ANEXO DE ESPECIFICACIONES TÉCNICAS

Renglón 1: Adquisición de nueva plataforma integral de seguridad.
1: Infraestructura de Seguridad
1.1. Firewall de Próxima Generación

DESCRIPCION GENERAL
a. Adquisición de una solución en High Availability (dos equipos de idénticas características y licencias) de protección de redes con características de Next Generation Firewall (NGFW) para la seguridad de la información perimetral que incluye filtro de paquetes, control de aplicaciones, administración de ancho de banda (QoS), VPN IPSec y SSL, IPS, prevención contra amenazas de virus, spyware y malware "Zero Day", actuando como controles de transmisión de datos y acceso a internet componiendo una plataforma de seguridad integrada y robusta. b. Por plataforma de seguridad se entiende hardware y software integrados de tipo appliance. c. Debe encontrarse en el Cuadrante de Lideres de los últimos cuatro reportes (2013, 2014, 2015 y 2016) de Gartner para Enterprise Network Firewall. d. La solución debe ser compatible y certificada (USGV6 en Firewall y/o IPS. No se aceptara certificación de otro tipo) para trabajar en IPv6. e. Debe poseer certificación ICSA LABS para network firewall.
CAPACIDAD Y CANTIDADES
a. La plataforma de seguridad debe poseer las capacidades y características siguientes: i. Throughput de 4 Gbps con la funcionalidad de control de aplicaciones habilitada para todas las firmas que el fabricante posea; ii. Throughput de 2 Gbps con las siguientes funcionalidades habilitadas simultáneamente para todas las firmas que la plataforma de seguridad posea debidamente activadas y actuando: control de aplicaciones IPS, Antivirus e Antispyware. Se deberá presentar documentación oficial de tipo Datasheet, Guía de Administración, etc., informando la performance del equipo ofertado, con todos los módulos activos. No se aceptarán documentos creados ad-hoc. iii. Soporte a, como mínimo, 500.000 de conexiones simultáneas; iv. Soporte a, como mínimo, 50.000 nuevas conexiones por segundo; v. Disco Solid State Drive (SSD) de, como mínimo, 120 GB; vi. 12 (doce) interfaces de red 10/100/1000 base-TX; vii. 8 (ocho) interfaces de red 1 Gbps SFP; viii. 2 (dos) Gbps interfaces dedicadas para alta disponibilidad; ix. 1 (una) interface de red 1 Gbps dedicada para administración; x. 1 (una) interface de tipo consola o similar; xi. Soporte a, como mínimo, 10 (diez) ruteadores virtuales; xii. Soporte a, como mínimo, 40 (cuarenta) zonas de seguridad; xiii. Soportar sin uso/necesidad de licenciamiento, 2.000 (mil) clientes de VPN SSL simultáneos; xiv. Soportar sin uso/necesidad de licenciamiento, 2.000 (mil) túneles de VPN IPSEC simultáneos; b. Por el equipamiento que compone la plataforma de seguridad, se entiende como hardware y licenciamiento de software necesarios para su funcionamiento; c. Por consola de administración y monitoreo, se entiende el licenciamiento de software necesario para las dos funcionalidades, también como hardware dedicado para el funcionamiento de las mismas. d. La consola de administración y monitoreo debe residir en el mismo appliance de seguridad de

red, teniendo un recurso de CPU, memoria, interfaz de red y sistema operacional dedicados para esta función;

b) Para efectos de la propuesta, ninguno de los modelos ofertados podrán estar listados en el site del fabricante como listas de end-of-life y end-of-sale.

CARACTERÍSTICAS GENERALES (cada equipo)

La solución debe consistir de un appliance de seguridad de red con funcionalidades de Next Generation Firewall (NGFW), y consola de administración y monitoreo
Por funcionalidades de NGFW se entiende: reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos
La plataforma debe ser optimizada para análisis de contenido de aplicaciones en Capa 7
El hardware y software que ejecuten las funcionalidades de seguridad de red y de administración y monitoreo, deben ser de tipo appliance. No serán aceptados equipamientos servidores y sistema operacional de uso genérico
Todos los equipamientos ofrecidos deben ser adecuados para montaje en rack 19”
El software deberá ser ofrecido en su versión más estable y/o más avanzada
Los dispositivos de seguridad de red deben poseer por lo menos las siguientes funcionalidades: - Soporte a 4094 VLAN Tags 802.1q; - Agregación de links 802.3ad; - Policy based routing o policy based forwarding; - Ruteo multicast (PIM-SM); - DHCP Relay; - DHCP Server; - Jumbo Frames; - Soporte a creación de objetos de red que puedan ser utilizados como dirección IP de interfaces L3; - Soportar sub-interfaces ethernet lógicas. - Debe soportar los siguientes tipos de NAT: - Nat dinámico (Many-to-1); - Nat dinámico (Many-to-Many); - Nat estático (1-to-1); - NAT estático (Many-to-Many); - Nat estático bidireccional 1-to-1; - Traducción de porta (PAT); - NAT de Origen; - NAT de Destino; - Soportar NAT de Origen y NAT de Destino simultáneamente; - Enviar log para sistemas de monitoreo externos, simultáneamente; - Debe tener la opción de enviar logs para los sistemas de monitoreo externos vía protocolo TCP y SSL; - Debe permitir configurar certificado caso necesario para autenticación del sistema de monitoreo externo de logs; - Seguridad contra anti-spoofing; - Para IPv4, debe soportar enrutamiento estático y dinámico (RIPv2, BGP y OSPFv2); - Para IPv6, debe soportar enrutamiento estático y dinámico (OSPFv3); - Soportar OSPF graceful restart; Soportar como mínimo las siguientes funcionalidades en IPv6: - SLAAC (address auto configuration), NAT64, Identificación de usuarios a partir de LDAP/AD, Captive Portal, IPv6 over IPv4 IPSec, Reglas de seguridad contra DoS (Denial of Service), Desencripción SSL y SSH, PBF (Policy Based Forwarding), QoS, DHCPv6 Relay, Activo/Activo, Activo/Pasivo, SNMP, NTP, SYSLOG, DNS y control de aplicaciones, sin necesidad de una licencia/suscripción anual; - Los dispositivos de seguridad deben tener la capacidad de operar de forma simultánea mediante el uso de sus interfaces físicas en los siguientes modos: Modo sniffer (monitoreo y análisis del trafico de red), Capa 2 (l2) y Capa 3 (l3); - Modo Sniffer, para inspección vía puerto espejo del tráfico de datos de la red; - Modo Capa – 2 (L2), para inspección de datos en línea y tener visibilidad del control del tráfico en nivel de aplicación; - Modo Capa – 3 (L3), para inspección de datos en línea y tener visibilidad del control del tráfico en

nivel de aplicación operando como default gateway de las redes protegidas; - Modo mixto de trabajo Sniffer, L2 e L3 en diferentes interfaces físicas; - La solución debe ser compatible y certificada (USGV6 en Firewall y/o IPS. No se aceptará certificación de otro tipo) para trabajar en IPv6. Soporte a configuración de alta disponibilidad Activo/Pasivo e Activo/Activo: - En modo transparente; - En layer 3; - La configuración en alta disponibilidad debe sincronizar: - Sesiones; - Configuraciones, incluyendo, mas no limitado a políticas de Firewall, NAT, QOS y objetos de red; - Certificados de-criptografados; - Asociaciones de Seguridad de las VPNs; - Tablas FIB; - El HA (modo de Alta-Disponibilidad) debe posibilitar monitoreo de fallo de link. - Las funcionalidades de control de aplicaciones, VPN IPSec y SSL, QOS, SSL y SSH Decription y protocolos de enrutamiento dinámico deben operar en carácter permanente, pudiendo ser utilizadas por tiempo indeterminado, incluso si no existe derecho de recibir actualizaciones o que no haya contrato de garantía de software con el fabricante.
Deberá soportar controles por zona de seguridad
Controles de políticas por puerto y protocolo.
Control de políticas por aplicaciones grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (basados en características y comportamiento de las aplicaciones) y categorías de aplicaciones
Control de políticas por usuarios, grupos de usuarios, IPs, redes y zonas de seguridad
Control de políticas por código de País (Por ejemplo: BR, USA, UK, RUS)
Control, inspección y desencripción de SSL por política para tráfico de entrada (Inbound) y Salida (Outbound)
Debe soportar offload de certificado en inspección de conexiones SSL de entrada (Inbound)
Debe desencriptar trafico Inbound y Outbound en conexiones negociadas con TLS 1.2
Control de inspección y desencripción de SSH por política
La plataforma de seguridad debe implementar espejamiento de trafico desencriptado (SSL y TLS) para soluciones externas de análisis (Análisis forense de red, DLP, Análisis de Amenazas, entre otras)
Es permitido el uso de appliance externo, específico para la desencripción de (SSL y TLS), con espejamiento de copia del trafico desencripción tanto para el firewall, como para las soluciones de análisis
Bloqueos de los siguientes tipos de archivos: bat, cab, dll, exe, pif, e reg
Traffic shaping QoS basado en Políticas (Prioridad, Garantía y Máximo)
QoS basado en políticas para marcación de paquetes (diffserv marking), inclusive por aplicaciones
Soporte a objetos y Reglas IPV6
Soporte a objetos y Reglas multicast
Soportar los atributos de agenda de las políticas con el objetivo de habilitar y deshabilitar políticas en horarios predefinidos automáticamente
Debe ser posible la liberación y bloqueo solamente de aplicaciones sin la necesidad de liberación de puertos y protocolos
Reconocer por lo menos 3000 aplicaciones diferentes, incluyendo, mas no limitado: el trafico relacionado a peer-to-peer, redes sociales, acceso remoto, update de software, protocolos de red, voip, audio, vídeo, proxy, mensajería instantánea, compartición de archivos, e-mail
Reconocer por lo menos las siguientes aplicaciones: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs, etc.
Debe inspeccionar el payload del paquete de datos con el objetivo de detectar a través de expresiones regulares firmas de aplicaciones conocidas por los fabricantes independiente del puerto y protocolo. El chequeo de firmas también debe determinar si una aplicación está utilizando su puerto default o no, incluyendo, mas no limitando a RDP en el puerto 80 en vez del 389
Debe aplicar análisis heurístico a fin de detectar aplicaciones a través de análisis del comportamiento del trafico observado, incluyendo, mas no limitado a Encrypted Bittorrent y aplicaciones VOIP que utilizan criptografía propietaria
Identificar el uso de tácticas evasivas, o sea, debe tener la capacidad de visualizar y controlar las aplicaciones y los ataques que utilizan tácticas evasivas vía comunicaciones criptografiadas, tales como Skype y ataques mediante el puerto 443

