CONSULTORIA TECNICA Y
SERVICIOS DE INGENIERIA
NIT 800127892.1

36 AÑOS
Hardware & Software Gold Reseller
Centro Autorizado de Servicio
Antivirus Authorized Reseller

Tunja, agosto 25 de 2026 No 202608254

Señores
MUNICIPIO DE SOGAMOSO
Oficina de Tecnologías de la Información y las Comunicaciones – TIC
Sogamoso – Boyacá

Asunto: Renovación del licenciamiento de protección antivirus ESET PROTECT Advanced.

Presentación

En atención a la solicitud presentada por el **Municipio de Sogamoso**, nos permitimos presentar la propuesta para la **renovación de quinientas (500) licencias ESET PROTECT Advanced**, solución de ciberseguridad empresarial destinada a la protección de estaciones de trabajo y servidores de la entidad.
La solicitud del Municipio contempla la renovación del licenciamiento de protección antivirus **ESET Endpoint Advanced**, para una cobertura de **500 licencias**, con alternativas de vigencia de uno (1), dos (2) y tres (3) años.
La presente propuesta tiene como propósito garantizar la continuidad de la protección de los activos tecnológicos del Municipio, manteniendo vigente la solución ESET y sus capacidades de prevención, detección y respuesta frente a las amenazas informáticas actuales.
La renovación permite, además, preservar la inversión realizada en la plataforma y mantener una administración centralizada de la seguridad, evitando procesos innecesarios de migración hacia una solución diferente.

♡ Renovación de ESET PROTECT Advanced

La presente oferta corresponde a la renovación del licenciamiento **ESET PROTECT Advanced**, solución empresarial diseñada para proporcionar protección multicapa de los equipos institucionales frente a malware, ransomware, amenazas avanzadas y otras formas de código malicioso.
La plataforma integra tecnologías de seguridad orientadas a prevenir, detectar y responder frente a las amenazas informáticas, administradas mediante una consola centralizada que facilita la gestión de los dispositivos protegidos.
La solución permite proteger:

- Equipos de escritorio.
- Computadores portátiles.
- Servidores compatibles.
- Dispositivos móviles compatibles.

Todo ello mediante una plataforma de administración centralizada que facilita al personal de tecnología el control de las políticas de seguridad, la supervisión de los equipos y la gestión de los eventos de seguridad.

🔒 ¿Por qué renovar ESET PROTECT Advanced?

La seguridad informática constituye un proceso permanente de actualización y mejora continua.

La renovación del licenciamiento permite que el Municipio continúe contando con:

✓ **Actualizaciones permanentes** de los mecanismos de protección y detección.

✓ **Inteligencia global de amenazas** desarrollada por los laboratorios de ESET.

✓ **Protección frente a ransomware** y otras amenazas avanzadas.

✓ **Actualización permanente de firmas, algoritmos y tecnologías de detección.**

✓ **Protección frente a amenazas emergentes**, incluyendo técnicas de evasión y ataques dirigidos.

✓ **Administración centralizada** de la plataforma de seguridad.

✓ **Continuidad del servicio de protección** para los equipos incluidos en el licenciamiento.

✓ **Soporte y actualizaciones** asociados al período de vigencia contratado.

La renovación permite mantener activa la infraestructura de seguridad sin necesidad de sustituir la solución actualmente utilizada por el Municipio.

🚀 Capacidades de ESET PROTECT Advanced

ESET PROTECT Advanced integra diferentes tecnologías especializadas para proteger los principales vectores de ataque utilizados actualmente por los ciberdelincuentes.

Entre sus principales capacidades se destacan:

🖥 Protección avanzada para Endpoints

- Antivirus y antimalware multicapa.
- Protección contra ransomware.
- Protección contra ataques basados en comportamiento.
- Tecnología de Machine Learning.
- Protección frente a exploits.
- Protección contra ataques de red.
- Control web.
- Control de dispositivos.
- Detección y bloqueo de amenazas conocidas y emergentes.

Estas tecnologías permiten establecer diferentes capas de protección que actúan durante las distintas etapas de un posible ataque.

🗄 Protección para servidores

La solución permite extender la protección a servidores compatibles, contribuyendo a preservar la integridad de la información institucional y la continuidad de los servicios tecnológicos.
La protección de servidores constituye un componente fundamental dentro de una estrategia integral de seguridad, debido a que estos equipos concentran información y servicios críticos para la operación de las entidades.

☁️ Protección avanzada en la nube

ESET PROTECT Advanced incorpora capacidades de análisis y detección apoyadas en servicios en la nube, permitiendo analizar archivos y comportamientos sospechosos y mejorar la capacidad de respuesta frente a amenazas desconocidas.
Esta arquitectura permite complementar las tecnologías tradicionales de antivirus con mecanismos avanzados de análisis y detección.

