La Entidad requiere una solución integral de ciberseguridad que permita prevenir, detectar, investigar, contener y remediar amenazas conocidas, desconocidas y de día cero en estaciones de trabajo, servidores, correo electrónico, datos y cargas de trabajo físicas, virtuales y en la nube. La solución deberá ofrecer administración centralizada, inteligencia de amenazas, automatización de respuesta, protección de información e interoperabilidad con la infraestructura tecnológica institucional.

OBJETO A CONTRATAR: Contratar la renovación del licenciamiento, implementación, configuración, soporte y actualización de la solución integral de ciberseguridad para la protección, detección, investigación y respuesta frente a amenazas en estaciones de trabajo, servidores, correo electrónico, datos y cargas de trabajo de la Entidad, con capacidades de antimalware, EDR/XDR, DLP, parchado virtual e integración con la infraestructura tecnológica institucional.

REQUERIMIENTOS TÉCNICOS MÍNIMOS:

La solución de antimalware deberá cumplir con mínimo los siguientes requerimientos:
1. Análisis de comportamiento dinámico detectando patrones anómalos en archivos, aplicaciones y tráfico de red antes de que se conviertan en amenazas activas.
2. Prevención contra exploits, malware conocido y desconocido, virus, troyanos, gusanos, rootkits, Spyware/Grayware, Ransomware, CVE exploit, Fileless como PowerShell malicioso o macros malintencionadas, Cryptojacking, APT, wipers, entre otros.
3. Identificación, análisis y bloqueo de archivos maliciosos, basado en el tipo de archivo real y verdadero, no solo en la extensión de archivo.
4. Identificación y bloqueo de archivos basados en contenido ejecutable incrustado o script.
5. Identificación análisis y bloqueo de procesos y archivos asociados a ataques de Ransomware
6. Uso de modelos predictivos de aprendizaje automático y análisis de comportamiento para identificar el comportamiento anómalo sobre archivos y procesos que buscan modificar/afectar el sistema o generar tareas de persistencia
7. Protección en tiempo de ejecución para detectar y bloquear el comportamiento de cifrado malicioso en tiempo real, incluso en variantes de ransomware desconocidas.
8. Bloqueo de ransomware multi-etapa detectando cadenas de ataque que involucran múltiples técnicas, como el cifrado selectivo combinado con exfiltración de datos.
9. Restauración de archivos cifrados usando copias de seguridad automáticas (de archivos críticos) generadas en tiempo real para restaurar sistemas afectados.
10. Configuración independiente para escaneo y protección frente amenazas en Tiempo Real, escaneo Manual, escaneo Programado o escaneo enviado por el administrador.

