Instituto Electoral y de Participación Ciudadana de Jalisco

CONVOCATORIA

LICITACIÓN IEPC-L-003/2018

Con fundamento en lo dispuesto por los artículos 116, fracción IV, inciso c), y 134 de la Constitución Política de los Estados Unidos Mexicanos; 98, párrafo 1 de la Ley General de Instituciones y Procedimientos Electorales; 12, bases III y IV de la Constitución Política del Estado de Jalisco; 116 y 136 del Código Electoral y de Participación Social del Estado de Jalisco, así como el artículo quinto transitorio, fracción II del Reglamento en Materia de Adquisiciones y Enajenaciones del Instituto Electoral y de Participación Ciudadana del Estado de Jalisco; y en cumplimiento a lo ordenado en el acuerdo AC04/CAE/27-02-2018, aprobado por la Comisión de Adquisiciones y Enajenaciones, en sesión ordinaria de fecha 27 veintisiete de febrero de 2018 dos mil dieciocho, el Instituto Electoral y de Participación Ciudadana del Estado de Jalisco

CONVOCA

A los interesados en participar en la licitación que se desarrollará de conformidad con las bases establecidas en la presente convocatoria, las cuales fueron aprobadas por la Comisión de Adquisiciones y Enajenaciones del organismo electoral en sesión ordinaria de fecha 27 veintisiete de febrero de 2018 dos mil dieciocho.

Únicamente podrán participar las personas físicas y jurídicas registradas en el padrón de proveedores del Instituto o del Gobierno del Estado, y que se encuentren debidamente constituidas que puedan garantizar al Instituto el cumplimiento de sus obligaciones.

CANTIDAD	DESCRIPCIÓN	CARACTERÍSTICAS Y ESPECIFICACIONES
1	Equipo de seguridad perimetral (firewall) de próxima generación con IPS (prevención de intrusos), Antivirus, AntiSpyware y Filtrado de contenidos URL.	Características y especificaciones en el Anexo Técnico. **(Anexo 1)**

El procedimiento de licitación se desarrollará de conformidad con el calendario siguiente:

ACTO	FECHA	LUGAR
Publicación de la convocatoria.	27 de febrero de 2018.	Página Web del IEPC*. http://www.iepcjalisco.org.mx/
Periodo de aclaraciones.	Del 27 de febrero al 09 de marzo de 2018.	Vía correo electrónico al correo: compras.cae@iepcjalisco.org.mx

Instituto Electoral y de Participación Ciudadana de Jalisco

Presentación de cotizaciones.	A partir de la publicación de la presente convocatoria y hasta el 12 de marzo de 2018, a más tardar a las 17:00 horas.	Oficialía de partes del IEPC*.
Sesión pública de fallo y adjudicación.	13 de marzo 2018, a las 11:00 horas.	Sala de consejeros del IEPC*.

* IEPC= Instituto Electoral y de Participación Ciudadana del Estado de Jalisco.

Bases.

El sobre que contenga su propuesta deberá estar debidamente cerrado, identificado con la **clave alfanumérica de la licitación** que se encuentra en la parte superior de la presente y rubricado en la solapa por el licitante o su representante legal, dirigido a la **Comisión de Adquisiciones y Enajenaciones.**

Cualquier aclaración deberá ser formulada por escrito por conducto del licitante o representante legal a través del correo o correos electrónicos oficiales de su empresa.

Su propuesta será recibida en la **OFICIALÍA DE PARTES** del instituto, ubicada en la planta baja de la finca marcada con el número 2370 de la calle Florencia, colonia Italia Providencia C.P. 44648, en la ciudad de Guadalajara, Jalisco.