🔍 Detección de amenazas avanzadas

La plataforma utiliza diferentes mecanismos de análisis para identificar comportamientos potencialmente maliciosos, incluyendo tecnologías de:

- Machine Learning.
- Análisis de comportamiento.
- Análisis de reputación.
- Detección basada en firmas.
- Protección contra exploits.
- Análisis avanzado de amenazas.

La combinación de estas tecnologías permite incrementar la capacidad de detección frente a amenazas conocidas y nuevas variantes de malware.

📱 Protección de dispositivos móviles

La plataforma permite complementar la estrategia de seguridad mediante capacidades de protección para dispositivos móviles compatibles, contribuyendo a ampliar el alcance de la seguridad institucional.

⭐ Principales diferenciadores de ESET

✅ Protección multicapa

ESET combina diferentes tecnologías de detección y prevención en una arquitectura multicapa, evitando depender exclusivamente de una única técnica de identificación de amenazas.

⚡ Bajo impacto sobre el rendimiento

ESET es reconocido por mantener un consumo eficiente de los recursos del sistema, permitiendo proporcionar protección de seguridad sin afectar significativamente el desempeño de los equipos de los usuarios.

🌎 Inteligencia global de amenazas

Los laboratorios de ESET analizan permanentemente eventos y muestras de malware provenientes de diferentes regiones del mundo, permitiendo actualizar continuamente los mecanismos de protección frente a nuevas amenazas.

📈 **Administración centralizada**

La infraestructura protegida puede administrarse desde una consola centralizada, facilitando:

- Inventario de dispositivos.
- Administración de políticas.
- Monitoreo.
- Gestión de alertas.
- Visualización de eventos.
- Generación de reportes.
- Administración de incidentes.

La administración centralizada permite simplificar las actividades del personal encargado de la seguridad informática y disponer de una visión consolidada del estado de protección de los equipos.

🤝 **Beneficios específicos para el Municipio de Sogamoso**

La presente propuesta corresponde a la **renovación de la solución de seguridad actualmente utilizada por el Municipio**, lo cual representa importantes ventajas técnicas y operativas.

Entre ellas:

- **Continuidad del servicio** de protección de los equipos.
- **Conservación de las políticas y configuraciones** actualmente implementadas, en la medida en que sean compatibles con la renovación.
- **Continuidad de la administración centralizada**.
- **Protección permanente** frente a malware, ransomware y amenazas avanzadas.
- **Actualización de las tecnologías de detección y protección** durante la vigencia contratada.
- **No requiere migrar hacia una plataforma de seguridad diferente.**
- **Aprovechamiento de la inversión realizada** previamente por el Municipio.
- **Reducción del riesgo operativo** asociado al vencimiento del licenciamiento.
- **Acompañamiento técnico especializado** por parte de COTEC S.A.S.

La renovación permite al Municipio continuar utilizando una solución empresarial de seguridad conocida por su personal de tecnología, reduciendo los impactos operativos que implicaría la adopción de una plataforma diferente.

Capacidad técnica y soporte especializado

La presente propuesta no comprende únicamente la renovación del licenciamiento ESET PROTECT Advanced. **COTEC S.A.S. garantiza adicionalmente la disponibilidad de capacidad técnica especializada para brindar acompañamiento y soporte durante la vigencia del licenciamiento.**

Como parte de sus condiciones de operación y soporte, **COTEC S.A.S. dispone dentro de su nómina de personal profesional certificado por el fabricante ESET para los productos y soluciones de seguridad ofrecidos**, con experiencia y vinculación laboral con la compañía superior a seis (6) meses.

Esta condición permite garantizar que el Municipio de Sogamoso no solamente adquiera el derecho de uso y actualización del licenciamiento, sino que cuente con el **respaldo técnico de personal con conocimiento especializado de la solución y certificación del fabricante**.

La condición de vinculación y permanencia del profesional podrá ser **acreditada documentalmente mediante las correspondientes planillas de seguridad social y aportes parafiscales**, correspondientes al período exigible, junto con la certificación de competencia expedida por el fabricante.

De esta manera, COTEC S.A.S. ofrece un esquema integral compuesto por:

✓ **Licenciamiento oficial ESET PROTECT Advanced.**
✓ **Actualizaciones y derecho de uso durante la vigencia contratada.**
✓ **Administración y acompañamiento técnico especializado.**
✓ **Personal profesional certificado por el fabricante.**
✓ **Soporte de primer nivel por parte de COTEC S.A.S.**
✓ **Escalamiento al fabricante cuando la naturaleza del incidente lo requiera.**
✓ **Acompañamiento durante la vigencia del licenciamiento.**

La disponibilidad de personal certificado y vinculado directamente a COTEC constituye un elemento fundamental para garantizar la **continuidad operativa, atención de incidentes y adecuado aprovechamiento de la plataforma ESET**, diferenciando la presente propuesta de una simple operación de suministro o renovación de licencias.

