UNMSM
Fundación
SAN MARCOS
Por el desarrollo de la Ciencia y la Cultura

DIPLOMADO DE ESPECIALIZACIÓN

GESTIÓN DE LA CIBERSEGURIDAD Y PRIVACIDAD

RESUMEN EJECUTIVO

Zero Trust Architecture

JULIO – OCTUBRE 2026

CENCAEP
CAPACITA

RESUMEN EJECUTIVO

Arquitectura Zero Trust — NIST SP 800-207

Nota de traducción: *Esta es una traducción/síntesis para fines académicos. La edición en inglés es la edición auténtica.*

1. Contexto y fundamento de Zero Trust

La evolución tecnológica ha fragmentado el perímetro corporativo. Una organización puede operar redes internas, oficinas remotas, trabajadores móviles, servicios cloud y dispositivos que no administra directamente. En este escenario ya no existe un único límite físico o lógico que concentre toda la protección. NIST advierte además que el modelo perimetral presenta una debilidad crítica: una vez superada la barrera externa, el movimiento lateral dentro del entorno puede quedar insuficientemente restringido.

Zero Trust responde a esta realidad adoptando una perspectiva de "entorno potencialmente comprometido". El punto de partida no es determinar qué parte de la red es confiable, sino qué recurso se intenta utilizar, quién o qué lo solicita, desde qué activo, bajo qué condiciones y con qué nivel de riesgo.

De perímetro a recursos

En el modelo tradicional, la ubicación de red funciona como una señal importante de confianza. En ZTA, la ubicación deja de ser una condición suficiente. Un equipo dentro de la red corporativa no recibe privilegios automáticos; de igual manera, un usuario remoto no queda excluido por el simple hecho de encontrarse fuera del perímetro. La decisión se desplaza hacia el nivel de la transacción y del recurso.

Qué protege Zero Trust

- Datos e información sensible.
- Aplicaciones y servicios empresariales.
- Dispositivos físicos y virtuales.
- Infraestructura de cómputo y componentes de red.
- Flujos de trabajo y procesos de negocio.
- Identidades humanas y entidades no humanas, como aplicaciones, servicios y procesos automatizados.

NIST define ZTA como el plan de ciberseguridad empresarial que utiliza conceptos Zero Trust y establece relaciones entre componentes, flujos de trabajo y políticas de acceso. Por tanto, adoptar ZTA implica tanto decisiones tecnológicas como cambios en políticas, procesos operativos y gestión del riesgo.

2. Principios fundamentales de Zero Trust

NIST formula siete principios básicos que constituyen la referencia conceptual de una ZTA. No se trata de una lista de productos, sino de objetivos de diseño que pueden implementarse mediante distintas tecnologías.

a) Todo dato y servicio es un recurso

Los recursos comprenden sistemas, aplicaciones, dispositivos, servicios SaaS, IoT, almacenamiento y otros componentes que puedan ser objeto de acceso. Incluso dispositivos personales pueden considerarse recursos cuando intervienen en el acceso a recursos corporativos.

b) Toda comunicación debe protegerse

La ubicación de red no determina confianza. Las comunicaciones deben utilizar el nivel de seguridad disponible para proteger confidencialidad, integridad y autenticidad del origen.

c) Acceso por sesión y mínimo privilegio

Cada recurso debe autorizarse de manera específica. Haber sido autenticado para un recurso no significa estar autorizado para otro. Los permisos deben limitarse a lo estrictamente necesario para realizar la actividad.

d) Políticas dinámicas

La decisión debe considerar atributos observables de identidad, aplicación, dispositivo y entorno. Entre los factores posibles se encuentran versión del sistema operativo, software instalado, ubicación, fecha y hora, comportamiento observado y situación de seguridad del activo.

e) Evaluación permanente del estado de los activos

Ningún activo es confiable por naturaleza. La organización debe conocer su postura de seguridad, vulnerabilidades, configuración y nivel de actualización, y utilizar esa información para decidir si permite, restringe o deniega el acceso.

f) Autenticación y autorización dinámicas

La evaluación no termina cuando comienza una sesión. Puede ser necesario volver a autenticar o autorizar ante determinados eventos, cambios de contexto, anomalías o solicitudes de nuevos recursos. NIST contempla el uso de MFA como parte de esta capacidad.

g) Recopilar información para mejorar la seguridad

Registros, telemetría, estado de activos, tráfico y solicitudes de acceso deben convertirse en información útil para ajustar políticas y mejorar las decisiones.

