Anexo Técnico

Plataforma de seguridad para detección y respuesta a amenazas.

Para: SOCIEDAD DE ACTIVOS ESPECIALES

SOCIEDAD DE ACTIVOS ESPECIALES

Tabla de contenidos

SOCIEDAD DE ACTIVOS ESPECIALES

1. Requisitos Mínimos Técnicos para protección de terminales

- La solución debe tener la capacidad de brindar protección contra malware, virus de red, conexiones sospechosas, amenazas web, spyware, análisis de archivos adjunto de correo POP3, monitoreo de comportamiento, ataques combinados y ataques de día cero para equipos de punto final (Endpoint).
- La solución de protección de Antimalware se debe poder desplegar 100% Onpremise o 100% en Nube y debe permitir como mínimo las características de Antimalware, Control de Aplicaciones y de dispositivos, protección avanzada contra Ransomware, mitigación de vulnerabilidades a través de parches virtuales y protección de fuga de información a través de expresiones regulares, diccionarios y características de los archivos.
- La solución de protección Antimalware debe permitir la implementación de protección antimalware, control de aplicaciones, control de dispositivos, prevención de fuga de información, protección web, mitigación de vulnerabilidades a través de parches virtuales en un solo agente.
- La solución debe permitir hacer backup y restauración automática de archivos ante intentos de cifrado no autorizados, con el fin de generar una protección proactiva contra Ransomware.
- La solución debe contar con firewall (reglas de conexiones de aplicación, IP, puerto y protocolo), reputación de archivos y/o reputación web.
- La solución debe permitir realizar escaneos de los endpoint de forma manual, programada y en tiempo real.
- La solución debe tener la capacidad de aislar los equipos o ponerlos en cuarentena cuando se detecta algún ataque para evitar la propagación de este dentro de la red.
- La solución debe tener la capacidad de brindar protección contra filtrado de datos sensibles y proporcionar un control de dispositivos.
- La solución debe permitir la integración con 1 o más dominios.
- La solución debe permitir la integración con Active Directory.
- La solución debe permitir realizar una migración a versiones superiores de la misma conservando las configuraciones, incluida la base de datos.
- La solución debe permitir el uso de una base de datos externa Microsoft SQL Server
- La solución debe permitir recuperar los archivos que sean enviados a cuarentena.
- La solución debe proporcionar protección a los agentes contra Ramsomware.
- La solución debe proporcionar una consola de administración que pueda ser utilizada desde un entorno web.
- La solución debe proporcionar una herramienta para la migración de la base de datos nativa de la solución a una base de datos SQL.
- La solución debe tener la capacidad de analizar la reputación de archivos.
- La solución debe permitir la creación, modificación y eliminación de roles y usuarios para la administración de esta.
- La solución debe tener la capacidad de proteger los equipos que se encuentren dentro de la red y fuera de ella.
- La solución debe tener un módulo de firewall que permita la creación de políticas a través de aplicaciones, aplicaciones específicas, llaves de registro de aplicaciones y estas se podrán aplicar a través de UDP, TCP y ICMP con puertos y direcciones IP

definidas según las necesidades.

- La solución debe tener la capacidad de programar la sincronización de los equipos para horas y fechas específicas.
- La solución debe permitir la configuración de un servidor SMTP para el envío de notificaciones vía Email
- La solución debe permitir seleccionar el criterio de las notificaciones para ser enviadas a la administración, cuando una amenaza sea detectada.
- La solución debe permitir la configuración de la plantilla del correo para el envío de notificaciones.
- La solución debe permitir seleccionar el criterio de las notificaciones para ser enviadas al administrador, cuando uno de los equipos sea enviado a cuarentena.
- La solución debe permitir la configuración de la plantilla del correo para el envío de notificaciones cuando los equipos sean enviados a cuarentena.
- La solución debe permitir la configuración de los tipos de eventos que serán notificados y visualizados en el agente, y adicionalmente configurar el mensaje de las alertas dependiendo de la criticidad del evento (High, Medium, Low)
- La solución debe tener la capacidad de finalizar sesiones en la consola de administración por tiempo de inactividad.
- La solución debe tener la capacidad de hacer Rollback de las actualizaciones de los componentes.
- La solución debe tener la capacidad de eliminar de los logs de los eventos del sistema, servidor y agentes, para que estos sean eliminados con una frecuencia especifica.

1.1 Consola de administración

- La consola de administración debe permitir administrar los agentes instalados en la red de equipos. Permitiendo conocer el estado de los agentes.
- La consola de administración debe estar en la Nube para garantizar la administración en todo el tiempo sin importar el lugar donde estén las maquinas administradas.
- La consola de administración debe permitir agrupar los agentes en grupos para facilitar la configuración y administración de estos.
- La consola de administración debe permitir configurar notificaciones sobre riesgos de seguridad y ver los Logs enviados por los agentes sobre los eventos de estos.
- La consola de administración debe proporcionar un Dashboard que brinde información global sobre los agentes, eventos de reputación web, usuarios afectados, eventos de comando y control, incidentes de filtración de datos, entre otros e igualmente debe permitir que secciones o widgets sean agregados o eliminados según se requiera.
- La consola de administración debe permitir consultar los Logs de instalación tanto del agente como el del servidor de administración.
- La consola de administración debe permitir visualizar estadísticas de históricos de actualizaciones de patrones de análisis de antivirus, antispyware, análisis de comportamiento, conexiones sospechosas, y exploits de los navegadores de internet.
- La consola de administración debe permitir visualizar los logs de los eventos sobre los equipos donde se encuentra instalado el agente, dichos eventos deben estar relacionados a temas de malware, spyware, reputación web, conexiones sospechosas,

archivos sospechosos, Command & Control Callbacks, Behavior Monitoring, Machine Learning, control de dispositivos, DLP, y escaneos. Adicionalmente la solución debe permitir filtrar dichos logs por periodos de tiempo preestablecidos, por rangos de fechas y por tipo de escaneo.
- La consola de administración debe permitir la visualización de los logs de registro de los eventos de la actualización del servidor de actualizaciones.
- La consola de administración debe permitir la visualización de los logs de registro de los eventos del servidor de administraciones.
- La consola de administración debe tener la capacidad de generar reporte en formato PDF, DOCX y XLSX
- La consola debe poder operarse en la nube sin requerir recursos de infraestructura y entregarse como software como servicio

1.2 Agentes

- Los agentes deben ser instalados mediante instalación web, link de instalación por correo, instalación por script, instalación remota, y/o paquete de instalación.
- Los agentes deben requerir contraseña de administración para ser desinstalados de los equipos.
- Las políticas de seguridad deben aplicarse en los agentes de forma individual y/o por grupos.
- El agente debe tener la capacidad de eliminar los archivos sospechosos de forma automática.
- El agente debe estar integrada en un solo agente para dar protección de amenazas, protección de vulnerabilidades, control de aplicaciones y DLP
- Los agentes deben tener la capacidad de conectarse a múltiples fuentes de actualización (patrones, firmas, url sospechosas, etc), si alguna de estas es inaccesible para el agente.

1.3 Regulatorio y cumplimiento

- La solución debe estar ubicada en el cuadrante de lideres de Gartner mínimo 3 años anteriores.
- La solución debe estar listada como líder en el último cuadrante de Forrester de Endpoint Security Suites
- El fabricante de la solución de Endpoint debe ser líder en el último cuadrante de Enterprise detection and Response de Forrester.
- El oferente deberá allegar certificado de distribuidor autorizado emitido por el fabricante de la solución a ofertar

1.4 Sistemas operativos soportados

- Windows 8/8.1 (32-bit/64-bit)
- Windows 10 (32-bit/64-bit)
- Windows 11 (32-bit/64-bit)
- Windows Embedded Standard 2009 (32-bit)
- Windows Embedded POSReady 2009 (32-bit)
- Windows Embedded POSReady 7 (32-bit/64-bit)
- Windows 8/8.1 Embedded (32-bit/64-bit)

- Windows 10 IoT Embedded (32-bit/64-bit)
- Windows Server 2008 (32-bit)
- Windows Server 2008 Failover Cluster (Active/Passive) (32-bit)
- Windows Server 2008 (64-bit)
- Windows Server 2008 R2 (64-bit)
- Windows HPC Server 2008 R2 (64-bit)
- Windows MultiPoint Server 2012 Standard, DataCenter y Server Core
- Windows MultiPoint Server 2012 R2 Standard, DataCenter y Server Core
- Windows Server 2016 Standard, DataCenter y Server Core
- Windows Storage Server 2016
- Windows Server 2019 Standard, DataCenter y Server Core

1.5 Servidor de retransmisión

- El servidor de retransmisión debe tener la capacidad de ser implementado en una red DMZ, cloud, etc; para permitir la conexión de los agentes que no se encuentran dentro de la Red de la organización.
- El servidor de retransmisión debe tener visualización y control de los agentes que se encuentran fuera de la red de la organización.

1.5.1 Sistemas operativos soportados

- Windows Server 2008 (32-bit/64-bit)
- Windows Server 2008 R2 (32-bit/64-bit)
- Windows HPC Server 2008 (32-bit/64-bit)
- Windows HPC Server 2008 R2 (64-bit)
- Windows Server 2012 (64-bit)
- Windows Server 2012 R2 (64-bit)
- Windows Server 2016 (64-bit)
- Windows Server 2019 (64-bit)
- Windows MultiPoint Server 2010 (64-bit)
- Windows MultiPoint Server 2012 (64-bit)
- Windows MultiPoint Server 2011 (64-bit)
- **Base de Datos**
    - SQL Server 2008 R2 Express o superior
    - SQL Server 2008 R2 o superior

1.5.2 Plataformas de visualización soportadas

- ESX/ESXi Server (Server Edition) 5.x, 6.x
- Server (Server Edition) 1.0.3, 2
- Workstation and Workstation ACE Edition 7.0, 7.1,8.0, 9.0, 10.0, 11.0, 12.0
- vCenter™ 5.0, 5.1, 5.5, 6.x
- View™ 5.0, 5.1, 5.3, 6.x
- Horizon® Air™ Desktops
- Horizon® Mirage™ 5.x
- Horizon® View™ 7
- XenDesktop 5.0, 5.5, 5.6, 7.x

- XenServer 6.5, 7.0
- XenApp 4.5, 5.0, 6.0, 6.5, 7.x
- VDI-in-a-Box 5.1
- Microsoft Hyper-V Server 2008/2008 R2 (64-bit)
- Microsoft Hyper-V Server 2012/2012 R2 (64-bit)
- Microsoft Hyper-V Server 2016 (64-bit)
- Windows Server 2008/2008 R2 (64-bit) Hyper-V
- Windows Server Hyper-V:
- Windows Server 2008/2008 R2 (64-bit) Hyper-V
- Windows Server 2012/2012 R2 (64-bit) Hyper-V
- Windows Server 2016 (64-bit) Hyper-V
- Windows 8/8.1 Pro/Enterprise (64-bit) Hyper-V
- Windows 10 Pro/Enterprise (64-bit) Hyper-V