Para tráfico criptografado (SSL y SSH), debe desencripción paquetes con el fin de posibilitar la lectura del payload para chequeo de firmas de aplicaciones conocidas por el fabricante
Debe realizar decodificación de protocolos con el objetivo de detectar aplicaciones encapsuladas dentro del protocolo y validar si el tráfico corresponde con la especificación del protocolo, incluyendo, mas no limitado a Yahoo Instant Messenger usando HTTP. La decodificación de protocolo también debe identificar funcionalidades específicas dentro de una aplicación, incluyendo, mas no limitado a la compartición de archivos dentro de Webex. También debe detectar el archivo y otros contenidos que deben ser inspeccionados de acuerdo a las Reglas de seguridad implementadas
Debe Identificar el uso de tácticas evasivas vía comunicaciones criptografiadas
Debe Actualizar la base de firmas de aplicaciones automáticamente
Debe Reconocer aplicaciones en IPv6
Limitar el ancho de banda (download/upload) usado por aplicaciones (traffic shaping), basado en IP de origen, usuarios y grupos del LDAP/AD
Los dispositivos de seguridad de red deben poseer la capacidad de identificar al usuario de red con integración al Microsoft Active Directory, sin la necesidad de instalación de agente en el Domain Controller, ni en las estaciones de los usuarios
Debe ser posible adicionar control de aplicaciones en todas las Reglas de seguridad del dispositivo, o sea, no limitándose solamente a la posibilidad de habilitar control de aplicaciones en algunas Reglas
Debe soportar múltiples métodos de identificación y clasificación de las aplicaciones, por lo menos chequeo de firmas, decodificación de protocolos y análisis heurístico
Para mantener la seguridad de la red eficiente, debe soportar el control sobre aplicaciones desconocidas y no solamente sobre aplicaciones conocidas
Permitir nativamente la creación de firmas personalizadas para reconocimiento de aplicaciones propietarias en la propia interface gráfica de la solución, sin la necesidad de acción por parte del fabricante, manteniendo la confidencialidad de las aplicaciones del órgano
La creación de firmas personalizadas debe permitir el uso de expresiones regulares, contexto (sesiones o transacciones), usando la posición en el payload de los paquetes TCP y UDP y usando decoders de por lo menos los siguientes protocolos: - HTTP - FTP - SMB - SMTP - Telnet - SSH - MS-SQL - IMAP - IMAP - MS-RPC - RTSP - File body
El fabricante debe permitir la solicitud de inclusión de aplicaciones en la base de firmas de aplicaciones
Debe posibilitar la diferenciación de tráficos de Instant Messaging (AIM, Gtalk, Facebook Chat, etc.) proveyendo granularidad de control/políticas para los mismos
Para seguridad del ambiente contra ataques, los dispositivos de seguridad deben poseer módulo de IPS, Antivirus y Anti-Spyware integrados en el propio appliance de Firewall
Debe incluir firmas de prevención de intrusos (IPS) y bloqueo de archivos maliciosos (Antivirus y Anti-Spyware)
Las funcionalidades de IPS, Antivirus y Anti-Spyware deben operar en carácter permanente, pudiendo ser utilizadas por tiempo indeterminado, incluso si no existe el derecho de recibir actualizaciones o que no haya contrato de garantía de software con el fabricante
Debe sincronizar las firmas de IPS, Antivirus, Anti-Spyware cuando esté implementado en alta disponibilidad Activo/Activo e Activo/pasivo
Cuando se utilicen las funciones de IPS, Antivirus y Anti-spyware, el equipamiento debe entregar el mismo performance (no degradar) entre tener 1 única firma de IPS habilitada o tener todas las firmas de IPS, Anti-Virus y Antispyware habilitadas simultáneamente
Las firmas deben poder ser activadas o desactivadas, o incluso habilitadas apenas en modo de monitoreo
Debe soportar granularidad en las políticas de IPS Antivirus y Anti-Spyware , permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio y la combinación de todos esos ítems
Debe permitir el bloqueo de vulnerabilidades
Debe permitir el bloqueo de exploits conocidos

Debe incluir seguridad contra ataques de negación de servicios
Poseer la capacidad de análisis de amenazas no conocidas
Debido a los Malwares hoy en día hay que ser muy dinámicos y un antivirus común no es capaz de detectar los mismos a la misma velocidad que sus variaciones son creadas, la solución ofertada debe poseer funcionalidades para análisis de Malwares no conocidos incluidas en la propia herramienta
El dispositivo de seguridad debe ser capaz de enviar archivos transferidos de forma automática para análisis "In Cloud" o local, donde el archivo será ejecutado y simulado en un ambiente controlado
Seleccionar a través de la política de Firewall que tipos de archivos sufrirán este análisis
Soportar el análisis como por lo menos 60 (sesenta) tipos de comportamientos maliciosos para el análisis de la amenaza no conocida
Soportar el análisis de archivos maliciosos en ambiente controlado como mínimo, sistema operacional Windows XP y Windows 7
Debe soportar el monitoreo de archivos transferidos por internet (HTTP, FTP, HTTP, SMTP) como también archivos transferidos internamente en los servidores de archivos usando SMB
El sistema de análisis “In Cloud” o local debe proveer informaciones sobre las acciones del Malware en la máquina infectada, informaciones sobre cuales aplicaciones son utilizadas para causar/propagar la infección, detectar aplicaciones no confiables utilizadas por el Malware, generar firmas de Antivirus y Anti-spyware automáticamente, definir URLs no confiables utilizadas por el nuevo Malware y proveer informaciones sobre el usuario infectado (su dirección ip y su login de red)
El sistema automático de análisis "In Cloud" o local debe emitir relación para identificar cuales soluciones de antivirus existentes en el mercado poseen firmas para bloquear el malware
Soportar el análisis de archivos ejecutables, DLLs, ZIP y criptografiados en SSL en el ambiente controlado
Soportar el análisis de archivos del paquete office (doc, docx, xls, xlsx, ppt, pptx), archivos java (.jar e class) y Android APKs en el ambiente controlado
Poseer SLA de, como máximo, 40 minutos para actualización de la base de vacunas contra malwares desconocidos identificados en el ambiente controlado
Debe incluir la capacidad de creación de políticas basadas en la visibilidad y control de quien está utilizando cuales aplicaciones a través de la integración como servicios de directorio, autenticación vía ldap, Active Directory, E-directory y base de datos local
Debe poseer integración con Radius para identificación de usuarios y grupos permitiendo la granularidad de control/políticas basadas en usuarios y grupos de usuarios
Debe poseer integración con Ldap para identificación de usuarios y grupos permitiendo la granularidad de control/políticas basadas en Usuarios y Grupos de usuarios
Soportar la creación de políticas por Geo localización, permitiendo que el tráfico de determinado País/Países sea bloqueado, sin tener que depender de una licencia/suscripción especifica que tenga que renovarse anualmente
Soportar VPN Site-to-Site y Cliente-To-Site
Soportar IPSec VPN
Soportar SSL VPN
Debe centralizar la administración de Reglas y políticas del clúster, usando una única interfaz de administración
Debe realizar correlacionamiento de datos, en la misma plataforma, sin necesidad de un equipo extra o software que tenga que instalarse en un endpoint o equipo de una marca diferente a la ofertada como NGFW, para realizar esta funcionalidad
Realizar logging en la misma plataforma, sin necesidad de un equipamiento extra, o software que tenga que instalarse en un endpoint, para realizar esta funcionalidad
La administración de la solución debe soportar acceso vía SSH, WEB (HTTPS) y API abierta sin necesidad de tener un software instalado en un endpoint/servidor externo de manera manual
En el caso de que sea necesaria la instalación de cliente para administración de la solución, el mismo debe ser compatible con sistemas operativos Windows y Linux
La administración debe permitir/hacer: - Creación y administración de políticas de firewall y control de aplicaciones; - Creación y administración de políticas de IPS y Anti-Spyware; - Creación y administración de políticas de filtro de URL - Monitoreo de logs; - Herramientas de investigación de logs; - Debugging; - Captura de paquetes
Debe permitir el acceso concurrente de administradores

Debe tener un mecanismo de búsqueda de comandos de administración vía SSH, facilitando la localización de los comandos
Debe permitir monitorear vía SNMP fallas en el hardware, inserción o remoción de fuentes, discos y ventiladores, uso de recursos por número elevado de sesiones, número de túneles establecidos de VPN cliente-to-site, porcentaje de utilización en referencia al número total soportado/licenciado y número de sesiones establecidas
Debe posibilitar la integración con otras soluciones de SIEM del mercado (third-party SIEM vendors)
Debe permitir la generación de logs de auditoría detallados, informando de la configuración realizada, el administrador que la realizó y el horario de la alteración
Debe ser posible exportar los logs en CSV
Deberá ser posible acceder al equipamiento a aplicar configuraciones durante momentos donde el tráfico sea muy alto y la CPU y memoria del equipamiento este siendo totalmente utilizada
Debe tener rotación de logs
Debe tener presentaciones de las siguientes informaciones, de forma histórica y en tiempo real (actualizado de forma automática y continua cada 1 minuto): - Debe mostrar la situación del dispositivo y del clúster; - Debe poder mostrar las principales aplicaciones; - Debe poder mostrar las principales aplicaciones por riesgo; - Debe poder mostrar los administradores autenticados en la plataforma de seguridad; - Debe poder mostrar el número de sesiones simultáneas; - Debe poder mostrar el estado de las interfaces; - Debe poder mostrar el uso de CPU;
Debe poder mostrar las principales aplicaciones
Debe poder mostrar las principales aplicaciones por riesgo
Generación de reportes. Como mínimo los siguientes reportes deben poder ser generados: - Resumen gráfico de las aplicaciones utilizadas; - Principales aplicaciones por utilización de ancho de banda de entrada y salida; - Principales aplicaciones por tasa de transferencia en bytes; - Principales hosts por número de amenazas identificadas; - Actividades de un usuario específico y grupo de usuarios del AD/LDAP, incluyendo aplicaciones accedidas y amenazas (IPS, y Anti-Spyware), de red vinculadas a este tráfico; - Debe permitir la creación de reportes personalizados;