3. Modelo de acceso y decisión de políticas

La arquitectura abstracta de NIST se apoya en dos funciones esenciales: el Policy Decision Point (PDP), encargado de decidir, y el Policy Enforcement Point (PEP), encargado de hacer cumplir la decisión. El PDP se divide conceptualmente en Policy Engine (PE) y Policy Administrator (PA).

Policy Engine (PE)

Es el componente que determina si una solicitud debe aprobarse, rechazarse o revocarse. Utiliza las políticas empresariales y señales procedentes de sistemas de gestión de activos, inteligencia de amenazas, registros y otras fuentes. El PE registra la decisión.

Policy Administrator (PA)

Ejecuta la decisión del PE. Puede establecer o cerrar el canal de comunicación, generar credenciales o elementos específicos de la sesión y ordenar al PEP que habilite, suspenda o termine una conexión.

Policy Enforcement Point (PEP)

Es el punto de control que habilita, supervisa y termina la comunicación entre el solicitante y el recurso. Puede dividirse entre un agente en el dispositivo y un gateway próximo al recurso, o implementarse mediante un portal que actúe como puerta de acceso.

Fuentes de información

- Sistemas de diagnóstico y mitigación de activos: postura, parches, software y vulnerabilidades.

- Sistemas de cumplimiento: requisitos regulatorios y políticas internas.
- Inteligencia de amenazas: malware, vulnerabilidades, indicadores y ataques conocidos.
- Registros de red y sistemas: actividad y eventos de seguridad.
- Políticas de acceso: reglas, atributos, privilegios y necesidades del negocio.
- PKI y gestión de identidades: certificados, cuentas, roles y atributos.
- SIEM: agregación y análisis de información relevante para la seguridad.

La arquitectura separa conceptualmente el plano de control, que establece y administra las comunicaciones, del plano de datos, que transporta el tráfico de las aplicaciones y servicios. Esta separación refuerza el control y permite gestionar los canales de comunicación de acuerdo con las decisiones de política.

4. Algoritmo de confianza y decisión basada en riesgo

En ZTA, el algoritmo de confianza es el mecanismo mediante el cual el Policy Engine transforma múltiples señales en una decisión de acceso. NIST no prescribe una fórmula única: cada organización debe determinar qué factores son relevantes y cómo ponderarlos de acuerdo con sus riesgos y procesos.

Principales entradas

- Solicitud de acceso: recurso solicitado y características del solicitante.
- Identidad: cuenta, proceso, atributos y resultados de autenticación.
- Estado del activo: sistema operativo, software, integridad, ubicación y nivel de parcheo.
- Requisitos del recurso: sensibilidad, MFA, restricciones geográficas y otras condiciones.
- Inteligencia de amenazas: indicadores de actividad maliciosa y vulnerabilidades.
- Historial de comportamiento: patrones previos del usuario, aplicación o dispositivo.

Dos formas de evaluar

Un algoritmo basado en criterios exige que se cumpla un conjunto de condiciones antes de autorizar. Un algoritmo basado en puntuación calcula un nivel de confianza a partir de distintas señales y pesos; si se supera el umbral establecido, se concede el acceso. En ambos casos, la decisión debe responder a la sensibilidad del recurso y al riesgo aceptable.

Decisión singular o contextual

Una evaluación singular analiza cada solicitud de forma aislada. Es más sencilla y puede ser rápida, pero puede no detectar una actividad maliciosa que permanezca dentro de los permisos habituales. Una evaluación contextual incorpora el comportamiento reciente y permite detectar desviaciones, por ejemplo, un volumen anormal de consultas, acceso en horarios inusuales o cambios relevantes de ubicación.

NIST señala que el enfoque contextual ofrece mayor capacidad de adaptación, pero exige conservar información histórica y equilibrar seguridad, usabilidad y coste. Durante una implantación inicial es normal requerir una etapa de ajuste de criterios y umbrales para reducir falsos rechazos o autorizaciones incorrectas.

5. Enfoques y modelos de implementación

Gobernanza de identidad reforzada

El acceso se estructura principalmente alrededor de la identidad y sus atributos. La postura del dispositivo y factores ambientales complementan la decisión. Este enfoque resulta especialmente útil en entornos con servicios cloud, usuarios externos o dispositivos diversos, donde el control directo de la infraestructura puede ser limitado.

Microsegmentación

Los recursos se colocan en segmentos específicos protegidos por gateways, firewalls de nueva generación, switches inteligentes, routers o agentes en los hosts. El PEP controla el acceso a cada recurso o pequeño conjunto de recursos. La ventaja principal es

reducir la superficie de movimiento lateral; el reto está en administrar dinámicamente numerosos puntos de control.

