ManageEngine

Guía de ManageEngine para la implementación de los **Controles de CIS®** en su organización

Índice

Índice

Descargo de responsabilidad

Este material y su contenido ("Material") tienen por objeto, entre otras cosas, presentar una visión general de cómo puede utilizar los productos y servicios de ManageEngine para implementar los Controles de CIS® en su organización. Cumplir plenamente con los controles de CIS requiere de 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 CIS. Junto con otras soluciones, procesos y personas apropiadas, las soluciones de ManageEngine ayudan a las organizaciones a implementar los controles de CIS. Este Material se proporciona con fines informativos únicamente y no debe considerarse como asesoramiento jurídico para la implementación de los Controles de CIS. ManageEngine no ofrece ninguna garantía, expresa, implícita o estatutaria, y no asume ninguna responsabilidad en cuanto a la información de este Material.

Una breve introducción a los controles de CIS®

Los Controles de CIS son un conjunto prescriptivo y prioritario de mejores prácticas en seguridad informática y acciones defensivas que pueden ayudar a prevenir los ataques más peligrosos y de mayor alcance. Estos controles ayudan a las organizaciones a fortalecer su defensa informática y ayudan a respaldar el cumplimiento en una era de múltiples marcos. Los Controles de CIS cumplen con la mayoría de los principales marcos de cumplimiento, los cuales incluyen NIST Cybersecurity Framework, NIST 800-53, NIST 800-171, la serie ISO 27000, y regulaciones tales como PCI DSS, HIPAA, NERC CIP, y FISMA. Por consiguiente, proporcionan una orientación específica y una vía clara para que las organizaciones alcancen las metas y los objetivos descritos por múltiples marcos jurídicos, reglamentarios y normativos.

La estructura de los controles de CIS®

Los Controles de CIS comprenden un conjunto de 20 recomendaciones de seguridad informática que se dividen en tres categorías distintas—básicos, Fundamentales y organizacionales—y estos 20 controles se dividen a su vez en sub-controles. Los controles de CIS no son una solución única para todo problema; según la madurez de la seguridad informática de su organización, usted puede planificar y priorizar la implementación de varios controles.

Controles de CIS básicos (1-6)

Estos son controles de seguridad de uso general que cada organización debe implementar para garantizar la disponibilidad de una defensa informática esencial.

Controles de CIS fundamentales (7-16)

Estos son controles que las organizaciones deben implementar para contrarrestar amenazas técnicas más específicas.

Controles de CIS organizacionales (17-20)

Estos controles están menos enfocados en aspectos técnicos y más enfocados en las personas y los procesos involucrados con la seguridad informática. La organización debe implementar estas prácticas clave internamente para garantizar la madurez de la seguridad a largo plazo.

Controles de CIS

Básicos	Fundamentales	Organizacionales
Inventario y control de activos de hardware	Protección de correo electrónico y navegador web	Implementar un programa de concienciación y capacitación en seguridad
Inventario y control de activos de software	Defensas contra malware	Seguridad del software de aplicación
Gestión continua de vulnerabilidades	Limitación y control de puertos de red, protocolos y servicios	Respuesta y gestión de incidentes
Uso controlado de los privilegios administrativos	Funciones de recuperación de datos	Pruebas de penetración y ejercicios de Red Team
Configuración segura para el hardware y el software de los dispositivos móviles, laptops, estaciones de trabajo y servidores	Configuración segura para dispositivos de red, tales como firewalls, routers y switches	
Mantenimiento, monitoreo, y análisis de logs de auditoría	Protección perimetral	
	Protección de datos	
	Control de acceso basado en la necesidad de saber	
	Control de acceso inalámbrico	
	Monitoreo y control de cuentas	

Los grupos de implementación de CIS

Además de los controles básicos, Fundamentales y organizacionales, en la última versión de los controles de CIS, V7.1, se priorizan los controles en Grupos de Implementación (IG). Cada IG identifica cuales Sub-Controles debería implementar una organización en función de su perfil de riesgo y de los recursos que disponga.

Se alienta a las organizaciones a que se autoevalúen y se clasifiquen dentro de uno de los tres IG para priorizar los controles de CIS a fin de mejorar su postura de seguridad informática. Las organizaciones deberían empezar por implementar los Sub-Controles en IG1, seguido de IG2 y luego IG3. La implementación de IG1 se debe considerar como una de las primeras cosas que se deben hacer como parte de un programa de seguridad informática. CIS se refiere a IG1 como "higiene cibernética"; es decir, las protecciones esenciales que se deben poner en marcha para defenderse de los ataques comunes.

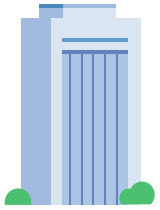
Para saber más sobre los controles de CIS y sub-controles, por favor visite su página web CIS Controls Navigator.

IG1

Las organizaciones con recursos limitados, en las que la sensibilidad de los datos es baja, tendrán que aplicar los Sub-Controles que típicamente entran en la categoría IG1.

IG2

Las organizaciones con recursos moderados y un mayor riesgo de exposición por manejar activos y datos más sensibles e importantes tendrán que implementar los controles de IG2 junto con los de IG1. Estos Sub-Controles se enfocan en ayudar a los equipos de seguridad a gestionar información sensible de clientes o empresas.



IG3

Las organizaciones maduras con recursos importantes y una alta exposición al riesgo para el manejo de activos y datos críticos necesitan implementar los Sub-Controles de la categoría IG3 junto con los de IG1 e IG2. Los Sub-Controles que ayudan a reducir el impacto de los ataques dirigidos de adversarios sofisticados normalmente entran en la categoría IG3.

Definiciones	1	2	3
GRUPO DE IMPLEMENTACIÓN 1 **Una organización con recursos limitados y con cierta exposición a riesgos** Sub-controles de CIS para pequeños entornos de software comercial o de oficina en casa, en los que la sensibilidad de los datos es baja y que típicamente entran en la categoría de IG1. IG1 representa una higiene cibernética básica para todas las organizaciones, incluidas aquellas con IG2 e IG3.	●		
GRUPO DE IMPLEMENTACIÓN 2 **Una organización con recursos moderados y una mayor exposición al riesgo** Los sub-controles de CIS (medidas de seguridad) se enfocan en ayudar a las organizaciones a manejar activos y datos de mayor sensibilidad. Las medidas de seguridad IG2 también deben ser adoptadas por las organizaciones que tienen IG3.	●	●	
GRUPO DE IMPLEMENTACIÓN 3 **Una organización madura con recursos importantes y una exposición de alto riesgo** Los sub-controles de CIS (medidas de seguridad) son necesarios para las organizaciones que manejan activos y datos críticos. IG3 engloba las medidas de seguridad en IG1 e IG3.	●	●	●

"La mayoría de las violaciones cibernéticas se producen cuando no se han aplicado y gestionado los controles de seguridad básicos. El Grupo de Implementación 1 de los controles de CIS son eficaces contra los 5 ataques principales como se describen en el Informe de violación de datos de Verizon."

– Curtis Dukes, vicepresidente ejecutivo del Grupo de Mejores Prácticas de Seguridad y Automatización en CIS

El rol de las soluciones de ManageEngine

El paquete de soluciones de gestión de TI de ManageEngine le ayudará a cumplir con los requisitos discretos de control de CIS y a su vez ayudará a su organización a planear cuidadosamente y desarrollar un programa de seguridad de primera clase para lograr una mejor higiene cibernética.

Productos de ManageEngine asignados a los Controles

Hemos asignado nuestros productos a los sub-controles de CIS que ayudan a cumplir.

CONTROLES DE CIS
BÁSICOS

CONTROL 1

Inventario y control de activos de hardware

Supervise activamente y gestione todos los dispositivos de hardware conectados a su red. Mantenga un inventario actualizado de todos sus activos tecnológicos y disponga de un sistema de autenticación para garantizar que los dispositivos no autorizados no tengan acceso a su red.