Su propuesta invariablemente deberá cumplir con los requisitos siguientes:

1. **Toda la documentación redactada por el licitante deberá ser presentada impresa en original y en papel membretado y en idioma español.**
2. **Con *firma autógrafa* del licitante o su representante legal para presentar propuesta económica, en la última hoja y al calce de cada una de las mismas; identificando por fuera del sobre al remitente.**
3. **Mencionar condiciones de pago, vigencia de cotización y garantía del servicio.**
4. **Manifestar bajo protesta de conducirse con verdad de que realizará el servicio solicitado con las especificaciones técnicas establecidas en el anexo y en la fecha requerida.**
5. **Las propuestas económicas deberán estarse a lo siguiente:**

    I. **Señalar tanto el precio unitario de cada uno de los bienes ofertados, como el subtotal y total cotizado, en moneda nacional, con número y letra, no se aceptarán propuestas en moneda extranjera;**
    II. **Al final de la cotización, en la parte relativa al monto total, se deberá presentar desglosado el monto; y**
    III. **Las cotizaciones que se presenten deberán ser claras y precisas.**
    IV. **Las cotizaciones deberán incluir todos los costos e impuestos involucrados, por lo que una vez presentada la propuesta no se aceptará ningún costo extra.**

Instituto Electoral y de Participación Ciudadana de Jalisco

Debiendo indicar:

"

_

CANTIDAD	DESCRIPCIÓN	CARACTERÍSTICAS	PRECIO UNITARIO	SUBTOTAL	(GRAN TOTAL)
				$	$

Para que su propuesta sea considerada deberá especificar cada uno de los siguientes puntos:	
Fecha de entrega:	
Calidad:	
Servicio:	
Condiciones de pago:	
Vigencia de la cotización:	
Garantía de los servicios:	Manifestar bajo protesta de conducirse con verdad que se cumplirá con proporcionar el bien o servicio conforme a las especificaciones y términos del presente procedimiento.

Manifestamos bajo protesta de conducirnos con verdad que la entrega del bien o servicio se realizará conforme a las especificaciones y términos establecidos en el presente procedimiento.

Lugar y fecha
Nombre y firma del representante"

DE LA GARANTÍA.

Para esta licitación el instituto electoral solicita al proveedor la garantía del cumplimiento del contrato, correspondiente al diez por ciento del monto total adjudicado, o en caso de solicitar anticipo la garantía será el equivalente a lo solicitado. Esta garantía deberá ser entregada antes de la firma del contrato y entrará en vigor a partir la firma del mismo y por todo el tiempo que se encuentren vigentes las obligaciones del proveedor.

La garantía de cumplimiento de contrato, podrá ser mediante fianza, cheque certificado o de caja a favor del instituto electoral.

La poliza de fianza debera contener el texto del **ANEXO 2**.

El proveedor queda obligado ante el instituto electoral a responder por los defectos y vicios ocultos de los bienes y servicios suministrados, así como de cualquier otra responsabilidad en que hubiere incurrido en los términos señalados en el contrato

respectivo y en el código civil para el estado de Jalisco y el de su respectivo procedimiento; en el entendido de que deberá someterse a la competencia de los tribunales del primer partido judicial del estado de Jalisco, renunciando a los tribunales que por razón de su domicilio presente o futuro le pudiera corresponder.

DE LA FIRMA DEL CONTRATO.

El proveedor deberá concurrir en un plazo no mayor a **diez días naturales** a partir de que resulte adjudicado a **suscribir** el contrato, en caso de no acudir el instituto, sin necesidad de un nuevo procedimiento podrá adjudicar el contrato al participante que haya presentado la siguiente proposición solvente más baja, siempre que la diferencia en precio con respecto a la proposición inicialmente adjudicada no sea superior a un margen del diez por ciento.

PREVENCIONES GENERALES.

Se hace de su conocimiento que para realizar adquisiciones de bienes y servicios requeridos, el Instituto se sujetará a la **suficiencia presupuestal** contenida en las partidas correspondientes.

El proveedor en su carácter intrínseco de patrón del personal que emplee para suministrar los bienes o servicios contratados, será el único responsable de las obligaciones derivadas de las disposiciones legales y demás ordenamientos en materia de seguridad social, sin que por ningún motivo se considere patrón al Instituto Electoral y de Participación Ciudadana del Estado de Jalisco.

En caso de resultar adjudicado no deberá subcontratar, ni ceder total o parcialmente los derechos y obligaciones que se deriven del contrato u orden de compra, en términos del reglamento de la materia.

