

CS-004 · Fundamentos

Confianza cero (Zero Trust)

No confiar nunca por omisión, verificar siempre y conceder solo el acceso que hace falta en este momento.

[Read this reference sheet in English](#)

[← CS-003](#)

Ficha 4 de 15

[CS-005 →](#)

Resumen ejecutivo

La confianza cero es un modelo de seguridad que elimina la confianza automática basada en la ubicación en la red. Toda solicitud de acceso a un recurso se verifica con identidad, estado del dispositivo y contexto, y el acceso se concede de forma estrecha y solo durante el tiempo que haga falta. Sustituye la vieja idea de una red interna confiable protegida por un perímetro exterior duro.

Qué es

La confianza cero es una estrategia construida sobre una premisa simple: estar dentro de la red no lo vuelve confiable. En los diseños antiguos, una vez que un usuario o un dispositivo pasaba el firewall se le confiaba casi todo, lo que significaba que una sola brecha podía extenderse sin freno. La confianza cero trata cada solicitud como si viniera de una red no confiable. Cada decisión de acceso considera quién pregunta, en qué dispositivo está, si ese dispositivo está en buen estado y si la solicitud encaja con el comportamiento habitual. Después el acceso se concede con el alcance más pequeño posible y se vuelve a evaluar de forma continua. La publicación NIST SP 800-207 ofrece la descripción más citada de la arquitectura de confianza cero.

Por qué importa

El trabajo ya no ocurre de forma ordenada dentro de la red de una oficina. Los servicios en la nube, el trabajo remoto, los contratistas y los dispositivos móviles hacen que el perímetro sea poroso o inexistente. Los atacantes explotan la confianza implícita para moverse de forma lateral después de lograr un primer apoyo. La confianza cero ataca ese problema de frente: verifica cada paso y limita a qué puede llegar una cuenta o un dispositivo comprometido. Para las organizaciones, reduce el radio de impacto de una brecha. Para los profesionales, la confianza cero se ha vuelto una expectativa estándar en las conversaciones de arquitectura, ingeniería y gobernanza, y muchos programas del sector público ya exigen avanzar hacia ella.

■ Cómo funciona

En el centro de la confianza cero hay un punto de decisión de políticas que evalúa cada solicitud contra reglas y señales, y un punto de aplicación que ejecuta la decisión. Las señales incluyen la identidad verificada, el estado del dispositivo, la ubicación, la sensibilidad del recurso y el contexto de comportamiento. Una identidad fuerte con autenticación multifactor es la base, porque la identidad se convierte en el plano de control principal. La microsegmentación limita cómo se comunican los sistemas entre sí, para que una brecha en un área no se extienda. El acceso se concede con el mínimo privilegio y con límite de tiempo, y todo se registra para que las decisiones puedan vigilarse y mejorarse. La confianza cero es un recorrido que se aplica a identidad, dispositivos, redes, aplicaciones y datos, no un producto único que se instala.

■ Diagrama de arquitectura



Flujo de trabajo

Inventariar usuarios, dispositivos, aplicaciones y los datos que deben protegerse. →

Establecer una identidad fuerte con autenticación multifactor como plano de control. →

Definir políticas de acceso con el mínimo privilegio para cada recurso. →

Agregar señales de estado del dispositivo y de contexto a las decisiones de acceso. →

Segmentar redes y aplicaciones para limitar el movimiento lateral. →

Vigilar, registrar y afinar las políticas de forma continua según el comportamiento real.

Ataques frecuentes

- Movimiento lateral después de que un atacante logra un primer apoyo
- Credenciales robadas usadas para llegar a sistemas que esa cuenta no debería tocar
- Dispositivos comprometidos que se conectan a recursos sensibles
- Cuentas con permisos excesivos de las que se abusa para acceder a datos amplios
- Abuso desde dentro que se apoya en la confianza implícita de la red

Errores frecuentes

- Tratar la confianza cero como un producto que se compra y no como una estrategia
- Agregar verificación y dejar en pie un acceso permanente y amplio
- Ignorar el estado del dispositivo y apoyarse solo en la identidad
- Omitir la segmentación, de modo que una brecha todavía puede extenderse hacia dentro
- Desplegar controles estrictos sin registro, así que no hay cómo afinarlos ni diagnosticarlos

Buenas prácticas

- Hacer de la autenticación fuerte y resistente al phishing la base de todo
- Conceder el mínimo privilegio y preferir el acceso justo a tiempo y con límite de tiempo
- Incluir el estado del dispositivo y el contexto en cada decisión de acceso
- Usar microsegmentación para contener el movimiento lateral
- Registrar todas las decisiones de acceso y vigilar las anomalías
- Adoptar la confianza cero por etapas, empezando por los activos más sensibles