Acreditación documental

Para efectos de acreditar esta capacidad, COTEC S.A.S. podrá aportar, cuando sea requerido por el Municipio y de acuerdo con las condiciones de presentación de la oferta, los documentos que permitan verificar:

- Certificación del profesional expedida por **ESET**, correspondiente a la solución ofrecida.
- Documentación que acredite la vinculación del profesional con COTEC S.A.S.

- **Planillas de seguridad social y aportes parafiscales** que permitan demostrar la vinculación durante el período correspondiente.
- Los demás documentos que resulten pertinentes para acreditar la idoneidad y disponibilidad del personal técnico.

Este esquema garantiza que detrás de la renovación del licenciamiento existe una **estructura técnica real para atender al Municipio**, respaldada por personal certificado y directamente vinculado con COTEC S.A.S.

🛠 Servicios incluidos

Como parte de la presente propuesta, **COTEC S.A.S.** ofrece acompañamiento durante el proceso de renovación, incluyendo:

- Acompañamiento durante la activación del nuevo período de licenciamiento.
- Validación del estado general de la plataforma.
- Soporte técnico especializado.
- Escalamiento directo con el fabricante cuando sea requerido.
- Orientación al personal de tecnología.
- Recomendaciones de mejores prácticas.
- Transferencia de conocimiento.
- Atención remota y presencial cuando sea requerida, de acuerdo con las condiciones del servicio.

Este esquema de acompañamiento busca garantizar que la renovación se realice de manera ordenada y que el Municipio mantenga la continuidad de su plataforma de protección.

💰 Condiciones económicas

La presente propuesta corresponde a la renovación de **quinientas (500) licencias ESET PROTECT Advanced**, ofreciendo al Municipio tres alternativas de vigencia.

CONCEPTO	1 AÑO	2 AÑOS	3 AÑOS
Solución	ESET PROTECT Advanced	ESET PROTECT Advanced	ESET PROTECT Advanced
Cobertura	500 licencias	500 licencias	500 licencias
Vigencia	12 meses	24 meses	36 meses
Valor total de la oferta	$27.379.350	$52.440.750	$77.502.150
IVA	Excluido	Excluido	Excluido
VALOR TOTAL A PAGAR	$27.379.350	$52.440.750	$77.502.150

Valores expresados en pesos colombianos (COP).

Los valores anteriores corresponden al precio final ofrecido por COTEC S.A.S. al Municipio.

⚖️ Tratamiento tributario

La solución ESET se suministra mediante una arquitectura de servicios tecnológicos que incorpora componentes de administración y protección en la nube.

De acuerdo con el tratamiento tributario aplicable a los servicios de **computación en la nube (Cloud Computing)**, estos servicios pueden encontrarse excluidos del Impuesto sobre las Ventas – IVA, de conformidad con lo establecido en el **artículo 476 del Estatuto Tributario**, siempre que se cumplan las condiciones establecidas por la normatividad tributaria vigente.

En consecuencia, para efectos de la presente propuesta, los valores económicos se presentan como **IVA EXCLUIDO**, de acuerdo con el tratamiento tributario aplicable al servicio objeto de la renovación.

📋 Resumen de la propuesta

CARACTERÍSTICA	DESCRIPCIÓN
Fabricante	ESET
Solución	ESET PROTECT Advanced
Tipo de operación	Renovación de licenciamiento
Cantidad	500 licencias
Alternativas	1, 2 y 3 años
Modalidad	Licenciamiento empresarial
Administración	Consola centralizada
Protección	Endpoints y servidores compatibles
Soporte	Acompañamiento COTEC S.A.S.
IVA	Excluido

✅ Consideraciones finales

La renovación de **ESET PROTECT Advanced** representa una alternativa conveniente para garantizar la continuidad de la estrategia de ciberseguridad del **Municipio de Sogamoso**, manteniendo vigente una plataforma empresarial de protección, administración y actualización permanente.

La solución permite continuar protegiendo los equipos institucionales frente a malware, ransomware y otras amenazas avanzadas, mediante una arquitectura de seguridad multicapa y administración centralizada.

Las tres alternativas de vigencia —**uno (1), dos (2) y tres (3) años**— permiten al Municipio seleccionar el período de renovación que mejor se ajuste a sus necesidades operativas y presupuestales.

COTEC S.A.S., como aliado tecnológico y **Antivirus Authorized Reseller nivel silver**, ratifica su compromiso de acompañar al Municipio de Sogamoso durante el proceso de renovación, proporcionando soporte, asesoría y acompañamiento especializado para contribuir a la continuidad y fortalecimiento de la seguridad de la información institucional.

Atentamente

Ing. JOSE ANTONIO MATHEUS ROCHA
Gerente Comercial - Representante legal

Requerimientos Técnicos

1. Se debe indicar que el Fabricante es ESET|
El servicio debe contar con un esquema de alta disponibilidad, que ante un incidente, problema o riesgo materializado, pueda asegurar la continuidad tecnológica de la operación de la plataforma.