1.2.: Solución de control de acceso a cuentas privilegiadas

DESCRIPCIÓN GENERAL
a) El proveedor deberá ser capaz de brindar una Administración Centralizada y segura que permita automatizar las contraseñas de las cuentas de administración de sistemas, de servicios y de aplicaciones, así como poder aplicar políticas de contraseñas fuertes para el acceso a los dispositivos y aplicaciones. b) El proveedor deberá impartir capacitación oficial sobre las soluciones ofertadas, la cual debe incluir derecho a examen de certificación. c) La solución deberá tener una visión global del uso de cuentas privilegiadas a través de reportes y tableros de control que permitan el cumplimiento de regulaciones.
SERVIDOR DE ADMINISTRACIÓN Y CONSOLA ADMINISTRATIVA
a) El Proveedor debe de estar incluido en el Informe de Gartner denominado “Magic Quadrant for Endpoint Protection Platforms” dentro del cuadrante de líderes en los últimos 5 períodos. b) El proveedor deberá impartir capacitación oficial sobre las soluciones ofertadas, la cual debe incluir derecho a examen de certificación. c) La solución debe disponer de una consola de gestión centralizada que permita la instalación, configuración, actualización y administración de todas las soluciones ofertadas de manera integral, facilitando la gestión de la seguridad.
CARACTERÍSTICAS GENERALES
La solución debe permitir soportar al menos los siguientes sistemas objetivos: • Servidores Windows • Servidores UNIX/LINUX • Mainframes IBM • Dispositivos de red • Servicios en la nube
La solución debe soportar tecnologías de Bases de datos (RDBMS) o Directorios (LDAP) para su repositorio propio.
La solución debe soportar los siguientes modos y entornos de trabajo en modo seguro: Modo: FIPS 140-2 Entorno: IPv4 y IPv6
La solución debe permitir controles de acceso granulares basado en perfiles de tiempo (día/fecha/hora) a nivel de usuario o de grupo de usuarios.
La solución debe permitir que la inscripción sea realizada por módulos de criptografía basado en hardware (HSM: Hardware Security Modules tales como Safenet & Thales) para cumplir con FIPS 140-2
La solución debe soportar los siguientes esquemas de implementación a nivel de arquitectura de red • Detrás de un Firewall • Detrás de una solución de VPN existente • En forma paralela a una solución de VPN existente • Entre redes Físicas y redes virtuales • En Entornos CITRIX Registrar la actividad de la sesión del usuario privilegiado realizada desde: • Línea de comandos • Entorno gráfico (incluido RDP) • VNC (virtual Network Computing) La solución PSM debe poder permitir la revisación de la actividad del usuario privilegiado a través de facilidades de ‘Playback’ de acciones realizadas. La solución PSM debe poder permitir la búsqueda de texto dentro de la grabación realizada. La solución debe tener mecanismos de autoprotección que eviten que los archivos de auditoría de

accesos puedan ser modificados o borrados.
La solución PSM debería poder grabar sesiones de acceso a aplicaciones web, de forma tal que todas las acciones de usuarios privilegiados que acceden a aplicaciones web sean grabadas tal como las otras grabaciones tareas administrativas.
La solución Privilege Threat Analytics (PTA) debe proveer de Algoritmos Heurísticos expertos que permitan identificar anomalías en el comportamiento del usuario y en la utilización de la cuenta privilegiada
La solución PTA debe proveer un 'scoring' de amenazas asignado a cada anomalía individual, incidente, o grupo de eventos que ayude a priorizar el tratamiento de eventos que implican un riesgo mayor.

La solución PTA debe proveer Alertas dirigidas y operables que incluyan información detallada del evento para permitir que los equipos de atención de incidentes respondan en forma focalizada al ataque.

La solución PTA debe proveer de Tableros de Control que brinden una representación visual fácil de comprender a nivel de incidentes y niveles de amenazas asociados a información histórica.

La solución PTA debe brindar facilidades de Respuestas Automatizadas que permitan tomar acciones inmediatas sobre las acciones de un usuario individual que presenta un nivel elevado de riesgo, arrancando la grabación de la sesión o pidiendo una segunda autenticación adicional.

La solución SUPM (Privilege elevation and Delegation Management) debe ser capaz de filtrar comandos para dispositivos o grupos de dispositivos a nivel de línea de comando para entornos accedidos vía TELNET, SSH y consolas seriales.

La solución SUPM debe ser capaz de filtrar comandos para dispositivos o grupos de dispositivos a nivel de línea de comando para entornos accedidos vía TELNET, SSH y consolas seriales sin necesidad de instalar agentes.

La solución SUPM debe ser capaz de implementar el filtrado de comandos siguiendo los criterios de:

- 'blacklists' (comandos prohibidos que un usuario no puede ingresar)
- 'whitelists'(comandos permitidos explícitamente , todo lo demás está prohibido)

La solución SUPM debe ser capaz de establecer diferentes tipo de acciones para el filtrado de comandos:

- Registrar (log)
- Alertar
- Remediar
- Evitar su ejecución (Parar)

La solución SUPM debe ser capaz de filtrar 'sockets' para restringir el acceso desde/hacia dispositivos tipo servidores.

La solución SUPM debe ser capaz de implementar el filtrado de 'sockets' siguiendo los criterios de Listas de filtros a nivel 'Socket' definiendo grupos de servidores o redes desde los cuales se pueden aplicar reglas que eviten el ataque 'a saltos' (leapfrog).

La solución SUPM debe proveer controles de monitoreo y acceso que permitan establecer políticas centralizadas de:

- Control de Acceso y Monitoreo de Archivos de Configuración
- Control de Acceso y Monitoreo de Procesos Críticos del Sistema
- Control de Acceso y Monitoreo de la Modificación de ejecutables críticos del sistema
- Control de Acceso y Monitoreo de la Delegación de Autoridad de Cuentas Privilegiadas (SUDO)

La solución SUPM debe brindar mecanismos de control y monitoreo de archivos críticos de la instalación de manera tal que si estos archivos son modificados sea generado un registro de auditoría que pueda ser ruteado de distintas maneras.

Ejemplo de archivos críticos:

For UNIX
/etc/services
/etc/protocols
/Etc/hosts

/Etc/hosts.equiv

La solución SUPM debe brindar mecanismos de y monitoreo que permitan controlar que la ejecución de un programa o comando sea realizado solo desde una biblioteca autorizada usando programas aprobados.
La solución SUPM debe brindar mecanismos de control y monitoreo de todos los tipos de archivos (NTFS, FAT, CDFS) en las plataformas soportadas, con controles granulares a nivel de lectura, escritura, modificación, borrado, etc., sin reemplazar o modificar los permisos de acceso a archivos nativos del sistema operativo.
La solución SUPM debe proveer mecanismos de control y monitoreo que protejan los servicios y procesos claves de los servidores críticos, detectando registrando, protegiendo y alertando su estado y modificaciones (stop, kill, restart, ID change, etc.).
La solución SUPM debe proveer mecanismos de control y monitoreo que permitan reforzar la integridad de los archivos y permita establecer la firma digital de programas sensibles y cualquier cambio al mismo sea detectado y no permita su ejecución hasta que sea autorizado nuevamente.
La solución SUPM debe proveer mecanismos de control y monitoreo que sean capaces de proteger comandos privilegiados y limitar su uso a personal autorizado, a través de listas de control de acceso u otros mecanismos, sin necesidad de reemplazar o modificar permisos nativos.
La solución SUPM debe proveer mecanismos de control y monitoreo que controlen el acceso online por terminal o consola a la función de surrogate (suid o sgid), controlando que los usuarios 'no root' asuman privilegios 'root'. Adicionalmente la solución debe proveer mecanismos que controlen el acceso a los programas (setuid, setgid) que puedan usar la función de surrogate (suid o sgid), controlando que los usuarios 'no root' asuman privilegios 'root'.
La solución SUPM debe proveer mecanismo de control y monitoreo que faciliten la Segregación de Funciones mediante mecanismos que eviten y/o en su defecto controlen la actividad de cuentas compartidas (share id). Describir mecanismos. (por ejemplo: que un administrador de sistema aún trabajando como 'root', no pueda modificar el archivo de configuración de base de datos (función del DBA).
La solución SUPM debe brindar mecanismo de control y monitoreo que permitan que los usuarios privilegiados puedan tener múltiples sesiones en un servidor con todos los controles pertinentes, sin necesidad de restringir la operatoria a una única sesión para poder controlar al usuario privilegiado.
La solución SUPM debe proveer mecanismos de control y monitoreo que controlen el acceso online por terminal o consola a la función de surrogate (suid o sgid), controlando que los usuarios 'no root' asuman privilegios 'root'. Adicionalmente la solución debe proveer mecanismos que controlen el acceso a los programas (setuid, setgid) que puedan usar la función de surrogate (suid o sgid), controlando que los usuarios 'no root' asuman privilegios 'root'.
La solución SUPM debe tener la capacidad de registrar todas las acciones de un usuario relacionándola con la identidad original, aún cuando el usuario haya realizado un 'surrogate' a un usuario diferente, incluyendo 'root' o 'administrator'.
La solución SUPM debe tener mecanismos de autoprotección que eviten que los archivos de auditoría de accesos puedan ser modificados o borrados por usuarios privilegiados que usen la autoridad de 'admin' o 'root'.

1.3.: Solución de AntiSpam

DESCRIPCIÓN GENERAL
Se deberá suministrar el equipamiento necesario para proporcionar el servicio de filtrado de correo y cifrado de correo electrónico a nivel de Gateway, para al menos 2500 usuarios en alta disponibilidad “activo-activo”.
CARACTERÍSTICAS GENERALES
La solución debe de ser ofrecida en Hardware Appliance de propósito único en arquitectura de procesadores en 64 bits.
La solución debe ofrecer protección del servicio de correo en múltiples capas, utilizando técnicas de filtrado de conexiones y escaneo profundo en los mensajes.
Protección que permita rechazar el correo no deseado (spam), mediante la previa verificación y comprobación de las direcciones ip de mensajería entrante, en bases de datos especializadas con registros de sitios considerados como altamente generadores de “spam”.
Deberá poseer al mínimo 3 capas de protección antivirus.
La solución debe de hacer cache de firmas de antivirus localmente en una BBDD que se actualiza automáticamente.
La solución debe ofrecer protección en tiempo real que bloqueará nuevos spam y los virus en tiempo real, sin tener que esperar nuevas definiciones estén descargadas en el appliance.
Deberá ser capaz de proteger correo electrónico entrante (desde Internet) y correo saliente (hacia Internet).
Capacidad incluida de conectarse en tiempo real a una base de datos centralizada en el fabricante para descargar actualizaciones.
Protección contra ataques de negación de servicio.
Verificaciones de DNS en reversa para proveer protección tipo Anti-Spoofing.
Establecer límites en la tasa de correos enviados y recibidos.
Capacidad de soportar múltiples dominios de correo electrónico.
Establecer políticas de correo electrónico por dominio, para correo entrante o correo saliente.
Capacidad de establecer perfiles (políticas) granulares de detección de SPAM.
Ruteo de correo basado en LDAP.
Capacidad de poder hacer cuarentena de correo entrante y saliente.
Soporte a colas de correo para mensajes fallidos, retardados y no entregables.
Poder hacer autenticación para SMTP a través de LDAP, RADIUS, POP3 o IMAP.
Filtraje de archivos anexos (attachments) y contenido de mensaje de correo.
Capacidad de bloquear usando listas RBL de SPAM.
Filtraje por palabra prohibida.
Administración de SPAM con capacidades de Aceptar, Reenviar (Relay) Rechazar (Reject) o descartar (discard).
Rastreo por análisis de imágenes para detectar SPAM.
Listas negras y blancas (usuarios/dominios/ direcciones IP)
La vigencia de la licencia de actualización deberá incluir la capacidad de poder hacer actualizaciones de firmas anti spam, antivirus y cualquier otra actualización necesaria para la correcta operación del equipo.
Bloqueo de spam en otros idiomas.
Deberá generar información del uso del filtro de SMTP, la cual debe poder ser leída y explotada por otro dispositivo mediante formato syslogs, txt y/o csv o xls sin generar una afectación a la continuidad del servicio.
Interface de configuración vía Web (HTTP, HTTPS).
Los administradores podrán ser por dominio y deberá poder asignarse de qué equipos (por dirección IP y máscara) puede el administrador conectarse.
Debe aceptar por lo menos dos niveles de administración: Lectura/Escritura (Read/Write) y Sólo Lectura (Read-Only)
Soporte a SNMP versión 1 / versión 2 usando MIBS estándares y MIBS privados con Traps basadas en umbrales.
Soporte a registro (logging) de actividad antispam
Soporte a syslog externo
Deberá poseer al mínimo 18 reportes diarios
Deberá generar reportes bajo demanda o un reportes calendarizados en intervalos específicos
Los reportes pueden ser generados y enviados como PDF
La solución debe ofrecer a los usuarios la capacidad de la lista blanca / lista negra de remitentes, así como gestionar su propio correo no deseado.
La solución debe ser capaz de realizar búsquedas federadas a través de los registros entre aparatos distribuidos.
La solución debe tener la capacidad para los administradores bloquear mensajes de correo electrónico a través de la cabecera / sujeto / body utilizando expresiones regulares expresiones y coincidencias de palabras exactas.

