

CONSULTORIA TECNICA Y SERVICIOS DE INGENIERIA

NIT 800127892.1

36 AÑOS
Hardware & Software Gold Reseller
Centro Autorizado de Servicio
Antivirus Authorized Reseller
No 202606304

Tunja, junio 30 de 2026

Señores:

GOBERNACION DE BOYACA

Atte:

Tunja.-

Ref. Cotización Renovación Licenciamiento Protección
Antivirus

Apreciados Señores:

En atención a su amable solicitud, le agradezco encontrar a continuación nuestra propuesta, para la renovación y ampliación del licenciamiento del producto antivirus de la referencia, así:

PRECIO DEL LICENCIAMIENTO Y SERVICIOS ANEXOS

(favor revisar documento anexo que contiene la especificación técnica detallada)

Aspectos más destacables del producto, por versión:

ESET PROTECT Entry – Protección esencial para los endpoints

Esta capa proporciona la base de seguridad necesaria para proteger los equipos corporativos mediante:

- Consola centralizada de administración en la nube o local.
- Protección antivirus y antimalware multicapa para estaciones de trabajo.
- Seguridad para servidores Windows y Linux.
- Protección contra ransomware
- Gestión centralizada de políticas, reportes y monitoreo.

Es una alternativa ideal para organizaciones que buscan una protección sólida y administración centralizada de sus dispositivos.

ESET PROTECT Advanced – Protección avanzada contra amenazas modernas

Además de todas las funcionalidades incluidas en Entry, incorpora:

- Defensa avanzada contra amenazas (Advanced Threat Defense) mediante análisis en sandbox cloud.
- Detección proactiva de malware desconocido y ataques de día cero.
- Cifrado completo de disco (Full Disk Encryption) para proteger la información almacenada en equipos y portátiles.
- Protección de dispositivos móviles Android e iOS mediante Mobile Threat Defense.

Esta capa permite fortalecer significativamente la postura de seguridad frente a amenazas avanzadas y reducir el riesgo de pérdida o exposición de información.

CONSULTORIA TECNICA Y SERVICIOS DE INGENIERIA

NIT 800127892.1

36 AÑOS

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

ESET PROTECT Complete – Protección integral multicapa

Incluye todas las capacidades de Entry y Advanced, adicionando protección para los principales vectores de ataque utilizados actualmente por los ciberdelincuentes:

- Seguridad para correo electrónico (Mail Server Security).
- Protección de aplicaciones en la nube (Cloud App Protection para Microsoft 365).
- Gestión de vulnerabilidades y parchado (Vulnerability & Patch Management).
- Protección avanzada para servidores, endpoints, correo y servicios en la nube desde una única consola.
- Mayor visibilidad del estado de seguridad de la organización y reducción de superficies de ataque.

Esta solución está diseñada para organizaciones que buscan una estrategia de protección integral, cubriendo usuarios, dispositivos, servidores, correo electrónico y aplicaciones corporativas en la nube.

Adicionalmente, nos gustaría coordinar un espacio virtual o presencial con nuestro equipo de especialistas comerciales y preventa para presentar en detalle las capacidades de cada capa, resolver inquietudes y validar la alternativa que mejor se adapte a sus necesidades actuales y futuras.

Todas las opciones poseen:

- Protección exhaustiva para endpoints con Windows, Soporte para la virtualización + Nueva tecnología. Es compatible con las máquinas virtuales y suministra protección ante criminales informáticos y botnets.
- Control del acceso a los datos integrado. Incluye el Control Web para limitar el acceso a los sitios Web, y el Firewall Bidireccional.
- Bajo impacto en el sistema. Deja libres más recursos del sistema a la vez que sigue suministrando una protección completa.

Administración: administra en su totalidad desde Consola unificada y centralizada.

Incluye ESET Endpoint Security

Protección para endpoints

Protección avanzada en múltiples niveles para PC, smartphones y máquinas virtuales

Incluye ESET Server Security

Seguridad para servidores de archivo

Protección en tiempo real para los datos corporativos que viajan a través de los servidores.