2. La plataforma deberá ser sometida al menos una vez cada año a un análisis de vulnerabilidades, con su debida remediación por parte del proveedor.

4. El servicio debe contar con un esquema de alta disponibilidad, que ante un incidente, problema o riesgo materializado, pueda asegurar la continuidad tecnológica de la operación de la plataforma.

5. El fabricante debe contar con estándares y certificaciones de cumplimiento reconocidos internacionalmente, tales como ISO/IEC 27001, que evidencien la implementación de un sistema de gestión de seguridad de la información alineado con buenas prácticas y controles de seguridad.

6. El fabricante debe contar con certificaciones de cumplimiento y gestión de calidad reconocidas internacionalmente, tales como ISO 9001, que evidencien la implementación de un sistema de gestión de calidad orientado a la mejora continua de sus procesos, productos y servicios.

7. El fabricante debe contar con un informe SOC 2 Tipo II vigente, que evidencie la implementación y efectividad operativa de controles relacionados con la seguridad, disponibilidad, confidencialidad, integridad del procesamiento y/o privacidad, según corresponda al alcance evaluado.

8. El proveedor debe implementar buenas prácticas relacionadas con la gestión del riesgo tecnológico como la ISO 31000 o similares.

9. El fabricante debe tener la política de seguridad de la información vigente, publicada y firmada por el representante legal o junta directiva.

10. La solución ofrecida deberá gestionar la información confidencial o sensible de manera cifrada, tanto en tránsito como en reposo.

11. El fabricante debe manejar un Recovery Point Objective u Objetivo de Punto de Recuperación cercano a 0 minutos.

12. El fabricante debe tener un Recovery Time Objective u Objetivo de Tiempo de Recuperación, el cuál debe ser < 1 hora.

13. El fabricante deberá contar con un SLA de disponibilidad de la infraestructura ≥ 99,9% mensual.

14. El fabricante debe especificar la cantidad de nuevas versiones o release en un año, mínima una versión al año; donde se identifique la capacidad de evolución tecnológica continua de la plataforma y los avances a nivel funcional, de seguridad y de componentes.

El fabricante deberá contar con un servicio de soporte técnico de 24/7.

1. Consola de Administración |

La arquitectura de gestión de la solución debe ser nativa de la nube (Cloud-native), garantizando alta disponibilidad y escalabilidad.

2. El agente debe ser compatible con Windows, MacOS, Linux. El proveedor debe adjuntar la matriz de versiones soportadas.

3. El agente debe tener un consumo moderado de recursos (CPU/RAM). El proveedor debe detallar los requisitos mínimos para el funcionamiento óptimo.

Debe permitir generar grupos de clientes dinámicos y grupos estáticos.
1. El fabricante debe proporcionar al menos tres diferentes formas de realizar la instalación de la consola de administración.

2. La solución debe garantizar una retención de datos de 30 días para fines de auditoría y búsqueda de amenazas.

3. La solución debe facilitar la administración mediante la creación y despliegue de políticas diferenciadas por áreas funcionales, roles de usuario o grupos organizacionales.

4. La consola de administración debe permitir la creación de perfiles de usuario y roles de acceso (RBAC) con permisos granulares y personalizados.

5. El software debe proveer conectores nativos y APIs escribibles que permitan la integración segura bidireccional con plataformas de terceros (SIEM, SOAR), garantizando el intercambio de alto volumen de datos y adaptación a nuevas necesidades.

6. La solución deberá tener una plataforma central de monitoreo, donde deberá brindar escalabilidad para ambientes empresariales medianos o grandes, permitiendo el crecimiento de hasta 50.000 endpoints.

7. La solución debe permitir la creación de reportes ejecutivos e informes técnicos totalmente personalizables y programables.

8. La solución debe soportar de manera nativa e integrada al menos un doble factor de autenticación (Aplicación/Passwordless).

9. Seguridad Antimalware | El agente debe contar con capacidades avanzadas para la detección de software malicioso. El proveedor debe detallar de forma técnica las metodologías empleadas, incluyendo, pero no limitándose a: detección basada en firmas, análisis heurístico, monitoreo de comportamiento en tiempo real y técnicas de sandboxing o inteligencia artificial (si aplican).

10. El agente debe ser capaz de identificar y bloquear de manera proactiva cualquier intento de escalamiento de privilegios no autorizado. El proveedor debe especificar cómo la solución monitorea comportamientos anómalos, intentos de explotación de vulnerabilidades locales o manipulaciones de tokens de acceso para prevenir que un usuario o proceso obtenga permisos de nivel superior

11. El agente debe integrar capacidades de detección de amenazas de día cero (zero-day) utilizando modelos de Machine Learning, ya sea de forma local (en el endpoint) o mediante análisis en la nube. El proveedor debe especificar cómo se entrenan estos modelos, el impacto en el rendimiento del equipo local y si la detección en la nube es obligatoria o complementaria para identificar archivos y comportamientos maliciosos nunca antes vistos.

