

GUÍA **ASEGURAR** **EQUIPOS**



ANCI
AGENCIA NACIONAL
DE CIBERSEGURIDAD

¿Qué equipos debemos asegurar?

Todo dispositivo que procese, almacene o transmita información institucional, o que pueda conectarse a los servicios de la organización, debe mantenerse identificado y protegido.

Esto incluye computadores, servidores, máquinas virtuales, dispositivos móviles, equipos utilizados para trabajo remoto, dispositivos IoT y OT, además de medios removibles, como memorias USB y discos externos.

Cada activo debe estar registrado, tener un responsable designado, una finalidad conocida y contar con medidas de seguridad proporcionales a su nivel de exposición, criticidad y al tipo de información que procesa.

No todos los equipos admiten los mismos controles. En dispositivos IoT, OT o sistemas antiguos puede ser necesario implementar medidas alternativas, como segmentación, aislamiento o monitoreo reforzado. Estas excepciones deben estar justificadas, documentadas y revisarse periódicamente.

¿Qué equipos debemos asegurar?

Asegurar los equipos permite disminuir la probabilidad de que sean comprometidos y ayuda a contener los incidentes antes de que se propaguen hacia otros sistemas.

También previene el robo de credenciales, la reutilización de sesiones, la instalación de herramientas no autorizadas, la extracción de información y la permanencia de mecanismos de acceso dentro de los equipos.

La seguridad de un equipo no depende de una única herramienta. Requiere mantener controles durante todo su ciclo de vida, desde su adquisición y configuración inicial hasta su reasignación o retiro.

¿Qué considerar a la hora de asegurar los equipos?

Inventario

Un inventario debe contener información sobre el tipo de dispositivo, responsable y área a la que pertenece, la función institucional, la versión, la ubicación, el soporte, sistema operativo, firmware, nivel de criticidad y tipo de información que procesa, el estado de autorización de actualización, fecha última revisión, entre otros.

El inventario debe mantenerse actualizado y compararse periódicamente con los equipos que realmente están conectados a la institución. Los activos desconocidos, no autorizados o que hayan dejado de reportar deben ser investigados, aislados o retirados.

Debe permitir responder preguntas concretas, como: ¿qué equipos están atrasados en sus actualizaciones?, ¿cuáles no tienen agentes de seguridad instalados?, ¿cuáles almacenan información sensible? y ¿cuáles deberían haber sido retirados?



Hardening

2 Tiene como finalidad reducir intencionalmente la superficie de ataque. Se trata de definir qué necesita cada equipo para cumplir su función y deshabilitar todo aquello que no sea necesario.

La configuración segura no debe realizarse una sola vez. Tiene que mantenerse durante la operación del equipo y revisarse cuando existan cambios importantes, nuevas amenazas o actualizaciones del sistema.

Una línea base segura debe ser conocida, repetible, estar documentada y ser suficientemente práctica para que la institución pueda mantenerla en el tiempo.

Algunos aspectos a considerar

- **Definir líneas base según el tipo de activo.** No todos los dispositivos cumplen la misma función. Se deben establecer configuraciones diferenciadas para computadores de usuario, servidores, dispositivos móviles, equipos OT, máquinas virtuales y otros activos.
- **Deshabilitar lo innecesario** los servicios, aplicaciones, protocolos, puertos y funciones que no sean necesarios deben desinstalarse o deshabilitarse. Un servicio olvidado puede mantener una vulnerabilidad durante años.

- **Eliminar las credenciales predeterminadas.** Las claves y credenciales proporcionadas por el fabricante deben cambiarse antes de poner el equipo en operación. También se deben deshabilitar las cuentas de invitado y eliminar aquellas que no se utilicen.
 - **Utilizar cuentas individuales.** Las personas deben trabajar con cuentas propias y evitar el uso de cuentas compartidas. Cuando sea posible, éstas deben administrarse desde un directorio central.
 - **Proteger las cuentas privilegiadas.** Las cuentas administrativas deben utilizarse únicamente cuando sean necesarias y no para actividades cotidianas, como navegar por Internet o revisar el correo electrónico.
 - **Identificar las cuentas especiales.** Las cuentas locales, de servicio, recuperación y emergencia deben estar registradas, protegidas y sujetas a revisión.
 - **Aplicar privilegios mínimos.** Cada usuario, aplicación o servicio debe contar únicamente con los permisos necesarios para cumplir su función. Las elevaciones de privilegios deben quedar registradas y mantenerse durante un tiempo limitado.
 - **Configurar el bloqueo de sesión.** Los equipos deben bloquearse automáticamente después de un período de inactividad y solicitar nuevamente autenticación para continuar.
- 

3

Protección y mantenimiento durante la operación

Los equipos deben ser monitoreados y mantenidos durante toda su operación. Algunas medidas son:

Cifrado: La información almacenada debe protegerse mediante mecanismos de cifrado adecuados, especialmente en notebooks, dispositivos móviles y otros equipos que puedan ser trasladados o extraviados.

Firewall del equipo: Cada equipo debe contar con un firewall activo, incluso cuando se encuentre dentro de la red institucional. Las reglas deben ser administradas, revisadas y, en lo posible, distribuidas de manera centralizada.

Antimalware y EDR: Estas soluciones deben mantenerse actualizadas, operativas y protegidas contra su desactivación. Cuando un equipo deje de reportar, presente fallas o intente deshabilitar sus mecanismos de protección, la institución debe recibir una alerta.