La solución debe ser capaz de bloquear los archivos adjuntos por tipo de archivo y extensión de archivo.
La solución debe tener la capacidad de obligar conexión SMTP a través de TLS al enviar o recibir correo electrónico de un dominio específico.
La solución debe tener la capacidad de utilizar una base de datos de direcciones IP y dominios para ayudar a bloquear el spam.
La solución debe ser capaz de bloquear los mensajes de devolución / NDR.
La solución debe tener la capacidad para hacer cumplir la política de correo electrónico basado en el tipo de caracteres en las partes del mensaje.
La solución debe ser capaz de realizar una búsqueda DNS inversa en la dirección IP del remitente, determinar el Top Level Domain (TLD) y correos electrónicos de bloques procedentes de direcciones IP asignadas a los proveedores en países conocidos comúnmente de enviar spam.
La solución debe permitir a los administradores crear reglas personalizadas basadas en los resultados de búsqueda de DNS inversa de la dirección IP del remitente.
La solución debe ser capaz de hacer cumplir la política de correo electrónico mediante la comprobación del servidor de nombres de un dominio de referencia en URL incrustado y validación frente a una lista de servidores de nombres conocidos de ser utilizados exclusivamente por spammers.
La solución debe ser capaz de hacer cumplir la política de correo electrónico mediante la inspección del contenido de los sitios web gratuitos, tales como GeoCities y Blogspot vinculados a los URL en los mensajes de spam.
La solución debe ser capaz de evitar que los spammers envíen grandes cantidades de correo electrónico al dispositivo a través de un corto período de tiempo desde cualquier dirección IP.
La solución debe ser capaz de utilizar SNMP para la supervisión y alertas y utilizar una API para hacer cambios de configuración sin tener que entrar en el aparato.
La solución debe ser capaz de proporcionar la seguridad de correo electrónico híbrido; nube de pre-filtrado de tráfico de correo electrónico entrante para detener el spam y el malware con la entrega de correo electrónico pre-filtrado en un appliance local.
La solución debe ser capaz de proporcionar la continuidad de correo electrónico a través de la cola en la nube y la entrega a un servidor de correo electrónico alternativo de ser necesario.
La solución debe ser capaz de hacer el cifrado de correo electrónico saliente con un Microsoft Outlook add-in.
La solución debe ser capaz de proporcionar una protección antivirus de correo electrónico interno con el Microsoft Exchange Agent Virus add-in que debe sincronizarse con el appliance local.
La solución debe ser capaz de recibir correos electrónicos de redes IPv6, aplicar políticas de contenido, y entregar a cualquier red IPv4 o IPv6.

1.4.: Solución SIEM

DESCRIPCIÓN GENERAL
La solución SIEM deberá poder correlacionar eventos casi en tiempo real, proporcionar granularidad de perfiles de seguridad, deberá poseer alta disponibilidad en todas las ramas de su implementación, deberá ser escalable en el tiempo, deberá poseer integración con herramientas de Análisis de Vulnerabilidades, deberá poseer licenciamiento perpetuo.
CARACTERÍSTICAS GENERALES
La solución SIEM debe proporcionar una gestión centralizada de todos los componentes y funciones administrativas desde una única interfaz basada en web (Actividad de logs, flujos de red, base de activos, vulnerabilidades, reportes y panales de administración).
La solución debe definir el acceso basado en roles, por dispositivo, grupo de dispositivos, rangos de red. También debe restringir a los usuarios y/o grupos acceso solo a la información de dispositivos, grupos de dispositivos y rangos de red respectivos. Esto incluye ser capaz de restringir el acceso de un usuario a funciones específicas de la solución que no está dentro del alcance de un papel usuarios incluyendo, pero no limitados a la administración, presentación de informes, el filtrado de eventos, de correlación, y / o la visualización de Dashboard.
La solución debe realizar el descubrimiento en forma automática de los activos que están siendo protegidos o monitoreados. Debe ser capaz de realizar la clasificación automática de los mismos.
La solución debe contar con una interfaz de trabajo (Dashboard) totalmente configurable, debe permitir el detachment de los Dashboard predefinidos de la Interfaz del usuario para ser utilizados en Dashboard customizados para el SOC o NOC
La solución debe proveer una API para el acceso a los datos almacenados en la Base de Datos
La solución deberá contar con un repositorio de aplicaciones (plug-ins) y contenidos adicionales para la incorporación de paquetes de reportes y funcionalidades de terceros (integraciones avanzadas).
La solución debe encontrarse como Líder en el último Gartner Magic Quadrant for Security Information and Event Management (Agosto 2016).
La solución debe tanto a nivel de gestión de LOGs y SIEM permitir la introducción de más capacidades de análisis y debe minimizar la necesidad de componentes adicionales del sistema, activándose mediante la adquisición de licencias.
La solución debe ser compatible con la actualización automática de la información de configuración con una intervención mínima del usuario. Por ejemplo, las actualizaciones de seguridad, actualizaciones de la taxonomía de reglas proveedor, soporte de dispositivos.
La solución debe poseer una interfaz gráfica de usuario basada en web para la gestión, el análisis y presentación de informes.
La solución debe soportar la configuración de alta disponibilidad en un modo integrado y sin la necesidad de software adicional de terceros. Debe asegurar que todos los componentes de sistemas distribuidos continúan funcionando cuando cualquier otra parte del sistema falla o pierde la conectividad. (Es decir, la consola de administración pudiera estar fuera de línea, todos los colectores separados todavía continúan trabajando en la captura de registros, que se actualizarán al restablecimiento de la comunicación.
La solución debe contar con un proceso de copia de seguridad / recuperación automatizada.
La solución debe en forma automática realizar Health Check y notificar en el caso de que se detecte algún inconveniente.
La solución debe mantener una base de datos de todos los activos descubiertos en la red. Estos datos de activos deben incluir información importante sobre el activo y de la información recolectada (es decir, los atributos del sistema, los atributos de red, estado de vulnerabilidad, etc.). La base de datos debe ofrecer la posibilidad de editar los atributos cuando no se pueden descubrir en forma automática (es decir, departamento, ubicación, etc.). El usuario debe ser capaz de realizar búsquedas en esta base de datos.
La solución debe poseer soporte local directo o a través de un asociado de negocio.
La solución debe integrarse con otras soluciones de seguridad y de inteligencia de red
La solución debe poder ampliarse/expandirse fácilmente para apoyar la demanda adicional sin límites. El fabricante debe acreditar implementaciones de al menos 800.000 EPS.
La solución debe poseer una base de datos distribuida para los eventos y actividad de la red de tal manera que pueda accederse a toda la información desde una única interfaz de usuario.
La solución debe poseer un modelo distribuido para la correlación de tal manera que los contadores, las secuencias y las búsquedas sean compartidos por todos los colectores (por ejemplo, buscar 25 intentos fallidos de conexión del mismo nombre de usuario seguido de un único inicio de sesión correcto para ese mismo nombre de usuario, donde los eventos vistos por un solo colector no superan el umbral de 25, pero a través de múltiples colectores superaría el umbral).
La solución debe poseer una taxonomía de eventos y campos. El usuario debe ser capaz de añadir sus propios nombres de eventos únicos (es decir, la posibilidad de añadir nuevos campos que no forman parte del esquema por defecto).
La solución debe tener una recopilación de registros y la arquitectura de archivo que admita tanto a corto plazo (en línea) y largo plazo (sin conexión) de almacenamiento de eventos

