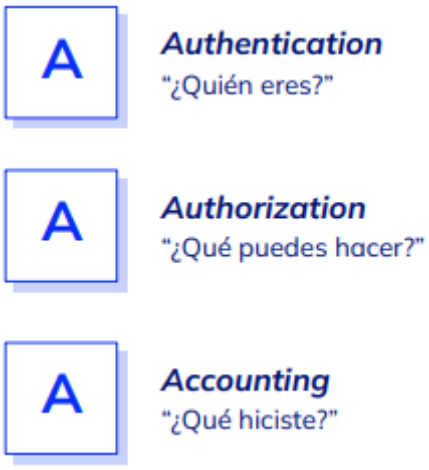
Femme Net-
AAA

Autenticación, autorización y contabilidad

¿Qué es AAA? Marco de seguridad informática fundamental para controlar el acceso a los datos y recursos del sistema, aplicar políticas y auditar acciones. Se compone de 3 pilares.



- *Autenticación*: verificar la identidad del usuario mediante el proceso de inicio de sesión en un sistema.

- *Autorización*: Determinar qué acciones y recursos puede acceder y realizar un usuario dentro del sistema

- *Contabilidad*: Registrar y rastrear la actividad del usuario en el sistema incluyendo accesos, modificaciones y fechas.

Beneficios de AAA

- ***Mayor seguridad***: reduce el riesgo de accesos no autorizados y robo de datos.
- ***Más eficiente:*** simplifica la administración de usuarios y permisos.
- *Mayor visibilidad*: permite auditar y analizar la actividad del usuario para identificar posibles amenazas.

AAA es una herramienta esencial para proteger la información y los recursos de una organización.

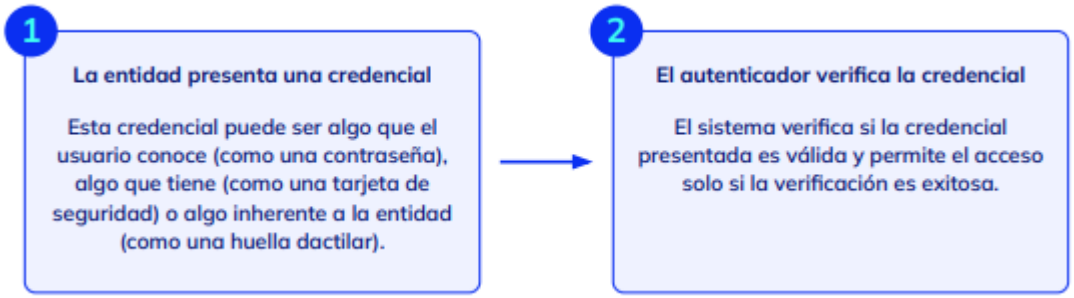
Autenticación

La autenticación es un pilar fundamental en la seguridad informática. Sirve para verificar la identidad de una entidad que intenta acceder a un recurso. Se puede comparar con la presentación de una identificación para entrar a un club exclusivo.

En este contexto, una entidad puede ser:

- Un usuario: la persona que intenta acceder a un sistema o red.
- Un servicio o proceso: un programa que se ejecuta en un ordenador o servidor y necesita comunicarse con otro sistema.
- Una estación de trabajo o servidor: el propio dispositivo que intenta conectarse a la red.
- Un dispositivo de red: un router, firewall u otro dispositivo que forma parte de la infraestructura de red.

¿Cómo funciona la *autenticación*?



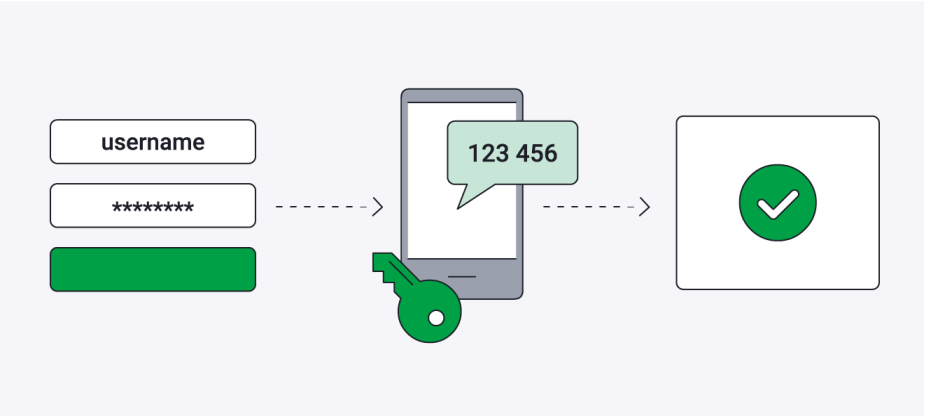
Autenticación multifactor(MFA)

Para fortalecer la seguridad, se suele utilizar la autenticación multifactor (MFA). La MFA requiere presentar dos o más factores de autenticación para acceder a un recurso.

