Informe Final

Antivirus ESET CRC

Señores:
Corporación Autónoma Regional del Cauca - CRC

Este documento presenta el informe del cumplimiento de las características técnicas mínimas exigidas por la entidad. Esto corresponde al punto 1.2 Condiciones y especificaciones técnicas de la carta de aceptación No.0395 de 2026.

STAC Tecnología SAS
Nit. 900.593.363-7
Carrera 9 # 1N – 39 - Barrio Modelo
PBX: (+57 2) 8353677
Popayán - Colombia

Informe final antivirus ESET CRC

Se realiza renovación de licenciamiento para 200 equipos del producto ESET Protect Complete con soporte y actualización por un año.

Imagen 1

CUMPLIMIENTO DE CONDICIONES TÉCNICAS EXIGIDAD POR LA CRC

La solución deberá poder realizar exploraciones en estado inactivo para poder brindar de esa forma, una protección proactiva mientras el equipo no está en uso.

• Debe tener un caché local para aumentar el rendimiento de los entornos virtuales, garantizando que el archivo sólo se explora una vez.

• El producto debe tener un control web para limitar el acceso a los sitios web por categoría, además de poderle mostrar al usuario una notificación de bloqueo.

• El bloqueo web deberá poder asignarse por un rango de tiempo, por grupo y por equipo.

• Deberá tener la capacidad de enviar una tarea para la actualización de los parches del sistema operativo.

• Dentro del módulo de firewall deberá contar con la funcionalidad de bloqueo de exploits.

• La solución de antivirus debe ejecutar un escaneo únicamente en los siguientes estados en la computadora:

• Protector de pantalla activo

• Sesión de usuario bloqueada

• Sesión de usuario finalizada

• La solución debe ser capaz de permitir o negar el uso de los dispositivos en base a los siguientes criterios:

• La solución debe ser capaz de definir un listado específico de usuarios quienes pueden hacer uso de los dispositivos. Para dispositivos de almacenamiento, la solución debe permitir configurar únicamente de los siguientes permisos:

➢ Lectura/Escritura

➢ Bloqueo

➢ Solo de lectura

➢ Advertir

• Cuando se conecta o usa un dispositivo de almacenamiento, la solución de antivirus debe proporcionar las siguientes opciones:

➢ Escanear

➢ No realizar ninguna acción

➢ Recordar esta acción

• Sistema de prevención de intrusiones basado en el host (HIPS)

• La solución debe tener sistema de prevención de intrusiones basado en el host. El sistema HIPS debe tener los siguientes modos de configuración:

➢ Modo automático

➢ Modo inteligente

➢ Modo interactivo

➢ Modo basado en políticas

➢ Modo aprendizaje

El aprendizaje automático avanzado o “machine learning” deberá tener cuatro umbrales: Intenso, Balanceado, Cauteloso y Desactivado.

• Debe tener una tarea para aislar a un equipo de la red.

• El HIPS debe incluir una inspección a fondo del comportamiento de todos los programas en ejecución, archivos y llaves de registro

• Debe contar con filtrado para mantener libre de SPAM a los clientes de correo.

• La solución debe capaz de verificar las comunicaciones usando protocolos SSL para hallar amenazas.

• Firewall personal, la solución de antivirus debe contar con un firewall personal. El firewall debe tener los siguientes modos de configuración:

➢ Modo automático

➢ Modo interactivo

➢ Modo basado en políticas

➢ Modo aprendizaje

• Las reglas de firewall creadas deberán ser capaces de permitir todas las siguientes acciones:

➢ Denegar

➢ Permitir

➢ Preguntar

SISTEMAS OPERATIVOS COMPATIBLES

• • Processors Supported

Intel or AMD processor, 64-bit (x64), 1 GHz or higher

ARM64-based processor, 1 GHz or higher

Intel 64-bit, Apple ARM 64-bit

• • Operating Systems

ESET Endpoint Antivirus, ESET Endpoint Security:

Microsoft® Windows® 11

Microsoft® Windows® 10

macOS Big Sur (11) to macOS Tahoe (26)

macOS Big Sur (11) to macOS Sonoma (14)

Ubuntu Desktop 22.04 LTS

Ubuntu Desktop 24.04 LTS

Red Hat Enterprise Linux 8, 9, 10 with supported desktop environment installed.