La solución debe ser compatible con los métodos de recopilación de logs de la industria (syslog, WMI, JDBC, SNMP, Checkpoint LEA, OPSEC, ALE, registros de FTP, SCP, SFTP).
La solución debe proporcionar recopilación sin agentes de los registros de eventos siempre que sea posible.
La solución debe proporcionar la capacidad de distribuir tanto el almacenamiento y el procesamiento de eventos a través de todo el despliegue de gestión de LOGs/ SIEM.
La solución debe ser compatible con el acceso a largo plazo a los eventos de seguridad detallada y datos de flujo de red. El sistema debe ser capaz de proporcionar el acceso a al menos 12 meses el valor de la información detallada.
La solución debe normalizar campos comunes de eventos (es decir, nombres de usuarios, direcciones IP, nombres de host e inicie sesión dispositivo fuente, etc.) de los distintos tipos de dispositivos en una arquitectura de múltiples proveedores.
La solución debe proporcionar la capacidad de almacenar / conservar tanto los eventos normalizados como el original en bruto para fines forenses.
La solución debe proporcionar la capacidad de normalizar campos de eventos globales que no están representados por los campos normalizados por defecto.
La solución debe normalizar las marcas de tiempo de eventos a través de múltiples zonas horarias.
La solución debe realizar un análisis en tiempo casi real de los eventos
La solución debe realizar análisis de tendencias a largo plazo de los eventos
La solución debe realizar el Drill-down avanzado de eventos en caso de ser necesario
La solución debe generar alertas basadas en análisis de anomalías y cambios de comportamiento en los eventos de la red y de seguridad
La solución debe apoyar y mantener un historial de la actividad de autenticación de usuario en función de cada activo
La solución debe proporcionar reportes, sobre todos los elementos disponibles para la gestión a través de la interfaz gráfica de usuario
La solución debe proporcionar un motor de informes configurable para la creación de informes personalizados.
La solución debe poseer plantillas para la creación y entrega de informes en múltiples niveles que van desde operaciones a actividades específicas de la entidad
La solución debe proporcionar informes out-of-the-box, para las cuestiones operativas típicas del negocio, como mínimo reportes de: - Autenticación - Identidad - Actividad del usuario - Cumplimiento de normativas - Gestión de configuraciones y cambios - Gestión de red - Seguridad - Monitoreo de uso - Actividad de las aplicaciones - Informes específicos por dispositivos (sistema operativos, base de datos, etc.) Gerenciales / Ejecutivos
La solución debe proporcionar reportes out-of-the-box de cumplimiento de las regulaciones específicas (PCI, SOX, FISMA) y marcos de control incluidos (NIST, COBIT, ISO).
La solución debe proporcionar un "Dashboard" para la visualización rápida de reportes de seguridad y la información de red. Como mínimo debe brindar - Cualquier búsqueda de eventos o flujo - Lista y estados de incidentes y ofensas - Top de ofensas, por destino, categoría y origen - Top de eventos por severidad - Top de eventos por origen - Estado del sistema - Reportes generados recientemente
La solución debe realizar informes de tendencias históricas.
La solución deberá incluir cientos de reglas de correlación para la detección automática de potenciales incidentes de seguridad.
La solución debe proporcionar la capacidad de correlacionar la información a través de dispositivos de distintos fabricantes.
La solución debe proporcionar alertas sobre la base de las anomalías observadas y los cambios de comportamiento en la actividad de red de datos (flujos de datos).
La solución debe proporcionar alertas en base a la política establecida. (por ejemplo, no se permite el tráfico de mensajes instantáneos).
La solución debe generar alertas basadas en criticidad, para tener en cuenta las prioridades. La criticidad

debe poder asignarse sobre la base de múltiples características, como el tipo de activos, el protocolo, la aplicación.
La solución debe proporcionar la capacidad de transmitir alertas usando múltiples protocolos y mecanismos a otras soluciones de gestión.
La solución debe proporcionar en la interfaz del usuario un asistente con la capacidad para minimizar los falsos positivos y entregar resultados precisos del ambiente.
La solución debe limitar la presentación de múltiples alertas similares.
La solución debe poseer la capacidad de tomar medidas tras haber recibido una alerta. Por ejemplo, la solución debe poder iniciar scripts o enviar un mensaje de correo electrónico.
La solución debe poseer la capacidad de correlacionar eventos contra información de productos de seguridad de terceros (es decir, la cartografía redes “botnets” conocidos, direcciones IP con mala reputación, etc.). Estas fuentes de datos de terceros deben ser actualizados automáticamente por la solución
La solución debe brindar la capacidad de correlacionar resultados del análisis de vulnerabilidad de productos de terceros, como mínimo debe soportar: - Tenable Nessus - Nmap - Rapid 7 - Qualys - AppScan - Guardium - Digital Defense
La solución debe vigilar y alertar cuando hay una interrupción en la recopilación de registros de un dispositivo. En otras palabras, si los registros no son vistos desde un servidor en una cantidad determinada de minutos, generar un alerta.
La solución debe proporcionar un mecanismo out-of-the-box para descubrir y clasificar los activos por tipo de sistema (es decir, servidores de correo frente a servidores de bases de datos) para minimizar los falsos positivos asociados a una mala clasificación de los activos.
La solución debe realizar la correlación de una secuencia fallida. Ejemplo un servicio parado, que no fue seguido del restablecimiento del mismo luego de 5 minutos.
La solución debe realizar la correlación de valores aditivos a través del tiempo. Por ejemplo, alerta cuando cualquier IP envía más de 1 GB de datos a un solo puerto a una sola IP de destino en un período de una hora de tiempo.
La solución debe proporcionar un mecanismo, para optimizar el tunning de las reglas, que permite la agrupación de valores de entrada similares de una regla de correlación que puede ser utilizado por varias reglas. Este mecanismo de agrupación deberá permitir tanto para grupos estáticos, como grupos dinámicos creados por otras reglas de correlación. Por ejemplo, el usuario del sistema puede definir un grupo de puertos/protocolos prohibidos que se debe utilizar a través de múltiples reglas de correlación que supervisan la actividad inapropiada en la red.
La solución debe proporcionar capacidad de enviar notificación de alertas correlacionadas a través de procedimientos bien definidos (es decir, traps SNMP, correo electrónico, etc.)
La solución debe poseer una herramienta de workflow integrado, que el personal de operaciones de seguridad pueda utilizar
La solución debe proporcionar una integración bidireccional con aplicaciones de gestión de mesa de ayuda (APIs).
La solución debe proporcionar un mecanismo para marcar incidente de seguridad/ofensas, y dirigirlas por el personal de las operaciones de seguridad.
La solución debe proporcionar un mecanismo para el seguimiento de los incidentes de seguridad a través de una amplia gama de atributos relevantes (es decir, direcciones IP, nombres de usuario, dirección MAC, de registro de origen, reglas de correlación, definido por el usuario, etc.). El usuario debe ser capaz de filtrar los incidentes utilizando los atributos definidos.
La solución deberá poder descubrir automáticamente las fuentes de eventos, y con solo recibirlos deberá poder catalogarlos automáticamente.
La solución deberá tener documentada y pública la lista de integraciones nativas soportadas, con al menos 200 módulos de integración, y el procedimiento con el cual se integra cada una de las fuentes

1.5: Marco Normativo de Seguridad Informática

DESCRIPCIÓN GENERAL
Elaborar la Política General de Seguridad y el conjunto de Normas, Guías y Estándares que se consideren necesarias para establecer un adecuado proceso de normalización, tomando como base de referencia la serie ISO/IEC 27000
CARACTERÍSTICAS GENERALES
El alcance del proyecto abarca lo siguiente: Redacción o revisión de la Política de Seguridad de la Información para toda la organización.
El alcance del proyecto abarca lo siguiente: Desarrollo del conjunto de documentos necesarios para que la organización disponga de un marco normativo acorde la Norma ISO/IEC 27002:2013. Aunque no es posible indicar de forma precisa el número exacto de documentos a desarrollar ya que, dicha cifra es una variable de la casuística específica de la organización; se prevé que el alcance del marco normativo abarque la totalidad de los temas y apartados referenciados por la Norma ISO/IEC 27001:2013, contemplando un máximo de 40 documentos.
El proyecto se estructura en las siguientes actividades:
Evaluación de la documentación existente en la actualidad con respecto Norma ISO/IEC 27001:2013.
Obtención y análisis de la información necesaria para la definición de los entregables a desarrollar.
Entrevistas con las personas involucradas con cada uno de los procesos a documentar.
Elaboración de una primera versión en formato borrador de los documentos para su revisión con los interlocutores de la organización.
Recopilación de comentarios y actualización de los documentos antes de presentarlos como definitivos.
Elaboración y propuesta final del marco normativo desarrollado de acuerdo a los lineamientos específicos Norma ISO/IEC 27001:2013.
Los entregables del proyecto acorde a las tareas anteriormente identificadas, deberán ser identificados oportunamente en conjunto con la organización.
La ejecución del mismo no dependerá de otros proyectos predecesores.
Se asegurará la participación de al menos dos recursos full time por parte de la organización para la coordinación de las actividades.

1.6.: Organización de la Seguridad

DESCRIPCIÓN GENERAL
Elaborar una propuesta de estructura organizativa y jerárquica enfocada en los distintos roles que participan en el gobierno de la seguridad (definición), contemplando la implantación, mantenimiento y control. Revisar el proceso de asignación de los propietarios de los activos. Definir los roles y responsabilidades, así como las funciones del Comité de Seguridad; el control, participación y seguimiento de incidentes y la gestión de los riesgos de forma continua.
CARACTERÍSTICAS GENERALES
Establecer una estructura organizativa para la gestión de la seguridad de la información.
Asignar eficientemente los roles y responsabilidades relativos a la seguridad de la información.
Concientizar a la organización para que la responsabilidad sobre la seguridad de la información no recaiga solamente sobre el Responsable o el Área de Seguridad.
Definir perfiles estándar para la realización de las tareas relativas a la seguridad de la información, evitando solapamientos en sus funciones.
Basándose en la Norma ISO/IEC 27001:2013 y en la experiencia con otras organizaciones, se definirán los siguientes aspectos:
Proponer una Estructura Organizativa de Seguridad de la Información eficiente, evitando solapamientos de funciones.
Revisar el proceso de asignación de los propietarios de los activos.
Definir los roles y responsabilidades relacionadas con la Seguridad de la Información.
Crear o revisar las funciones del Comité de Seguridad de la Información. Diseño del modelo de actas y estatuto de actuación.
Asignar las funciones definidas en el Modelo Organizativo de la Seguridad de la Información.
Entregables
Propuesta Estructura Organizativa de Seguridad de la Información.
Modelo de Acta del Comité de Seguridad de la Información.
Norma de Definición de Roles y Responsabilidades de Seguridad de la Información.
Informes de seguimiento del proyecto.

1.7.: Inventario de Activos

DESCRIPCIÓN GENERAL
Definición del modelo de datos y estructura del inventario de activos.
CARACTERÍSTICAS GENERALES
Designación de los responsables del mantenimiento del inventario de activos.
Implementación de las tareas de inventariado de activos de información.
Asesoramiento y acompañamiento en las tareas de gestión y mantenimiento del inventario (de acuerdo con el plan de acción programado).
El proyecto se estructura en las siguientes actividades:
Elaboración de un plan de acción conteniendo las principales actividades del proyecto.
Definición del modelo de datos y de los modelos de resultados.
El Diseño de la estructura de la base de datos del inventario de activos deberá considerar los siguientes tipos
procesos de la organización: compras, atención al ciudadano, etc.;
recursos de información: bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad, información archivada, etc.;
recursos de software: software de aplicaciones, software de sistemas, herramientas de desarrollo y utilitarios;
activos físicos: equipamiento informático (procesadores, monitores, computadoras portátiles, módems), equipos de comunicaciones, medios magnéticos, medios ópticos, otros equipos técnicos (suministro de electricidad, unidades de aire acondicionado), mobiliario, lugares de emplazamiento;
Servicios: servicios informáticos y de comunicaciones, utilitarios generales (Ej.: calefacción, iluminación, energía eléctrica, aire acondicionado, etc.).
Diseño de la solución de inventario de activos y despliegue en un entorno de pruebas.
Desarrollo y pruebas de los componentes de la solución de inventario de activos.
Validación del entorno por parte de la organización antes del despliegue en producción.
Planificación del despliegue en producción de la solución de inventario de activos.
Documentación técnica y formación que proporcione la información necesaria para que los actores desempeñen su papel de forma adecuada.
La Identificación de los activos que componen el dominio, determinando sus características, atributos y tipificación. La tipificación determinará el conjunto de salvaguardas y vulnerabilidades que podrán declararse sobre cada activo.
El establecimiento de las dependencias entre los activos del inventario (la identificación de los procesos de negocio y los elementos de TI en los que éstos se apoyan). Los niveles superiores de la jerarquía representan aspectos del negocio, y los niveles inferiores aspectos tecnológicos.
Acompañamiento (coaching) a los recursos internos la organización, abarcando tareas relacionadas con el inventariado de los activos de información y sus relaciones (de acuerdo con el plan de acción presentado).
Entregables
Diseño del inventario de activos de información.
Desarrollo de la solución de inventario de activos de información.
Obtención del Informe de inventario de activos de información.
Documentación técnica y formación para los actores involucrados.
Informes de seguimiento del proyecto.

