"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"

"Año de la Esperanza y el Fortalecimiento de la Democracia"

TERMINOS DE REFERENCIA
CONTRATACION DEL SERVICIO DE SUSCRIPCION DE LICENCIAS DE SOFTWARE ANTIVIRUS

1. AREA QUE REALIZA EL REQUERIMIENTO.
Oficina de Tecnología de Información

2. OBJETO DE LA CONTRATACION
Contratación del Servicio de Suscripción de Licencias de Software Antivirus.

3. ACTIVIDAD VINCULADA AL POI
Con el presente servicio se podrá dar cumplimiento al Plan Operativo Institucional – POI del presente ejercicio en la actividad operativa Monitoreo e Implementación de Soluciones Tecnológicas de Sistemas Informáticos para la Entidad.

4. FINALIDAD PÚBLICA
El presente proceso permitirá continuar las condiciones de seguridad de los usuarios que usan los equipos de cómputo de la entidad, a fin de cumplir con las funciones asignadas de conformidad con lo regulado en el Reglamento de la Organización y Funciones - ROF de la Entidad, aprobado mediante el Decreto Supremo N° 006-2015-MTC, en su artículo 34°, señala las funciones de la Oficina de Tecnología de Información.

5. OBJETIVO DE LA CONTRATACIÓN
- Objetivo General: Proteger la infraestructura informática de la entidad ante ataques informáticos que pudieran causar perdida de información.

- Objetivo Especifico: Mantener los recursos informáticos protegidos ante diferentes tipos de infección cibernética.

6. ALCANCES Y DESCRIPCIÓN DEL SERVICIO

ITEM	DESCRIPCION	UNIDAD DE MEDIDA	CANTIDAD
01	Suscripción Anual de Software de antivirus para mil cuatrocientos (1,400) equipos de computo de la entidad	Servicio	01

6.1 Instalación y Puesta en Funcionamiento
El contratista deberá de realizar la implementación, configuración y funcionamiento del software antivirus, considerando por ello lo siguiente:

1. Los trabajos programados serán supervisados por el personal de la Oficina Tecnología de Información.
2. Instalación de la herramienta para la sede principal de la SUTRAN.
3. Instalación de la consola principal, además de subconsolas de ser el caso, las cuales serán determinadas por la Oficina de Tecnología de la Información.
4. Instalación y configuración del software de antivirus en las estaciones de trabajo de la entidad, ubicados en la Sede Principal y Sub Sedes de SUTRAN.
5. Toda la solución debe estar basada únicamente en software, la solución no deberá incluir la adquisición de ningún tipo de equipamiento adicional como complemento de este.
6. El software no debe afectar lentitud en los equipos de cómputo conectados a la Red de la SUTRAN.
7. Asimismo, el software antivirus a adquirir deberá contar como mínimo las siguientes características técnicas.

6.2 Requerimientos del fabricante

1. El fabricante debe ser una empresa de confianza y estar presente en el negocio de ciberseguridad durante al menos 20 años.
2. Los expertos del fabricante deben tener experiencia comprobada en el descubrimiento de vulnerabilidades y campañas de APTs a nivel global.
3. El proveedor debe poseer una variedad de servicios de inteligencia de seguridad que demuestren fortaleza general en el dominio
4. El fabricante debe tener un grupo experto de investigación de amenazas dedicado para la región LATAM.

6.3 Consola de administración – características

1. La solución debe disponer de una consola de gestión centralizada que permita la instalación, configuración, actualización y administración de todas las soluciones ofertadas de manera integral, facilitando la gestión unificada de la seguridad tanto en modalidad On-Premise como en la Nube.
2. Se debe acceder a la consola On-Premise vía WEB (HTTPS), MMC.
3. Compatibilidad con Windows Failover clustering u otra solución de alta disponibilidad en el caso de consola On-Premise.
4. Capacidad de eliminar remotamente cualquier solución de seguridad (propia o de terceros) que esté presente en las estaciones y servidores.
5. Capacidad de instalar remotamente la solución en las estaciones y servidores Windows, a través de la administración compartida, login script y/o GPO de Active Directory.
6. Capacidad de gestionar estaciones de trabajo y servidores (tanto Windows como Linux y Mac) protegidos por la solución.
7. Capacidad de gestionar smartphones y tablets (tanto Android y iOS) protegidos por la solución.
8. Capacidad de generar paquetes personalizados (autoejecutables) conteniendo la licencia y configuraciones del producto.
9. Capacidad de actualizar los paquetes de instalación con las últimas vacunas, para que cuando el paquete sea utilizado en una instalación ya contenga las últimas vacunas lanzadas.
10. Capacidad de monitorear diferentes subnets de red con el objetivo de encontrar máquinas nuevas para que sean agregadas a la protección.
11. Capacidad de monitorear grupos de trabajos ya existentes y cualquier grupo de trabajo que sea creado en la red, a fin de encontrar máquinas nuevas para ser agregadas a la protección.
12. Capacidad de, al detectar máquinas nuevas en el Active Directory, subnets o grupos de trabajo, automáticamente importar la máquina a la estructura de protección de la consola y verificar si tiene el antimalware instalado. En caso de no tenerlo, debe instalar el antimalware automáticamente.
13. Capacidad de agrupamiento de máquinas por características comunes entre ellas, por ejemplo: agrupar todas las máquinas que no tengan el antimalware instalado, agrupar todas las máquinas que no recibieron actualización en los últimos 2 días, etc.
14. Capacidad de definir políticas de configuraciones diferentes por grupos de estaciones, permitiendo que sean creados subgrupos y con función de herencia de políticas entre grupos y subgrupos.
15. Capacidad de importar la estructura de Active Directory para encontrar máquinas.
16. Debe permitir bloquear que el usuario cambie las configuraciones de la solución instalada en las estaciones y servidores.
17. Capacidad de reconectar máquinas clientes al servidor administrativo más próximo, basado en reglas de conexión como:
    - Cambio de gateway;
    - Cambio de subnet DNS;

- Cambio de dominio;
- Cambio de servidor DHCP;
- Cambio de servidor DNS;
- Cambio de servidor WINS;
- Aparición de nueva subnet;

18. Capacidad de configurar políticas móviles para que cuando una computadora cliente esté fuera de la estructura de protección pueda actualizarse vía internet.
19. Capacidad de instalar otros servidores administrativos para balancear la carga y optimizar el tráfico de enlaces entre sitios diferentes.
20. Solución debe tener la capacidad de manejar jerarquía de consolas con bases de datos independientes y debe ser multinivel, esto es tener la consola principal (maestra) y otras secundarias (esclavas).
21. Capacidad de interrelacionar servidores en estructura de jerarquía para obtener informes sobre toda la estructura de endpoints.
22. Capacidad de herencia de políticas en la estructura jerárquica de servidores administrativos.
23. Capacidad de elegir cualquier computadora cliente como repositorio de actualización y de paquetes de instalación, sin que sea necesario la instalación de un servidor administrativo completo, donde otras máquinas clientes se actualizarán y recibirán paquetes de instalación, con el fin de optimizar el tráfico de red.
24. Capacidad de hacer de este repositorio de actualización un Gateway para conexión con el servidor de administración, para que otras máquinas que no logran conectarse directamente al servidor puedan usar este gateway para recibir y enviar informaciones al servidor administrativo.
25. Capacidad de exportar informes para los siguientes tipos de archivos: PDF, HTML y XML.
26. Capacidad de generar traps SNMP para monitoreo de eventos.
27. Capacidad de enviar correos electrónicos para cuentas específicas en caso de algún evento.
28. Debe tener documentación de la estructura del banco de datos para generación de informes a partir de herramientas específicas de consulta
29. (Crystal Reports, por ejemplo).
30. Capacidad de conectar máquinas vía Wake on Lan para realización de tareas (barrido, actualización, instalación, etc.), inclusive de máquinas que estén en subnets diferentes del servidor).
31. Capacidad de realizar inventario de hardware de todas las máquinas clientes.
32. Capacidad de realizar inventario de aplicativos de todas las máquinas clientes.
33. Capacidad de diferenciar máquinas virtuales de máquinas físicas.
34. La solución debe ser capaz de integrarse con soluciones SIEM.
35. La solución debe poder enviar notificaciones por correo electrónico.
36. La solución debe tener diferentes funciones de administrador que tengan una única interfaz / tablero durante el inicio de sesión y controladas por privilegios y derechos en función de sus roles (Administrador, Revisor, Investigador, etc.).
37. La solución debe responder rápidamente en caso de una epidemia de virus, activando una política alternativa preconfigurada desde la consola de administración, donde cualquier configuración del agente de protección pueda ser modificada (desde reglas de firewall, hasta control de aplicativos, dispositivos y acceso a web).
38. La solución debe contar con doble factor de autenticación.
39. La solución debe admitir el inicio de sesión único (SSO) mediante NTLM y Kerberos.
40. La solución debe distribuir automáticamente los equipos a grupos de administración (si aparecen nuevos equipos en la red). Debe brindar la capacidad de establecer las reglas de transferencia o movimiento según la dirección IP, el

tipo de sistema operativo y la ubicación en las unidades organizativas de Active Directory.