Linux Mint 21, 22

Debian 12

Debian 13

Android 9 (Pie) and later

ESET Endpoint Encryption Client, ESET Full Disk Encryption*:*

Windows 11 (21H2, 22H2, 23H2, 24H2, 25H2)

Windows 10

Windows Server 2025

Windows Server 2022

Windows Server 2019

Windows Server 2016

macOS Tahoe (26.x)

macOS Sequoia (15.x)

macOS Sonoma (14.x)

macOS Ventura (13.x)

macOS Monterey (12.x)

macOS Big Sur (11.x)

macOS Catalina (10.15)

macOS Mojave (10.14)

- • ESET Mail Security, ESET Server Security:

Microsoft Windows Server 2025 (Server Core and Desktop Experience)

Microsoft Windows Server 2022 (Server Core and Desktop Experience)

Microsoft Windows Server 2019 (Server Core and Desktop Experience)

Microsoft Windows Server 2016

Microsoft Windows Server 2012 R2

Red Hat Enterprise Linux (RHEL) 8

Red Hat Enterprise Linux (RHEL) 9

Red Hat Enterprise Linux (RHEL) 10

Ubuntu Server 22.04 LTS

Ubuntu Server 24.04 LTS

Debian 11

Debian 12

Debian 13

SUSE Linux Enterprise Server (SLES) 15

SUSE Linux Enterprise Server (SLES) 16

Alma Linux 8

Alma Linux 9

Alma Linux 10

Rocky Linux 8

Rocky Linux 9

Rocky Linux 10

Oracle Linux 81

Oracle Linux 91

Oracle Linux 101

Amazon Linux 2023

- • ESET Cloud Office Security

STAC Tecnología SAS
Nit. 900.593.363-7
Carrera 9 # 1N – 39 - Barrio Modelo
PBX: (+57 2) 8353677
Popayán - Colombia

Navegadores compatibles

Mozilla Firefox

Microsoft Edge

Google Chrome

Opera

Safari

Se requiere lo siguiente para comenzar tu protección

- • Planes de suscripción compatibles de Microsoft 365
- • Acceso de administrador a Azure Active Directory (Azure AD)
- • Servicios en la nube de Azure – Exchange | OneDrive | SharePoint | Teams
- • Una cuenta en ESET PROTECT Hub
- • Planes de suscripción compatibles de Google Workspace
- • Acceso de administrador a la cuenta de Google Workspace
- • Una cuenta en ESET PROTECT Hub

De la consola

- • Deberá permitir la ejecución remota de scripts, batch files y paquetes personalizados a través de la consola, de terceros.
- • Deberá ser una solución que pueda ser usada y sea administrable desde la consola de antivirus en sistemas operativos Windows, Linux y Mac.
- • Debe permitir generar grupos de clientes dinámicos y grupos estáticos.

El fabricante debe proporcionar al menos tres diferentes formas de realizar la instalación de la consola de administración:

➢ Instalador todo en uno

➢ Instalación por componentes

➢ Aparato virtual

• El Appliance virtual debe soportar al menos las siguientes plataformas de virtualización:

➢ VMWare vSphere

➢ Oracle Virtual Box

➢ Microsoft Hyper-V

➢ Azure - ambiente basado en la nube

• La consola de Administración deberá estar basada en Cloud.

• Activar el acceso a la consola de antivirus con doble factor de autenticación, deber estar integrada a la misma consola de antivirus, sin ningún add-on o software adicional.

• Debe contar con des instalador de antivirus de terceros.

• Debe contar con un módulo específico para la protección contra ransomware.

• Deberá tener la capacidad para aplicar durante cierto periodo de tiempo las reglas de control de dispositivo y de control de acceso web a través de la consola de administración.

• Deberá contar con etiquetas independiente al LDAP, para identificar y buscar objetos similares.

• Obtener a través de la consola de administración de seguridad del punto final inventario de aplicaciones y de hardware de cada uno de los equipos protegidos.

• A través de la misma consola de administración de seguridad de punto final debe manejar la tecnología de Sandboxing en nube para el análisis de posibles amenazas, cifrado de los discos de almacenamiento de los puntos finales e integrarse con la solución de detección y respuesta del punto final.

• A través de la consola de administración de seguridad del punto final debe ser posible administrar dispositivos móviles iOS y Android.