3. Esquema de Soporte y Servicios

A continuación, les presentamos el esquema de soporte y servicios que acompañan nuestra propuesta:

CONSULTORIA TECNICA Y SERVICIOS DE INGENIERIA

NIT 800127892.1

36 AÑOS

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

- Se incluye la asistencia para verificación de la actual instalación y re-configuración de la solución de ESET, en caso que se determine que así debe hacerse.
 - Soporte técnico. Los días hábiles de 8AM a 5PM. Para horarios diferentes en días no hábiles se realizará un acuerdo dependiendo de las necesidades de la Gobernación de Boyacá.
 - o Telefónico.
 - o Vía e-mail.
 - o Mensajería instantánea
 - Soporte técnico ante incidentes de seguridad. Los días hábiles de 8AM a 5PM. Para horarios diferentes en días no hábiles se realizará un acuerdo dependiendo de las necesidades de la Gobernación de Boyacá.
 - o A través de acceso remoto
 - o Visitas on site
 - Laboratorio ESET Latinoamérica. Recolección (por acceso remoto) y envío de muestras a nuestro laboratorio para el análisis de nuevas amenazas.
 - Capacitación técnica. Se realizará de manera presencial / virtual, entrenamientos en el uso de las soluciones de ESET adquiridas, mediante la dirección de especialistas del producto.
 - Visitas proactivas. Se realizará una visitas periodicas por parte del partner asignado, para revisar los logs y la configuración de los productos de ESET implementados, proponiendo a partir de esto las mejoras respectivas.
- Información detallada del producto: <http://www.eset-la.com/empresas/eset-endpoint-security>

eset PROTECT						
ESET PROTECT MDR Ultimate	ESET PROTECT MDR	ESET PROTECT Elite	ESET PROTECT Enterprise	ESET PROTECT Complete	ESET PROTECT Advanced	ESET PROTECT Entry
Management Console	Management Console	Management Console	Management Console	Management Console	Management Console	Management Console
Modern Endpoint Security	Modern Endpoint Security	Modern Endpoint Security	Modern Endpoint Security	Modern Endpoint Security	Modern Endpoint Security	Modern Endpoint Security
Server Security	Server Security	Server Security	Server Security	Server Security	Server Security	Server Security
Mobile Threat Defense	Mobile Threat Defense	Mobile Threat Defense	Mobile Threat Defense	Mobile Threat Defense	Mobile Threat Defense	
Advanced Threat Defense	Advanced Threat Defense	Advanced Threat Defense	Advanced Threat Defense	Advanced Threat Defense	Advanced Threat Defense	
Full Disk Encryption	Full Disk Encryption	Full Disk Encryption	Full Disk Encryption	Full Disk Encryption	Full Disk Encryption	
Mail Server Security	Mail Server Security	Mail Server Security		Mail Server Security		
Cloud App Protection	Cloud App Protection	Cloud App Protection		Cloud App Protection		
Vulnerability & Patch Management	Vulnerability & Patch Management	Vulnerability & Patch Management		Vulnerability & Patch Management		
XDR	XDR	XDR	XDR			
Authentication	Authentication	Authentication				
ESET MDR Ultimate	ESET MDR					
Premium Support Ultimate	Premium Support					

CONSULTORIA TECNICA Y SERVICIOS DE INGENIERIA

NIT 800127892.1

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

VALOR DE LA PROPUESTA: RENOVACION DEL LICENCIAMIENTO PROTECCION ANTIVIRUS

DENOMINACION: ESET PROTECT Entry –

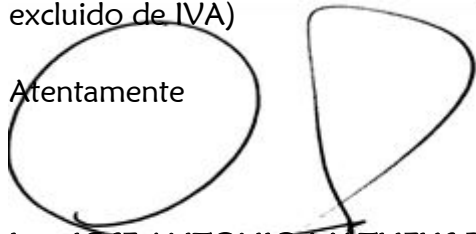
ORIENTACIÓN: Protección esencial para los endpoints.

Forma de control y administración: On-premise o Cloud.

Número total de Licencias: 1200 nodos (PCS & Servidores)

**Licenciamiento tres (3) años \$114.265.600,00 (valor total. Producto Cloud
excluido de IVA)**

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.

CONSULTORIA TECNICA Y SERVICIOS DE INGENIERIA

NIT 800127892.1

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

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 $\geq 99,9\%$ 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.

