DOCUMENTO TÉCNICO

Trabajando hacia el cumplimiento de NIS2: cómo Zero Trust debe ser una parte fundamental de este camino

Índice

1. Resumen ejecutivo: NIS2 y el papel de un modelo Zero Trust en la mejora de la ciberresiliencia 3

2. Descripción general de la Directiva NIS2 y su ámbito de aplicación 4

3. El enfoque de Zero Trust de Zscaler respalda la Directiva NIS2 5

4. Áreas clave de cumplimiento de NIS2 y cómo Zscaler puede ayudar 6

- 4.1 Medidas de gestión de riesgos de ciberseguridad NIS2 7
- 4.2 Gobernanza y gestión de riesgos de NIS2 7
- 4.3 Requisitos de notificación de incidentes de NIS2 8
- 4.4 Supervisión y cumplimiento de NIS2 9

Resumen ejecutivo

NIS2 y el papel de un modelo Zero Trust en la mejora de la ciberresiliencia

La promulgación de la directiva de seguridad de las redes y de la información 2 (NIS2) marca una evolución significativa en el compromiso de la Unión Europea (UE) de reforzar la ciberseguridad en todos sus estados miembros. NIS2 reemplaza a la Directiva NIS anterior y amplía su alcance a una gama más amplia de sectores y subsectores, al tiempo que endurece los requisitos de seguridad, incluyendo la elevación de la ciberseguridad a un imperativo de gestión y gobernanza. Si bien la Directiva NIS2 entró en vigor en 2023, la fecha límite clave es octubre de 2024, cuando los estados miembros de la UE deben tener leyes nacionales ejecutables que implementen la Directiva NIS2. Debido a que la implementación de la Directiva NIS2 puede variar ligeramente en cada estado miembro, este documento técnico se centra en los requisitos y principios de alto nivel de la propia directiva.

Ninguna solución o proveedor de software puede garantizar el cumplimiento de NIS2. Sin embargo, la adhesión a los principios Zero Trust (que la propia directiva sugiere que las entidades adopten como una práctica básica de higiene cibernética) aborda una serie de criterios exigidos por la directiva. La implementación de la arquitectura Zero Trust dentro del entorno de una organización, los elementos distribuidos de una red y los de terceros de una organización puede reducir radicalmente las superficies de ataque y eliminar una variedad de variables técnicas que pueden obstaculizar el progreso hacia el cumplimiento de NIS2. Zero Trust debería ser el vehículo principal que utilicen las organizaciones para mejorar la resiliencia; un socio proveedor de Zero Trust potente puede respaldar las iniciativas de cumplimiento de las organizaciones.

El proceso de cumplimiento normativo debe estructurarse y comunicarse entre las organizaciones que se rigen por la nueva Directiva. Encuestas recientes realizadas por Zscaler a equipos de TI europeos analizaron el grado de preparación de las organizaciones para el cumplimiento normativo.

El 71 % de los líderes de TI encuestados cree que la modernización de la seguridad requiere un cambio de mentalidad significativo, no solo un ejercicio de cumplimiento normativo.

Sin embargo, las actitudes de las diferentes partes interesadas que impulsarán el cumplimiento varían enormemente. Si bien el 80% de los líderes de TI encuestados confían en que sus organizaciones cumplirán antes de la fecha límite, solo el 53 % cree que sus equipos comprenden completamente el alcance de las obligaciones bajo NIS2. Cuando se pregunta sobre la comprensión del liderazgo corporativo de las obligaciones de cumplimiento, esa cifra se reduce al 49 %. Más del 60 % de los encuestados creen que NIS2 requerirá un cambio significativo en su estrategia de seguridad actual.

