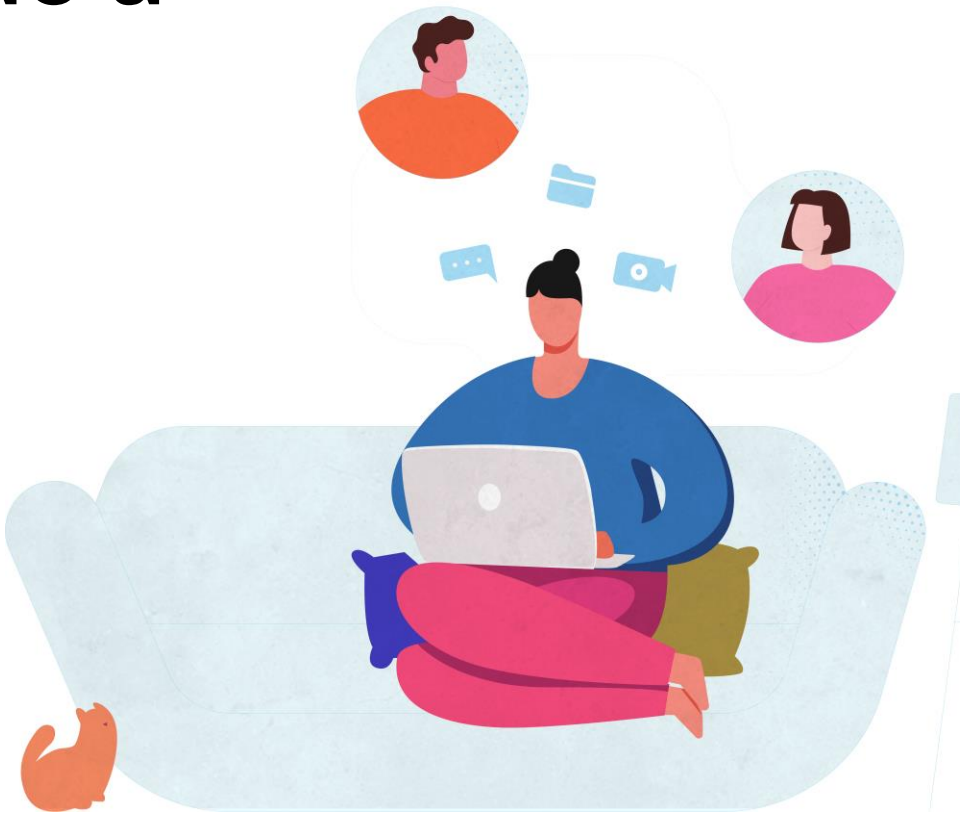
CIS Controls aplicado a Endpoint

Ruben Caballero
CEH | SECURITY+ | CND | ISO 27001 | PENTEST



ethical SHIELDS

ManageEngine Endpoint Central

Agenda

- Que son los Controls CIS ?
- Beneficios de los controles CIS en la organización
- La estructura de los controles CIS
- Grupos de implementación
- Implementación los controls CIS desde la gestion de endpoint
- 3 Ejemplos de Endpoint Central - ManageEngine

ManageEngine

Que son los controles CIS ?

Desarrollados por el Center for Internet Security, los Controles de Seguridad Critica de CIS son un conjunto prescriptive y prioritario de mejores prácticas en seguridad cibernética y acciones defensivas que pueden ayudar a prevenir los ataques más peligrosos y de mayor alcance, apoyar el cumplimiento en una era de múltiples marcos.

ManageEngine

Beneficios de los controles de CIS en la Organización

Desarrollar una estructura fundamental para su programa de seguridad de la información, y un marco para toda su estrategia de seguridad.

Seguir un enfoque comprobado de gestión de riesgos para la seguridad informática basado en la eficacia del mundo real.

