Informe técnico del Modelo de Madurez de Zero Trust de CISA

© 2025 Zscaler, Inc. Todos los derechos reservados.

DOCUMENTO TÉCNICO

Resumen ejecutivo

En el panorama actual de la ciberseguridad en constante evolución, las organizaciones se enfrentan a una creciente variedad de amenazas sofisticadas. Los modelos tradicionales de seguridad basados en el perímetro son cada vez más ineficaces para proteger las redes, a medida que se acelera la transformación digital y el trabajo 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 retos, la Agencia de Ciberseguridad y Seguridad de las Infraestructuras (CISA) ha desarrollado un Modelo de Madurez de Zero Trust para guiar a las organizaciones en la adopción e implementación efectiva de los principios de zero trust.

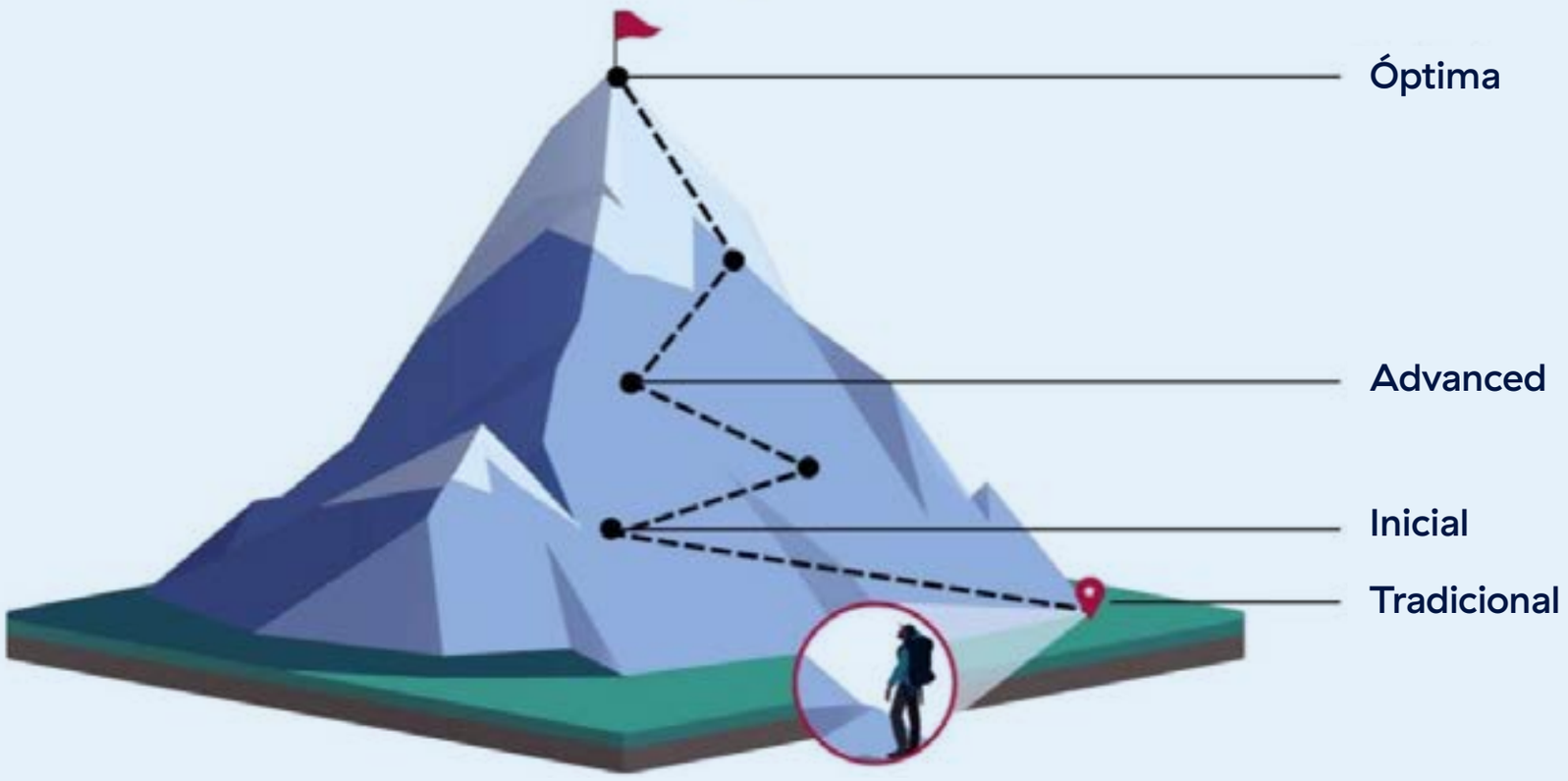
¿Qué es Zero Trust?