• Por disponibilidad de la solución de protección de punto final, la consola de administración debe tener la capacidad para construir ambientes distribuidos donde pueda asignarse roles independientes a cada componente, así tener un componente diferente para:

➢ Administrador de equipos móviles.

➢ Distribuidor de actualizaciones, paquetes de instalación y reenvío de comunicación entre el punto final y el servidor.

➢ Detector de puntos finales no administrados.

➢ Y a su vez debe mostrar toda la información en la consola central de administración del punto final de forma nativa.

• La solución debe tener el mecanismo para desinstalar otras soluciones antivirus presentes en el equipo final. Este mecanismo debe ser y estar:

➢ Integrado al paquete de instalación de la solución de protección de punto final.

➢ Disponible solamente a través de la misma consola de administración de protección al punto final.

Endpoint Security For Android

- • La solución de antivirus debe realizar análisis a las aplicaciones instaladas, archivos. DEX.
- • La solución de antivirus ofertada deberá analizar memoria interna y tarjeta SD para cualquier tipo de archivo.
- • Ser capaz de mostrar un listado de las aplicaciones instaladas, controlar el tiempo del uso de aplicaciones y tener el detalle de los permisos que usan los aplicativos del dispositivo móvil.
- • El análisis de la solución de protección de punto final deberá explorar hasta 3 anidados.
- • La protección del dispositivo móvil debe contar con una protección en tiempo real, además de contar con un sistema de reputación de archivos.
- • Deberá poder administrar las aplicaciones que deberían estar instaladas en los dispositivos móviles.
- • Debe tener la capacidad para detectar de forma automática aplicaciones no deseadas y no seguras para usar en el dispositivo móvil.
- • La solución debe poder enviar mensajes SMS al administrador cuando existen usuarios no autorizados manipulando el dispositivo móvil.
- • La solución será capaz de proteger y seleccionar los navegadores a usar.
- • La solución de antivirus deberá ser inteligente para optimizar la batería del dispositivo y ejecutar el análisis al dispositivo únicamente cuando esté completamente cargado o conectado a la energía eléctrica.
- • La solución será capaz de detectar nuevas tarjetas SIM instaladas en el dispositivo y bloquearlas.
- • Es importante que la solución sea capaz de generar códigos de verificación SMS temporales al administrador para ejecutar tareas de desbloqueo de dispositivos o regresar a configuración de fábrica.
- • La solución será capaz de mantener un control de aplicaciones, bloquearlas según los permisos de la aplicación o por categoría, deberá limitarse a instalar aplicaciones únicamente desde Google Play, y poder bloquear cualquier aplicación en el momento que se necesite.
- • La solución será capaz de evitar ataques de suplantación de identidad de sitios web.

STAC Tecnología SAS
Nit. 900.593.363-7
Carrera 9 # 1N – 39 - Barrio Modelo
PBX: (+57 2) 8353677
Popayán - Colombia

Server Security

- • En servidores que usan “OneDrive for Business” debe explorar los archivos almacenados en esta nube, en búsqueda de algún archivo comprometido o posible malware.

- • La solución de protección en servidores debe incluir la detección y bloqueo de intrusiones, agregar a lista negra aquellas direcciones que han sido identificadas con este comportamiento malicioso.

- • La solución deberá agregar de forma automática las exclusiones que correspondan a aplicaciones críticas del servidor.

- • Optimizar el rendimiento de infraestructuras mixtas (hardware y virtuales) siendo capaz de eliminar la duplicidad de exploraciones en archivos, excluyendo los archivos ya explorados y limpios.

Liveguard

- • Uso de Sandboxing en la nube para analizar el comportamiento de archivos.

- • Es posible crear una exclusión por ruta, detección y su hash (SHA-1).

- • Capacidad de sincronizar su licenciamiento con la nube y la consola de administración en sitio o en la nube.

- • Detectar un archivo sospechoso ejecutado por primera vez se debe mostrar una advertencia, si el análisis se completa antes de ejecutar el archivo por primera vez, no se muestra el aviso archivo en análisis.

- • Debe borrar automáticamente las muestras de los archivos/ejecutables en los servidores donde fue analizado el comportamiento.

- • Capacidad para enviar correos SPAM para su análisis.

- • Debe tener únicamente estos umbrales de detección: desconocido, limpio, sospechoso, altamente sospechoso y malicioso.