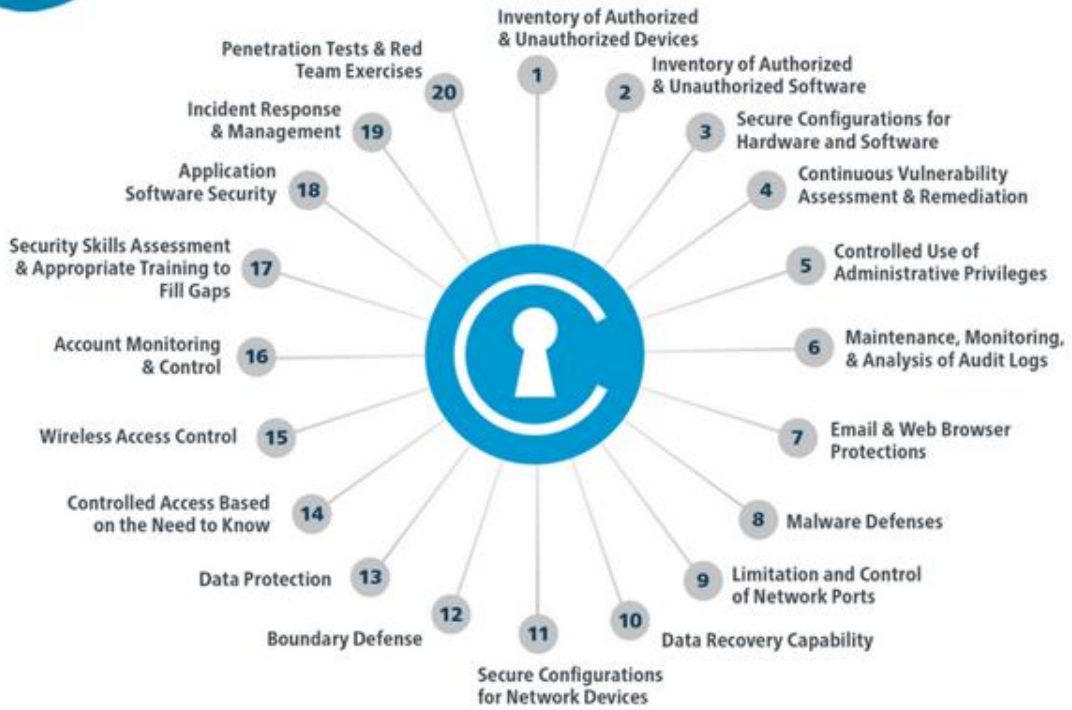
Enfocarse en el conjunto más efectivo y específico de medidas técnicas disponibles para mejorar la postura de defensa de su organización.

Ajustarse fácilmente a otros marcos y regulaciones, incluidos NIST Cybersecurity Framework, NIST 800-53, NIST 800-171, serie ISO 27000, PCI DSS, HIPAA, NERC CIP, y FISMA.

ManageEngine

La estructura de los controles de CIS

CIS Controls



CIS Center for Internet Security

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 fundacionales (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.

Básicos	Fundacionales	Organizacionales
1. Inventario y control de activos de hardware	7. Protección de correo electrónico y navegador web	17. Implementar un programa de concienciación y capacitación en seguridad
2. Inventario y control de activos de software	8. Defensas contra malware	18. Seguridad del software de aplicación
3. Gestión continua de vulnerabilidades	9. Limitación y control de puertos de red, protocolos y servicios	19. Respuesta y gestión de incidentes
4. Uso controlado de los privilegios administrativos	10. Funciones de recuperación de datos	20. Pruebas de penetración y ejercicios de Red Team
5. Configuración segura para el hardware y el software de los dispositivos móviles, laptops, estaciones de trabajo y servidores	11. Configuración segura para dispositivos de red, tales como firewalls, routers y switches	
6. Mantenimiento, monitoreo, y análisis de logs de auditoría.	12. Protección perimetral	
	13. Protección de datos	
	14. Control de acceso basado en la necesidad de saber	
	15. Control de acceso inalámbrico	
	16. Monitoreo y control de cuentas	

ManageEngine

Grupo de Implementación

Grupo de Implementación 1 (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

Grupo de Implementación 2 (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.