LAS PROPUESTAS NO ELABORADAS Y ENTREGADAS EN LOS TÉRMINOS SEÑALADOS EN LAS CARACTERÍSTICAS, ESPECIFICACIONES, INFORMACIÓN Y PLAZOS SEÑALADOS EN EL PRESENTE PROCEDIMIENTO *NO SERÁN TOMADAS* EN CUENTA POR LA COMISIÓN DE ADQUISICIONES Y ENAJENACIONES DEL IEPC JALISCO.

ATENTAMENTE
Guadalajara, Jalisco; a 27 de febrero de 2018.

MIGUEL GODÍNEZ TERRÍQUEZ
CONSEJERO ELECTORAL PRESIDENTE DE LA COMISIÓN DE ADQUISICIONES Y ENAJENACIONES

LUIS ALFONSO CAMPOS GUZMÁN
SECRETARIO TÉCNICO

JUSTIFICACIÓN

Dispositivo de seguridad perimetral (Firewall)

Un firewall es un dispositivo de seguridad de la red que monitorea el tráfico de red entrante y saliente, y decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad.

Los dispositivos de seguridad perimetral o firewalls han constituido una primera línea de defensa en seguridad de la red durante más de 25 años. Establecen una barrera entre las redes internas protegidas y controladas en las que se puede confiar, y redes externas que no son de confianza, como Internet.

Los firewalls han evolucionado más allá de la inspección activa y el filtrado simple de paquetes, y son llamados **firewalls de próxima generación (NGFW)**. La mayoría de las empresas están implementando estos firewalls de próxima generación para bloquear las amenazas modernas, como los ataques de la capa de aplicación y el malware avanzado.

Según la definición de Gartner, Inc., un firewall de próxima generación debe incluir lo siguiente:

- Funcionalidades de firewall estándares, como la inspección con estado
- Prevención integrada de intrusiones
- Reconocimiento y control de aplicaciones para ver y bloquear las aplicaciones peligrosas
- Rutas de actualización para incluir fuentes de información futuras
- Técnicas para abordar las amenazas de seguridad en evolución

Para el instituto resulta muy importante proteger la red informática, tanto interna como externamente, así como proteger cada equipo de posibles amenazas, por lo que este proyecto de adquisición de un dispositivo de seguridad perimetral (firewall) constituye un esfuerzo coordinado para poder contar con un **equipo de nueva generación** y poder brindar protección al sitio central de este Instituto, debido a la alta demanda en temas de seguridad, así como otorgar conexiones seguras a los diferentes sistemas para los órganos desconcentrados, administrar las conexiones internas, y aumentar los anchos de banda de los enlaces de Internet.

ADQUISICIÓN DE DISPOSITIVO DE SEGURIDAD PERIMETRAL (FIREWALL)

"ANEXO TÉCNICO"

CARACTERÍSTICAS Y ESPECIFICACIONES

El presente anexo describe las características que deberá cumplir la solución de Seguridad Perimetral para el aseguramiento de la red informática del INSTITUTO ELECTORAL Y DE PARTICIPACION CIUDADANA DEL ESTADO DE JALISCO.

1. Características del equipo para el sitio central:

A. El equipo involucrado deberá de incluir las siguientes características:

- El equipo deberá proveer los servicios de: Firewall, VPN, Prevención de Amenazas y Filtrado de Contenido
- Desempeño del firewall con control de aplicaciones: mínimo 940 Mbps
- Desempeño de Prevención de Amenazas (IPS, Antivirus, AntiSpyware, y URL Filtering simultáneamente): 610 Mbps
- Desempeño de VPN: mínimo 400 Mbps
- Máximas sesiones soportadas: 128,000
- Túneles VPN Soportados: 1,000
- Ruteadores virtuales soportados: 5
- Zonas de seguridad soportadas: 30
- Puertos de Red: mínimo 4 x 10/100/1000Base RJ45 y 8 x 1 GbE en SFP
- Puertos de Red SFP con posibilidad de usarse para conexiones con RJ45 a GbE, 4 como mínimo
- Puertos de Red SFP sobrantes con transceptor de 1GbE incluidos
- Puerto adicional para la administración fuera de línea y dos interfaces predefinidas para la alta disponibilidad
- Disco Duro de estado sólido local mínimo de (SSD): 240 GB
- Certificación EAL4 y NIST usg6 del tipo NPD (Network Protection Device) certificando los módulos de FW y IPS
- Suscripción a actualizaciones por 12 Meses con el Fabricante
- Soporte Técnico y Garantías por Fabricante por 12 Meses con Garantía en 8x5