11. Definición manual o recomendada de acciones sobre la identificación de amenazas, como enviar a cuarentena, eliminar, bloquear la acción o generar log
12. Uso de servicios de remediación y limpieza automática definidos y soportados por el fabricante de la solución ofertada
13. Configuración de excepciones por directory path, Files o Extensions
14. Protección frente amenazas incluso si el agente pierde la conexión a la consola de gestión
15. Protección contra intentos de desinstalación o eliminación de procesos del agente de protección.
16. Identificación sobre archivos comprimidos o que intentan generar ataques conocidos como bombas zip
17. Uso de servicio global de inteligencia de amenazas para la actualización en tiempo real sobre nuevas amenazas o factores de riesgo a nivel global.
18. Capacidad de Web Reputation sobre la navegación de los usuarios
19. Configuración de uso de CPU sobre los dispositivos
20. Capacidad de correlación automática de datos entre múltiples capas integrando información de endpoints, servidores, red, correo electrónico, servidores y cargas de trabajo en la nube para ofrecer una visión centralizada y holística de las amenazas.
21. Uso de modelos de correlación incluidos y soportados por la solución ofertada, con posibilidad de generar modelos de correlación personalizados.
22. capacidad de verificar el perfil de ejecución/análisis de causa raíz (perfil de ejecución y análisis de causa raíz) para ver las acciones que una amenaza llevó a cabo en el endpoint.
23. Capacidad de aislar un dispositivo si es identificado como el "Paciente cero" que propaga la amenaza
24. Conexión por shell remota al dispositivo para un análisis adicional sobre la amenaza o afectación en el sistema
25. Posibilidad de generar casos asignados a diferentes analistas que generan los procesos de investigación
26. Línea de tiempo de cada evento relacionado con la amenaza que fue identificada y correlacionada
27. Posibilidad de documentar cada investigación realizada por el analista directamente en la plataforma de la solución ofertada
28. Posibilidad de modificar el estado del evento o correlación generada a un estado en proceso, cerrado, falso positivo, verdadero positivo, entre otros
29. Descripción detallada de correlación generada incluyendo, línea de tiempo, mapeo directo con el framework de MITRE ATT&CK, comandos usados, rutas de ejecución, archivos o elementos usados, conexiones de red, entre otros
30. Posibilidad de tomar acciones de remediación automática o manual a través de Playbook. Acciones como aislar el dispositivo, iniciar un shell remoto, generar una búsqueda adicional con un criterio especifico, ejecutar script personalizados, ejecutar un OSquery, ver el detalle del dispositivo o elemento identificado, entre otros.
31. Posibilidad de ver activos adicionales que están relacionados con el dispositivo que fue identificado con un evento anómalo

32. Uso asistente virtual por medio de IA generativa que permite ayudar a los equipos de seguridad a interpretar de mejor forma cada amenaza identificada además de recomendaciones que se pueden ejecutar
33. Sección específica para el análisis de técnicas tácticas y procedimientos basados en MITRE ATT&CK
La solución debe contar con una consola centralizada que cumpla con mínimo las siguientes características:
34. Capacidad retención mínima para log de seguridad de 180 días, telemetría por 30 días y eventos correlacionados por 180 días
35. Funcionalidad para crear roles granulares por sección para la asignación a usuarios específicos.
36. Integración con directorios y servicios de identidad locales o en la nube mediante SAML 2.0, OIDC, OAuth 2.0, LDAP o LDAPS para uso de autenticación centralizada a la plataforma de gestión usando SAML
37. Uso de IA para generar recomendaciones de configuración y acciones de remediación.
38. Posibilidad de restringir el acceso a la plataforma de gestión a direcciones de IP específicas
39. Gestión centralizada para diferentes tenant o compañías del mismo grupo en una única consola de administración
40. Integración con soluciones de terceros como:
• Seguridad de red: capacidad de integración con los controles de red de la Entidad mediante Syslog, CEF, APIs documentadas, STIX/TAXII u otros mecanismos estándar.
• SIEM: capacidad de integración mediante Syslog, CEF, LEEF, API documentada u otros formatos estándar, incluyendo la plataforma institucional.
• SOAR: capacidad de integración mediante API documentada, webhooks, conectores estándar o mecanismos equivalentes.
• Gestión de servicios de TI: capacidad de integración mediante API documentada, correo, webhooks o conectores estándar.
• Inteligencia de amenazas: compatibilidad con STIX/TAXII, MISP u otros formatos y fuentes interoperables.
• Simulación de brechas y ataques: integración mediante API documentada o conectores compatibles con las herramientas disponibles en la Entidad.
a. Gestión de identidades y accesos: integración con servicios de directorio e identidad locales o en la nube mediante LDAP/LDAPS, SAML 2.0, OIDC, OAuth 2.0 o API documentada, permitiendo correlacionar el comportamiento de los usuarios con la telemetría de seguridad.
b. Gestión de vulnerabilidades: capacidad de integración mediante API documentada, archivos estructurados o conectores con herramientas de gestión de vulnerabilidades reconocidas.
41. API disponible para ejecutar diferentes acciones de administración, reportes, configuración, IoC, Integración con terceros, entre otros
42. El esquema de licenciamiento deberá ser flexible y permitir habilitar las capacidades requeridas, mediante suscripción, licencias por activo, consumo, créditos u otra modalidad equivalente, indicando claramente métricas, límites y costos.

