones	
Coordinación de Mantenimiento y Operación de Servicios de Cómputo	Lic. Omar Saúl Hernández García Titular de la Coordinación de Mantenimiento y Operación de Servicios de Cómputo	
	Ing. Gabriel Arturo Barrón Montiel Titular de la Coordinación Técnica de Seguridad de Tecnologías de la Información y Comunicaciones	



INSTITUTO MEXICANO DEL SEGURO SOCIAL
DIRECCIÓN DE INNOVACIÓN Y DESARROLLO TECNOLÓGICO

HOJA 5 DE 5

Formato SGMP F05
Apéndice MST

VERSIÓN 5.0

Apéndice “Seguridad Perimetral para el servicio de CCIMSS”

Ing. Abraham Gutiérrez Castillo
Titular de la División de Seguridad
Informática Integral