Infraestructura de red y perímetros definidos por software

La red puede utilizarse para construir canales de acceso dinámicos mediante conceptos como Software Defined Perimeter, Software Defined Networking o redes basadas en intención. El Policy Administrator configura la infraestructura según las decisiones del Policy Engine.

Modelos de despliegue

- Agente de dispositivo/gateway: un agente en el equipo solicita acceso y un gateway protege el recurso.
- Gateway de enclave: un punto de control protege un conjunto de recursos, útil para aplicaciones heredadas.
- Portal de recursos: un gateway único controla solicitudes y facilita escenarios BYOD o colaboración entre organizaciones.
- Sandboxing de aplicaciones: aplicaciones autorizadas se ejecutan de forma compartimentada para reducir el impacto de un host potencialmente comprometido.

NIST indica que una organización puede combinar modelos y enfoques diferentes según el proceso de negocio. No existe una arquitectura universal; la selección debe responder a activos, riesgos, capacidades actuales y restricciones operativas.

6. Escenarios de aplicación

La ZTA resulta particularmente relevante en organizaciones distribuidas. El documento analiza escenarios que reflejan problemas frecuentes de seguridad empresarial.

Trabajo remoto y sedes distribuidas

Los usuarios y dispositivos remotos no deben asumir que su red local es segura. La comunicación debe autenticarse, autorizarse y protegerse. El acceso a recursos cloud no debería depender necesariamente de regresar primero a la infraestructura corporativa.

Entornos multicloud

Cuando aplicaciones y datos se distribuyen entre diferentes proveedores cloud, el perímetro corporativo deja de ser una frontera

útil. Zero Trust permite aplicar políticas centradas en identidades, recursos, cargas de trabajo y contexto.

Contratistas y no empleados

Los proveedores, contratistas y otros colaboradores pueden requerir acceso a recursos corporativos desde dispositivos que la organización no controla completamente. El modelo debe diferenciar los niveles de confianza y limitar el acceso al mínimo necesario.

Colaboración entre organizaciones

La cooperación interempresarial requiere mecanismos que permitan compartir recursos sin extender confianza generalizada. La identidad federada y las políticas específicas de acceso adquieren especial importancia.

Servicios públicos y orientados al cliente

NIST distingue los procesos internos de aquellos destinados al público anónimo. La organización no puede imponer sus políticas internas a cualquier usuario de Internet, pero sí puede aplicar controles Zero Trust a clientes registrados u otros actores con una relación definida.

Criterio profesional

La utilidad de ZTA no consiste en aplicar la misma tecnología a todos los escenarios. El principio rector es conservar una decisión de acceso explícita y proporcional al riesgo, incluso cuando cambian la ubicación, el dispositivo, el proveedor de infraestructura o la naturaleza del colaborador.

7. Amenazas y limitaciones de una ZTA

Zero Trust reduce determinadas formas de exposición, pero no elimina las amenazas. La propia arquitectura crea componentes críticos que deben protegerse y dimensionarse adecuadamente.

Manipulación del proceso de decisión

Si un atacante compromete el Policy Engine, Policy Administrator, PEP o las fuentes de información, podría influir en las decisiones de acceso. Por ello, los componentes que determinan confianza se convierten en activos de alta criticidad.

Denegación de servicio y pérdida de conectividad

PE, PA y PEP son esenciales para el funcionamiento de los procesos. Una interrupción puede impedir accesos legítimos. La arquitectura debe prever capacidad, disponibilidad y escalabilidad, especialmente en portales y servicios centralizados.

Credenciales robadas y amenazas internas

Una identidad válida no debe considerarse suficiente. El análisis del dispositivo, contexto y comportamiento ayuda a detectar usos anómalos de credenciales comprometidas o acciones de insiders.

Visibilidad insuficiente

Un modelo de confianza requiere datos fiables. Si la organización no conoce el estado de sus activos, aplicaciones y comunicaciones, la calidad de las decisiones disminuirá.

Dependencia de datos y formatos propietarios

El documento identifica riesgos asociados a depender de soluciones cerradas o formatos que dificulten la interoperabilidad. La ausencia de interfaces comunes puede complicar la integración de componentes.

Entidades no humanas

Las aplicaciones, servicios y procesos automatizados también solicitan acceso. Su identidad, credenciales y privilegios deben gestionarse con el mismo principio de mínimo privilegio.

Conclusión operativa: ZTA no debe confundirse con “seguridad automática”. Requiere controles de disponibilidad, gestión de identidades, monitoreo, protección de los componentes de decisión y procedimientos de respuesta.