2. Requerimientos de Data Loss Prevention DLP

- La solución debe tener la capacidad de prevenir y/o informar sobre la fuga o perdida de información sensible de la organización ya sea de forma accidental o deliberada.
- La solución debe permitir identificar o configurar los activos digitales que se desean proteger.
- La solución debe permitir la creación de políticas que limiten la transmisión o transferencias de activos digitales por los canales de comunicación convencionales (email y/o dispositivos externos).
- La solución debe tener la capacidad de igualmente brindar protección y aplicar políticas para transferencia de activos digitales mediante cliente de correo ya será software o web.
- La solución debe permitir que la organización haga cumplir con las normas de privacidad establecidas.
- La solución debe tener la capacidad de brindar protección contra filtrado de datos sensibles y proporcionar un control de dispositivos, permitiendo configurar reglas o políticas para ser aplicadas a grupos o agentes individuales.
- La solución debe proporcionar identificadores de datos y/o plantillas para la creación de políticas.
- La solución debe tener la capacidad de identificar o reconocer archivos ejecutables, documentos, gráficos vectoriales, archivos multimedia, archivos comprimidos, bases de datos, hojas de cálculo, presentación, archivos vinculados e incrustados, y/o archivos encriptados.
- La solución debe tener la capacidad de localizar activos digitales almacenados en portátiles, equipos de escritorio, y servidores.
- La solución debe tener la capacidad de proporcionar filtros de protección para canales de red como FTP o HTTP, canales de aplicaciones o periféricos.
- La solución debe tener la capacidad de detectar datos estructurados y no estructurados.
- La solución debe mantener un monitoreo constante.
- La solución debe proveer plantillas que permitan el cumplimiento de estándares como GLBA, HIPAA, PCI-DSS o SB-1386.
- La solución debe permitir la integración con Directorio Activo y permitir la delegación de administración.

- La solución debe contar con una consola de administración WEB que permita la configuración de políticas e implementaciones, reportes de los equipos, extracción de huellas digitales, y actualizaciones.
- La solución debe contar con una herramienta que analice los activos digitales que se encuentran almacenados en los portátiles o computadores de escritorio aun así no estén conectados en la red de la organización.
- La solución debe tener la capacidad de identificar los activos digitales almacenados en los dispositivos o el tráfico en la red utilizando expresiones regulares (predefinidas y/o personalizadas), atributos de archivos (tipo y/o tamaño), huellas digitales, palabras clave, y/o plantillas (predefinidas y/ personalizadas)
- Las plantillas de identificación de activos digitales deben permitir combinar identificadores de datos (expresiones, atributos de archivos, huellas digitales, lista de palabras).
- La solución debe permitir usar plantillas predefinidas por el fabricante, personalizarlas, crear plantillas, importar plantillas, exportar plantillas, y eliminar las plantillas.
- La solución debe permitir implementar políticas independientes tanto para agentes en los dispositivos como para agentes en la red.
- La solución debe permitir generar reportes ya sea por demanda o de forma programada (Diario, semanal o mensual), estos reportes deben contener información de los logs de los agentes. Dichos reportes deben mostrar información relevante como top de incidentes, información resumida, reporte de auditoría, entre otros.
- La solución debe permitir almacenar reportes y estos deben estar disponibles en formatos PDF, HTML, o Microsoft Excel.
- La solución debe tener la capacidad de administrar los logs de manera que pueda eliminar los Logs que tengan un tiempo de más de 90 días, igualmente debe permitir la realización de una copia de seguridad y limpieza de los mismos de forma manual.
- La solución debe permitir que las actualizaciones puedan ser implementadas en ambientes de pruebas y producción para validar el funcionamiento de los mismos.
- "
- La solución debe soportar la detección de fuga de información en los siguientes tipos de archivo:
    - .pdf .odt, .ott, .stw, .sxw .wpd, .wps .xml .xbd, .xdw .htm .jtd .sam .doc, .docm, .docx, .dot, .dotm, .dotx .wri .rtf .sgml .wsd, .bmp .dib .dcm .eps .img .gif .jpg .mac .png .tif, .tiff .ico .pcx, .dxf .dwg, .dws .cel, .dgn .cdb .CATDrawing, .CATPart, .CATProduct .cdr .dvi .gds .attr, .sgfx, .ssht .drw .ps .prt .svf .prtdot, .sldasm, .slddrw, .sldprt, .swf .aiff .mod .mov .avi .mid .mpeg .mpg .au .wav .wma .wmv, .7z .arc .arj .bz2 .Z .cpio .gz .lzh .chm .msg .pst .dbx .eml .pgp .rar .shar .tar .rpm .uue .zip, .sas .db .dif .dbf .fp7 .tbl .accdb, .mdb, ods, .ots, .stc, .sxc .csv .123 .wk1 .wk3 .wk4 .wke .wks .xlam .xlc .xls .xlsb .xlsm .xlsx .xltm .xltx .xlw .qpw .wb3 .wb2 .wb1 .wq1, .odp, .otp, .sti, .sxi .shw .pre .pot, .potm, .potx, .pps, .ppsm, .ppsx .ppt .pptm .pptx .vdw, .vdx, .vsd, .vss, .vst, .vsx, .vtx, .7z, .rar, .zip .accdb, .doc, .docx, .pdf, .ppt, .pptx, .w b1, .wb2, .wq1, .wpd, .xls, .xlsx, .mml .pub .qxp .one .mpp .hlp .iam, .idw, .ipt, .msoffice, .pqw y .pif"
- La solución debe permitir configurar las fuentes de actualización para los parches o hot fixes y adicionalmente permitir configurar la periodicidad de las mismas.
- La herramienta de análisis local debe tener la capacidad de adquirir huellas digitales

para los archivos almacenados en el equipo.

- La solución provee expresiones predefinidas para los números de tarjetas de crédito. A estos números se les realiza una verificación adicional por el número de prefijo, y verificación con LUHN.
- La solución provee expresiones predefinidas para las direcciones de correo electrónico
- La solución provee expresiones predefinidas para los números de cuentas de bancos internacionales (IBAN).
- La solución provee expresiones predefinidas para códigos de identificación de negocio SWIFT BIC.
- El servidor de administración debe tener la capacidad de ser implementado en entornos VMWare Workstation versiones 6.0, 6.5, 7.0, y/o 8.0
- El servidor de administración debe tener la capacidad de ser implementado en entornos VMWare ESX(i) versiones 3.5, 4.0 y/o 4.1.
- La solución provee una lista de palabras predefinidas para la validación de formularios como fecha de nacimiento, fecha de expiración, Nombres y apellidos, lugar de nacimiento, departamentos o ciudades y direcciones de domicilios.
- La solución provee una lista de palabras que pueden ser usadas en contextos ofensivos, racistas o que incluyan elementos para causar daño (armas)
- La solución provee una lista de palabras que puedan identificar comandos o instrucciones en lenguajes de programación como C#, C/C++, COBOL, Java, Perl y VB.
- La solución debe permitir exportar e importar datos como políticas de seguridad y roles de usuarios.
- La solución debe permitir configurar y programar el reinicio de los dispositivos de forma que no afecte negativamente las operaciones de la organización.

3. Requerimientos de Control de aplicaciones

- La solución debe tener la capacidad de prevenir la ejecución de aplicaciones no deseadas o desconocidas en los endpoint
- La solución debe tener la capacidad de ser administrada mediante una consola web.
- La solución debe tener la capacidad de configurar acciones sobre los archivos que estén en la lista de Suspicious Objects proporcionada por el fabricante para sus soluciones de seguridad.
- La solución debe permitir la instalación de los agentes mediante un asistente de instalación o mediante la consola de comandos.
- Los agentes de protección de los equipos deben tener la capacidad de protegerse contra intentos de desinstalación o cancelación de los procesos por los usuarios o por una aplicación de terceros.
- La solución debe permitir ocultar del icono del agente y las notificaciones en los endpoint.
- La solución debe permitir bloquear o permitir aplicaciones de acuerdo a puntaje de seguridad propio del fabricante.
- La solución debe tener la capacidad de bloquear o permitir aplicaciones basada en patrones y puntaje de prevalencia de la aplicación.
- La consola de administración de la solución debe ser compatible con servidores web como Apache Tomcat 8 o Microsoft Internet Information Server (IIS) 7.0 o superior.
- La solución debe permitir el uso de protocolos TLS/SSL para la comunicación entre los

agentes y el servidor de administración.

- La solución debe tener la capacidad de proteger las contraseñas enviadas entre el navegador web y el servidor de administración mediante cifrado RSA y Hash.
- La solución debe permitir configurar el intervalo en el que los logs de los agentes son recolectados por el servidor de administración.
- La solución debe permitir configurar el intervalo en el que los agentes actualizan las políticas consultando el servidor de administración.
- La solución debe permitir la realización de backups de los datos de configuraciones de la solución, los certificados SSL, datos de los agentes, y logs almacenados en el servidor de administración.
- La solución debe permitir la realización de backups de los logs almacenados en los agentes.
- La consola de administración de la solución debe proporcionar gráficos y estadísticas de distribución de la solución, distribución de políticas y agentes administrados.
- La solución debe tener la capacidad de identificar o agrupar los logs por políticas, inventario de equipos, aplicaciones conocidas, acciones del administrador, mensajes de los agentes y mensajes del servidor.
- La solución debe tener la capacidad de generar o permitir importar los certificados de autenticación del servidor
- La solución debe permitir realizar una sincronización de la lista de objetos sospechosos obtenidos de otras soluciones del mismo fabricante.
- La solución debe contar con roles definidos con diferentes niveles de acceso para editar y/o visualizar los datos y configuraciones de la solución.
- La solución debe permitir realizar búsquedas en los registros o logs, haciendo uso de filtros y permitir exportarlos en archivos con formato (CVS o XLSX).
- La solución debe permitir establecer reglas para el cumplimiento de control de aplicaciones, dichas reglas deben permitir o bloquear aplicaciones de acuerdo con las políticas de la organización.