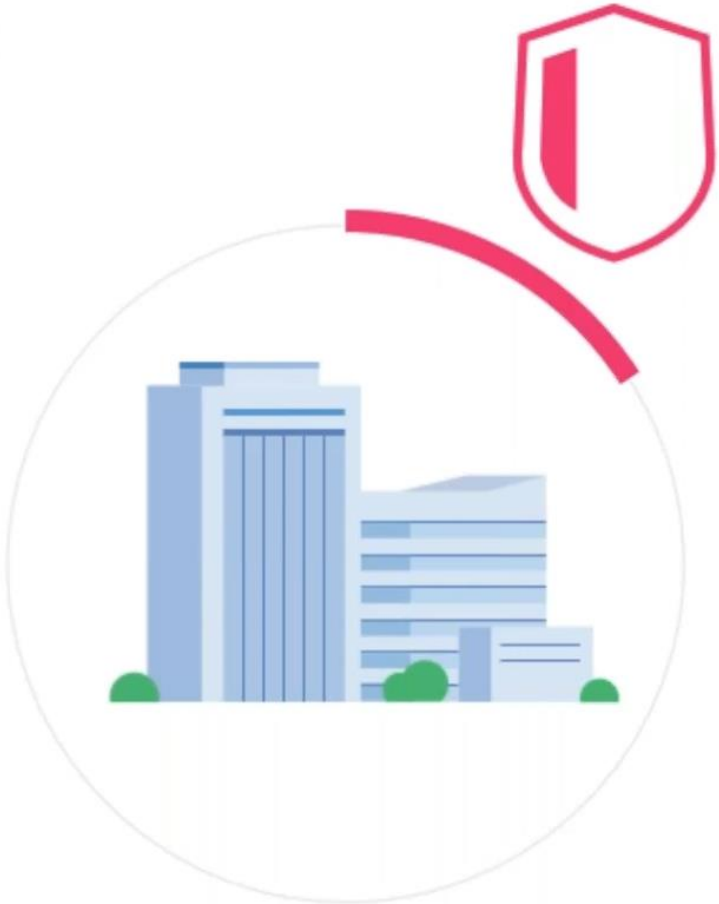
Grupo de Implementación 3 (IG3)

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.

ManageEngine

Implementando controles de CIS desde la gestión de endpoints

CONTROLES DE CIS
BÁSICOS



ManageEngine

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

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 está ejecutando en su red.

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

CONTROL 3

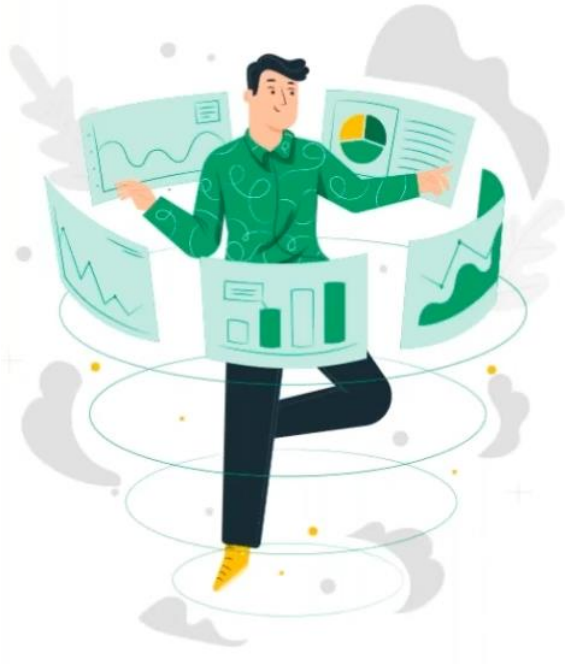
Gestión continua de vulnerabilidades

Analice continuamente sus activos para identificar vulnerabilidad 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 mas recientes.