La zero trust es un modelo de seguridad que parte del supuesto de que las amenazas pueden ser internas o externas y, por tanto, no se debe confiar por defecto en ningún usuario o dispositivo. Cada solicitud de acceso, ya sea desde dentro o fuera de la red, se autentica rigurosamente, se autoriza y se monitorea de forma continua. El marco Zero Trust se centra en garantizar el mantenimiento de la seguridad en toda la infraestructura de una organización, poniendo especial atención a la identidad, la gestión de accesos y la supervisión en tiempo real.

¿Qué es el modelo de madurez de zero trust de CISA?

El Modelo de Madurez de Zero Trust de CISA proporciona a las organizaciones un marco para adoptar y madurar progresivamente los principios de la Zero Trust. Este modelo esboza un enfoque por fases para implantar la Zero Trust en toda una organización, desde la sensibilización y la planificación iniciales hasta la madurez total de las operaciones de seguridad integradas. Proporciona un método estructurado para comprender en qué punto se encuentra una organización en su camino hacia la Zero Trust y qué pasos debe seguir posteriormente para mejorar la seguridad.

El camino hacia la madurez de la zero trust



Fuente: CISA

© 2025 Zscaler, Inc. Todos los derechos reservados.

El modelo CISA divide la Zero Trust en varias áreas clave, como la gestión de identidades y accesos, la seguridad de dispositivos, la seguridad de redes, la seguridad de datos, la seguridad de aplicaciones y la visibilidad y analítica. El modelo de madurez ayuda a las organizaciones a evaluar sus capacidades actuales en cada una de estas áreas y a establecer una ruta clara para reforzar su postura de seguridad. Las organizaciones se evalúan en función de cuatro etapas de madurez (tradicional, inicial, avanzada y óptima), en las que cada etapa requiere un mayor nivel de protección, con un crecimiento exponencial de los esfuerzos y los beneficios.

El Modelo de Madurez de Zero Trust de CISA se utiliza cada vez más como punto de referencia global para la implementación de la 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 asignado su Zero Trust Advancement Center al modelo de madurez, reforzando aún más su papel como marco común para organizaciones de todo el mundo. A medida que crece la adopción de la Zero Trust, el Modelo de Madurez proporciona un lenguaje compartido y una hoja de ruta de madurez, ayudando a las entidades tanto del sector público como del privado a evaluar sus progresos y perfeccionar sus estrategias de seguridad.

COMPONENTES CLAVE DEL MODELO

1. **Gestión de identidad y acceso (IAM):** Establece mecanismos de autenticación sólidos, 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 red:** Implementa segmentación y monitoreo para restringir el movimiento lateral y detectar actividades sospechosas dentro de la red.

4. **Seguridad de datos:** Protege datos confidenciales mediante la aplicación de cifrado, controles de acceso estrictos y la supervisión del uso de datos.

5. **Seguridad de las aplicaciones:** Garantiza que las aplicaciones sean seguras mediante la implementación de prácticas de desarrollo seguras, monitoreo continuo y gestión de vulnerabilidades.

