CONSOLA DE ADMINISTRACIÓN DE “FIREWALL” PARA SEGURIDAD DE ACCESO A REDES DE SUBESTACIÓN

ESPECIFICACIÓN
CFE G0100-10

DICIEMBRE 2011

MÉXICO

P R E F A C I O

Esta **especificación** ha sido elaborada de acuerdo con las Bases Generales para la Normalización en CFE. La propuesta de revisión fue preparada por la **Subdirección de Transmisión.**

Revisaron y aprobaron la presente **especificación** las áreas siguientes:

COORDINACIÓN DE PROYECTOS DE TRANSMISIÓN Y TRANSFORMACIÓN

GERENCIA DE ABASTECIMIENTOS

GERENCIA DE LAPEM

GERENCIA DE TECNOLOGIAS DE INFORMÁCIÓN

SUBDIRECCIÓN DE TRANSMISIÓN

El presente documento normalizado entra en vigor a partir de la fecha abajo indicada y será actualizado y revisado tomando como base las observaciones que se deriven de la aplicación del mismo. Dichas observaciones deben enviarse a la Gerencia de **LAPEM**, cuyo Departamento de Normalización y Metrología coordinará la revisión.

AUTORIZO:

ING. LUIS JAVIER FREYRE RIZO
GERENTE DEL LAPEM

NOTA: Entra en vigor a partir de: 120224

111223											

C O N T E N I D O

1 OBJETIVO

Establecer las características técnicas de calidad, requerimientos y los servicios de apoyo técnico que deben reunir los equipos, accesorios y elementos que conforman la consola de monitoreo y administración de los “firewall” para la implementación de seguridad de acceso a las redes de las subestaciones.

2 CAMPO DE APLICACIÓN

En la seguridad en redes de datos de Subestaciones de Potencia en el proceso operativo de los equipos. Esta especificación debe actuar en la aplicación de proyectos de Subestaciones nuevas, ampliaciones y modernización.

3 NORMAS QUE APLICAN

NOM-008-SCFI-2002	Sistema General de Unidades de Medida.
IEC 60068-2-1-2007	Environmental testing - Part 2-1: Tests - Test A: Cold.
IEC 60068-2-2-2007	Environmental testing - Part 2-2: Tests - Test B: Dry heat.
IEC 60068-2-3-1969	Basic Environmental Testing Procedures Part 2: Tests – Tests Ca. Damp Heat, Steady State.
IEC 60068-2-6-2007	Environmental Testing Part 2: Test – Test FC: Vibration (Sinusoidal).
IEC 61000-4-2-2008	Electromagnetic Compatibility (EMC) - Part 4-2: Testing and Measurement Techniques - Electrostatic Discharge Immunity Test.
IEC 61000-4-3-2010	Amendment 2 - Electromagnetic Compatibility (EMC) - Part 4-3: Testing and Measurement Techniques - Radiated, Radio-Frequency, Electromagnetic Field Immunity Test.
IEC 61000-4-4-2011	Electromagnetic Compatibility (EMC) - Part 4-4: Testing and Measurement Techniques - Electrical fast Transient/burst Immunity Test.
IEC 61000-4-11-2010	Interpretation Sheet 1 - Electromagnetic Compatibility (EMC) - Part 4-11: Testing and Measurement Techniques - Voltage Dips, Short Interruptions and Voltage Variations Immunity Tests.
NRF-001-CFE-2007	Empaque, Embalaje, Embarque, Transporte, Descarga, Recepción y Almacenamiento de Bienes Muebles Adquiridos por CFE.
NRF-002-CFE-2009	Manuales, Procedimientos e Instructivos Técnicos.
CFE L0000-36-2005	Consideraciones económicas en la Supervisión del Montaje, Pruebas y Puesta en Servicio.
CFE U0000-11-1991	Pruebas para Evaluar el Comportamiento del Equipo Electrónico en Condiciones de Operación.
CFE G0100-12-2011	Equipo para Seguridad de Redes en Subestaciones Eléctricas.