Asignación de los Sub-Controles a los productos de ManageEngine

Sub -Control	Tipo de activo	Función de seguridad	Título del control	Descripción del control	Productos de ManageEngine	Grupos de qimplementación		
						1	2	3
1.1	Dispositivos	Identificar	Utilizar una herramienta de descubrimiento activa	Utilice una herramienta de descubrimiento activa para identificar los dispositivos conectados a la red de la organización y para actualizar el inventario de activos de hardware.	**Desktop Central** y **AssetExplorer:** Conéctese a su entorno Active Directory (AD) y analice los detalles de su inventario en su infraestructura.		IG2	IG3
1.2	Dispositivos	Identificar	Utilizar una herramienta de descubrimiento de activos pasiva	Utilice una herramienta de descubrimiento pasiva para identificar los dispositivos conectados a la red de la organización y así actualizar automáticamente el inventario de activos de hardware de la organización.	**OpUtils:** Analice periódicamente la red para detectar nuevos sistemas o dispositivos. Puede marcar los sistemas y dispositivos como confiables, invitados y maliciosos. Utilizando esta herramienta, usted también puede bloquear el puerto de switch de dispositivos maliciosos.			IG3
1.3	Dispositivos	Identificar	Utilizar el registro de DHCP para actualizar el inventario de activos	Registre todos los servidores DHCP o herramientas de gestión de direcciones IP mediante el protocolo de configuración dinámica de host (DHCP) para actualizar el inventario de activos de hardware de la organización.	**OpUtils:** Monitoree los alcances DHCP para encontrar el recuento disponible de direcciones IP con la ayuda del monitor de alcance de DHCP. Cuando el recuento de direcciones IP disponibles está por debajo de un número determinado, los resultados se muestran en rojo.		IG2	IG3

Sub -Control	Tipo de activo	Función de seguridad	Título del control	Descripción del control	Productos de ManageEngine	Grupos de qimplementación		
						1	2	3
1.4	Dispositivos	Identificar	Mantener un inventario de activos detallado	Mantenga un inventario preciso y actualizado de todos los activos tecnológicos con potencial para almacenar o procesar información. Este inventario incluirá todos los activos, ya sea que estén conectados a la red de la organización o no.	**Desktop Central** y **AssetExplorer:** Conéctese a su entorno AD y analice los detalles de su inventario en su infraestructura.	IG1	IG2	IG3
1.5	Dispositivos	Identificar	Mantener información del inventario de activos	Garantice que el inventario de activos de hardware registre la dirección de red, la dirección de hardware, el nombre del equipo, el propietario del activo de datos y el departamento de cada activo, y si el activo de hardware ha sido aprobado para conectarse a la red.	**Desktop Central** y **AssetExplorer:** Conéctese a su entorno AD y analice los detalles de su inventario en su infraestructura.		IG2	IG3
1.6	Dispositivos	Responder	Tratar los activos no autorizados	Garantice que los activos no autorizados sean removidos de la red, puestos en cuarentena o que el inventario sea actualizado de manera oportuna.	**OpUtils:** Detecte dispositivos no autorizados mediante análisis manuales o automáticos de su red. También puede marcar una dirección IP como confiable, bloquear dispositivos maliciosos y manipular los puertos de sus switches para prevenir que los dispositivos no autorizados tengan acceso a su red.	IG1	IG2	IG3

Sub -Control	Tipo de activo	Función de seguridad	Título del control	Descripción del control	Productos de ManageEngine	Grupos de qimplementación		
						1	2	3
1.7	Dispositivos	Proteger	Implementar el control de acceso a nivel de puerto	Utilice el control de acceso a nivel de puerto siguiendo el estándar 802.1x para controlar cuál dispositivo puede ser autenticado para la red. El sistema de autenticación estará enlazado con los datos de inventario de activos de hardware para garantizar que solamente los dispositivos autorizados puedan conectarse a la red.	**OpUtils:** Utilice el acceso a nivel de puerto para apagar o habilitar una conexión de interfaz en un puerto de switch. Usted puede gestionar los dispositivos conectados en un puerto; no obstante, esta acción se debe realizar manualmente para restringir a los dispositivos que puedan conectarse a su red. Tendrá que seleccionar los dispositivos (único o múltiple) a la vez para restringir su conexión a su red. Al agregar dispositivos confiables, usted puede subir un archivo CSV o configurar al producto para que busque esa información en AD.		IG2	IG3
1.8	Dispositivos	Proteger	Utilizar certificados de cliente para autenticar activos de hardware	Utilice certificados de cliente para autenticar activos de hardware conectados a la red confiable de la organización.	**Desktop Central:** Analice los equipos de la red para obtener datos de inventario. Puede autenticar activos de hardware utilizando los detalles del certificado de activo específico.			IG3

CONTROL 2

Inventario y control de activos de software

Disponga de un sistema de inventario de software para supervisar y gestionar activamente todo el software que se esté ejecutando en su red.

Utilice la lista blanca de aplicaciones para garantizar que sólo se instale y ejecute software autorizado y que se bloquee el software no autorizado.

Asignación de los Sub-Controles a los productos de ManageEngine

Sub -Control	Tipo de activo	Función de seguridad	Título del control	Descripción del control	Productos de ManageEngine	Grupos de qimplementación		
						1	2	3
2.1	Aplicaciones	Identificar	Mantener un inventario de software autorizado	Mantenga una lista actualizada de todo software autorizado requerido por la empresa para cualquier propósito de negocios en cualquier sistema de negocios.	**Desktop Central:** Gestione el software autorizado en su empresa.	IG1	IG2	IG3
2.3	Aplicaciones	Identificar	Utilizar her-ramientas de inventario de software	Utilice herramientas de inventario de software en toda la organización para automatizar la documentación de todo el software en los sistemas de negocio.	**Desktop Central:** Analice los sistemas para cualquier software que esté instalado.		IG2	IG3
2.4	Aplicaciones	Identificar	Supervisar la información de inventario de software	El sistema de inventario de software debe hacer un seguimiento del nombre, la versión, el proveedor y la fecha de in-stalación de todo el software, incluidos los sistemas operativos autorizados por la organización.	**Desktop Central:** Analice los sistemas para obtener información de software.		IG2	IG3
2.5	Aplicaciones	Identificar	Integrar los inventarios de activos de software y hardware	El sistema de inventario de software debe estar enlazado con el inventario de activos de hardware para que todos los dispositivos y software asociado puedan ser supervisados desde un solo lugar.	**Desktop Central:** Obtenga la lista completa del software instalado en cada equipo.			IG3

Sub -Control	Tipo de activo	Función de seguridad	Título del control	Descripción del control	Productos de ManageEngine	Grupos de qimplementación		
						1	2	3
2.6	Aplicaciones	Responder	Tratar el software no aprobado	Garantice que el software no autorizado sea removido o que el inventario sea actualizado de manera oportuna.	**Desktop Central:** Programe un análisis de inventario, y elimine el software que esté marcado como prohibido.	IG1	IG2	IG3
2.7	Aplicaciones	Proteger	Utilizar una lista blanca de aplicaciones	Utilice la tecnología de lista blanca de aplicaciones en todos los activos para garantizar que solamente el software autorizado se ejecute, y que se bloquee la ejecución de todo software no autorizado en los activos.	**Application Control Plus:** Analice los sistemas para identificar el software instalado en su red. Puede hacer una lista blanca de aplicaciones y permitir que sólo esos programas se ejecuten en dispositivos gestionados.			IG3
2.8	Aplicaciones	Proteger	Implementar una lista blanca de aplicaciones en bibliotecas	El software de lista blanca de aplicaciones de la organización debe garantizar que solamente las bibliotecas de software autorizado (tales como *.dll, *.ocx, *.so, etc.) estén permitidas para ser cargadas en un proceso del sistema.	**Application Control Plus:** Establezca la política más segura basada en el valor de hash del archivo ejecutable. Se mostrarán todos los archivos ejecutables de los procesos en ejecución, incluidos los que no tienen un certificado digital válido. Puede elegir todos los archivos que desee incluir en la lista blanca; después de eso, incluso el más pequeño cambio en el archivo, como una revisión de la versión del archivo, cambiará su valor de hash, lo que significa que el archivo se eliminará instantáneamente de la lista blanca de aplicaciones.			IG3
2.10	Aplicaciones	Proteger	Segregar de forma física o lógica las aplicaciones de alto riesgo	Los sistemas segregados física o lógicamente deben ser utilizados para aislar y ejecutar software que es requerido para las operaciones de negocios, pero que incurren en un mayor riesgo para la organización.	**Desktop Central:** Genere informes para identificar los sistemas que ejecuten operaciones de negocios.			IG3

CONTROL 3

Gestión continua de vulnerabilidades

Analice continuamente sus activos para identificar vulnerabilidades potenciales y poder remediarlas a tiempo. Fortalezca la seguridad de su red garantizando que el software y los sistemas operativos utilizados en su organización ejecuten las actualizaciones de seguridad más recientes.