43. Posibilidad de aplicar controles de seguridad a los agentes de protección para evitar su desinstalación o eliminación de procesos activos
44. Integración con soluciónes de SIEM y SOAR para el envío de logs
Protección contra amenazas en los servidores:
Requerimientos técnicos Generales
Licenciamiento de la protección anti-malware para mínimo 300 servidores.
La solución debe brindar protección para mínimo los siguientes sistemas operativos:
• Windows Server, en versiones vigentes o heredadas que la Entidad mantenga en operación y que sean declaradas compatibles por el fabricante.
• Linux, para la versión distribuciones empresariales de Linux en versiones soportadas o heredadas declaradas compatibles por el fabricante.
• Linux para la versión distribuciones comunitarias de Linux en versiones soportadas o heredadas declaradas compatibles por el fabricante.
• Linux en sus diferentes distribuciones.
• Validar con Infraestructura las diferentes distribuciones.
• La solución debe detectar, identificar y contener malware.
La solución debe realizar protección en tiempo real contra malware.
1. Posibilidad de almacenamiento de eventos correlacionados por 180 días
2. Sección específica para la creación de consultas personalizadas enfocadas en threat hunting sobre la telemetría recopilada por los agentes, usuarios, correo y servidores
3. Posibilidad de construir, guardar y reutilizar búsquedas para Threat Hunting
4. Posibilidad de generar consultas con atributos de búsqueda, operadores y valores especificados en una única consulta de búsqueda.
5. Permitir guardar búsquedas para encontrar nueva data relacionada a los mismos criterios de búsqueda
6. Resultados de búsquedas con posibilidad de exportar a CSV o JSON
7. Posibilidad de notificar o alertar un match con una búsqueda o filtro personalizado, en un periodo de tiempo
8. Escaneo de recomendaciones y asignación de reglas automáticamente, identificando y bloqueando únicamente el tráfico malicioso.
9. Asignación de reglas por política genera par aun grupo de dispositivos o por host independiente
10. Posibilidad de generar escaneos de recomendaciones y reportes de reglas de vulnerabilidades aplicadas y recomendadas para aplicar, además de reglas disponibles según la vulnerabilidad
11. La solución deberá disponer oportunamente de reglas de parchado virtual para vulnerabilidades críticas publicadas por los fabricantes de los sistemas operativos y aplicaciones soportados.
12. Protección de intentos de explotación de vulnerabilidades sobre el tráfico de red del dispositivo
13. Despliegue de reglas de Virtual Patch sin necesidad de reinicio del dispositivo
14. Soporte para proteger vulnerabilidades sobre sistemas legados como sistemas operativos vigentes y heredados inventariados por la Entidad, o distribuciones de Linux