UIT-T X.509 Information Technology – Open Systems Interconnection – The Directory: Public-key and Attribute Certificate Frameworks.

NOTA: En caso de que los documentos anteriores sean revisados o modificados, debe tomarse en cuenta la edición en vigor en la fecha de la convocatoria de la licitación, salvo que la CFE indique otra cosa.

4 DEFINICIONES

4.1 Alta Disponibilidad

Medidas que tienden a garantizar el funcionamiento continúo del equipo por un largo periodo de tiempo.

4.2 Bootp

Es un protocolo de red UDP utilizado por los clientes de red para obtener su dirección IP automáticamente.

4.3 Dispositivo Electrónico Inteligente (DEI)

Dispositivo que contiene uno o más procesadores con la capacidad de recibir y/o enviar información a una fuente externa: En esta especificación se refieren a los Relevadores de Protección, Medidores Multifunción, Registradores de Disturbio y SCADA.

4.4 Evento de Seguridad

La ocurrencia identificada de un estado de red, servicio o sistema que indica una posible desviación de la política de seguridad o falla de los elementos de seguridad.

4.5 Failover

Modo de configuración en cual en caso de falla de un elemento este transfiere la operación a otro elemento de manera automática y sin intervención del usuario.

4.6 Incidente de Seguridad

Evento o serie de eventos de seguridad de la información inesperados o no deseados que tienen una probabilidad significante de comprometer las operaciones de negocios y amenazan la seguridad de la información.

4.7 Protocolo

Conjunto de reglas que determinan el comportamiento funcional de la comunicación entre dispositivos.

4.8 Protocolo Abierto

Protocolo que cuenta con sus especificaciones estandarizadas o disponibles públicamente.

4.9 Software Propietario

Aplicaciones que sus especificaciones no están disponibles públicamente. Y los derechos de patente son propiedad intelectual del fabricante.

4.10 Redundancia

Existencia de más de un medio necesario para realizar una función en un punto.

4.11 Política

Procedimiento en el cual se definen un cierto número de indicaciones a seguir.

5 SIMBOLOS Y ABREVIATURAS

API Application Programming Interface.

ASN Abstract Syntax Notation.

CompactPCI Compact Peripheral Computer Interface (IEEE 1101, IEEE 1076).

CTS Clear To Send.

DHCP Dynamic Host Configuration Protocol.

DTE Data Terminal Equipment.

DTR Data Terminal Ready.

EGP Exterior Gateway Protocol.

EMC Electromagnetic Compatibility.

EMI Electromagnetic Interference.

FL Fiber Link.

GUI Graphic User Interface.

HTTP Hypertext Transfer Protocol.

HTTPS Hypertext Transfer Protocol Secure.

ICMP Internet Control Message Protocol.

IGMP Internet Group Management Protocol.

IPSec Internet Protocol Security.

ISAKMP/IKE Internet Security Association and Key Management Protocol/ Internet Key Exchange.

LAN Local Area Network.

L2TP Layer 2 Tunneling Protocol.

MTBF Mean Time Between Failure.

MTTR Mean Time To Repair.

NAT Network Address Translation.

NTP Network Time Protocol.

ODBC Open Data Base Connectivity.

OSI Open System Interconnection.

OSPF Open Shortest Path First.

PLC Programmable Logic Controller.

PPP Point to Point Protocol.

PPPoE Point-to-Point Protocol over Ethernet.

PPTP Point to Point Tunneling Protocol.

RDBMS Relational Data Base Management Systems.

RADIUS Remote Authentication Dial In User Service.

SNMP Simple Network Management Protocol.

SPI Stateful Packet Inspection.

TCP/IP Transmisión Control Protocol/Internet Protocol.

UDP User Datagram Protocol.

UTP Unshielded Twisted-Pair.

WAN Wide Area Network.

WRR Weighted Round Robin.

6 CARACTERÍSTICAS Y CONDICIONES GENERALES

Las unidades de medidas utilizadas en la presente especificación están de acuerdo con lo indicado en la norma NOM-008-SCFI.