■ Lista de verificación

- ✓ MFA aplicada en todas partes, con métodos resistentes al phishing para el acceso de alto riesgo
- ✓ Acceso amplio permanente retirado a favor del mínimo privilegio
- ✓ Estado del dispositivo verificado antes de conceder acceso a recursos sensibles
- ✓ Segmentación de red y de aplicaciones que limite el movimiento lateral
- ✓ Decisiones de acceso registradas y revisadas
- ✓ Una hoja de ruta documentada que vaya de la confianza de perímetro a la confianza cero

■ Herramientas recomendadas

Proveedor de identidad con MFA y acceso condicional

Verifica la identidad y aplica la política en cada solicitud

Gestión de dispositivos y verificación de su estado

Confirma que un dispositivo está en buen estado antes de conceder acceso

Microsegmentación y perímetro definido por software

Limita qué sistemas pueden alcanzarse entre sí

SIEM y registro de accesos

Vigila y afina las decisiones de acceso con el tiempo

■ Normas del sector

NIST SP 800-207

Descripción fundacional de la arquitectura de confianza cero

Modelo de Madurez de Confianza Cero de CISA

Marco para medir el avance en cada pilar

Marco de Ciberseguridad del NIST (CSF) 2.0

Resultados de protección y detección que la confianza cero sostiene

Relevancia profesional

La confianza cero es un tema central para arquitectos de seguridad, ingenieros de seguridad y especialistas en identidad, y aparece de forma constante en las descripciones de puesto actuales. Los analistas de GRC, los auditores y los profesionales de gobernanza de la inteligencia artificial deben entenderla para evaluar madurez y cumplimiento, sobre todo donde los entornos públicos o regulados exigen avanzar hacia ella. Es uno de los conceptos de seguridad con más demanda hoy.

Preguntas de entrevista

- ¿Qué problema resuelve la confianza cero que un perímetro tradicional no resuelve?
- ¿Por qué se dice que la identidad es el plano de control en la confianza cero?
- ¿Qué es la microsegmentación y cómo limita a un atacante?
- ¿Cómo empezaría un despliegue de confianza cero en un entorno ya existente?
- ¿Qué señales además de la identidad deberían pesar en una decisión de acceso?

Certificaciones relacionadas

ISC2 CISSP

CompTIA Security+

ISACA CISM (para trayectorias de gobernanza)

Para profundizar

- [NIST SP 800-207, arquitectura de confianza cero \(en inglés\)](#)
- [Modelo de Madurez de Confianza Cero de CISA \(en inglés\)](#)

Puntos clave

- La confianza cero elimina la confianza automática basada en la ubicación en la red.
- Toda solicitud se verifica con identidad, estado del dispositivo y contexto.
- El acceso es de mínimo privilegio y, en lo posible, con límite de tiempo y vigilado.
- La microsegmentación limita hasta dónde puede extenderse una brecha.
- Es una estrategia y un recorrido, no un producto único que se instala.

Preguntas frecuentes

► **¿Confianza cero significa que no se confía en nadie?**

► **¿La confianza cero es un producto que se compra?**

► **¿En qué se diferencia de la defensa en profundidad?**

Carreras relacionadas

PUESTOS RELACIONADOS

[Security Engineer](#)

[Security Architect](#)

[Grc Analyst](#)

CERTIFICACIONES RELACIONADAS

[ISC2 CISSP](#)

[CompTIA Security+](#)

[ISACA CISM \(para trayectorias de gobernanza\)](#)

VACANTES ACTUALES

Las vacantes aparecen en la versión web. Vea la bolsa de empleo para los puestos vigentes de GRC y seguridad.

GUÍAS Y SALARIOS

[Vacantes en español](#)

[Glosario GRC](#)

[Empezar en privacidad](#)

[Cumplimiento por país](#)

[Ver todas las vacantes](#)

RUTA DE APRENDIZAJE SUGERIDA

- 1 Afiance las bases con [CS-001 Ciberseguridad](#)
- 2 Estudie esta ficha: **Confianza cero (Zero Trust)**
- 3 Profundice: [Ciberseguridad](#)
- 4 Profundice: [Defensa en profundidad](#)
- 5 Valídelo: trabaje hacia **ISC2 CISSP**
- 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-005 Superficie de ataque](#)

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

[CS-002 La tríada CIA](#)

MÁS DE FUNDAMENTOS

[CS-001 Ciberseguridad](#)

[CS-002 La tríada CIA](#)

[CS-003 Defensa en profundidad](#)

[CS-005 Superficie de ataque](#)

[CS-006 Actores de amenaza](#)

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

[← CS-003](#)

Ficha 4 de 15

[CS-005 →](#)

Compartir

[LinkedIn](#)

[Facebook](#)

[X](#)

[Correo](#)