15. Inspección profunda de paquetes bidireccionalmente para analizar y prevenir ataques a vulnerabilidades en las aplicaciones instaladas en cada servidor, incluidas vulnerabilidades conocidas y de día cero
16. Capacidad de aplicar reglas con acciones de bloqueo y monitoreo, además, poder capturar el stream o la cadena de caracteres de la ejecución de un ataque que permita el análisis del evento y alertamiento.
17. Protección adicional frente ataques de tipo SQL Injection, Cross-Site Scripting y otras vulnerabilidades de aplicaciones web
18. 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
19. Capacidad de crear reglas de Firewall que protege servidores físicos, y/o virtuales y/o en la nube administrados desde la misma plataforma, permitiendo sólo las comunicaciones requeridas entre ellos. Filtrado bidireccional ICMP, IGMP, GGP, TCP, PUP, UDP, IDP, ND, RAW, TCP+UDP, Direcciones MAC, Direcciones IP y Puertos TCP & UDP entre otros
20. Posibilidad 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.
21. Asignación de reglas por política general, por dispositivo o por interfaz
22. La solución deberá incluir un catálogo actualizado de reglas predefinidas de monitoreo de integridad para sistemas operativos y aplicaciones, además de permitir reglas personalizadas para detectar cambios no autorizados en rutas críticas.
23. Posibilidad de crear políticas personalizadas de File Integrity Monitoring para monitorear rutas críticas, archivos, o carpetas, definiendo la severidad, rutas o archivos a monitorear y excepciones de las mismas
24. Permite generar un monitoreo de integridad, en tiempo real, programado o a demanda
25. Permite la creación de una línea base del servidor, modificación o actualización de esta al crear o agregar nuevas rutas o archivos que serán monitoreadas
26. Cuenta con un escaneo de recomendaciones que permite aplicar reglas automáticamente acordes al sistema operativo o aplicaciones identificadas en el sistema, para File Integrity Monitoring y Log Inspection.
Protección DLP
Licenciamiento de la protección DLP para mínimo 2400 endpoints.
La solución debe tener un componente de prevención de fuga de información a nivel de Endpoint incluido en el mismo agente de protección antimalware.
La solución debe brindar protección DLP a nivel de datos o información con mínimo las siguientes funcionalidades:
• Monitoreo y protección a partir de diccionarios o palabras clave.
• Implementar políticas de detección y protección.
• Permitir la implementación de políticas para la protección de los archivos almacenados en los Endpoint de la Entidad.
• Detectar y prevenir intentos de copia o cifrar datos de manera no autorizada.

1. 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.
2. La solución debe permitir identificar o configurar los activos digitales que se desean proteger.
3. 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).
4. 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.
5. La solución debe permitir que la organización haga cumplir con las normas de privacidad establecidas.
6. 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.
7. La solución debe proporcionar identificadores de datos y/o plantillas para la creación de políticas.
8. 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.
9. La solución debe tener la capacidad de localizar activos digitales almacenados en portátiles, equipos de escritorio, y servidores.
10. La solución debe tener la capacidad de proporcionar filtros de protección para canales de red como FTP o HTTP, canales de aplicaciones o periféricos.
11. La solución debe tener la capacidad de detectar datos estructurados y no estructurados.
12. La solución debe mantener un monitoreo constante.
13. La solución debe proveer plantillas que permitan el cumplimiento de estándares como GLBA, HIPAA, PCI-DSS o PII.
14. La solución debe permitir la integración con servicio de directorio institucional y permitir la delegación de administración.
15. 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.
16. 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.
17. 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)
18. Las plantillas de identificación de activos digitales deben permitir combinar identificadores de datos (expresiones, atributos de archivos, huellas digitales, lista de palabras).