4. Requerimientos de herramientas de cifrado

- La solución debe contar con cifrado basado en hardware y en software para entornos mixtos
- La solución debe permitir la administración de las claves de cifrado, y la sincronización de políticas con todos los equipos
- La solución debe garantizar el cifrado de archivos, carpetas y medios extraíbles.
- La solución debe tener capacidad de implementar comandos remotos, recuperar datos perdidos y una sincronización de políticas en tiempo real
- "La solución debe tener integración con UEFI (Unified Extensible Firmware Interface), responsable de inicializar el hardware de los equipos antes de dar el control al sistema operativo.
- "
- La solución debe cifrar todas las unidades de disco físicas que tenga disponibles el equipo.
- "La solución debe contar con varios métodos de autenticación para el inicio de sesión en los equipos.
-

- ColorCode: Una secuencia única de colores.
- Domain Authentication: Sincronización LDAP de Active Directory para inicio de sesión único (SSO).
- Fixed Password: Una cadena de caracteres, números y símbolos.
- PIN: Un número de identificación personal estándar.
- Remote Help: Autenticación interactiva para usuarios que olvidan sus credenciales o dispositivos que no tienen políticas sincronizadas dentro de un período de tiempo predeterminado.
- Self Help: Combinaciones de preguntas y respuestas que permiten a los usuarios restablecer una contraseña olvidada sin ponerse en contacto con el Soporte técnico.
- Smart Card: Una tarjeta física utilizada junto con un PIN o una contraseña fija.
- "
- La consola debe proporcionar la capacidad de administrar los usuarios para agregar o eliminar cuentas, restablecer contraseñas, cambiar permisos, configurar prioridad de políticas, importar usuarios desde Active Directory y buscar cuentas de usuario específicas.
- La consola debe mostrar un estado actual de los discos cifrados de cualquier equipo con las fechas de última sincronización y política aplicada.
- La consola debe brindar la posibilidad de mostrar en todos los dispositivos los intentos fallidos de inicio de sesión.
- La consola debe mostrar los dispositivos que se encuentran bloqueados debido a restricciones de políticas.
- La consola cuenta con una lista de políticas donde muestra la información y el estado de las políticas creadas para todos los usuarios.
- La solución debe permitir el cifrado completo de disco incluyendo aplicaciones, configuraciones de registro, archivos temporales, archivos de intercambio, spoolers de impresión y archivos eliminados.
- La solución debe contar con un cifrado de archivos en el cual se pueda establecer una clave para cada archivo en específico sin importar que se encuentren en el mismo equipo.
- La solución debe usar cifrado AES
- La solución debe permitir a los usuarios restablecer una contraseña olvidada o una cuenta bloqueada antes de poder iniciar sesión el dispositivo.
- La consola debe generar un reporte en el que se muestren todas las posibles violaciones de seguridad en relación con conexiones fallidas, intento de manipulación de las políticas o intentos de modificación de los logs.
- La solución debe permitir la generación de informes donde se muestren datos como estados de cifrado, versiones de dispositivos, últimos usuarios conectados a los dispositivos.
- La solución debe utilizar los estándares de cifrado OPAL y OPAL 2.
- La solución debe contar con la certificación FIPS (Federal Information Processing Standard) 140-2
- El agente para el cifrado debe proteger los archivos y las carpetas ubicados en cualquier dispositivo que aparezca como una unidad dentro del sistema operativo.
- Los agentes deben integrarse con las soluciones de cifrado que vienen en los sistemas operativos. Microsoft BitLocker, Apple FileVault.

- LA HERRAMIENTA DE CIFRADO DEBERA SER COMPATIBLO MINIMO CON LOS SIGUIENTES SISTEMAS OPERATIVOS:
- Windows™ 8 (32-bit/64-bit)
- Windows™ 8.1 (32-bit/64-bit)
- Windows™ 10 (32-bit/64-bit)
- Windows™ Embedded POSReady 7 (32-bit/64-bit)
- OS X™ Sierra
- OS X™ El Capitan
- OS X™ Yosemite
- OS X™ Mavericks
- OS X™ Mountain Lion

5. Requerimientos de seguridad WEB

- La solución debe brindar protección frente amenazas de Malware, Ataques dirigidos, Vulnerabilidades de Dia cero Amenazas Avanzadas y Ransomware
- La solución debe ser en su totalidad as a Services
- La solución debe contar con reputación web adicional reputación de archivos
- La solución debe permitir el filtrado URL y control de aplicaciones que requieren navegación en Internet
- La solución debe analizar el tráfico entrante y saliente en busca de Malware
- Es requisito contar con la habilidad de configurar permisos granulares en la consola de administración para delegar operaciones y trabajos específicos a diversos usuarios o grupos de usuarios, así como perfiles de auditoría que solo permitan visualizar datos pero sin la capacidad de modificar ninguna configuración
- La solución debe permitir la integración con el Active Directory
- La solución debe permitir realizar un control de Ancho de Banda
- la solución debe permitir la implementación de políticas para evitar que los usuarios publiquen contenido en redes sociales o sitios de webmail
- La solución debe contar con un módulo de prevención de pérdida de datos y contar con políticas definidas por default, permitiendo usar palabras claves y templates
- La solución debe permitir la inspección de tráfico HTTP Y HTTPS
- La solución debe brindar alta disponibilidad del servicio
- La solución propuesta debe contar con un Dashboard el cual permita visualizar en tiempo real C&C, Ancho de banda usado, amenazas detectas, estado del servidor, estado de los agentes
- La solución debe proteger la navegación en los equipos móviles, endpoint y equipos que salen de la red corporativa
- El filtrado de URL de la solución debe estar definido por categorías
- Si una URL no está en la base de datos para verificar su confiabilidad esta debe ser testeada en tiempo real utilizando tecnología de categorización dinámica
- Se podrán crear usuario y roles para el acceso a la plataforma de administración
- La solución debe contar con la posibilidad de aplicar políticas de DLP para proteger la extracción de la información
- La actualización de patrones, firmas y mantenimiento de la plataforma será por parte del proveedor de la solución
- La solución debe contar con un analizador de objetos sospechosos en ambientes

controlados
- La solución debe notificar al usuario y al administrador cuando este incumpliendo las políticas o sea detectada una amenaza

6. Requerimientos de Aplicaciones WEB (Microsoft office 365)

- La solución deberá tener la capacidad para proteger correos internos de la organización que provengan de la plataforma de Microsoft Office 365.
- La solución deberá tener la capacidad para proteger correos de dominios externos y ajenos a la empresa que provengan de la plataforma de Microsoft Office 365.
- La solución deberá tener motores para la detección de malware con la capacidad de identificar Exploits en documentos y archivos de Office.
- La solución deberá tener Sandbox para análisis de amenazas desconocidas y ataques de día cero.
- La solución deberá ofrecer un análisis de riesgo para reducir el impacto en los usuarios
- La solución deberá tener escaneo de URL en el cuerpo de los correos y en los archivos adjuntos.
- La solución deberá ofrecer protección avanzada contra amenazas para OneDrive y SharePoint
- La solución deberá ofrecer protección avanzada contra amenazas para BOX, Dropbox y Google Drive.
- La solución deberá tener plantillas customizables de DLP para controlar la fuga de información permitiendo realizar pruebas de expresiones regulares y listados de palabras para nuevas plantillas
- La solución deberá tener DLP a nivel de Email con la capacidad de descubrir y reportar violaciones a las políticas.
- La solución deberá tener DLP a nivel de SharePoint y One Drive, con la capacidad de descubrir y reportar violaciones a las políticas.
- La solución deberá tener DLP a nivel de Box, Dropbox y Google Drive, con la capacidad de descubrir y reportar violaciones a las políticas.
- La solución no deberá exceder 1 minuto de latencia.
- La solución debe tener la capacidad de integrarse a una consola central de administración, desde la cual se puedan administrar otras soluciones del mismo fabricante como la solución para la protección de la navegación web, antivirus y se puedan aplicar políticas para evitar la fuga de información confidencial desde un punto central tanto en el Gateway como en el endpoint.
- La solución deberá tener la capacidad desde la consola en la nube, de crear políticas basadas en reglas según el correo entrante o saliente y a los cuales se les pueda personalizar las acciones a tomar en categorías de (Clean, Delete, Tag, encriptar, notificar).
- La solución deberá tener la capacidad en la consola en la nube de mostrar distintos gráficos para dar seguimiento al tráfico de correo y cuarentenas.
- La solución deberá tener la capacidad en la consola en la nube de habilitar a los usuarios finales la capacidad de aprobar remitentes para sacarlos de cuarentena.
- La solución deberá tener la capacidad de analizar los enlaces que se encuentren en el cuerpo del mensaje de los correos electrónicos, igualmente debe tener la capacidad de analizar los enlaces que se encuentren ocultos en el cuerpo del mensaje, ya sea en

botones, banners o imágenes en el momento en el que el usuario le de clic en el enlace

- La solución deberá tener la capacidad en la consola en la nube de reportar ataques dirigidos.
- La solución deberá permitir la aplicación de reglas de forma granular es decir que dichas políticas puedan ser aplicadas a cuentas de usuario especificas o elementos del correo.
- La solución debe proporcionar seguridad para la información que se encuentra almacenada en la nube y garantizar la privacidad de la misma.
- La solución debe tener la capacidad de identificar amenazas que aun no han sido reportadas con el análisis de los archivos.
- La solución debe proporcionar protección contra ataques de BEC (Bussiness Email Compromise) con el análisis de los mensajes.
- La solución debe tener la capacidad de detectar ataques dirigidos mediante explotación de archivos.
- La solución debe tener la capacidad de realizar un análisis avanzado de los archivos usando Machine Learning, para identificar amenazas que aún no han sido reportadas, pero que pueden generar una afectación sobre los datos o el sistema que está utilizando el usuario.
- La solución debe tener la capacidad de brindar protección contra ataques avanzados como Bussiness Email Compromise (BEC), Ramsomware, Phishing avanzado entre otros ya sea mediante firmas anti-spam o reglas heurísticas.
- La solución debe tener la capacidad de tomar una acción sobre los correos que sean identificados como spam avanzado, dichas acciones deben permitir eliminar, permitir, enviar a cuarentena o agregar una etiqueta al asunto del correo.
- La solución debe tener la capacidad de tomar alguna acción sobre los correos que sean analizados con el sandbox y sean identificados como maliciosos o sospechosos, dichas acciones deben permitir eliminar, permitir, enviar a cuarentena o agregar una etiqueta al asunto del correo.
- La solución debe tener la capacidad de tomar una acción sobre los archivos localizados en el servicio SharePoint Online o One Drive Bussiness y que sean analizados con el sandbox e identificados como maliciosos o sospechosos, dichas acciones deben permitir eliminar, permitir, enviar a cuarentena o agregar una descripción en el correo para informar al usuario por que el correo ha sido enviado a cuarentena o eliminados.
- La solución debe tener la capacidad de tomar una acción sobre los archivos localizados en el servicio Box for Business and Enterprise, Dropbox Business o Google Drive y que sean analizados con el sandbox e identificados como maliciosos o sospechosos, dichas acciones deben permitir eliminar, permitir, enviar a cuarentena o agregar una descripción en el correo para informar al usuario por que el correo ha sido enviado a cuarentena o eliminados.
- La solución debe tener la capacidad de notificar al usuario cuando algún correo que iba dirigido a tuvo alguna acción reactiva, basado en las reglas configuradas, dicha notificación debe indicarle que acción se tomó sobre el correo que iba dirigido y la razón de esta.
- La solución debe tener la capacidad de sincronizarse y actualizar la lista de objetos sospechosos cuando se existe la integración con el Trend Micro Control Manager.
- La solución debe tener la capacidad de integrarse con el Active Directory Federation

Services o Microsoft Azure AD, para permitir agregar usuarios administradores locales que puedan administrar la consola usando las credenciales registradas en estos servicios.