8. Requisitos tecnológicos y operativos

Una arquitectura Zero Trust depende de capacidades de base. NIST señala que la organización debe disponer de información suficiente para distinguir activos, evaluar su postura y aplicar políticas de acceso.

Identidad y credenciales

- Gestión de identidades y atributos.
- Autenticación sólida y, cuando corresponda, MFA.
- Credenciales y certificados gestionados de forma segura.
- Capacidad para autenticar usuarios y entidades no humanas.

Gestión de activos

La organización debe conocer qué dispositivos y cargas de trabajo existen, quién los administra, qué software ejecutan, cuál es su nivel de parcheo y cuál es su postura de seguridad.

Telemetría y registros

La ZTA necesita datos de actividad de red, sistemas, aplicaciones y accesos. La información debe poder analizarse en tiempo real o casi real para alimentar decisiones y detectar anomalías.

Protección de comunicaciones

La arquitectura debe asegurar confidencialidad, integridad y autenticación del origen. Las comunicaciones no deben confiarse únicamente a la ubicación de red.

PEP como punto obligatorio de acceso

Los recursos empresariales no deberían aceptar conexiones arbitrarias desde Internet. El acceso debe pasar por los mecanismos de aplicación de políticas previstos por la arquitectura.

Escalabilidad y resiliencia

La infraestructura que soporta las decisiones de acceso debe dimensionarse para las cargas esperadas y poder escalar. Un diseño que protege muy bien pero se convierte en un cuello de botella puede afectar directamente la continuidad del negocio.

En términos de gobierno, estas capacidades deben relacionarse con políticas, procesos de negocio, gestión de riesgos, administración de cambios y métricas. La tecnología es un habilitador; la decisión sobre qué proteger y con qué nivel de control proviene del riesgo y de la misión de la organización.

9. Integración con la gestión de ciberseguridad

NIST presenta Zero Trust como un enfoque compatible con otros programas y marcos de seguridad. No se propone sustituir de manera indiscriminada las capacidades existentes, sino utilizar los principios Zero Trust para reforzar la protección de recursos y decisiones de acceso.

Gestión de riesgos

La migración debe partir de una comprensión de los procesos críticos, los activos involucrados y las consecuencias de un acceso indebido. Las decisiones de arquitectura deben reflejar el nivel de riesgo aceptable.

Gestión de identidades y acceso

La identidad es una pieza central, pero no suficiente. ZTA combina identidad con postura del dispositivo, contexto, políticas y comportamiento.

Monitoreo continuo

La supervisión no debe limitarse al momento del inicio de sesión. Los eventos posteriores pueden modificar el nivel de confianza y activar nuevas verificaciones o el cierre de la sesión.

Protección de datos

La granularidad de las políticas permite asociar privilegios a recursos específicos y aplicar controles diferenciados según sensibilidad. El objetivo es reducir exposición y movimiento lateral.

Privacidad y uso responsable de datos

El modelo puede requerir recolectar información contextual y de comportamiento. Esa capacidad debe administrarse conforme a las obligaciones legales, políticas internas y necesidades legítimas de seguridad.

Continuidad y resiliencia

Como los componentes de decisión pasan a ser críticos para el negocio, deben contemplarse disponibilidad, redundancia, capacidad de recuperación y mecanismos para evitar que una falla de control paralice procesos esenciales.

Desde la perspectiva de un profesional de ciberseguridad, el valor de ZTA aumenta cuando se integra en un programa de gestión y no se trata como un proyecto aislado de infraestructura.

10. Ruta de migración hacia Zero Trust

NIST enfatiza que la transición a ZTA es un proceso. No consiste en reemplazar de una vez la infraestructura existente. La mayoría de las organizaciones avanzará mediante una arquitectura híbrida, combinando elementos Zero Trust con controles perimetrales durante un período de modernización.

Paso 1 — Identificar actores

Determinar quiénes y qué entidades solicitan acceso: empleados, contratistas, aplicaciones, servicios y otros sujetos. Deben conocerse sus identidades y atributos relevantes.

Paso 2 — Identificar activos

Construir una visión de los recursos empresariales: datos, aplicaciones, dispositivos, servicios, infraestructura y cargas de trabajo. Sin inventario no existe una política de acceso confiable.

Paso 3 — Identificar procesos y riesgos

Relacionar actores y activos con procesos de negocio. Determinar qué puede ocurrir si un recurso es comprometido, qué accesos son indispensables y qué nivel de protección requiere cada proceso.

Paso 4 — Formular políticas

Definir las condiciones de acceso por recurso: identidad, dispositivo, nivel de autenticación, sensibilidad, ubicación, horario, comportamiento y otros factores relevantes.