12. El agente debe mantener sus capacidades de detección, análisis de comportamiento y respuesta ante incidentes (prevención y bloqueo) de forma local y autónoma, sin depender de una conexión activa a internet o a la consola de administración.

13. El agente debe permitir la configuración y personalización de las notificaciones que se muestran en el endpoint del usuario final. El proveedor debe especificar el nivel de granularidad de estas alertas, incluyendo la capacidad de modificar el texto (mensajes

instructivos o de cumplimiento), el logotipo corporativo, y la opción de silenciar avisos no críticos para evitar interrupciones innecesarias en la productividad.

14. La solución propuesta debe incluir todas las funcionalidades de detección y respuesta en endpoints (EDR) o detección y respuesta extendida (XDR) e identificación de aplicativos y sistemas vulnerables con capacidad de remediación desde la consola de administración, dentro del esquema de licenciamiento base o estándar ofertado. El proveedor debe garantizar que no se requieren suscripciones adicionales, módulos independientes o costos incrementales para habilitar la visibilidad completa de los controles de seguridad.

15. El agente debe contar con la capacidad de realizar la reversión automática de archivos (rollback) afectados por un ataque de cifrado.

16. El agente debe integrar capacidades de detección y bloqueo de intentos de Phishing para proteger la identidad y datos del usuario.

17. El agente debe tener la capacidad de inspeccionar tráfico de red cifrado para detectar amenazas ocultas en túneles SSL/TLS.

18. La solución debe integrar capacidades de filtrado de contenido web basadas en categorías (ej. sitios maliciosos, apuestas, redes sociales, contenido adulto). El proveedor debe garantizar que las políticas puedan aplicarse de forma granular por grupos de usuarios o equipos, permitiendo el bloqueo, permiso o monitoreo de la navegación independientemente de la red a la que el dispositivo esté conectado

19. La solución debe contar con capacidades avanzadas para identificar y bloquear amenazas antes de que el código malicioso se ejecute en el sistema. El proveedor debe garantizar que el agente utilice técnicas como análisis estático por IA/ML, inspección de atributos de archivos y reputación en tiempo real para prevenir la activación de malware, scripts maliciosos o exploits, asegurando que la amenaza sea neutralizada en su estado pasivo.

20. La solución debe contar con un motor avanzado de consultas para threat hunting con soporte para búsqueda histórica, indicadores de compromiso (IoCs) y sugerencias predictivas.

21. La solución debe contar con la capacidad de fusionar y agrupar automáticamente múltiples eventos o alertas relacionadas (basadas en el mismo host, usuario, vector de ataque o indicadores de compromiso) dentro de un único caso o incidente unificado.

22. La solución debe integrar una funcionalidad de terminal remoto seguro para la ejecución de tareas de respuesta directa en los endpoints.

23. El sistema debe alertar automáticamente sobre la ejecución de procesos maliciosos conocidos basándose en reglas e indicadores de compromiso (IoCs).

24. Protección contra Amenazas de día cero | La solución deberá proporcionar una capa adicional de defensa avanzada frente a amenazas de día cero, amenazas desconocidas, ataques dirigidos y ransomware, mediante tecnologías especializadas de análisis fuera del endpoint.
25. La solución deberá operar con una arquitectura basada en la nube para el análisis de muestras sospechosas, evitando depender exclusivamente de capacidades locales del equipo protegido.

26. La solución deberá contar con un esquema de detección multinivel o multicapa, donde distintas capas de análisis emitan veredictos complementarios y el resultado final se construya con base en la evaluación integral de la muestra.

27. La solución deberá permitir proteger archivos adjuntos de correo mediante integración con la solución de seguridad de correo del fabricante o equivalente, evitando la entrega de mensajes con contenido malicioso al destinatario final.

28. La solución deberá contemplar integración con plataformas de endpoint, servidor y seguridad de correo o colaboración cloud, de modo que la defensa contra amenazas desconocidas se aplique de forma coordinada en múltiples superficies.

29. La solución deberá contribuir a prevenir la ejecución de ransomware y otras amenazas desconocidas antes de que alcancen el entorno de producción, utilizando análisis externo y veredictos especializados sobre archivos sospechosos.

30. La solución deberá fortalecer la postura de seguridad frente a ataques dirigidos, amenazas persistentes avanzadas y campañas que utilicen vectores novedosos o no reconocidos por mecanismos tradicionales.

31. La solución deberá ofrecer un tiempo máximo de análisis de cinco minutos, si la muestra ya fue analizada anteriormente, el resultado debe tardar hasta dos minutos.

32. La solución deberá permitir clasificar las muestras analizadas con veredictos diferenciados, tales como malicioso, altamente sospechoso, sospechoso o limpio

33. Protección de datos en Endpoint por medio de Cifrado de Disco | La solución deberá permitir el cifrado de disco completo en equipos de usuario final y estaciones

de trabajo, con el fin de proteger la información almacenada localmente ante pérdida, robo o acceso no autorizado.