- La solución debe permitir a los administradores configurar la lista de excepciones, de los archivos detectados mediante Machine Learning como maliciosos o sospechosos.
- La solución debe permitir restaurar archivos que sean enviados a cuarentena ya sea por fueron detectados como maliciosos o que no cumplen con las políticas de prevención de filtración de datos de la organización.
- La solución debe permitir realizar un escaneo manual en modo de evaluación para permitir a los administradores verificar las reglas que seran aplicadas para proteger Office 365 sin tomar ninguna acción sobre dichos correos o archivos.

7. Requerimientos para protección de correo electrónico

- La solución debe ser totalmente administrable por medio de una consola web en la nube
- La consola de administración deberá ser capaz de integrarse con Microsoft Active Directory para la administración de usuarios y grupos.
- La solución debe permitir la creación de políticas globales para todas las cuentas, por perfiles e individualmente para cada usuario
- "La consola debe mostrar gráficamente la pestaña Estadísticas principales de las direcciones de correo electrónico que recibieron la mayor cantidad de mensajes relacionados con Business Email Compromise (BEC).
-
- (BEC) es un tipo de estafa dirigida a las empresas que realizan transferencias bancarias, las cuentas de correo electrónico corporativas, de ejecutivos, empleados de alto nivel relacionadas con finanzas o relacionadas con pagos de transferencias electrónicas son falsificadas y/o comprometidas mediante keyloggers o ataques de phishing para realizar transferencias fraudulentas, lo que resulta en cientos de miles de dólares en pérdidas."
- La consola debe tener la capacidad de mostrar la cantidad total de mensajes de correo electrónico escaneados por categoría detectada.
- La consola debe mostrar en detalle la cantidad de mensajes detectados como ransomware.
- La consola debe mostrar gráficamente las amenazas y el porcentaje total de mensajes detectados como amenaza.
- La consola debe tener conexión con un sanbox con el fin de analizar muestras de archivos con características sospechosas. Debe realizar análisis estáticos y simulación de comportamiento en diversos entornos de tiempo de ejecución para identificar características potencialmente maliciosas.
- La consola deberá contar con espacios independientes para la administración de políticas de protección tanto de entrada como de salida.
- La consola debe mostrar las direcciones de correo electrónico que recibieron la mayor cantidad de mensajes que contienen amenazas avanzadas, malware, spam.
- La solución debe permitir la configuración de políticas para comunicación cifrada.
- "La consola debe hacer trazabilidad de Time-of-Click realizado a las URL´s y la acción realizada por la solución.

- La disponibilidad del servicio de Time-of-Click debe detectar malware basado en enlaces y ataques de phishing al analizar la reputación de una URL al momento del clic de los usuarios y no solo en el momento de la entrega a del email. "
- La solución debe realizar Machine Learning para identificación y predicción de amenazas desconocidas.
- La consola debe enviar las notificaciones de las alertas generadas vía correo electrónico.
- La solución debe permitir crear reglas que tomen medidas sobre tipos de mensajes potencialmente no deseados como Spam , Phishing , Graymail , Reputación Web o Ingeniería social.
- La solución debe permitir la creación de reglas específicas que tengan acciones en mensajes que contienen malware, gusanos, troyanos u otro código malicioso.
- La consola debe permitir administrar los correos y archivos enviados a cuarentena con el fin de poder revisarse y borrarse o entregarse manualmente.
- La solución debe permitir importar y exportar los remitentes, los destinatarios y las listas de excepciones para las reglas de política tanto en la protección de entrada como de salida.
- La consola debe dar la opción de crear y administrar listas de remitentes bloqueados y aprobados.
- La solución debe brindar la información para permitir tomar medidas sobre los ataques de BEC mostrando los usuarios de alto perfil que son más vulnerables a estos tipos de ataques.
- La solución deberá utilizar una combinación de exploración basada en patrones y heurística para detectar explotaciones de documentos y otras amenazas utilizadas en ataques dirigidos.
- La solución debe permitir al usuario final administrar su propia consola de correos en cuarentena.
- La solución debe permitir la administración de Graymail (mensajes de correo electrónico masivos solicitados que no son spam) por separado del spam.
- La solución debe tener la capacidad de tomar un acción sobre los correos que sean analizados con el sandbox y sean identificados como maliciosos o sospechosos, dichas acciones deben permitir eliminar, enviar a cuarentena o agregar una etiqueta al asunto del correo.
- La solución debe ser 100 % compatible de para la protección en cloud con Microsoft Exchange, Microsoft® Office 365 y Google Gmail.

7.1 Regulatorios y cumplimiento

- La solución debe contar con certificaciones de privacidad de datos como ISO9001.
- La solución no puede superar una latencia de un minuto en la entrega del correo electrónico.
- La asistencia técnica debe estar disponible para de forma ininterrumpida por correo electrónico o por teléfono.
- Se debe proporcionar compatibilidad con el cumplimiento de GDPR en plantillas de prevención de pérdida de datos (DLP).
- La solución debe tener un sistema de validación para detectar y evitar la suplantación

de correo electrónico
- La solución deberá contar con DLP, con el fin de proteger la pérdida de datos mediante el control del tráfico de correo saliente.

7.2 Reportes

- La solución permite la generación de reportes bajo demanda o calendarizados.
- La solución debe tener un módulo de registros de auditoría que permita rastrear la administración y los eventos ocurridos
- La consola deberá mostrar la cantidad total de mensajes aceptados y bloqueados junto con su porcentaje total en un rango de fechas especifico.

8. Requerimientos para protección de dispositivos móviles

8.1 Consola de administración y gestión

- La consola de administración debe contar con Dashboards que permitan monitorear los dispositivos de forma sencilla y estos pueden ser personalizados por el administrador
- La consola de administración deberá permitir control y visibilidad de los dispositivos móviles que cuenten con un agente instalado.
- La solución deberá permitir la creación, modificación y eliminación de grupos, los cuales servirán para estructurar los agentes y poderlos administrarlos más fácilmente.
- La solución deberá permitir estructurar los dispositivos administrados en grupos para facilitar su administración.
- La solución deberá tener la capacidad de crear, modificar o eliminar políticas y asignarlas a un dispositivo o a un grupo de dispositivos.
- La solución deberá permitir configurar los escaneos de para un solo dispositivo o para múltiples dispositivos.
- La solución deberá permitir la eliminación de un dispositivos o eliminación de múltiples dispositivos
- La solución deberá permitir la administración de las aplicaciones permitidas para ser instaladas en los dispositivos.
- La solución deberá permitir la creación, modificación y eliminación de cuentas de usuarios y roles, para la consola de administración y gestión.
- La solución deberá tener la capacidad de realizar la búsqueda de los dispositivos permitiendo el uso de filtros como (teléfono, IMEI, Numero del Serial, Dirección MAC, etc) para búsquedas avanzadas.
- La solución deberá tener la capacidad de recuperar las licencias de las aplicaciones desde los dispositivos.
- La consola de administración debe tener la capacidad de generar reportes relacionados a las vulnerabilidades recomendadas a proteger, así como identificar cuales vulnerabilidades ya fueron parchadas en el servidor y que deben ser deshabilitadas.
- La solución deberá permitir la carga de certificados en formatos como .pfx, .p12, .cer, .crt o .der para ser utilizados por el Servidor de administración, e igualmente deberá permitir la eliminación de los mismos.
- La solución deberá tener la capacidad de visualizar mediante la consola de administración las aplicaciones sospechosas, certificados maliciosos instalados en los dispositivos que están siendo administrados por la solución.

- La solución deberá tener la capacidad de enviar notificaciones (Detecciones de Malware, Certificados Maliciosos, Errores de Sistema, etc) y reportes vía email a los administradores y/o usuarios.
- La consola de administración deberá ser capaz de integrarse con Microsoft Active Directory para la administración de usuarios de acceso a la consola y realizar búsqueda de nuevos dispositivos en el dominio
- La solución deberá permitir localizar un dispositivo y acceder remotamente para reiniciar contraseñas, bloquearlo o eliminar toda la información en caso de pérdida del dispositivo.
- La solución deberá ser capaz de generar reportes desde la consola de administración, permitiendo generarlos por rango de tiempo (máximo 30 días).
- La solución deberá tener la capacidad de programar la generación de reportes (diario, semanal, mensual)
- La solución debe tener la capacidad de realizar las actualizaciones de los componentes de forma programada o manual, y notificar a los dispositivos cuando las actualizaciones estén disponibles.
- La solución debe tener la capacidad de conectarse con el servicio de Microsoft Exchance Server para permitir administrar los dispositivos que user Exchange ActiveSync.
- La solución debe permitir integración con aplicaciones de terceros como AirWatch, y/o Mobile Iron.
- La solución debe tener la capacidad de realizar un análisis estático de los archivos sospechosos con el uso de Predictive Machine Learning.
- La solución debe permitir el registro de dispositivos mediante unlaces web, códigos QR o una descarga desde iTunes.
- La solución debe permitir el aprovisionamiento y des aprovisionamiento de los dispositivos de forma remota utilizando una VPN, Exchange ActiveSync y WI-FI.
- La solución debe permitir que los agentes tengan la capacidad de conectarse con el servidor de administración ya sea que este se encuentre implementado dentro de la organización o este implementado en un ambiente en la nube
- La consola de administración deberá ser accedida mediante los navegadores Internet Explorer 9.0 o superior, Chrome 17 o superior, Firefox 14 o superior y/o Safari 6 o superior.