El presente documento describe las características generales de la consola de monitoreo y administración de los Equipos de Seguridad utilizados para controlar el intercambio de información y el acceso autorizado o rechazos de accesos hacia los dispositivos que se encuentran dentro de la zona segura.

6.1 Arquitectura

Debe permitir el acceso a usuarios a todos los dispositivos conectados a la red “ethernet” de la zona segura de la subestación usando protocolo TCP/IP.

Se requiere la administración, configuración y el monitoreo en forma regionalizada de tal manera que debe contar con la funcionalidad necesaria para que desde cualquier punto de la red LAN/WAN, se utilice el “software” propietario de cada “firewall” para las operaciones de configuración y monitoreo a través de la red LAN.

6.2 Consola de Monitoreo

6.2.1 Características Generales

La consola de monitoreo debe tener las funciones de configuración y supervisión de los equipos de seguridad ("firewall"), a los que se refiere la especificación G0100-12 bajo su administración.

Debe tener la funcionalidad para implementar el acceso de usuarios para administración protegidas por claves de acceso ("passwords") y/o certificados digitales y permitir al administrador asignar los perfiles requeridos para que cada usuario tenga acceso a los recursos asignados, de acuerdo a los siguientes perfiles y cumplir con lo marcado en el Apéndice A:

Función	Administrador	Operador	Especialista	Visitante
Creación y "mantto" de cuentas de usuarios	X			
Acceso a todas las funciones, configuración, "mantto" y ajustes de los equipos "firewall"	X			
Navegación, visualización y consulta de información	X	X	X	X
Reconocer, habilitar y deshabilitar alarmas	x	X		
Acceso a "firewall´s" para consulta y/o cambios de ajuste	X		X	
Generación, visualización e impresión de reportes	X	X	X	

La Consola de monitoreo debe presentar en la pantalla a través de páginas las diferentes condiciones operativas de los Equipos de Seguridad a través del intercambio de información por medio de la Intranet de la CFE, incluyendo alarmas propias de los equipos y el estado de comunicación de los mismos.

La Consola de monitoreo debe cumplir con las siguientes características de operación:

a) Capacidad de configuración centralizada desde otra consola.

b) Monitoreo de los "firewall´s" administrados por la consola.

c) Disponibilidad (en operación 1+1 con posibilidad de agregar cluster, vigía del sistema (watch-dog)). Los sistemas requeridos con características operativas y continuidad de servicio durante las 24 h del día, los 365 días del año.

d) Respaldos de configuraciones de la consola, políticas de seguridad de los "firewalls" administrados y las bitácoras de operación y eventos.

e) Control de versiones de las políticas de seguridad de los "firewalls" administrados. Incluir la opción de guardar la política completa o una parte especifica de la misma.

f) Sincronización de tiempo vía NTP. La Consola de monitoreo deben tener soporte para el cambio automático de horario de verano, configurable por el usuario (habilitación/deshabilitación y fecha de inicio - termino).

g) Inicialización automática al normalizarse la alimentación, hasta el punto de arrancar todas las aplicaciones e iniciar el registro de información.

h) El usuario debe suministrar su clave y contraseña para ingresar a la consola de monitoreo.

i) Autodiagnóstico al arranque.

j) Debe de contar con la funcionalidad de crear reportes que permitan crear estadísticas.

k) Debe de permitir su monitoreo vía protocolo SNMP, por lo menos, de lo siguiente:

- % de utilización del o los CPU´s,
- % de memoria utilizada,
- % de utilización de medios de almacenamiento,
- % de utilización de interfaz de red.

l) Debe mostrar al menos los eventos de 2 meses hacia atrás a partir de la fecha actual del sistema, la capacidad de almacenamiento debe ser mínima de 250 GB para el registro de eventos en caso de requerir otra capacidad se indica en **Características Particulares**. El registro de la información de alarmas en la consola de monitoreo debe incluir la estampa de tiempo con por lo menos día, mes, año, hora, minuto y segundo.

m) Para la visualización debe incluir y estar disponible un tutorial gráfico para el acceso, operación y búsqueda de la información por parte de los usuarios del sistema, así como las instrucciones y método para la obtención e impresión de reportes.