B. El dispositivo involucrado deberá contar con las siguientes funcionalidades:

- Capacidad de identificar y controlar aplicaciones independientemente del puerto, protocolo, encripción SSL o SSH, o táctica evasiva
- Deberá permitir policitas de uso positivo de aplicaciones, es decir, permitir, negar, habilitar políticas por horario, inspeccionar
- Deberá incluir la capacidad de actualización para identificar nuevas

aplicaciones

- Deberá incluir la capacidad de creación de políticas basadas en el control por aplicación, por categoría de aplicación, subcategoría de aplicación, tecnología y factor de riesgo
- Deberá incluir la capacidad de creación de políticas basadas en nombre de usuario, grupo de usuario o dirección IP
- Deberá permitir definir instancias virtuales dentro del firewall físico (firewall virtuales)
- Los recursos que podrán asignarse a un firewall virtual deberán incluir como mínimo:
    - Número máximo de sesiones para un sistema virtual
    - Número máximo de reglas de seguridad
    - Número máximo de reglas de NAT
    - Número máximo de reglas de calidad de servicio
    - Número máximo de reglas de ruteo basada en política
    - Número de túneles Site-to-Site
- La tecnología de identificación de aplicaciones deberá estar habilitada por default (motor de inspección base) sin necesidad de habilitar funcionalidades adicionales
- Deberá incluir herramientas graficas que permitan tener la vista de aplicaciones que fluyen a través del firewall
- Deberá identificar usuarios a través de integración con Active Directory, LDAP, eDirectory, Syslog Listener y XML-API
- Deberá realizar políticas que permitan el control de aplicaciones, usuarios y contenido mediante una sola política
- Deberá incluir mecanismos de protección contra paquetes fragmentados
- Deberá incluir mecanismos de protección contra ataques de reconocimiento (escaneo)
- La identificación de aplicaciones deberá realizarse tan pronto la información llegue al firewall, sin depender de tecnología de firewall de estado
- Deberá permitir el manejo de aplicaciones no identificadas, ya sea creando políticas para su inspección y control, además de permitir, desarrollar firmas para la identificación de aplicaciones desconocidas
- Para garantizar el acceso de la plataforma de seguridad incluso en períodos de alta cantidad de tráfico la solución deberá contar con procesadores y memorias dedicados a un plano de control (administración del equipo) y deberá integrar procesadores y memorias separados y dedicados específicamente al plano de datos (inspección de usuarios)
- Para aquellos usuarios que no estén integrados al directorio de la convocante, por ejemplo red invitados, deberá permitir la integración con soluciones de autenticación a través de un XML-API configurable.
    - Para el punto anterior deberá incluir el soporte de identificación de usuarios que utilicen direcciones IPv4 e IPv6
- Deberá incluir mecanismos que protejan contra ataques de denegación de servicio (DoS) o ataque de denegación de servicio distribuida (DDoS)
- Deberá incluir sin costo ni de hardware adicional tecnología que permita de-