Zscaler está posicionado de manera única para ayudar a las organizaciones a navegar los cambios introducidos por NIS2 dada nuestra experiencia en seguridad en la nube. Al adoptar la arquitectura Zero Trust de Zscaler, las organizaciones de todos los tamaños pueden abordar los requisitos centrales de la directiva: mejorar sus mecanismos de defensa, reducir su exposición a los riesgos cibernéticos y agilizar las actividades de cumplimiento. Los principios Zero Trust se alinean estrechamente con los objetivos de NIS2 al eliminar sistemáticamente los derechos de acceso innecesarios, verificar rigurosamente todas las conexiones y minimizar el impacto potencial de los incidentes de seguridad. Zscaler proporciona una variedad de capacidades y herramientas que respaldan los esfuerzos de cumplimiento con disposiciones específicas de NIS2, incluidos la aplicación de políticas, la detección de incidentes y los procesos de respuesta.

Descripción general de la Directiva NIS2 y su alcance

NIS2 entró en vigor en 2023, y el plazo de implementación para los estados miembros de la UE finaliza en octubre de 2024. Los responsables de las políticas de la UE promulgaron esta nueva legislación crítica en respuesta a la necesidad de que la UE aumente su resiliencia cibernética en una era de crecientes ciberataques a los ciudadanos, las empresas y las economías europeas. NIS2 enfatiza la responsabilidad de las entidades de garantizar la seguridad de las redes y los sistemas de información, instándolas a contar con una cultura de gobernanza y marcos integrales de gestión de riesgos. La Directiva NIS2 es coherente con una tendencia creciente en la UE hacia una regulación más directa de los esfuerzos de resiliencia cibernética. (Por ejemplo, la ley de Resiliencia Operacional Digital (DORA), que entrará en vigor en enero de 2025, es un marco separado para gestionar y mitigar el riesgo de las TIC en el sector financiero).

La Directiva NIS2 añade nuevos sectores industriales, así como nuevos tipos de entidades dentro de sectores existentes, a la Directiva NIS original. Esta expansión responde a la creciente comprensión de que una amplia gama de actividades económicas y sociales dependen críticamente de la infraestructura de TI, que las ciberamenazas a estos sectores están aumentando y que las disrupciones pueden tener efectos en cascada en toda la UE.

Los sectores industriales en NIS2 se clasifican como "esenciales" o "importantes" para reflejar su criticidad o el servicio que brindan. Si bien los requisitos de ciberseguridad y de informes de incidentes para ambos grupos son los mismos, las dos categorías de entidades estarán sujetas a regímenes de supervisión y cumplimiento ligeramente diferentes, incluido el tamaño de las posibles multas por incumplimiento (más sobre esto a continuación).

> **"Con la fecha límite a la vuelta de la esquina, las organizaciones se enfrentan a una aceleración de los esfuerzos de cumplimiento, posiblemente a expensas de otros aspectos vitales de la ciberseguridad. El 60 % de los encuestados expresa su preocupación de que la concentración de esfuerzos en el cumplimiento de NIS2 pueda resultar en la desatención de otras áreas críticas de seguridad. Por consiguiente, es imperativo que los líderes de organizaciones brinden un apoyo sustancial a los departamentos de TI, garantizando un enfoque integral del cumplimiento que mitigue los riesgos de vulnerabilidades y contratiempos operativos."**
>
> **James Tucker,** director de CISO residentes de EMEA en Zscaler

Sectores y subsectores cubiertos por la Directiva NIS2[1]

Entidades esenciales (“Sectores de alta importancia”)	
Energía	Incluye electricidad, petróleo, gas, calefacción y refrigeración urbanas e hidrógeno.
Transporte	Incluye aire, ferrocarril, agua y carretera.
Banca (entidades de crédito)	
Infraestructura de mercados financieros	
Salud	Incluye atención sanitaria y productos farmacéuticos.
Agua potable	
Aguas residuales	
Infraestructura digital	Incluye proveedores de puntos de intercambio de Internet (IXP), proveedores de servicios DNS, registros de nombres TLD, proveedores de servicios de computación en la nube, proveedores de servicios de centros de datos, proveedores de redes de distribución de contenido, proveedores de servicios de confianza, proveedores de redes públicas de comunicaciones electrónicas y proveedores de servicios de comunicaciones electrónicas disponibles públicamente.
Gestión de servicios de TIC (de empresa a empresa)	Incluye proveedores de servicios gestionados y proveedores de servicios de seguridad gestionados
Administraciones públicas	Entidades de la administración pública de los gobiernos centrales y de los niveles regionales según lo definido en las leyes nacionales de los Estados miembros
Espacio (operadores de infraestructura terrestre)	
Entidades importantes (“Otros sectores críticos”)	
Servicios postales y de mensajería	
Gestión de residuos	
Fabricación, producción y distribución de productos químicos	
Producción, procesamiento y distribución de alimentos	
Fabricación	Incluye una amplia gama de manufacturas tales como dispositivos médicos, computadoras y productos electrónicos, equipos eléctricos, maquinaria y equipos, vehículos de motor, equipos de transporte.
Proveedores digitales	Incluye proveedores de mercados en línea, proveedores de motores de búsqueda en línea y proveedores de plataformas de servicios de redes sociales.
Organizaciones de investigación	