- • Debe tener la siguiente información de un archivo enviado al Sanboxing en la nube: nombre del equipo desde donde se ingresó el archivo, el usuario que lo ingresó, la razón, hash en SHA-1, nombre del archivo ingresado, tamaño del archivo, categoría.

- • Debe tener protección proactiva, es decir, que el archivo/ejecutable sea bloqueado hasta recibir el resultado del Sandbox en la nube.

- • Se debe tener capacidad para integrarse con la solución de antivirus o protección del punto final, para tener mayores posibilidades de protección y aplicación de políticas.

- • Enviar un archivo/ejecutable a través de una consola de administración del punto final.

- • ESET Liveguard permite la configuración detallada de políticas por equipo, de modo que el administrador puede controlar lo que se envía y lo que debe ocurrir en función del resultado recibido.

STAC Tecnología SAS
Nit. 900.593.363-7
Carrera 9 # 1N – 39 - Barrio Modelo
PBX: (+57 2) 8353677
Popayán - Colombia

Full disk encryption

- • La solución deberá ser capaz de cifrar los Endpoints con sistemas operativos Windows y MacOS.
- • La solución deberá disponer de diversas posibilidades de recuperación de Passwords para usuarios remotos que se vean bloqueados.
- • La solución deberá poder programar las tareas de cifrado sobre los Endpoints deseados con la posibilidad de pausar la ejecución para retomar luego desde el último punto.
- • La solución deberá poder ser administrada desde la misma consola central junto con las otras soluciones descriptas en el TDR.
- • La solución de cifrado debe permitir anular la contraseña de inicio de sesión de la estación de trabajo.

Solución mail security (servidores de correo)

- • La solución deberá Utilizar un motor, para evitar que el spam llegue a los buzones de los usuarios. Incluye validación SPF y DKIM, protección de retrodispersión y protección SMTP.
- • La solución deberá proporcionar la detección de adjuntos sospechosos o maliciosos para evitar que los usuarios se infecten.
- • La solución deberá evitar que los usuarios accedan a páginas web conocidas por phishing analizando los cuerpos de los mensajes y las líneas de asunto para identificar las URL. A continuación, las URL se comparan con la base de datos y las reglas de phishing para decidir si son buenas o malas.
- • La solución deberá permitir que utilice Microsoft Exchange en una configuración híbrida.
- • La solución deberá permitir a los administradores definir manualmente las condiciones de filtrado del correo electrónico y las acciones a tomar con los correos filtrados.

Solución para integración tenant office 365 o google workspace

- • La solución deberá proteger y administrar múltiples inquilinos de Microsoft 365 y Google Workspace desde una sola consola de ESET Cloud Office Security. Azure Active Directory (Azure AD) organiza los objetos, como usuarios y aplicaciones, en grupos llamados inquilinos. Los inquilinos le permiten definir políticas sobre los usuarios y aplicaciones de su organización para cumplir con las políticas de seguridad y operativas.
- • La solución debería utilizar un motor antispam de avanzada que previene intentos de spam y phishing con tasas muy altas de captura. El motor antispam debe alcanzar un resultado de una tasa de captura de spam del 99,99% con cero falsos positivos.
- • La solución deberá evitar que los usuarios accedan a páginas web conocidas por phishing. Mensajes de correo electrónico que pudieran contener enlaces que conducen a páginas web con phishing,

- • La solución debería utilizar un analizador que busca en el cuerpo del mensaje y asunto de los mensajes de correo electrónico entrantes para identificar dichos vínculos (URL).

- • La solución debe ofrecer ajustes de protección basados en políticas, que se pueden asignar a inquilinos, usuarios, grupos del equipo o sitios de SharePoint seleccionados. Puede personalizar las políticas según sus necesidades.

- • La solución debe ofrecer un Dashboard con estadísticas de detección.

- • La solución debe permitir Informes (cuarentena de correo y estadística)

Solución para la gestión y parcheo de vulnerabilidades

- • La solución debe permitir Analizar miles de aplicaciones, como Adobe Acrobat, Mozilla Firefox y Zoom Client, y es compatible con varias versiones de Windows (y, próximamente, de macOS).

- • La solución debe detectar más de 35.000 vulnerabilidades y exposiciones comunes (CVE).

- • La solución debe priorizar y filtra las vulnerabilidades por puntuación de exposición y gravedad.

- • La solución debe permitir sacar Informes de vulnerabilidades del software y los dispositivos más vulnerables.