n) Debe de contar con una herramienta de diseño para el desarrollo de pantallas de visualización dinámica del total de la información contenida en la base de datos del sistema.

o) Debe tener la capacidad de aceptar crecimiento modular tanto en “hardware” como “software”.

p) Debe permitir realizar altas o bajas de dispositivos “firewall” del sistema.

q) Procesar 30,000 eventos por segundo

r) Almacenamiento de acuerdo a **Características Particulares**. Se debe considerar la capacidad mínima necesaria para el registro de eventos (véase inciso o) del punto anterior y para la operación normal del sistema operativo y software instalado.

s) Las comunicaciones entre todos los componentes que pertenezcan a un solo dominio de administración (consola y “firewall”), deben establecer comunicaciones seguras a través del uso de certificados.

t) Incluir una entidad CA (Certificate Authority) interna que cumpla con el estándar X.509, que genere certificados a los equipos de seguridad y a los usuarios para una fácil autenticación en las VPNs.

u) Incluir una herramienta de administración de los objetos de red definidos en la consola que incluya búsqueda para permitir fácilmente filtrar objetos de red. Debe también incluir la opción de buscar objetos duplicados (con la misma IP) y objetos no usados (en una regla o política) y una lista de las reglas en que un objeto especifico es usado.

v) Incluir la opción de segmentar las reglas de acceso, usando etiquetas o títulos de sección y de esa forma organizar las políticas

w) Incluir la habilidad de distribuir y aplicar centralizadamente nuevas versiones de “software” para los equipos de seguridad que administra.

x) Son considerados eventos de seguridad:

- registro de una comunicación ofensiva,
- denegaciones de servicio,
- virus,
- sondeo o escaneo de puertos de la consola,
- acceso a cuentas privilegiadas,
- SPAM,
- troyanos,
- gusanos,
- usos no autorizados,
- violaciones de derechos,
- daños a registros internos,
- pérdida de registro de usuarios,
- entrada de código malicioso.

6.2.2 Registro y estado

a) Las bitácoras, deben ser parte del mismo sistema de administración y opcionalmente los administradores deben poder instalar servidores de Logs por separado.

b) Se debe poder diferenciar entre “logs” de usuarios regulares y los “logs” propios de la administración.

c) Para cada coincidencia de una política, se debe poder configurar alguna de las siguientes opciones: guardar en bitácora, enviar una alerta vía correo electrónico o mediante alarmas por SNMP (trap), o ejecutar una rutina (script) definida por el usuario.

d) Los “logs” deben ser transferidos de forma cifrada entre los equipos de seguridad y el servidor de administración. De la misma manera desde y hacia la consola de administración del servidor.

e) Se debe poder exportar los “logs” en formato texto.

6.2.3 Monitoreo de los equipos de seguridad

El servidor de administración debe permitir la supervisión de los equipos de seguridad que conformara lo siguiente:

a) Incluir una interfase grafica de monitoreo que facilite la revisión del status de los equipos de seguridad.

b) Proveer por lo menos la siguiente información por cada equipo de seguridad: Sistema Operativo, Uso de Memoria, CPU, todas las particiones de disco y % de espacio libre en disco.

c) Proveer el status de cada uno de los componentes de cada equipo de seguridad ("firewall, vpn, cluster").

d) Incluir el estado de todos los túneles de VPN, sitio a sitio y cliente a sitio.

e) Permitir configurar límites que tomen acciones cuando sean superados. Las acciones deben incluir: guardar en bitácora, enviar una alerta via correo electrónico o mediante alarmas por SNMP (trap), o ejecutar una rutina (script) definida por el usuario.

f) Incluir graficas predefinidas de monitoreo del tráfico y contadores del sistema contra tiempo. Se debe monitorear por lo menos: Reglas de seguridad con más incidencias, usuarios con mayor uso de las VPNs y trafico de red. Debe permitir la opción de generar gráficas personalizadas.

g) Permitir grabar las vistas de tráfico y contadores del sistema a un archivo, para análisis posterior.

h) Incluir la posibilidad de agregar reglas dinámicas y eventuales, para bloquear temporalmente paquetes basados en origen, destino y servicio. Las reglas eventuales deben evitar no rehacer la regla principal.

i) Reconocer funcionamientos inadecuados y problemas de conectividad entre dos puntos conectados a través de una VPN, y alertar y crear "logs" cuando el túnel de VPN se encuentre abajo.