1. Existen algunas excepciones a estas categorías; véanse los Anexos I y II de la Directiva para obtener más detalles. También quedan excluidas las entidades de la administración pública cuyas actividades sean predominantemente de seguridad nacional, seguridad pública, defensa o aplicación de la ley. Además, la Directiva se aplica únicamente a las entidades que se califican como “empresas medianas” en la UE (empresas con más de 250 personas y un volumen de negocios anual superior a 50 millones de euros). Al mismo tiempo, algunas excepciones de la Directiva NIS2 se aplican a su vez a algunas entidades más pequeñas.

El enfoque Zero Trust de Zscaler respalda la Directiva NIS2

La plataforma Zero Trust Exchange™ de Zscaler reduce la complejidad asociada a la seguridad de red tradicional, facilitando a las organizaciones el cumplimiento de los requisitos de la Directiva NIS2. Zero Trust Exchange™ es una arquitectura nativa de la nube basada en SASE, diseñada específicamente para satisfacer las demandas de las operaciones comerciales globales con diversos requisitos tecnológicos y operativos. El uso de segmentación granular para compartimentar una red, la aplicación de acceso con privilegios mínimos para restringir los permisos de los usuarios y la supervisión continua del tráfico son medidas proactivas que ayudan a identificar y responder a las amenazas, minimizando así los posibles daños y el impacto de los ataques.

Zero Trust Exchange™ también permite a las organizaciones reducir su superficie de ataque, prevenir el movimiento lateral y disminuir los riesgos de infracción al abstraer la seguridad de la infraestructura de red. Esto garantiza que los usuarios se conecten de forma segura a las aplicaciones sin exponer las redes a Internet, lo que reduce significativamente el riesgo de ataques. Las capacidades de la plataforma respaldan los esfuerzos de cumplimiento requeridos por los mandatos NIS2 para la gestión seguro de los datos, controles de acceso y gestión de incidentes.

La plataforma mejora la seguridad al proteger todo el tráfico, los usuarios y los dispositivos, garantizando el bloqueo de amenazas en tiempo real y una inspección completa del tráfico. Zscaler también mejora la productividad del administrador con una gestión global unificada y la administración de políticas, eliminando la necesidad de mantenimiento de hardware y permitiendo centrarse en actividades de valor añadido. La plataforma Zscaler mejora el rendimiento de Internet para los usuarios finales y las conexiones directas a internet. Además, nuestro cumplimiento con los principales marcos de seguridad, como ISO 27001 y SOC2 Tipo II, mejora aún más la experiencia general del usuario y la seguridad de la organización. Puede encontrar más información sobre Zero Trust y el enfoque de Zscaler para la arquitectura Zero Trust en Zpediade Zscaler.