encripción de tráfico SSL y SSH
  - En relación al punto anterior deberá permitir:
    - Bloqueo de sesiones SSL con certificados expirados
    - Bloqueo de sesiones SSL con certificados no confiables
    - Bloqueo de sesiones SSL y SSH para mecanismos de encripción no soportados
- Deberá incluir sin costo la capacidad de limitar transferencia de archivos no autorizados
- Deberá permitir el control de trasferencia de archivos por aplicación
- Deberá de identificar más de 40 tipos de archivos (DLL, ZIP, EXE, etc)
- Deberá permitir la inspección de archivos comprimidos que utilicen el algoritmo deflate (ZIP, GZIP, etc.)
- Deberá incluir sin costo y en el mismo equipo tecnología de identificación de malware moderno
- Deberá incluir la capacidad de análisis malware día cero de archivos ejecutando archivos desconocidos en un SandBox virtualizado
- Deberá incluir la inspección de malware en día cero para documentos tipo ejecutables y dll, Office (Word, Excel, Powerpoint), pdf, apk, jar (Java), MacOS y Adobe Flash
- Deberá incluir VPN IPsec Site to Site con las siguientes características:
  - Encripción 3Des, AES 128, 192 y 256 bits
  - Autenticación MD5, SHA1, SHA256, SHA384, SHA512
- El firewall deberá tener la capacidad de operar en los siguientes modos de manera simultánea mediante el uso de sus interfaces físicas modo sniffer (monitoreo y análisis del tráfico de la red), capa 2 (L2) y capa 3 (L3)
  - Modo sniffer, para inspección vía un puerto espejo del tráfico de datos de la red
  - Modo capa-2 (L2), para inspección de datos en línea y tener visibilidad y control del tráfico a nivel aplicación
  - Modo capa-3 (L3), para inspección de datos en línea y tener visibilidad y control del tráfico a nivel aplicación. Con capacidad de generar ruteo virtual para al menos 10 ruteadores virtuales y manejo de tráfico entre diferentes zonas de seguridad y sub-redes, soportando al menos 40 zonas de seguridad
- El equipo deberá contar con soporte para los siguientes servicios:
  - Soporte de 4,000 redes virtuales VLANs 802.1q,
  - Traducción de direcciones de red (NAT) por fuente y destino, por direcciones IP dinámicas y pool de puertos.
  - Soporte traducción de direcciones IPv6 NAT64
  - Al menos 20,000 direcciones en tabla de ruteo en IPv4
  - Al menos 20,000 direcciones en tabla de ruteo en IPv6
  - PPPoE
  - Enrutamiento BGP, OSPFv3 y rip2
  - Soporte de enrutamiento en base a políticas
  - Soporte de enrutamiento multicast
  - PIM-SM o PIM-SSM

- IGMP v1,v2,v3
- DHCP server y DHCP relay

- En caso de aplicaciones desconocidos, deberá contar con un editor de firmas
- Control de tráfico IPv4 e IPv6, este último también incluye visibilidad e inspección de amenazas en aplicaciones y control de contenido IPv6 debe ser soportado en interfaces trabajando en L2 y L3
- Soporte SLAAC en interfaces de IPv6
- Deberá permitir la administración de ancho de banda (QoS)
  - Realiza el control de políticas de uso en base a aplicaciones: permitir, negar, calendarizar, inspeccionar y controlar el uso del ancho de banda asociado a aplicación, usuario y grupo de usuarios
  - Definición de hasta 8 clases de tráfico, con parámetros de ancho de banda garantizado, máximo ancho de banda y prioridad
  - Con la finalidad de controlar aplicaciones cuyo consumo pueda ser excesivo (como youtube, ustream, etc) y tener un alto consumo de ancho de banda, se requiere que la solución, además de poder permitir o negar ese tipo de aplicaciones, debe tener la capacidad de controlarlas por políticas de máximo ancho de banda cuando sean solicitadas por diferentes usuarios o aplicaciones, tanto de audio como video streaming
  - Realizar el monitoreo del uso que hacen las aplicaciones por bytes, sesiones y por usuario
  - Deberá soportar definición de parámetros de QoS para las aplicaciones en texto claro, así como para el tráfico que saldrá del firewall dentro de un túnel de VPN
- Soporte de alta disponibilidad
  - Modo activo-activo
  - Modo activo-pasivo
  - Activar alta disponibilidad en base a estado de interface o Monitoreo de conectividad para activar alta disponibilidad
- Soporte de geo localización incluida en el equipo para creación de políticas en base a región/país geográfica
- Definición de criterios y complejidad mínima para contraseña. Soportar al menos e incluir las siguientes capacidades de administración y reporteo con los siguientes criterios:
  - Longitud mínima de contraseña
  - Número mínimo de mayúsculas
  - Número mínimo de minúsculas
  - Número mínimo de caracteres numéricos
  - Número mínimo de caracteres no alfanuméricos
  - Prevenir el uso de contraseñas previas
  - Prevenir el uso de nombre de usuario como contraseña
  - Advertencia de expiración de contraseña
  - Forzar el cambio de contraseña en un periodo especifico