1.8.:Clasificación y Tratamiento de Activos

DESCRIPCIÓN GENERAL
Definir una metodología de clasificación y tratamiento de la información en virtud de su importancia y de las dimensiones básicas de seguridad: confidencialidad, integridad, disponibilidad, así como los datos personales. Asimismo, el proyecto se enfoca en la realización de las tareas operativas relacionadas con la clasificación, etiquetado y tratamiento de los soportes.
CARACTERÍSTICAS GENERALES
El proyecto se circunscribe a la totalidad de los activos de información de la organización, con independencia del formato o medio en el que se encuentre. Se acompañará (coaching) al personal interno de la organización en las tareas operativas propias de la clasificación, a fin de garantizar efectividad en la transferencia metodológica. El objetivo final será que los "propietarios" adquieran la metodología de clasificación y los "custodios" implementen las medidas necesarias para proteger adecuadamente la información de la organización.
El proyecto se estructura en base a las siguientes actividades:
Recopilación de la documentación existente de los activos e información necesaria para la realización de la tarea. Esta actividad corresponde a la implantación del proyecto "Inventario de Activos" y será necesario contar con ella antes de comenzar con la Clasificación y Tratamiento de Activos.
Recopilación de los documentos relacionados con la "Organización de la Seguridad" (normas de definición de roles y responsabilidades de seguridad de la información).
Definición de la metodología y de los criterios de clasificación de la información.
Clasificar la información basándose en las escalas de sensibilidad y criticidad especificadas por el responsable de definir la seguridad en la organización.
Definición de procedimientos de etiquetado y tratamiento de la información, contemplando un tratamiento especial para la información crítica o sensible y la reclasificación de activos en función de su degradación en el tiempo o eventos específicos.
Definición de procedimientos de manipulación de copias, almacenamiento, transmisión electrónica o verbal y destrucción de información de forma segura (disposición de medios).
Acompañamiento (coaching) a los recursos internos de la organización, abarcando la totalidad de las áreas, en tareas operativas relacionadas con la clasificación, etiquetado y tratamiento de los soportes.
Los entregables del proyecto acorde a las tareas anteriormente identificadas, serán los siguientes:
Metodología de clasificación y tratamiento.
Informe conteniendo los resultados de la clasificación efectuada (listado de activos de información, niveles asignados y propietarios.
Procedimiento de etiquetado y tratamiento de la información.
Procedimiento de manipulación de copias, almacenamiento, transmisión electrónica o verbal y destrucción de información de forma segura.
"Herramienta de clasificación de la información" que servirá para agilizar las tareas operativas de clasificación.
Informes de seguimiento del proyecto.
Dependencias
El presente proyecto depende de forma directa del proyecto "Inventario de Activos" y se relaciona con el proyecto "Organización de la Seguridad". Asimismo, los tres proyectos podrían ser parte integral de un "Análisis de Riesgos". Es recomendable que su ejecución se realice en forma conjunta.

1.9.: Programa de Concientización en Seguridad Informática

DESCRIPCIÓN GENERAL
Los objetivos del proyecto se centran en la transmisión de los conceptos básicos relacionados con la seguridad de la información, a fin de que todas aquellas personas con responsabilidad en los sistemas de información de la organización, comprendan la importancia de los principios de la seguridad y su relación con la actividad laboral.
CARACTERÍSTICAS GENERALES
La política general o corporativa de seguridad de la información, las normas y procedimientos implantados.
Las responsabilidades del personal con respecto a la seguridad de la información (roles y responsabilidades de seguridad), así como los criterios de clasificación y asignación de la propiedad de la información.
La importancia de la confidencialidad, integridad, disponibilidad de la información de la organización, así como de la protección de los datos personales.
Las consideraciones a tener en cuenta con respecto a los empleados, los accesos de terceras partes y externos a la Organización.
El alcance del proyecto abarca lo siguiente:
La elaboración y puesta en marcha de un Programa de Formación y Concienciación para todos los empleados, en los aspectos relevantes de seguridad que cubra los diferentes niveles de la Organización.
El análisis y evaluación de las relaciones y dependencias que posee la organización con respecto a los empleados, proveedores, conexiones con terceros, etc.
El proyecto se estructura en las siguientes actividades
Programa de formación y concientización de los empleados: Definición del alcance, objetivos, y estructura del programa. Identificación y clasificación de posibles destinatarios y audiencias. Diseño de los mensajes que se deben comunicar y selección de las herramientas de trasmisión de acuerdo a la audiencia: Relaciones Públicas Publicidad Interacción Cara a Cara Marketing Directo Incentivos a Corto Plazo Obtención de indicadores iníciales (previo a la formación). Formación de docentes internos y formadores voluntarios (responsables de multiplicar el conocimiento dentro de la organización). Formación y concienciación de la gente (divulgación y difusión de los mensajes). Revisión y mantenimiento del programa: Obtener retroalimentación (indicadores). Medir la efectividad del Programa. Mejorar el Programa.
Estudio de los riesgos asociados a los recursos humanos y a las dependencias de la organización: Política de seguridad vigente en la organización. Empleados internos y externos, rotación de funciones, tareas asignadas a cada empleado, derechos de acceso, etc. Recursos de resguardo de información (backups). Metodologías y estándares de documentación.

1.10.: Regularización de Usuarios

DESCRIPCIÓN GENERAL
La reingeniería de procesos de gestión de usuarios se realiza bajo los lineamientos descriptos en el apartado 'características generales' del presente documento.
CARACTERÍSTICAS GENERALES
Mayor conocimiento y control de los procesos.
Mayor aceptación del usuario final debido a una mejor definición de procesos y tareas.
Conseguir mejorar los flujos de información y los niveles de seguridad.
El alcance del proyecto incluye la gestión de credenciales y autorizaciones en los principales sistemas y aplicaciones que dispongan de mecanismos y procesos de control de acceso existentes en la organización.
El proyecto se estructura en base a las siguientes actividades:
Planificación: Diseño del plan de proyecto.
Recabado de información: Se mantendrán reuniones con la dirección del proyecto con el fin de definir los objetivos de alto nivel, y el alcance del proyecto respecto a los ámbitos y entornos a analizar. Para ello se recabará toda la documentación sobre aplicaciones, políticas y normas referentes a la Gestión de Usuarios. Se definirán dos documentos: Objetivos de alto nivel.- alcance detallado del proyecto (se definirán los tipos de usuarios que existirán, gestión de las cuentas, realización de resguardos, etc.). Política de gestión de usuarios.- definición de todos los aspectos relacionados con la gestión de usuarios (creación, modificación y eliminación de los usuarios; la nomenclatura a emplear, contraseñas, etc.).
Análisis: Con el fin de poder definir los nuevos procesos de gestión de usuarios, es necesario analizar previamente a nivel técnico y organizativo cómo se está realizando dicha gestión en la actualidad. Este será el objetivo de esta actividad. Se contempla entrevistar a los responsables de cada proceso incluido en el alcance del proyecto para obtener la información necesaria. En esta fase se entregará un documento de Análisis por cada entorno definido en el alcance del proyecto. En el análisis se ha de contemplar lo siguiente: Relación con otros procesos o actividades. Inputs y Outputs principales. Normativas y/o Procedimientos asociados. Sistemas informáticos en que se basa el proceso. Recursos humanos actualmente involucrados. Estadísticas de carga de trabajo. Workflow. Indicadores y controles de calidad existentes.
Reingeniería: En función de las directrices de la dirección del proyecto y de la realidad de la organización ya analizada, se propondrán cambios en los procesos de gestión de usuarios actuales y en sus relaciones, se plantearán nuevos procesos y se eliminarán otros.
Mapeo: Tras el análisis de los procesos existentes y de los nuevos procesos propuestos, el objetivo de esta tarea es asignar los nuevos roles a los diferentes estamentos de la organización para garantizar que los nuevos procesos pueden implementarse correctamente. Para ello en esta actividad se definirán roles y responsabilidades para cada entidad involucrada en los procesos, desde los usuarios hasta los administradores, pasando por la mesa de ayuda, los propietarios, los responsables de departamento, etc. Por tanto se procederá a: Identificar actores definidos Identificar actores actuales Clasificar tareas definidas Clasificar tareas actuales Describir perfiles (skills) de actores definidos Relacionar tareas definidas con tareas actuales Mapear actores El documento general del mapeo organizativo con los resultados de las etapas de esta tarea, contendrá lo siguiente: Tareas realizadas actualmente Tareas asignadas y equivalencia con los actores definidos. Tareas asignadas y equivalencia con los actores actuales. Tareas nuevas asignadas por actor. Tareas reemplazadas por actor. Skills necesarios para realizar las tareas asignadas
Los entregables del proyecto acorde a las tareas anteriormente identificadas serán los siguientes:
Objetivos de alto nivel.

Política de gestión de usuarios.
Propuesta de reingeniería de gestión de accesos.
Documento general del mapeo organizativo.
Informes de seguimiento del proyecto.

