ANCI
AGENCIA NACIONAL
DE CIBERSEGURIDAD

9 BÁSICOS DE LA CIBERSEGURIDAD

1 Actualizar periódicamente

La organización debe actualizar sus sistemas operativos, firmware y aplicaciones automáticamente en los dispositivos de usuario, y tan frecuentemente como sea posible en todos los aparatos. Para esto, conviene activar la opción de realizar actualizaciones automáticas.

Para asegurar que todos los sistemas y aplicaciones de la organización estén al día, es necesario contar con un adecuado inventario de sus activos digitales. Esto incluye:

- Implementación de métodos de detección automática de activos.
- Eliminación de los programas que ya no se utilizan.
- Reemplazo de aquellos que dejaron de tener actualizaciones de seguridad por parte del proveedor (o en el caso de que no sea posible, aislar ese dispositivo del resto de la red).

No se deben instalar más programas que los necesarios y explícitamente definidos por la organización.

La organización debe contar con planes para implementar actualizaciones de seguridad en activos críticos cuya indisponibilidad pueda afectar su normal funcionamiento, ya que esto puede disuadir a muchos organismos de actualizar sistemas críticos con la periodicidad necesaria.

Capacitar periódicamente

Los trabajadores de la institución deben recibir capacitaciones periódicas para aprender a detectar casos de phishing, y el manejo seguro de información en sus trabajos.

Todos los usuarios deben estar entrenados e informados desde que entran a la organización, y con refuerzos periódicos, sobre sus políticas de seguridad de la información o sus normas de ciberseguridad industrial. Esta comunicación debe procurar que cada persona sepa cuál es su responsabilidad en materia de ciberseguridad y de protección de los datos que maneja la organización.

Así, se debe hablar de los riesgos existentes en internet, como phishing, fraudes, exposición de información sensible, e incidentes, entre otros. Es positivo preparar ambientes de práctica, e implementar evaluaciones luego de cualquier instancia de capacitación.

El equipo de recursos humanos debe poner en práctica los contenidos aprendidos en capacitaciones contra phishing, fraude y uso seguro de recursos.

Minimizar privilegios

La cuenta de cada usuario debe contar con los mínimos privilegios necesarios para realizar su trabajo. Esto incluye los permisos de acceso a los diferentes sistemas de la organización.

Es necesario, para la entrega de permisos efectiva, realizar una identificación previa de los tipos de información que maneja la institución, y quién debe tener acceso a qué tipos de datos. Considerar asimismo la implementación de limitaciones geográficas y temporales para la conexión a ciertos sistemas.

Debe existir un procedimiento de validación para los usuarios que pidan mayores permisos para realizar tareas específicas, y que estos sean retirados en cuanto hayan terminado. Las cuentas de administrador deben contar con autenticación multifactor (MFA). Asimismo, es necesario determinar los niveles de privilegio que se entregue a proveedores, clientes y socios, y asegurarse de que entiendan sus roles y responsabilidades.

En sectores de mayor criticidad, se puede definir que las cuentas estén excluidas de conectarse a internet, salvo excepciones explícitas.

Deben existir mecanismos automatizados para monitorear el uso de cuentas en sistemas críticos de la organización, detectando posibles amenazas internas, y que permitan, incluso, bloquear cuentas de usuario. Es recomendable que toda cuenta sea desactivada automáticamente tras cierto período de inactividad, a menos que fuera considerada esencial. Y que se monitoree todo acceso remoto a los sistemas de la organización.

4 Respaldar periódicamente la información

Tanto los dispositivos laborales de cada trabajador deben contar con planes de respaldo periódico, los que deben ser almacenados en un aparato habilitado especialmente para ello, en un lugar distinto al del dispositivo respaldado y no estar permanentemente conectado al mismo.

Se debe privilegiar el respaldo de las aplicaciones más críticas para la normal operación de la institución. Los procedimientos de restauración deben estar planificados y ser testeados periódicamente como parte de los ejercicios de recuperación ante incidentes. Los respaldos también deben estar segmentados, impidiendo el acceso, modificación o borrado de los más sensibles por parte de usuarios que no los necesitan. Definir la periodicidad de los respaldos considerando cuánta información se perdería en el caso de un incidente.

Debe haber en la organización planes de respuesta a incidentes y planes de recuperación, los que deben ser regularmente actualizados, comunicados al personal, y practicados. Los respaldos críticos de sistema deben ser almacenados en un lugar diferente de los respaldos críticos de información, para una recuperación más rápida. Asegurar que solo usuarios específicos tengan permisos para implementar y modificar los respaldos.

Asegurar redes

Las redes de la institución deben segmentarse de tal modo de que queden separados los dispositivos de los trabajadores según su división interna o sus responsabilidades. Los dispositivos deben poder acceder solamente a los equipos internos que necesitan para que los trabajadores puedan cumplir sus funciones.

Puede ser necesario, para una segmentación efectiva, realizar una identificación previa de los tipos de información que maneja la institución, quién debe tener acceso a qué tipos de datos, cuáles son los flujos de información, y qué partes de la red y del ambiente IT/OT de la organización es realmente necesario que compartan qué tipo de información.