- Administración de políticas, objetos, directamente en el equipo a través de interface gráfica embebida en el equipo Firewall basada en web y de CLI (ssh y puerto consola)
- Soporte de Syslog y SNMP v3
- Deberá desplegar resumen grafico de aplicaciones y amenazas
- Deberá desplegar las aplicaciones con el mayor número de sesiones
- Deberá desplegar las aplicaciones con el mayor factor de riesgo
- Deberá incluir reportes de principales usuarios con mayor uso de ancho de banda
- Deberá incluir reportes de principales aplicaciones con mayor uso de ancho de banda
- Creación automática de búsqueda a la base de datos de registros a partir de la navegación de uso principal de aplicaciones
- Generación de reportes de actividad de usuarios, en base a tiempo, los cuales deberán incluir:
    - Listado de aplicaciones utilizadas
    - Categoría y subcategoría de aplicaciones utilizadas
- Envío de reportes por correo de manera automática
- Generación de reportes personalizados permitiendo seleccionar la base de datos de registro a utilizar así como el periodo de tiempo a emplear en el reporte
- Deberá incluir la capacidad de proporcionar resumen grafico
- El Firewall deberá incluir la capacidad de proporcionar un resumen gráfico de las aplicaciones utilizadas, y las amenazas encontradas diariamente por aplicación
- Deberá contar la funcionalidad para exportar logs de tráfico y amenazas
- Deberá permitir la creación de reportes personalizados
- Deberá contar con herramientas para crear filtros de monitoreo, de las sesiones en el Firewall, por aplicación de origen y/o destino
- El equipo deberá proporcionar como mínimo los siguientes tipos de reportes:
    - Utilización en bytes por aplicación
    - Número de sesiones por aplicación
    - Comparativo de aplicaciones incrementando o decrementando su utilización (por consumo o por sesiones) con respecto a 24 horas y 7 días
    - Principales aplicaciones circulando a través del Firewall
    - Principales direcciones IP (fuente o destino) por aplicación
    - Reporte de actividades específicas para un usuario
    - Origen o destino del tráfico por aplicación-usuario
- Soporte de reportes para identificar equipos infectados por Botnet con base a los siguientes criterios:
    - Visita a sitios de malware
    - Uso de sitios de DNS dinámicos
    - Visita de dominios de reciente registro
    - Uso de aplicaciones desconocidas
    - Presencia de trafico IRC

