

CS-002 · Fundamentos

La tríada CIA

Confidencialidad, integridad y disponibilidad, los tres objetivos que sirve todo control de seguridad.

[Read this reference sheet in English](#)

[← CS-001](#)

Ficha 2 de 15

[CS-003 →](#)

■ Resumen ejecutivo

La tríada CIA describe los tres objetivos fundamentales de la seguridad de la información: mantener los datos confidenciales, preservar su integridad y asegurar su disponibilidad. Casi todo control de seguridad existe para proteger una o varias de estas tres propiedades. Es el modelo mental que usan los profesionales para razonar sobre qué están defendiendo en realidad.

■ Qué es

La tríada CIA es un modelo que divide la seguridad de la información en tres objetivos. La confidencialidad significa que solo las personas y los sistemas autorizados pueden ver los datos. La integridad significa que los datos son exactos y completos, y que no han sido alterados sin autorización, ya sea por un atacante o por accidente. La disponibilidad significa que los datos y los sistemas que los sirven están accesibles para los usuarios autorizados cuando se necesitan. Toda decisión de seguridad relevante se puede rastrear hasta uno o varios de estos objetivos, y por eso la tríada aparece en casi todos los marcos de seguridad y en casi todas las certificaciones.

■ Por qué importa

La tríada da a los equipos un lenguaje común para los compromisos. Cerrar un sistema con mucha dureza puede proteger la confidencialidad y dañar la disponibilidad si los usuarios legítimos no logran entrar. Apresurarse a restablecer la disponibilidad tras una caída puede socavar la integridad si eso implica recuperar desde datos no verificados. Entender qué propiedad protege un control, y cuál podría debilitar, permite tomar decisiones deliberadas en lugar de accidentales. Para cualquiera en un puesto de seguridad, riesgo, auditoría o gobernanza, saber asociar una amenaza o un control con la tríada es una expectativa básica.

■ Cómo funciona

En la práctica, los equipos eligen controles que refuerzan cada propiedad. La confidencialidad se apoya en el control de accesos, el cifrado y la clasificación de datos. La integridad se apoya en el hash, las firmas digitales, el control de versiones y la gestión de cambios. La disponibilidad se apoya en la redundancia, las copias de seguridad, la planificación de capacidad y una arquitectura resistente. Un mismo control suele servir a más de un objetivo a la vez, y un mismo incidente suele amenazar a más de uno. El ransomware, por ejemplo, ataca la disponibilidad al bloquear los archivos y cada vez más ataca la confidencialidad al robarlos antes. La tríada es una lista para razonar, no un conjunto de productos.

■ Diagrama de arquitectura

Confidencialidad: solo las personas correctas ven los datos

Integridad: los datos son exactos y no han sido alterados

Disponibilidad: los datos están ahí cuando se necesitan

Equilibrio: los controles deben servir a los tres sin romper ninguno

Cada vértice de la tríada es un objetivo distinto, y los controles se eligen para reforzar uno o varios sin perjudicar a los demás.

■ Flujo de trabajo

Clasificar el dato o el sistema y decidir cuál de los tres objetivos pesa más en su caso.



Identificar las amenazas que podrían romper la confidencialidad, la integridad o la disponibilidad.



Seleccionar controles que refuercen los objetivos en riesgo.



Comprobar que un control que protege un objetivo no debilite gravemente otro.



Probar los controles en condiciones realistas, incluida la falla.



Revisar el equilibrio de nuevo cada vez que el sistema o sus datos cambien.

■ Ataques frecuentes

- Robo de datos y escucha no autorizada, que rompen la confidencialidad
- Manipulación de registros, archivos o transacciones, que rompe la integridad
- Denegación de servicio y ransomware, que rompen la disponibilidad
- Ataques de intermediario, que pueden romper la confidencialidad y la integridad a la vez
- Abuso desde dentro, que socava en silencio cualquiera de los tres objetivos

■ Errores frecuentes

- Concentrarse solo en la confidencialidad y olvidar la integridad y la disponibilidad
- Añadir controles sin notar que perjudican la disponibilidad para usuarios legítimos
- Tratar las copias de seguridad como control de disponibilidad y no verificar nunca su integridad
- Suponer que el cifrado por sí solo protege datos que también corren riesgo de manipulación
- No clasificar los datos, de modo que todo activo se protege de la misma forma genérica

■ Buenas prácticas

- Clasificar los datos para que la protección corresponda a su sensibilidad e importancia
- Usar cifrado en tránsito y en reposo para proteger la confidencialidad