8.2 Regulatorios y cumplimiento

- El servicio debe cumplir como controles compensatorios en PCI Compliance 3.2 relacionados a los numerales 5 y 6 que indican la necesidad de identificación y protección de vulnerabilidades

8.3 Agentes

- Los agentes deben permitir ser instalados mediante el servidor de administración o mediante la tienda de Google Play
- Dispositivos Móviles Android
    - El dispositivo debe contar con una versión del sistema operativo Android en la versión 2.1 o superior
    - El dispositivo debe contar con un mínimo de memoria de almacenamiento de 8

MB
    - El dispositivo debe contar con una memoria ram de al menos de 10 MB
- Dispositivos Móviles iOS
    - El dispositivo debe contar con una versión del sistema operativo iOS en la versión 4.3 o superior
    - El dispositivo debe contar con un mínimo de memoria de almacenamiento de 3 MB
    - El dispositivo debe contar con una memoria ram de al menos de 4 MB
- Dispositivos Móviles Windows Phone
    - El dispositivo debe contar con una versión del sistema operativo Windows Phone 8.0 o 8.1

8.4 Reportes

- La solución debe tener la capacidad de generar, visualizar, programar y enviar reportes y debe permitir descargarlos y/o enviarlos por email.
- La solución debe permitir generar un reporte de seguridad que debe incluir información sobre malware detectado, aplicaciones modificadas, riesgos de privacidad, aplicaciones vulnerables, descripción de trafico de red, puntos de acceso no confiables, certificados SSL maliciosos, perfiles iOS maliciosos, configuraciones de desarrollo, estado de usuarios Root/Jailbreak de los dispositivos, y el Top 10 de los sitios web bloqueados.
- La solución debe permitir generar un reporte del inventario de dispositivos que contengan información de todos los dispositivos administrados.
- La solución debe permitir generar reportes que contengan información sobre los dispositivos que se encuentren en el programa de inscripción de dispoositivos. (Aplica para Apple únicamente).
- La solución debe permitir generar reportes acerca de las violaciones de cumplimiento y/o inventario de aplicaciones.
- La solución debe permitir la modificación de la plantilla del correo que se usa para enviar los reportes por email.

8.5 Servidor de comunicación y servidor de administración

- El servidor de comunicación deberá tener la capacidad de ser implementado en entornos en la nube, en un servidor local o en el mismo servidor donde se encuentra el servidor de administración.

8.6 Sistemas operativos y software

- Windows Server 2008 R2 Enterprice Edition
- Windows Server 2008 Enterprise Edition SP1
- Windows Server 2008 Standard Edition
- Windows Web Server 2008 Edition SP1
- Windows Server 2016
- Windows 2008 Server Family
- Windows 2008 R2 Server Family
- Windows 2012 Server Family
- Windows Server 2012 R2 Family

- Microsoft Internet Informaton Server (ISS) 7.0/7.5/8.0
- Microsoft Exchange Server 2007
- Microsoft Exchange Server 2010
- Microsoft Exchange Server 2013
- Microsoft SQL Server 2008
- Microsoft SQL Server 2008 Express Edition
- Microsoft SQL Server 2008 R2
- Microsoft SQL Server 2008 R2 Express Edition
- Microsoft SQL Server 2012
- Microsoft SQL Server 2012 Express Edition
- Microsoft SQL Server 2014
- Microsoft SQL Server 2014 Express Edition
- MOBILE SECURITY EXCHANGE CONNECTOR
    - Windows Server 2008 R2 (64-bit)
    - Windows Server 2012 (64-bit)
    - Windows Server 2012 R2 (64-bit)
    - Microsoft .Net Framework 3.5 SP1

9. Requerimientos para solución extendida de detección y respuesta (XDR)

- La solución debe permitir la detección de amenazas tipo Fileless a través de la exploración de memoria mejorada para detectar comportamientos de procesos sospechosos. El agente debe tener la capacidad de terminar los procesos sospechosos antes de que se pueda hacer cualquier daño.
- "La solución debe permitir evaluar el alcance del daño causado por un ataque dirigido, proporcionar información sobre la llegada y progresión del ataque y ayudar en la planificación de una respuesta efectiva a incidentes de seguridad.
- "
- La solución debe permitir generar investigaciones preliminares para identificar rápidamente los puntos finales que son posibles candidatos para un análisis adicional.
- La solución deberá permitir graficar toda la cronología de los eventos generados en una investigación por medio de un gráfico de anillos que muestra el número total de puntos finales clasificados ya sea estén relacionados, o no relacionados a otros procesos, en cola o cancelados. La información debe estar siendo actualizada en tiempo real y de forma automática mientras avanza una investigación.
- La solución debe permitir la búsqueda de Indicadores de Compromiso (IoC) en búsqueda de comunicaciones específicas, actividad de registro, actividad de la cuenta autenticada en el sistema y procesos en curso.
- La solución debe permitir la integración con información externa de IoC (Indicators Of Compromises) como reglas YARA, OpenIoC, STIX, TAXII
- La solución debe permitir el análisis de comportamiento de un malware, actividades especificas de IoC y conexiones de comando a control.
- La interfaz de la solución debe estar integrada con la consola de administración de las soluciones de seguridad para tener desde un solo punto el análisis, el contexto completo de los eventos y la línea de tiempo de los sucesos.
- La solución debe convivir con cualquier solución de malware en el caso que el equipo a proteger tenga otro tipo de protección.

- La solución debe controlar los programas que demuestran un comportamiento anormal asociado con ataques de exploits.
- La solución debe escanear documentos en busca de códigos de exploits integrados y vulnerabilidades conocidas
- La solución debe analizar los archivos desconocidos de baja prevalencia utilizando algoritmos de aprendizaje automático para determinar si el archivo es malicioso.
- La solución debe ser capaz de recopilar datos del sensor en los endpoints(IOC) y almacenarlos de forma centralizada para su posterior análisis.
- La solución instantáneas de datos volátiles: maneja archivos, claves de registro, procesos, hilos, controladores cargados, , tareas, servicios, DNS, ARP, socket, etc.
- La solución debe contar con la capacidad de registrar eventos basados en criterios establecidos.
- La solución debe tener la capacidad de realizar barrido de IOC en todos los dispositivos con sensor.
- La solución debe tener la capacidad de asociar los datos de registro y logs de los procesos con otros artefactos de disco y/o memoria.
- La solución debe solo usar un agente para realizar la protección antimalware, virtual patching, DLP, control de aplicaciones y EDR.
- La solución debe tener la capacidad de buscar reglas de Yara en: memoria, memoria de proceso, registros, archivos individuales, carpetas, disco entero y eventos.
- La solución debe permitir realizar consultas y luego crear alertas personalizadas con base en ellas.
- La solución debe permitir la exportación de inteligencia de amenazas a través de STIX/TAXII
- La solución debe mostrar todos los dispositivos en los que un proceso principal (padre) inicia otros procesos (hijos) especialmente de tipo powershell y cmd.
- La solución debe tener la capacidad de identificar amenazas aún cuando usen powershell codificado.
- La solución debe detectar tareas programadas maliciosas.
- La solución debe revelar la cadena completa de procesos afectados por el malware/comportamiento malicioso.
- La solución debe contar con la capacidad de mostrar la línea de tiempo de incidentes.
- La solución debe tener la capacidad de mostrar en una sola vista todo el ciclo de vida del ataque de la amenaza
- La solución permitirá que el trabajo de investigación continúe en el dispositivo aislado sin permitir que se extienda la actividad maliciosa por medio de cuarentena y/o aislamiento de los sistemas infectados
- La solución de XDR no debe requerir un agente adicional a los agentes de Endpoint y Server Protection instalados en las maquinas
- La solución de detección y respuesta debe permitir la correlación entre, endpoints y los servidores de mismo fabricante del XDR
- XDR debe contar con modelos de detección avanzados que detectan actividades de bajo perfil en distintas capas de seguridad para encontrar nuevos ataques.
- Los modelos de correlación deben combinar múltiples reglas y filtros usando una variedad de técnicas de análisis como, pero no limitándose, a Data Stacking y Machine Learning.

- La Plataforma de detección y respuesta debe proveer la posibilidad de encender y apagar modelos según la tolerancia al riesgo y preferencias de la entidad.
- Debe contar con gráficas: una representación visual de los objetos que levantaron la alerta y la relación entre ellos.
- XDR debe permitir entender la historia del ataque con una representación visual e interactiva de los eventos.
- Debe tener la capacidad de verificar el perfil de ejecución/análisis de causa raíz (Execution Profile/Root Cause Analysis) para ver las accionas que una amenaza llevó a cabo en un servidor, endpoint, o carga de trabajo en la nube.
- Debe permitir investigar adicionalmente desde la perspectiva de red (Network Analysis) para reproducri las comunicaciones y ver el detalle de acciones de un atacante como comunicaciones de comando y control o movimientos laterales.
- Debe permitir la búsqueda proactiva a traves de endpoint, red, email, y servidores (como telemetría, NetFlow, metadata, etc.) usando un simple constructor de consultas.
- Debe permitir hacer un barrido con IoC (indicadores de compromiso) o búsquedas personalizadas usando múltiples parámetros, y filtrar los resultados añadiendo criterios adicionales de búsqueda.
- Desde el resultado de una búsqueda se debe poder ejecutar acciones de respuesta y generar un análisis de causa raíz.
- Se debe poder construir, guardar y reutilizar búsquedas para Threat Hunting básico.
- Debe detectar proactivamente con búsquedas automáticas de IoC publicados por el vendor
- La capacidad de Threat Intelligence embebida debe ser capaz de identificar la campana asociada, la Plataforma atacada, las Técnicas, Tácticas y Procedimientos (TTPs) alineadas a MITRE ATT&CK™ y debe proveer enlaces/links a entradas de blog relacionados si están disponibles.
- Enlaces desde la consola centralizada de visibilidad de eventos a la documentación del framework de MITRE ATT&CK.
- En una sola ubicación debe poder iniciar y ver estado de respuesta en endpoint, email, servidores y red.
- Debe ofrecer opciones de respuesta “context aware” para acciones rápida desde la plataforma.
- Debe permitir ejecutar acciones de respuesta rápidamente haciendo click derecho en el workbench o desde los resultados de búsqueda de Threat Intelligence.
- Una API pública debe poder ser usada por clientes para integrarse con SIEM y herramientas SOAR.
- Debe proveer un conector para Splunk nativo.
- Debe ser una solución hospedada y administrada en Nube (SaaS) para tomar ventaja de tecnologías Cloud
- La solución deberá contar con una aplicación que permita asegurar el acceso hacia aplicaciones internas y en la nube para cualquier usuario, dispositivo y ubicación, en cualquier momento.
- La solución deberá permitir administrar el riesgo de los usuarios y controlar el acceso a recursos mediante la definición de reglas de acceso privado, acceso a Internet y reglas basadas en riesgo.
- La solución podrá integrarse con soluciones de identidades como Azure AD, Okta y

Active Directory con el objetivo de permitir monitorear los intentos de inicio de sesión, acceso a los datos de los usuarios y realizar acciones sobre las cuentas de los usuarios.