CONSULTORIA TECNICA Y SERVICIOS DE INGENIERIA

NIT 800127892.1

36 AÑOS

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

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

CONSULTORIA TECNICA Y SERVICIOS DE INGENIERIA

NIT 800127892.1

36 AÑOS

*Hardware & Software Gold Reseller
Centro Autorizado de Servicio
Antivirus Authorized Reseller*

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.

CONSULTORIA TECNICA Y SERVICIOS DE INGENIERIA

NIT 800127892.1

36 AÑOS

*Hardware & Software Gold Reseller
Centro Autorizado de Servicio
Antivirus Authorized Reseller*

- 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

CONSULTORIA TECNICA Y SERVICIOS DE INGENIERIA

NIT 800127892.1

36 AÑOS

*Hardware & Software Gold Reseller
Centro Autorizado de Servicio
Antivirus Authorized Reseller*

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

CONSULTORIA TECNICA Y SERVICIOS DE INGENIERIA

NIT 800127892.1

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

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.

CONSULTORIA TECNICA Y SERVICIOS DE INGENIERIA

NIT 800127892.1

36 AÑOS

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

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.

CONSULTORIA TECNICA Y SERVICIOS DE INGENIERIA

NIT 800127892.1

36 AÑOS

*Hardware & Software Gold Reseller
Centro Autorizado de Servicio
Antivirus Authorized Reseller*

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.

CONSULTORIA TECNICA Y SERVICIOS DE INGENIERIA

NIT 800127892.1

36 AÑOS

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

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.

CONSULTORIA TECNICA Y SERVICIOS DE INGENIERIA

NIT 800127892.1

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

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.

CONSULTORIA TECNICA Y SERVICIOS DE INGENIERIA

NIT 800127892.1

36 AÑOS

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

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.

CONSULTORIA TECNICA Y SERVICIOS DE INGENIERIA

NIT 800127892.1

36 AÑOS

*Hardware & Software Gold Reseller
Centro Autorizado de Servicio
Antivirus Authorized Reseller*

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



Protección en múltiples niveles para
endpoints, con machine learning y una
fácil administración



PROTECT ENTRY

- Consola de gestión
- Protección para endpoints
- Seguridad para servidores de archivo

Proteja las computadoras, los equipos portátiles y los dispositivos móviles de su empresa con productos de seguridad de última generación que se administran desde una única consola basada en la nube.

- La consola de administración ESET PROTECT se puede implementar en las instalaciones o en la nube, según los requisitos del usuario, lo que ofrece una administración de seguridad de TCO más baja.
- Gestión remota que ofrece visibilidad de amenazas, usuarios y elementos en cuarentena desde una única pantalla.
- Las endpoints y los móviles de la compañía se encuentran seguros con una tecnología avanzada, que ahora también incluye protección contra ataques de fuerza bruta.
- La mejor seguridad para endpoints de su clase, que utiliza el enfoque comprobado de ESET de protección en varias capas, reuniendo lo mejor de cada mundo: la reputación basada en la nube, el *machine learning* y el análisis del comportamiento en profundidad.
- La multipremiada protección para endpoints combina las últimas técnicas de aprendizaje automático con décadas de experiencia humana.



¿Tiene un presupuesto ajustado? ESET PROTECT Entry On-Prem está disponible para la implementación local de su consola de administración.

PROTECCIÓN PARA ENDPOINTS Y SERVIDORES DE ARCHIVO EN MÚLTIPLES CAPAS

ESET Endpoint Security brinda protección avanzada para la prevención de malware y exploits, y permite detectar amenazas antes, durante y después de la ejecución. Ahora también cuenta con protección contra ataques de fuerza bruta.

ESET Server Security ofrece a los servidores seguridad liviana en múltiples capas para garantizar la continuidad del negocio.

- Bloqueo de ataques dirigidos
- Prevención violaciones de datos
- Detiene los ataques sin archivos
- Detecta amenazas persistentes avanzadas

CONSOLA DE GESTIÓN REMOTA

ESET PROTECT es una herramienta remota multifuncional basada en la nube para la administración de la seguridad de red de los productos de seguridad corporativos de ESET en todos los sistemas operativos. Permite implementar la seguridad con un solo clic y le suministra visibilidad de la red sin necesidad de tener hardware adicional, lo que reduce el costo total de propiedad.