Asignación de los Sub-Controles a los productos de ManageEngine

Sub -Control	Tipo de activo	Función de seguridad	Título del control	Descripción del control	Productos de ManageEngine	Grupos de qimplementación		
						1	2	3
3.1	Aplicaciones	Detectar	Ejecutar herramientas de análisis de vulnerabilidades automatizadas	Utilice una herramienta actualizada de análisis de vulnerabilidades conforme al Protocolo de Automatización de Contenidos de Seguridad (SCAP) para analizar automáticamente todos los sistemas de la red semanalmente, o con mayor frecuencia, para identificar todas las vulnerabilidades potenciales de los sistemas de la organización.	**Vulnerability Manager Plus:** Analice los sistemas para identificar vulnerabilidades del sistema operativo, vulnerabilidades de terceros y vulnerabilidad de día cero y remediar la vulnerabilidad si el proveedor ha lanzado un parche para ello.		IG2	IG3
3.2	Aplicaciones	Detectar	Realizar un análisis de vulnerabilidades autenticado	Realice un análisis de vulnerabilidades autenticado con agentes que se ejecuten localmente en cada sistema o con escáneres remotos que estén configurados con derechos elevados en el sistema que se esté probando.	**Vulnerability Manager Plus:** El modelo basado en el agente del producto se pone en contacto con el servidor cada 90 minutos para recibir actualizaciones.		IG2	IG3

Sub -Control	Tipo de activo	Función de seguridad	Título del control	Descripción del control	Productos de ManageEngine	Grupos de qimplementación		
						1	2	3
3.4	Aplicaciones	Proteger	Implementar una herramienta de gestión de parches del sistema operativo automatizada	Implemente una herramienta de actualización de software automatizada para garantizar que los sistemas operativos se ejecuten con las actualizaciones de seguridad más recientes proporcionadas por el proveedor de software.	**Desktop Central:** Lleve a cabo la instalación de parches de múltiples maneras. El producto identifica los parches faltantes en los sistemas y automatiza su instalación.	IG1	IG2	IG3
3.5	Aplicaciones	Proteger	Implementar una herramienta de gestión de parches de software automatizada	Implemente una herramienta de actualización de software automatizada para garantizar que el software de terceros se ejecute con las actualizaciones de seguridad más recientes proporcionadas por el proveedor de software.	**Desktop Central:** El producto es compatible con más de 250 aplicaciones de terceros para la gestión de parches.	IG1	IG2	IG3
3.6	Aplicaciones	Responder	Comparar los de análisis de vulnerabilidades entre sí	Compare regularmente los resultados de los análisis de vulnerabilidades consecutivos para verificar que las vulnerabilidades han sido remediadas de manera oportuna.	**Vulnerability Manager Plus:** Los sistemas vulnerables son removidos de la base de datos de vulnerabilidades únicamente cuando se ha corregido la vulnerabilidad. Una vez que se ha realizado la corrección, el producto marcará al sistema como saludable.		IG2	IG3
3.7	Aplicaciones	Responder	Utilizar un proceso de clasificación de riesgos	Utilice un proceso de clasificación de riesgos para dar prioridad a la corrección de vulnerabilidades descubiertas.	**Vulnerability Manager Plus:** El producto categoriza las vulnerabilidades en función de la gravedad y el estado de explotación, y puede implementar parches basados en esta información.		IG2	IG3

CONTROL 4

Uso controlado de los privilegios administrativos

Monitoree los controles de acceso y el comportamiento de los usuarios de las cuentas privilegiadas para evitar el acceso no autorizado a los sistemas críticos. Garantice que sólo las personas autorizadas tengan privilegios elevados para evitar el uso indebido de los privilegios administrativos.

Asignación de los Sub-Controles a los productos de ManageEngine

Sub -Control	Tipo de activo	Función de seguridad	Título del control	Descripción del control	Productos de ManageEngine	Grupos de qimplementación		
						1	2	3
4.1	Usuarios	Detectar	Mantener el inventario de las cuentas administrativas	Utilice herramientas automatizadas para hacer un inventario de todas las cuentas administrativas, incluidas las cuentas de dominio y las cuentas locales, para garantizar que sólo las personas autorizadas tengan privilegios elevados	**Desktop Central:** Reciba informes sobre los usuarios administradores de dominio. **ADManager Plus:** Reciba informes de todos los grupos en AD y sus miembros. **Password Manager Pro:** Descubra los recursos de su infraestructura e identifique las cuentas locales en sus sistemas.		IG2	IG3
4.2	Usuarios	Proteger	Cambiar las contraseñas predeterminadas	Antes de implementar cualquier activo nuevo, cambie todas las contraseñas predeterminadas para tener valores consistentes con las cuentas de nivel administrativo.	**Desktop Central:** Cambie las contraseñas de las cuentas locales.	IG1	IG2	IG3

Sub -Control	Tipo de activo	Función de seguridad	Título del control	Descripción del control	Productos de ManageEngine	Grupos de qimplementación		
						1	2	3
4.4	Usuarios	Proteger	Usar contraseñas únicas	Cuando no sea compatible la autenticación multifactor (como las cuentas de administrador local, root o de servicio), las cuentas utilizarán contraseñas exclusivas de ese sistema.	**Password Manager Pro:** Establece una contraseña única para las cuentas locales, o permite que el producto cree una contraseña por sí mismo.		IG2	IG3
4.8	Usuarios	Detectar	Registrar y alertar cambios de miembros en grupos administrativos	Configure los sistemas para que generen una entrada de log y una alerta cuando se añada o elimine una cuenta de cualquier grupo al que se le hayan asignado privilegios administrativos.	**ADAudit Plus:** Reciba una alerta cada vez que haya un cambio de permiso en AD.		IG2	IG3
4.9	Usuarios	Detectar	Registrar y alertar inicios de sesión fallidos en cuentas administrativas	Configure los sistemas para generar una entrada de log y una alerta sobre los inicio de sesión fallidos en una cuenta administrativa.	**ADAudit Plus:** Acceda a los informes predeterminados sobre los inicios de sesión exitosos y fallidos.		IG2	IG3

CONTROL 5

Configuración segura para el hardware y el software de los dispositivos móviles, laptops, estaciones de trabajo y servidores

Establezca y mantenga configuraciones de seguridad basadas en los estándares de configuración aprobados por su organización. Defina un riguroso sistema de gestión de configuraciones que monitoree y alerte sobre las configuraciones erróneas e implemente un proceso de control de cambios para impedir que los atacantes se aprovechen de los servicios y configuraciones vulnerables.

Asignación de los Sub-Controles a los productos de ManageEngine

Sub -Control	Tipo de activo	Función de seguridad	Título del control	Descripción del control	Productos de ManageEngine	Grupos de qimplementación		
						1	2	3
5.2	Aplicaciones	Proteger	Mantener imágenes seguras	Mantenga imágenes o plantillas seguras para todos los sistemas de la empresa basadas en los estándares de configuración aprobados por la organización. Se debe crear una imagen de cualquier implementación de un nuevo sistema o un sistema existente que se vea comprometido usando una de esas imágenes o plantillas.	**OS Deployer:** Cree una imagen de un sistema existente y úsela como plantilla para crear una imagen de otros sistemas (sólo en Windows). El producto ofrece múltiples formas de crear una imagen de un sistema en línea o fuera de línea.		IG2	IG3

Sub -Control	Tipo de activo	Función de seguridad	Título del control	Descripción del control	Productos de ManageEngine	Grupos de qimplementación		
						1	2	3
5.3	Aplicaciones	Proteger	Almacenar de forma segura de las imágenes maestras	Almacene las imágenes maestras y las plantillas en servidores configurados de forma segura, validados con herramientas de monitoreo de la integridad, para garantizar que sólo se puedan realizar cambios autorizados en las imágenes.	**OS Deployer:** Cambie la ubicación del repositorio de imágenes a una ruta segura.		IG2	IG3
5.4	Aplicaciones	Proteger	Implementar herramientas de gestión de configuración del sistema	Implemente herramientas de gestión de la configuración del sistema que aplicarán y volverán a implementar automáticamente los ajustes de configuración en los sistemas a intervalos regulares programados.	**Desktop Central:** Aplique y vuelva a implementar automáticamente los ajustes de configuración en cada inicio o conexión del sistema.		IG2	IG3
5.5	Aplicaciones	Proteger	Implementar sistemas de monitoreo de configuración automatizado	Utilice un sistema de monitoreo de configuración que cumpla con el Protocolo de Automatización de Contenidos de Seguridad (SCAP) para verificar todos los elementos de la configuración de seguridad, catalogar las excepciones aprobadas y alertar cuando ocurran cambios no autorizados.	**Desktop Central:** Reciba alertas automatizadas cuando falle una configuración implementada**.**		IG2	IG3

CONTROL 6

Mantenimiento, monitoreo, y análisis de logs de auditoría

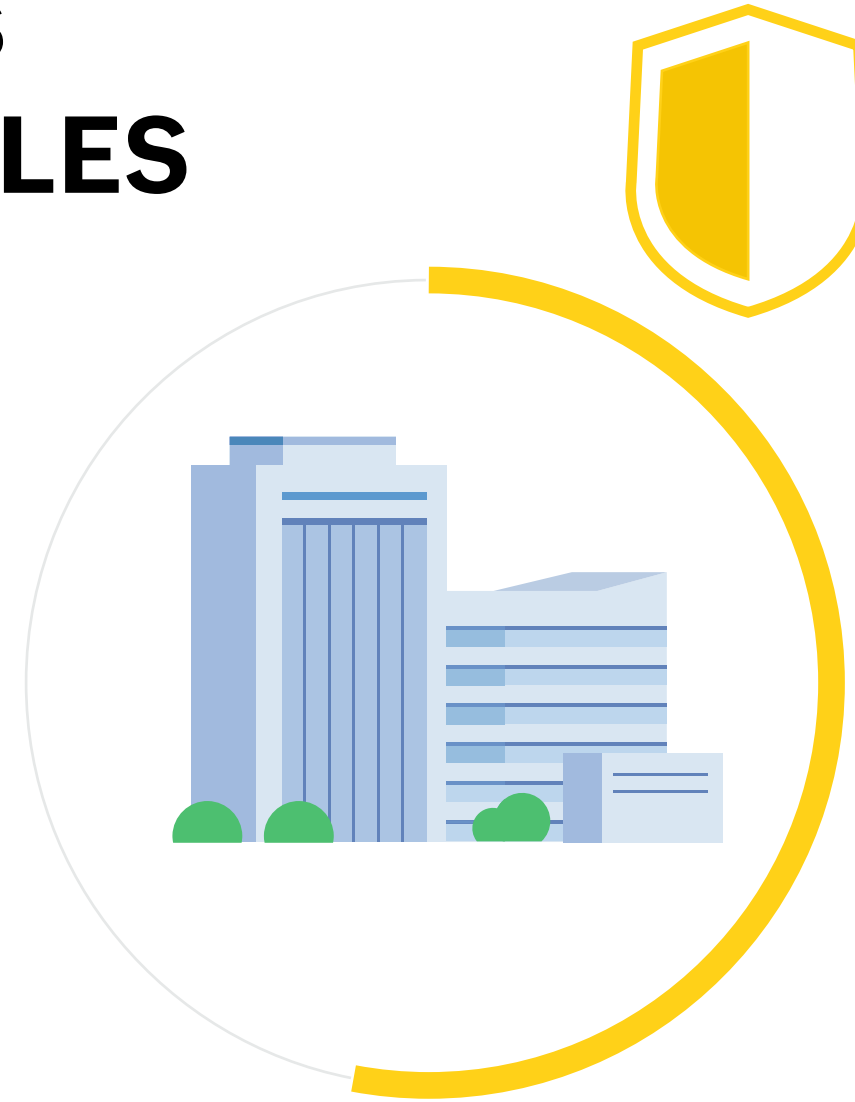
Recopile, gestione y analice los logs de auditoría de los eventos para detectar anomalías. Mantenga registros de log para comprender los detalles de los ataques a fin de responder a los incidentes de seguridad de manera eficaz.

Asignación de los Sub-Controles a los productos de ManageEngine

Sub -Control	Tipo de activo	Función de seguridad	Título del control	Descripción del control	Productos de ManageEngine	Grupos de qimplementación		
						1	2	3
6.1	Red	Detectar	Usar tres fuentes de tiempo sincronizadas	Utilice por lo menos tres fuentes de tiempo sincronizadas de las que todos los servidores y dispositivos de red recuperen información de tiempo de manera regular, de modo que las marcas de tiempo en los logs sean consistentes.	**Desktop Central:** Utilice una configuración de Windows para establecer un servidor de tiempo para todos los sistemas que maneja Desktop Central.		IG2	IG3
6.2	Red	Detectar	Activar el registro de auditoría	Garantice que se ha habilitado el registro local en todos los sistemas y dispositivos de red.	**EventLog Analyzer:** Reciba informes de inicio de sesión para estaciones de trabajo, servidores, bases de datos y dispositivos de red como routers y switches.	IG1	IG2	IG3
6.3	Red	Detectar	Habilitar el registro detallado	Permita que el registro del sistema incluya información detallada como la fuente del evento, la fecha, el usuario, la hora, las direcciones de la fuente, las direcciones de destino y otros elementos útiles.	**EventLog Analyzer:** Reciba informes detallados de todos los elementos mencionados en la descripción del Control.		IG2	IG3

Sub -Control	Tipo de activo	Función de seguridad	Título del control	Descripción del control	Productos de ManageEngine	Grupos de qimplementación		
						1	2	3
6.5	Red	Detectar	Gestión central de logs	Garantice que los logs apropiados se agreguen a un sistema central de gestión de logs para su análisis y revisión.	**Log360:** Recopile los logs de varias fuentes y gestiónelos en una sola consola. (Se puede acceder a los logs de AD recopilados en ADAudit Plus y los logs de red recopilados en EventLog Analyzer a través de una sola consola en Log360).		IG2	IG3
6.6	Red	Detectar	Implementar SIEM o herramientas de análisis de logs	Implemente la Gestión de Eventos e Información de Seguridad (SIEM) o herramientas de análisis de logs para la correlación y el análisis de logs.	**Log360:** Este producto ofrece una completa gestión de eventos e información de seguridad (SIEM).		IG2	IG3
6.7	Red	Detectar	Revisar regularmente los logs	Revise regularmente los logs para identificar anomalías o eventos anormales.	**Log360:** Analice los logs de diferentes fuentes, incluidos firewalls, routers, estaciones de trabajo, bases de datos y servidores de archivos, con la ayuda de la función de análisis del comportamiento de usuarios y entidades (UEBA) del producto. Cualquier desviación del comportamiento normal se clasifica como una anomalía de tiempo, de recuento o de patrón. Reciba información procesable a través de puntuaciones de riesgo, tendencias de anomalías e informes intuitivos.		IG2	IG3

CONTROLES DE CIS
FUNDAMENTALES



CONTROL 7

Protección de correo electrónico y navegador web

Proteja y gestione los navegadores web y los sistemas de correo electrónico contra las amenazas basadas en la web para minimizar su superficie de ataque. Deshabilite los navegadores no autorizados y los plug-ins de los clientes de correo electrónico, y garantice que los usuarios puedan acceder sólo a sitios web de confianza manteniendo filtros de URL basados en la red.

Asignación de los Sub-Controles a los productos de ManageEngine

Sub -Control	Tipo de activo	Función de seguridad	Título del control	Descripción del control	Productos de ManageEngine	Grupos de qimplementación		
						1	2	3
7.1	Aplicaciones	Proteger	Garantizar el uso de sólo navegadores y clientes de correo electrónico que sean totalmente compatibles	Garantice que sólo los navegadores web y los clientes de correo electrónico totalmente compatibles puedan ejecutarse en la organización, idealmente utilizando solamente la última versión de los navegadores y clientes de correo electrónico proporcionados por el proveedor.	**Browser Security Plus:** Reciba informes sobre equipos con navegadores desactualizados. Active las actualizaciones automáticas para Internet Explorer y Chrome. **Desktop Central:** Instale las últimas versiones de los navegadores con la ayuda de la función de implementación de software del producto.	IG1	IG2	IG3
7.2	Aplicaciones	Proteger	Deshabilitar los plugins innecesarios o no autorizados del navegador o del cliente de correo electrónico	Desinstale o deshabilite cualquier plugin o aplicación add-on no autorizada del navegador o del cliente de correo electrónico.	**Browser Security Plus:** Permita o impida a los usuarios instalar extensiones y plug-ins.		IG2	IG3

Sub -Control	Tipo de activo	Función de seguridad	Título del control	Descripción del control	Productos de ManageEngine	Grupos de qimplementación		
						1	2	3
7.3	Aplicaciones	Proteger	Limitar el uso de los lenguajes de scripting en los navegadores web y los clientes de correo electrónico	Garantice que sólo los lenguajes de scripting autorizados puedan ejecutarse en todos los navegadores web y clientes de correo electrónico.	**Browser Security Plus:** Habilite o deshabilite JavaScript en los equipos de destino.		IG2	IG3
7.4	Red	Proteger	Mantener y aplicar filtros de URL basados en la red	Aplique filtros de URL basados en la red que limiten la capacidad de un sistema para conectarse a sitios web no aprobados por la organización. Este filtrado se aplicará a cada uno de los sistemas de la organización, ya sea que se encuentren o no físicamente en las instalaciones de la organización.	**Browser Security Plus:** Cree una lista blanca de sitios web en Internet Explorer para que los usuarios puedan acceder sólo a los sitios web de confianza que ya han sido configurados.		IG2	IG3
7.6	Red	Detectar	Registrar todas las solicitudes de URL	Registre todas las solicitudes de URL de cada uno de los sistemas de la organización, ya sea en el sitio o en un dispositivo móvil, a fin de identificar actividades potencialmente maliciosas y ayudar a los encargados de solucionar los incidentes a identificar los sistemas potencialmente comprometidos.	**Firewall Analyzer:** Recopile los logs de los firewalls y registre las URL a las que acceden los usuarios (requiere un firewall compatible).		IG2	IG3
7.7	Red	Proteger	Utilizar servicios de filtrado DNS	Utilice servicios de filtrado de DNS para ayudar a bloquear el acceso a dominios maliciosos conocidos.	**Browser Security Plus:** Bloquee el acceso a los dominios maliciosos.	IG1	IG2	IG3

CONTROL 8

Defensas contra malware

Controle la instalación y ejecución de código malicioso en varios puntos de su empresa para prevenir los ataques. Configure e implemente software antimalware y optimice el uso de la automatización para permitir una rápida actualización de las defensas y una rápida acción correctiva cuando se producen los ataques.