- La solución deberá permitir dentro de las reglas de acceso, la configuración de perfiles de postura para los usuarios VIP, con el fin de permitir o denegar el acceso con base en la definición de criterios como sistema operativo, política de firewall, software de antivirus y control de aplicaciones, esto con el fin de poder mitigar riesgos por el uso de aplicaciones como WhatsApp.
- La solución dentro de la aplicación de Acceso Seguro deberá contar con una pantalla que proporcione logs detallados sobre el acceso de usuarios y dispositivos a aplicaciones internas y en la nube.
- La solución deberá proveer un servicio de control de riesgo que permita identificar usuarios y dispositivos que exhiban comportamientos riesgosos o maliciosos, así como tomar medidas de mitigación manuales y automatizadas como la des habilitación de cuentas de usuarios, forzar cierre de sesión o forzar el restablecimiento de la contraseña.

10. Requerimientos para protección avanzada de servidores y cargas de trabajo

10.1 consola de administración y gestión

- La solución de protección de servidores debe incluir módulos de Antimalware, File Integrity Monitoring, Control de aplicaciones, Firewall, prevención de Intrusiones en host, escaneos de vulnerabilidades recomendados y deben ser administrado sobre una única consola de la solución usando un único agente
- La solución deberá tener la capacidad de reconocer los agentes desplegados en la red por medio de una tarea manual o programada
- La solución deberá tener la capacidad de proteger los servidores a través de scripts, los cuales pueden ejecutarse de forma manual o programada en servidores físicos, virtuales o de nube.
- Es requisito contar con la habilidad de configurar permisos granulares en la consola de administración para delegar operaciones y trabajos específicos a diversos usuarios o grupos de usuarios, así como perfiles de auditoría que solo permitan visualizar datos pero sin la capacidad de modificar ninguna configuración
- La solución permite la generación de reportes bajo demanda o calendarizados permitiendo el envío de dichos reportes vía e-mail
- La solución de virtual patching debe estar en una única consola y debe permitir la administración de todos los agentes instalados en servidores sin importar el tipo de infraestructura ya sea en nube, virtual o física.
- La consola de administración debe tener la capacidad de generar reportes relacionados a las vulnerabilidades recomendadas a proteger, así como identificar cuales vulnerabilidades ya fueron parchadas en el servidor y que deben ser deshabilitadas.
- La consola de administración debe tener la capacidad de generar reporte en formato PDF protegidos con contraseña
- La consola de administración debe tener la permitir incluir el logotipo de la empresa en los reportes.
- La consola de administración deberá ser capaz de integrarse con Microsoft Active

Directory para la administración de usuarios de acceso a la consola y realizar búsqueda de nuevas máquinas en el dominio

- La consola de administración deberá contar con la capacidad de etiquetar eventos importantes de seguridad y de duplicar esas etiquetas para eventos futuros
- La Consola de administración debe ser Cloud
- La solución debe contar con políticas por defecto que eviten la desinstalación del agente de seguridad y/o la baja de servicios del mismo. (Agent Self Protection)
- La solución debe permitir la creación de políticas globales para todas las maquinas, por perfil e individualmente para cada host
- Se debe tener acceso a la consola con una previa configuración de roles y perfiles granulares para la programación de los escaneos, aplicación de reglas de protección y acceso a tableros de control de la solución para el análisis de vulnerabilidades, activación de reglas de protección y que permita visualizar el estado de seguridad de las aplicaciones y del sistema operativo.
- La solución deberá ser administrada por consola web y debe soportar certificado digital para su gerenciamiento
- La comunicación entre la consola de administración y los agentes debe estar cifrada
- La consola debe permitir tener múltiple factor de autenticación para los administradores
- La consola de administración debe contar con Dashboard que permitan monitorear los equipos de forma sencilla y estos pueden ser personalizados por el administrador
- La consola de administración de servidores debe integrarse nativamente con la solución de XDR de su mismo fabricante
- La Consola de la solución debe proporcionar monitoreo continuo para visibilidad instantánea y completa del entorno, notificaciones en tiempo real de las actividades y eventos que ocurran; permitir la generación de reportes customizables y desde el mismo dashboard de la consola de la solución poder administrar entornos físicos, virtuales y en la nube
- La solución deberá detectar automáticamente nuevos servidores en los diferentes sistemas de infraestructuras de servidores públicas y privadas en vCenter, AWS, Microsoft Azure, vCloud Air, Directorio Activo
- El servicio debe cumplir como controles compensatorios en PCI Compliance 3.2 relacionados a los numerales 5 y 6 que indican la necesidad de identificación y protección de vulnerabilidades
- El fabricante de la solución debe estar ubicado por tercer año consecutivo en el cuadrante de lideres de Gartner para soluciones de Endpoint relacionado a servidores y equipos de usuario final
- La solución debe dar cumplimiento como control compensatorio para los principales requisitos reglamentarios para PCI DSS 3.2, HIPAA, NIST, SSAE 16, entre otros.

10.2 Agentes

- La solución deberá permitir la distribución de patrones, motores y nuevos componentes a través de los agentes de actualización que pueden distribuirse en todo el ambiente
- Los agentes de actualización deben buscar las actualizaciones de firmas y componentes y distribuirlas a los agentes, estas actualizaciones deben realizarse en modo seguro utilizando comunicación SSL con el servidor del cual se descarga dicha información

- El agente debe tener la capacidad de realizar un escaneo por servidor para determinar las vulnerabilidades presentes en el sistema operativo y las aplicaciones instaladas.
- La solución debe permitir una protección coordinada para el firewall, prevención de Intrusiones, escaneo de vulnerabilidades usando un único agente instalado en cada servidor para mínimo los siguientes sistemas operativos de Microsoft Windows: Windows Server 2022, Windows Server 2019, Windows Server 2016 (64-bit),Windows Server 2012 or 2012 R2 (64-bit),Windows Server 2008 R2 (64-bit),Windows Server 2008 (32-bit and 64-bit) y Windows Server 2003 (32-bit and 64-bit)
- La solución debe permitir una protección coordinada para el firewall, prevención de Intrusiones, escaneo de vulnerabilidades usando un único agente instalado en cada servidor para mínimo los siguientes kernels de UNIX: Solaris 9, 10 y 11 (SPARC de 64 bits), Solaris 10 y 11 (x86 de 64 bits), AIX 5.3, 6.1, 7.1
- La solución debe permitir una protección coordinada para el firewall, prevención de Intrusiones, escaneo de vulnerabilidades usando un único agente instalado en cada servidor para mas de 2000 kernels de Linux dentro de los que se deben soportar con mínimo los siguientes: Red Hat Enterprise Linux 8 (64-bit), Red Hat Enterprise Linux 7 (64-bit), Red Hat Enterprise Linux 6 (32-bit and 64-bit), CentOS 7 (64-bit), CentOS 6 (32-bit and 64-bit), Oracle Linux 7 (64-bit), Oracle Linux 6 (32-bit and 64-bit), SUSE Enterprise Linux 12 (64-bit), SUSE Enterprise Linux 11 SP1, SP2,SP3, and SP4 (32-bit and 64-bit), CloudLinux 7 (64-bit), Debían 8 (64-bit), Ubuntu 16.04 LTS (64-bit)
- El agente debe permitir tener identificación de maquinas con Docker y generar protección a estos.
- La solución debe permitir la protección de ambientes Docker en los cuales aplican para Docker Community Edition (CE) and Docker Enterprise Edition (EE), como mínimo debe soportar las siguientes versiones: Docker v1.12, v1.13 y Docker 17.03-ce, v1.13

10.3 Antimalware

- "La solución debe tener la capacidad de brindar protección contra malware, virus de red, conexiones sospechosas, amenazas web, spyware, monitoreo
- de comportamiento, ataques combinados y ataques de día cero para equipos de punto final (Endpoint)."
- La solución de protección de Servidores se podrá implementar en más de 2000 kernels de Linux.
- La solución de protección de servidores debe soportar sistemas legacy tales como Windows 2003 y 2008 Server.
- La solución de protección de servidores y protección de Endpoints deben ser del mismo fabricante.
- "La solución debe permitir hacer backup y restauración automática de archivos ante intentos de cifrado no autorizados, con el fin de generar una
- protección proactiva contra Ransomware."
- La solución debe permitir realizar escaneos de los endpoint de forma manual, programada y en tiempo real.
- "La solución debe tener la capacidad de aislar los equipos o ponerlos en cuarentena cuando se detecta algún ataque para evitar la propagación del
- mismo dentro de la red."

- La solución debe permitir la integración con 1 o más dominios.
- La solución debe permitir recuperar los archivos que sean enviados a cuarentena.
- La solución debe proporcionar protección a los agentes contra Ramsomware.
- La solución debe proporcionar una consola de administración que pueda ser utilizada desde un entorno web.
- "La solución deberá permitir la distribución de patrones, motores y nuevos componentes a través de los agentes de actualización que pueden distribuirse
- en todo el ambiente."
- Los agentes de actualización deben buscar las actualizaciones de firmas y componentes y distribuirlas a los agentes, estas actualizaciones deben realizarse en modo seguro utilizando comunicación SSL con el servidor del cual se descarga dicha información.
- La solución debe tener la capacidad de analizar la reputación de archivos.
- La solución debe permitir la creación, modificación y eliminación de roles y usuarios para la administración de la misma.
- La solución debe tener la capacidad de proteger los equipos que se encuentren dentro de la red y fuera de ella.
- La solución debe tener la capacidad de programar las sincronizaciones de los equipos para horas y fechas específicas.
- La solución debe permitir la configuración de un servidor SMTP para el envió de notificaciones vía Email
- La solución debe permitir seleccionar el criterio de las notificaciones para ser enviadas a la administración, cuando una amenaza sea detectada.
- La solución debe permitir la configuración de la plantilla del correo para él envió de notificaciones.
- La solución debe permitir seleccionar el criterio de las notificaciones para ser enviadas al administrador, cuando uno de los equipos sea enviado a cuarentena.
- La solución debe permitir la configuración de la plantilla del correo para él envió de notificaciones cuando los equipos sean enviados a cuarentena.
- La solución debe permitir la configuración de los tipos de eventos que serán notificados y visualizados en el agente, y adicionalmente configurar el mensaje de las alertas dependiendo de la criticidad del evento (High, Medium, Low)
- La solución debe tener la capacidad de finalizar sesiones en la consola de administración por tiempo de inactividad.
- La solución debe tener la capacidad de hacer Rollback de las actualizaciones de los componentes.
- La solución debe tener la capacidad de eliminar de los logs de los eventos del sistema, servidor y agentes, para que estos sean eliminados con una frecuencia especifica.