La implementación de firewalls también debiera extenderse a aparatos, como smartphones o tablets, que interactúen con los sistemas de la organización, y todos los firewalls debieran contar con un antivirus. Considere instalar un sistema de detección y prevención de intrusiones (IDPS).

Los event logs deben estar protegidos contra modificación y borrado, y ser revisados de forma oportuna para detectar eventos de ciberseguridad, los que pueden convertirse en incidentes.

Asegurar equipos

Los dispositivos de los trabajadores deben mantener contraseñas u otros sistemas de autentificación robustos, además de contar con mecanismos de protección de información en reposo como cifrado en disco. Revisar que no haya programas con claves por defecto o privilegios de acceso especiales.

Se deben implementar programas de control de las aplicaciones en los equipos de los trabajadores, restringiendo el uso a programas, ejecutables, bibliotecas de software, scripts, instaladores, HTML compilado, aplicaciones HTML y applets de panel de control previamente autorizados.

Deshabilitar el uso de navegadores sin soporte, y que los navegadores permitidos no procesen elementos como Java o avisos web. También impedir que estas opciones puedan ser modificadas por los usuarios.

Los event logs están protegidos contra modificación y borrado, y son revisados de forma oportuna para detectar eventos, incidentes o ciberataques.

No ignorar la seguridad física de los dispositivos y contar con un inventario de los activos en los que se contenga o procese información, para lo que pudiera considerarse el uso de una herramienta de administración de activos TI con la capacidad de detectar usos indebidos. De suceder esto último, el hardware en cuestión debe ser revisado, puesto en cuarentena o cambiado, según un procedimiento establecido previamente.

Es necesario contar con un inventario del software en uso en la organización, que registre y alerte de cualquier cambio en las plataformas y aplicaciones en uso. Si se detecta software no autorizado, deberá ser puesto en cuarentena para su posible eliminación.

Si alguna de estas actividades está externalizada, las condiciones mencionadas previamente deben estar bien explicitadas en el contrato con la empresa respectiva.

Analizar si existen activos que deban ser cifrados debido a su confidencialidad, ya sea durante su transporte o almacenamiento.

7 Monitorear en tiempo real

Cada equipo de la organización debe contar con algún sistema de monitoreo de eventos de ciberseguridad en tiempo real, para detectar actividad maliciosa.

El sistema debe ser elegido e implementado por el equipo responsable de ciberseguridad de la institución, no por cada trabajador individualmente. El programa antimalware debe incorporar actualizaciones frecuentes para reconocer nuevas amenazas.

Establecer una contraseña robusta para el firewall, conocida solo por quienes sea necesario, además de implementar un segundo factor de autenticación. También resulta útil obtener inteligencia de amenazas proveniente de foros y otras fuentes. Deben monitorearse los sistemas críticos para detectar todo uso no autorizado de sus sistemas y conexiones no autorizadas.

Una buena administración de antivirus requiere que se controle permanentemente que todos los activos institucionales tengan su agente instalado y actualizado. Adicionalmente, se debe configurar la ejecución periódica de escaneos profundos en búsqueda de amenazas.

Usar mecanismos de Múltiples Factores de Autenticación (MFA)

Los usuarios deben contar con más de un mecanismo de autenticación para ingresar a sus dispositivos y cuentas de usuario.

Estos mecanismos deben considerar al menos dos de las siguientes categorías: “algo que sabes” (contraseñas o PIN), “algo que tienes” (smartphone, tarjeta de coordenadas, token) y “algo que eres” (huella dactilar, reconocimiento facial o de iris, entre otros).

Al momento de implementar MFA, priorizar las cuentas de los servicios más sensibles, y considerar no solo aquellas cuentas propias de la organización, sino también las que sus miembros pueden emplear en sistemas de proveedores, clientes u entes relacionados.

Es imprescindible contar con MFA para sistemas expuestos a internet, como los que entregan acceso remoto (VPN, RDP).

Debe existir asimismo una política de contraseñas que implemente medidas como el cambio de todas las claves por defecto y la imposición de ciertos mínimos de extensión y complejidad de las mismas. No es recomendable obligar a los usuarios a cambiar sus contraseñas periódicamente.

Usar gestor de contraseñas

Todos los usuarios de la entidad deben utilizar adecuadamente un gestor de contraseñas, el cual debe contar con una clave extensa y memorizable, y debe almacenar todas las credenciales relacionadas con el ejercicio del trabajo de la persona.

Las claves de otras cuentas institucionales deben ser aleatorias y generadas por el gestor de contraseñas.

Un gestor de contraseñas protege a la persona en la medida que sea utilizado. Esto se logra cuando las claves almacenadas son aleatorias y largas, y las personas nos vemos obligadas a usarlo porque no podemos recordar las claves almacenadas.

Buenas prácticas incluyen instalar la extensión oficial del gestor para el navegador, configurar el navegador para que no almacene las claves, e imprimir la hoja de recuperación (cuando el gestor ofrece esta opción).

ANCI
AGENCIA NACIONAL
DE CIBERSEGURIDAD

ANCI.GOB.CL/9BASICOS

V1 \ NOVIEMBRE **2025**