- Usar hash, firmas y control de cambios para proteger la integridad
- Construir redundancia y copias de seguridad probadas para proteger la disponibilidad
- Documentar a qué objetivo sirve cada control importante
- Revisar los compromisos cada vez que un control frene o bloquee de forma visible a los usuarios

■ Lista de verificación

- ✓ Esquema de clasificación de datos definido y aplicado a los activos clave
- ✓ Cifrado en tránsito y en reposo para los datos sensibles
- ✓ Verificaciones de integridad (hash o firmas) en archivos o registros críticos
- ✓ Redundancia o conmutación por falla en los sistemas que deben seguir disponibles
- ✓ Copias de seguridad probadas con una restauración limpia y verificada
- ✓ Revisiones de acceso que confirmen que solo los usuarios autorizados llegan a los datos

■ Herramientas recomendadas

Herramientas de cifrado (TLS, cifrado de disco y de archivos)

Protegen la confidencialidad de los datos en tránsito y en reposo

Hash y monitorización de integridad de archivos

Detectan cambios no autorizados para proteger la integridad

Sistemas de copia de seguridad y replicación

Sostienen la disponibilidad y la recuperación tras una pérdida o un ataque

Gestión de identidades y accesos (IAM)

Impone quién puede ver y modificar los datos

■ Normas del sector

ISO/IEC 27001

Enmarca la seguridad de la información en

NIST SP 800-53

Catálogo de controles cuyas salvaguardas

proteger la confidencialidad, la integridad y la disponibilidad

corresponden a los tres objetivos de la tríada

Marco de Ciberseguridad del NIST (CSF) 2.0

Organiza la protección, la detección y la recuperación que sirven a la tríada

■ Relevancia profesional

La tríada CIA es la base para analistas de SOC, ingenieros de seguridad, analistas de GRC, auditores y arquitectos. Quien entrevista la usa para comprobar si un candidato razona sobre seguridad en lugar de solo nombrar herramientas. Los profesionales de privacidad y de gobernanza de la inteligencia artificial, el público al que sirve GRC Careers, también se apoyan en ella para explicar por qué existe un control o un requisito determinado.

■ Preguntas de entrevista

- ¿Cuáles son las tres partes de la tríada CIA? Dé un control para cada una.
- Dé un ejemplo de un control que proteja la confidencialidad y pueda dañar la disponibilidad.
- ¿Qué parte de la tríada ataca el ransomware y cómo ha cambiado eso?
- ¿Cómo protegería la integridad de un registro financiero crítico?
- ¿Por qué en algunos sistemas la disponibilidad puede pesar más que la confidencialidad?

■ Certificaciones relacionadas

CompTIA Security+
(más profunda)

ISC2 Certified in Cybersecurity (CC)

ISC2 CISSP (para una cobertura

■ Para profundizar

- [Glosario del NIST: confidencialidad, integridad, disponibilidad \(en inglés\)](#)
- [Marco de Ciberseguridad del NIST 2.0 \(en inglés\)](#)
- [CISA: buenas prácticas de ciberseguridad \(en inglés\)](#)

Puntos clave

- La tríada CIA son los tres objetivos centrales de la seguridad: confidencialidad, integridad y disponibilidad.
- Casi todo control existe para proteger una o varias de estas propiedades.
- Proteger un objetivo puede debilitar otro, así que el equilibrio es una decisión deliberada.
- La tríada es una herramienta de razonamiento que asocia amenazas y controles con objetivos reales.
- Es un concepto básico que se espera en puestos de seguridad, GRC y gobernanza.

Preguntas frecuentes

► ¿La tríada CIA sigue vigente frente a las amenazas actuales?

► ¿Hay añadidos a la tríada CIA?

► ¿Cómo se relaciona la tríada con un marco como el CSF del NIST?

Carreras relacionadas

PUESTOS RELACIONADOS

Soc Analyst

Grc Analyst

Security Engineer

CERTIFICACIONES RELACIONADAS

CompTIA Security+

ISC2 Certified in Cybersecurity (CC)

ISC2 CISSP (para una cobertura más profunda)

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: **La tríada CIA**
- 3 Profundice: [Ciberseguridad](#)
- 4 Profundice: [Defensa en profundidad](#)
- 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-003 Defensa en profundidad](#)

[CS-009 Principios básicos de seguridad](#)

[CS-010 Higiene cibernética](#)

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

MÁS DE FUNDAMENTOS

[CS-001 Ciberseguridad](#)

[CS-003 Defensa en profundidad](#)

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

[CS-005 Superficie de ataque](#)

[CS-006 Actores de amenaza](#)

[CS-007 La cadena de ataque \(Cyber Kill Chain\)](#)

Compartir

LinkedIn

Facebook

X

Correo