CONTROL 4

Uso controlado de los privilegios administrativos

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



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.

CONTROL 6

Mantenimiento, monitoreo, y análisis de logs de auditoria

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.

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 solo a sitios web de confianza manteniendo filtros de URL basados en la red.

CONTROL 8

Defensa contra malware

Controle la instalacion 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.

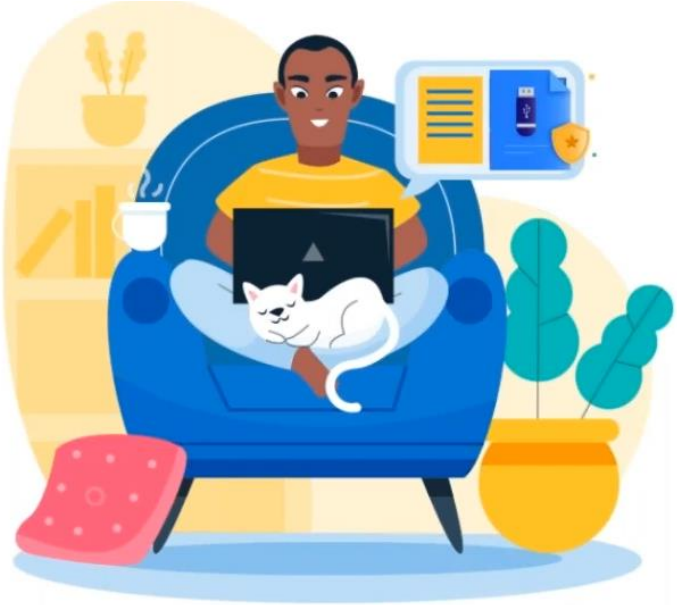
CONTROL 9

Limitación y control de puertos de red, protocolos y servicios

Para aquellas organizaciones que ya han optado software como servicios (SaaS), trabajar de forma remota es bastante simple. Un navegador y una buena conexión a internet es todo lo que se necesita para realizar el trabajo. Sin embargo, trabajar desde la casa tiene una buena cantidad de desafíos. La web alberga tanto distracciones como malware.

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.



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 perdida de datos, para garantizar la privacidad e integridad de los datos sensibles.

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 critica 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.

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 vulnerabilidad en los equipos de clientes inalámbricos para detectar vulnerabilidades explotables.

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

CONTROLES DE CIS
ORGANIZACIONES

A diferencia de los control básicos y funcionales, se trata de practicas que su organización debe adoptar internamente para garantizar una buena higiene cibernética.

CONTROL 17

Implemente un programa de concienciación y capacitación en seguridad.

Implemente un plan integrado para educar a los empleados en las habilidades y destrezas especificas 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.

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 datos y restaurar las operaciones rápidamente.

CONTROL 20

Pruebas de penetración y ejercicios de Red Team

Evalué periódicamente la preparación de su organización para defenderse de los ataques mediante la realización de pruebas. Simule objetivos y acciones de un atacante.

