GUÍA RÁPIDA

MINIMIZAR PRIVILEGIOS

ANCI
AGENCIA NACIONAL
DE CIBERSEGURIDAD

¿Qué es?

El principio de mínimos privilegios consiste en otorgar a los usuarios de una organización el **mínimo de permisos a los recursos, aplicaciones e información,** con el objetivo de evitar que terceros accedan a datos críticos y confidenciales.

Gracias a esto, es posible **controlar los permisos y responsabilidades,** asignando a cada persona el acceso que corresponda según sus roles y requisitos del trabajo: no más, ni menos.

¿Por qué es importante el principio del mínimo privilegio?

- **Minimiza** la superficie de ataque en caso de que un tercero logre acceder a una cuenta. El daño que podrá hacer dependerá de los permisos habilitados para dicha cuenta.
- **Fortalece** la seguridad de las instituciones.
- **Contiene** filtraciones de datos y disminuye el daño en caso de un acceso no autorizado.
- **Reduce** costos y tiempo al gestionar a los usuarios de forma segura.

Plan para minimizar privilegios

Para implementar esta práctica de forma efectiva, es importante elaborar un plan que establezca diversos criterios, como:

1. **Realiza un inventario** con los sistemas de accesos y permisos existentes en la institución. Así también, identifica si las aplicaciones utilizadas tienen la licencia adecuada y los proveedores de los que depende tu organización.

2. **Define los perfiles** que existen en tu institución. Por ejemplo, administración de sistemas, soporte, finanzas, producto, atención al cliente, proveedor externo, entre otros.

   Para comenzar con la definición de perfiles, puedes utilizar el organigrama. Considera que no es necesario que todo un equipo tenga los mismos permisos.

3. **Analiza el tipo de información que maneja tu institución.** Con esto claro, puedes establecer qué perfiles deben acceder a los distintos tipos de datos.

4. **Define el acceso restringido a todo recurso por defecto**, con el objetivo de evitar que una persona tenga acceso a un recurso por error o no definición.

   Los permisos en recursos críticos como datos confidenciales, servidores, bases de datos, etc., deben estar en listas de acceso específicas, esto quiere decir, todo bloqueado, excepto una lista.

5 **Evalúa continuamente el uso de los privilegios de cada usuario**, de manera de eliminar permisos a quienes no los requieran y garantizar que puedan seguir trabajando sin interrupciones.

Es recomendable automatizar la bajada de perfiles y permisos por no uso.

6 **Define un plan de gestión de permisos permanentes,** considerando pasos y responsables para solicitar, modificar y eliminar perfiles de permisos de los usuarios.

7 **Define un plan de gestión de permisos temporales.** Muchas veces será necesario que una persona tenga acceso temporal a un recurso o funcionalidad. Elabora un plan que considere un responsable de autorizar este permiso (jefatura, por ejemplo), un plazo máximo de autorización y un responsable de dar y quitar los permisos.

8 **Considera limitaciones geográficas (usando GPS o GeoIP) y temporales** en la asignación de perfiles para la conexión a ciertos sistemas, en especial si los turnos de trabajo se ejecutan en rangos de horario y lugares específicos.

9 **Monitorea y revisa periódicamente privilegios** para aquellas cuentas con acceso a sistemas críticos, para detectar posibles amenazas internas e identificar privilegios que ya no son necesarios, de manera de reducir, ajustar o revocar permisos.

Puedes utilizar herramientas automatizadas como la gestión de acceso e identidad (IAM), la gestión de eventos e información de seguridad (SIEM) y la gestión de acceso privilegiado (PAM).

10 **No uses cuentas genéricas (admin, soporte, etc.).** Asócialas a personas, usando un nombre de usuario reconocible.

Las únicas cuentas que se recomiendan de uso genérico son aquellas para integraciones y automatizaciones, las que deben estar específicamente restringidas (ubicación, IP), limitadas a los mínimos accesos para ejecutar su función, tienen que estar diferenciadas para cada integración y ser configurables solo por administradores de sistemas.

Otros aspectos a considerar:

- Todas las cuentas, especialmente las de administración, **deben tener activado el doble factor de autenticación (MFA).**
- **Limita el acceso a sistemas administrativos** solo a quienes se conecten a través de una VPN.
- **Monitorea** todo acceso remoto a los sistemas de la organización, en especial si proviene de ubicaciones no reconocidas o se realiza en horarios poco comunes.