- Configuración e implementación perfectas
- La implementación en la nube no requiere hardware o software adicional
- Gestión de la seguridad de la red desde un único lugar
- Optimización de tiempo con tareas automatizadas



Todas las soluciones de ESET para endpoints se gestionan desde una única pantalla: la consola basada en la nube de ESET PROTECT, que le permite visualizar el estado de seguridad de su red completa.

Acerca de ESET

Desde hace más de 30 años, desarrollamos soluciones de seguridad que ayudan a más de 100 millones de usuarios en el mundo a disfrutar la tecnología de forma segura.

Al no estar limitados por las exigencias de accionistas del mercado, podemos enfocarnos exclusivamente en la seguridad de la información, mediante investigación y desarrollo constante.

ESET EN NÚMEROS

+110 millones
de usuarios
en el mundo

+400 mil
clientes
corporativos

+200
países y
territorios

13
centros de
investigación
y desarrollo

ALGUNOS DE NUESTROS CLIENTES



protegido por ESET desde
2017, más de 9.000 endpoints



protegido por ESET desde
2016, más de 4.000 buzones
de correo



protegido por ESET desde
2016, más de 32.000
endpoints



partner de seguridad ISP
desde 2008 con una base de
clientes de 2 millones

ALGUNOS DE NUESTROS PREMIOS MÁS IMPORTANTES



ESET recibió el premio Business Security APPROVED de AV-Comparatives en el Business Security Test en diciembre de 2021.



ESET logra consistentemente las mejores clasificaciones en la plataforma global de revisión de usuarios G2 y sus soluciones son avaladas por clientes de todo el mundo.



Las soluciones de ESET fueron reconocidas por el analista Forrester como sample vendor en "The Forrester Tech Tide(TM): Zero Trust Threat Detection and Response, Q2 2021".



PROTECT ADVANCED

La mejor protección para endpoints contra el ransomware y las amenazas 0-day, respaldada por una potente seguridad de datos



Consola



Protección
moderna para
endpoints



Seguridad para
servidores



Defensa
avanzada de
amenazas



Cifrado de disco
completo

Progress. Protected.



Consola



Protección moderna para endpoints



Seguridad para servidores



Defensa avanzada de amenazas



Cifrado de disco completo

Proteja las computadoras, los equipos portátiles y los dispositivos móviles de su empresa con productos de seguridad que se administran desde una consola local o basada en la nube. La solución incluye tecnología de defensa avanzada de amenazas, que previene los nuevos tipos de amenazas nunca antes vistos, así como la funcionalidad de cifrado de disco completo, para una protección de datos optimizada.

CÓMO SE BENEFICIARÁ SU ORGANIZACIÓN

- Suministra protección mejorada contra ransomware y amenazas 0-day a través de la tecnología de modo sandbox en la nube.
- Ayuda a cumplir con las reglamentaciones de protección de datos gracias a sus funcionalidades de cifrado de disco completo en Windows y macOS.
- La consola ESET PROTECT Cloud de fácil acceso mejora el costo total de propiedad de la gestión de la seguridad.
- La administración remota ofrece visibilidad de amenazas, usuarios y elementos en cuarentena desde una única pantalla.
- Las endpoints y los dispositivos móviles de la empresa se mantienen seguros con una tecnología avanzada de varias capas, que incluye la protección contra ataques por fuerza bruta.



ESET SECURITY SERVICES

Este servicio trabaja conjuntamente con sus productos de ESET de seguridad para endpoints y ofrece una solución completa fortaleciendo a su equipo de seguridad de TI con el soporte técnico permanente de los expertos de ESET, que están listos para ayudar si surge algún problema de seguridad.

UN ESPECTRO COMPLETO DE FUNCIONALIDADES



DEFENSA AVANZADA CONTRA AMENAZAS CON MODO SANDBOX EN LA NUBE PARA EVITAR EL RANSOMWARE

ESET LiveGuard Advanced brinda protección proactiva contra las nuevas amenazas nunca antes vistas mediante la ejecución de todas las muestras sospechosas enviadas en un potente entorno aislado de modo sandbox en la nube, con el fin de evaluar su comportamiento utilizando feeds de inteligencia de amenazas, las múltiples herramientas internas de ESET para el análisis estático y dinámico, y datos de reputación de los archivos.