Paso 5 — Seleccionar soluciones

Elegir las capacidades tecnológicas que permitan ejecutar las políticas. La selección debe partir de los requisitos y no de una herramienta previamente elegida.

Paso 6 — Desplegar y monitorear

Comenzar con un caso de uso controlado, medir resultados, ajustar políticas y observar efectos sobre seguridad, disponibilidad y experiencia de usuario.

Paso 7 — Expandir

Una vez estabilizado el primer caso, ampliar el modelo a otros recursos y procesos, reutilizando capacidades y lecciones aprendidas.

La secuencia muestra una idea fundamental: el punto de partida no es comprar tecnología Zero Trust; es entender qué se protege, quién necesita acceder, bajo qué condiciones y qué riesgo se acepta.

11. Consideraciones para un programa de implementación

Priorizar por riesgo

Una organización no necesita transformar todo su entorno al mismo tiempo. Es más efectivo comenzar con activos críticos, procesos sensibles, accesos privilegiados, aplicaciones expuestas o escenarios donde el movimiento lateral tenga consecuencias significativas.

Establecer una línea base

Antes de aplicar controles dinámicos, conviene conocer el estado actual: inventario de activos, identidades, privilegios, flujos de datos, dependencias, vulnerabilidades y mecanismos de monitoreo.

Medir resultados

- Reducción de privilegios innecesarios.
- Disminución de rutas de movimiento lateral.
- Porcentaje de activos con postura conocida.
- Cobertura de MFA y autenticación fuerte.
- Porcentaje de recursos protegidos por PEP.
- Tiempo de detección y respuesta ante cambios de comportamiento.
- Número de accesos denegados legítimos y falsos positivos durante el ajuste.

Evitar errores de diseño

- No asumir que la red interna es confiable.
- No convertir la autenticación inicial en un permiso general.
- No diseñar políticas sin inventario de activos y procesos.
- No centralizar decisiones sin considerar disponibilidad y escalabilidad.
- No recolectar telemetría sin definir cómo será utilizada.
- No tratar Zero Trust como una sustitución inmediata de todos los controles perimetrales.

Gobernanza

La responsabilidad debe distribuirse entre seguridad, infraestructura, identidad, propietarios de datos, responsables de procesos y áreas de cumplimiento. Las políticas de acceso deben tener un propietario, criterios de revisión y mecanismos para modificarlas cuando cambien los riesgos o los procesos.

El enfoque de NIST es deliberadamente tecnológico-agnóstico: distintas tecnologías pueden cumplir la misma función lógica. Esto permite adaptar la arquitectura al tamaño, madurez y restricciones de cada organización.

12. Conclusiones para el profesional de ciberseguridad

La Arquitectura Zero Trust representa un cambio de paradigma: la pregunta deja de ser “¿está dentro de la red?” y pasa a ser “¿esta solicitud concreta debe permitirse, para este recurso, en estas condiciones y con este nivel de riesgo?”. Esta diferencia es esencial para comprender por qué el modelo resulta adecuado para organizaciones con usuarios remotos, cloud, BYOD, servicios distribuidos y colaboración entre entidades.

El núcleo de la ZTA es la decisión de acceso. Identidad, postura del dispositivo, contexto, inteligencia de amenazas, políticas y comportamiento proporcionan las señales; el Policy Engine evalúa; el Policy Administrator ejecuta; y el Policy Enforcement Point hace cumplir la decisión. El proceso puede repetirse durante la sesión y cambiar cuando cambian las condiciones.

La arquitectura también exige reconocer sus propios puntos críticos. PE, PA, PEP, sistemas de identidad, telemetría y fuentes de información deben protegerse y dimensionarse. Un atacante que comprometa la capacidad de decisión podría obtener un impacto significativo; una interrupción de estos componentes puede afectar la continuidad del negocio.

Conclusiones clave

- Zero Trust es un enfoque de arquitectura y gestión del riesgo, no un producto.
- La confianza implícita debe reducirse y sustituirse por decisiones explícitas y verificables.
- El mínimo privilegio debe aplicarse por recurso y por sesión.
- La identidad debe combinarse con la postura del dispositivo y el contexto.
- El monitoreo continuo es parte del modelo, no una actividad posterior.
- La microsegmentación, la gobernanza de identidad y los perímetros definidos por software son medios posibles, no fines en sí mismos.
- La migración debe ser incremental, priorizada por riesgos y casos de uso.
- Los entornos híbridos serán una realidad durante la transición.
- El éxito depende tanto de procesos, políticas y gobierno como de tecnología.