19. La solución debe permitir usar plantillas predefinidas por el fabricante, personalizarlas, crear plantillas, importar plantillas, exportar plantillas, y eliminar las plantillas.
20. La solución debe permitir implementar políticas independientes tanto para agentes fuera de la red corporativa como para agentes dentro de la red.
21. 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.
22. La solución debe permitir almacenar reportes y estos deben estar disponibles en formatos PDF, HTML, o Microsoft Excel.
23. La solución debe tener la capacidad de administrar los logs de manera que pueda eliminar los Logs que tengan un tiempo de más de 180 días, igualmente debe permitir la realización de una copia de seguridad y limpieza de los mismos de forma manual.
24. La solución debe permitir que las actualizaciones puedan ser implementadas en ambientes de pruebas y producción para validar el funcionamiento de estos.
25. La Solución debe tomar acción como mínimo en documentos y métodos de codificación, Gráficos, Archivos multimedia, Archivos comprimidos, Bases de datos, Hojas de cálculo, Archivos de presentaciones y diagramas, Archivos vinculados e incrustados, Archivos cifrados, cuando técnicamente sea posible.
dBase (.dbf), Microsoft Access (.mdb, .accdb), KIRI Database (.tbl), SAS System Data Set (.sas7bdat), Bitmap (.bmp), EPS (.eps), GIF (.gif), TIFF (.tif), JPEG (.jpg), PNG (.png), DICOM (.dcm), PostScript (.ps), AutoDesk (.dwg), AutoCAD (.dxf), SolidWorks (.abc, .slddrw, .sldprt, .sldasm), Siemens NX Unigraphics (.prt), CATIA (.CATDrawing, .CATPart, .CATProduct), Graphic Data System (.gds), Lotus Ami Pro (.sam), RTF (.rtf), Microsoft Word for Windows - Non-encrpyted (.doc, .dot, .docx, .dotx, .docm, .dotm), WordPerfect (.wp, .wpd), WordStar (.wsd), Microsoft Write (.wri), Adobe PDF - Non-encrypted (.pdf), HTML (.htm), XML (.xml), Xerox DocuWorks (.xdw, .xbd), Ichitaro (.jtd), Microsoft Wave (.wav), MIDI (.mid), AVI (.avi), MPEG (.mpeg), Apple QuickTime (.mov), Adobe Flash (.swf), Zipped File (.zip) PAK/ARC (.arc), compress (.Z), GZ (.gz), TAR (.tar), MIME (.eml), PGP Keyring (.pgp) Microsoft Outlook (.pst), RAR (.rar), LHA (.lzh), Microsoft Outlook Express (.dbx), ARJ (.arj), bzip2 (.bz2), Microsoft Compiled HTML Help (.chm), Microsoft Outlook (.msg) 7-Zip (.7z), Quattro (.qpw, .wb3, .wb2, .wb1, .wq1), Lotus 1-2-3 (.123, .wk1, .wk3, .wk4, .wke, .wks), Microsoft Excel - Non-encrypted (.xls, .xlw, .xlsx, .xltx, .xlsb, .xltm, .xlsm, .xlc, .xlam), Microsoft PowerPoint for Windows - Non-encrypted (.ppt, .pot, .pps, .pptx, .potx, .ppsx, .potm, .pptm, .ppsm), Microsoft Visio (.vdx, .vsd, .vss, .vst, .vsx, .vtx, .vdw), OLE (.ipt, .idw, .iam, .pqw, .msoffice), Encrypted compressed files (.rar, .zip), Encrypted documents (.accdb, .doc, .docx, .pdf, .ppt, .pptx, .wb1, .wb2, .wq1, .wpd, .xls, .xlsx)
26. La herramienta de análisis local debe tener la capacidad de adquirir huellas digitales para los archivos almacenados en el equipo.
27. 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.