ManageEngine Endpoint Central

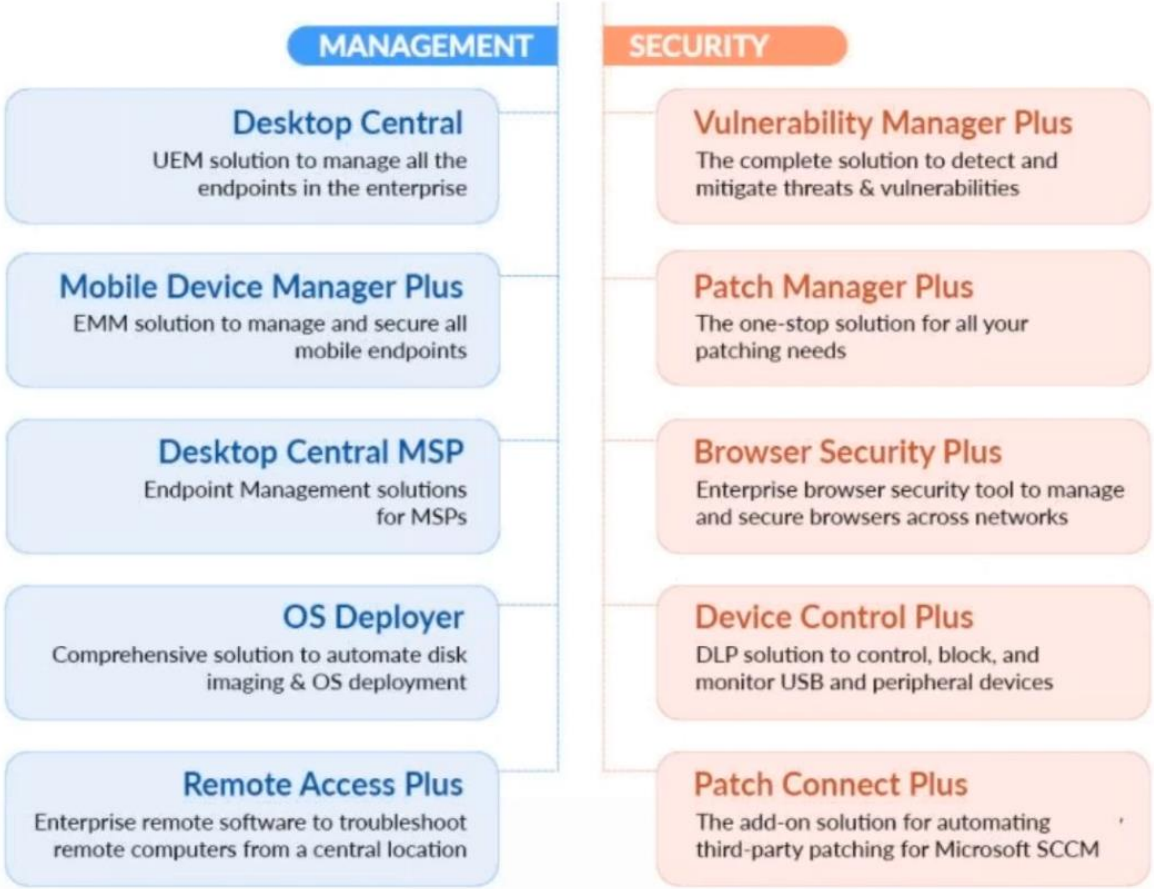
Que es ManageEngine Endpoint Central ?

Es una solución de administración unificada de endpoints (UEM) que ayuda a administrar servidores, computadoras portátiles, computadoras de escritorio, smartphones y tablets desde una ubicación central.

Lista de Controles CIS que abarcamos

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

Endpoint Management and Security



ManageEngine

Vulnerability Manager – CIS Controls 3,8,9

ID del parche	ID de boletín	Descripción del parche	Aprobar estado	Sistemas que faltan
325347	TU-024	7 Zip (exe) (x64) (22.00)	Aprobado	2
325084	TU-296	PuTTY (x64) (0.77)	Aprobado	2
325177	TU-034	Notepad++ (x64) (8.4.2)	Aprobado	1
325133	TU-058	FileZilla Client (x64) (3.60.1)	Aprobado	1
33956	MSRT-001	Windows Malicious Software Remova...	Aprobado	2
33296	MSRT-001	Windows Malicious Software Remova...	Aprobac	
325359	TU-037	CCleaner (6.01.9825)	Aprobac	
325469	TU-027	Mozilla Firefox (102.0)	Aprobac	

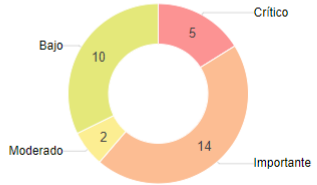
Vulnerabilidades | Configuraciones de seguridad | Sistemas | Parches