Asignación de los Sub-Controles a los productos de ManageEngine

Sub -Control	Tipo de activo	Función de seguridad	Título del control	Descripción del control	Productos de ManageEngine	Grupos de qimplementación		
						1	2	3
8.2	Dispositivos	Proteger	Garantizar que el software anti-malware y las firmas estén actualizadas	Garantice que el software anti-malware de la organización actualice su motor de exploración y su base de datos de firmas de forma regular.	**Desktop Central:** Envíe las actualizaciones del antivirus.	IG1	IG2	IG3
8.3	Dispositivos	Detectar	Habilitar las funciones de anti-explotación del sistema operativo/implementar tecnologías antiexplotación	Habilite las funciones anti-explotación como la Prevención de ejecución de datos (DEP) o la Aleatorización del diseño del espacio de direcciones (ASLR) que están disponibles en los sistemas operativos o implemente los kits de herramientas adecuados que pueden configurarse para proteger un conjunto más amplio de aplicaciones y ejecutables.	**Vulnerability Manager Plus:** Determine si los sistemas de la red tienen DEP y ASLR habilitados		IG2	IG3

Sub -Control	Tipo de activo	Función de seguridad	Título del control	Descripción del control	Productos de ManageEngine	Grupos de qimplementación		
						1	2	3
8.4	Dispositivos	Detectar	Configurar el análisis anti-malware de los medios extraíbles	Configure los dispositivos para que realicen automáticamente un análisis antimalware de los medios extraíbles al insertarlos o conectarlos.	**ADAudit Plus:** Audite los dispositivos extraíbles que se conectan a los sistemas e identifique qué archivos se han leído, modificado o copiado y pegado. **Desktop Central:** Bloquee los dispositivos para que no se conecten a sus sistemas de red. **Device Control Plus:** Establezca permisos de sólo lectura para los dispositivos extraíbles que se conectan a los sistemas.	IG1	IG2	IG3
8.6	Dispositivos	Detectar	Centralizar los registros antimalware	Envíe todos los eventos de detección de malware a las herramientas de administración antimalware y a los servidores de log de eventos para análisis y alertas.	**EventLog Analyzer:** Recopile los logs de los sistemas antimalware, y obtenga una visión holística de todos los logs recopilados.		IG2	IG3

CONTROL 9

Limitación y control de puertos de red, protocolos y servicios

Supervise y controle la actividad en los puertos, protocolos y servicios de los dispositivos de la red para reducir el alcance de los ataques mediante las vulnerabilidades del servicio. Aproveche los firewalls de los host para garantizar que sólo se permita el acceso al tráfico apropiado.

Asignación de los Sub-Controles a los productos de ManageEngine

Sub -Control	Tipo de activo	Función de seguridad	Título del control	Descripción del control	Productos de ManageEngine	Grupos de qimplementación		
						1	2	3
9.1	Dispositivos	Identificar	Asociar puertos, servicios y protocolos activos al inventario de activos	Asocie puertos, servicios y protocolos activos a los activos de hardware en el inventario de activos.	**Vulnerability Manager Plus:** Obtenga la lista de todos los puertos abiertos en cada sistema, así como las aplicaciones que están instaladas en él.		IG2	IG3
9.2	Dispositivos	Proteger	Garantizar solamente los aprobados	Garantice que sólo aquellos puertos de red, protocolos y servicios que escuchan un sistema con necesidades comerciales validadas sean ejecutados en cada sistema.	**Desktop Central:** Cree configuraciones para establecer reglas de firewall y active o desactive puertos.		IG2	IG3
9.3	Dispositivos	Proteger	Realizar análisis de puertos automatizados de forma regular	Realice análisis de puertos automáticos de forma regular contra todos los sistemas y alerte si se detectan puertos no autorizados en un sistema.	**Vulnerability Manager Plus:** Obtenga toda la información que necesita sobre los puertos en uso en sus sistemas de red en una sola consola con la función de auditoría de puertos.		IG2	IG3

CONTROL 10

Funciones de recuperación de datos

Establezca procesos y herramientas para garantizar que la información crítica de su organización esté debidamente respaldada, y disponga de un sistema de recuperación de datos fiable para la restauración de los datos a fin de superar los ataques que ponen en peligro los datos críticos.

Asignación de los Sub-Controles a los productos de ManageEngine

Sub -Control	Tipo de activo	Función de seguridad	Título del control	Descripción del control	Productos de ManageEngine	Grupos de qimplementación		
						1	2	3
10.1	Datos	Proteger	Garantizar copias de seguridad automáticas regulares	Garantice que todos los datos del sistema sean respaldados automáticamente de forma regular.	**RecoveryManager Plus:** Configure un cronograma para hacer copias de seguridad de Active Directory, Microsoft 365, y Exchange on premises.	IG1	IG2	IG3
10.2	Proteger	Proteger	Realizar respaldos de sistemas completos	Garantice que todos los sistemas clave de la organización estén respaldados como un sistema completo, a través de procesos como imágenes, para permitir la rápida recuperación de un sistema completo.	**RecoveryManager Plus:** Realice copias de seguridad y restaure sistemas críticos como controladores de dominio y Exchange Servers cuando sea necesario.	IG1	IG2	IG3

CONTROL 11

Configuración segura para dispositivos de red, tales como firewalls, routers y switches

Establezca, implemente y gestione la configuración de seguridad de los dispositivos de red para evitar que los atacantes se aprovechen de las configuraciones predeterminadas vulnerables. Disponga de un proceso estricto de gestión y control de configuraciones para garantizar que éstas no se encuentren en un estado explotable.

Asignación de los Sub-Controles a los productos de ManageEngine

Sub -Control	Tipo de activo	Función de seguridad	Título del control	Descripción del control	Productos de ManageEngine	Grupos de qimplementación		
						1	2	3
11.1	Red	Identificar	Mantener configuraciones de seguridad estandarizadas en equipos de red	Mantenga los estándares de configuración de seguridad documentados para todos los dispositivos de red autorizados.	**Network Configuration Manager:** Realice automáticamente una copia de seguridad de las configuraciones de red de forma programada.		IG2	IG3
11.3	Red	Detectar	Usar herramientas automatizadas para verificar las configuraciones estándar de los dispositivos y detectar cambios	Compare todas las configuraciones de los dispositivos de red con las configuraciones de seguridad aprobadas y definidas para cada dispositivo de red en uso, y alerte cuando se descubra cualquier desviación.	**Network Configuration Manager:** Cree una configuración básica para su red y compárela con las configuraciones que se están ejecutando actualmente en sus dispositivos de red.		IG2	IG3
11.4	Red	Proteger	Instalar la última versión estable de cualquier actualización relacionada con la seguridad en todos los dispositivos de la red	Instale la última versión estable de cualquier actualización relacionada con la seguridad en todos los dispositivos de la red.	**Network Configuration Manager:** Garantice que sus dispositivos tengan instaladas las últimas actualizaciones del sistema operativo.	IG1	IG2	IG3

CONTROL 12

Protección perimetral

Detecte, prevenga y controle el flujo de información a través de los perímetros de su red para evitar que los atacantes obtengan acceso pasando por alto los sistemas perimetrales. Configure el monitoreo perimetral, deniegue el acceso no autorizado e implemente sistemas de detección de intrusos para reforzar la protección perimetral.

Asignación de los Sub-Controles a los productos de ManageEngine

Sub -Control	Tipo de activo	Función de seguridad	Título del control	Descripción del control	Productos de ManageEngine	Grupos de qimplementación		
						1	2	3
12.1	Red	Identificar	Mantener un inventario del perímetro de la red	Mantenga un inventario actualizado de todos los perímetros de la red de la organización.	**OpUtils:** Reciba la lista de todas las subredes de su infraestructura analizando los routers.	IG1	IG2	IG3
12.2	Red	Detectar	Analizar en búsqueda de conexiones no autorizadas a través de los perímetros de la red de confianza	Realice análisis regulares desde fuera de cada perímetro de la red de confianza para detectar cualquier conexión no autorizada a la que se pueda acceder a través del perímetro.	**OpUtils:** Reciba una alerta cada vez que un nuevo dispositivo se conecta a su red. El dispositivo de red envía un mensaje de syslog a OpUtils para activar la alerta.		IG2	IG3
12.3	Red	Proteger	Denegar las comunicaciones con direcciones IP maliciosas conocidas	Deniegue las comunicaciones con direcciones IP maliciosas conocidas o no utilizadas de Internet y limite el acceso únicamente a los rangos de direcciones IP confiables y necesarias en cada uno de los perímetros de la red de la organización.	**OpUtils:** Bloquee un puerto del switch al recibir una alerta sobre comunicaciones con direcciones IP maliciosas o no utilizadas, o sobre el acceso a través de una dirección IP sospechosa.		IG2	IG3

Sub -Control	Tipo de activo	Función de seguridad	Título del control	Descripción del control	Productos de ManageEngine	Grupos de qimplementación		
						1	2	3
12.5	Red	Detectar	Configurar sistemas de monitoreo para registrar paquetes de red	Configure los sistemas de monitoreo para registrar los paquetes de red que pasan por el límite en cada uno de los perímetros de la red de la organización.	**NetFlow Analyzer:** Monitoree los flujos (NetFlow, JFlow, sFlow, IPFIX, y Netstream) a través de los perímetros de la red.		IG2	IG3
12.6	Red	Detectar	Implementar sensores IDS basados en la red	Implemente los sensores de los Sistemas de Detección de Intrusos (IDS) basados en la red para buscar mecanismos de ataque inusuales y detectar el compromiso de estos sistemas en cada uno de los límites de la red de la organización.	**EventLog Analyzer:** Genere informes sobre ataques inusuales, sistemas objetivo y tendencias de ataque.		IG2	IG3
12.7	Red	Proteger	Implementar sistemas de prevención de intrusiones basados en la red	Implemente sistemas de prevención de intrusiones (IPS) basados en la red para bloquear el tráfico de red malicioso en cada uno de los perímetros de la red de la organización.	**EventLog Analyzer:** Este producto es compatible con dispositivos Cisco, Juniper, SonicWall, Barracuda, Palo Alto Networks, WatchGuard, NetScreen, Fortinet y Check Point. Una vez configurado, EventLog Analyzer recopila automáticamente los logs IDS/IPS de estos dispositivos y los almacena en una ubicación central. Los informes predefinidos del producto ayudan a cubrir varios aspectos de su red y ofrecen información de la situación general de la seguridad de su red. Una vez que identifique el tráfico malicioso, puede bloquearlo mediante las políticas de firewall.			IG3

Sub -Control	Tipo de activo	Función de seguridad	Título del control	Descripción del control	Productos de ManageEngine	Grupos de qimplementación		
						1	2	3
12.8	Red	Detectar	Implementar recopiladores NetFlow en los dispositivos perimetrales de la red	Habilite la recopilación de NetFlow y el registro de datos en todos los dispositivos perimetrales de la red.	**NetFlow Analyzer:** Capture información sobre los flujos con la ayuda de un dispositivo que tiene la capacidad de exportar flujos.		IG2	IG3
12.11	Usuarios	Proteger	Requerir autenticación multifactor en todos los inicios de sesión remotos	Requiera que todos los accesos remotos a la red de la organización codifiquen los datos en tránsito y utilicen una autenticación multifactor.	**Password Manager Pro:** Analice los recursos de su red y proporcione acceso a los usuarios que lo requieran. Deshabilite el acceso de los usuarios cuando ya no se necesite. La autenticación multifactor (MFA) está disponible para acceder a la herramienta.		IG2	IG3
12.12	Dispositivos	Proteger	Gestionar todos los dispositivos remotos que se conectan a la red interna	Analice todos los dispositivos de la empresa que se conectan de forma remota a la red de la organización antes de acceder a la red para garantizar que cada una de las políticas de seguridad de la organización se ha aplicado de la misma manera que a los dispositivos de red local.	**Desktop Central:** Gestione los dispositivos en su WAN para garantizar que las políticas se establezcan correctamente en sus sistemas.			IG3

CONTROL 13

Protección de datos

Identifique y segregue los datos sensibles e implemente una combinación de procesos, incluidos la codificación, los planes de protección contra la infiltración de datos y las técnicas de prevención de pérdida de datos, para garantizar la privacidad e integridad de los datos sensibles.

Asignación de los Sub-Controles a los productos de ManageEngine

Sub -Control	Tipo de activo	Función de seguridad	Título del control	Descripción del control	Productos de ManageEngine	Grupos de qimplementación		
						1	2	3
13.3	Datos	Detectar	Monitorear y bloquear el tráfico de red no autorizado	Implemente una herramienta automatizada en los perímetros de la red que monitoree la transferencia no autorizada de información sensible y bloquee dichas transferencias mientras alerta a los profesionales de seguridad de la información.	**DataSecurity Plus:** Audite la información sensible que se crea, modifica, borra, copia y pega, o se almacena en sus servidores de archivos.	IG1	IG2	IG3
13.6	Datos	Proteger	Codificar los datos de los dispositivos móviles	Utilice mecanismos criptográficos aprobados para proteger los datos de la empresa almacenados en todos los dispositivos móviles.	**Mobile Device Manager Plus:** Proteja los datos de la empresa que se almacenan en los dispositivos móviles de los usuarios mediante la contenedorización.	IG1	IG2	IG3
13.7	Datos	Proteger	Gestionar dispositivos USB	Si se requieren dispositivos de almacenamiento USB, se debe utilizar un software empresarial que pueda configurar los sistemas para permitir el uso de dispositivos específicos. Se debe mantener un inventario de dichos dispositivos.	**Desktop Central** y **Device Control Plus:** Permita que dispositivos USB específicos se conecten a su red.		IG2	IG3
13.8	Datos	Proteger	Gestionar las configuraciones de lectura y escritura de los medios extraíbles externos del sistema	Configure los sistemas para que no escriban datos en medios extraíbles externos, si no hay necesidad comercial de utilizar tales dispositivos.	**Device Control Plus:** Permita a los usuarios solamente leer la información de un medio externo.			IG3

CONTROL 14

Control de acceso basado en la necesidad de saber

Supervise, controle y proteja el acceso a los activos críticos, como la información, los recursos y los sistemas. Permita el acceso a información crítica sobre la base de la necesidad de saberla y establezca un registro detallado de los servidores a fin de supervisar el acceso e investigar los incidentes en los que se haya accedido indebidamente a los datos.

Asignación de los Sub-Controles a los productos de ManageEngine

Sub -Control	Tipo de activo	Función de seguridad	Título del control	Descripción del control	Productos de ManageEngine	Grupos de qimplementación		
						1	2	3
14.6	Datos	Proteger	Proteger la información mediante listas de control de acceso	Proteja toda la información almacenada en los sistemas con listas de control de acceso específicas de sistemas de archivos, recurso de red, reclamaciones, aplicaciones o bases de datos. Estos controles harán cumplir el principio de que sólo las personas autorizadas deben tener acceso a la información en función de su necesidad de acceder a la información como parte de sus responsabilidades.	**Desktop Central:** Proporcione a usuarios específicos acceso a archivos y carpetas. **Password Manager Pro:** Proporcione a usuarios específicos acceso a sistemas, bases de datos, aplicaciones y dispositivos de red.	IG1	IG2	IG3
14.9	Datos	Detectar	Aplicar un registro detallado para el acceso o cambios en los datos sensibles	Aplique un registro detallado de auditoría para el acceso a datos sensibles o cambios en los datos sensibles (utilizando herramientas como el monitoreo de la integridad de los archivos o monitoreo de eventos e información de seguridad).	**ADAudit Plus:** Recopile información sobre los archivos a los que se ha accedido, modificado o eliminado.			IG3

CONTROL 15

Control de acceso inalámbrico

Supervise, controle y proteja sus redes de área local inalámbricas (WLAN), puntos de acceso y sistemas de clientes inalámbricos para evitar que los atacantes manipulen sus defensas perimetrales. Implemente un sistema de detección de intrusos inalámbricos y lleve a cabo un análisis de vulnerabilidades en los equipos de clientes inalámbricos para detectar vulnerabilidades explotables.

Asignación de los Sub-Controles a los productos de ManageEngine

Sub -Control	Tipo de activo	Función de seguridad	Título del control	Descripción del control	Productos de ManageEngine	Grupos de qimplementación		
						1	2	3
15.1	Red	Identificar	Mantener un inventario de puntos de acceso inalámbrico autorizados	Mantenga un inventario de los puntos de acceso inalámbrico autorizados conectados a la red cableada.	**AssetExplorer:** Analice su red a través de SNMP y obtenga un inventario de los puntos de acceso en la red.		IG2	IG3
15.2	Red	Detectar	Detectar los puntos de acceso inalámbrico conectados a la red cableada	Configure las herramientas de exploración de vulnerabilidades de la red para detectar y alertar sobre los puntos de acceso inalámbrico no autorizados conectados a la red cableada.	**OpUtils:** Analice su red para identificar los sistemas recién añadidos, como los puntos de acceso. Una vez que se detecta un dispositivo, usted puede establecer alertas personalizadas para acciones específicas.		IG2	IG3
15.3	Red	Detectar	Usar un sistema de detección de intrusión inalámbrica	Use un sistema de detección de intrusos inalámbricos (WIDS) para detectar y alertar sobre puntos de acceso inalámbrico no autorizados conectados a la red.	**OpUtils:** Active alertas personalizadas para los accesos no autorizados.		IG2	IG3

Sub -Control	Tipo de activo	Función de seguridad	Título del control	Descripción del control	Productos de ManageEngine	Grupos de qimplementación		
						1	2	3
15.4	Dispositivos	Dispositivos	Deshabilitar el acceso inalámbrico a los dispositivos si no es necesario	Deshabilite el acceso inalámbrico en los dispositivos que no tienen un propósito de negocio para el acceso inalámbrico.	**Desktop Central:** Active y desactive los adaptadores inalámbricos.			IG3
15.5	Dispositivos	Proteger	Limitar el acceso inalámbrico en los dispositivos cliente	Configure el acceso inalámbrico en los equipos cliente que tienen un propósito de negocio inalámbrico esencial, para permitir el acceso sólo a las redes inalámbricas autorizadas y restringir el acceso a otras redes inalámbricas.	**Desktop Central:** Active y desactive los adaptadores inalámbricos.			IG3
15.9	Dispositivos	Proteger	Deshabilitar el acceso periférico inalámbrico a dispositivos	Deshabilite el acceso periférico inalámbrico de los dispositivos [como Bluetooth y Comunicación de Campo Cercano (NFC)], a menos que dicho acceso sea necesario para un propósito de negocio.	**Desktop Central:** Cree una configuración de registro para desactivar el Bluetooth y la NFC en los sistemas.			IG3

CONTROL 16

Monitoreo y control de cuentas

Gestione activamente todo el ciclo de vida de sus sistemas y cuentas de aplicaciones, desde su creación, uso e inactividad hasta su eliminación, para evitar que los atacantes exploten las cuentas de usuarios legítimos pero inactivos.

Asignación de los Sub-Controles a los productos de ManageEngine

Sub -Control	Tipo de activo	Función de seguridad	Título del control	Descripción del control	Productos de ManageEngine	Grupos de qimplementación		
						1	2	3
16.2	Usuarios	Proteger	Configurar un punto de autenticación centralizado	Configure el acceso a todas las cuentas a través de la menor cantidad posible de puntos centralizados de autenticación, incluidos la red, la seguridad y los sistemas de nube.	**Password Manager Pro:** La solución actúa como una consola central para los recursos de infraestructura, incluidos sistemas, aplicaciones, dispositivos de red, bases de datos y sitios web. Proporcione acceso a los usuarios, y permita que los usuarios accedan a los recursos desde ese mismo portal.		IG2	IG3
16.3	Usuarios	Proteger	Requerir autenticación multi-factor	Requiera la autenticación multi factor para todas las cuentas de usuario, en todos los sistemas, tanto si se gestionan localmente o por un proveedor de terceros.	**Password Manager Pro:** Habilite la MFA.		IG2	IG3
16.4	Usuarios	Proteger	Codificar o hashear todas las credenciales de autenticación	Utilice técnicas de codificación o hash combinado con salt con todas las credenciales de autenticación cuando se almacenan.	**Password Manager Pro:** La base de datos utilizada está codificada a través de AES-256		IG2	IG3

Sub -Control	Tipo de activo	Función de seguridad	Título del control	Descripción del control	Productos de ManageEngine	Grupos de qimplementación		
						1	2	3
16.5	Usuarios	Proteger	Codificar la transmisión de nombres de usuario y credenciales de autenticación	Garantice que todos los nombres de usuario de las cuentas y las credenciales de autenticación se transmitan a través de redes utilizando canales codificados.	**Password Manager Pro:** Ejecute Password Manager Pro en HTTPS para garantizar que nadie pueda interceptar la comunicación mientras se comparten las contraseñas privilegiadas.		IG2	IG3
16.6	Usuarios	Identificar	Mantener un inventario de cuentas	Mantenga un inventario de todas las cuentas organizadas por el sistema de autenticación.	**Password Manager Pro:** Construya un inventario de todas las cuentas descubiertas en su red.		IG2	IG3
16.7	Usuarios	Proteger	Establecer un proceso para revocar el acceso	Establezca y siga un proceso automatizado para revocar el acceso al sistema inhabilitando las cuentas inmediatamente después de la terminación contractual o cambio de responsabilidades de un empleado o contratista. Desactivar estas cuentas, en lugar de eliminarlas, permite preservar las pistas de auditoría.	**Password Manager Pro:** Habilite y deshabilite el acceso de los usuarios cuando sea necesario utilizando la solución como punto central de contacto para todos los accesos.		IG2	IG3
16.8	Usuarios	Responder	Deshabilitar cualquier cuenta no asociada	Deshabilite cualquier cuenta que no pueda asociarse con un proceso de negocio o un propietario de la organización.	**Password Manager Pro:** Deshabilite las cuentas si es necesario.	IG1	IG2	IG3

Sub -Control	Tipo de activo	Función de seguridad	Título del control	Descripción del control	Productos de ManageEngine	Grupos de qimplementación		
						1	2	3
16.9	Usuarios	Responder	Deshabilitar cuentas inactivas	Deshabilite automáticamente las cuentas inactivas después de un período determinado de inactividad.	**ADManager Plus:** Configure un flujo de trabajo para desactivar una cuenta (usuario AD) después de un período de tiempo configurado. **Password Manager Pro:** Rote la contraseña una vez que el usuario haya completado la sesión.	IG1	IG2	IG3
16.10	Usuarios	Proteger	Garantizar que todas las cuentas tengan una fecha de caducidad	Garantice que todas las cuentas tengan una fecha de vencimiento que sea monitoreada y aplicada.	**ADManager Plus:** Garantice que todas las cuentas tengan una fecha de caducidad. Genere informes para las cuentas que nunca expiran. Modifique las cuentas de forma masiva para cambiar su configuración.		IG2	IG3
16.11	Usuarios	Proteger	Bloquear sesiones de estaciones de trabajo tras inactividad	Bloquee automáticamente las sesiones de la estación de trabajo después de un período estándar de inactividad.	**Desktop Central:** Bloquee los equipos después de un período de inactividad con la configuración del producto out of the box.	IG1	IG2	IG3
16.12	Usuarios	Detectar	Monitorear los intentos de acceso a cuentas desactivadas	Monitoree los intentos de acceso a cuentas desactivadas a través de los registros de auditoría.	**ADAudit Plus:** Genere alertas para los intentos de acceso a cuentas desactivadas.		IG2	IG3
16.13	Usuarios	Detectar	Alertar sobre la desviación del comportamiento de inicio de sesión de cuentas	Genere alertas cuando los usuarios se desvían del comportamiento normal de inicio de sesión, como la hora del día, la ubicación de la estación de trabajo y la duración.	**Log360: Comprenda el comportamiento del usuario con la ayuda del UEBA.**			IG3

CONTROLES DE CIS
ORGANIZACIONALES

A diferencia de los controles básicos y fundamentales, se trata de prácticas que su organización debe adoptar internamente para garantizar una buena higiene cibernética.

CONTROL 17

Implementar un programa de concienciación y capacitación en seguridad

Implemente un plan integrado para educar a los empleados en las habilidades y destrezas específicas que deben poseer para apoyar la defensa de la empresa de acuerdo con su rol funcional en la organización.

CONTROL 18

Seguridad del software de aplicación

Ponga a prueba regularmente todo su software interno y adquirido para detectar vulnerabilidades. Disponga de un programa eficaz para abordar la seguridad a lo largo de todo el ciclo de vida del software interno, desde el establecimiento de los requisitos, la capacitación, las herramientas y las pruebas, y disponga de criterios estrictos de evaluación de la seguridad al adquirir software de terceros.

CONTROL 19

Respuesta y gestión de incidentes

Desarrolle e implemente un sistema de gestión de incidentes definido en su organización para descubrir rápidamente los ataques, contener eficazmente los daños, revocar el acceso del atacante a su red y restaurar las operaciones rápidamente.

CONTROL 20

Pruebas de penetración y ejercicios de Red Team

Evalúe periódicamente la preparación de su organización para defenderse de los ataques mediante la realización de pruebas de penetración. Simule los objetivos y acciones de un atacante con la ayuda de Red Teams para inspeccionar su actual postura de seguridad y así obtener valiosos conocimientos sobre la eficacia de sus defensas.

La lista de control de CIS-ManageEngine

Hemos asignado nuestros productos a los correspondientes sub-controles de CIS a los que dan soporte para facilitarle la identificación del producto de ManageEngine adecuado para cumplir con cada control.

Productos de ManageEngine	Sub-controles compatibles
Desktop Central	1.1, 1.4, 1.5, 1.8, 2.1, 2.3, 2.4, 2.5, 2.6, 2.10, 3.4, 3.5, 4.1, 4.2, 5.4, 5.5, 6.1, 7.1, 8.2, 8.4, 9.2, 12.12, 13.7, 14.6, 15.4, 15.5, 15.9. 16.11
Application Control Plus	2.7, 2.8
Vulnerability Manager Plus	3.1, 3.2, 3.6, 3.7, 8.3, 9.1, 9.3
OS Deployer	5.2, 5.3
Browser Security Plus	7.1, 7.2, 7.3, 7.4, 7.7
Device Control Plus	8.4, 13.7, 13.8
Mobile Device Manager Plus	13.6
AssetExplorer	1.1, 15.1
OpUtils	1.2, 1.3, 1.6, 1.7, 12.1, 12.2, 12.3, 15.1, 15.2
ADManager Plus	4.1, 8.4, 16.9, 16.10
Password Manager Pro	4.1, 4.4, 4.5, 12.11, 14.6, 16.2, 16.3, 16.4, 16.5, 16.6, 16.7, 16.8, 16.9
ADAudit Plus	4.8, 4.9, 14.9, 16.12
DataSecurity Plus	13.3
EventLog Analyzer	6.1, 6.2, 8.6, 8.7, 12.6, 12.7
Log360	6.5, 6.6, 6.7, 16.13
RecoveryManager Plus	10.1, 10.2
Firewall Analyzer	7.6
Network Configuration Manager	11.1, 11.3, 11.4, 11.5
NetFlow Analyzer	12.5, 12.8, 13.5

Los productos de ManageEngine que le ayudarán en el proceso de implementación

Aquí está la lista completa de los productos de ManageEngine que ayudarán a su organización a cumplir con los controles de CIS.

Desktop Central: Gestión integrada de desktop y dispositivos móviles (On-premises | Cloud | MSP)

Application Control Plus: Control de aplicaciones y gestión de privilegios de endpoints (On-premises)

Vulnerability Manager Plus: Gestión integrada de amenazas y vulnerabilidades (On-premises)

OS Deployer: Imágenes e implementación del sistema operativo (On-premises)

Browser Security Plus: Seguridad y gestión del navegador (On-premises)

Device Control Plus: Prevención de pérdidas de datos para dispositivos extraíbles (On-premises)

Mobile Device Manager Plus: Gestión integral de dispositivos móviles (On-premises | Cloud | MSP)

AssetExplorer: ITAM con CMDB integrada (On-premises)

OpUtils: Gestión de puertos de switch y direcciones IP (On-premises)

ADManager Plus: Gestión e informes de AD, Microsoft 365 y Exchange (On-premises)

Password Manager Pro: Gestión de cuentas privilegiadas (On-premises | MSP)

ADAudit Plus: Auditoría e informes de AD (On-premises)

DataSecurity Plus: Auditoría de archivos, prevención de pérdida de datos y evaluación de riesgos de los datos (On-premises)

EventLog Analyzer: Gestión de logs, auditoría de TI y gestión de cumplimiento (On-premises)

Log360: SIEM integral, con una avanzada mitigación de amenazas y UEBA basado en ML (On-premises | Cloud)

RecoveryManager Plus: Respaldo y recuperación de AD, Microsoft 365 y Exchange (On-premises)

Firewall Analyzer: Gestión de reglas, configuración y logs del firewall (On-premises)

Network Configuration Manager: Gestión de cambios y configuraciones de la red (On-premises)

NetFlow Analyzer: Monitoreo del ancho de banda y análisis de tráfico (On-premises)

Asignación del Grupo de Implementación y del sub-control

Hemos asignado los diversos sub-controles de CIS con sus respectivos grupos de implementación, IG1, IG2 e IG3, para su mejor comprensión. Visite la página web CIS Controls Navigator para obtener más información.

Grupo de Implementación	Sub-controles de CIS correspondientes
IG1	1.4, 1.6, 2.1, 2.2, 2.6, 3.4, 3.5, 4.2, 4.3, 5.1, 6.2, 7.1, 7.7, 8.2, 8.4, 8.5, 9.4, 10.1, 10.2, 10.4, 10.5, 11.4, 12.1, 12.4, 13.1, 13.2, 13.6, 14.6, 15.7, 15.10, 16.8, 16.9, 16.11, 17.3, 17.5, 17.6, 17.7, 17.8, 17.9, 19.1, 19.3, 19.5, 19.6
IG2	1.1, 1.3, 1.4, 1.5, 1.6, 1.7, 2.1, 2.2, 2.3, 2.4, 2.6, 3.1, 3.2, 3.3, 3.4, 3.5, 3.6, 3.7, 4.1, 4.2, 4.3, 4.4, 4.5, 4.7, 4.8, 4.9, 5.1, 5.2, 5.3, 5.4, 5.5, 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 9.1, 9.2, 9.3, 9.4, 10.1, 10.2, 10.3, 10.4, 10.5, 11.1, 11.2, 11.3, 11.4, 11.5, 11.6, 11.7, 12.1, 12.2, 12.3, 12.4, 12.5, 12.6, 12.8, 12.11, 13.1, 13.2, 13.4, 13.6, 13.7, 14.1, 14.2,14.3, 14.4, 14.6, 15.1, 15.2, 15.3, 15.6, 15.7, 15.9, 15.10, 16.1, 16.2, 16.3, 16.4, 16.5, 16.6, 16.7, 16.8, 16.9, 16.10, 16.11, 16.12, 17.1, 17.2, 17.3, 17.4, 17.5, 17.6, 17.7, 17.8, 17.9, 18.1, 18.2, 18.3, 18.4, 18.5, 18.6, 18.7, 18.8, 18.9, 18.10, 18.11, 19.1, 19.2, 19.3, 19.4, 19.5, 19.6, 19.7. 20.1, 20.2, 20.4, 20.5, 20.6, 20.8
IG3	1.1, 1.2, 1.3, 1.4, 1.5, 1.6, 1.7, 1.8, 2.1, 2.2, 2.3, 2.4, 2.5, 2.6, 2.7, 2.8, 2.9, 2.10, 3.1, 3.2, 3.3, 3.4, 3.5, 3.6, 3.7, 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 5.1, 5.2, 5.3, 5.4, 5.5, 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9, 7.10, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 9.1, 9.2, 9.3, 9.4, 9.5, 10.1, 10.2, 10.3, 10.4, 10.5, 11.1, 11.2, 11.3, 11.4, 11.5, 11.6, 11.7, 12.1, 12.2, 12.3, 12.4, 12.5, 12.6, 12.7, 12.8, 12.9, 12.10, 12.11, 12.12, 13.1, 13.2, 13.3, 13.4, 13.5, 13.6, 13.7, 13.8, 13.9, 14.1, 14.2, 14.3, 14.4, 14.5, 14.6, 14.7, 14.8, 14.9, 15.1, 15.2, 15.3, 15.4, 15.5, 15.6, 15.7, 15.8, 15.9, 15.10, 16.1, 16.2, 16.3, 16.4, 16.5, 16.6, 16.7, 16.8, 16.9, 16.10, 16.11, 16.12, 16.13, 17.1, 17.2, 17.3, 17.4, 17.5, 17.6, 17.7, 17.8, 17.9, 18.1, 18.2, 18.3, 18.4, 18.5, 18.6, 18.7, 18.8, 18.9, 18.10, 18.11, 19.1, 19.2, 19.3, 19.4, 19.5, 19.6, 19.7, 19.8, 20.1, 20.2, 20.3, 20.4, 20.5, 20.6, 20.7, 20.8

Alineando TI con el negocio

ManageEngine desarrolla un software de gestión de TI integral para todas las necesidades de su empresa.

Gestión de servicios de TI

- Mesa de ayuda lista para ITIL®
- Gestión de activos de TI con CMDB
- Base de conocimientos con autoservicio para el usuario
- Flujos de trabajo incorporados y personalizados
- Organización de todas las funciones de gestión de TI
- Informes y análisis
- Gestión de servicios para todos los departamentos

Gestión de accesos e identidades

- Gobernanza y administración de identidades
- Gestión de accesos e identidades privilegiadas
- Gestión y auditoría de AD y Azure AD
- SSO para aplicaciones on-premises y en la nube, con MFA
- Autoservicio y sincronización de contraseñas
- Gestión y auditoría de Office 365 y Exchange
- Respaldo y recuperación de AD y Exchange
- Autoservicio y sincronización de contraseñas

Gestión unificada de endpoints

- Gestión de desktops
- Gestión de dispositivos móviles
- Gestión de parches
- Implementación de SO y software
- Asistencia para desktop remoto
- Seguridad del navegador web
- Monitoreo y control de los dispositivos periféricos
- Gestión de privilegios de los endpoints y control de aplicaciones

Gestión de la seguridad de TI

- SIEM unificado para la nube y on-premises
- UEBA basado en IA
- Analíticas de logs de firewall
- Gestión de claves SSH y certificados SSL
- Seguridad de dispositivos endpoint
- Prevención de pérdida de datos y evaluación de riesgos
- Cumplimiento con la normativa y la privacidad

Gestión de operaciones de TI

- Monitoreo del rendimiento de redes, servidores y aplicaciones
- Monitoreo del ancho de banda con análisis de tráfico
- Gestión de cambios y configuraciones de red
- Descubrimiento de aplicaciones y asignación de dependencias
- Monitoreo de la infraestructura y el costo de la nube
- Monitoreo de la experiencia del usuario final
- AIOps

Análisis avanzado de TI

- Análisis avanzado de TI mediante autoservicio
- Visualización de datos e inteligencia de negocios para TI
- Cientos de informes y dashboards incorporados
- Creación de informes instantáneos y flexibles
- Compatibilidad out of the box para múltiples fuentes de datos

Acerca de ManageEngine

ManageEngine desarrolla el conjunto de software de gestión de TI más completo de la industria. Tenemos todo lo que necesita —más de 90 productos y herramientas gratuitas— para gestionar todas sus operaciones de TI, desde redes y servidores hasta aplicaciones, mesa de ayuda, Active Directory, seguridad, desktops y dispositivos móviles.

Desde 2001, los equipos de TI como el suyo han recurrido a nosotros para obtener un software asequible, rico en funciones y fácil de usar. Puede encontrar nuestras soluciones on-premises y en la nube que impulsan la TI de más de 180.000 empresas en todo el mundo, incluidas nueve de cada diez empresas de la lista Fortune 100.

A medida que usted se prepara para los desafíos de la gestión de TI que se avecinan, nosotros lideraremos el camino con nuevas soluciones, integraciones contextuales y otros avances que sólo pueden provenir de una empresa dedicada singularmente a sus clientes. Y al ser una división de Zoho Corporation, seguiremos trabajando por establecer una estrecha alineación de TI con los negocios que usted necesitará para aprovechar las oportunidades en el futuro.

Más de 180 000 organizaciones confían su TI a ManageEngine.

ManageEngine

www.manageengine.com/latam

ManageEngine LATAM ManageEngine LATAM ManageEngine LATAM