1.11.: Servicios conexos de Implementación, puesta en Marcha, Capacitación y Soporte de la solución

Descripción General
El servicio de implementación deberá cumplir como mínimo con las siguientes actividades: • Presentación de la descripción de trabajo. • Asistencia técnica, respuesta calificada a consultas, aclaración de dudas, sobre el conjunto de hardware y software componente de la solución, para todo el personal designado. • Apoyo técnico para aprovechar las características de la solución de hardware y software contratado y transferencia de conocimientos. • Análisis, determinación, corrección y documentación de los problemas de hardware y software, si los hubiere. • Implementación, chequeo y revisión de la seguridad interna y externa. • Implementación de resguardo y regeneración de imágenes según corresponda y aplique. • Definición y documentación de los procesos. • Pruebas de Aceptación. ***1.11.1 Cronograma del Proyecto*** La primera tarea será la de Planificación de la Implementación de todos los productos a instalar y poner en servicio, para ello se deberá identificar el entorno de instalación del hardware y software de base, tanto desde el punto de vista técnico, como desde el punto de vista de seguridad. Como resultado de la planificación surgirá un cronograma del proyecto, que será la guía para la ejecución de todas las tareas que la implementación involucre, que estará debidamente aprobado por el cliente y que deberá respetar los plazos fijados para instalación e implementación. Se dará seguimiento periódico al cronograma, junto a personal del cliente pudiendo realizarse ajustes que sea debidamente justificados y mediante aprobación por parte del cliente (proceso de control de cambios). Entregables: Documento de Cronograma del proyecto ***1.11.2 Instalación*** En primer término, el Proveedor deberá entregar al cliente la documentación necesaria para la Instalación. Esta documentación debe incluir el detalle del plan de trabajo completo para efectuar la instalación, en todos y cada uno de los dispositivos que compondrán la solución final; además en ella se deben especificar: • Los recursos necesarios para la instalación • Cada uno de los pasos que se deben efectuar • Los tiempos de ejecución de cada uno de los pasos El Proveedor será el responsable de la instalación, y de las tareas que se describen a continuación, las que finalmente deberán ser aprobadas por el cliente: • Implementación básica del hardware y software en todos sus componentes • Documentar las pruebas de funcionamiento del hardware y software • Pruebas de Aceptación Entregables: Documento de Instalación incluyendo plan de trabajo y recursos involucrados ***1.11.3 Reunión de inicio del Proyecto*** El Gerente de Proyecto del cliente se reunirá con el equipo de proyecto del Proveedor, para determinar todos los requisitos exigidos para la finalización satisfactoria de este proyecto. El grupo tendrá como tareas: 1. Confirmar los requisitos y expectativas del cliente. 2. Priorizar requisitos (obligatorio y deseable). 3. Identificar claramente al representante técnico del cliente para este proyecto, otros miembros

del equipo del cliente y el proceso de estalación interno del cliente.

4. Identificar a los responsables del Proveedor, incluyendo al Gerente de Proyecto, otros miembros del equipo del Proveedor, y el proceso de estalación interno del Proveedor.
5. Identificar al personal que recibirá la transferencia de conocimientos.
6. Definir metodologías, procedimientos, especificaciones, estándares, criterios para medición y sistemas de gestión que se utilizarán en todo el proyecto.
7. Discutir sobre los objetivos, estalación de eventos y ciclo de revisión.
8. Revisar los siguientes procedimientos, con el objetivo de esclarecer eventuales dudas:
    i. Sucesión de Documentos
    ii. Control de Cambios
    iii. Pruebas
    iv. Transmisión de Conocimientos
    v. Formación General y Específica.
    vi. Evaluación de la Calidad.
9. Revisión de la Organización y Recursos del cliente
10. Producir una agenda de proyecto equilibrada con el Documento delineado en este acuerdo de compromiso.
11. Los documentos generados deberán ser firmados por el Representante Técnico del cliente, el Responsable Técnico del Proveedor y ambos Gerentes de Proyecto, comprobando su aceptación, dedicación en el proyecto y el acuerdo mutuo acerca de los objetivos.

Entregables:

- Minuta detallada de la reunión
- Lista de ajustes que se harán a la documentación y/o procesos.

1.11.4 Documento del Proyecto

A partir de las funciones descriptas anteriormente, se confeccionará el Documento del Proyecto (Bitácora de proyecto). Este documento reflejará los eventos de la reunión y describirá el ámbito total del proyecto incluyendo todos los cambios y retoques efectuados para cada etapa. El proyecto no entrará en la fase siguiente hasta que se haya acordado una versión final de este documento y la hayan firmado ambas partes.

Entregables: Documentación actualizada del proyecto, incluyendo:

- Cronograma actualizado
- Control de Cambios
- Documento de Arquitectura y diseño
- Plan de implementación
- Plan de pruebas de aceptación

1.11.5 Implementación de la Solución Integral

El Proveedor del Equipamiento deberá trabajar junto al cliente en la implementación de todo el equipamiento de la solución, muchos de estos requerimientos podrían ser ejecutados paralelamente. La instalación deberá incluir la puesta en marcha de la instalación física de todos los componentes, actualización de software a últimas versiones estables según el fabricante, configuraciones iníciales.

Entregables:

- Infraestructura instalada y configurada
- Aceptación del cliente

1.11.6 Pruebas de Aceptación

El Proveedor del Equipamiento deberá trabajar junto al cliente en completar el protocolo de pruebas de aceptación oportunamente documentado. Durante las pruebas deberá verificarse el funcionamiento de las características técnicas de la solución requeridas en el presente pliego, incluyendo pruebas de operatividad y de simulación de fallas y tolerancia a las mismas. Las pruebas de aceptación deberán ser documentadas y aprobadas por el cliente.

Entregables:

- Completar el documento de pruebas de aceptación, indicando el resultado de las pruebas realizadas, y la conformidad del cliente.

1.11.7 Transferencia de Conocimiento

El Proveedor del Equipamiento deberá otorgar una transferencia de conocimiento de las tareas efectuadas durante la implementación, puesta en marcha y pruebas de aceptación. Dicha tarea no deberá llevar menos de 3 días y participará un grupo de responsables designados por el cliente. El temario y formato de esta actividad deberá ser presentado con anterioridad para previa aceptación por parte del cliente.

Entregables:

- Dictado de la transferencia de conocimiento
- Documentación técnica para los participantes
- Control de asistencia y cumplimiento de horarios
- Aceptación del cliente y encuesta de satisfacción

1.11.8 Soporte Operativo

El Soporte del Proveedor es adicional al que ofrece el fabricante. Es el servicio de postventa que se hace cargo de resolver las fallas de los servicios y dispositivos del cliente y realizar el mantenimiento preventivo durante el plazo de TREINTA Y SEIS (36) meses.

El Soporte deberá contemplar los siguientes servicios:

- **Gestión de Fallas**: El Proveedor es responsable de atender al cliente cuando falla un servicio o un dispositivo de seguridad soportado, de acuerdo a los SLAs definidos.
- **Mantenimiento Preventivo**: Actividades preventivas enfocadas a mantener el rendimiento y funcionamiento de las herramientas y reducir las amenazas y vulnerabilidades de los sistemas, se realiza el update y upgrade de software.
- **Update de SW**: Instalación de parches y hotfix.
- **Upgrade de SW**: Cambio en las versiones de SW liberadas por los fabricantes, las que son previamente testeadas por El Proveedor para certificar las mejoras incluidas.
- **Reemplazo de Partes**: Recambio de partes de Hardware, de acuerdo a los SLAs definidos
- **Escalamiento a proveedores ante fallas**: El Proveedor realiza escalamiento al fabricante en caso de necesitar apoyo ante falla.

Gestión de Fallas

La Gestión de Fallas se hace cargo de las acciones de diagnóstico y solución de fallas en el ámbito de la plataforma soportada. Opera a partir de una condición detectada por el equipo del Proveedor (variable de salud crítica) o informada por el cliente (recepción de SPAM, por ejemplo). La Gestión de Fallas considera diversas actividades como reconfiguración de dispositivos, restauración de configuración entre otras. La gestión de fallas puede ser ejecutada remotamente o en dependencias del cliente conforme a la situación específica.
La forma de operación del Proveedor en caso de una falla deberá ser presentada en un documento membretado del Proveedor.

Mantenimiento Preventivo

Consiste en visitas de mantenimiento preventivo para actualización de versiones de software, revisión de errores en la plataforma y verificación del correcto funcionamiento de la plataforma. Esta visita será programada en horas y/o días de común acuerdo.

Escalamiento a fabricantes

En caso que se produzca una falla en el equipo del cliente y sea necesaria la intervención del fabricante,

el Proveedor es responsable de realizar el escalamiento y seguimiento, para lo cual se debe abrir un caso con la fábrica y asegurar la resolución de la falla y conformidad del cliente.

Servicios Gestionados / Administración

Los alcances del servicio gestionado son los siguientes:

- Operación de la plataforma: Implica las actividades para mantener la plataforma de seguridad en óptimo funcionamiento.
- Atención de requerimientos de clientes: Atención de los requerimientos de configuración y de información del cliente.
- Monitoreo de disponibilidad y salud: Monitoreo 7x24 de las variables críticas de la plataforma para controlar proactivamente la disponibilidad de los dispositivos y el performance, con el fin de que los dispositivos cumplan correctamente sus funcionalidades.
- Sintonización y mejora continua: Ajuste y modificación proactiva y permanente de las reglas de correlación para ajustar el sistema de detección a las nuevas amenazas.
- Gestión de logs: Implica las actividades de respaldo y rotación de logs con el fin de mantenerlos almacenados y disponibles durante el período comprometido con el cliente.
- Asesoría Especialista: Implica las actividades que realiza un ingeniero experto en las plataformas que adquiere el cliente con el fin de optimar el funcionamiento y uso de ellas.

Renglón 2: RENOVACIÓN DE PRODUCTOS QUE COMPONEN LA SOLUCION Y SERVICIOS DE SEGURIDAD PERIMETRAL

CARACTERÍSTICAS GENERALES
La solución a proveer deberá incluir la protección de datos frente a amenazas y software malintencionado siendo una recopilación de tecnología vital e integrada en un único agente para puestos de trabajo, que se pueda implementar y gestionar conjuntamente desde una sola consola, las mismas deberán interactuar entre si y deberán cumplir las siguientes condiciones y características de cada una y todos los casos: 1.1. <u>Solución de puestos de Trabajo</u> Deberá permitir la consolidación de los puestos de trabajo en una infraestructura unificada (en arquitecturas físicas, virtuales y en la nube) y que permita implementar nuevas aplicaciones de la solución principal en forma sencilla y unificada, no interfiriendo con la instalación principal. Deberá poder virtualizar los equipos de escritorio y minimizar el trafico y por ende el tamaño de los archivos de patrones de virus. Esto deberá permitir el incremento de la virtualización sin comprometer la seguridad. Deberá permitir el bloqueo instantáneo del acceso a archivos y sitios Web maliciosos. Deberá poder detectar y bloquear amenazas, con el respaldo de pruebas realizadas en condiciones reales y en tiempo real. Deberá tener la capacidad de acceder al centro de reputación de archivos y sitios web y deberá tener capacidad de integración con las soluciones actuales de Windows de Legislatura. Deberá evitar y bloquear las posibilidades de acceso de las actuales técnicas de infección impidiendo el robo de identidades, la pérdida de datos, los tiempos de inactividad y las infracciones de cumplimiento de normativas. Deberá ser escalable de acuerdo a las necesidades y crecimiento de esta Legislatura y a la evolución de la tecnología aplicable. Deberá proteger el end point tanto virtuales como físicos, tanto dentro como fuera de la red de este organismo, permitiendo la incorporación de plug in fácilmente para incorporar nuevas capacidades de seguridad, sin necesidad de tener que volver a implementar toda la solución. Deberá poseer algún módulo de Reputación de Archivos que consulte información actualizada on line sobre la reputación de un archivo antes de que se le permita el acceso. Deberá contar con módulo de Reputación Web, el cual deberá proteger del malware de Internet y del robo de datos. Deberá impedir a clientes y aplicaciones acceder a sitios Web maliciosos o infectados, utilizando tecnología Smart Protection Network para determinar la seguridad de sitios Web y que estos sean valorados de forma dinámica. Deberá proporcionar protección en tiempo real dentro de cualquier entorno de red. Deberá ofrecer protección en tiempo real contra: Virus, Amenazas Web, Spyware, Rootkits, Gusanos de Red, Hackers, y Amenazas combinadas, protegiendo distintos puntos de protección ya sea usuarios y Servidores de archivos. <u>Solución de Gate Way</u>