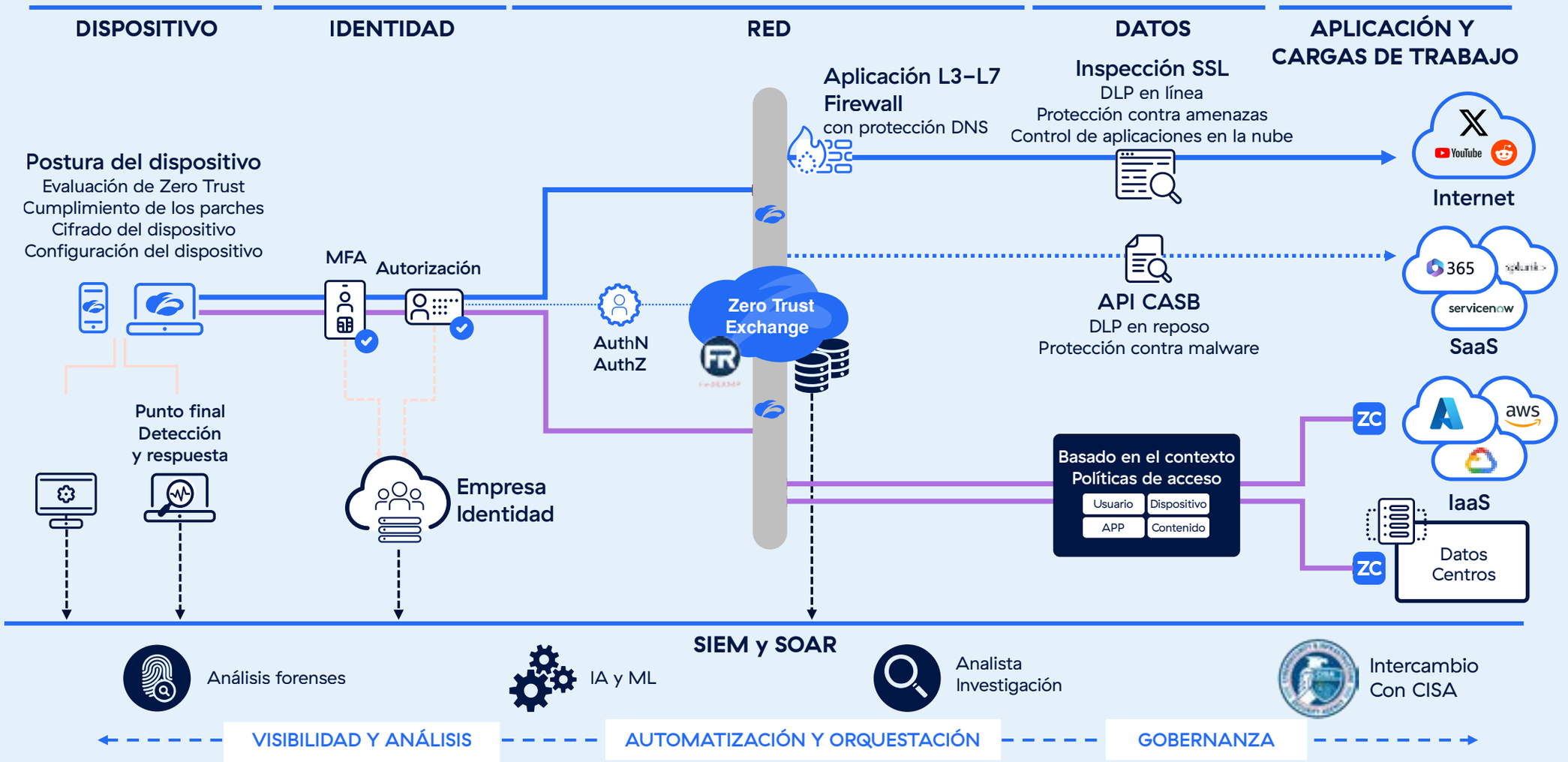
6. **Visibilidad y análisis:** Mejora el conocimiento de la situación al monitorear continuamente todo el tráfico y los eventos, identificar comportamientos anómalos y brindar alertas en tiempo real.