34. La solución deberá permitir el cifrado de discos, particiones y unidades completas del sistema, asegurando la protección integral de la información almacenada en el endpoint.

35. La solución deberá incorporar una capa adicional de seguridad mediante autenticación previa al arranque del sistema (pre-boot authentication o pre-boot login), evitando el acceso al sistema operativo.

36. La solución deberá permitir la administración remota centralizada del cifrado desde una consola local, en la nube o híbrida, según el modelo operativo definido por la entidad.

37. La solución deberá integrarse con la consola de administración de seguridad de la organización, permitiendo una gestión unificada junto con otras capacidades de protección del endpoint.

38. La solución deberá permitir la aplicación de políticas centralizadas para la activación, administración y monitoreo del cifrado sobre equipos gestionados remotamente.

39. La solución deberá soportar la administración basada en grupos, tareas y reportes, con el fin de facilitar la operación empresarial y el seguimiento del estado de cifrado de los equipos.

40. La solución deberá permitir su implementación y activación remota en endpoints conectados a la infraestructura de gestión, reduciendo la intervención manual sobre cada dispositivo.

41. La solución deberá brindar soporte, como mínimo, para estaciones de trabajo Windows y macOS en lo relacionado con cifrado de disco completo administrado centralmente.

42. La solución deberá ayudar a la entidad a fortalecer el cumplimiento de normativas y regulaciones de protección de datos, al reducir la exposición de información sensible almacenada en endpoints.

43. La solución deberá utilizar algoritmos de cifrado robustos y reconocidos por la industria. Se requiere que el fabricante ofrezca cifrado de al menos AES de 256 bits y

preferiblemente con validaciones o certificaciones reconocidas, tales como FIPS 140-2 o equivalente.

44. La solución deberá permitir al administrador programar tareas de cifrado sobre los endpoints seleccionados, con la posibilidad de pausar el proceso y reanudarlo posteriormente desde el último punto ejecutado.

45. La solución deberá ofrecer mecanismos de recuperación de acceso para usuarios remotos que se bloqueen o pierdan la posibilidad de autenticarse, permitiendo diversas opciones de recuperación de contraseña o desbloqueo seguro.

46. Para equipos con sistema operativo Windows, la solución deberá permitir la opción de inicio de sesión único (SSO) o funcionalidad equivalente, para facilitar la experiencia de autenticación del usuario sin debilitar la seguridad del cifrado.

47. Protección de Correo Electrónico | La solución debe proporcionar una protección avanzada multi tenant compatible con los ecosistemas Microsoft 365 y Google Workspace

48. La solución deberá ofrecer una consola de administración web centralizada, accesible remotamente, para la gestión de políticas, configuración, monitoreo y operación de la plataforma.

49. La solución deberá contar con capacidades de filtrado antispam, análisis antimalware y protección anti-phishing, con el fin de proteger las comunicaciones corporativas frente a amenazas recibidas por correo electrónico.

50. La solución deberá ser capaz de analizar el contenido de Microsoft 365 y la suite de aplicaciones.

51. La solución deberá ser capaz de analizar el contenido de Gmail y Google Drive vía API.

52. Puede definir las reglas personalizadas de verificación del remitente y contra la suplantación de identidad con condiciones que contengan métodos de autenticación, como SPF, DKIM, DMARC y ARC.

53. La solución de correo electrónico, deberá contar con una capa de protección adicional, para amenazas de día cero.

54. La solución debe tener la capacidad de analizar documentos adjuntos, enlaces de URL, códigos QR o cualquier elemento incrustado en el correo electrónico que busca exfiltrar información o engañar al usuario final.

55. Debe tener la capacidad de crear listas blancas y negras de remitentes y direcciones IP.

56. La solución de correo electrónico deberá contar con una capa adicional de protección para amenazas avanzadas o de día cero, mediante mecanismos de sandboxing en la nube o tecnología equivalente del fabricante para el análisis aislado de archivos o muestras sospechosas.

57. La solución de protección de correo electrónico deberá permitir la creación de reglas personalizadas de seguridad de correo, con el fin de definir condiciones y acciones específicas sobre mensajes entrantes o procesados por la plataforma.

58. La solución deberá permitir la evaluación de condiciones asociadas al remitente, dirección IP del remitente, dominio del remitente, valores del encabezado From, nombre del remitente, asunto, cuerpo del mensaje, nombre de adjuntos, extensión de adjuntos, tipo de archivo adjunto y fecha u hora de recepción del mensaje.

59. La solución deberá permitir la definición de acciones sobre mensajes que cumplan determinadas condiciones, incluyendo como mínimo cuarentena del mensaje, eliminación del mensaje, eliminación de adjuntos, movimiento a carpeta de correo no deseado, adición de prefijos al asunto y adición de banners en el cuerpo del mensaje.