Esto añade capas adicionales de seguridad a los procesos de inicio de sesión tradicionales, haciendo más difícil para los atacantes acceder a los sistemas, incluso si obtienen una contraseña.

Veamos los tres factores principales utilizados en la autenticación multifactor:

- Algo que sabes (contraseña, PIN).
- Algo que tienes (token RSA).
- Algo que eres (huella dactilar, reconocimiento facial).



Beneficios de la autenticación multifactor

- Mayor seguridad: añade capas adicionales que dificultan el acceso no autorizado a los sistemas, incluso si un atacante obtiene una contraseña.
- Reducción del riesgo de fraude: proporciona una barrera adicional contra ataques de phishing y fuerza bruta.
- Mayor cumplimiento normativo: algunas regulaciones exigen el uso de MFA para proteger la información sensible.

Autenticación VS Verificación de identidad

»Si bien la verificación de identidad (identity proofing) y la autenticación son conceptos relacionados con la seguridad informática, tienen propósitos distintos.

Autenticación

Su objetivo es **verificar la identidad de alguien que ya posee credenciales de acceso.**

Se produce durante el inicio de sesión en un sistema o aplicación.

Ejemplo: Ingresar tu nombre de usuario y contraseña para acceder a tu correo electrónico o usar tu huella dactilar para desbloquear tu teléfono.

En resumen, **verifica si alguien es quien dice ser en base a credenciales previamente emitidas.**

vs.

Verificación de identidad
(Identity Proofing)

Su objetivo es **validar la identidad de alguien antes de otorgarle credenciales de acceso.**

Ocurre antes de establecer una cuenta o emitir credenciales.

Ejemplo: presentar un documento de identidad oficial (como un pasaporte o licencia de conducir) para abrir una cuenta bancaria o verificar la edad al ingresar a un sitio web para adultos.

En resumen, **confirma la identidad de alguien antes de otorgarle credenciales.**

Reglas generales de contraseña

Las contraseñas son la primera línea de defensa para proteger cuentas en línea. Las contraseñas débiles son fáciles de adivinar o descifrar para los atacantes, ponen en riesgo la información personal y financiera.

Se deben seguir estas reglas generales para crear y administrar contraseñas fuertes:

- Fuerza de la contraseña.
- Seguridad de la contraseña.
- Prevención de ataques.

Fuerza de la contraseña

- *Mínimo 8 caracteres*: cuanto más larga sea la contraseña, más difícil será romper.
- *Complejidad*: combina letras mayúsculas y minúsculas, números y símbolos especiales (@, #, $, etc.) para crear una contraseña aleatoria y difícil de adivinar. Evita patrones simples como "qwerty" o secuencias consecutivas (12345).

Seguridad de la contraseña

- *Nunca escribir una contraseña*: no apuntar las contraseñas en notas adhesivas, documentos de texto o celulares. Considerar un gestor de contraseñas seguro para almacenarlas.
- *No compartir contraseñas*: evitar compartir contraseñas (ni siquiera con amigos o familiares).
- *Cambiar tus contraseñas regularmente*: actualizar las contraseñas en forma periódica, especialmente para cuentas importantes como el correo electrónico, banca online y redes sociales. Se recomienda cambiarlas cada 60 a 90 días.