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

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

© 2025 Zscaler, Inc. Todos los derechos reservados.

Modelo de madurez de zero trust 2.0



Implementación del Modelo de Madurez Zero Trust de CISA con Zscaler

La implementación de Zscaler ZTE mejora inmediatamente su postura de seguridad al pasar de la seguridad tradicional basada en el perímetro a una defensa más completa y en capas. Al verificar continuamente usuarios, dispositivos y datos, las organizaciones pueden reducir el riesgo de violaciones de datos, amenazas internas y ataques externos. Este enfoque minimiza la superficie de ataque y evita el movimiento lateral de los atacantes. Zscaler también permite a las organizaciones avanzar en su estrategia del Modelo de Madurez Zero trust de CISA ofreciendo productos y funciones sólidas que soportan las áreas clave, incluyendo la gestión de identidades y accesos, seguridad de dispositivos, seguridad de redes, seguridad de datos, seguridad de aplicaciones y 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 de zero trust se refuerzan con la integración de SSO/MFA, lo que garantiza una autenticación sólida y reduce el riesgo de que las credenciales se vean comprometidas.

© 2025 Zscaler, Inc. Todos los derechos reservados.

- **Monitoreo continuo de usuarios:** ZTE garantiza que los usuarios estén continuamente autenticados y que su comportamiento sea monitoreado 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 sólidas 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.

- **Aplicación basada en agentes:** El agente de software ligero Zscaler Client Connector (ZCC) de Zscaler asegura que todo el tráfico de usuario se enrute a través de la nube de seguridad Zscaler, lo que permite la visibilidad y la aplicación uniforme de las políticas de seguridad.

- **Zero Trust para IoT/dispositivos no gestionados:** Las soluciones de Zscaler incluyen capacidades para controlar el acceso de dispositivos no gestionados, incluido IoT, mediante políticas de comportamiento y controles de acceso granulares.

RED

- **Zero Trust Network Access (ZTNA):** Zscaler Private Access (ZPA) sustituye a las VPN tradicionales con ZTNA. A los usuarios se les concede acceso “menos privilegiado” 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 puertas de enlace web seguras (SWG) y cortafuegos en la nube, 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 violación.

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

APLICACIONES Y CARGAS DE TRABAJO

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

- **Seguridad de la carga de trabajo:** Zscaler Workload Segmentation (ZWS) asegura las comunicaciones entre cargas de trabajo en entornos de nube pública y privada garantizando una “microsegmentación basada en identidades”.

- **Monitoreo continuo:** el monitoreo a nivel de aplicación rastrea la actividad del usuario y los patrones de acceso para detectar anomalías, lo que garantiza que las cuentas comprometidas no puedan escalar privilegios.

- **Seguridad SaaS:** Cloud Access Security Broker (CASB) de Zscaler controla el acceso a aplicaciones SaaS autorizadas y no autorizadas, lo que evita el acceso y uso no autorizado de datos.

© 2025 Zscaler, Inc. Todos los derechos reservados.

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 erróneas 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.

- **Descubrimiento de TI en la sombra:** Zscaler CASB identifica y limita el uso de apps/servicios no aprobados o de alto riesgo, protegiendo los datos de filtraciones accidentales o del uso malintencionado.

GOBERNANZA, VISIBILIDAD Y ANÁLISIS, AUTOMATIZACIÓN Y ORGANIZACIÓN

- **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 los incidentes.

- **Inteligencia de amenazas:** Zscaler aprovecha la inteligencia global de amenazas y el análisis de comportamiento para detectar y responder proactivamente a las amenazas en todo el tejido ZT.

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

El enfoque de implementación de la ZT de Zscaler y el MM de ZT de CISA son muy similares y se alinean en varias áreas clave, no solo en los pilares de ZT. La arquitectura de Zscaler admite funciones de MM de ZT clave como la aplicación dinámica de políticas, la visibilidad centralizada y los controles de acceso adaptables basados en el riesgo, elementos críticos en la maduración de una estrategia Zero Trust. Al utilizar un enfoque en línea y 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 la zero trust

Tanto la Implementación de Zscaler como el Modelo de Madurez de Zero Trust de CISA ofrecen una hoja de ruta estratégica para que las organizaciones adopten los principios de Zero Trust. Dividimos el proceso de implementación en etapas manejables, lo que permite a las organizaciones fijar objetivos y plazos realistas para cada fase. Esta hoja de ruta garantiza que las organizaciones adopten un enfoque estructurado para la implantación de Zero Trust, reduciendo el riesgo de lagunas o tropiezos.

© 2025 Zscaler, Inc. Todos los derechos reservados.

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 implantación de Zero Trust sin sobrecargar los sistemas o recursos existentes. También permite a las organizaciones monitorear el progreso y ajustar las estrategias según sea necesario. Esto permite a Zscaler lanzar continuamente nuevos productos para mejorar la postura de seguridad de nuestros clientes, pero también permitirá a CISA en el futuro cambiar 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 ZTE de Zscaler y el Modelo de Madurez de Zero trust de CISA son lo suficientemente flexibles como para ser personalizados para alinearse con los objetivos, retos y recursos específicos de una organización. Tanto si una organización ha adoptado plenamente Zero Trust como si acaba de iniciar la transformación, el modelo proporciona la orientación necesaria para adaptar el marco de Zero Trust a sus requisitos.

Medición del progreso y el éxito

El modelo de madurez incluye métricas y criterios de evaluación claros, que permiten a las organizaciones seguir sus progresos a lo largo del tiempo. Al medir el éxito con respecto a etapas predefinidas, las organizaciones pueden identificar áreas de mejora y asegurarse de que avanzan en la dirección correcta hacia la consolidación de un entorno de zero trust maduro.

Conclusión

El Modelo de Madurez de Zero Trust de CISA 2.0 proporciona a las organizaciones un marco claro y estructurado para adoptar y avanzar en los principios de la zero trust. Al implantar este modelo, las organizaciones pueden mejorar significativamente su postura de ciberseguridad, mitigar los riesgos y garantizar el cumplimiento de los requisitos normativos.

A medida que el panorama de las amenazas siga evolucionando, la importancia de la Zero Trust no dejará de aumentar, lo que convierte al modelo CISA en una herramienta crucial para las organizaciones que buscan proteger sus entornos digitales frente a las amenazas avanzadas de la actualidad. Mediante una implantación estratégica y gradual, las organizaciones pueden adoptar Zero Trust de una forma que se ajuste a sus necesidades y capacidades específicas, garantizando el éxito a largo plazo en su transformación de ciberseguridad.

Acerca de Zscaler

Zscaler (NASDAQ: ZS) acelera la transformación digital para que los clientes puedan ser más ágiles, eficientes, resistentes y seguros. Zscaler Zero Trust Exchange protege a miles de clientes de ciberataques y pérdida de datos al conectar de manera segura usuarios, dispositivos y aplicaciones en cualquier ubicación. Distribuido en más de 150 centros de datos en todo el mundo, Zero Trust Exchange basado en SSE es la plataforma de seguridad en la nube en línea más grande del mundo. Obtenga más información en **zscaler.com/mx** o síganos en Twitter **@zscaler**.

© 2025 Zscaler, Inc. Todos los derechos reservados. Zscaler™ y otras marcas comerciales listadas en **zscaler.com/mx/legal/trademarks** son (i) marcas comerciales registradas o marcas de servicio o (ii) marcas comerciales o marcas de servicio de Zscaler, Inc. en los Estados Unidos y/u otros países. Cualquier otra marca comercial es propiedad de sus respectivos propietarios.

+1 408.533.0288 **Zscaler, Inc. (Oficinas centrales) • 120 Holger Way • San José, CA 95134** **zscaler.com/mx**

zscaler™

Zero Trust Everywhere