Deberá ser una solución de seguridad SaaS híbrida funcional para correo electrónico que se integra un appliance virtual in situ con la seguridad SaaS para correo electrónico basada en Internet. Deberá permitir control flexible de la información saliente de carácter confidencial. Deberá bloquear las amenazas de spam y virus desde la red, generando cuarentena local de ser necesario. Deberá utilizar tecnología de seguridad SaaS híbrida para correo electrónico, y así poder consolidar la información del data center.
Deberá poder tener una protección proactiva deteniendo el spam en Internet, fuera de la red
Deberá proteger a la red de enlaces maliciosos y malware
Deberá poder personalizar controles desde una consola de gestión unificada
Deberá proteger de las siguientes amenazas: Spam, Virus, Spyware, Phishing, Amenazas mixtas, Pérdida de datos, Amenazas combinadas, Contenido inapropiado y Enlaces Web Maliciosos, en los puntos a proteger de Gateway de mensajería e Internet.

1.2. Solución de seguridad web y filtrado

Deberá implementarse una solución tipo appliance de software virtual que combine el control de aplicaciones con la exploración antimalware avanzada, la reputación Web en tiempo real y el filtrado de URL flexible para proporcionar una protección frente a las amenazas de Internet, que permita la visibilidad de las aplicaciones ya sea in situ y/o en la nube de los empleados de la legislatura sin limitaciones.
Deberá poder integrarse en entornos VMware para una protección sin agente y también permitir el uso del agente para servidores físicos y equipos de escritorio virtuales en el modo local.
Deberá combinar exploración antimalware, reputación Web en tiempo real y filtrado de URL flexible, visualizando aplicaciones basadas en la nube y/o en la red.
Deberá tener una gestión centralizada y poder supervisar el uso de Internet mientras se realiza. Deberá poder supervisar más de 420 protocolos de Internet incluidos los de mensajería instantánea, aplicaciones P2P, aplicaciones de redes sociales y multimedia de transmisión por secuencias, y poder generar informes sobre los mismos.
Deberá permitir a los usuarios acceder a aplicaciones basadas en la nube pero aplicando políticas restrictivas de ser necesario.
Deberá poder ofrecer funciones de supervisión y reporte en tiempo real, aplicando solución al problema en tiempo real y centralizando la gestión de los gateways de Internet distribuidos por la WAN.
Deberá permitir la implementación inmediata de nuevas capacidades a medida que se necesitan y permitiendo la recuperación tras cortes de suministro imprevistos con funciones nativas de conmutación por error y redundancia.
Deberá implementar con rapidez sistemas operativos reforzados y personalizados y aplicaciones de seguridad de Internet integradas a la plataforma de hardware elegida y/o a elegirse por este organismo, independientemente de las actualizaciones de sistemas operativos y seguridad, permitiendo mayor escalabilidad.
Deberá tener un modulo y/o función de reputación web con datos sobre amenazas correlacionados que permita el bloqueo a sitios con actividad maliciosa para proteger frente a las amenazas nuevas y no conocidas en tiempo real. Deberá poder tener tecnología Trend Micro Smart Protection Network o similar para poder ofrecer una visión panorámica de las amenazas de Internet.
Deberá poseer una interfaz filtrado de URL y de código activo, utilizando la categorización y reputación de URL en tiempo real para identificar sitios inapropiados o maliciosos, ofreciendo por lo menos seis acciones distintas de políticas para el control del acceso Web (supervisar, permitir, advertir, bloquear, bloquear con invalidación de contraseña y forzar cuotas de tiempo). Deberá poder bloquear a nivel de objetos dentro de páginas Web dinámicas como aplicaciones híbridas Web 2.0., y asimismo detener las descargas automáticas y bloquear el acceso a sitios Web relacionados con spyware y phishing.
Deberá poder implementarse e integrarse con la plataforma actual en forma confiable y flexible, proporcionando distintas y variadas opciones de implementación en la red, incluido el puente transparente, ICAP, WCCP, proxy de reenvío o proxy inverso.
Deberá garantizar la escalabilidad, el rendimiento y la fiabilidad sin equilibradores de carga externos, admitiendo LDAP, Active Directory™, Syslog y SNMP para una integración más estrecha y un menor TCO.
Deberá poder integrarse con TM™ Damage Cleanup Services para eliminar automáticamente las amenazas de los puestos de trabajo infectados, generando limpieza automática.

Deberá poder funcionar como un appliance de software dedicado en servidores estándar del sector o como un appliance virtual.
Deberá gestionar funciones de antivirus y antispyware en el Gateway, explorando el tráfico HTTP, HTTPS y FTP entrante y saliente en busca de malware, y poder detener las descargas de virus y

spyware, los programas robot, los intentos de llamada a casa y la infiltración de malware.
Deberá tener función de reputación Web con datos sobre amenazas correlacionados para así poder bloquear el acceso a sitios con actividad maliciosa para proteger frente a las amenazas nuevas y no conocidas en tiempo real, integrándose a tecnologías tipo o similar a Trend Micro Smart Protection Network.
Deberá poder generar informes y realizar gestión centralizada en tiempo real (con el módulo opcional Advanced Reporting and Management o similar).
Deberá proteger de las siguientes amenazas: Spam, Virus, Spyware, Phishing, Amenazas mixtas, Pérdida de datos, Amenazas combinadas, Contenido inapropiado Enlaces Web Maliciosos, y Contenido no relacionado ni autorizado por el organismo.
Deberá permitir distintas opciones de implementación, como ser, Transparent Bridge, Forward Proxy, ICAP, WCCP, Reverse Proxy, etc.
Deberá poder integrarse con LDAP, Active Directory, SNMP, etc.

1.3. Consola de control centralizada

La solución propuesta deberá contar con una consola de gestión y control centralizada Web, que permita realizar un seguimiento del rendimiento de la seguridad, informes sobre sucesos de malware e infracciones de políticas y automatizar las tareas de rutina. Deberá ser personalizable y con acceso directo a las estadísticas de las amenazas publicadas por TM Smart Protection Network o similar, deberá poder gestionar las actualizaciones y configurar alertas, permitiendo el acceso en cualquier momento y lugar con la interfaz basada en Web
Deberá proteger de las siguientes amenazas: Spam, Virus, Spyware, Phishing, Amenazas mixtas, Pérdida de datos, Amenazas combinadas, Contenido inapropiado Enlaces Web Maliciosos, y Ataques de denegación de servicios

1.4. Protección para servidores físicos, virtuales y en Internet

Deberá tener una solución de seguridad completa para servidores físicos, virtuales y basados en la nube, protegiendo las aplicaciones y los datos frente a filtraciones e interrupciones, garantizando así la seguridad del servidor, las aplicaciones y los datos en servidores físicos, virtuales y basados en la nube así como en equipos de escritorio virtuales. Deberá poder permitir elegir una protección sin agente o basada en agente que incluya características de antimalware, detección y prevención de intrusiones, protección de aplicaciones Web, supervisión de la integridad e inspección de registros. Deberá garantizar la seguridad de servidores virtuales sin carga adicional para el sistema. Deberá poder proteger los servidores y equipos de escritorio virtuales mientras se desplazan entre el centro de datos y la nube pública. Deberá ofrecer protección frente a vulnerabilidades para priorizar la codificación segura y la implementación de los parches no programados. Deberá detectar y eliminar el malware de los servidores virtuales en tiempo real, proteger de las vulnerabilidades conocidas y no conocidas de las aplicaciones empresariales y los sistemas operativos, poder usar alguna de las bases de datos de reputación de dominios más extensas y reconocidas para evitar que los sistemas accedan a sitios Web comprometidos. Deberá proteger el hipervisor del ataque a las vulnerabilidades, utilizando tecnología Intel TMP/TXT, entre otras.
Deberá cumplimentar los requisitos principales de las normativas PCI DSS 2.0, HIPAA, NIST y SAS 70.
Deberá poder generara informes detallados y auditables que describen los ataques que se han evitado y el estado de cumplimiento de políticas.

Deberá poder implementar en forma sencilla y sin agentes módulos con características de antimalware, cortafuegos, IDS/IPS, protección de las aplicaciones Web, control de las aplicaciones y supervisión de la integridad de la red.

1.5. Solución de Monitoreo de red

Deberá proporcionarse una solución de monitoreo de red para descubrir la presencia de amenazas internas ocultas o amenazas de día cero. Deberá poder identificar una amplia gama de aplicaciones no autorizadas, que afectan los servicios de la red y plantean problemas de seguridad. Deberá poder colaborar con tecnología Smart Protection Network o similar, realizando un análisis de la presencia y comportamiento de malware en la red y una correlación de los eventos y proveer información exacta a través de informes técnicos que permitan conocer detalladamente el estado de situación de la red y tomar acciones precisas. En todo momento se podrá visualizar el conjunto de eventos producidos en la red en tiempo real.

Deberá poder detectar actividades maliciosas a nivel de red Malware que intenta propagarse o infectar otros usuarios, Malware oculto que se comunica con terceras partes para fugar información o

recibir comandos, ataques basados en contenido web o email, tales como exploits Web, cross-site scripting y phishing.
Deberá poder descubrir aplicaciones y servicios disruptivos, como detectar la utilización de la red de servicios como mensajería instantánea, P2P o contenido multimedia streaming. Identificar servicios no autorizados que provocan riesgos de seguridad como relays SMTP abiertos o servicios DNS no declarados.
Deberá poder inspeccionar los protocolos existentes de capa 2 a la 7, correlacionando eventos sospechosos con posibles amenazas y analizar el contenido de archivos.
Deberá poder implementarse fuera de línea y así realizar sniffing pasivo de la red sin afectar otros servicios.