

CS-009 · Fundamentos

Principios básicos de seguridad

Los principios de diseño, como el mínimo privilegio y la falla segura, que hay detrás de las buenas decisiones de seguridad.

[Read this reference sheet in English](#)

[← CS-008](#)

Ficha 9 de 15

[CS-010 →](#)

Resumen ejecutivo

Los principios básicos de seguridad son ideas de diseño probadas con el tiempo que guían las decisiones sólidas de seguridad: el mínimo privilegio, la separación de funciones, la falla segura y la simplicidad del diseño. No son herramientas ni productos, sino reglas prácticas que ayudan a construir sistemas resistentes desde el diseño. Entenderlos permite razonar sobre seguridad de forma consistente en cualquier tecnología.

Qué es

Los principios básicos de seguridad son un conjunto de ideas fundacionales, afinadas durante décadas, que describen cómo diseñar y operar sistemas seguros. El mínimo privilegio significa dar a cada usuario, proceso o sistema solo el acceso que de verdad necesita. La separación de funciones reparte las acciones sensibles entre varias personas, de modo que nadie pueda actuar en solitario. La defensa en profundidad superpone controles para que ninguna falla aislada sea fatal. La falla segura significa que, cuando algo sale mal, el sistema queda por omisión en un estado seguro y cerrado. Otros principios muy citados son mantener los diseños simples, no depender del secreto del diseño, reducir la superficie de ataque y la mediación completa, que consiste en verificar cada acceso en lugar de confiar en una verificación anterior.

Por qué importa

Las tecnologías cambian sin parar, pero estos principios permanecen, y eso los convierte en una forma duradera de razonar sobre seguridad. Quien los interioriza puede evaluar rápido un sistema desconocido con unas pocas preguntas: si concede el mínimo privilegio, si falla de forma segura y si su diseño es más complejo de lo necesario. Aplicar los principios temprano, durante el diseño, es mucho más barato que añadir seguridad después. Para las organizaciones, un diseño con principios reduce la cantidad y la gravedad de las debilidades. Para las carreras, estos principios aparecen a lo largo de las certificaciones y las entrevistas, y sostienen toda la práctica del diseño seguro.

■ Cómo funciona

Los principios se aplican como preguntas y restricciones durante el diseño, la revisión y la operación. Al conceder acceso, los equipos se preguntan cuál es el mínimo necesario y conceden solo eso. Al diseñar un flujo sensible, separan funciones para que quien aprueba no sea quien ejecuta. Al manejar errores, se aseguran de que las fallas dejen el sistema cerrado y no abierto. Al revisar una arquitectura, buscan la complejidad innecesaria que esconde defectos. Los principios se refuerzan entre sí: el mínimo privilegio limita el daño de una brecha, la defensa en profundidad hace que una falla aislada sea sobrevivible y la mediación completa asegura que el acceso siempre se verifique. Juntos forman una manera consistente de pensar, no una lista que se completa una vez.

■ Diagrama de arquitectura



Los principios envuelven al sistema y cada uno moldea decisiones de diseño, del acceso al comportamiento ante una falla.

Flujo de trabajo

Durante el diseño, preguntar cuál es el acceso mínimo que cada parte necesita de verdad. →

Separar las funciones sensibles para que ningún actor pueda completarlas solo. →

Superponer controles para que una falla no deje todo expuesto. →

Diseñar las rutas de error y de falla para que queden por omisión en un estado cerrado. →

Simplificar el diseño y retirar la complejidad innecesaria. →

Asegurar que cada acceso se verifique, en lugar de confiar en una decisión anterior.

Ataques frecuentes

- Abuso de privilegios cuando las cuentas tienen más acceso del necesario
- Fraude posible cuando una sola persona controla todo un proceso sensible
- Explotación de un control único, sin profundidad detrás
- Sistemas que fallan abiertos y conceden acceso durante un error
- Rutas de evasión escondidas en diseños demasiado complejos y difíciles de revisar

Errores frecuentes

- Conceder acceso amplio por comodidad y no recortarlo nunca
- Permitir que la misma persona solicite y apruebe acciones sensibles
- Confiar en el secreto del diseño en lugar de en controles sólidos
- Diseñar sistemas que fallan abiertos cuando algo se rompe

- Añadir complejidad que nadie entiende del todo ni puede revisar

Buenas prácticas

- Conceder el mínimo privilegio y revisar los accesos con regularidad
- Separar funciones en las acciones sensibles o de alto valor
- Superponer controles para que ninguna falla aislada sea catastrófica
- Diseñar las rutas de falla para que por omisión fallen de forma segura
- Preferir diseños simples y revisables antes que la complejidad ingeniosa
- Verificar cada acceso en lugar de confiar en una decisión previa