41. La solución debe proporcionar la administración centralizada de los almacenamientos de respaldo y cuarentena en todos los recursos de red donde esté instalado el agente de protección.
42. La solución debe tener la funcionalidad para crear múltiples perfiles dentro de una política de protección con diferentes configuraciones de protección que puedan estar activas simultáneamente en uno o varios dispositivos según las siguientes reglas de activación:
    - Estado del dispositivo
    - Etiquetas
    - Directorio activo
    - Propietarios del dispositivo
    - Hardware
43. La solución debe tener la capacidad de definir un rango de direcciones IP, con el fin de limitar el tráfico de clientes hacia el servidor de administración en función del tiempo y la velocidad.
44. La solución debe permitir al administrador establecer un período de tiempo después del cual un ordenador no conectado al servidor de administración, sus datos relacionados se eliminan automáticamente del servidor.
45. La solución debe tener una herramienta para recopilar de forma remota los datos necesarios para la resolución de problemas desde los puntos finales, sin necesidad de acceso físico.
46. La solución debe permitir al administrador crear un túnel de conexión entre un dispositivo cliente remoto y el servidor de administración si el puerto utilizado para la conexión al servidor de administración no está disponible en el dispositivo.
47. La solución debe tener una funcionalidad integrada para conectarse de forma remota al punto final mediante la tecnología de uso compartido de escritorio de Windows. Además, la solución debe poder mantener la auditoría de las acciones del administrador durante la sesión.
48. La solución debe incluir soporte para la implementación basada en nube a través de:
    - Amazon Web Services
    - Microsoft Azure

6.4 Compatibilidad

La solución propuesta debe ser compatible con la instalación en los siguientes sistemas operativos:

1. Windows Server 2008 R2 Standard with Service Pack 1 and later 64-bit
2. Windows Server 2012 Server Core 64-bit
3. Windows Server 2012 Datacenter 64-bit
4. Windows Server 2012 Essentials 64-bit
5. Windows Server 2012 Foundation 64-bit
6. Windows Server 2012 Standard 64-bit
7. Windows Server 2012 R2 Server Core 64-bit
8. Windows Server 2012 R2 Datacenter 64-bit
9. Windows Server 2012 R2 Essentials 64-bit
10. Windows Server 2012 R2 Foundation 64-bit
11. Windows Server 2012 R2 Standard 64-bit
12. Windows Server 2016 Datacenter (LTSB) 64-bit
13. Windows Server 2016 Standard (LTSB) 64-bit
14. Windows Server 2016 Server Core (Installation Option) (LTSB) 64-bit
15. Windows Server 2019 Standard 64-bit
16. Windows Server 2019 Datacenter 64-bit
17. Windows Server 2019 Core 64-bit

18. Windows Server 2022 Standard 64-bit
19. Windows Server 2022 Datacenter 64-bit
20. Windows Server 2022 Core 64-bit
21. Windows Storage Server 2012 64-bit
22. Windows Storage Server 2012 R2 64-bit
23. Windows Storage Server 2016 64-bit
24. Windows Storage Server 2019 64-bit
25. Debian GNU/Linux 10.x (Buster) 64-bit
26. Debian GNU/Linux 11.x (Bullseye) 64-bit
27. Debian GNU/Linux 12 (Bookworm) 64-bit
28. Ubuntu Server 18.04 LTS (Bionic Beaver) 64-bit
29. Ubuntu Server 20.04 LTS (Focal Fossa) 64-bit
30. Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64-bit
31. CentOS 7.x 64-bit
32. CentOS Stream 9 64-bit
33. Red Hat Enterprise Linux Server 7.x 64-bit
34. Red Hat Enterprise Linux Server 8.x 64-bit
35. Red Hat Enterprise Linux Server 9.x 64-bit
36. SUSE Linux Enterprise Server 12 (all Service Packs) 64-bit
37. SUSE Linux Enterprise Server 15 (all Service Packs) 64-bit
38. Astra Linux Special Edition RUSB.10015-01 (operational update 1.6) 64-bit
39. Astra Linux Special Edition RUSB.10015-01 (operational update 1.7) 64-bit
40. Astra Linux Common Edition (operational update 2.12) 64-bit
41. ALT SP Server 10 64-bit
42. ALT Server 10 64-bit
43. ALT Server 9.2 64-bit
44. ALT 8 SP Server (LKNV.11100-01) 64-bit
45. ALT 8 SP Server (LKNV.11100-02) 64-bit
46. ALT 8 SP Server (LKNV.11100-03) 64-bit
47. Oracle Linux 7 64-bit
48. Oracle Linux 8 64-bit
49. Oracle Linux 9 64-bit
50. RED OS 7.3 Server 64-bit
51. RED OS 7.3 Certified Edition 64-bit
52. ROSA COBALT 7.9 64-bit

La solución propuesta debe soportar los siguientes servidores de bases de datos:

1. Microsoft SQL Server 2012 Express 64-bit
2. Microsoft SQL Server 2014 Express 64-bit
3. Microsoft SQL Server 2016 Express 64-bit
4. Microsoft SQL Server 2017 Express 64-bit
5. Microsoft SQL Server 2019 Express 64-bit
6. Microsoft SQL Server 2014 (all editions) 64-bit
7. Microsoft SQL Server 2016 (all editions) 64-bit
8. Microsoft SQL Server 2017 (all editions) on Windows 64-bit
9. Microsoft SQL Server 2017 (all editions) on Linux 64-bit
10. Microsoft SQL Server 2019 (all editions) on Windows 64-bit (requires additional actions)
11. Microsoft SQL Server 2019 (all editions) on Linux 64-bit (requires additional actions)
12. Microsoft Azure SQL Database
13. All supported SQL Server editions in Amazon RDS and Microsoft Azure cloud platforms
14. MySQL 5.7 Community 32-bit/64-bit
15. MySQL Standard Edition 8.0 (release 8.0.20 and later) 32-bit/64-bit

16. MySQL Enterprise Edition 8.0 (release 8.0.20 and later) 32-bit/64-bit
17. MariaDB 10.1 (build 10.1.30 and later) 32-bit/64-bit
18. MariaDB 10.3 (build 10.3.22 and later) 32-bit/64-bit
19. MariaDB 10.4 (build 10.4.26 and later) 32-bit/64-bit
20. MariaDB 10.5 (build 10.5.17 and later) 32-bit/64-bit
21. MariaDB Server 10.3 32-bit/64-bit with InnoDB storage engine
22. MariaDB Galera Cluster 10.3 32-bit/64-bit with InnoDB storage engine
23. PostgreSQL 13.x 64-bit
24. PostgreSQL 14.x 64-bit
25. Postgres Pro 13.x (all editions)
26. Postgres Pro 14.x (all editions)

Linux:

1. MySQL 5.7 Community 32-bit/64-bit
2. MySQL 8.0 32-bit/64-bit
3. MariaDB 10.4 (build 10.4.26 and later) 32-bit/64-bit
4. MariaDB 10.5 (build 10.5.17 and later) 32-bit/64-bit
5. MariaDB Galera Cluster 10.3 32-bit/64-bit with InnoDB storage engine
6. PostgreSQL 13.x 64-bit
7. PostgreSQL 14.x 64-bit
8. 10.4.2.1.8 PostgreSQL 15.x 64-bit
9. 10.4.2.1.9 Postgres Pro 13.x 64-bit (all editions)
10. Postgres Pro 14.x 64-bit (all editions)
11. Postgres Pro 15.x 64-bit (all editions)
12. Platform V Pangolin 5.4.0 64-bit

La solución propuesta debe soportar las siguientes plataformas virtuales:

Windows:

1. VMware vSphere 6.7
2. VMware vSphere 7.0
3. VMware Workstation 16 Pro
4. Microsoft Hyper-V Server 2012 64-bit
5. Microsoft Hyper-V Server 2012 R2 64-bit
6. Microsoft Hyper-V Server 2016 64-bit
7. Microsoft Hyper-V Server 2019 64-bit
8. Microsoft Hyper-V Server 2022 64-bit
9. Citrix XenServer 7.1 LTSR
10. Citrix XenServer 8.x
11. Parallels Desktop 17
12. Oracle VM VirtualBox 6.x

Linux:

1. VMware vSphere 6.7
2. VMware vSphere 7.0
3. VMware vSphere 8.0
4. VMware Workstation 16 Pro
5. VMware Workstation 17 Pro
6. Microsoft Hyper-V Server 2012 64-bit
7. Microsoft Hyper-V Server 2012 R2 64-bit
8. Microsoft Hyper-V Server 2016 64-bit
9. Microsoft Hyper-V Server 2019 64-bit
10. Microsoft Hyper-V Server 2022 64-bit
11. Citrix XenServer 7.1 LTSR
12. Citrix XenServer 8.x