6.2.4 Acceso mediante navegador de internet para administración

a) Incluir la posibilidad de ver las políticas de seguridad a través de un navegador, administrar "logs" y usuarios dando acceso a gerentes y auditores sin necesidad de tener acceso total a la consola. La conexión con el navegador debe ser mediante HTTPS.

b) Permitir el acceso usando uno de los siguientes navegadores: "internet explorer, firefox o chrome".

6.2.5 Directorio de usuarios

a) Permitir integrarse con un directorio LDAP, para autenticar y autorizar usuarios, basados en perfiles predefinidos.

b) Incluir la opción de extender el esquema de LDAP o el uso de una plantilla interna, para el uso de propiedades no predefinidas.

c) Incluir una interfase grafica que permita adicionar, eliminar, remover y editar usuarios que están almacenados en el directorio LDAP.

d) Incluir perfiles predefinidos para Microsoft Active Directory, Novell.

e) Permitir realizar requerimientos a diferentes servidores LDAP, para tener un esquema de redundancia y encontrar usuarios distribuidos por múltiples servidores.

6.2.6 Control de Cambios

a) Incluir un sistema de control de cambios integrado al servidor de administración.

b) Permitir el seguimiento visual de los cambios realizados, resaltando los cambios y listándolos.

c) Generar reportes de cambios realizados durante una sesión, para control del administrador y de los auditores.

d) Generar reportes de cambios realizados entre 2 sesiones diferentes, resumiendo todos los cambios realizados en el periodo de tiempo entre ambas sesiones.

e) Contar con la opción de forzar al administrador a que deba requerir la aprobación de un gerente o supervisor antes de permitir la instalación de políticas.

6.3 Licencias

El equipo debe tener los derechos de uso de las licencias de todo el “software” suministrado para la explotación legal de los equipos, con objeto de respetar las leyes internacionales en materia de los derechos de autor, el equipo debe tener las licencias originales del “software” empleado, así como los discos compactos, medios ópticos y manuales correspondientes en forma electrónica.

La licencia para el numero de de equipos administrados se define en **Características Particulares**.

6.4 Capacitación

Cuando se solicite en características particulares se debe impartir un curso de capacitación. El temario, duración, alcances y perfil del instructor se describen en **Características Particulares.**

7 CONDICIONES DE OPERACIÓN

No aplica.

8 CONDICIONES DE DESARROLLO SUSTENTABLE

No aplica.

9 CONDICIONES DE SEGURIDAD INDUSTRIAL

No aplica.

10 CONTROL DE CALIDAD

El sistema es requerido para utilizarse en una sala de control que requieren características operativas con base en una referencia de tiempo real, en condiciones de exigencias estrictas bajo demandas de alta confiabilidad y continuidad de servicio durante las 24 h del día, los 365 días del año.

Los equipos deben ser diseñados y construidos para operar sin presentar fallas ocasionadas por condiciones ambientales. El diseño se debe haber comprobado a fin de evitar consecuencias de errores en el mismo. Las condiciones de transporte deben ser consideradas a fin de evitar mal funcionamiento debido al mismo.

Es requisito indispensable la seguridad de operación de cada una de las funciones que se asignen al sistema, evitando cualquier posibilidad de falsa operación, inadecuada aplicación de funciones y fundamentalmente de operación autónoma o errónea de telecontroles por interpretación de mensajes erróneos o fallas de equipamiento (hardware). Por lo tanto, se requiere que el sistema cuente con los elementos necesarios de seguridad y verificación a nivel de programación y componentes.