Lista de verificación

- ☒ Accesos concedidos con el mínimo privilegio y revisados de forma periódica
- ☒ Separación de funciones aplicada a los procesos sensibles
- ☒ Controles que se traslapan, sin un punto único de falla
- ☒ Estados de error y de falla que quedan cerrados, no abiertos
- ☒ Diseño revisado en busca de complejidad innecesaria
- ☒ Verificaciones de acceso aplicadas de forma consistente, sin omitirse tras la primera concesión

Herramientas recomendadas

Gestión de identidades y accesos (IAM)

Impone el mínimo privilegio y las revisiones de acceso

Gestión de accesos privilegiados (PAM)

Controla y separa el acceso administrativo de alto riesgo

Sistemas de flujo de trabajo y aprobación

Sostienen la separación de funciones en las acciones sensibles

Herramientas de configuración y política como código

Codifican valores por omisión de falla segura y verificaciones consistentes

■ Normas del sector

NIST SP 800-53

Controles que reflejan el mínimo privilegio, la separación de funciones y más

NIST SP 800-160

Orientación para construir sistemas confiables y con principios

ISO/IEC 27001

Sistema de gestión que refleja un diseño de accesos y controles con principios

■ Relevancia profesional

Los principios de diseño seguro son la base para ingenieros de seguridad, arquitectos, personas que programan con prácticas seguras y analistas de GRC que evalúan si un diseño es sólido. Aparecen a lo largo de las certificaciones de entrada y avanzadas, y son material frecuente de entrevista porque revelan si alguien sabe razonar sobre seguridad y no solo operar herramientas. Los profesionales de gobernanza de la inteligencia artificial aplican los mismos principios a cómo se accede y se controlan los sistemas de IA.

■ Preguntas de entrevista

- ¿Qué significa el mínimo privilegio y por qué resulta tan eficaz?
- Explique la separación de funciones con un ejemplo práctico.
- ¿Qué significa que un sistema falle de forma segura en lugar de fallar abierto?
- ¿Por qué la simplicidad se considera un principio de seguridad?
- ¿Qué es la mediación completa y por qué importa?

■ Certificaciones relacionadas

CompTIA Security+

ISC2 CISSP

ISC2 Certified in Cybersecurity (CC)

■ Para profundizar

- [Catálogo de controles NIST SP 800-53 \(en inglés\)](#)

- NIST SP 800-160, ingeniería de seguridad de sistemas (en inglés)
- CISA: seguro por diseño (en inglés)

Puntos clave

- Los principios básicos son ideas de diseño duraderas, no herramientas ni productos.
- El mínimo privilegio y la separación de funciones limitan el daño de cualquier compromiso.
- La falla segura significa quedar por omisión en un estado seguro y cerrado ante un error.
- La simplicidad y la mediación completa hacen los sistemas más fáciles de asegurar y revisar.
- Aplicar los principios en el diseño cuesta mucho menos que corregir defectos después.

Preguntas frecuentes

- ▶ ¿Cuál es la diferencia entre mínimo privilegio y confianza cero?
- ▶ ¿Qué significa falla segura en términos simples?
- ▶ ¿Por qué la simplicidad es un principio de seguridad?

Carreras relacionadas

PUESTOS RELACIONADOS

Security Engineer

Security Architect

Grc Analyst

CERTIFICACIONES RELACIONADAS

CompTIA Security+

ISC2 CISSP

ISC2 Certified in Cybersecurity (CC)

VACANTES ACTUALES

GUÍAS Y SALARIOS

Las vacantes vigentes están en la bolsa de empleo.

[Ver todas las vacantes](#)

[Vacantes en español](#)

[Glosario GRC](#)

[Empezar en privacidad](#)

[Cumplimiento por país](#)

RUTA DE APRENDIZAJE SUGERIDA

- 1 Afiance las bases con [CS-001 Ciberseguridad](#)
- 2 Estudie esta ficha: **Principios básicos de seguridad**
- 3 Profundice: [Ciberseguridad](#)
- 4 Profundice: [La tríada CIA](#)
- 5 Valídelo: trabaje hacia **CompTIA Security+**
- 6 Encuentre el puesto: [vea las vacantes disponibles](#)

Las vacantes se publican en el idioma del empleador, por lo general en inglés.

FICHAS RELACIONADAS

[CS-001 Ciberseguridad](#)

[CS-002 La tríada CIA](#)

[CS-003 Defensa en profundidad](#)

[CS-004 Confianza cero \(Zero Trust\)](#)

[CS-010 Higiene cibernética](#)

MÁS DE FUNDAMENTOS

[CS-001 Ciberseguridad](#)

[CS-002 La tríada CIA](#)

[CS-003 Defensa en profundidad](#)

[CS-004 Confianza cero \(Zero Trust\)](#)

[CS-005 Superficie de ataque](#)

[CS-006 Actores de amenaza](#)

Compartir

LinkedIn

Facebook

X

Correo