- Permitir la creación de expresiones regulares para hacer búsquedas o consultas
- Deberá permitir la muestra de los registros del Firewall y amenazas del IPS en base a la información de contexto que se esté mostrando en ese momento en la herramienta de monitoreo
- Funcionalidades de Prevención de Amenazas
- El equipo deberá tener un rendimiento mínimo de 1 Gbps en modo de IPS
- La licencia de IPS deberá permitir protección contra amenazas de virus, spyware y otras clases de malware sin costo adicional. Deberá incluir también, dentro del mismo equipo, el control de transferencia de archivos y bloqueo de archivos por tipo
- Protección contra una amplia variedad de malware, como virus, incluyendo PDF, HTML y Javascript, spyware phone home y C2 (Comando y Control), Troyanos, etc.
- Deberá incluir la capacidad de creación de políticas de inspección basadas en nombre de aplicación, categoría de aplicación y tipo de tecnología
- Deberá incluir la capacidad de creación de políticas de inspección basadas en nombre de usuario, grupos de usuarios o Dirección IP
- El IPS deberá permitir crear firmas para identificar las aplicaciones desarrolladas por la entidad. Deberá permitir la personalización de firmas "phone home" de spyware
- La solución deberá permitir el diseño de firmas de vulnerabilidades
- La solución de IPS deberá permitir la detección y bloqueo de amenazas sobre puertos no estándares, tomando como criterio la política de seguridad definida en base a aplicación
- Protección contra amenazas de virus, malware y spyware
- Deberá incluir la funcionalidad de protección contra amenazas de red, bloqueo de virus, spyware, control de transferencia de archivos, control de la navegación en internet y bloqueo archivos por tipo. Protección contra descargas involuntarias usando http de archivos ejecutables maliciosos
- Escaneo de virus en PDF
- Deberá permitir la inspección en archivos comprimidos que usan algoritmo deflate (zip, gzip, etc.)
- La actualización de firmas de ataques deberá ser diaria, semanal y de emergencia
- El dispositivo debe tener los siguientes mecanismos y realizar la detección y protección de ataques de Red como:
    - DoS (Denial of Services) y DDoS (Distributed Denial of Service)
    - Análisis basado en protocolo
    - Protección contra anomalías basadas en protocolo para detectar uso de protocolos sin cumplimento de RFC
    - Identificación de patrones que detecte ataques a través de más de un paquete, tomando en cuenta elementos como el orden y secuencia de arribo
    - Análisis heurísticos que detecten paquetes anómalos y patrones de tráfico como port scans y host sweeps

- Bloqueo de paquetes malformados o inválidos, desfragmentación IP, re ensamble TCP para protección contra métodos de ofuscación y evasión
- Protección contra malformación de paquetes
- Análisis heurístico
- Permita el diseño de firmas de vulnerabilidades

- El análisis malware en día cero de archivos desconocidos deberá realizarse en un entorno de nube segura para determinar si el archivo se trataba de malware o no. Dentro del análisis en el entorno de nube deberán identificarse al menos 100 comportamientos maliciosos
- Como resultado del análisis de los archivos descrito anteriormente deberá obtenerse en el caso de malware, la firma correspondiente para identificar al archivo en cuestión como malware
- Soporte de firmas basadas en DNS para detectar búsquedas específicas de DNS hacia nombres de equipo que han sido asociados con malware. La solución deberá permitir habilitar/deshabilitar las firmas de DNS para crear excepciones

2.- Características de Servicios de los Dispositivos por parte del Proveedor:

I. Deberán de otorgar servicios de instalación y configuración en sitio con disponibilidad de 8x5.

II. Deberán de contar con Póliza de Soporte Técnico 8x5 por parte del Proveedor que incluya:
- Soporte Telefónico
- Soporte Remoto
- Visitas en sitio en eventos críticos
- Préstamo de Equipo en caso de falla

III. El proveedor deberá otorgar capacitación básica en el uso y configuración de la solución presentada para mínimo 2 personas que se designen

IV. Para objeto de los servicios relacionados con la instalación, configuración, soporte técnico y capacitación, el Proveedor deberá contar con personal técnico suficiente debidamente certificado en los dispositivos y temas de Seguridad presentando sus debidos certificados

V. El proveedor deberá de contar con la experiencia suficiente para poder solucionar cualquier problema que pudiera suscitarse, por lo cual es necesario que sea distribuidor autorizado de la marca

FIN DEL ANEXO TÉCNICO

Instituto Electoral y de Participación Ciudadana

ANEXO 2

Para el caso de que el proveedor opte por la figura de la fianza, ésta se otorgará mediante póliza que expida la compañía autorizada con domicilio en el estado de Jalisco, tratándose de proveedores domiciliados en esta entidad.

Cuando éstos tengan su domicilio fuera de Jalisco, deberán exhibir la garantía, con la aceptación de la afianzadora que la expida de someterse a la competencia de los juzgados del fuero común o federal con jurisdicción en la ciudad de Guadalajara, Jalisco.