- • La solución debe admitir multitenencia en entornos de red complejos; permite la visibilidad de vulnerabilidades en partes específicas de la organización.

- • La solución debe tener visión general unificada a través de una única consola, con soporte multilingüe y ligeras exigencias a su infraestructura de TI Gestión de parches.

- • La solución debe permitir lanzar actualizaciones y parches inmediatos a través de opciones personalizables, o de forma manual.

- • La solución debe simplificar el proceso de aplicación de parches: priorizar los activos críticos y programar el resto para las horas de menor actividad para evitar interrupciones.

- • La solución deberá proporcionar un inventario actualizado de parches con nombre del parche, nueva versión de la aplicación, CVE, gravedad/importancia del parche, aplicaciones afectadas.

Soporte

- • El fabricante deberá tener soporte técnico en castellano.

- • Que el fabricante directamente brinde servicios de seguridad informática como por ejemplo penetration testing, vulnerability assessment o análisis de GAP. (Valor adicional al licenciamiento).

- • El fabricante deberá tener la capacidad de ofrecer directamente un servicio de caza de amenazas. (Valor adicional al licenciamiento).

- • Que tenga oficinas de la marca en Latinoamérica y presencia local en el país.

- • El fabricante deberá tener programas de “colaborador seguro” (Valor adicional al licenciamiento).
- • El Fabricante deberá tener un laboratorio de análisis y detección de malware en Latinoamérica.
- • El Fabricante debe tener presencia directa a nivel en Latinoamérica, país y en sitio o ciudad del cliente.
- • El Fabricante deberá haber sido incluido al menos una vez el TOP Rated de AV-Comparativos en los años 2020 y 2021.
- • El Fabricante no deberá tener falsos positivos en las pruebas de AV-Comparativos en los años 2020 y 2021.
- • El Fabricante deberá haber recibido al menos una vez el Gold Award por las pruebas de Performance de AV-Comparativos en los ultimos 3 años.
- • El fabricante debe haber sido considerado "Top Player" en los últimos 3 años (2021 – 2023) dentro del “APT Protection Market Quadrant” de Radicati.
- • El fabricante debe haber ser reconocido como "Champion" dentro de la “Global Cybersecurity Leadership Matrix” de Canalys en los últimos 3 años (2019 – 2021).
- • El Fabricante deberá contar con la certificación ISO 9001 para el departamento de Soporte que brinde el servicio.
- • El Fabricante deberá tener presencia comprobable en Colombia.
- • El Fabricante deberá haber sido considerado al menos una vez como "Outstanding Product" en los Summary Report de AV-Comparatives entre los años 2020 y 2021.
- • El Fabricante deberá haber recibido al menos una vez el Gold Award en la categoría “Performance” en los Summary Report de AV-Comparativos en los años.
- • El Fabricante deberá contar con un portal de entrenamiento y capacitación para todo tipo de usuarios (empresariales, home).
- • El Fabricante debe ser parte de iniciativas que orienten a la sensibilización en ciberseguridad para la comunidad en general en forma de voluntariados o como apoyo a iniciativas de Resposabilidad Social Emnpresarial.
- • El Fabricante no deberá tener sanciones o restricciones a nivel global por parte de entidades de control.

CERTIFICACIONES

- • Certificación expedida por el Mayorista o representante de la marca en Colombia, donde conste que está autorizado a: Comercializar, soportar, y capacitar en el producto mínimo desde hace 10 años.
- • El partner y/o sus ingenieros que darán soporte deben contar con certificaciones de la marca.

SERVICIOS INCLUIDOS DEL PARTNER

- • Capacitación remota
- • Soporte técnico en sitio y remoto ilimitado sin costo durante el licenciamiento.
- • El soporte técnico remoto y en sitio cuando sea necesario y se debe contar con presencia en la ciudad de Popayán, verificable en cámara de comercio del canal para garantizar la atención en el menor tiempo posible.
- • El vendedor debe ofrecer un sistema de atención a incidencias de soporte mediante un portal web, garantizando la atención a casos y realizar respectivo seguimiento a incidentes, enviando información de mesa ayuda y URL de la misma.

Informe realizado por:

Geraldin Vergara Fajardo
Ingeniera de soporte
STAC Tecnología SAS
Celular: 310 859 3122
Correo: soporteingenieria@stac.com.co