Prevención de ataques

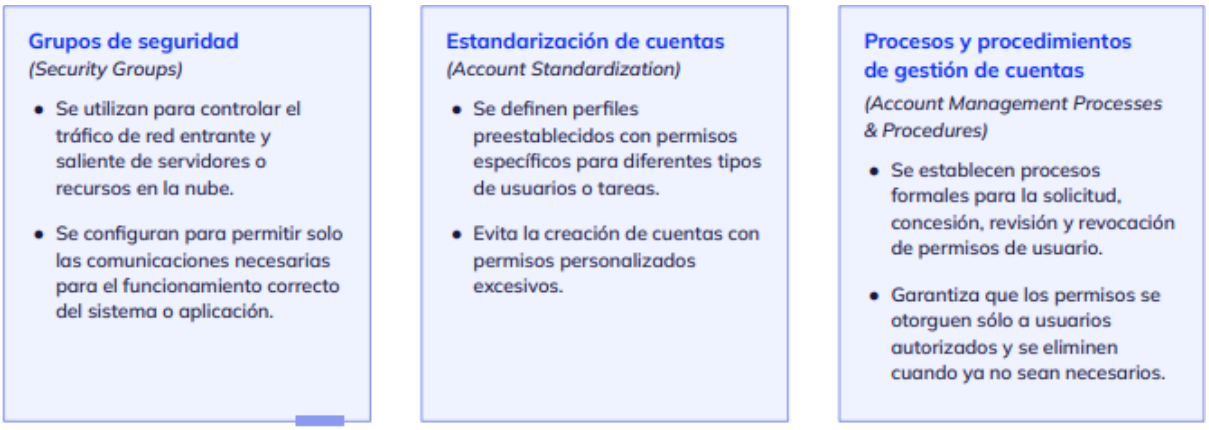
- No reutilizar contraseñas: evitar usar la misma contraseña para múltiples cuentas. Si un atacante descubre la contraseña de una cuenta, no podrá acceder a todas las demás si se utilizaron contraseñas diferentes.
- No permitir la reutilización de contraseñas anteriores: muchos sistemas obligan a elegir una contraseña nueva que no sea igual a las últimas cuatro o más contraseñas utilizadas.
- Políticas de bloqueo de cuenta: implementar políticas de bloqueo de cuenta que bloquean el acceso, después de un número determinado de intentos de inicio de sesión fallidos (por ejemplo, 3 intentos fallidos). Esto ayuda a prevenir ataques de fuerza bruta.
- Contraseñas predeterminadas seguras: cambiar siempre las contraseñas predeterminadas asignadas a las cuentas de usuario nuevas. Estas contraseñas predeterminadas suelen ser débiles y fácilmente adivinables. Además, configurar las contraseñas predeterminadas para que caduquen después del primer uso, obligando al usuario a crear una contraseña segura.

Autorización

El principio del mínimo privilegio (Least Privilege en inglés) es una estrategia fundamental en seguridad informática que garantiza que a usuarios,

sistemas, procesos y aplicaciones se les otorguen únicamente los permisos mínimos e imprescindibles para realizar sus tareas asignadas.

¿Cómo implementar el mínimo privilegio?



Denegación implícita

La denegación implícita (en inglés, Implicit Deny) es un principio fundamental en el control de acceso informático. Funciona bajo la premisa de "lo que no está permitido, está denegado". Imagina una puerta cerrada con llave. A menos que tengas la llave correcta (permiso), no puedes entrar.

Se implementa principalmente a través de Listas de Control de Acceso (ACLs), que son conjuntos de reglas que definen qué usuarios o sistemas tienen permitido acceder a recursos específicos. En la denegación implícita, se configura una regla predeterminada en la ACL para denegar cualquier acceso que no esté explícitamente permitido por otra regla.

Ventajas de la denegación implícita:

- Mejora la seguridad: reduce el riesgo de accesos no autorizados al denegar por defecto cualquier intento no permitido.
- Simplifica la administración: solo se necesita crear reglas explícitas para los accesos necesarios, minimizando la complejidad de la ACL.
- Mayor control: permite un control granular sobre quién y qué puede acceder a los recursos.

Contabilidad

La contabilidad juega un papel muy importante en lo relacionado a auditoría, controles y la administración de incidentes.

Importancia de la contabilidad en:

- Integridad de los registros.
- Retención de registros.
- Auditoría de registros.
- Cumplimiento normativo.
- Respuesta a incidentes.

-*Integridad de los registros*: Además de la recolección de registros, es crucial garantizar la integridad de los mismos. Esto implica proteger los registros contra modificaciones no autorizadas o eliminaciones. La implementación de medidas como el cifrado de registros, firmas digitales y controles de acceso estrictos ayuda a preservar la integridad de la información registrada.
-*Retención de registros*: Las organizaciones deben establecer políticas claras de retención de registros para determinar cuánto tiempo deben mantenerse los registros de eventos. Estas políticas pueden estar influenciadas por requisitos legales, regulatorios y empresariales.
-*Auditoría de registros:* La auditoría periódica de los registros de eventos es fundamental para garantizar la integridad y la seguridad del sistema. Se deben revisar y analizar los registros en busca de anomalías, actividades sospechosas, o violaciones de políticas de seguridad.
-*Cumplimiento normativo*: La contabilidad también juega un papel importante en el cumplimiento de regulaciones y estándares de seguridad. Muchas normativas requieren la implementación de controles de contabilidad para garantizar la trazabilidad y la transparencia en las operaciones de TI.
-*No repudio en la contabilidad:* En el contexto de la integridad de los registros, el no repudio se relaciona con asegurar que los registros no puedan ser modificados o eliminados de manera que una entidad pueda negar haber realizado una acción registrada. Es decir, que aseguran de cierta forma la integridad de la contabilidad.