13. Parallels Desktop 17
14. Oracle VM VirtualBox 6.x
15. Oracle VM VirtualBox 7.x
16. Kernel-based Virtual Machine (all Linux operating systems supported by Administration server)

6.5 Sistemas Windows

Características:

1. La solución debe incluir los siguientes componentes dentro de un único agente de protección:
2. Antimalware de archivos
3. Antimalware web
4. Antimalware de correo electrónico
5. Firewall
6. Protección de ataques de red
7. IPS de host (para estaciones de trabajo)
8. Autoprotección (contra ataques a los servicios/procesos del antimalware)
9. Control de dispositivos externos
10. Control de acceso a sitios web
11. Control de ejecución de aplicativos
12. Control de vulnerabilidades de windows y de los aplicativos instalados.
13. Administración de parches de Windows.
14. Cifrado
15. La solución debe ser capaz de detectar los siguientes tipos de amenazas: virus (incluidos los polimórficos), gusanos, troyanos, puertas traseras, rootkits, spyware, adware, ransomware, keyloggers, crimeware, sitios y enlaces de phishing, vulnerabilidades de día cero y otros software maliciosos y no deseados.
16. La solución debe proporcionar tecnologías de protección de última generación como: la protección contra amenazas sin archivos, provisión de protección basada en aprendizaje automático (ML) de múltiples capas y análisis de comportamiento durante las diferentes etapas de la cadena de ataque.
17. La solución debe usar ML estático para la pre-ejecución y ML dinámico para las etapas post-ejecución del kill chain.
18. La solución debe soportar la detección basada en firmas además de la detección asistida por la nube y heurística.
19. La solución debe ser compatible con la interfaz de escaneo antimalware (AMSI).
20. La solución debe contar con protección Anti-Ransonware que actué de forma proactiva ante un proceso de cifrado en las carpetas de red compartidas. Esta capacidad Anti-Ransonware debe permitir la definición granular de las carpetas a proteger en los servidores.
21. La solución debe incluir un componente dedicado a escanear conexiones cifradas.
22. La solución debe poder descifrar y escanear el tráfico de red transmitido a través de conexiones cifradas.
23. La solución debe permitir anular y reparar las acciones maliciosas que han sido realizadas por el malware, en el sistema operativo, antes de ser detectado.
24. Capacidad de elegir qué módulos se instalarán, tanto en instalación local como en la instalación remota.
25. Capacidad de detección de presencia de antimalware de otro fabricante que pueda causar incompatibilidad, bloqueando la instalación.
26. Las actualizaciones de firmas deben ser actualizadas por el fabricante y estar disponibles a los usuarios, como máximo cada hora, independientemente del nivel de las amenazas encontradas en el período (alto, medio o bajo).
27. Capacidad de agregar carpetas/archivos para una zona de exclusión, con el fin de excluirlos de la verificación. Capacidad, también, de agregar objetos a la lista de

exclusión de acuerdo con el resultado del antimalware, (ej.: "Win32.Trojan.banker") para que cualquier objeto detectado con el resultado elegido sea ignorado.

28. Posibilidad de deshabilitar automáticamente barridos agendados cuando la computadora esté funcionando mediante baterías (notebooks).
29. Capacidad de pausar automáticamente barridos agendados en caso de que otros aplicativos necesiten más recursos de memoria o procesamiento.
30. Capacidad de verificar solamente archivos nuevos y modificados.
31. Antes de cualquier intento de desinfección o exclusión permanente, el antimalware debe realizar un respaldo del objeto.
32. La solución debe incorporar tecnología de autoprotección del agente de protección:
    - Protección contra la gestión remota no autorizada de un servicio de la aplicación.
    - Protección del acceso a los parámetros de la aplicación mediante el establecimiento de una contraseña.
    - Prevención de la desactivación de la protección por parte de malware, delincuentes o usuarios aficionados.
33. La solución debe responder rápidamente en caso de una epidemia de virus, activando una política alternativa preconfigurada desde la consola de administración, donde cualquier configuración del agente de protección pueda ser modificada (desde reglas de firewall, hasta control de aplicativos, dispositivos y acceso a web).
34. La solución debe permitir detectar y bloquear acciones que no son típicas de los equipos (estaciones de trabajo) en la red empresarial utilizando un conjunto de reglas (escenarios habituales de actividad maliciosa) para supervisar un comportamiento inusual. Estas reglas deben funcionar en modo aprendizaje por al menos dos semanas y luego bloquear o permitir
35. La solución debe incluir un componente de control capaz de aprender a reconocer el comportamiento típico del usuario en estaciones de trabajo, y luego identificar y bloquear acciones anómalas y potencialmente dañinas realizadas por ese equipo o usuario.
36. La solución debe ser capaz de bloquear ataques de red e informar la fuente del ataque.
37. La solución debe incluir protección contra ataques que exploten vulnerabilidades en el protocolo ARP para falsificar la dirección MAC.
38. Capacidad de distinguir diferentes subnets y brindar opción de activar o no el firewall para una subnet específica.
39. Debe tener módulo IDS/IPS para protección contra port scans y exploración de vulnerabilidades de software.
40. El módulo de Firewall debe contener, como mínimo, dos conjuntos de reglas:
    - Filtrado de paquetes: donde el administrador podrá elegir puertas, protocolos o direcciones de conexión que serán bloqueadas/permitidas;
    - Filtrado por aplicativo: donde el administrador podrá elegir cuál aplicativo, grupo de aplicativo, fabricante de aplicativo, versión de aplicativo o nombre de aplicativo tendrá acceso a la red, con la posibilidad de elegir qué puertas y protocolos podrán ser utilizados.
41. Capacidad de verificar correos electrónicos recibidos y enviados en los protocolos POP3, IMAP, NNTP, SMTP y MAPI, así como conexiones cifradas (SSL) para POP3 y IMAP (SSL).
42. Capacidad de verificar enlaces introducidos en correos electrónicos contra phishings.
43. En caso de que el correo electrónico contenga código que parece ser, pero no es definitivamente malicioso, este debe mantenerse en cuarentena.
44. Capacidad de filtrar adjuntos de correos electrónicos, borrándolos o renombrándolos de acuerdo con la configuración hecha por el administrador.

45. Capacidad de modificar los puertos monitoreadas por los módulos de web y correo electrónico.
46. En la verificación de tráfico web, en caso de que se encuentre código malicioso el programa debe:
    - Bloquear la amenaza.
    - Notificar al usuario, con un mensaje de la amenaza, y permitiendo la descarga del objeto.
47. Posibilidad de agregar sitios web en una lista de exclusión, donde no serán verificados por el antimalware de web.
48. Debe tener módulo de bloqueo de Phishing, con actualizaciones incluidas en las vacunas, obtenidas por Anti-Phishing Working Group (http://www.antiphishing.org/).
49. Capacidad de agregar aplicativos a una lista de "aplicativos confiables", donde las actividades de red, actividades de disco y acceso al registro de Windows no serán monitoreadas.
50. Capacidad de limitar el acceso de los aplicativos a recursos del sistema, como claves de registro y carpetas/archivos del sistema, por categoría, fabricante o nivel de confianza del aplicativo.
51. La solución debe tener la capacidad de restringir las actividades de las aplicaciones dentro del sistema según el nivel de confianza asignado a la aplicación, y limitar los derechos de las aplicaciones para acceder a ciertos recursos, incluidos los archivos del sistema y de los usuarios (funcionalidad HIPS).
52. La solución debe bloquear la ejecución de aplicaciones prohibidas, que están en listas negras, y bloquear la ejecución de aplicaciones que no están en listas blancas. Por tanto, la autorización y denegación de aplicaciones haciendo uso de listas blancas y listas negras debe realizarse sin recurrir a la supervisión de procesos en el sistema operativo del endpoint.
53. La solución debe permitir la ejecución de aplicaciones basadas en sus certificados de firma digital, MD5, SHA256, META Data, File Path y categorías de seguridad predefinidas.
54. La solución debe soportar un modo de prueba (para el control de aplicaciones) con generación de informes sobre el lanzamiento de aplicaciones bloqueadas, para facilitar posterior configuración en modo bloqueo.
55. Debe tener módulo que habilite o no el funcionamiento de los siguientes dispositivos externos, como mínimo:
    - Discos de almacenamiento locales
    - Almacenamiento extraíble
    - Impresoras
    - CD/DVD
    - Drives de disquete
    - Modems
    - Wi-Fi
    - Adaptadores de red externos
    - Dispositivos MTP
    - Dispositivos Bluetooth
    - Cámaras y escáneres
56. Capacidad de liberar acceso a un dispositivo específico y usuarios específicos por un período de tiempo específico, sin la necesidad de deshabilitar la protección, sin deshabilitar el gerenciamiento central o de intervención local del administrador en la máquina del usuario.
57. Capacidad de limitar la escritura y lectura en dispositivos de almacenamiento externo por usuario.
58. Capacidad de limitar la escritura y lectura en dispositivos de almacenamiento externo por agendamiento.
59. Capacidad de configurar las reglas de control de dispositivos por Hardware ID, modelo y máscara del dispositivo.

60. La solución debe proporcionar una función Anti-Bridging para las estaciones de trabajo de Windows a fin de evitar puentes no autorizados a la red interna que eludan las herramientas de protección perimetral. Los administradores deben poder prohibir el establecimiento de conexiones simultáneas por cable, Wi-Fi y módem.
61. La solución debe ser capaz de registrar operaciones de archivos (escritura y eliminación) en dispositivos de almacenamiento USB. Esto no debería requerir la instalación de ninguna licencia o componente adicional en el punto final.
62. La solución debe tener la capacidad de bloquear la ejecución de cualquier archivo ejecutable desde el dispositivo de almacenamiento USB.
63. Capacidad de limitar el acceso a sitios web de internet por categoría, por contenido (video, audio, etc.), con posibilidad de configuración por usuario o grupos de usuarios y agendamiento.
64. La solución debe tener una categoría de detección específica para bloquear los banners del sitio web.
65. La solución debe soportar políticas basadas en el usuario para el control de dispositivos, web y aplicaciones.
66. La solución debe realizar un borrado remoto de datos en sistemas operativos Windows (estaciones de trabajo), mediante tareas o comandos enviados desde la consola central y ejecutados por el agente de protección. Debe contar con al menos dos modos de eliminación de datos: inmediata y pospuesta (al activarse alguna condición).
67. La solución debe tener las siguientes funciones de borrado remoto de datos:
    - En modo silencioso
    - En discos duros y unidades extraíbles
    - Para todas las cuentas de usuario en la computadora
68. La funcionalidad de borrado remoto de datos debe admitir los siguientes métodos de eliminación de datos:
    - Eliminación mediante el uso de los recursos operativos: los archivos se eliminan, pero no se envían a la papelera de reciclaje.
    - Eliminación completa, sin recuperación: es prácticamente imposible restaurar los datos después de la eliminación.

6.6 Compatibilidad

Estaciones de trabajo

1. Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1 or later
2. Windows 8 Professional / Enterprise
3. Windows 8.1 Professional / Enterprise
4. Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise / Enterprise multi-session
5. Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise

Servidores

1. Windows Small Business Server 2011 Essentials / Standard (64-bit)
2. Windows MultiPoint Server 2011 (64-bit)
3. Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1 or later
4. Windows Web Server 2008 R2 Service Pack 1 or later
5. Windows Server 2012 Foundation / Essentials / Standard / Datacenter (including Core Mode)
6. Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter (including Core Mode)
7. Windows Server 2016 Essentials / Standard / Datacenter (including Core Mode)
8. Windows Server 2019 Essentials / Standard / Datacenter (including Core Mode)

9. Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (including Core Mode)

6.7 Sistemas Linux

Características:

1. La solución debe incluir los siguientes componentes dentro de un único agente de protección:
2. Antimalware de archivos
3. Antimalware web
4. Gestión del firewall
5. Autoprotección (contra ataques a los servicios/procesos del antimalware)
6. Control de dispositivos externos
7. Control de ejecución de aplicativos
8. La solución debe ser capaz de detectar los siguientes tipos de amenazas: virus (incluidos los polimórficos), gusanos, troyanos, puertas traseras, rootkits, spyware, adware, ransomware, keyloggers, crimeware, sitios y enlaces de phishing, vulnerabilidades de día cero y otros software maliciosos y no deseados.
9. La solución debe proporcionar tecnologías de protección de última generación como: la protección contra amenazas sin archivos, provisión de protección basada en aprendizaje automático (ML) de múltiples capas y análisis de comportamiento durante las diferentes etapas de la cadena de ataque.
10. La solución debe usar ML estático para la pre-ejecución y ML dinámico para las etapas post-ejecución del kill chain.
11. La solución debe soportar la detección basada en firmas además de la detección asistida por la nube y heurística.
12. Capacidad de configurar el permiso de acceso a las funciones del antimalware con, como mínimo, opciones para las siguientes funciones:
    - Gerenciamiento de estatus de tareas (iniciar, pausar, parar o reanudar tareas);
    - Gerenciamiento de respaldo: Creación de copias de los objetos infectados en un reservorio de respaldo antes del intento de desinfectar o eliminar tal objeto, siendo de esta manera posible la recuperación de objetos que contengan informaciones importantes.
    - Gerenciamiento de cuarentena: Cuarentena de objetos sospechosos y corrompidos, guardando tales archivos en una carpeta de cuarentena;
    - Verificación por agendamiento: búsqueda de archivos infectados y sospechosos (incluyendo archivos dentro de un rango especificado); análisis de archivos; desinfección o eliminación de objetos infectados.
13. En caso de errores, debe tener capacidad de crear logs automáticamente, sin necesidad de otros softwares.
14. Capacidad de pausar automáticamente barridos agendados en caso de que otros aplicativos necesiten más recursos de memoria o procesamiento.
15. Capacidad de verificar objetos usando heurística.
16. Control de dispositivos conectados con limitaciones de tiempo y de usuario a través de Samba Active Directory y Microsoft Active Directory en la tarea Control de dispositivos.
17. Administración del acceso de los usuarios a los dispositivos instalados o conectados por tipo de dispositivo y buses de conexión.
18. Escaneo del tráfico HTTP / HTTPS y FTP entrante del equipo del usuario y la detección de direcciones web maliciosas y suplantación de identidad (phishing).
19. Debe permitir controlar la ejecución de aplicaciones por medio de la aplicación de listas blancas y listas negras.
20. La solución debe proporcionar escaneo de memoria del kernel para estaciones de trabajo Linux.

21. La solución debe tener componentes dedicados para monitorear, detectar y bloquear actividades en servidores y estaciones de trabajo, para proteger contra ataques de cifrado remoto.
22. La solución debe incluir la capacidad de configurar y administrar configuraciones de firewall integradas en los sistemas operativos, a través de su consola de administración.
23. La solución debe tener la capacidad de priorizar tareas de escaneo personalizadas y a demanda.
24. La solución debe ser capaz de bloquear ataques de red e informar la fuente del ataque.
25. La solución debe incluir protección contra ataques que exploten vulnerabilidades en el protocolo ARP para falsificar la dirección MAC.
26. La solución debe proteger sus archivos en los directorios locales contra el cifrado malicioso remoto. Si la solución considera que las acciones de un equipo remoto constituyen un cifrado malicioso, este dispositivo se agrega a una lista de dispositivos no confiables y pierde el acceso a los directorios de red compartidos.

6.8 Compatibilidad

Sistemas de 32 bits:

1. CentOS 6.7 and later
2. Debian GNU / Linux 11.0 and later
3. Debian GNU / Linux 12.0 and later
4. Mageia 4
5. Red Hat Enterprise Linux 6.7 and later
6. ALT 8 SP Workstation.
7. ALT 8 SP Server.
8. ALT Workstation 10
9. ALT SP Workstation release 10

Sistemas de 64 bits

1. AlmaLinux OS 8 and later.
2. AlmaLinux OS 9 and later.
3. AlterOS 7.5 and later.
4. Amazon Linux 2.
5. Astra Linux Common Edition 2.12.
6. Astra Linux Special Edition RUSB.10015-01 (operational update 1.5).
7. Astra Linux Special Edition RUSB.10015-01 (operational update 1.6).
8. Astra Linux Special Edition RUSB.10015-01 (operational update 1.7).
9. Astra Linux Special Edition RUSB.10015-16 (release 1) (operational update 1.6)
10. CentOS 6.7 and later
11. CentOS 7.2 and later.
12. CentOS Stream 8.
13. CentOS Stream 9.
14. Debian GNU/Linux 11.0 and later.
15. Debian GNU/Linux 12.0 and later.
16. EMIAS 1.0 and later.
17. EulerOS 2.0 SP5.
18. Kylin 10.
19. Linux Mint 20.3 and up.
20. Linux Mint 21.1 and later.
21. OpenSUSE Leap 15.0 and later.
22. Oracle Linux 7.3 and later.
23. Oracle Linux 8.0 and later.
24. Oracle Linux 9.0 and later.
25. Red Hat Enterprise Linux 6.7 and later

26. Red Hat Enterprise Linux 7.2 and later.
27. Red Hat Enterprise Linux 8.0 and later.
28. Red Hat Enterprise Linux 9.0 and later.
29. Rocky Linux 8.5 and later.
30. Rocky Linux 9.1.
31. SberLinux 8.8 (Dykhtau).
32. SUSE Linux Enterprise Server 12.5 or later.
33. SUSE Linux Enterprise Server 15 or later.
34. Ubuntu 20.04 LTS.
35. Ubuntu 22.04 LTS.
36. ALT 8 SP Workstation.
37. ALT 8 SP Server.
38. ALT Workstation 10
39. ALT Server 10.
40. ALT SP Workstation release 10.
41. ALT SP Server release 10.
42. Atlant, Alcyone build, version 2022.02.
43. GosLinux 7.17.
44. GosLinux 7.2.
45. MSVSPHERE 9.2 SERVER.
46. MSVSPHERE 9.2 ARM.
47. RED OS 7.3.
48. ROSA Cobalt 7.9.
49. ROSA Chrome 12.
50. SynthesisM Client 8.6.
51. SynthesisM Server 8.6.

Sistemas de 64 bits ARM

1. Astra Linux Special Edition RUSB.10152-02 (operational update 4.7).
2. CentOS Stream 9.
3. EulerOS 2.0 SP8.
4. SUSE Linux Enterprise Server 15.
5. Ubuntu 22.04 LTS.
6. ALT Workstation 10.
7. ALT Server 10.
8. ALT SP Workstation release 10.
9. ALT SP Server release 10.
10. RED OS 7.3.

6.9 Estaciones Mac OS X

Características:

1. Debe proporcionar protección residente para archivos (antispyware, antitroyano, antimalware, etc.) que verifique cualquier archivo creado, accedido o modificado;
2. La solución debe ser capaz de detectar los siguientes tipos de amenazas: virus (incluidos los polimórficos), gusanos, troyanos, puertas traseras, rootkits, spyware, adware, ransomware, keyloggers, crimeware, sitios y enlaces de phishing, vulnerabilidades de día cero y otros software maliciosos y no deseados.
3. La solución debe proporcionar tecnologías de protección de última generación como: la protección contra amenazas sin archivos, provisión de protección basada en aprendizaje automático (ML) de múltiples capas y análisis de comportamiento durante las diferentes etapas de la cadena de ataque.
4. La solución debe usar ML estático para la pre-ejecución y ML dinámico para las etapas post-ejecución del kill chain.

5. La solución debe soportar la detección basada en firmas además de la detección asistida por la nube y heurística.
6. Capacidad de elegir de qué módulos se instalarán, tanto en instalación local como en la instalación remota.
7. Las vacunas deben ser actualizadas por el fabricante y estar disponibles a los usuarios, como máximo cada hora, independientemente del nivel de las amenazas encontradas en el período (alto, medio o bajo).
8. Capacidad de volver a la base de datos de la vacuna anterior.
9. Capacidad de agregar carpetas/archivos para una zona de exclusión, con el fin de excluirlos de la verificación. Capacidad, también, de agregar objetos a la lista de exclusión de acuerdo con el resultado del antimalware, (ej.: "Win32.Trojan.banker") para que cualquier objeto detectado con el resultado elegido sea ignorado.
10. Posibilidad de deshabilitar automáticamente barridos agendados cuando la computadora esté funcionando mediante baterías (notebooks).
11. Capacidad de verificar objetos usando heurística.
12. Antes de cualquier intento de desinfección o exclusión permanente, el antimalware debe realizar un respaldo del objeto.
13. Capacidad de verificar archivos de formato de correo electrónico.
14. Posibilidad de trabajar con el producto por la línea de comando, con como mínimo opciones para actualizar las vacunas, iniciar un barrido, para el antimalware e iniciar el antimalware por la línea de comando.
15. Capacidad de ser instalado, removido y administrado por la misma consola central de gestión.

6.10 Compatibilidad

Mac Intel o Mac Sillon

6.11 Smartphones y tablets

Características:

1. La solución debe poder administrar y monitorear dispositivos móviles desde la misma consola que se usa para administrar computadoras y servidores.
2. La solución debe poder escanear archivos abiertos en el dispositivo.
3. La solución debe poder escanear programas instalados desde la interfaz del dispositivo.
4. La solución debe poder escanear objetos del sistema de archivos en el dispositivo o en tarjetas de extensión de memoria conectadas a pedido del usuario o según un cronograma.
5. La solución propuesta debe permitir la protección del sistema de archivos del teléfono inteligente y la interceptación y el escaneo de todos los objetos entrantes transferidos a través de conexiones inalámbricas.
6. La solución debe proporcionar el aislamiento confiable de objetos infectados en una ubicación de almacenamiento de cuarentena.
7. La solución debe incluir la actualización de bases de datos antivirus utilizadas para buscar programas maliciosos y eliminar objetos peligrosos.
8. La solución debe poder escanear dispositivos móviles en busca de malware y otros objetos no deseados a pedido y según un cronograma y tratarlos automáticamente.
9. La solución debe tener la capacidad de bloquear sitios maliciosos diseñados para difundir códigos maliciosos y sitios web de phishing diseñados para robar datos confidenciales del usuario y acceder a la información financiera del usuario.
10. La solución debe tener la funcionalidad de agregar un sitio web excluido del escaneo a una lista de permitidos.
11. La solución debe incluir el filtrado de sitios web por categorías y permitir al administrador restringir el acceso del usuario a categorías específicas (por

ejemplo, sitios web relacionados con juegos de azar o categorías de redes sociales).

12. La solución debe permitir al administrador obtener información sobre el funcionamiento del antimalware y la protección web en el dispositivo móvil del usuario.
13. La solución debe tener la funcionalidad para detectar y notificar al administrador sobre ataques al dispositivo (rooteo).
14. La solución debe permitir al administrador tomar una fotografía (Mugshot) desde la cámara frontal del móvil cuando este se encuentre bloqueado.
15. La solución debe permitir restablecer el PIN de un dispositivo móvil de forma remota.
16. La solución debe proporcionar una funcionalidad antirrobo, de modo que los dispositivos perdidos o desplazados se puedan ubicar, bloquear y borrar de forma remota.
17. La solución debe proporcionar la posibilidad de bloquear el lanzamiento de aplicaciones prohibidas en el dispositivo móvil.
18. La solución debe poder aplicar configuraciones de seguridad, como restricciones de contraseñas y cifrado, en dispositivos móviles.
19. La solución debe tener la capacidad de enviar aplicaciones recomendadas o requeridas por el administrador al teléfono móvil.
20. La solución debe tener un control de aplicaciones con los modos de aplicación prohibida o permitida.
21. La solución debe incluir la opción de enrolar dispositivos mediante sistemas EMM de terceros:
    - VMware AirWatch 9.3 o posterior
    - MobileIron 10.0 o posterior
    - IBM MaaS360 10.68 o posterior
    - Microsoft Intune 1908 o posterior
    - SOTI MobiControl 14.1.4 (1693) o posterior
22. La solución debe permitir la configuración de nombres de puntos de acceso (APN) para conectar un dispositivo móvil a servicios de transferencia de datos en una red móvil.
23. La solución debe ofrecer controles para garantizar que todos los dispositivos cumplan con los requisitos de seguridad corporativos. El control de cumplimiento debe basarse en un conjunto de reglas que deben incluir los siguientes componentes:
    - Criterios de verificación del dispositivo
    - Plazo asignado para que el usuario solucione el incumplimiento
    - Acción que se tomará en el dispositivo si el usuario no soluciona el incumplimiento dentro del plazo establecido
    - Capacidad para remediar los dispositivos que no cumplen con las normas
24. La solución debe tener la funcionalidad de borrar de forma remota lo siguiente de los dispositivos android: datos en contenedores, cuentas de correo electrónico corporativas, configuraciones para conectarse a la red Wi-Fi corporativa y VPN, Nombre del punto de acceso (APN), Perfil de Android for Work, Contenedor KNOX y Clave de KNOX License Manager.
25. La solución debe ser compatible con todos los métodos de implementación que se indican a continuación para el agente móvil:
    - Google Play, Huawei App Gallery y Apple App Store
    - Portal de inscripción móvil KNOX
    - Paquetes de instalación preconfigurados independientes
26. Para el caso de dispositivos iOS la solución debe:
    - Brindar protección contra amenazas en línea para dispositivos iOS.
    - Tener la funcionalidad para detectar y notificar al administrador sobre ataques al dispositivo (rooteo, jailbreak).

- Tener la funcionalidad de borrar de forma remota lo siguiente: todos los perfiles de configuración y de aprovisionamiento, el perfil MDM de iOS y aplicaciones para las que se ha seleccionado la casilla de verificación Eliminar.

6.12 Compatibilidad:

1. Apple iOS 10.0 o superior.
2. iPad OS 13 o superior.
3. Android 5 o superior

6.13 Cifrado de datos

Características:

1. La solución debe admitir el cifrado para estaciones de trabajo Windows.
2. La solución debe admitir el cifrado en varios niveles:
   - Cifrado de disco completo, incluido el disco del sistema
   - Cifrado de archivos y carpetas
   - Cifrado de medios extraíbles
   - Gestionar el cifrado de BitLocker y MacOS Filevault.
3. La solución debe ofrecer una funcionalidad de cifrado a nivel de archivo (FLE) integrada que permita:
   - El cifrado de archivos en unidades de computadora locales.
   - La creación de listas de cifrado de archivos por extensión o grupo de extensiones.
   - La creación de listas de cifrado de carpetas en unidades de computadora locales.
4. La solución debe ofrecer una funcionalidad de cifrado a nivel de archivo (FLE) integrada que permita el cifrado de archivos en unidades extraíbles. Esto debe incluir la capacidad de:
   - Especificar una regla de cifrado predeterminada por la cual la aplicación aplica la misma acción a todas las unidades extraíbles.
   - Configurar reglas de cifrado para archivos almacenados en unidades extraíbles individuales.
5. La solución propuesta debe ofrecer una funcionalidad de cifrado a nivel de archivo (FLE) integrada que admita varios modos de cifrado de archivos para unidades extraíbles:
   - El cifrado de todos los archivos almacenados en unidades extraíbles
   - El cifrado de archivos nuevos solo cuando se guardan o crean en unidades extraíbles.
6. La solución propuesta debe ofrecer la funcionalidad de cifrado de nivel de archivo (FLE) integrado que permita cifrar los archivos en unidades extraíbles en modo portátil. Debe permitir el acceso a archivos cifrados en unidades extraíbles que estén conectadas a equipos sin funcionalidad de cifrado.
7. La solución propuesta debe ofrecer la funcionalidad de cifrado de nivel de archivo (FLE) integrado que permita cifrar todos los archivos que aplicaciones específicas puedan crear o modificar, tanto en discos duros como en unidades extraíbles.
8. La solución propuesta debe ofrecer la funcionalidad de cifrado de nivel de archivo (FLE) integrado que permita la gestión de reglas de acceso de aplicaciones a archivos cifrados, incluida la definición de una regla de acceso a archivos cifrados para cualquier aplicación. Debe permitir el bloqueo del acceso a archivos cifrados o permitir el acceso a archivos cifrados solo como texto cifrado.
9. La solución propuesta debe ofrecer la capacidad de restaurar dispositivos cifrados si un disco duro cifrado o una unidad extraíble está dañado.
10. La solución propuesta debe ofrecer la funcionalidad de cifrado de disco completo (FDE) integrado para discos duros y unidades extraíbles. Al igual que con FLE,

debe existir la capacidad de especificar una regla de cifrado predeterminada mediante la cual la aplicación aplique la misma acción a todas las unidades extraíbles o de configurar reglas de cifrado para unidades extraíbles individuales.

11. La solución propuesta debe ofrecer un módulo de cifrado que se administre de manera centralizada en todas las computadoras, con la capacidad de aplicar políticas de cifrado y modificar o detener las configuraciones de cifrado.
12. La solución propuesta debe ofrecer la capacidad de monitorear de manera centralizada el estado del cifrado y generar informes sobre las computadoras o dispositivos cifrados.
13. La solución propuesta debe ofrecer un cifrado que sea completamente transparente para los usuarios finales y que no tenga un impacto adverso en el rendimiento y el uso del sistema.
14. La solución propuesta debe ofrecer cifrado de disco completo que admita la administración centralizada de usuarios autorizados, incluida la adición, eliminación y restablecimiento de contraseñas. Solo los usuarios autorizados deben tener permiso para iniciar el disco cifrado.
15. La solución propuesta debe tener la capacidad de bloquear el acceso de la aplicación a los datos cifrados si es necesario.
16. La solución propuesta debe admitir el cifrado automático de dispositivos de almacenamiento extraíbles y debe poder evitar que los datos se copien a medios no cifrados.
17. La solución propuesta debe proporcionar una función para crear contenedores protegidos con contraseña que se puedan usar para intercambiar datos con usuarios externos.
18. La solución propuesta debe proporcionar una ubicación central para el almacenamiento de claves de cifrado y múltiples opciones de recuperación.
19. El servidor de administración o administrador de la solución propuesta debe tener la capacidad de descifrar todos los datos cifrados, independientemente de la ubicación o el usuario.
20. La solución propuesta debe admitir tanto los diseños de teclado QWERTY como AZERTY para la autorización previa al arranque.
21. La solución propuesta debe admitir la autorización previa al arranque para los siguientes dispositivos: Safe Net eToken 4100, Gemalto IDPrime .NET (511), Rutoken ECP Flash.
22. La solución propuesta debe proporcionar la funcionalidad para personalizar la configuración de cifrado de Microsoft BitLocker, lo que incluye:
    - Uso del módulo de plataforma segura y la configuración de contraseñas.
    - Uso de cifrado de hardware para estaciones de trabajo y cifrado de software si el cifrado de hardware no está disponible.
    - Uso de autenticación que requiere la entrada de datos en un entorno previo al arranque, incluso si la plataforma no tiene la capacidad para la entrada previa al arranque (por ejemplo, con teclados de pantalla táctil en tabletas).
23. La solución propuesta debe admitir el cifrado en tabletas Microsoft Surface.

6.14 Gestión de sistemas:

Características:

1. La solución debe tener la capacidad de gestión de sistemas aplicable a plataformas Windows.
2. La solución debe incluir funciones para administrar computadoras de forma
3. remota, entre ellas:
    - Instalación remota de software de terceros
    - Generación de informes sobre el software y el hardware existentes
    - Eliminación de software no autorizado
4. Capacidad de detectar software de Microsoft y de terceros vulnerables, creando así un informe de software vulnerables.

5. Capacidad de corregir las vulnerabilidades de software de cualquier proveedor, haciendo el download centralizado o descentralizado de la corrección o actualización y aplicando esa corrección o actualización en las máquinas gestionadas de manera transparente para los usuarios. (opcional).
6. Permite la planificación de fecha y hora para el despliegue de parches y actualizaciones, discriminando PCs y Servidores.
7. Sincronización con Microsoft Update, para el despliegue centralizado de Parches y actualizaciones Microsoft.
8. La solución debe proporcionar la posibilidad de seleccionar qué parches se descargarán o enviarán a los puntos finales, en función de su criticidad. (opcional)
9. La solución debe proporcionar informes completos sobre las vulnerabilidades descubiertas y los parches faltantes, así como sobre los puntos finales y el estado de implementación de los parches.
10. La solución debe permitir al administrador aprobar actualizaciones.
11. La solución debe poder identificar automáticamente los parches faltantes en los puntos finales individuales e implementar solo los que sean necesarios o falten. (opcional)
12. La solución debe tener la funcionalidad de compatibilidad con el modo de prueba de parches. (opcional)
13. La solución propuesta debe permitir que el administrador configure reglas para la instalación de parches o actualizaciones de Microsoft y de terceros: (opcional)
    - Iniciar la instalación al reiniciar o apagar la computadora.
    - Instalar los requisitos generales del sistema necesarios.
    - Permitir la instalación de nuevas versiones de aplicaciones durante las actualizaciones.
14. Descargar actualizaciones al dispositivo sin instalarlas. (opcional)
15. La solución debe incluir campos dedicados que contengan información sobre "Exploit encontrado para la vulnerabilidad".
16. La solución debe incluir campos dedicados que contengan información sobre "Amenaza encontrada para la vulnerabilidad".
17. La solución debe poder implementar o enviar archivos EXE, MSI, bat, cmd y MSP de forma remota, y permitir que el administrador defina el parámetro de línea de comandos para la instalación remota.
18. Capacidad de gestionar licencias de software de terceros.
19. Utilización de Puntos de distribución para el despliegue de parches y actualizaciones en entornos WAN para reducir la utilización de ancho de banda. (opcional)
20. Capacidad de gestionar un inventario de hardware, con la posibilidad de registro de dispositivos (ej.: router, switch, proyector, accesorio, etc.), informando fecha de compra, lugar donde se encuentra, service tag, número de identificación y otros.
21. Capacidad de registro de información adicional en los activos de la empresa mediante campos personalizados.

6.15 EDR

Características:

1. El agente EDR debe tener integración con la aplicación Endpoint Protection, es decir debe constituir un agente único.
2. La solución sugerida debe complementar la información del veredicto con los artefactos del sistema sobre la detección.
3. La solución sugerida debe admitir la generación automática de indicadores de compromiso (IoC) después de que se produzca la detección con la capacidad de aplicar una acción de respuesta.

4. La solución debe tener la capacidad de forzar la ejecución de un escaneo de IoC en todos los puntos finales con agentes EDR instalados.
5. La solución debe admitir la ejecución de análisis de IoC de acuerdo a una planificación indicada por el administrador o analista.
6. La solución debe admitir escaneos mediante IoCs utilizando un conjunto de IoC generado automáticamente y además importado de terceros en formato OpenIoC para detectar amenazas no detectadas anteriormente.
7. La solución debe admitir la exportación de IoC generado por la solución a un archivo en formato OpenIoC.
8. La solución debe permitir la visibilidad detallada del incidente relacionada con la amenaza detectada en un endpoint.
9. La información detallada del incidente debe incluir al menos la siguiente información de la amenaza detectada:
    - Gráfico de la cadena de desarrollo de amenazas (kill chain).
    - Información sobre el dispositivo en el que se detecta la amenaza (nombre, dirección IP, dirección MAC, lista de usuarios, sistema operativo).
    - Información general sobre la detección, incluido el modo de detección.
    - Cambios de registro asociados a la detección.
    - Historial de presencia de archivos en el dispositivo.
    - Acciones de respuesta realizadas por la aplicación.
10. El gráfico de la cadena de desarrollo de amenazas (kill chain) debe proporcionar información visual sobre los objetos involucrados en el incidente, por ejemplo, sobre procesos clave en el dispositivo, conexiones de red, bibliotecas, registro, etc.
11. La información de un incidente debe presentar una vista detallada de los artefactos del sistema y los datos relacionados con el incidente para el análisis de la causa raíz:
    - Proceso de spawning
    - Conexiones de red
    - Cambios en el registro
    - Descarga de archivos
    - Dropped de objetos
12. El agente EDR debe tener un mecanismo de autodefensa para evitar que el agente modifique archivos relacionados con el agente / entradas de componentes del sistema, etc.
13. La solución sugerida debe admitir al menos las siguientes acciones de respuesta que un administrador puede realizar cuando se detectan amenazas:
    - Impedir la ejecución de objetos (para Windows y mac)
    - Aislamiento del equipo
    - Eliminar objeto del host o grupo de hosts
    - Terminar un proceso en el dispositivo
    - Poner en cuarentena un objeto (para Windows y mac)
    - Ejecución remota de programas/procesos/comandos
    - Iniciar escaneo de IoC para un grupo de hosts.
14. La solución debe admitir la detección automatizada de actividad maliciosa mediante tecnologías sandbox para sistemas windows y mac.
15. La solución sugerida debe admitir la integración con el portal de inteligencia de amenazas, que contiene y muestra información sobre la reputación de los archivos y las URL.

6.16 Compatibilidad

Sistemas listados en el ítem de compatibilidad con sistemas Windows, Linux y Mac.

6.17 Protección para MS Office 365 (opcional)

a) La Solución de Seguridad debe integrarse con Microsoft Office 365 de manera nativa mediante Microsoft Office 365 API sin influir ni requerir cambios en los flujos de tráfico de correo electrónico.
b) La solución debe disponer de una consola de gestión que permita la configuración y administración multi-usuario de todas las capacidades ofertadas de manera integral, facilitando la gestión de la seguridad en Microsoft Office 365.
c) La solución no debe requerir cambio alguno en los registros MX de correo o en las aplicaciones de Microsoft Office 365 para su funcionamiento.
d) La solución debe de validar de Spam, Phishing, Ransomware, BEC, amenazas conocidas y desconocidas en tiempo real para correos electrónicos entrantes, salientes y aquellos que fluyen internamente en la propia instancia de Microsoft Office 365.
e) La solucion debe utilizar heurística avanzada, aislamiento de procesos, aprendizaje automático y otras tecnologías de última generación para proteger a las empresas que utilizan Microsoft Exchange Online, Microsoft Teams, Microsoft OneDrive y Microsoft SharePoint Online contra el ransomware, archivos adjuntos maliciosos, spam, phishing, correos electrónicos que comprometen la seguridad de la empresa (BEC) y amenazas desconocidas.
f) La solución debe cumplir con el Reglamento General de Protección de Datos (RGDP) y protección de los datos.
g) La solución debe de contar con tecnologías de detección Anti-Spam, AntiPhishing, Anti-Malware, Anti-Ransomware, Anti-BEC & capacidades de filtrado de contenido.
h) La solución debe de contar con tecnologías proactivas para la detección de amenazas avanzadas o de día 0.
i) La solución debe de contar con tecnologías de detección avanzadas para la detección y neutralización de amenazas del tipo Ransomware.
j) La solución debe disponer de capacidades de escaneo bajo demanda sobre buzones de correo pudiendo seleccionar.
    1. Grupos de usuarios
    2. Usuarios
    3. Todos los usuarios
k) La solución debe poder clasificar los correos basura en dos categorías: Spam y correos masivos y poder definir las acciones a tomarse en cada uno de los casos.
l) La solución debe contar con capacidades de generar direcciones de lista blanca y negra para cada uno de los módulos de seguridad que propone.
m) La solución debe disponer de funciones de validación y autentificación del remitente de manera automática que incluyan:
    1. DKIM
    2. DMARK
    3. SPF
n) La solución debe de disponer de modulo anti malware para la detección oportuna de amenazas conocidas, desconocidas y avanzadas en Microsoft Exchange Online, Microsoft OneDrive, Microsoft SharePoint Online y Microsoft Teams bajo tecnologías de:
    1. Firmas
    2. Análisis heurísticos
    3. Comportamiento.
o) La solucion debe de disponer una visibilidad unificada de las amenazas detectadas por los sevicios de seguridad base de Microsoft Exchange Online mediante la visualizacion de una cuarentena unica.
p) Debe contar con cuadros de mandos, KPIs y reportes de seguimientos de las detecciones realizadas.
q) La solución no debe almacenar datos sensibles como usuarios y contraseñas y para esto debe de poder integrase con Microsoft Office 365 mediante OAuth 2.0

r) La protección de anti-malware para Microsoft SharePoint Online debe permitir la exclusión y selección de sitios protegidos.
s) La protección de anti-malware para Microsoft OneDrive debe permitir la exclusión y selección de usuarios protegidos.
t) Debe contar con protección frente a virus, troyanos y otras clases de malware para MS Teams.
u) Debe disponer de un módulo de supervisión de fuga de datos con el objetivo del descubrimiento de información confidencial transmitida y almacenada por los usuarios en los buzones de correo de Exchange Online, en los almacenamientos de OneDrive y en los sitios de SharePoint Online de la organización relacionadas con datos de tarjetas de crédito.
v) La solución debe contar con capacidades de escaneo retrospectivo de amenazas que incluya los buzones de correo y de Ms Office 365 y los repositorios de datos de OneDrive.
w) Debe contar con protección basada en firmas mediante aprendizaje automático junto con análisis conductuales y heurísticos avanzados.
x) Debe usar una combinación de SPF (marco de directivas de remitente), DKIM (DomainKeys Identified Mail), validación de correo electrónico de DMARC (Autenticación de mensajes, informes y conformidad basada en dominios) y el método de detección de similitudes para detectar y prevenir spoofing y phishing de correos electrónicos, ataques BEC y spam.
y) Debe proveer heurística mediante redes neurales de aprendizaje profundo.
z) Debe incluir protección contra ataques de inyección de código y mailsploit/spoofing que son posibles debido a los errores de los clientes de correo.
aa) Debe contar con mecanismo de detección de spam al nivel de la dirección IP.

6.18 Plataforma de entrenamiento (opcional)

a) La solución propuesta debe incluir formación en ciberseguridad dentro de la aplicación.
b) La solución propuesta debe dividir el entrenamiento en varios módulos, donde cada uno de los modulo debe estar en una serie de secciones.
c) Los módulos propuestos deben incluir teoría relevante y capacidad de realizar tareas interactivas en un entorno simulado.
d) La solución propuesta debe permitir descargar un certificado que acredite los logros una vez completadas todas las secciones de un módulo.
e) La solución propuesta debe ser 100% en nube
f) Los módulos propuestos deben ser de entrenamientos en ciberseguridad diagnósticos entre los que se encuentren Respuestas a Incidentes, Software Malicioso, Aseguramiento de Directorio Activo y Seguridad para servidores, entre otros.

6.19 SOPORTE TÉCNICO

a) Soporte y actualización de licencias antivirus por el periodo de ejecución del servicio.
b) El contratista debe contar con soporte técnico 24x7x365 con la posibilidad de escalar casos técnicos en cualquier momento hacia la casa matriz haciendo uso del sistema del fabricante.
c) El contratista brindará los datos como números telefónicos y correos electrónicos para las coordinaciones y comunicación con la Entidad.
d) Si en caso la llamada realizada por el personal de soporte técnico no tuviera éxito en contactarse, se procederá a enviar un correo electrónico que deberá asignar el contratista para la atención inmediata, una vez realizado él envió el contratista tendrá que devolver la llamada en un tiempo máximo de 180 minutos.
e) Si se presenta cualquier incidencia o vulnerabilidad en la red de la solución de seguridad del contrato, el área usuaria reportará la incidencia a través de correo

electrónico y el contratista tendrá un tiempo de respuesta de 04 horas como máximo desde reportada la incidencia, para dar solución a la incidencia reportada.

f) El proveedor podrá brindar el soporte de forma remota, para lo cual se le brindará el acceso respectivo para evaluar la incidencia y atenderla. Luego de atendida la incidencia, el proveedor deberá remitir un correo electrónico indicando la culminación de la atención.

g) En caso la incidencia no pueda ser atendida de forma remota, el proveedor asignará un técnico el cual se apersonará a las instalaciones de la Entidad, dentro de las 24 horas siguientes de ser reportada la incidencia.

6.20 CONSIDERACIONES PARA LA EJECUCIÓN DEL SERVICIO

a) A fin de poder elaborar su mejor propuesta, el contratista podrá realizar una visita a la Oficina de Tecnología de Información y solicitar la información pertinente, durante los horarios de oficina (8:30 am – 5:30 pm), a fin de obtener un mejor conocimiento de la implementación, equipamiento técnico, necesidades de configuración de los equipos u otros componentes, que tengan que incluir en la implementación y ejecución del requerimiento.

b) El contratista deberá garantizar la operatividad de los servicios ininterrumpido durante el período de inicio de la implementación.

c) El software de antivirus provisto por el contratista debe cumplir con las características técnicas propuestas.

7. REQUISITOS DE CALIFICACION

Perfil

- Persona natural o jurídica.

Requisitos

- Contar con Registro Único de Contribuyente (RUC) vigente.
- Contar con Registro Nacional de Proveedores (RNP) vigente cuando el SERVICIO es superior a una (01) UIT.
- No tener impedimento para contratar con el Estado.
- El Postor deberá acreditar la autorización o representación otorgada por el fabricante de las licencias ofertadas mediante una carta simple

Experiencia

El postor debe acreditar un monto facturado acumulado equivalente a S/ 50,000.00 (Cincuenta mil y 00/100 Soles), por la contratación de servicios iguales o similares al objeto de la contratación, durante los cinco (05) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.

Nota: La experiencia requerida se acreditará de la siguiente forma: (i) contratos u órdenes de compra, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con voucher de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por Entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago.

Se considerarán prestaciones similares: Servicios de instalación de soluciones de software de antivirus o de venta de licencias de software antivirus.

PERSONAL CLAVE

UN (01) ESPECIALISTA

FORMACIÓN ACADÉMICA

Profesional Técnico en Redes y Comunicaciones Titulado, o Bachiller, o Titulado como: Ingeniero Eléctrico o Ingeniero Electrónico o Ingeniero Industrial o Ingeniero de Sistemas o Ingeniero Informático o Ingeniero de Software o Ingeniero Industrial.

CAPACITACIÓN

Curso relacionado a la configuración de Sistemas de software de antivirus corporativo, otorgada por el fabricante del software de antivirus propuesto.

Acreditación:

Se deberá adjuntar constancias y/o certificados que acrediten la capacitación.

EXPERIENCIA

Deberá contar con tres (03) años de experiencia en actividades relacionadas a la configuración de antivirus como especialista en sistemas de software de antivirus corporativo.

Acreditación:

La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.

8. PLAZO DE INSTALACIÓN E IMPLEMENTACION DEL SERVICIO

La implementación del servicio deberá coincidir con la finalización del servicio actual, la cual vence el 23 de diciembre de 2026.

Culminado la configuración y despliegue del software antivirus, el contratista emitirá un acta de despliegue y configuración de las licencias desplegadas el cual estará suscrita por el personal de OTI y el proveedor. En caso surjan observaciones, estás deberán ser plasmadas en dicha acta, teniendo un plazo de tres (03) días calendario para absolver y/o resolver dichas observaciones.

9. LUGAR DE PRESTACION DEL SERVICIO

El servicio se ejecutará en las instalaciones propias de la SUTRAN ubicada en la Av. Avenida Arenales Nº 452 Lima – Perú y/o fuera de SUTRAN.

10. ENTREGABLES POR EL SERVICIO

Una vez culminada la configuración y despliegue del software antivirus se suscribirá un acta de despliegue y configuración de las licencias, para ello el proveedor deberá entregar la siguiente documentación técnica:

- Acta de despliegue y configuración de las licencias.

El informe que corresponde ser presentado por el contratista, podrá ser remitido a la Sede Central de la SUTRAN, ubicada en la dirección: **Av. Arenales Nro. 452, distrito de Jesús María, provincia y departamento de Lima** y/o a través de mesa de partes virtual: http://virtual.sutran.gob.pe/mesa- departes- virtual.html

11. PLAZO DE PRESTACION DE SERVICIO

El plazo de prestación del servicio será de trecientos sesenta y cinco (365) días, el cual iniciará a la firma del Acta de despliegue y configuración de las licencias.

12. FORMA DE PAGO

El pago se realizará en una sola armada, culminado el despliegue y configuración de las licencias y la previa conformidad por parte de la Oficina de Tecnología de Información.

13. PENALIDAD

En caso de retraso injustificado del contratista en la ejecución de las prestaciones objeto del contrato, la entidad contratante le aplica automáticamente una penalidad por mora por cada día de atraso que le sea imputable. La penalidad se aplica automáticamente y se calcula de acuerdo al artículo 120 del Reglamento de la Ley N°32069, Ley General de Contrataciones Públicas, conforme a la siguiente fórmula:

Penalidad diaria = 0.10 x monto / F x plazo	*Donde F tiene los siguientes valores: Para bienes y servicios: F = 0.40*

14. CONFORMIDAD

La conformidad será emitida por la Oficina de Tecnología de Información, dentro de un plazo hasta cinco (05) días hábiles, contados a partir del día siguiente de recepcionado el comprobante de pago respectivo del proveedor.

15. RESOLUCIÓN DEL CONTRATO POR INCUMPLIMIENTO

Cualquiera de las partes puede resolver el contrato, de conformidad con el numeral 68.1 del artículo 68 de la Ley N° 32069, Ley General de Contrataciones Públicas. De encontrarse en alguno de los supuestos de resolución del contrato, LAS PARTES procederán de acuerdo con lo establecido en el artículo 122 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado mediante Decreto Supremo N° 009-2025-EF.

16. CUMPLIMIENTO

Son causales de resolución de contrato la presentación con información inexacta o falsa de la Declaración Jurada de Prohibiciones e Incompatibilidades a que se hace referencia en la Ley de prevención y mitigación del conflicto de intereses en el acceso y salida de personal del servicio público. Asimismo, en caso se incumpla con los impedimentos señalados en el artículo 5 de dicha ley se aplicará la inhabilitación por cinco años para contratar o prestar servicios al Estado, bajo cualquier modalidad

17. CONFIDENCIALIDAD

El proveedor guardará, bajo responsabilidad a que hubiere lugar, estricta confidencialidad respecto de la información a la que acceda para la realización de sus actividades, así como de la información que produzca, la cual es de propiedad de la SUTRAN. Queda prohibida la utilización de la información proporcionada para un fin distinto al contratado, así como expresamente se prohíbe su divulgación por cualquier medio.

18. ANTICORRUPCION

EL CONTRATISTA declara y garantiza no haber ofrecido, negociado, prometido o efectuado ningún pago o entrega de cualquier beneficio o incentivo ilegal, de manera directa o indirecta, a los evaluadores del proceso de contratación o cualquier servidor de la entidad contratante. Asimismo, EL CONTRATISTA se obliga a mantener una conducta proba e íntegra durante la vigencia del contrato, y después de culminado el mismo en caso existan controversias pendientes de resolver, lo que supone actuar con probidad, sin cometer actos ilícitos, directa o indirectamente. Aunado a ello, EL CONTRATISTA se obliga a abstenerse

de ofrecer, negociar, prometer o dar regalos, cortesías, invitaciones, donativos o cualquier beneficio o incentivo ilegal, directa o indirectamente, a funcionarios públicos, servidores públicos, locadores de servicios o proveedores de servicios del área usuaria, de la dependencia encargada de la contratación, actores del proceso de contratación y/o cualquier servidor de la entidad contratante, con la finalidad de obtener alguna ventaja indebida o beneficio ilícito. En esa línea, se obliga a adoptar las medidas técnicas, organizativas y/o de personal necesarias para asegurar que no se practiquen los actos previamente señalados. Adicionalmente, EL CONTRATISTA se compromete a denunciar oportunamente ante las autoridades competentes los actos de corrupción o de inconducta funcional de los cuales tuviera conocimiento durante la ejecución del contrato con LA ENTIDAD CONTRATANTE. Tratándose de una persona jurídica, lo anterior se extiende a sus accionistas, participacioncitas, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores o cualquier persona vinculada a la persona jurídica que representa; comprometiéndose a informarles sobre los alcances de las obligaciones asumidas en virtud del presente contrato.

Finalmente, el incumplimiento de las obligaciones establecidas en esta cláusula, durante la ejecución contractual, otorga a LA ENTIDAD CONTRATANTE el derecho de resolver total o parcialmente el contrato. Cuando lo anterior se produzca por parte de un proveedor adjudicatario de los catálogos electrónicos de acuerdo marco, el incumplimiento de la presente cláusula conllevará que sea excluido de los Catálogos Electrónicos de Acuerdo Marco. En ningún caso, dichas medidas impiden el inicio de las acciones civiles, penales y administrativas a que hubiera lugar.

19. GESTIÓN DE RIESGOS:

LAS PARTES realizan la gestión de riesgos de acuerdo con lo establecido en el presente contrato y los documentos que lo conforman, a fin de tomar decisiones informadas, aprovechando el impacto de riesgos positivos y disminuyendo la probabilidad de los riesgos negativos y su impacto durante la ejecución contractual, considerando la finalidad pública de la contratación.

20. GARANTÍAS:

No corresponde.

21. SOLUCIÓN DE CONTROVERSIAS:

Las controversias que surjan entre las partes durante la ejecución del contrato se resuelven mediante conciliación, conforme a lo establecido en Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas".