# Informe técnico del modelo de madurez de Zero Trust de la CISA



DOCUMENTO TÉCNICO

## Resumen ejecutivo

En el panorama de ciberseguridad en rápida evolución actual, las organizaciones enfrentan una gama cada vez mayor de amenazas sofisticadas. Los modelos de seguridad tradicionales basados en el perímetro son cada vez más ineficaces para proteger las redes, a medida que la transformación digital se acelera y trabajar en todas partes se convierte en la norma. La ciberseguridad debe evolucionar para proteger los datos y los sistemas independientemente de dónde se encuentren los usuarios o los dispositivos. En respuesta a estos desafíos, la Agencia de ciberseguridad y seguridad de las infraestructuras (CISA) ha desarrollado un modelo de madurez Zero Trust para guiar a las organizaciones en la adopción e implementación eficaz de los principios Zero Trust.

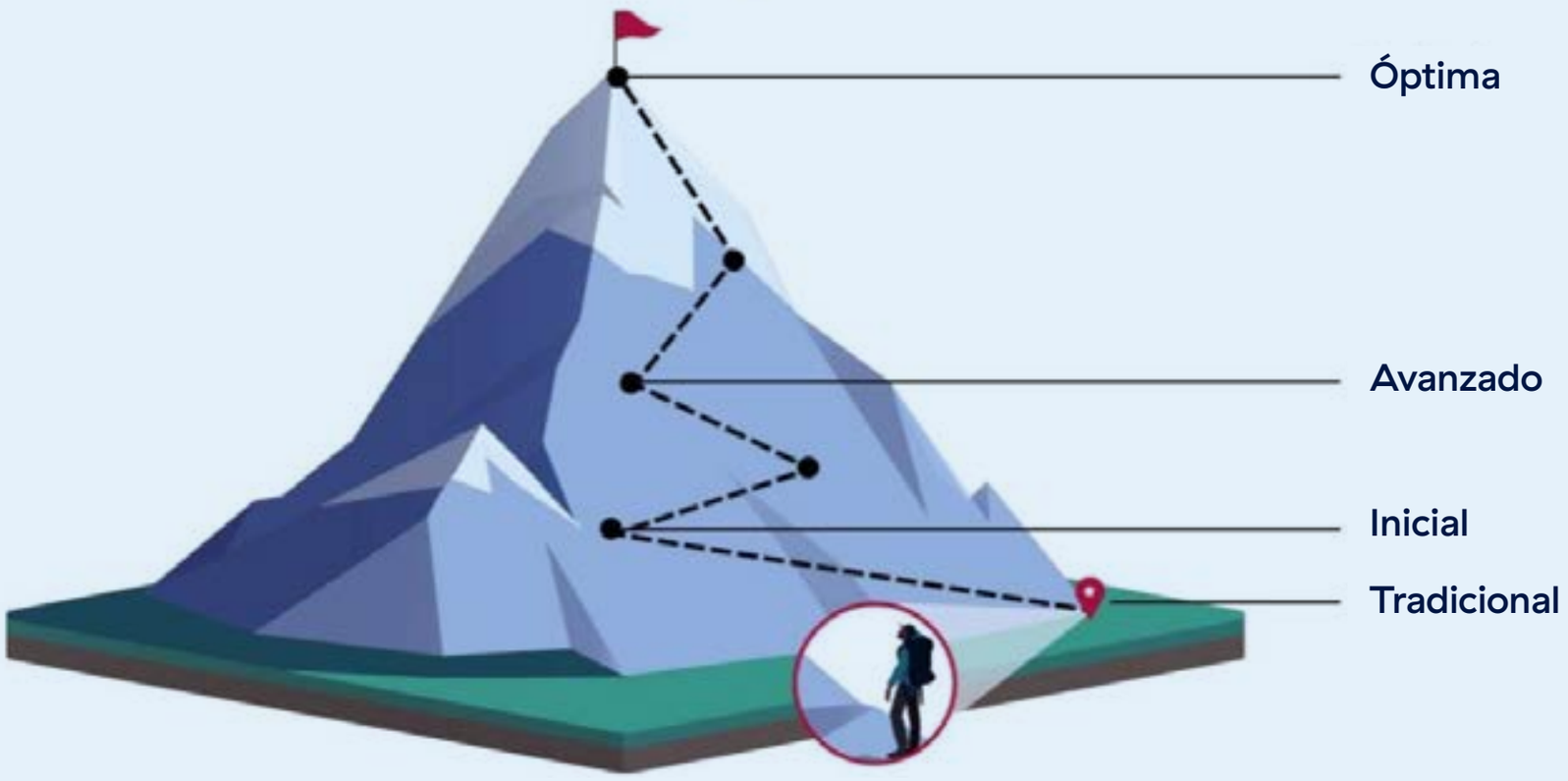
## ¿Qué es la confianza cero?

Zero Trust es un modelo de seguridad que opera bajo el supuesto de que las amenazas pueden ser internas o externas y, por lo tanto, no se debe confiar en ningún usuario o dispositivo de forma predeterminada. Cada solicitud de acceso, ya sea desde dentro o fuera de la red, se autentica rigurosamente, se autoriza y se supervisa continuamente. El marco de Zero Trust se centra en garantizar que la seguridad se mantenga en toda la infraestructura de una organización, con un gran énfasis en la identidad, la gestión de acceso y la supervisión en tiempo real.

## ¿Qué es el modelo de madurez de Zero Trust de la CISA?

El modelo de madurez de Zero Trust de la CISA proporciona a las organizaciones un marco para adoptar y madurar progresivamente los principios de Zero Trust. Este modelo describe un enfoque gradual para implementar Zero Trust en toda la organización, desde la concientización y la planificación iniciales hasta operaciones de seguridad totalmente maduras e integradas. Proporciona un método estructurado para comprender dónde se encuentra una organización en su camino hacia Zero Trust y qué pasos debe tomar a continuación para mejorar la seguridad.

## El camino hacia la madurez de Zero Trust




**Fuente: CISA**

El modelo de la CISA divide Zero Trust en varias áreas clave, que incluyen la gestión de identidad y acceso, la seguridad de dispositivos, redes, datos y aplicaciones, y la visibilidad y los análisis. El modelo de madurez ayuda a las organizaciones a evaluar sus capacidades actuales en cada una de estas áreas y definir un camino claro para fortalecer su postura de seguridad. Las organizaciones se evalúan en función de cuatro etapas de madurez (tradicional, inicial, avanzada y óptima), y cada etapa requiere un mayor nivel de protección, con un crecimiento exponencial de esfuerzos y beneficios.

El modelo de madurez de Zero Trust de la CISA se utiliza cada vez más como referencia global para la implementación de Zero Trust. Los gobiernos internacionales, incluidos los del Reino Unido y Australia, han alineado sus estrategias de ciberseguridad con el modelo de madurez, reconociendo su enfoque estructurado para avanzar en las capacidades de Zero Trust. Más allá de los gobiernos, la Cloud Security Alliance también ha alineado su Centro de avance de Zero Trust al modelo de madurez, reforzando aún más su papel como marco común para las organizaciones de todo el mundo. A medida que crece la adopción de Zero Trust, el modelo de madurez proporciona un lenguaje compartido y una hoja de ruta de madurez, que ayuda a las entidades del sector público y privado a evaluar su progreso y perfeccionar sus estrategias de seguridad.

## COMPONENTES CLAVE DEL MODELO

1. **Gestión de identidad y acceso (IAM):** establece mecanismos de autenticación potentes, como la autenticación multifactor (MFA), para verificar la identidad de los usuarios antes de concederles acceso.

2. **Seguridad del dispositivo:** garantiza que los dispositivos sean seguros, estén administrados y cumplan con las políticas de seguridad antes de acceder a los recursos de la organización.

3. **Seguridad de la red:** implementa segmentación y supervisión para restringir el movimiento lateral y detectar actividades sospechosas dentro de la red.

4. **Seguridad de datos:** protege los datos confidenciales aplicando cifrado, controles de acceso estrictos y supervisión del uso de los datos.

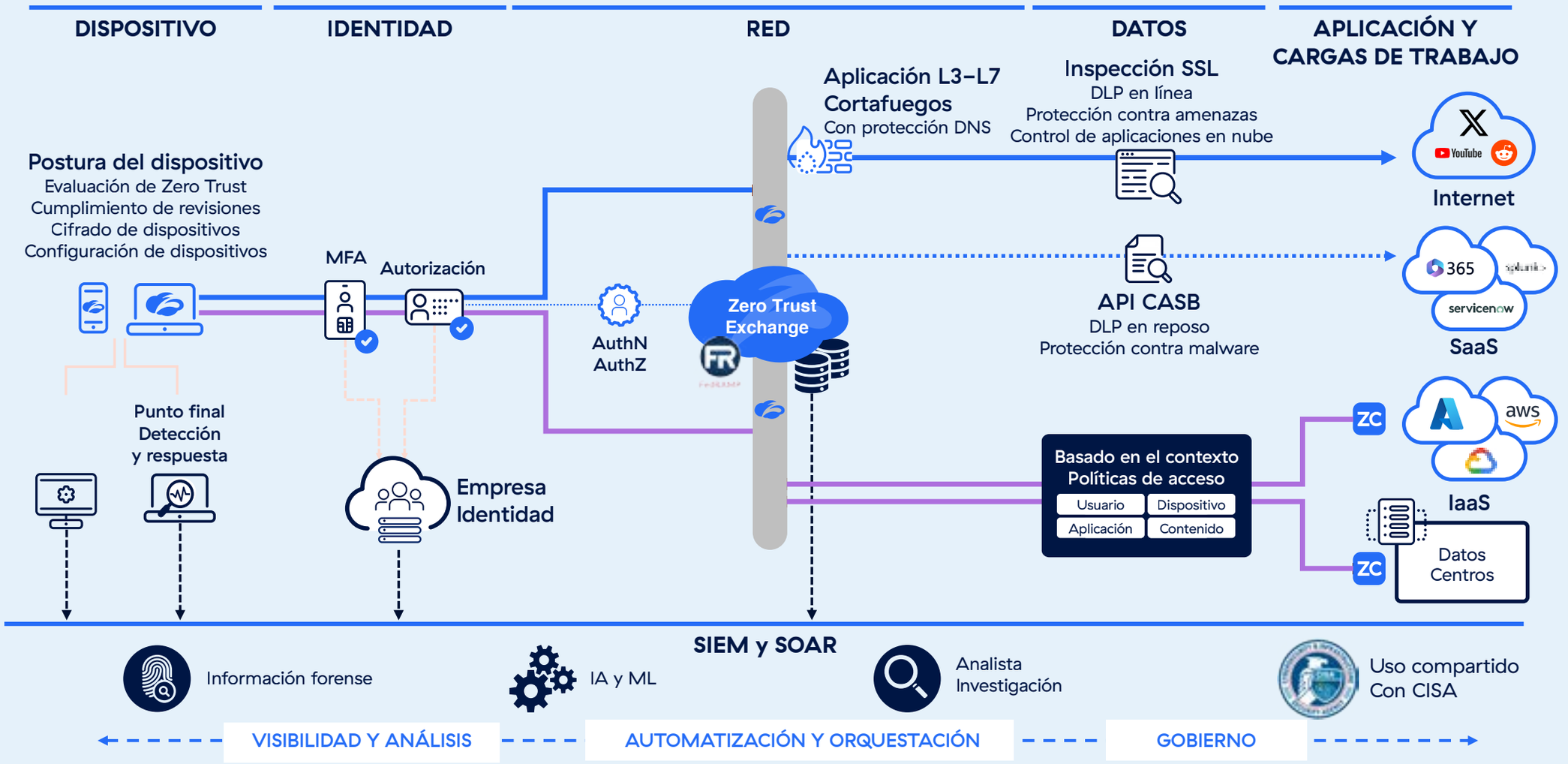
5. **Seguridad de las aplicaciones:** garantiza que las aplicaciones sean seguras mediante la aplicación de prácticas de desarrollo seguro, la supervisión continua y la gestión de vulnerabilidades.

6. **Visibilidad y análisis:** mejora la conciencia situacional mediante la supervisión continua de todo el tráfico y los eventos, identificando comportamientos anómalos y proporcionando alertas en tiempo real.

7. **Automatización y orquestación:** integra y automatiza sistemas para mejorar la eficacia y la eficiencia de los sistemas cibernéticos.

8. **Gobernanza:** establece políticas, procedimientos y mecanismos de supervisión para garantizar su implementación efectiva.

# Modelo de madurez Zero Trust 2.0




## Implementación del modelo de madurez de Zero Trust de la CISA con Zscaler

La implementación de Zscaler ZTE mejora de inmediato su postura de seguridad al pasar de la seguridad tradicional basada en el perímetro a una defensa más integral y en capas. Al verificar continuamente usuarios, dispositivos y datos, las organizaciones pueden reducir el riesgo de infracciones de datos, amenazas internas y ataques externos. Este enfoque minimiza la superficie de ataque y evita el movimiento lateral de los atacantes.  Zscaler también ayuda a las organizaciones a avanzar en la adopción del modelo de madurez de Zero Trust de la CISA, ofreciendo productos y funcionalidades avanzadas que respaldan áreas clave como la gestión de identidades y accesos, la seguridad de dispositivos, redes, datos y aplicaciones, además de proporcionar visibilidad y análisis.

### IDENTIDAD

- **Acceso con privilegios mínimos:** Zscaler minimiza las cuentas con permisos excesivos al aplicar controles de acceso granulares basados en roles (RBAC) y políticas contextuales (por ejemplo, ubicación del usuario, postura del dispositivo).

- **Inicio de sesión único (SSO) y autenticación multifactor (MFA):** las políticas Zero Trust se refuerzan con integración SSO/MFA, garantizando una autenticación potente y reduciendo el riesgo de comprometer las credenciales.

- **Supervisión continua de usuarios:** ZTE garantiza que los usuarios estén autenticados continuamente, y que su comportamiento sea supervisado para mitigar el riesgo.

- **Integración con proveedores de identidad (IdP):** Zscaler se integra perfectamente con proveedores de identidad líderes como Okta, Microsoft Azure AD y Ping Identity para implementar políticas potentes de autenticación y autorización de usuarios.

## DISPOSITIVOS

- **Verificaciones de postura del dispositivo:** Zscaler utiliza integraciones con herramientas de detección y respuesta de puntos finales (EDR) para realizar verificaciones de postura y garantizar que solo los dispositivos seguros y administrados puedan acceder a recursos confidenciales.

- **Cumplimiento basado en agentes:** el agente de software ligero Zscaler Client Connector (ZCC) de Zscaler garantiza que todo el tráfico del usuario se enrute a través de la nube de seguridad de Zscaler, lo que garantiza una visibilidad y un cumplimiento constante de las políticas de seguridad.

- **Zero Trust para IoT/dispositivos no administrados:** las soluciones Zscaler incluyen capacidades para controlar el acceso de dispositivos no administrados, incluidos los dispositivos IoT, mediante políticas de comportamiento y controles de acceso granulares.

## RED

- **Acceso a la red Zero Trust (ZTNA):** Zscaler Private Access (ZPA) reemplaza a las VPN tradicionales con ZTNA. Los usuarios reciben acceso con privilegios mínimos a aplicaciones específicas, no a toda la red.

- **Secure Access Service Edge (SASE):** Zscaler cumple con los requisitos de la arquitectura SASE al brindar servicios de seguridad escalables, como Secure Web Gateways (SWG) y Cloud Firewall, en entornos distribuidos.

- **Microsegmentación:** Zscaler garantiza que los usuarios y las cargas de trabajo estén segmentados a nivel de aplicación, minimizando el movimiento lateral en caso de una infracción.

- **Supervisión de cifrado de extremo a extremo:** Zscaler inspecciona el tráfico de Internet cifrado mediante la interceptación SSL/TLS, sin comprometer el rendimiento ni la privacidad.

## APLICACIONES Y CARGAS DE TRABAJO

- **Segmentación de aplicaciones:** Zscaler ZPA proporciona segmentación basada en aplicaciones en lugar de la segmentación de red tradicional, lo que permite conexiones directas y seguras entre el usuario y la aplicación.

- **Seguridad de la carga de trabajo:** Zscaler Workload Segmentation (ZWS) protege las comunicaciones entre cargas de trabajo en entornos de nube pública y privada al garantizar la microsegmentación basada en identidad.

- **Supervisión continua:** la supervisión a nivel de aplicación rastrea la actividad de los usuarios y sus patrones de acceso para detectar anomalías, garantizando que las cuentas comprometidas no puedan escalar privilegios.

- **Seguridad SaaS:** Cloud Access Security Broker (CASB) de Zscaler controla el acceso tanto a aplicaciones SaaS autorizadas como no autorizadas, evitando así el acceso indebido a los datos y su uso no autorizado.

### DATOS

- **Prevención de pérdida de datos (DLP):** la DLP en la nube de Zscaler ayuda a proteger datos confidenciales en correo electrónico, web, SaaS y aplicaciones privadas. Identifica y previene la exfiltración de propiedad intelectual (PI) e información de identificación personal (PII).

- **Gestión de la postura de seguridad en la nube (CSPM):** Zscaler proporciona información y soluciones a configuraciones incorrectas en los sistemas de almacenamiento de datos en la nube, lo que reduce los riesgos de exposición.

- **Control de cifrado:** Zscaler aplica protocolos de cifrado estrictos tanto para datos en tránsito como en reposo, lo que garantiza que la información confidencial esté protegida de extremo a extremo.

- **Detección de TI en la sombra:** el CASB de Zscaler identifica y limita el uso de aplicaciones o servicios no aprobados o de alto riesgo, protegiendo los datos frente a filtraciones accidentales o usos malintencionados.

### GOBERNANZA, VISIBILIDAD Y ANÁLISIS, AUTOMATIZACIÓN Y ORQUESTACIÓN

- **Gestión de seguridad centralizada:** Zscaler Zero Trust Exchange ofrece una vista única del tráfico, las políticas y los incidentes de seguridad.

- **Análisis de seguridad integrado:** Zscaler proporciona visibilidad en tiempo real de la actividad de los usuarios y las aplicaciones a través de paneles y registros avanzados, que se integran con plataformas SIEM/SOAR para una respuesta optimizada a incidentes.

- **Inteligencia sobre amenazas:** Zscaler aprovecha la inteligencia global sobre amenazas y el análisis de comportamiento para detectar y responder de forma proactiva a las amenazas en toda la arquitectura Zero Trust.

- **Cumplimiento de políticas:** Zscaler automatiza los cambios de políticas y los controles de cumplimiento, lo que garantiza una gobernanza uniforme entre usuarios, aplicaciones y datos.

El enfoque de Zscaler para la implementación de Zero Trust y el modelo de madurez de Zero Trust (ZT MM) de la CISA son muy similares y se alinean en varias áreas clave, no solo en el pilar de Zero Trust.  La arquitectura de Zscaler admite funciones clave de ZTMM, como la aplicación dinámica de políticas, la visibilidad centralizada y los controles de acceso adaptativos basados en riesgos: elementos fundamentales para el desarrollo de una estrategia Zero Trust. Al aprovechar un enfoque en línea nativo de la nube, Zscaler ayuda a las organizaciones a avanzar en sus niveles de madurez descritos en el modelo de CISA, reduciendo las superficies de ataque y agilizando el acceso seguro.

## Hoja de ruta estratégica para la adopción de Zero Trust

Tanto la implementación de Zscaler como el modelo de madurez de Zero Trust de la CISA ofrecen una hoja de ruta estratégica que las organizaciones pueden seguir al adoptar los principios de Zero Trust. Dividimos el proceso de implementación en etapas manejables, lo que permite a las organizaciones establecer objetivos y cronogramas realistas para cada fase. Esta hoja de ruta garantiza que las organizaciones adopten un enfoque estructurado para la implementación de Zero Trust, reduciendo el riesgo de brechas o errores.

## Implementación incremental

La implementación incremental permite a las organizaciones mejorar gradualmente sus capacidades de Zero Trust a lo largo del tiempo. Este enfoque gradual facilita la implementación de Zero Trust sin sobrecargar los sistemas o recursos existentes. También permite a las organizaciones supervisar el progreso y ajustar las estrategias según sea necesario. Esto permite a Zscaler lanzar continuamente nuevos productos para reforzar la postura de seguridad de sus clientes, pero también permitirá que la CISA, en el futuro, pueda redefinir los objetivos. Lo que hoy se considera “óptimo” puede ser “avanzado” en el futuro.

## Ninguna organización es igual

Las necesidades y la infraestructura de ciberseguridad de cada organización son únicas.
La implementación de Zero Trust Exchange (ZTE) de Zscaler y el modelo de madurez de Zero Trust de la CISA son lo suficientemente flexibles como para adaptarse a los objetivos, desafíos y recursos específicos de cada organización. Tanto si una organización ha adoptado plenamente Zero Trust como si apenas ha iniciado el camino, el modelo ofrece la orientación necesaria para adaptar el marco Zero Trust a sus propios requisitos.

## Evaluación del progreso y del éxito

El modelo de madurez incluye métricas claras y criterios de evaluación que permiten a las organizaciones seguir su progreso a lo largo del tiempo. Al medir el éxito en función de etapas predefinidas, las organizaciones pueden identificar áreas de mejora y asegurarse de que avanzan en la dirección correcta hacia la consecución de un entorno Zero Trust maduro.

## Conclusión

El modelo de madurez de Zero Trust 2.0 de la CISA ofrece a las organizaciones un marco claro y estructurado para adoptar y avanzar en los principios de Zero Trust. Al implementar este modelo, las organizaciones pueden mejorar significativamente su postura de ciberseguridad, mitigar riesgos y garantizar el cumplimiento de los requisitos regulatorios.

A medida que el panorama de amenazas continúa evolucionando, la importancia de Zero Trust no hará más que aumentar, convirtiendo al modelo de la CISA en una herramienta crucial para las organizaciones que buscan proteger sus entornos digitales frente a las amenazas avanzadas actuales. Mediante una implementación estratégica e incremental, las organizaciones pueden adoptar Zero Trust de una manera que se alinee con sus necesidades y capacidades específicas, garantizando el éxito a largo plazo en su camino hacia la ciberseguridad.



**+1 408.533.0288** **Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134** **zscaler.com/es**

Zero Trust Everywhere