10.1 Notificación y Documentación de las Pruebas

El proveedor en conjunto con personal de CFE, deben establecer el programa de pruebas a efectuarse, cuyo documento debe presentarse por lo menos con 20 días de anticipación a éstas, para la aprobación final de CFE.

Al término de las pruebas en fábrica se debe presentar el reporte con todas las condiciones, características y resultados obtenidos. Cada prueba debe reportarse conteniendo:

a) Identificación del equipo sometido a pruebas.

b) Descripción de la prueba.

c) Descripción de todas las intervenciones, correcciones, modificaciones y preparaciones llevadas a cabo en los equipos.

d) Certificado o documentación que avale la consola cumple con los requisitos establecidos en esta Especificación.

Los reportes son responsabilidad del proveedor y deben ser entregados con original.

Los procedimientos de prueba serán discutidos y acordados por el fabricante y usuario antes de hacer las mismas. No habrá pruebas en fábrica.

10.2 Pruebas de Aceptación

10.2.1 Pruebas tecnológicas

a) Tiempos de actualización en pantalla y verificación de la adquisición de datos en tiempo real.

b) Avalancha del 100 % de la capacidad total.

c) Autodiagnóstico global, periféricos, redes, fuentes de alimentación.

d) Reporte de los diagnósticos.

e) Verificación de la comunicación de todo el sistema, así como los medios de monitoreo de los enlaces.

10.2.2 Criterios de aceptación o rechazo

El lote de equipos se rechaza si no cumple con lo establecido en esta especificación y con las pruebas y sus valores de aceptación.

10.2.3 Procedimiento a seguir en caso de fallas

Cualquier falla origina la suspensión de la prueba corriente y se debe reiniciar ésta desde el primer paso. En caso de una interrupción causada por una avería sólo se repetirán las pruebas que involucren a la componente defectuosa. Al producirse una falla, se deben tomar las acciones siguientes:

a) Suspensión de la prueba.

b) Identificación y análisis de falla.

c) Corrección de la falla.

El inspector de Comisión podrá requerir la repetición de la prueba completa de acuerdo a su criterio, determinado si la falla es crítica y es el resultado de un mal diseño.

11 MARCADO

No aplica.

12 EMPAQUE, EMBALAJE, EMBARQUE, TRANSPORTACIÓN, DESCARGA, RECEPCIÓN, ALMACENAJE Y MANEJO

No aplica.

13 BIBLIOGRAFÍA

No aplica.

14 CARACTERÍSTICAS PARTICULARES

Las **Características Particulares** a que se refiere la presente especificación se indican en el formato CPE-469, anexo a este documento.

APÉNDICE A

CONSOLA DE MONITOREO (REQUERIMIENTOS MÍNIMOS)

Software	R75
Sistema operativo	Secure Platform
Puertos 10/100/1000	10
Rendimiento Firewall	9 Gbps
Rendimiento de VPN	2.4 Gbps
Sesiones concurrentes	1.2 Millones
Rendimiento IPsec software blade	7.5 Gbps
Numero de licencias	Ilimitado
VLANs	1 024
Acelerador de almacenamiento	Si
Disco Duro	250 GB
Dimensionamiento	Rack 19 pulgadas
Compatibilidad	Software de administración Smart Center Server con módulos Smart provisioning y Smart Defense

CARACTERISTICAS PARTICULARES PARA: CONSOLA DE ADMINISTRACIÓN DE “FIREWALL” PARA SEGURIDAD DE ACCESO A REDES DE SUBESTACIÓN (LLENADO POR EL USUARIO)

Correspondiente a la especificación CFE G0100-10

CARACTERÍSTICAS GENERALES

1. Software

2. Sistema operativo

3. Puertos 10/100/1000

4. Rendimiento Firewall

5. Rendimiento de VPN

6. Sesiones concurrentes

7. Rendimiento IPsec software blade

8. Número de licencias

9. VLANs

10. Acelerador de almacenamiento

11. Disco Duro

12. Dimensionamiento

13. Compatibilidad

CAPACITACIÓN

1. Perfil del instructor:

2. Alcances:

3. Duración:

4. Temario: