

# Guía de ManageEngine para implementar la norma de seguridad de la información ISO 27001 en su organización



# Tabla de contenido

|                                                                             |    |
|-----------------------------------------------------------------------------|----|
| Una breve introducción a la norma ISO 27001:2022                            | 3  |
| Entonces, ¿por qué ISO 27001?                                               | 4  |
| La estructura de la norma ISO 27001:2022                                    | 5  |
| Las cláusulas de la ISO 27001                                               | 5  |
| Los controles y objetivos de control de la norma ISO 27001                  | 7  |
| El rol de ManageEngine en su viaje de cumplimiento de la ISO 27001          | 8  |
| Productos de ManageEngine correlacionados con los controles de la ISO 27001 | 8  |
| A.5 Controles organizacionales                                              | 8  |
| A.6 Controles de personas                                                   | 31 |
| A.7 Controles físicos                                                       | 33 |
| A.8 Controles tecnológicos                                                  | 34 |
| Los productos de ManageEngine y los controles de la ISO 27001 compatibles   | 50 |
| Tome el control de su TI                                                    | 51 |

## Aviso legal

Copyright © Zoho Corporation Pvt. Ltd. Todos los derechos reservados Este material y su contenido ("Material") están previstos, entre otras cosas, presentar un resumen general de cómo puede usar los productos y servicios de ManageEngine para implementar los controles de la ISO 27001:2022 en su organización. Cumplir completamente con la norma ISO 27001:2022 requiere una variedad de soluciones, procesos, personas y tecnologías. Las soluciones mencionadas en este Material son algunas de las formas en que las herramientas de gestión de TI pueden ayudar con algunos de los controles de la ISO 27001. Junto con otras soluciones, procesos y personas adecuados, las soluciones de ManageEngine ayudan a las organizaciones a cumplir con la norma ISO 27001:2022. Este Material se da solo para fines informativos y no debe considerarse como una asesoría legal para implementar la norma ISO 27001:2022. ManageEngine no da garantía alguna, expresa, implícita o reglamentaria, y no asume responsabilidad o compromiso alguno con respecto a la información de este Material.

No puede copiar, reproducir, distribuir, publicar, mostrar, representar, modificar, crear trabajos derivados, transmitir o de forma alguna explotar el Material sin el permiso escrito expreso de ManageEngine. El logotipo y otras marcas de ManageEngine son marcas registradas de Zoho Corporation Pvt. Ltd. Cualquier otro nombre de productos de software o compañías citadas en este Material y no mencionadas aquí expresamente son las marcas registradas de sus respectivos propietarios

# Una breve introducción a la norma ISO 27001:2022

La norma ISO/IEC 27001:2022 forma parte de la familia ISO/IEC 27000:2018 de normas y controles de seguridad de la información. Estas normas proporcionan a las organizaciones un conjunto de requisitos basados en riesgos y agnósticos de la tecnología para implementar un sistema de gestión de la seguridad de la información (SGSI).

La Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC) desarrollaron conjuntamente estas normas.

Mientras que la familia ISO 27000 contiene muchas normas, solo hay dos normas certificables incluidas bajo esta familia:

- 1. ISO/IEC 27001:2022** — Esta norma proporciona los requisitos para la implementación de un SGSI.
- 2. ISO/IEC 27701:2019** — Esta norma proporciona los requisitos para implementar un sistema de gestión de información de privacidad (SGIP).

Para implementar un SGIP, las organizaciones primero necesitan implementar un SGSI. Después de todo, sin medidas de seguridad de datos, es imposible garantizar la privacidad de sus datos. Por lo tanto, para obtener la certificación ISO 27701, la norma sobre el SGIP, las organizaciones primero necesitan estar certificadas con la ISO 27001.

## Entonces, ¿por qué ISO 27001?

Si su organización maneja información confidencial de cualquier tipo (PII, ePHI o datos de propiedad), debe aspirar a una certificación ISO 27001.

Los requisitos y controles especificados en la norma ISO 27001 pueden ayudar a su organización a identificar riesgos e implementar controles para mitigarlos. Esto fortalecerá la postura de seguridad de su organización.

El cumplimiento de esta norma también ayuda a generar confianza del cliente en las prácticas de seguridad de la información de su organización. Algunos clientes internacionales también podrían solicitar pruebas de cumplimiento de la norma ISO 27001 como evidencia de prácticas sólidas de seguridad de la información.

Debido a su estructura tecnológica independiente, esta norma se puede asignar fácilmente a otras normas y marcos, como los controles de seguridad críticos CIS, NIST SP-800-53 (Controles de seguridad y privacidad para sistemas de información y organizaciones), etc.

El cumplimiento de la norma ISO 27001 también puede actuar como un paso importante en su viaje para garantizar el cumplimiento de las normas de privacidad de datos como el GDPR, la CCPA y más.

# La estructura de la norma ISO 27001:2022

La norma ISO 27001 consta de 10 cláusulas. De estas, solo siete cláusulas tienen requisitos aplicables.

Las cláusulas 1 a 3 establecen el alcance de la norma, enumeran las referencias utilizadas y definen los diversos términos que se utilizan en todo el documento.

Las cláusulas 4 a 10 proporcionan requisitos detallados sobre los procesos, políticas y acciones que deben implementarse para garantizar el cumplimiento de esta norma. Cada uno de estos requisitos es obligatorio si desea lograr el cumplimiento de la norma ISO 27001.

## Cláusulas de la ISO 27001

### **Cláusula 4: Contexto de la organización**

Esta cláusula cubre el contexto en el que se está aplicando el SGSI. Tendrá que enumerar lo que hace su organización, los requisitos de las distintas partes interesadas (internas y externas) y el alcance del SGSI. Esta información ayuda a los auditores a comprender el objetivo de su SGSI, permitiéndoles evaluarlo de manera efectiva.

### **Cláusula 5: Liderazgo**

Esta cláusula cubre el rol del liderazgo para garantizar el éxito del SGSI. Implica implementar una política de seguridad de la información, integrar los requisitos de SGSI en los procesos organizativos, y más. Asimismo, tendrá que asignar la responsabilidad de monitorear y mejorar el SGSI para garantizar el cumplimiento de la norma.



## Cláusula 6: Planeación

Esta cláusula trata sobre la gestión de riesgos en su organización. La documentación de esta sección deberá cubrir el proceso de identificación, análisis y tratamiento (mitigación, evitación o aceptación) de riesgos. La documentación incluirá la asignación de titulares de riesgos que son responsables de gestionar estos riesgos.

## Cláusula 7: Soporte

Esta cláusula cubre los recursos necesarios para respaldar, mantener y mejorar el SGSI. Deberá crear, mantener, actualizar (según sea necesario) y garantizar la disponibilidad de toda la documentación que la norma requiera. También tendrá que garantizar que su gente esté al tanto de los requisitos del SGSI, la necesidad del SGSI y las consecuencias del incumplimiento.

## Cláusula 8: Operación

Esta cláusula trata sobre la implementación de los requisitos cubiertos en la cláusula 6. Abarca las evaluaciones de riesgos y la aplicación del plan de tratamiento de riesgos. Combinadas, las cláusulas 6 a 8 deberían conducir a la creación de un plan completo de mitigación de riesgos integral.

## Cláusula 9: Evaluación del rendimiento

Esta cláusula cubre el monitoreo de la eficacia de su SGSI. Esto incluye el qué, cómo, quién y cuándo del monitoreo y análisis. También cubre auditorías internas y otros requisitos para probar y mejorar su SGSI.

## Cláusula 10: Mejora

Esta cláusula trata sobre el control y la mejora de daños. Requiere que su organización tome medidas correctivas para manejar una inconformidad. También requiere que revise su SGSI para asegurarse de que no vuelva a ocurrir. Enumera la mejora continua del SGSI (por encima de esto) como un requisito.

# Los controles y objetivos de control de la norma ISO 27001

Además de las 10 cláusulas mencionadas anteriormente, el anexo de la norma ISO 27001 también contiene 93 controles divididos en cuatro categorías: Controles organizativos, de personas, físicos y tecnológicos (cláusulas 5 a 8).

Estos controles proporcionan requisitos detallados que aseguran la implementación efectiva de un SGSI. A diferencia de las cláusulas mencionadas en la sección anterior, no es necesario implementar todos estos controles. De hecho, algunos de ellos pueden no ser aplicables para su organización.

Sin embargo, tendrá que explicar por qué los omitió en un documento de declaración de aplicabilidad que se compartirá con su auditor de certificación. Esto garantiza que su auditor sea consciente de por qué no ha actuado sobre estos controles.

En resumen, para obtener la certificación de conformidad con la norma ISO 27001, debe:

- Cumplir con todas las cláusulas mencionadas en el apartado anterior.
- Implementar todos los controles que sean aplicables a su organización a partir de los 93 listados en la Tabla A.1 del Anexo A de la norma ISO 27001.

Omitir cualquiera de estos requisitos puede anular sus posibilidades de obtener esta certificación.

# El rol de ManageEngine en su viaje de cumplimiento de la ISO 27001

El conjunto de soluciones de gestión de TI de ManageEngine puede ayudarlo a cumplir con los diversos requisitos de control relacionados con TI de la norma ISO 27001. Esto puede ayudar a su organización a desarrollar el mejor programa de gestión de seguridad de la información y lograr el cumplimiento de otras normas de seguridad y privacidad.

## Productos de ManageEngine correlacionados con los controles de la ISO 27001

Hemos correlacionado los productos de ManageEngine con los controles de la ISO 27001 que pueden ayudarlo a implementar.

### A.5 Controles organizacionales

| Control                         | Definición/Requisitos del control                                                                                                               | Productos de ManageEngine que pueden ayudar                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 5.7<br>Inteligencia de amenazas | La información relativa a las amenazas a la seguridad de la información debe recopilarse y analizarse para producir información sobre amenazas. | <b>Log360:</b> Integre y recopile información de fuentes y servicios de inteligencia sobre amenazas.<br><br><b>Endpoint Central:</b> Implemente una gestión integral de vulnerabilidades con una evaluación y visibilidad constantes de las amenazas desde una única consola. Emplee la corrección incorporada para resolver las vulnerabilidades detectadas. Garantice un parcheo sin problemas para Windows, Mac, Linux y más de 850 aplicaciones de terceros, y gestione actualizaciones para Windows, iOS, Android, ChromeOS, firmware y aplicaciones móviles. |

|                                                                |                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>5.9 Inventario de información y otros activos asociados</p> | <p>Debería elaborarse y mantenerse un inventario de información y otros activos asociados, incluidos los propietarios.</p> | <p><b>ServiceDesk Plus o AssetExplorer:</b> Descubra e identifique todos los activos de TI y no TI utilizando varios métodos de descubrimiento, como análisis de dominios, escaneos de red y scripts de autoanálisis, y análisis basados en agentes. Clasifique los activos, asigne propietarios y consolide en un repositorio centralizado para una visibilidad completa. Implemente prácticas de gestión de activos certificadas por ITIL para mantener el inventario preciso y actualizado.</p> <p><b>Endpoint Central:</b> Mantenga un inventario de todos los endpoints (incluidos los dispositivos móviles) y los activos de software, y gestione los desde una consola central.</p> <p><b>Log360:</b> Mantenga un inventario de software instalado en todos los endpoints, realice un seguimiento de los detalles de propiedad y asegúrese de que todos los activos de la organización se contabilizan y gestionan de manera efectiva.</p> <p><b>OpManager Plus:</b> Gestione un inventario completo de la infraestructura de red y supervise su estado, disponibilidad y rendimiento en tiempo real.</p> |
|----------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|  |  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--|--|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  |  | <p><b>Site24x7:</b> Utilice la herramienta de detección de redes para crear un inventario preciso de toda su red, identificando automáticamente todos los dispositivos y conexiones.</p> <p><b>PAM360:</b> Descubra todos los endpoints junto con sus cuentas locales para consolidar, rotar certificados y gestionar credenciales de identidad privilegiadas como contraseñas, claves SSH y certificados TLS.</p> <p><b>DataSecurity Plus:</b> Busque, analice y realice un seguimiento de datos personales confidenciales, también conocidos como PII o ePHI, que residen en sus servidores de archivos de Windows, Microsoft SQL Server y clústeres de failover.</p> <p><b>AppCreator:</b> Cree un repositorio de información de inventario y otros activos asociados, incluidos los propietarios.</p> <p><b>Analytics Plus:</b> Obtenga una visión completa de cada endpoint, activo y dispositivo desde paneles de inventario consolidados.</p> |
|--|--|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|



|                                       |                                                                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>5.11<br/>Devolución de activos</p> | <p>El personal y otras partes interesadas, según corresponda, deben devolver todos los activos de la organización en su poder al cambio o terminación de su empleo, contrato o acuerdo</p> | <p><b>ServiceDesk Plus o AssetExplorer:</b> Garantice la devolución de los activos de la organización compatibles mediante una base de datos de inventario como una única fuente de información para todos los activos. Utilice flujos de trabajo predefinidos para rastrear el retorno de activos y activar automáticamente las notificaciones si un activo está marcado como perdido. Automatice las aprobaciones para garantizar el cumplimiento durante la desvinculación.</p> <p><b>Endpoint Central:</b> Garantice una visibilidad completa de los activos de endpoints con dashboards detallados y funciones de informes de activos listas para usar.</p> <p><b>Log360:</b> Monitoree los cambios en las cuentas de los usuarios para garantizar que los empleados que salen ya no tengan acceso, realice un seguimiento del software instalado para verificar y recuperar los activos proporcionados por la organización y garantice que los datos críticos se archiven de forma segura antes de la desvinculación para evitar la pérdida de datos.</p> <p><b>PAM360:</b> Revoque automáticamente el acceso privilegiado a los endpoints aprovisionados al usuario que se está mudando a un equipo/departamento diferente o al finalizar su empleo, contrato o acuerdo.</p> |
|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                                         |                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                         |                                                                                                                                                                                                                                     | <p>Rote todas las contraseñas y claves SSH que el usuario respectivo utilizó para obtener acceso privilegiado en el pasado reciente.</p> <p><b>DataSecurity Plus:</b> Busque, analice y realice un seguimiento de datos personales confidenciales, también conocidos como PII o ePHI, que residen en sus servidores de archivos de Windows, Microsoft SQL Server y clústeres de failover.</p> <p><b>AppCreator:</b> Cree un repositorio de gestión de activos y realice un seguimiento de los activos desde la adquisición y la asignación hasta el desaprovisionamiento.</p> <p><b>Analytics Plus:</b> Consolide el HRMS y los datos de activos. Durante los cambios de personal, obtenga alertas automáticas para rastrear y garantizar la devolución de los activos y dispositivos asignados.</p> |
| 5.12<br>Clasificación de la información | La información debe clasificarse de acuerdo con las necesidades de seguridad de la información de la organización, en función de la confidencialidad, integridad, disponibilidad y requisitos relevantes de las partes interesadas. | <p><b>Data Security Plus:</b> Busque, analice y realice un seguimiento de datos personales confidenciales, también conocidos como PII o ePHI, que residen en sus servidores de Windows, Microsoft SQL Server y clústeres de failover.</p> <p><b>Endpoint Central:</b> Permita a los administradores de TI descubrir y clasificar varios tipos de datos estructurados y no estructurados utilizando mecanismos avanzados como huellas dactilares, RegEx, filtros basados en extensiones de archivos y búsqueda de palabras clave.</p>                                                                                                                                                                                                                                                                 |

|                                                 |                                                                                                                                                                                                                |                                                                                                                                                                                                            |
|-------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>5.13</p> <p>Etiquetado de la información</p> | <p>Debe elaborarse y aplicarse un conjunto adecuado de procedimientos de etiquetado de la información de conformidad con el sistema de clasificación de la información que la organización adopte.</p>         | <p><b>Endpoint Central:</b> Encuentre, analice y realice un seguimiento de datos personales confidenciales, también conocidos como PII o ePHI, que residen en sus redes.</p>                               |
| <p>5.14</p> <p>Transferencia de información</p> | <p>Deben existir normas, procedimientos o acuerdos de transferencia de información para todos los tipos de instalaciones de transferencia dentro de la organización y entre la organización y otras partes</p> | <p><b>Log360:</b> Monitoree las transferencias de archivos, el acceso de los usuarios y los eventos del sistema en entornos locales y en la nube para garantizar un intercambio seguro de información.</p> |

|                                      |                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>5.15</p> <p>Control de acceso</p> | <p>Se establecerán y aplicarán normas para controlar el acceso físico y lógico a la información y otros activos asociados sobre la base de los requisitos de seguridad empresarial y de la información.</p> | <p><b>AD360:</b> Configure las reglas de MFA basadas en la IP del usuario, la geolocalización, el tiempo de acceso y el dispositivo utilizado para restringir o permitir el acceso a la información y los activos necesarios. Revise y verifique periódicamente el acceso de los usuarios a los recursos de la organización con campañas de certificación de acceso.</p> <p><b>Identity360:</b> Establezca permisos y roles detallados y automatizados a medida que los usuarios se muevan dentro de su organización. Proteja los recursos garantizando que los usuarios adecuados tengan los privilegios adecuados.</p> <p><b>ServiceDesk Plus:</b> Reciba, autorice y administre solicitudes de aprovisionamiento de acceso aprovechando las funciones de gestión de solicitudes de servicio certificadas por ITIL. Unifique los servicios a través de un catálogo de servicios centralizado y ofrézcalos a grupos específicos de empleados según sus funciones. Implemente un escrutinio detallado a través de flujos de trabajo visuales integrados con aprobaciones multinivel. Organice el aprovisionamiento de acceso a través de automatizaciones de flujo de trabajo de un solo toque activadas en función de eventos como las aprobaciones.</p> |
|--------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|  |  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--|--|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  |  | <p><b>PAM360:</b> Aproveche los controles de acceso de confianza cero para aplicar flujos de trabajo de solicitud-liberación de contraseña y así exigir la aprobación del administrador para cada solicitud de acceso remoto. Además, asocie puntuaciones de confianza a cada usuario y endpoint, que estén determinadas por condiciones como la dirección IP del usuario, la hora de inicio de sesión, los plugins instalados del navegador, etc. Cree políticas de acceso basadas en dichas puntuaciones de confianza para denegar el acceso a los endpoints si la puntuación de confianza cae por debajo del umbral predefinido, lo que obliga a un control de acceso basado en políticas.</p> <p><b>Log360:</b> Aplique controles de acceso mediante la supervisión de los inicios de sesión, las actividades de sesión y los intentos de autenticación de los usuarios en entornos locales y en la nube. Supervise los cambios en la cuenta, los intentos de acceso fallidos y las políticas de acceso condicional para detectar el acceso no autorizado, garantizar el cumplimiento y reforzar los controles de seguridad.</p> |
|--|--|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|  |  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--|--|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  |  | <p><b>Endpoint Central:</b> Utilice la gestión de privilegios de endpoints para aplicar el principio de privilegios mínimos. Habilite la gestión de privilegios específicos de aplicaciones y el acceso justo a tiempo a los usuarios finales. Ponga las aplicaciones de software en la lista de permitidos/bloqueados en los endpoints críticos utilizando el módulo de control de aplicaciones. Implemente políticas de acceso condicional para validar que los usuarios autorizados accedan a los sistemas y datos críticos para el negocio.</p> <p><b>OpManager Plus:</b> Aproveche el control de acceso basado en roles para garantizar que los usuarios solo puedan acceder a los dispositivos asignados por los administradores, y los cambios realizados en estos dispositivos se envíen automáticamente a los administradores para su aprobación.</p> <p><b>AppCreator:</b> Aplique controles de acceso detallados con base en reglas para aplicaciones de atención médica personalizadas creadas en AppCreator. Amplíe estos controles de acceso a aplicaciones de terceros integradas con sus aplicaciones personalizadas.</p> |
|--|--|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                                   |                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 5.16 Gestión de identidades       | Se gestionará todo el ciclo de vida de las identidades.                                                                                                                                                      | <b>AD360 o Identity360:</b> Optimice la gestión del ciclo de vida de la identidad con el aprovisionamiento masivo de usuarios en todas las plataformas, la automatización, las plantillas personalizables y la integración perfecta de HCM.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 5.17 Información de autenticación | La asignación y gestión de la información de autenticación se controlarán mediante un proceso de gestión, incluido el asesoramiento al personal sobre el manejo adecuado de la información de autenticación. | <p><b>AD360:</b> Simplifique la gestión de contraseñas para los administradores de TI y reduzca la dependencia de la mesa de ayuda para los usuarios finales con la gestión de contraseñas de autoservicio, políticas de contraseñas sólidas, sincronización de contraseñas y notificaciones de caducidad de contraseñas.</p> <p><b>Log360:</b> Realice un seguimiento de los cambios en las cuentas de usuario y los detalles de autenticación en los sistemas y bases de datos. Monitoree los intentos de inicio de sesión y asegure el control adecuado de la información de autenticación, como contraseñas, para evitar el acceso no autorizado.</p> <p><b>Endpoint Central:</b> Establezca políticas de código de acceso para dispositivos móviles que se ejecuten en Android, Apple y Windows, asegurando que los usuarios finales creen códigos de acceso seguros para sus dispositivos. Utilice estas directivas para configurar el número máximo de intentos de código fallidos, el tiempo de inactividad máximo permitido antes del bloqueo automático y otras configuraciones.</p> |

|                                       |                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>5.18</p> <p>Derechos de acceso</p> | <p>Los derechos de acceso a la información y otros activos asociados se aprovisionarán, revisarán, modificarán y eliminarán de acuerdo con la política de la organización sobre temas específicos y las reglas para el control de acceso.</p> | <p><b>AD360:</b> Revise periódicamente el acceso de los usuarios a los recursos de la organización a través de campañas de certificación de acceso.</p> <p><b>Identity360:</b> Automatice las actualizaciones detalladas de roles y permisos a medida que los usuarios cambian de roles y proteja los recursos con privilegios precisos.</p> <p><b>PAM360:</b> Aplique el acceso con menos privilegios en los endpoints a través del control de acceso basado en roles y políticas, lo que limita la visibilidad de los usuarios remotos de acuerdo con los requisitos de seguridad de la información de la organización.</p> <p><b>ServiceDesk Plus:</b> Habilite y gestione las modificaciones de acceso a través de formularios de solicitud de acceso detallados. Recopile información precisa a través de campos de plantilla cada vez que se solicite una modificación de los derechos de acceso. Maneje la gobernanza de acceso con aprobaciones multinivel.</p> <p><b>OpManager Plus:</b> Aproveche el RBAC para restringir el acceso de los usuarios a los activos para los cambios de configuración. Además, cualquier cambio realizado en los activos accesibles se enruta automáticamente a los administradores para su aprobación.</p> |
|---------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|  |  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--|--|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  |  | <p><b>Log360:</b> Monitoree los cambios en la cuenta de usuario, las modificaciones de grupo y las actividades de inicio de sesión para garantizar que los derechos de acceso se alineen con las políticas de la organización; supervise el acceso a la base de datos y a los dispositivos de red para evitar el uso no autorizado.</p> <p><b>Endpoint Central:</b> Utilice la gestión de privilegios de endpoints para aplicar el principio de privilegios mínimos. Habilite la gestión de privilegios específicos de aplicaciones y el acceso justo a tiempo a los usuarios finales. Ponga las aplicaciones de software en la lista de permitidos/bloqueados en los endpoints críticos utilizando el módulo de control de aplicaciones. Implemente políticas de acceso condicional para validar que los usuarios autorizados accedan a los sistemas y datos críticos para el negocio.</p> <p><b>AppCreator:</b> Aplique controles de acceso detallados con base en reglas para aplicaciones de atención médica personalizadas y datos asociados creados en AppCreator.</p> |
|--|--|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                                                                                         |                                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                             |
|-----------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>5.19</p> <p>Seguridad de la información en la relación con el proveedor</p>          | <p>Se definirán e implementarán procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados al uso de los productos o servicios de los proveedores.</p> | <p><b>ServiceDesk Plus:</b> Cree módulos a la medida para manejar las evaluaciones de riesgo de los proveedores. Incruste estos módulos personalizados con campos que ayudan a registrar y categorizar los riesgos. Inicie acciones de mitigación, como notificar a las partes interesadas y crear tickets a través de automatizaciones de código bajo.</p> |
| <p>5.21 Gestión de la seguridad de la información en la cadena de suministro de TIC</p> | <p>Se definirán y aplicarán procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados a la cadena de suministro de productos y servicios de TIC.</p>  | <p><b>ServiceDesk Plus:</b> Aproveche los módulos personalizados y cree cuestionarios de evaluación de riesgos personalizados para registrar los riesgos asociados con el proveedor de la cadena de suministro de TIC. Active automatizaciones personalizadas dependiendo del riesgo identificado.</p>                                                      |

|                                                                                    |                                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>5.23</p> <p>Seguridad de la información para el uso de servicios en la nube</p> | <p>Los procesos de adquisición, uso, gestión y salida de los servicios en la nube deben establecerse de acuerdo con los requisitos de seguridad de la información de la organización.</p> | <p><b>Log360:</b> Garantice el uso seguro de la nube mediante la auditoría de la actividad del usuario, los controles de acceso y los cambios de configuración.</p> <p><b>Identity360:</b> Implemente la gestión del ciclo de vida de la identidad con aprovisionamiento masivo de usuarios y plantillas personalizables. Establezca permisos automatizados y detallados a medida que los usuarios transitan, simplificando la gestión del acceso a la nube.</p> <p><b>ServiceDesk Plus:</b> Cree flujos de trabajo visuales dedicados y optimice el proceso para solicitar y adquirir servicios en la nube. Asocie y gestione órdenes de compra y contratos junto con las aprobaciones, y realice un seguimiento de sus fechas de vencimiento con notificaciones automatizadas.</p> <p><b>Site24x7:</b> Monitoree de manera integral la seguridad de los sitios web y las aplicaciones web de acceso público mediante monitores como comprobaciones de desfiguración de sitios web, validación de certificados SSL/TLS, evaluaciones de la reputación de la marca y comprobaciones de listas de bloqueo en tiempo real. Genere informes para identificar posibles amenazas y vulnerabilidades en sus sitios web.</p> |
|------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                                                                                                            |                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>5.24</p> <p>Planificación y preparación de la gestión de incidentes de seguridad de la información</p>  | <p>La organización planificará y preparará la gestión de incidentes de seguridad de la información definiendo, estableciendo y comunicando procesos, roles y responsabilidades de gestión de incidentes de seguridad de la información.</p> | <p><b>ServiceDesk Plus:</b> Desarrolle plantillas estructuradas de gestión de incidentes que definan roles, responsabilidades, SLA, tareas y procedimientos de respuesta. Cree flujos de trabajo predefinidos con notificaciones automatizadas a través de Microsoft Teams para mantener actualizadas a las partes interesadas. Realice un análisis de impacto en detalle con una CMDB integrada para identificar los activos, servicios y dependencias afectados para lograr resoluciones más rápidas.</p> |
| <p>5.25</p> <p>Evaluación y decisión sobre los eventos relacionados con la seguridad de la información</p> | <p>La organización evaluará los eventos de seguridad de la información y decidirá si se han de categorizar como incidentes de seguridad de la información.</p>                                                                              | <p><b>ServiceDesk Plus:</b> Aproveche la clasificación con IA para categorizar, priorizar y dirigir con precisión los incidentes de seguridad de la información a los equipos de respuesta a incidentes adecuados. Inicie flujos de trabajo visuales que guíen a los miembros de IRT en la evaluación del impacto y la toma de decisiones con automatizaciones integradas.</p>                                                                                                                              |

|                                                                             |                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>5.26</p> <p>Respuesta ante incidentes de seguridad de la información</p> | <p>Se debe responder ante incidentes de seguridad de la información de acuerdo con los procedimientos documentados.</p> | <p><b>Log360:</b> Identifique los incidentes de seguridad a través del análisis de eventos del sistema, supervise la actividad del firewall para detectar conexiones sospechosas y analice los datos de amenazas para garantizar una respuesta oportuna y mitigación según los procedimientos documentados. Además, automatice la respuesta y resolución de primer nivel para incidentes comunes mediante automatizaciones de flujo de trabajo. Estos flujos de trabajo pueden activar acciones predefinidas, como deshabilitar cuentas de usuario comprometidas, bloquear IP sospechosas o notificar a los equipos de seguridad en tiempo real, lo que garantiza una contención más rápida y reduce la intervención manual.</p> <p><b>ServiceDesk Plus:</b> Recopile evidencia a través de campos de ticket preconstruidos y campos personalizados en todo el proceso de respuesta a incidentes. Establezca POE y dirija la gobernanza a través de flujos de trabajo de respuesta a incidentes prediseñados. Realice RCA detallados y aborde las causas subyacentes con un módulo de gestión de problemas estrechamente integrado.</p> |
|-----------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                                                                              |                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>5.27</p> <p>Aprender de los incidentes de seguridad de la información</p> | <p>Los conocimientos adquiridos en los incidentes de seguridad de la información se utilizarán para reforzar y mejorar los controles de seguridad de la información.</p>                              | <p><b>ServiceDesk Plus:</b> Genere revisiones detalladas posteriores al incidente con las funciones generativas de la IA de Zia. Resuma las conversaciones dentro del ticket para una mejor comprensión del contexto. Transfiera estos resúmenes y conocimientos como notas para comunicar claramente los historiales de incidentes. Documente la resolución en un repositorio central de conocimientos para establecer POE y reducir el impacto de futuros incidentes.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <p>5.28</p> <p>Recopilación de pruebas</p>                                   | <p>La organización establecerá e implementará procedimientos para la identificación, recopilación, adquisición y preservación de pruebas relacionadas con eventos de seguridad de la información.</p> | <p><b>Log360:</b> Registre y preserve datos de eventos de seguridad críticos mediante la auditoría de inicios de sesión, la actividad del firewall, los cambios de archivos y el seguimiento de procesos en sistemas, bases de datos y entornos de nube. Garantice la preparación forense mediante la recopilación de pruebas sobre inicios de sesión fallidos, uso de disco extraíble y anomalías del tráfico de red.</p> <p><b>Endpoint Central:</b> En caso de un evento sospechoso registrado en la red de TI, registre y reenvíe los ataques y los detalles relacionados con los endpoints al administrador de la red o al equipo del SOC.</p> <p><b>ServiceDesk Plus:</b> Asegure la recopilación diligente de evidencia a través de campos de ticket prediseñados y campos personalizados en respuesta a incidentes y otras prácticas de ITSM. Genere revisiones luego de incidentes con GenAI.</p> |

|                                                               |                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                               |                                                                                                                                                                                   | <p>Establezca POE y manuales estratégicos para la recopilación de pruebas utilizando flujos de trabajo visuales, donde los campos son obligatorios y se notifica a las partes interesadas.</p> <p><b>PAM360:</b> Audite todos los registros de acceso privilegiado con los detalles de “quién”, “cuándo”, “dónde” y “para qué” se aprovisionó o concedió un acceso. Registre todas las actividades realizadas por los usuarios en las sesiones remotas privilegiadas para fines de investigación y revisión de acceso.</p>                                                                                                                                                                                                                                                                                                                                                   |
| 5.30<br>Preparación de la TIC para la continuidad corporativa | La preparación de la TIC se planificará, aplicará, mantendrá y probará sobre la base de los objetivos de continuidad de las operaciones y los requisitos de continuidad de la TIC | <p><b>Endpoint Central:</b> Aproveche el motor de antivirus de nueva generación (NGAV) para garantizar una defensa proactiva contra amenazas cibernéticas, como el malware con tecnología de detección de comportamiento en tiempo real asistida por IA y tecnología de aprendizaje profundo. Utilice las funciones forenses de incidentes de la plataforma para analizar la causa raíz y la gravedad de las amenazas. Ponga en cuarentena automáticamente los endpoints afectados mediante el módulo NGAV para detectar comportamientos sospechosos o malware y vuelva a implementarlos en la producción después del análisis forense y la remediación. Utilice copias de seguridad de archivos no borrables, capturadas cada tres horas con el servicio de copia oculta de Microsoft para restaurar instantáneamente cualquier archivo que un ransomware haya cifrado.</p> |

|                                                                              |                                                                                                                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>5.31 Requisitos legales, estatutarios, reglamentarios y contractuales</p> | <p>Los requisitos legales, estatutarios, reglamentarios y contractuales relevantes para la seguridad de la información y el enfoque de la organización para cumplir con estos requisitos se identificarán, documentarán y mantendrán actualizados.</p> | <p><b>ServiceDesk Plus:</b> Garantice el cumplimiento identificando, documentando y actualizando periódicamente artículos de conocimiento sobre requisitos legales, estatutarios, reglamentarios y contractuales. Incruste estos artículos en el portal de autoservicio para proporcionar a los empleados un fácil acceso a estos requisitos y orientación relacionada.</p> <p><b>Log360:</b> Aproveche los informes integrados para identificar y documentar los requisitos legales y contractuales. Garantice un monitoreo continuo y mantenga registros precisos para agilizar las auditorías y las evaluaciones regulatorias.</p> <p><b>Endpoint Central:</b> Implemente los controles de endpoints necesarios y genere informes listos para auditoría para garantizar el cumplimiento de los mandatos de privacidad de datos regionales y globales y las normas de seguridad de la información, como el GDPR, los controles de seguridad críticos del CIS, el marco de ciberseguridad del NIST y más.</p> <p><b>OpManager Plus:</b> Utilice el módulo de gestión de configuración para garantizar el cumplimiento de normas como los puntos de referencia del CIS, PCI DSS, SOX y HIPAA. Para requisitos de directiva adicionales, puede definir políticas personalizadas estableciendo sus propias reglas. Además, cualquier regla que no cumpla puede remediarse automáticamente.</p> |
|------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|



|                                        |                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------------|-------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                        |                                                                                                             | <p><b>Nota:</b> Las soluciones de ManageEngine pueden ayudar a organizaciones como la suya a cumplir con varios mandatos de privacidad de datos regionales y globales y normas de seguridad de la información, como el GDPR, los controles de seguridad críticos del CIS, el marco de ciberseguridad del NIST y más. Visite esta página para más información.</p>                                                                                               |
| 5.32 Derechos de propiedad intelectual | La organización implementará procedimientos apropiados para proteger los derechos de propiedad intelectual. | <p><b>Endpoint Central:</b> Busque, analice y realice un seguimiento de información confidencial (como patentes, contratos y otros archivos confidenciales) que resida en sus redes.</p> <p><b>Analytics Plus:</b> Identifique y categorice las instalaciones de software no autorizadas por riesgo y cumplimiento. Analice las tendencias de uso para proporcionar alternativas más seguras donde sea necesario y evite la reaparición de la TI invisible.</p> |

|                                            |                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>5.33</p> <p>Protección de registros</p> | <p>Los registros estarán protegidos contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada.</p> | <p><b>AD360:</b> Realice copias de seguridad periódicas de los datos en Active Directory (AD), Microsoft 365, Google Workspace y Exchange Server, y guárdelos de forma segura como varias versiones cifradas, garantizando que se puedan restaurar en el improbable caso de pérdida de datos. Proteja los registros del acceso no autorizado mediante métodos de MFA sólidos.</p> <p><b>PAM360:</b> Aplique flujos de trabajo de aprobación de administradores para solicitudes de acceso remoto a endpoints con registros confidenciales.</p> <p><b>Endpoint Central:</b> Aplique controles para evitar la pérdida de datos corporativos a través de dispositivos periféricos, cargas en la nube pública, impresión de páginas web y portapapeles. Aplique políticas de acceso condicional para validar el acceso de los usuarios autorizados a los sistemas y datos críticos para el negocio.</p> |
|--------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                                                      |                                                                                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>5.34</p> <p>Privacidad y protección de la PII</p> | <p>La organización identificará y cumplirá los requisitos relativos a la preservación de la privacidad y la protección de la PII de acuerdo con las leyes y reglamentos aplicables y los requisitos contractuales.</p> | <p><b>ServiceDesk Plus:</b> Dentro de las solicitudes de servicios empresariales y de TI que reciba, encripte los campos que contienen PII para proteger la información personal de los solicitantes. Configure los parámetros de privacidad en ServiceDesk Plus para anonimizar y borrar los datos de la aplicación cuando sea necesario.</p> <p><b>AD360 o Identity360:</b> Proteja la PII con métodos modernos y resistentes al phishing, al tiempo que garantiza el cumplimiento de regulaciones como PCI DSS, HIPAA, GDPR y NIS2.</p> <p><b>Endpoint Central:</b> Encuentre, analice y realice un seguimiento de datos personales confidenciales, también conocidos como PII o ePHI, que residen en sus redes. Aplique controles sobre el uso compartido de archivos y el uso de dispositivos periféricos para evitar la pérdida de datos a través de unidades USB, impresoras, cargas de archivos a la nube pública y más.</p> <p><b>AppCreator:</b> Encripte datos personales como PII o ePHI registrados en aplicaciones de atención médica personalizadas creadas en AppCreator para garantizar la protección y privacidad de la PII.</p> <p><b>OpManager Plus:</b> Busque y encuentre PII almacenada dentro de los diversos módulos de OpManager Plus.</p> |
|------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                                                                                                  |                                                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>5.36</p> <p>Cumplimiento de las políticas, reglas y normas de seguridad de la información</p> | <p>El cumplimiento de la política de seguridad de la información de la organización, las políticas, reglas y normas específicas de cada tema se revisará regularmente.</p> | <p><b>AD360:</b> Aproveche los informes prediseñados para revisar e identificar posibles desviaciones de cumplimiento con las regulaciones y normas.</p> <p><b>ServiceDesk Plus:</b> Documente y gestione las políticas y reglas de seguridad de la información de la organización como artículos de conocimiento en un repositorio central. Establezca mecanismos de revisión y aprobación de documentos con acceso basado en roles para mantener la información actualizada.</p> <p><b>Endpoint Central:</b> Utilice informes integrados para generar informes e información sobre el estado de los endpoints de la organización con fines de gobernanza y auditoría.</p> <p><b>Firewall Analyzer o OpManager Plus:</b> Optimice sus auditorías de cumplimiento de firewall con las funciones de gestión de cumplimiento integradas de Firewall Analyzer, que ofrecen informes de normas de seguridad listos para usar alineados con mandatos regulatorios como PCI DSS, ISO 27001, NIST, SANS, NERC-CIP, SOX, GDPR, GLBA, HIPAA y más.</p> |
|--------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## A.6 Controles de personas

| Control            | Definición/Requisitos del control                                                                                                                                                                               | Productos de ManageEngine que pueden ayudar                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 6.7 Trabajo remoto | Las medidas de seguridad se implementarán cuando el personal esté trabajando de forma remota para proteger la información a la que se accede, procesa o almacena fuera de las instalaciones de la organización. | <p><b>Endpoint Central:</b> Aproveche los protocolos de encriptación avanzada (AES) de 256 bits durante las operaciones de resolución de problemas remotas. Ejecute endpoints en modo FIPS para garantizar operaciones seguras y protegidas.</p> <p><b>PAM360:</b> Aplique flujos de trabajo de aprobación de administradores para solicitudes de acceso remoto. Asocie puntuaciones de confianza a usuarios y dispositivos remotos en función del número de intentos de inicio de sesión no válidos, inicios de sesión durante horas no laborales, plug-ins instalados en el navegador, autenticación de dos factores, etc. Cree políticas de acceso y mapéelas a endpoints privilegiados para examinar las solicitudes de acceso de usuarios remotos con puntuaciones de confianza que no reflejen las normas organizativas.</p> <p><b>AD360:</b> Proteja las sesiones de acceso remoto con MFA, ya sea a nivel cliente o equipo de destino, mediante autenticadores fuertes.</p> |

|                                                        |                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                             |
|--------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                        |                                                                                                                                                                                             | <p><b>Analytics Plus:</b> Cree dashboards consolidados para proteger cada elemento del trabajo remoto desde una sola ventana. Evalúe el cumplimiento de los parches de activos, descubra las instalaciones de TI invisible, identifique contraseñas débiles, identifique cuentas obsoletas y más para agilizar sin esfuerzo las prácticas de seguridad.</p> |
| 6.8 Informes de eventos de seguridad de la información | La organización proporcionará un mecanismo para que el personal informe oportunamente sobre los eventos de seguridad de la información observados o sospechosos por los canales apropiados. | <p><b>ServiceDesk Plus:</b> Aproveche un sistema de registro de incidentes omnicanal integrado con varias herramientas de monitoreo de TI, UEM, SIEM y colaboración. Una vez que se registra el ticket, clasifique, administre y resuelva incidentes a través de automatizaciones de flujo de trabajo de extremo a extremo y asistencia de IA.</p>          |

## A.7 Controles físicos

| Control                                            | Definición/Requisitos del control                                                                                                                                                                                                                             | Productos de ManageEngine que pueden ayudar                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 7.10 Medios de almacenamiento                      | Los medios de almacenamiento se gestionarán a lo largo de su ciclo de vida de adquisición, uso, transporte y eliminación de acuerdo con el esquema de clasificación y los requisitos de manejo de la organización.                                            | <p><b>ServiceDesk Plus:</b> Clasifique los activos de TI como medios de almacenamiento, gástelos desde un repositorio central y tenga flujos de trabajo visuales dedicados para cada paso del ciclo de vida del activo, desde la adquisición hasta la eliminación.</p> <p><b>Endpoint Central:</b> Aproveche las funciones de gestión de dispositivos periféricos para bloquear dispositivos de almacenamiento externos. Cree una lista de dispositivos de confianza que sus usuarios finales puedan usar en sus endpoints. Utilice el módulo de gestión de activos integrado para rastrear los activos de medios de almacenamiento, desde la adquisición hasta la eliminación. Asegure la eliminación segura de cualquier información corporativa u otros datos confidenciales de los activos antes de su eliminación.</p> |
| 7.14 Eliminación segura o reutilización de equipos | Los elementos de los equipos que contengan medios de almacenamiento se verificarán para garantizar que los datos sensibles y los programas informáticos autorizados se hayan eliminado o sobrescrito de forma segura antes de su eliminación o reutilización. | <p><b>Endpoint Central:</b> Realice borrados remotos para garantizar la seguridad de los datos corporativos en caso de que se pierda un dispositivo. Restablezca de fábrica dispositivos para que los administradores puedan reasignar dispositivos utilizados por exempleados sin problemas para su uso por arte de un empleado actual.</p> <p><b>ServiceDesk Plus:</b> Cuando un activo de TI llega al final de su vida útil o necesita eliminarse, notifique automáticamente a las partes interesadas necesarias para eliminar cualquier dato sensible o software con licencia.</p>                                                                                                                                                                                                                                      |

## A.8 Controles tecnológicos

| Control                                         | Definición/Requisitos del control                                                                                           | Productos de ManageEngine que pueden ayudar                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8.1<br>Dispositivos de endpoint de los usuarios | La información almacenada, procesada o accesible a través de los dispositivos de endpoint de los usuarios estará protegida. | <p><b>Endpoint Central:</b> Encuentre, analice y realice un seguimiento de datos personales confidenciales que residen en sus redes. Implemente la contenedorización de datos personales y corporativos para garantizar la seguridad de los datos corporativos. Establezca políticas de código de acceso y aplique medidas de seguridad de dispositivos y navegadores para minimizar los riesgos de seguridad. Implemente el cifrado de almacenamiento de dispositivos y controles DLP para evitar la pérdida de datos a través de dispositivos periféricos, cargas a la nube pública y mucho más.</p> <p><b>ServiceDesk Plus:</b> Identifique estaciones de trabajo con software prohibido y notifique al personal apropiado. Integre con soluciones UEM como Endpoint Central y Microsoft Intune para realizar acciones correctivas como asociar/disociar perfiles, borrar datos corporativos o geolocalizar dispositivos móviles.</p> <p><b>AD360 o Identity360:</b> Proteja el acceso a los endpoints empresariales mediante autenticación sólida y adaptativa.</p> |

|                                            |                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8.2 Derechos de acceso privilegiado        | La asignación y el uso de los derechos de acceso privilegiado se restringirán y gestionarán.                                                           | <p><b>PAM360:</b> Aplique flujos de trabajo de aprobación de administradores para solicitudes de acceso remoto. Asigne puntuaciones de confianza a usuarios y dispositivos remotos en función de condiciones predefinidas, como intentos de inicio de sesión no válidos, inicios de sesión durante horas no laborales, plug-ins del navegador instalados y autenticación de dos factores. Implemente el control de acceso basado en roles (RBAC) para garantizar que los usuarios solo puedan acceder a los recursos en función de sus roles. Defina políticas de acceso y vincule a endpoints privilegiados para evaluar y controlar las solicitudes de acceso remoto basadas en estos puntajes de confianza.</p> <p><b>Endpoint Central:</b> Utilice la función de gestión de privilegios de endpoints para aplicar el principio de privilegios mínimos. Habilite la gestión de privilegios específicos de la aplicación y el acceso justo a tiempo para los usuarios finales.</p> |
| 8.3 Restricción de acceso a la información | El acceso a la información y otros activos asociados se restringirá de acuerdo con la política de control de acceso por temas específicos establecida. | <p><b>AD360:</b> Restrinja el acceso a los recursos mediante reglas de MFA basadas en la IP del usuario, la geolocalización, la hora de acceso y el dispositivo utilizado. Revise y valide regularmente el acceso de los usuarios a los recursos de la organización con campañas de certificación de acceso.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

|  |  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--|--|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  |  | <p><b>Identity360:</b> Gestione los permisos de acceso eficientemente con la sincronización de roles automatizada y la gestión de acceso masivo, manteniendo los recursos seguros.</p> <p><b>PAM360:</b> Controle el acceso privilegiado a través del flujo de trabajo de aprobación, la elevación justo a tiempo y las funciones de elevación de autoservicio. Proporcione privilegios de acceso basados en políticas de control de acceso y evaluación en tiempo real de la postura de riesgo del usuario y el dispositivo.</p> <p><b>Endpoint Central:</b> Utilice la gestión de privilegios de endpoints para aplicar el principio de privilegios mínimos. Habilite la gestión de privilegios específicos de aplicaciones y el acceso justo a tiempo a los usuarios finales.</p> <p>Ponga las aplicaciones de software en la lista de permitidos/bloqueados en los endpoints críticos utilizando el módulo de control de aplicaciones. Implemente políticas de acceso condicional para validar que los usuarios autorizados accedan a los sistemas y datos críticos para el negocio.</p> |
|--|--|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                                        |                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>8.5</p> <p>Autenticación segura</p> | <p>Se aplicarán tecnologías y procedimientos de autenticación seguros basados en las restricciones de acceso a la información y en la política temática específica sobre el control de acceso.</p> | <p><b>AD360:</b> Implemente MFA adaptativa utilizando métodos fuertes como las contraseñas FIDO resistentes al phishing, YubiKey y datos biométricos. Lleve a cabo revisiones periódicas del acceso de los usuarios a los recursos de la organización a través de campañas de certificación de acceso.</p> <p><b>Identity360:</b> Optimice la gestión de acceso con actualizaciones de roles, asegúrese de que los usuarios tengan los privilegios adecuados y proteja los recursos.</p> <p><b>OpManager Plus:</b> Controle y asegure el acceso a los componentes de red con diversas opciones de autenticación, incluyendo el servidor RADIUS, AD, SAML y autenticación de dos factores.</p> <p><b>PAM360:</b> Requiera la aprobación del administrador para las solicitudes de acceso remoto. Calcule las puntuaciones de confianza para usuarios y dispositivos remotos en función de factores predefinidos como intentos de inicio de sesión fallidos, inicios de sesión fuera del horario de oficina, extensiones de navegador instaladas y autenticación de dos factores. Utilice el control de acceso basado en roles para restringir el acceso en función de los roles de usuario y los niveles de confianza. Configure políticas de acceso y asócielas con endpoints privilegiados para evaluar y regular las solicitudes de acceso remoto de acuerdo con estos puntajes de confianza.</p> |
|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                             |                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                             |                                                                                                                    | <p><b>Endpoint Central:</b> Aproveche Windows Hello para dispositivos Windows y configure la autenticación de dos factores para los usuarios finales de Windows. Garantice el acceso seguro a las aplicaciones corporativas mediante el SSO empresarial basado en Kerberos o la autenticación basada en certificados mediante SCEP.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 8.6 Gestión de la capacidad | El uso de los recursos se supervisará y ajustará de acuerdo con las necesidades de capacidad actuales y previstas. | <p><b>OpManager Plus:</b> Garantice un monitoreo de almacenamiento y previsión de capacidad sin interrupciones desde una interfaz unificada aprovechando el motor de ML integrado para procesar datos de red, analizar métricas clave y generar tendencias de pronóstico a través de informes, gráficos y visualizaciones.</p> <p><b>Site24x7:</b> Vea y supervise las métricas de utilización de recursos como CPU, memoria y almacenamiento con la funcionalidad de planificación de capacidad. Monitoree la salud y el estado de los recursos agrupados en el monitor de capacidad, pronostique y gestione la capacidad de recursos y optimice la distribución de la carga de trabajo mediante el análisis N superior/N inferior.</p> <p><b>Endpoint Central:</b> Analice la duración del uso del software y el número de veces que se utiliza cada software para tomar decisiones informadas sobre las compras de software mientras se determinan las tendencias de uso de activos importantes. Evalúe la adecuación del inventario actual de licencias de software en función de las tendencias de uso utilizando el módulo de gestión de licencias. Controle las licencias de software que van a expirar y las expiradas.</p> |

|                                        |                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                        |                                                                                                                                    | <p><b>Analytics Plus:</b> Acceda a inventarios detallados de activos y recursos. Obtenga predicciones precisas que incorporen las necesidades cambiantes de la organización. Ejecute simulaciones para visualizar los recursos necesarios para cumplir con los objetivos de negocio y abordar las brechas de capacidad. Agilice la planificación de la capacidad sin esfuerzo.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| 8.7<br>Protección<br>contra<br>malware | La protección<br>contra el malware<br>se implementará y<br>estará respaldada<br>por el<br>conocimiento<br>adecuado del<br>usuario. | <p><b>Endpoint Central:</b> Aproveche el motor NGAV integrado para detectar de forma proactiva malware con tecnología de detección de comportamiento en tiempo real asistida por IA y tecnología de aprendizaje profundo. Utilice la capacidad forense de incidentes activos del software para permitir que SecOps analice la causa raíz y la gravedad de las amenazas detectadas. Ponga en cuarentena automáticamente los endpoints tras la detección de comportamientos sospechosos y vuelva a implementarlos en la producción después de un análisis forense exhaustivo y la corrección/restauración de datos (si es necesario).</p> <p><b>AD360:</b> Proteja los endpoints contra ataques con una autenticación fuerte y adaptable. Realice copias de seguridad de los datos con regularidad y almacénelos de forma segura en múltiples versiones cifradas, lo que garantiza una fácil restauración en caso de un ataque.</p> |

|                                          |                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                          |                                                                                                                                                                                                                       | <p><b>Log360:</b> Detecte y analice las amenazas de malware mediante el monitoreo de los registros de antivirus, la actividad del firewall y los eventos de seguridad de los endpoints. Identifique archivos sospechosos, realice un seguimiento de las amenazas basadas en correos electrónicos y mejore la protección con inteligencia de amenazas en tiempo real en todos los sistemas y redes.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 8.8 Gestión de vulnerabilidades técnicas | <p>Se obtendrá información sobre las vulnerabilidades técnicas de los sistemas de información en uso, se evaluará la exposición de la organización a dichas vulnerabilidades y se tomarán las medidas apropiadas.</p> | <p><b>Endpoint Central:</b> Adopte la gestión de vulnerabilidades basada en el riesgo para los sistemas de información críticos y no críticos. Priorice las vulnerabilidades en función de métricas como la puntuación CVSS, la disponibilidad de parches y más. Garantice una gestión integral de vulnerabilidades con una evaluación constante y visibilidad de todas las amenazas detectadas en una sola consola. Utilice la herramienta de corrección integrada para parchear o mitigar cualquier vulnerabilidad detectada dentro de su red.</p> <p><b>OpManager Plus:</b> Mantenga las defensas de red actualizadas con la información sobre amenazas más reciente utilizando las funciones avanzadas de detección de vulnerabilidades del módulo de gestión de configuración, que se actualiza diariamente con datos de la Base de datos nacional de vulnerabilidades (NVD) y fuentes directas de proveedores. Obtenga información sobre las vulnerabilidades de los dispositivos, los activos expuestos y la distribución de versiones para garantizar una cobertura de seguridad completa.</p> |

|                                        |                                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>8.9 Gestión de la configuración</p> | <p>Las configuraciones, incluidas las configuraciones de seguridad, de hardware, software, servicios y redes, se establecerán, documentarán, implementarán, supervisarán y revisarán.</p> | <p><b>OpManager Plus:</b> Utilice el módulo de gestión de configuración para programar copias de seguridad de la configuración de dispositivos, supervisar la actividad del usuario y detectar cambios mediante la comparación de versiones de configuración desde una interfaz gráfica de usuario web centralizada. Garantice la seguridad cifrando todos los datos de configuración recuperados de los dispositivos mediante el cifrado AES de 256 bits y almacenándolos de forma segura en la base de datos</p> <p><b>Site24x7:</b> Utilice la herramienta de gestión de la configuración de red (NCM) para gestionar las configuraciones de dispositivos de red dentro de su organización mediante la detección proactiva y el tratamiento de configuraciones inexactas o cambios no autorizados. Garantice una rápida restauración de las configuraciones funcionales de los dispositivos y minimice las interrupciones.</p> <p><b>Endpoint Central:</b> Prohíba a los usuarios instalar software innecesario y listas de permisos/listas de bloqueo para su entorno de TI. Evite que los ejecutables se ejecuten automáticamente. Controle los procesos secundarios que surjan de otras aplicaciones. Aplique políticas y configuraciones de seguridad para todos los endpoints y navegadores corporativos.</p> |
|----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                                           |                                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                           |                                                                                                                                                                        | <p><b>ServiceDesk Plus:</b> Cree y mantenga una CMDB de alta integridad que proporcione datos de dependencia precisos a través de mapas visuales. Registre y supervise las dependencias posteriores con el mapeo de relaciones impulsado por integraciones con soluciones de observabilidad como Site24x7.</p> <p><b>Log360:</b> Supervise y audite los cambios de configuración en las bases de datos, los servicios en la nube y los dispositivos de red para garantizar que los ajustes de seguridad se implementen y mantengan correctamente.</p>                                                               |
| 8.10<br>Eliminación de información        | La información almacenada en sistemas de información, dispositivos o en cualquier otro medio de almacenamiento se eliminará cuando ya no sea necesaria.                | <b>Endpoint Central:</b> Realice borrados remotos para garantizar la seguridad de los datos corporativos en caso de que se pierda un dispositivo. Aplique la contenedorización en dispositivos móviles para borrar de forma segura los datos corporativos y dejar intactos los datos personales.                                                                                                                                                                                                                                                                                                                    |
| 8.12<br>Prevención de la pérdida de datos | Las medidas de prevención de pérdidas de datos se aplicarán a los sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información sensible. | <b>Endpoint Central:</b> Utilice funciones avanzadas de prevención de pérdidas de datos para detectar y clasificar la información de identificación personal (PII). Obtenga un control completo sobre el flujo de datos dentro de su entorno de TI y configure políticas para transferencias de datos a través de servicios en la nube y dispositivos periféricos. Implemente y aplique políticas de BYOD en todos los dispositivos de usuario final para garantizar una separación clara entre los datos personales y corporativos en los dispositivos de usuario final, manteniendo la privacidad y la seguridad. |

|                                            |                                                                                                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                            |                                                                                                                                                                                                         | <p><b>Log360:</b> Garantice que la información confidencial permanezca protegida mediante la detección y el análisis en tiempo real de los incidentes de movimiento de datos y seguridad.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <p>8.13<br/>Respaldo de la información</p> | <p>Las copias de seguridad de la información, el software y los sistemas se mantendrán y probarán periódicamente de acuerdo con la política de copia de seguridad acordada sobre temas específicos.</p> | <p><b>Log360:</b> Garantice las copias de seguridad regulares y la integridad de los datos mediante el monitoreo de las actividades de copia de seguridad y restauración, la auditoría de las operaciones de almacenamiento y el seguimiento de los eventos del sistema. Verifique los procesos de copia de seguridad en bases de datos, entornos de nube y dispositivos de red para alinearse con las políticas de copia de seguridad y evitar la pérdida de datos.</p> <p><b>AD360:</b> Realice copias de seguridad de datos periódicas y guárdelas de forma segura como múltiples versiones cifradas, asegurándose de que puedan restaurarse en el improbable caso de pérdida de datos.</p> <p><b>PAM360:</b> Genere copias de seguridad periódicas de todas las credenciales de identidad privilegiadas, como contraseñas, claves SSH, token y certificados TLS en un archivo zip cifrado. Utilice las exportaciones cifradas de emergencia para mantener una copia de todas las credenciales privilegiadas en un dispositivo de respaldo o en el almacenamiento en la nube.</p> |

|               |                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|               |                                                                                                                                                     | <p><b>Endpoint Central:</b> Genere copias de seguridad instantáneas y no borrables de los archivos de su red cada tres horas aprovechando el servicio de copia oculta de volumen de Microsoft. Restaure cualquier archivo infectado con ransomware o dañado con su copia de seguridad más reciente con un solo clic.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 8.15 Registro | <p>Los logs que registren actividades, excepciones, fallos y otros eventos relevantes deberán producirse, almacenarse, protegerse y analizarse.</p> | <p><b>Log360:</b> Almacene y proteja los logs que recopilan actividades, excepciones y fallos en todos los sistemas, bases de datos y dispositivos de red.</p> <p><b>Endpoint Central:</b> Audite y supervise el acceso de los usuarios a endpoints críticos que llevan aplicaciones sensibles con informes de inicio de sesión de los usuarios. Obtenga informes de auditoría detallados que contengan solicitudes de acceso para aplicaciones populares en la lista de bloqueo.</p> <p><b>PAM360:</b> Registre todas las actividades relacionadas con el acceso privilegiado, como solicitudes de acceso, aprobaciones, motivo del acceso y las actividades reales realizadas en los endpoints accedidos.</p> <p><b>Firewall Analyzer:</b> Obtenga inteligencia de red crítica sobre intentos de violar la seguridad de la red y ataques como troyanos, ataques DDoS y más con un análisis en profundidad de los logs de seguridad del firewall. Utilice informes detallados del log de seguridad del firewall para llevar a cabo análisis del log de seguridad, visualizar escenarios de amenazas de red y planificar estrategias para defenderse contra estas amenazas.</p> |

|                                             |                                                                                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>8.16</p> <p>Actividades de monitoreo</p> | <p>Las redes, los sistemas y las aplicaciones se supervisarán en busca de comportamientos anómalos y se tomarán las medidas adecuadas para evaluar posibles incidentes de seguridad de la información.</p> | <p><b>Log360:</b> Monitoree sistemas, redes y aplicaciones para detectar comportamientos anómalos mediante el análisis de la actividad de inicio de sesión, los eventos del sistema y los cambios de configuración.</p> <p><b>Endpoint Central:</b> Aproveche el motor NGAV incorporado para detectar de forma proactiva el comportamiento anómalo con tecnología de aprendizaje profundo asistida por IA y detección de comportamiento en tiempo real.</p> <p><b>PAM360:</b> Monitoree continuamente las sesiones remotas en tiempo real para rastrear las actividades de los usuarios, detectar comportamientos sospechosos y garantizar el cumplimiento. Aproveche la integración de PAM360 con el motor UEBA de Log360 para analizar patrones, identificar anomalías y activar alertas de posibles amenazas de seguridad, mejorando el control general del acceso y la mitigación de riesgos.</p> <p><b>NetFlow Analyzer:</b> Aproveche la tecnología del motor de minería de flujo continuo para detectar una amplia gama de amenazas de seguridad externas e internas. Monitoree anomalías en la red que pasan su firewall e identifique anomalías sensibles al contexto e intrusiones el día cero con precisión.</p> <p><b>Site24x7:</b> Monitoree redes, sistemas y aplicaciones para detectar comportamientos anómalos, identificar posibles incidentes de seguridad y activar respuestas adecuadas en tiempo real. Aproveche los conocimientos impulsados por la IA y el análisis automatizado de la causa raíz para garantizar la mitigación proactiva de amenazas y el rendimiento de TI sin interrupciones.</p> |
|---------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                                                     |                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                     |                                                                                                                                               | <p><b>AD360:</b> Identifique y analice los riesgos de seguridad en entornos de AD y Microsoft 365, incluidos inicios de sesión fallidos, acceso a archivos, cambios de rol y actualizaciones de licencia con el informe Evaluación de riesgos de identidad. El motor UBA incorporado ayuda a detectar amenazas internas mediante el seguimiento de usuarios maliciosos, la identificación de cuentas comprometidas y la detección de abuso de privilegios.</p> |
| 8.18 Uso del programa de herramientas privilegiadas | Se restringirá y controlará rigurosamente el uso de programas de herramientas que puedan sobrepasar los controles de sistemas y aplicaciones. | <p><b>ServiceDesk Plus:</b> Escanee e identifique el software instalado en las estaciones de trabajo y clasifíquelo como gestionado o prohibido. Alerta al personal designado cuando se identifique software prohibido. Cree un dashboard de cumplimiento para identificar infracciones de políticas de software, como instancias de software sin licencia.</p>                                                                                                |
| 8.19 Instalación de software en sistemas operativos | Se aplicarán procedimientos y medidas para gestionar de forma segura la instalación de software en los sistemas operativos.                   | <p><b>Endpoint Central:</b> Implemente de forma segura aplicaciones de software en los sistemas de los usuarios finales. Agregue paquetes de software a los portales de autoservicio de los usuarios finales, lo que les permite instalar las aplicaciones a su conveniencia. Prohíba a los usuarios instalar aplicaciones innecesarias y cree listas de permisos/listas de bloqueo para el software en su entorno de TI.</p>                                  |

|                                           |                                                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>8.20</p> <p>Seguridad de las redes</p> | <p>Las redes y los dispositivos de red deberán estar protegidos, gestionados y controlados para proteger la información en sistemas y aplicaciones.</p> | <p><b>OpManager Plus:</b> Proteja su infraestructura de red con protocolos SSH y métodos de autenticación avanzados, incluyendo la autenticación de dos factores y AD.</p> <p><b>Network Configuration Manager:</b> Protéjase contra vulnerabilidades de firmware y optimice las actualizaciones de firmware sin esfuerzo utilizando configlets.</p> <p><b>Firewall Analyzer:</b> Mejore los controles de firewall para fortalecer la seguridad de la red de TI. Garantice el cumplimiento de las normas regulatorias de la industria. Supervise y analice la actividad de la red para detectar y abordar eventos de seguridad anómalos de manera efectiva.</p> <p><b>Log360:</b> Proteja y gestione los dispositivos de red mediante la supervisión de la actividad de inicio de sesión, los cambios de configuración y los eventos de seguridad</p> <p><b>Endpoint Central:</b> Configure el firewall de Windows para usuarios finales. Realice auditorías detalladas de puertos en su entorno de TI y reduzca su superficie de ataque bloqueando y asegurando los puertos abiertos. Habilite la navegación segura mediante la aplicación de extensas configuraciones de protección contra amenazas. Prohíba a los usuarios finales descargar archivos potencialmente maliciosos y acceder a sitios web maliciosos conocidos. Fortalezca los servidores web y corrija configuraciones erróneas de seguridad.</p> <p><b>AD360 o Identity360:</b> Proteja el acceso a todos los endpoints en las redes empresariales con métodos sólidos de MFA.</p> |
|-------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                                           |                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8.21<br>Seguridad de los servicios de red | Se identificarán, implementarán y supervisarán los mecanismos de seguridad, los niveles de servicio y los requisitos de servicio de los servicios de red. | <b>Firewall Analyzer:</b> Monitoree e informe sobre el uso de reglas, políticas y ACL de firewall. Recupere todas las reglas de firewall y genere informes de uso detallados y específicos de las reglas. Estos conocimientos le permiten evaluar la efectividad de sus reglas de firewall y optimizarlas para mejorar el rendimiento.                                                                                                     |
| 8.22<br>Segregación de redes              | Los grupos de servicios de información, usuarios y sistemas de información deberán estar segregados en las redes de la organización.                      | <b>Endpoint Central:</b> Aproveche la función de grupo personalizado para segregar lógicamente los sistemas para gestionarlos y protegerlos de manera más efectiva. Cree diferentes grupos estáticos o dinámicos para diferentes entornos operativos en función de los requisitos de la organización.                                                                                                                                      |
| 8.23<br>Filtrado web                      | El acceso a sitios web externos se gestionará para reducir la exposición a contenidos maliciosos.                                                         | <b>Endpoint Central:</b> Bloquee sitios web maliciosos para evitar que los usuarios accedan a ellos.                                                                                                                                                                                                                                                                                                                                       |
| 8.24 Uso de criptografía                  | Se definirán y aplicarán normas para el uso efectivo de la criptografía, incluida la gestión de claves criptográficas.                                    | <p><b>Endpoint Central:</b> Cifre dispositivos de usuarios finales mediante BitLocker para sistemas Windows y cifrado FileVault para dispositivos Mac.</p> <p><b>PAM360:</b> Encripte todas las credenciales, cuentas y otras entidades críticas, tanto a nivel de aplicación como de base de datos, utilizando el algoritmo de cifrado simétrico AES-256; y almacene solo estos datos encriptados en la base de datos de contraseñas.</p> |

|                                |                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>8.32 Gestión de cambios</p> | <p>Los cambios en las instalaciones de tratamiento de la información y los sistemas de información estarán sujetos a procedimientos de gestión de cambios</p> | <p><b>ServiceDesk Plus:</b> Gestione los cambios en las instalaciones y sistemas de procesamiento de información con funciones de habilitación de cambios certificadas por ITIL. Controle los cambios con flujos de trabajo definidos, mecanismos de evaluación de riesgos impulsados por IA y procedimientos de autorización para minimizar los riesgos y las violaciones de cumplimiento.</p> <p><b>OpManager Plus:</b> Gestione los cambios de forma efectiva utilizando el módulo de gestión de configuración. Obtenga notificaciones de cambios en tiempo real, evite las modificaciones no autorizadas mediante el control de acceso basado en roles, vuelva rápidamente a versiones de confianza con una funcionalidad de reversión e identifique sin problemas los cambios de configuración mediante la vista de diferencias, la función de comparación codificada por colores dentro del producto.</p> |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

# Los productos de ManageEngine y los controles de la ISO 27001 compatibles

| Productos de ManageEngine                                                                                         | Controles compatibles                                                                                                                                                                                       |
|-------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  ServiceDesk Plus                | 5.9, 5.11, 5.15, 5.18, 5.19, 5.21, 5.23, 5.24, 5.25, 5.26, 5.27, 5.28, 5.31, 5.34, 5.36, 6.8, 7.10, 7.14, 8.1, 8.9, 8.18, 8.32                                                                              |
|  Endpoint Central                | 5.7, 5.9, 5.11, 5.12, 5.13, 5.15, 5.17, 5.18, 5.28, 5.30, 5.31, 5.32, 5.33, 5.34, 5.36, 6.7, 7.10, 7.14, 8.1, 8.2, 8.3, 8.5, 8.6, 8.7, 8.8, 8.9, 8.10, 8.12, 8.13, 8.15, 8.16, 8.19, 8.20, 8.22, 8.23, 8.24 |
|  AD360                           | 5.15, 5.16, 5.17, 5.18, 5.33, 5.34, 5.36, 6.7, 8.1, 8.3, 8.5, 8.7, 8.13, 8.16, 8.20                                                                                                                         |
|  Identity360                     | 5.15, 5.16, 5.18, 5.34, 8.1, 8.3, 8.5, 8.20                                                                                                                                                                 |
|  PAM360                          | 5.9, 5.11, 5.15, 5.18, 5.28, 5.33, 6.7, 8.2, 8.3, 8.5, 8.13, 8.15, 8.16, 8.24                                                                                                                               |
|  Log360                        | 5.7, 5.9, 5.11, 5.14, 5.15, 5.17, 5.18, 5.23, 5.26, 5.28, 5.31, 8.7, 8.9, 8.12, 8.13, 8.15, 8.16, 8.20                                                                                                      |
|  OpManager Plus                | 5.9, 5.15, 5.18, 5.31, 5.34, 5.36, 8.5, 8.6, 8.8, 8.9, 8.20, 8.32                                                                                                                                           |
|  Site24x7                      | 5.9, 5.23, 8.6, 8.9, 8.16                                                                                                                                                                                   |
|  Analytics Plus                | 5.9, 5.11, 5.32, 6.7, 8.6                                                                                                                                                                                   |
|  AppCreator                    | 5.9, 5.11, 5.15, 5.18, 5.34                                                                                                                                                                                 |
|  Firewall Analyzer             | 5.36, 8.15, 8.20, 8.21                                                                                                                                                                                      |
|  DataSecurity Plus             | 5.9, 5.11, 5.12                                                                                                                                                                                             |
|  AssetExplorer                 | 5.9, 5.11                                                                                                                                                                                                   |
|  Network Configuration Manager | 8.20                                                                                                                                                                                                        |
|  NetFlow Analyzer              | 8.16                                                                                                                                                                                                        |

# Tome el control de su TI

Supervise, administre y proteja su empresa digital con ManageEngine.



## **Gestiona identidades digitales y acceso**

Gestione, controle y proteja las identidades digitales en toda su organización con orquestación de identidades, seguridad de acceso privilegiado, CIEM, MFA, SSO, controles de acceso basados en roles y más.

[manageengine.com/latam/herramientas-de-gestion-de-identidades-y-accesos-iam.html](https://manageengine.com/latam/herramientas-de-gestion-de-identidades-y-accesos-iam.html)



## **Ofrezca experiencias de servicio inteligentes**

Mejore sus flujos de trabajo de entrega de servicios a través de las mejores prácticas de ITSM recomendadas por la industria, la potente orquestación y las funciones nativas de IA.

[manageengine.com/latam/gestion-de-servicios-usm.htm](https://manageengine.com/latam/gestion-de-servicios-usm.htm)



## **Controle y proteja cada endpoint**

Gestione, proteja y controle todos sus endpoints a través de diversas funciones como computación de usuario final, ciberseguridad, gobernanza, riesgo y cumplimiento, I/O y más.

[manageengine.com/latam/soluciones-seguridad-gestion-unificada-de-endpoints.html](https://manageengine.com/latam/soluciones-seguridad-gestion-unificada-de-endpoints.html)



## **Fortalezca las operaciones de red y TI**

Logre una visibilidad de toda su red y pila de aplicaciones con la observabilidad impulsada por la IA. Resuelva problemas de forma proactiva, optimice el rendimiento y mejore la seguridad de TI.

[manageengine.com/latam/herramientas-de-gestion-de-operaciones-ti.html](https://manageengine.com/latam/herramientas-de-gestion-de-operaciones-ti.html)



### **Aumente la seguridad y cumplimiento de la TI**

Detecte, investigue y responda a las amenazas de seguridad con UEBA, inteligencia de amenazas y monitoreo del log. Cumpla con las normas y mitigue los riesgos con informes listos para la auditoría.

[manageengine.com/latam/soluciones-gestion-de-eventos-e-informacion-de-seguridad-siem.html](https://manageengine.com/latam/soluciones-gestion-de-eventos-e-informacion-de-seguridad-siem.html)



### **Percepciones unificadas de toda la TI**

Visualice cada faceta de la TI fácilmente. Con la inteligencia de decisiones, identifique y aborde los riesgos de manera preventiva, y obtenga estrategias contextuales prácticas para los cuellos de botella operativos.

[manageengine.com/latam/herramientas-analisis-avanzado-ti-sitios-web.html](https://manageengine.com/latam/herramientas-analisis-avanzado-ti-sitios-web.html)



### **Optimice la TI con aplicaciones de código bajo**

Amplíe las funciones de su proceso de TI combinando código bajo y GenAI. Aborde rápidamente los desafíos de TI e innove con una codificación mínima, lo que hace que su organización sea más ágil.

[manageengine.com/latam/herramientas-desarrollo-aplicaciones-con-low-code.html](https://manageengine.com/latam/herramientas-desarrollo-aplicaciones-con-low-code.html)

# Sobre ManageEngine

ManageEngine confecciona el paquete más grande de software para la gestión de TI en la industria. Tenemos todo lo que necesita, más de 60 productos, para gestionar todas sus operaciones de TI, desde redes y servidores hasta aplicaciones, mesas de servicio, Active Directory, seguridad, desktop y dispositivos móviles. Desde 2002, equipos de TI como el suyo han venido a nosotros en busca de un software asequible y rico en funciones que sea fácil de usar.

Mientras se prepara para los retos de la gestión de TI que tiene en frente, seguiremos siendo pioneros con nuevas soluciones, integraciones contextuales y otros avances que solo pueden venir de una compañía singularmente dedicada a sus clientes. Y como una división de Zoho Corporation, continuaremos trabajando para buscar el estrecho alineamiento con las TI comerciales que necesita para que aproveche las oportunidades en el futuro.





Para  
más  
información

[www.manageengine.com/latam/](http://www.manageengine.com/latam/) |  
[sales@manageengine.com](mailto:sales@manageengine.com)