Actualizaciones: La institución debe mantener un inventario del software instalado y contar con un proceso para identificar, priorizar, probar y desplegar actualizaciones.

Este proceso debe considerar sistemas operativos, aplicaciones, controladores y firmware.

Software sin soporte: Cuando un software deja de recibir soporte es un riesgo, ya que puede mantener vulnerabilidades para las que no existirán nuevas correcciones. Por ello, es importante anticipar su reemplazo y evitar procesar o almacenar información crítica en ellos.

Registros y monitoreo: Los equipos deben generar registros para detectar actividades anómalas e investigar incidentes. Es fundamental mantener su hora sincronizada para facilitar la correlación de los eventos. Los registros relevantes deben enviarse a una plataforma central para que no dependan únicamente del equipo afectado.

Navegadores

4

Los navegadores procesan contenido proveniente de fuentes externas y potencialmente no confiables. Por esto, deben considerarse aplicaciones críticas dentro de la gestión de seguridad institucional.

Se deben utilizar navegadores con soporte vigente y mantener las actualizaciones automáticas habilitadas. Los navegadores que hayan dejado de recibir soporte deben ser retirados.

Las extensiones y políticas del navegador deben ser administradas centralizadamente, y es fundamental restringir la sincronización de información institucional con cuentas personales y evitar el almacenamiento no autorizado de credenciales.

Control de aplicaciones

5 Permite reducir la ejecución de programas, instaladores, scripts o componentes que no hayan sido autorizados por la institución. Su implementación se debe realizar gradualmente. Por lo general, este control falla cuando se activa sin contar previamente con un inventario del software utilizado. Para ello, se recomienda:

- Identificar las aplicaciones instaladas y utilizadas.
- Evaluar su finalidad, procedencia y necesidad.
- Definir las aplicaciones, fabricantes o componentes autorizados.
- Implementar inicialmente el control en modo de auditoría.
- Realizar una prueba con un grupo limitado de equipos.
- Corregir incompatibilidades y documentar las excepciones.
- Activar progresivamente el bloqueo.
- Monitorear los intentos de ejecución no autorizados.

Las aplicaciones deben obtenerse desde fuentes oficiales o repositorios aprobados. Se recomienda que los usuarios no cuenten con permisos para instalar un software sin autorización.

El control debe considerar no solo los programas tradicionales, sino también aplicaciones portables, scripts, macros y otras herramientas que puedan ejecutarse sin una instalación convencional.

6

Dispositivos móviles, medios removibles, acceso remoto y seguridad física

- **Celulares y Tablet:** Los dispositivos móviles que acceden a recursos de la institución, como correos, documentos o sistemas institucionales, deben ser considerados dentro de las medidas de seguridad. Esto aplica especialmente a los dispositivos móviles que pertenecen a la organización.
- **Medios extraíbles y USB:** Pueden introducir malware o facilitar la extracción de información. Su uso debe responder a una necesidad, limitarse a dispositivos autorizados y proteger los datos mediante análisis de seguridad y cifrado.
- **Acceso remoto:** Debe considerar MFA, equipos administrados, verificación de cumplimiento y el uso de servicios que no estén expuestos directamente a Internet.
- **Seguridad física:** Permite prevenir el acceso o la modificación no autorizada de los equipos. Se deben mantener áreas restringidas, bloqueo de sesión y una adecuada custodia de los dispositivos.
- **Pérdida de un equipo:** Se debe reaccionar rápidamente, considerando el reporte del incidente, la revocación de accesos, la preservación de evidencia y el control de la custodia, de manera que sea posible responder oportunamente.

Ciclo de vida del equipo

7 La seguridad de un equipo comienza antes de encenderlo y se extiende desde su adquisición hasta su devolución, reasignación o retiro.

Antes de entregar un equipo, se recomienda:

- Incorporarlo al inventario.
- Configurar el equipo según la línea base correspondiente.
- Recibir las actualizaciones disponibles.
- Tener instaladas y activas las herramientas de seguridad.
- Contar con cifrado, en caso de que corresponda.
- Tener un responsable asignado.
- Ser sometido a una verificación antes de entrar en operación.

En caso de que sea reasignado, se debe retirar la información del usuario anterior, revisar su configuración y registrar al nuevo responsable.

Si es retirado, hay que revocar los certificados y credenciales asociados, eliminar su inscripción de las plataformas institucionales y actualizar el inventario.

La información se debe sanitizar, según el tipo de almacenamiento y la sensibilidad de los datos. Este procedimiento debe quedar registrado y, cuando corresponda, contar con evidencia de su ejecución.

Lista de comprobación

8

Antes de considerar que un equipo se encuentra adecuadamente protegido, la institución debería poder confirmar:

- El equipo está registrado y tiene un responsable.
- Su finalidad, ubicación y nivel de criticidad son conocidos.
- Utiliza una configuración segura y documentada.
- Está dentro de soporte y cuenta con las actualizaciones necesarias.
- Tiene cifrado, firewall y herramientas de protección operativas.
- Solo utiliza aplicaciones autorizadas.
- Genera los registros necesarios para detectar e investigar incidentes.
- El acceso remoto requiere autenticación multifactor.
- Las desviaciones y excepciones están documentadas.
- Existe un procedimiento para actuar ante su pérdida o robo.
- Su reasignación o retiro considera la sanitización de la información y la actualización del inventario.