10.4 Escáner de vulnerabilidades

- El servicio debe tener la capacidad de ejecutar escaneos que permitan identificar vulnerabilidades a nivel de Sistema Operativo y aplicaciones
- La solución deberá contar con la capacidad de realizar escaneos de vulnerabilidades de aplicaciones en las que se busquen las 10 vulnerabilidades más altas catalogadas por la OWASP y los criterios de prueba de WASC.
- La solución deberá contar con la capacidad de realizar escaneos de recomendaciones

bajo demanda y programados, sin límite de escaneos, para detectar vulnerabilidades relacionadas con la plataforma (sistema operativo, aplicativo de servidor web y aplicativo de servidor de aplicaciones) sobre la cual están montados los sitios web expuestos a Internet

- Los escaneos deben realizarse desde un agente ligero instalado en los servidores revisando llaves de registro, metadata para validar la existencia y falta de parches y vulnerabilidades en las aplicaciones y el sistema operativo
- La solución deberá contar con reportes y bitácoras que contengan la lista de todas las vulnerabilidades encontradas en la plataforma de los servidores dónde se encuentran los sitios web, clasificadas por nivel de severidad, haciendo referencia al identificadores como Bugtraq, Secunia, CVE (Common Vulnerabilities and Exposures) y en el caso de Microsoft al boletín.
- La solución debe generar reglas de protección tanto para amenazas conocidas como desconocidas de día Zero y estas reglas de protección deben permitir la acción de bloquear o monitorear y deben ser enfocadas en técnicas de explotación, protección de la vulnerabilidad y en reglas inteligentes para identificar comportamiento anómalo.

10.5 Firewall

- La solución deberá contener un firewall que proteja servidores físicos, y/o virtuales y/o en la nube administrados desde la misma consola, permitiendo sólo las comunicaciones requeridas entre ellos. Este filtrado debe ser bidireccional y hacerse al menos sobre los siguientes parámetros: Protocolos: ICMP, IGMP, GGP, TCP, PUP, UDP, IDP, ND, RAW, TCP+UDP, Direcciones MAC, Direcciones IP y Puertos TCP & UDP
- El Firewall debe permitir la activación de un stateful inspection por tipo de servicio (FTP, WEB) y por interfaz, el cual permitirá corregir y proteger respecto a anomalías comunes de fragmentación de los paquetes, conexiones anómalas, saturación o tormentas de ACK, elevación en el numero de paquetes que intenten generar una denegación de servicio de las aplicaciones y afectación del sistema operativo.
- El Firewall debe ser capaz de reconocer y bloquear direcciones IP que estén realizando escaneos de reconocimiento, port scan, TCP Null Scan, TCP SYNFYN Scan, TCP Xmas Scan por hasta 30 minutos.

10.6 virtual patching

- Las brechas de seguridad descubiertas por medio de escaneo de recomendaciones deben ser protegidas de forma automática y transparente, interrumpiendo únicamente el tráfico malicioso.
- El administrador de la solución deberá contar con la posibilidad de aplicar automáticamente la protección para las vulnerabilidades a través de un perfil o por host
- El servicio debe tener la capacidad de ejecutar escaneos de puertos
- El fabricante de la solución debe estar ubicado en el top de grupos de investigación de vulnerability research para el descubrimientos de vulnerabilidades de día Zero que permitan generar la inteligencia en el desarrollo de reglas para vulnerabilidades desconocidas.
- La solución debe permitir la aplicación de reglas para la protección de vulnerabilidades de forma automática posterior a un escaneo de vulnerabilidades
- la solución debe permitir visualizar si una vulnerabilidad ya fue remediada o fue instalado el parche en su aplicación o sistema operativo

- La solución desde la misma consola debe permitir la gestión y protección de servidores e instancias privadas y publicas
- La solución debe permitir la creación de tareas programadas para la generación de escaneos de recomendaciones y reportes de reglas de vulnerabilidades aplicadas y recomendadas para aplicar
- La creación de tareas programadas de escaneos de vulnerabilidad debe ser para un servidor en específico o un grupo de servidores
- La solución debe tener una subscripción al Microsoft Active Protection Program (MAPP) para que cuente con la información oportuna con la cual proteger de vulnerabilidades conocidas y que esto no genere costos adicionales de licenciamiento.
- La solución debe permitir generar un inventario de aplicaciones y sistemas donde se identifiquen las vulnerabilidades a las cual está expuesto, esta validación se debe realizar sin afectar las aplicaciones con un solo agente en el equipo validando internamente llaves de registros y metadata que identifiquen la vulnerabilidad o parches faltantes en los sistemas.
- El fabricante de la solución debe reactivamente desplegar parches virtuales para vulnerabilidades críticas de Microsoft en el mismo día o antes de que sean publicados por parte de Microsoft y deben estar disponibles inmediatamente en la solución
- La aplicación de reglas de protección de vulnerabilidades se debe realizar sobre el tráfico de red, de forma transparente, sin generación de falsos positivos, sin afectar tráfico no anómalo y no deben requerir reinicio de máquinas, ni afectación del Sistema operativo, aplicaciones o código existente en el ambiente de la corporación.
- La solución debe estar en capacidad de generar parches virtuales para vulnerabilidades críticas de día Zero para aplicaciones y sistemas donde todavía el fabricante no ha desplegado el parche oficial
- La solución debe seguir generando de forma inmediata parches de protección para vulnerabilidades en Sistemas Operativos Windows 2003 y Windows 2000 que ya no soportados y donde el fabricante no genera parches para corrección vulnerabilidades
- La solución deberá ser capaz de realizar una inspección profunda de los paquetes bidireccionalmente para analizar y prevenir ataques a vulnerabilidades en las aplicaciones instaladas en cada servidor, incluidas vulnerabilidades conocidas y de día cero
- Las reglas de protección de vulnerabilidades deben tener la capacidad de ser aplicadas con acciones de bloqueo y monitoreo y deben capturar el stream o la cadena de caracteres de la ejecución de un ataque que permita el análisis del evento y alertamiento.
- Las vulnerabilidades deberán ser protegidas frente aquellas descubiertas recientemente y aplicando la protección en los servidores sin tener que reiniciar el sistema o modificar el código fuente de la(s) aplicación(es) o sistema operativo
- La solución debe proteger ataques de tipo Inyección de SQL, secuencias de comandos de sitios cruzados (Cross-Site Scripting) y otras vulnerabilidades de las aplicaciones web
- La solución deberá generar un inventario de aplicación e identificar las vulnerabilidades y recomendar automáticamente reglas en base al sistema operativo y aplicaciones instaladas en cada uno de los servidores.

10.7 Monitoreo de integridad de los archivos (FIM) inspección de LOGS

- La solución debe contar con mas de 200 políticas predefinidas de File Integrity Monitoring
- la solución debe tener políticas predefinidas de File Integrity Monitoring para Sistemas Operativos y aplicaciones
- La solución debe permitir crear políticas personalizadas de File Integrity Monitoring y se debe poder definir una severidad
- Las políticas personalizadas de File Integrity Monitoring deben permitir crear políticas para archivos y llaves de registro
- Las políticas personalizadas de File Integrity Monitoring deben permitir monitoreo en tiempo real
- La solución de File Integrity Monitoring debe contar con reglas asociadas al Enterprise Matriz de MITRE
- La solución debe contar con políticas predefinidas de File inspección de Logs
- La solución debe tener como mínimo 15 tipos de severidad para las alertas
- la solución debe permitir alertar los logs dependiendo la severidad de la alerta
- La solución debe permitir crear políticas personalizadas de Log Inspección
- Las reglas de Log Inspección deben permitir configurar dependencia de otras reglas o evento configuradas

10.8 Integración

- La solución debe contar con conectores de cloud para al menos: VCloud, AWS y Azure y que estos se administren desde la misma consola que el resto de módulos
- La consola de administración de alertas sobre los eventos de seguridad, deberá ser enviado a sistemas de correlación (SIEM) vía protocolos o métodos estándares, como Syslog (LEEF, CEF), SNMP y/o correo electrónico además de integrarse con diferentes tecnologías de SIEM (ArcSight, NetIQ, Intellitactics, RSA Envision, Q1Labs, Loglogic, Sentinel) en caso de ser requerido
- La solución debe permitir en caso de ser necesario y de forma nativamente la gestión externa desde plataformas de correlación como Splunk y QRadar
- La consola de administración deberá ser capaz de integrarse con Microsoft Active Directory para la administración de usuarios de acceso a la consola y realizar búsqueda de nuevas máquinas en el dominio
- La solución debe permitir la integración por medio de SOAP Web Service API para la gestión externa de plataformas de administración internas de la organización.

10.9 Nube

- La solución deberá adaptarse a la capacidad AutoScaling para Instancias en AWS de forma que la protección se genere de forma inmediata una vez creada la instancia
- La solución debe permitir desde la misma consola la integración por medio de conectores de Azure Microsoft para la gestión de plataformas y protección de forma automatizada que permita identificar cuando una instancia esta encendida, apagada o sin gestión
- La solución debe permitir el aprovisionamiento automatico de deployment scripts para instancias creadas sin protección en sus aplicaciones y sistema operativo
- La solución debe permitir adaptarse a la capacidad AutoScaling para Instancias en AWS,

AZURE de forma que la protección se genere de forma inmediata una vez creada la instancia.
- La solución de protección de servidores debe contar en caso de ser requerida una consola en nube para la protección de instancias de Microsoft Azure y Amazon AWS desplegadas por Marketplace
- La solución debe contar con conectores de cloud para al menos: VCloud, AWS y Azure y que estos se administren desde la misma consola que el resto de módulos.
- Para ambientes en cloud como Microsoft Azure y Amazon AWS la solución deberá permitir distintas modalidades de pago, como mínimo: licencia anual o pago por uso

10.10 Reportes

- Debe tener un reporte con el resumen gráfico de vulnerabilidades agrupadas por severidad encontradas por aplicación web.
- Debe tener un reporte con el Gráfico de tendencia en el tiempo (con la información de todos los escaneos realizados) de vulnerabilidades encontradas por aplicación web.
- Debe tener un reporte con la lista de vulnerabilidades clasificadas por severidad
- Debe tener un reporte con la lista de vulnerabilidades clasificadas por tipo de plataforma
- Debe tener un reporte con el Detalle de cada una de las vulnerabilidades encontradas, dónde se incluya la severidad, la descripción de la vulnerabilidad, CVSS score, la fecha en la que fue encontrada por primera vez en la aplicación web y la solución para corregir el hueco de seguridad.
- La solución debe permitir generar informes de Antimalware
- La solución debe permitir generar un informe de monitoreo de la integridad
- La solución debe permitir generar un reporte de reputación web
- La solución debe permitir generar un reporte de firewall
- La solución debe permitir generar un reporte de la inspección de logs