TEXTO DE FIANZA

(*NOMBRE DE LA AFIANZADORA*), EN EL EJERCICIO DE LA AUTORIZACIÓN QUE ME OTORGA EL GOBIERNO FEDERAL A TRAVÉS DE LA SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO EN LOS TÉRMINOS DE LOS ARTÍCULOS 36° Y 37° DE LA LEY DE INSTITUCIONES DE SEGUROS Y DE FIANZAS, ME CONSTITUYO FIADORA POR LA SUMA DE $_____ *(CANTIDAD CON LETRA)* A FAVOR DEL INSTITUTO ELECTORAL Y DE PARTICIPACIÓN CIUDADANA DEL ESTADO DE JALISCO.

PARA: GARANTIZAR POR (*NOMBRE DEL **"PROVEEDOR"***) CON DOMICILIO EN _____ COLONIA_____ CIUDAD_____, EL FIEL Y EXACTO CUMPLIMIENTO DE TODAS Y CADA UNA DE LAS OBLIGACIONES CONTRAÍDAS EN EL **CONTRATO No. ____, DE FECHA** _____, CELEBRADO ENTRE NUESTRO FIADO Y EL INSTITUTO ELECTORAL Y DE PARTICIPACIÓN CIUDADANA DEL ESTADO DE JALISCO, CON UN IMPORTE TOTAL DE $_____.

ÉSTA FIANZA ESTARÁ EN VIGOR A PARTIR DE LA FIRMA DEL CONTRATO Y POR TODO EL TIEMPO QUE SE ENCUENTREN VIGENTES LAS OBLIGACIONES DE NUESTRO FIADO, PARA GARANTIZAR LA BUENA CALIDAD DE LOS BIENES SUMINISTRADOS, ASÍ COMO LA REPARACIÓN DE LOS DEFECTOS Y VICIOS OCULTOS QUE PUDIEREN APARECER Y QUE SEAN IMPUTABLES A NUESTRO FIADO Y SOLO PODRÁ SER CANCELADA CON LA PRESENTACIÓN POR PARTE DE NUESTRO FIADO, DE LA ORIGINAL DE LA MISMA.

ESTA FIANZA PERMANECERA EN VIGOR AUN EN LOS CASOS DE QUE EL INSTITUTO ELECTORAL Y DE PARTICIPACIÓN CIUDADANA DEL ESTADO DE JALISCO OTORGUE PRORROGAS A (PROVEEDOR), PARA EL CUMPLIMIENTO DE SUS OBLIGACIONES.

LA AFIANZADORA RENUNCIA EN FORMA EXPRESA A APLICAR LO ESTABLECIDO POR EL ARTÍCULO 179 DE LA LEY FEDERAL DE INSTITUTCIONES DE FIANZAS QUE DICE LA PRORROGA O ESPERA CONCEDIDA PARA EL ACREEDOR AL DEUDOR PRINCIPAL, SIN CONSENTIEMIENTO DE LA INSTITUCIÓN DE FIANZAS, EXTINGUE LA FIANZA.

ESTA FIANZA ESTARÁ VIGENTE EN CASO DE SUBSTANCIACIÓN DE JUICIOS O RECURSOS HASTA SU TOTAL RESOLUCIÓN DEFINITIVA, DE FORMA TAL QUE SU VIGENCIA NO PODRA ACOTARSE EN RAZON DEL PLAZO DE EJECUCIÓN DEL CONTRATO PRINCIPAL FUENTE DE LAS OBLIGACIONES, O CUALQUIER OTRA CIRCUNSTANCIA.

EN EL CASO DE QUE LA PRESENTE SE HAGA EXIGIBLE, LA AFIANZADORA Y EL FIADO ACEPTAN EXPRESAMENTE SOMETERSE AL PROCEDIMIENTO DE EJECUCIÓN ESTABLECIDO EN LOS ARTÍCULOS 178, 279 AL 283 Y DEMÁS RELATIVOS DE LA LEY DE INSTITUCIONES DE SEGUROS Y FIANZAS EN VIGOR, ACEPTANDO SOMETERSE A LA COMPETENCIA DE LOS TRIBUNALES DEL PRIMER PARTIDO JUDICIAL DEL ESTADO DE JALISCO, RENUNCIANDO A LOS TRIBUNALES QUE, POR RAZÓN DE SU DOMICILIO PRESENTE O FUTURO, LES PUDIERA CORRESPONDER.