28. La solución provee expresiones predefinidas para las direcciones de correo electrónico
29. La solución provee expresiones predefinidas para los números de cuentas de bancos internacionales (IBAN).
30. La solución provee expresiones predefinidas para códigos de identificación de negocio SWIFT BIC.
31. La solución deberá proveer 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.
32. La solución debe proveer una lista de palabras que pueden ser usadas en contextos efectivos, racistas o que incluyan elementos para causar daño (armas)
33. La solución deberá proveer una lista de palabras que puedan identificar comandos o instrucciones en lenguajes de programación como C#, C/C++, COBOL, Java, Perl y VB.
Protección XDR
Licenciamiento de la protección XDR para mínimo 300 servidores y 2400 endpoints
La solución debe permitir identificar, investigar y responder a amenazas avanzadas de manera automatizada.
La solución debe integrarse y correlacionarse con el SIEM institucional mediante Syslog, CEF, API documentada u otro mecanismo estándar disponible
La solución podrá utilizar uno o más agentes, siempre que estén integrados, sean administrados centralmente y no generen incompatibilidades, duplicidad innecesaria de consumo de recursos ni afectación significativa del desempeño.
La solución XDR deberá aprovechar la telemetría de los agentes de protección instalados o integrarse con ellos mediante mecanismos documentados. Si requiere componentes adicionales, el oferente deberá indicar su función, consumo de recursos y método de administración centralizada.
La solución de detección y respuesta debe permitir la correlación entre, endpoints y los servidores protegidos por la solución XDR o integrados mediante mecanismos documentados e interoperables
Integración con las plataformas de seguridad e infraestructura de la Entidad mediante estándares abiertos y mecanismos documentados, como Syslog, CEF, STIX/TAXII, SAML 2.0, OIDC, LDAP/LDAPS, API REST y webhooks. El oferente deberá indicar las integraciones nativas disponibles y el procedimiento para desarrollar o habilitar integraciones adicionales.
Integración con el servicio de directorio institucional para identificación de comportamiento maliciosos sobre los usuarios que alteren el nivel de riesgo por relación a una posible amenaza o brecha de datos
Capacidad de deshabilitar el usuario, forzarlo a un cierre de sesión y forzar el reseteo de la contraseña si es identificado con comportamiento malicioso
Protección completa contra Phishing, Spam, Graymail, Malware Avanzado con múltiples técnicas de protección, incluyendo análisis del remitente, de contenido e imágenes usando Machine Learning

Protección completa contra Phishing, Spam, Graymail, Malware Avanzado con múltiples técnicas de protección, incluyendo análisis del remitente, de contenido e imágenes usando Machine Learning	
La solución deberá incluir protección antispam para los servidores de correo Microsoft Exchange Server de la Entidad, con capacidad de inspeccionar y filtrar el correo electrónico interno entre buzones del mismo dominio, además del correo entrante y saliente.	
La protección deberá analizar mensajes, remitentes, encabezados, contenido, URL y archivos adjuntos, mediante técnicas de reputación, reglas, análisis de contenido, aprendizaje automático u otros mecanismos equivalentes, con el fin de detectar spam, phishing, suplantación, malware y mensajes no deseados.	
La solución deberá permitir aplicar políticas diferenciadas al flujo de correo interno, entrante y saliente, con acciones configurables como permitir, etiquetar, bloquear, rechazar, eliminar o enviar a cuarentena.	
La solución deberá integrarse con Microsoft Exchange Server mediante agentes de transporte, conectores, diario de correo, API, gateway interno u otro mecanismo oficialmente soportado. El oferente deberá describir la arquitectura propuesta y demostrar que el correo interno será efectivamente inspeccionado.	
Advanced Email Protection - 2300 cuentas de correo	
La solución deberá tener la capacidad para proteger correos entrante, saliente, internos, de la organización sobre la plataforma Google Workspace, O365, Exchange, entre otros	
La solución deberá proporcionar cuarentena administrable, listas de permitidos y bloqueados, excepciones, trazabilidad de mensajes, reportes y registros de auditoría para la protección antispam.	
La solución debe tener la capacidad de detección de correos internos que suplantan a usuarios de alto perfil (ejecutivos) o provienen de cuentas comprometidas.	
La solución deberá analizar el contenido de los correos internos, los cuales no salen a internet, con filtros antispam ajustables, con cuarentena de usuario final y nivel de confianza de spam.	
La solución deberá permitir aplicar controles contra suplantación de identidad y spoofing interno, incluyendo validaciones de remitente, dominio y autenticidad del mensaje cuando sean aplicables.	
Protección completa contra Phishing, Spam, Graymail, Malware Avanzado con múltiples técnicas de protección, incluyendo análisis del remitente, de contenido e imágenes usando Machine Learning	
Detectar y bloquear ransomware y otros tipos de malware de día cero que llegan por correo mediante machine learning previo a la ejecución, análisis de macro, detección de exploit y análisis dinámico en sandbox para archivos y URL	
La solución deberá permitir el despliegue mediante API documentada, integración con el flujo de correo o mecanismos equivalentes, indicando los cambios técnicos requeridos.	
La solución podrá ofrecerse en modalidad SaaS, local o híbrida, siempre que cumpla los requisitos de seguridad, disponibilidad, administración y protección de datos de la Entidad.	