10.11 Postura de seguridad en la nube

- Integración con el proveedor de nube sin generar alguna disrupción en la implementación u operación de servicios existentes o futuras de la organización y deberá monitorear al menos 60 de los servicios en las diferentes Nubes (AWS, Azure, GCP).
- El monitoreo debe cubrir al menos las siguientes áreas: costos, rendimiento, operación de la nube, fiabilidad de los servicios, seguridad y sostenibilidad.
- La integración debe permitir la parametrización de servicios que se desean monitorear mediante una modificación sencilla de las políticas de la nube.
- Deberá proporcionar visibilidad de múltiples cuentas, de diferentes nubes desde una sola consola, con la capacidad de personalizar las reglas de monitoreo en cada una de ellas.
- Tener la capacidad de personalizar reglas de alertamiento, deben considerar al menos:
- Región o zona de disponibilidad
- Listas blancas y negras de sistemas operativos
- Tamaño de las instancias
- Puertos de comunicación permitidos ya sea de entrada o salida.
- Nomenclatura permitida en la creación de los recursos.
- Deberá monitorear los diferentes servicios de la nube publica y alertar cuando alguno se

encuentra fuera de las mejores prácticas o con alguna configuración que pueda ocasionar un riesgo operativo o de seguridad.

- Permitir la generación de reportes calendarizados, automáticos o bajo demanda de los resultados del análisis de la infraestructura de las diferentes nubes y deberán poderse extraer al menos por: tipo de servicio, región o zona de disponibilidad, tags asociados, recurso o activo especifico, nivel de riesgo, proveedor de nube, standard o Framework de seguridad (ISO27001, SOC2, NIST, GDPR, CIS, Well Architected Framework entre otros)
- Monitorear en tiempo real la creación, eliminación y modificación de servicios dentro de la nube pública.
- Alertar en tiempo real mediante correo electrónico, integración nativa con la nube o terceros cuando exista un riesgo de seguridad, cumplimiento normativo o performance.
- Para cada uno de las desviaciones o riesgos detectados deberá proporcionar una base de conocimiento accesible directamente desde la consola que pueda ser consultada en cualquier momento para entender la razón del riesgo y como se puede mitigar, ya sea desde la línea de comandos o mediante la interfaz gráfica.
- Deberá permitir la remediación automática de las malas configuraciones, esto mediante la integración de servicios nativos de la propia nube.
- Permitir el uso de etiquetas propias de la plataforma que brinda el servicio, adicional a las que proporciona el proveedor de nube.
- Contar con una API publica para todos los procesos de automatización que se requieran
- Proporcionar un análisis de la infraestructura como código, antes de que ésta sea desplegada en la nube pública, ya sea de forma manual o de forma automática mediante la integración por API o integración directamente en los procesos de CI/CD
- La solución debe funcionar en el sistema de análisis de metadatos vía API, sin acceso a lectura o escritura de datos
- Debería permitir administrar múltiples cuentas de múltiples servicios en la nube desde la misma consola
- Debe integrarse con al menos las siguientes herramientas: ServiceNow, JIRA, PagerDuty, Microsoft Teams y Slack
- El fabricante debe tener una base de conocimiento con un catálogo de reglas y controles de infraestructura
- Las reglas de la base de conocimiento deben cubrir al menos AWS, Microsoft Azure y GCP
- Debe tener reglas de corrección/remediación, con guías por Interfaz grafica y línea de comando
- Debe monitorear actividades y cambios en la configuración de la cuenta en tiempo real
- La solución debe admitir la creación de reglas personalizadas
- El tablero debe mostrar un resumen de las cuentas integrado en la consola, informando el porcentaje de cumplimiento de las cuentas
- La solución debe informar cuántos controles se realizaron y el resultado, si el control cumple o no
- Al hacer clic para ver todas las reglas, debería ser posible verlas por regla, por función (servicio) y por marco/patrón
- Debe ser posible filtrar las reglas al menos por: servicio, tipo de recurso, categorías, marcos/estándares, regiones de servicio, reglas, nivel de riesgo, estado, por fecha de

verificación

- Los usuarios con permisos administrativos deben poder suprimir u ocultar las reglas identificadas
- Los resultados del escaneo deben estar disponibles en la consola, mostrando el nivel de riesgo de incumplimiento, teniendo al menos niveles bajo, medio, alto y muy alto
- El tablero debe mostrar el nivel de cumplimiento por cuenta, informando este nivel por categorías, teniendo como mínimo el cumplimiento general de la cuenta, la seguridad, la optimización de costos, la excelencia operativa, la confiabilidad y la eficiencia en el desempeño
- La consola debe mostrar un resumen de las últimas actividades realizadas por los usuarios y los últimos eventos detectados. Para ambos, debe haber un enlace o botón para ver los registros completos
- Para cada uno de los niveles de cumplimiento mostrados, la solución debe proporcionar un botón o enlace para detallar las detecciones
- La solución debe mostrar la evolución del cumplimiento de los últimos 6 meses por cada cuenta, por categoría
- La consola debe informarle sobre las fallas más críticas, así como un enlace a la base de conocimientos que debe explicar cómo solucionar la falla
- Debería ser posible filtrar los datos del tablero por cuenta integrada, mostrando información perteneciente a todas las cuentas o una cuenta seleccionada
- La solución debe permitir el envío de notificaciones por correo electrónico y por teléfono
- Deberá integrarse con la plataforma de ciberseguridad para ayudar al descubrimiento de la superficie de ataque permitiendo visualizar los activos que se tengan dentro de AWS, Microsoft Azure y GCP.
- Dentro de la plataforma se deberá identificar la ubicación geográfica de los activos en la nube y evaluar si hay algún activo en la nube inesperado en una región específica.
- La solución deberá poder ordenar de forma rápida los activos en la nube por puntaje o calificación de riesgo.
- La solución deberá poder ordenar de forma rápida los activos en la nube por puntaje o calificación de riesgo.

Alcance del servicio

El servicio debe y productos requeridos que deben brindar capacidad de protección y respuesta total en la infraestructura tecnológica de SAE
Capacidad de monitoreo y protección en todos los tipos de dispositivos sin importar su tecnología y ubicación
Protección que garantica los principios de confidencialidad, integridad y disponibilidad de la información de la entidad.
El servicio debe contar con disponibilidad 24/7 en la atención de fallos, preguntas, modificaciones, actualizaciones que requiera la plataforma o por cambios en normatividad interna o externa.

Listado de elementos del Servicio

- Suite de soluciones de seguridad informática que incluya:
  - Protección total a Endpoints virtuales y físicos
  - XDR
  - DLP
  - Cifrado
  - Protección total de correo electrónico y mensajería
  - Protección total en la nube
- Software para análisis de postura de seguridad organizacional onpremise y nube
- Protección avanzada para servidores tipo workload security
- Licencias o créditos para la integración con XDR cloud

Requisito	Descripción
El servicio incluye soporte, mantenimiento, administración y capacitación.	El proveedor debe ofrecer un servicio de soporte y mantenimiento sobre la herramienta entregada 7x24 con mínimo (1) revisión anual del estado de la tecnología El proveedor debe proporcionar resolución de dudas por diferentes canales sobre dudas de los compromisos detectados, El proveedor se encargará de capacitar al personal seleccionado por la organización. El proveedor debe ofrecer co-administración dos (2) días a la semana mínimo de dos (2) horas para grupo delegado de cuatro (4) personas en administración de la tecnología
Implementación del servicio	El **OFERENTE** se encargará de entregar un plan de trabajo guía para la implementación y una memoria técnica al finalizar la implementación del servicio. La implementación debe ser realizada directamente por el **Fabricante** de la tecnología

Volúmenes Estimados a Contratar

PRODUCTO	CANTIDAD	PERIODO (Meses)
SUITE DE SOLUCIONES DE SEGURIDAD INFORMATICA QUE INCLUYA (ENPOINT PROTECTION, XDR, DLP, CIFRADO, PROTECCION DE CORREO ELECTRONICO, PROTECCION PARA APLICACIONES EN LA NUBE)	800	12
SOFTWARE PARA ANALISIS DE POSTURA DE SEGURIDAD EN LA NUBE	4	12
PROTECCION AVANZADA PARA SERVIDORES TIPO WORKLOAD SECURITY	176	12
LICENCIAS O CREDITOS PARA INTEGRACION CON XDR CLOUD	18400	12

Acuerdos de Nivel de Servicio (ANS)

Disponibilidad

Descripción	Unidad	Requisito	Medición	Penalidad
Disponibilidad de los servicios	Porcentaje de Disponibilidad	99.99%	**SAE** puede solicitar al OFERENTE la estadística de disponibilidad en el momento que lo desee.	1.0 % del valor total en la factura
Disponibilidad de portal de gestión	Porcentaje de disponibilidad	99.99%	**SAE** puede solicitar al OFERENTE la estadística de disponibilidad en el momento que lo desee.	1.0 % del valor total en la factura
Informe	Informe	Un informe mensual	Debe ser entregado y presentado a la Oficina de Gestión de la Información OGI de SAE, un informe del servicio prestado antes de primeros cinco días hábiles calendario	1.0 % del valor total en la factura
Atención a Incidentes	Horas	Crítico > 1 Alto > 2 Medio > 4 Bajo > 24	**SAE** puede solicitar al OFERENTE la estadística de atención a incidentes reportados por la tecnología	1.0 % del valor total en la factura

ANS para soporte

Nivel de criticidad	Descripción	Tiempo máximo de atención	Tiempo máximo de solución	Disponibilidad de atención	Penalidad
Nivel 3 – Criticidad baja	Refiere incidentes que no afectan la disponibilidad de los servicios ofrecidos pero que requieren ser atendidos dentro del esquema de soporte técnico prestado.	4 horas	24 horas	5x8	0.5% del valor total en la factura
Nivel 2 – Criticidad media	Refiere incidentes que afectan la disponibilidad de alguno de los servicios o componentes de este.	1 hora	4 horas	5x8	1.0 % del valor total en la factura
Nivel 1 – Criticidad Alta	Refiere incidentes que afectan por completo la Disponibilidad del servicio.	15 minutos	2 horas	7x24	1.5% del valor total en la factura