31
Vulnerabilidades totales

13
Vulnerabilidades corregibles

18
Vulnerabilidades con resolución manual

Resumen de gravedad de vulnerabilidades — Todos



Matriz de antigüedad de vulnerabilidades — Todos

Fecha de publicación | Fecha de la detección

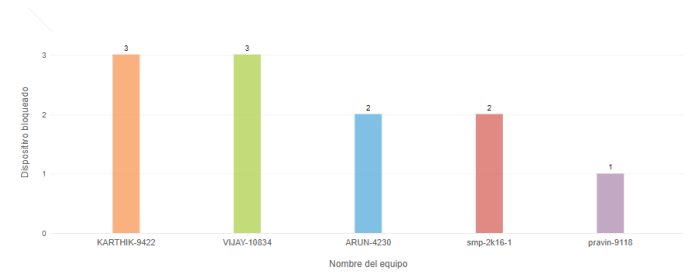
	Critical	Important	Moderate	Low	Info	Unrated
>90 días	3	5	2	0	0	0
60-90 días	0	1	0	1	0	0
30-60 días	1	7	0	8	0	0
<30 días	1	1	0	1	0	0

Device Control Plus – CIS Controls 8,13

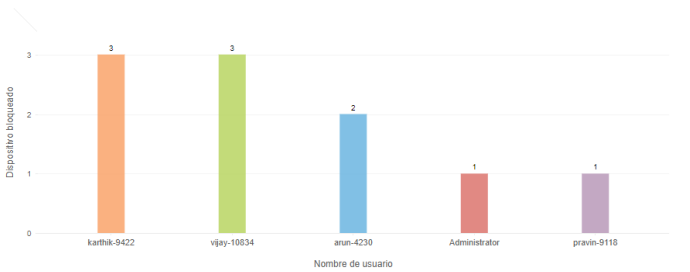
6	1
Equipos con directiva	Equipos sin directiva

11	18
Dispositivos bloqueados	Dispositivos permitidos

Equipos con dispositivos bloqueados



Usuarios con dispositivos bloqueados



1	1	1	2
Solicitudes de acceso temporal de los agentes	Solicitudes de acceso temporal aprobadas	Solicitudes de acceso temporal rechazadas	Solicitudes de acceso temporal revocadas

Dispositivos portátiles de Windows	Bloquear
Dispositivos Apple	Permitir
Dispositivos bluetooth	Sin cambio
Impresoras	Sin cambio
Módems	Bloquear
Adaptadores de red inalámbrica	Permitir
Dispositivos de creación de imágenes	Bloquear
Puertos serie (COM)	Sin cambio
Ver más	Sin cambio
	Bloquear

Browser Security Center – CIS Con

Prevencion Fuga Auditoria

Estado de mantenimiento del equipo

Mantenga un registro del estado de los equipos.

Categorización de los equipos no conformes

Haga un seguimiento de los equipos que no sean conformes a las r

Distribución predeterminada del navegador

Haga un seguimiento de los navegadores que los equipos de su organización utilizan de manera predeterminada.

Extensiones potencialmente nocivas

Haga un seguimiento de las extensiones que podrían causar vulne

Imprimir página web	Permitir	Restringir	No configurado
Imprimir desde almacenamiento en la nube	Permitir	Restringir	No configurado
Sincronización automática del navegador	Permitir	Restringir	No configurado
Guardar historial del navegador	Permitir	Restringir	No configurado
Autorrellenar	Permitir	Restringir	No configurado
Carga de archivos en páginas web	Permitir	Restringir	No configurado
Realizar capturas de pantalla	Permitir	Restringir	No configurado
Recordar contraseñas	Permitir	Restringir	No configurado
Sitio por proceso	Habilitar	Deshabilitar	No configurado
Sugerencias de búsqueda	Habilitar	Deshabilitar	No configurado
Notificación de métricas a Google	Habilitar	Deshabilitar	No configurado
Preguntar la ubicación de descarga	Habilitar	Deshabilitar	No configurado

Muchas Gracias

ethical SHIELDS

ManageEngine Endpoint Central