Detectar malware avanzado y exploits en archivos PDF, Microsoft® Office y otros documentos a través de la lógica estática o heurística para detectar y examinar anomalías	
La solución debe contar con fuentes de inteligencia del fabricante que permita tener información sobre amenazas, para correlacionar registros de Internet, emails, archivos, dominios y muchas otras fuentes de amenazas para identificar las infraestructuras del atacante antes de que se ejecuten	
La solución deberá tener Sandbox para análisis de amenazas desconocidas y ataques de día cero.	
La solución deberá tener escaneo de URL en el cuerpo de los correos y en los archivos adjuntos.	
La solución deberá ofrecer protección avanzada para los servicios institucionales de almacenamiento y colaboración en la nube.	
La solución deberá admitir conectores o API documentadas para servicios de almacenamiento y colaboración en la nube utilizados por la Entidad.	
La solución deberá tener DLP y plantillas customizables 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 aplicar capacidades DLP a los servicios de almacenamiento y colaboración en la nube integrados, detectando y reportando incumplimientos de políticas.	
La solución no deberá exceder 1 minuto de latencia.	
La solución deberá ofrecer disponibilidad del servicio superior a >99%.	
Integración para autenticación de administradores con servicios de identidad locales o en la nube mediante SAML 2.0, OIDC u otro estándar equivalente, con soporte de autenticación multifactor.	
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 proteccion avanzada contra ataques de BEC (Business Email Compromise) con el análisis de los mensajes y usando tecnicas de aprendizaje de estilos de escritura.	
La solución debe tener la capacidad de detectar ataques dirigidos mediante explotacion de archivos.	
La solución debe tener la capacidad de realizar un análisis avanzado de los archivos usando Machine Learning, para identificar amenazas que aun no han sido reportadas, pero que pueden generar una afectacion sobre los datos o el sistema que esta utilizando el usuario.	
La solución debe tener la capacidad de brindar proteccion contra ataques avanzados como Business Email Compromise (BEC), Ransomware, Phishing avanzado	
La solución debe tener la capacidad de tomar un accion 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 un accion 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 deberá permitir aplicar acciones sobre archivos almacenados en servicios de colaboración en la nube que sean identificados como maliciosos, sospechosos o contrarios a las políticas, incluyendo permitir, bloquear, eliminar, poner en cuarentena y notificar al usuario.	
La solución debe tener la capacidad de notificar al usuario cuando algun correo que iba dirigido a el tuvo alguna accion reactiva, basado en las reglas configuradas, dicha notificacion debe indicarle que accion se tomo sobre el correo que iba dirigido a el y la razon de esta.	
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 Prevencion de filtracion de datos de la organización.	
Debe permitir entender la historia del ataque con una representación visual e interactiva de los eventos correlacionados.	
La solución debe permitir realizar un escaneo manual en modo de evaluacion para permitir a los administradores verificar las reglas que seran aplicadas para proteger la plataforma de correo y colaboración en la nube de la Entidad sin tomar ninguna accion sobre dichos correos o archivos.	
Envío de registros al SIEM mediante Syslog, CEF, API documentada u otro mecanismo estándar e interoperable.	
Creación de usuarios y roles personalizados con permisos granulares en la consola de administración	
Debe permitir la creación de reportes programados y por demanda de las detecciones que se tienen	
Debe contar con un Dashboard permitiendo ver la información relevante de amenazas identificadas	

La solución debe acreditar capacidades de seguridad de correo mediante evaluaciones independientes, certificaciones reconocidas o informes técnicos verificables	
La solución deberá ofrecer mecanismos de autenticación de multiple factor (MFA) para usuarios administradores.	