60. Se deberá contar con la posibilidad de enviar notificaciones por correo electrónico de alerta a los responsables de seguridad o administrador, por alertas y eventos que se identifiquen como maliciosos

61. Gestión de Vulnerabilidades | La solución deberá permitir la detección continua de vulnerabilidades en sistemas operativos y aplicaciones instaladas en los equipos administrados, con el fin de identificar oportunamente riesgos de seguridad sobre los activos de la entidad.

62. La solución debe identificar y priorizar automáticamente vulnerabilidades en endpoints (Windows, Mac, Linux) y realizar la remediación mediante parches o cambios de configuración desde la consola.

63. La solución deberá permitir la identificación de vulnerabilidades mediante referencias estandarizadas como CVE (Common Vulnerabilities and Exposures) y facilitar su consulta, agrupación y seguimiento desde la consola.

64. La solución deberá permitir el filtrado granular de vulnerabilidades por criterios como nombre de aplicación, versión, proveedor, puntuación de riesgo, identificador CVE, nombre del equipo, categoría de vulnerabilidad, fecha de detección y tipo de sistema operativo.

65. La solución deberá disponer de una puntuación de riesgo para las vulnerabilidades detectadas, construida a partir de criterios técnicos y contextuales como métricas CVSS, popularidad del CVE, tasa de riesgo comprometido, antigüedad o ciclo de vida del CVE, o metodología equivalente del fabricante

66. La solución deberá permitir la corrección de vulnerabilidades mediante aplicación de parches cuando exista un parche disponible para el software o sistema operativo afectado.

67. La solución deberá permitir la definición de ventanas de mantenimiento o franjas horarias específicas para la instalación de parches y actualizaciones, con el objetivo de minimizar interrupciones operativas.

68. La solución deberá permitir la gestión de excepciones de parcheo, incluyendo el registro y seguimiento de exclusiones o aplicaciones exceptuadas del proceso automático de actualización.

69. La solución deberá soportar aplicación automática de parches para aplicaciones y sistemas operativos, incluyendo la definición de estrategias de despliegue tales como aplicar todos los parches, solo los permitidos o todos excepto los excluidos, o capacidades equivalentes

70. La solución deberá contemplar medidas de remediación adicionales cuando no exista parche o cuando así lo determine el administrador, tales como desinstalación de la aplicación vulnerable, aislamiento del dispositivo o mecanismos equivalentes de contención y mitigación

71. La solución deberá permitir verificar si un CVE específico está cubierto por la plataforma y si dicha vulnerabilidad se encuentra presente en el entorno de la entidad, indicando en cuántos equipos ha sido detectada.

72. Al identificar una vulnerabilidad en el sistema, la información que se compartirá a la consola de gestión será: Nombre de la aplicación, Versión de la aplicación, Proveedor, Puntuación de riesgo de 0 a 100, número CVE (vulnerabilidades y exposición comunes), Nombre del equipo, Tipo de sistema operativo.
La puntuación del riesgo de las vulnerabilidades se clasifica, de acuerdo con los siguientes parámetros.

CVSSv2/CVSSv3
Popularidad de CVE
Ciclo de vida de CVE
Tasa de riesgo comprometido
Amarillo (0–40): gravedad media
Rojo (41–100): gravedad crítica

73. Analiza miles de aplicaciones y detecta más de 35.000 vulnerabilidades y exposiciones comunes (CVE).

74. Respuesta Extendida | La solución deberá brindar soporte multiplataforma, permitiendo el monitoreo y la operación sobre endpoints con sistemas operativos Windows, macOS y Linux.

75. La solución deberá permitir que las detecciones o reglas estén alineadas o referenciadas con marcos reconocidos de ciberseguridad, preferiblemente con MITRE ATT&CK, con el fin de facilitar el análisis y la contextualización de técnicas maliciosas.

76. La solución deberá soportar escalabilidad suficiente para ambientes empresariales medianos o grandes, permitiendo el crecimiento de hasta 25.000 endpoints.

77. El agente EDR/XDR debe proporcionar visibilidad completa y detallada sobre los eventos del sistema en tiempo real. El proveedor debe garantizar la capacidad de monitorear y registrar actividades relacionadas con: procesos (árboles de ejecución, inyección de código), sistema de archivos (creación, modificación y borrado), conexiones de red (IPs origen/destino, puertos y protocolos) y registros del sistema (modificaciones de llaves, persistencia). Esta telemetría debe estar disponible para auditoría y análisis forense.

78. La solución EDR/XDR debe generar de forma automática una línea de tiempo cronológica y detallada para cada incidente detectado. El proveedor debe especificar cómo la consola visualiza el flujo del ataque, permitiendo la correlación de eventos (procesos padre/hijo, cambios en archivos y conexiones de red) en una vista unificada que facilite la identificación de la causa raíz (root cause analysis) y el impacto total de la amenaza.