- Desempaquetado y exploración avanzados
- Aprendizaje automático de última generación
- Análisis exhaustivo del comportamiento
- Modo sandbox en la nube



PROTECCIÓN MULTICAPA PARA ENDPOINTS CON SEGURIDAD PARA SERVIDORES

ESET Endpoint Security suministra una fuerte protección contra el malware y los exploits, y es capaz de detectar actividad maliciosa antes, durante y después de su ejecución. Ahora también cuenta con tecnología que evita la adivinación de contraseñas.

ESET Server Security ofrece una protección liviana y multicapa de los servidores, a fin de garantizar la continuidad del negocio.

- Bloquee los ataques dirigidos
- Evite las vulneraciones de datos
- Detenga los ataques sin archivos
- Detecte las amenazas persistentes avanzadas



CIFRADO POTENTE GESTIONADO POR ESET EN FORMA NATIVA

ESET Full Disk Encryption es una función de cifrado del disco completo, nativa de la consola ESET PROTECT. Permite implementar la solución y cifrar los datos en las endpoints Windows y Mac conectadas con un solo clic. ESET Full Disk Encryption aumenta considerablemente la seguridad de los datos corporativos y lo ayuda a cumplir con las normativas de protección de datos.

- Administre el cifrado en máquinas Windows y macOS
- Cifre discos, particiones o unidades completas del sistema
- Despliegue, active y cifre dispositivos con una sola acción



CONSOLA: INTERFAZ DE LA PLATAFORMA UNIFICADA DE ESET

ESET PROTECT es una herramienta remota de administración de la seguridad de red multifuncional, ya sea local o basada en la nube, para los productos de seguridad corporativos de ESET en todos los sistemas operativos. Permite desplegar la seguridad con un solo clic y la consola en la nube le suministra visibilidad de la red sin necesidad de comprar o mantener hardware adicional, lo que reduce el costo total de propiedad.

- Configuración e implementación sin inconvenientes
- La implementación en la nube no requiere hardware ni software adicional
- Se gestiona la seguridad de toda la red desde un único punto
- Ahorro de tiempo mediante las tareas automatizadas



Acerca de ESET

CUANDO LA TECNOLOGÍA PERMITE EL PROGRESO, ESET® ESTÁ AQUÍ PARA PROTEGERLA.

ESET aporta más de 30 años de innovación impulsada por la tecnología y ofrece las soluciones de ciberseguridad más avanzadas del mercado. Nuestra moderna protección para endpoints se basa en las exclusivas tecnologías de seguridad multicapa ESET LiveSense®, combinadas con el uso continuo del aprendizaje automático y la computación en la nube. Gracias al respaldo de la mejor inteligencia e investigación sobre amenazas del mundo, los productos de ESET ofrecen el equilibrio perfecto entre capacidades de prevención, detección y respuesta. Con una gran facilidad de uso y una velocidad insuperable, nos dedicamos a proteger el progreso de nuestros clientes, garantizando la máxima seguridad.

ESET EN NÚMEROS

**MÁS DE 1000
MILLONES**

de usuarios de Internet
protegidos

**MÁS DE
400 MIL**

clientes
corporativos

195

países y
territorios

13

centros de
investigación
y desarrollo
mundiales

ALGUNOS DE NUESTROS CLIENTES



protegido por ESET desde
2017 más de 9.000 endpoints



protegido por ESET desde
2016 más de 4.000 buzones
de correo



protegido por ESET desde
2016 más de 32.000
endpoints



partner de seguridad ISP
desde 2008
base de clientes de 2 millones

RECONOCIMIENTOS



ESET recibió el premio Business Security APPROVED en las Pruebas de seguridad para empresas realizadas en diciembre de 2022 por AV-Comparatives.



ESET obtiene sistemáticamente las mejores clasificaciones en la plataforma global de reseñas de usuarios G2 y sus soluciones son valoradas por clientes de todo el mundo.



ESET recibió la mención Top Player por cuarto año consecutivo en el Cuadrante de Mercado de Radicati para la Protección frente a Amenazas Persistentes Avanzadas de 2023.