79. La solución EDR/XDR debe integrar capacidades de análisis automático para determinar el origen de cualquier alerta de seguridad generada. El proveedor debe detallar cómo el sistema correlaciona eventos de red con la actividad del endpoint para identificar el proceso, usuario o archivo que inició la amenaza. Este análisis debe ser exhaustivo siempre que la telemetría del endpoint esté disponible, proporcionando una visualización clara del vector de entrada y la secuencia de ejecución.

80. El sistema debe garantizar la detección de técnicas de ataque en todas las fases del ciclo de vida de una amenaza (Cyber Kill Chain), incluyendo acceso inicial, ejecución, persistencia, comando y control y exfiltración.

81. La solución debe permitir la configuración de respuestas automáticas (Playbooks) ante la detección de eventos críticos confirmados.

82. La solución debe integrar un sistema nativo para la gestión completa de incidentes que permita: asignación de responsables, envío de notificaciones automáticas, registro de comentarios/bitácora, y transiciones de estados (ej. Abierto, En Investigación, Remediado, Cerrado). Asimismo, debe incluir un sistema de scoring (puntuación) automático y personalizable por el administrador, así como la visualización directa de tácticas, técnicas y procedimientos (TTPs) alineados a MITRE ATT&CK y todos los artefactos relacionados al caso.

83. La solución debe integrar una funcionalidad de terminal remoto seguro para la ejecución de tareas de respuesta directa en los endpoints.

84. La solución debe permitir el aislamiento o cuarentena inmediata de procesos o eventos sospechosos para prevenir su propagación.

85. La plataforma deberá permitir capacidades de threat hunting o búsqueda proactiva de amenazas mediante mecanismos de búsqueda y filtrado de Indicadores de Compromiso (IoC).

86. El sistema debe alertar automáticamente sobre la ejecución de procesos maliciosos conocidos basándose en reglas e indicadores de compromiso (IoCs).

87. Autenticación de Usuarios | La plataforma deberá contar con consola central de administración basada en web, permitiendo la gestión remota de usuarios, políticas, aprovisionamiento y métodos de autenticación.

88. La solución de autenticación multifactor deberá permitir la validación de identidad de los usuarios mediante un segundo factor de autenticación, complementando el uso de credenciales corporativas tradicionales.

89. La solución deberá soportar mecanismos de autenticación basados en dispositivos móviles, incluyendo como mínimo notificaciones push y contraseñas de un solo uso (OTP), para facilitar un proceso de autenticación seguro y de fácil adopción por parte de los usuarios.

90. La solución deberá soportar métodos alternativos de autenticación, tales como OTP basada en tiempo o evento, SMS y tokens de hardware compatibles con estándares abiertos, con el propósito de adaptarse a distintos perfiles operativos y escenarios de contingencia.

91. La solución deberá ser compatible con dispositivos móviles con sistemas operativos iOS y Android para el uso de autenticación push y aplicación móvil de autenticación.

92. La solución deberá agregar autenticación de dos factores (2FA) a entornos basados en Microsoft Active Directory, de manera que se fortalezca el control de acceso a recursos corporativos.

93. La solución deberá permitir proteger el acceso mediante Remote Desktop Protocol (RDP) a través de autenticación multifactor.

94. La solución deberá permitir proteger el inicio de sesión en equipos Windows, mediante un componente o plugin específico para autenticación multifactor en estaciones de trabajo Windows

95. La solución deberá permitir la protección de aplicaciones web mediante plugins o mecanismos compatibles con entornos Microsoft Web Applications.

96. La solución deberá contribuir a la reducción del riesgo asociado al robo de credenciales, contraseñas débiles, accesos no autorizados y compromiso de cuentas de usuario o administrativas.

97. Equipo de Seguridad del fabricante a nivel local para garantizar soporte del mismo

Ser profesional en Ingeniería de Telecomunicaciones, Ingeniería de Sistemas. O Ing. Electronica
El profesional deberá contar con especialización en Seguridad de Redes.
Contar con Master en Ciberseguridad y Privacidad.
Contar con especialización en Seguridad Informática
Contar con certificación Certified in Cybersecurity – CC de ISC2
Contar con certificación en ISO/IEC 27001:2022 o formación certificada
1. Acreditar mínimo 15 certificaciones de producto del fabricante o solución de seguridad propuesta.

98. Equipo de Seguridad del proponente para garantizar soporte de primer nivel y coordinar las tareas de soporte con el fabricante en línea con el Cliente.

Ser profesional en Ingeniería de Telecomunicaciones, Ingeniería de Sistemas, o Ing. Electrónica

El profesional deberá contar con certificación del fabricante para los productos ofrecidos.

Demostrar vinculación con el proponente, mediante el aporte de parafiscales en los últimos seis meses (6).

Aportar tarjeta profesional vigente, mediante la cual se demuestra 5 o mas años de experiencia