Alineación de Zscaler con NIS2

El enfoque integral de Zscaler en seguridad y cumplimiento nos permite reaccionar con rapidez y alinearnos con las regulaciones existentes, nuevas y emergentes, como NIS2. El programa interno de gestión de riesgos de ciberseguridad de Zscaler garantiza el cumplimiento de estándares internacionalmente reconocidos, como ISO 27001 y SOC 2. La alineación con estos estándares fundamentales permite a Zscaler integrar eficazmente un conjunto diverso de controles de seguridad para identificar, prevenir, detectar, responder y recuperarse de las amenazas asociadas en nuestros productos y servicios. Zscaler aprovecha un marco estructurado de controles comunes que se centra en competencias clave de ciberseguridad, como el establecimiento de un programa de gestión de riesgos de seguridad de la información, prácticas seguras en la cadena de suministro, la gestión de riesgos de terceros, las evaluaciones continuas de riesgos, la notificación de incidentes, la divulgación de vulnerabilidades, etc. Puede encontrar una lista actualizada de los estándares de seguridad y cumplimiento que Zscaler mantiene en la **página de resumen de cumplimiento de Zscaler**.

Además, Zscaler mantiene el **portal Zscaler Trust** para brindar a los clientes información en tiempo real sobre las operaciones de Zscaler y sirve como el principal foro de comunicaciones para **incidentes** y **avisos relacionados con Zscaler**.

Áreas clave de cumplimiento de NIS2 y cómo Zscaler puede ayudarle

La Directiva NIS2 delinea la responsabilidad de las entidades de garantizar la seguridad de las redes y los sistemas de información, exigiéndoles que tengan una cultura de gobernanza y marcos de gestión de riesgos establecidos, integrales y bien integrados. Para alcanzar estos objetivos, NIS2 incluye medidas de gestión de riesgos de ciberseguridad, medidas de gobernanza, requisitos de notificación de incidentes y supervisión y cumplimiento, todos ellos descritos a continuación.

En la encuesta de líderes de TI europeos mencionada anteriormente, el 56 % de los encuestados le dijo a Zscaler que sus equipos sienten que carecen de apoyo del liderazgo para cumplir con la fecha límite de cumplimiento de NIS2. Para respaldar sus procesos de cumplimiento, los líderes de TI encuestados dijeron que los cambios más significativos requeridos en sus organizaciones eran los siguientes:

- Actualización de pilas tecnológicas y soluciones de ciberseguridad: 34 %
- Formación de los empleados: 20 %
- Formación del liderazgo: 17 %

Medidas de gestión de riesgos de ciberseguridad de NIS2

Las entidades incluidas en el ámbito de aplicación de la Directiva deben adoptar medidas técnicas, operativas y organizativas proactivas para gestionar los riesgos que se plantean a la seguridad de las redes y sistemas de información que dichas entidades utilizan para sus operaciones o para la prestación de sus servicios, y para prevenir o minimizar el impacto de los incidentes en los destinatarios de sus servicios y en otros servicios que las organizaciones puedan prestar.

El artículo 21 de la Directiva enumera las medidas mínimas de gestión de riesgos de ciberseguridad que deben adoptar las organizaciones, mientras que los considerandos 78 y 89 proporcionan más información sobre lo que esperan los autores de la ley.

- **El artículo 21 (medidas mínimas de gestión de riesgos de ciberseguridad)** , especifica que las entidades deben implementar políticas sobre análisis de riesgos y seguridad de los sistemas de información; continuidad de negocio y gestión de crisis; seguridad de la cadena de suministro, incluyendo los procedimientos de calidad y desarrollo seguro de productos y las prácticas de ciberseguridad de sus proveedores y prestadores de servicios; prácticas básicas de ciberhigiene y capacitación en ciberseguridad; políticas y procedimientos sobre el uso de cifrado; seguridad de los recursos humanos, políticas de control de acceso y gestión de activos; y uso de soluciones de autenticación multifactor o autenticación continua.
- **Según el considerando 78**, las medidas de gestión de riesgos de ciberseguridad aplicadas por las entidades en el ámbito de aplicación de la Directiva deben tener en cuenta el grado de dependencia de la entidad con respecto a las redes y los sistemas de información; identificar cualquier riesgo de incidentes; prevenir, detectar, responder y recuperarse de los incidentes y mitigar su impacto; cubrir los datos almacenados, transmitidos y procesados; y prever un análisis sistémico, teniendo en cuenta el factor humano.
- **El Considerando 89** insta a las entidades a implementar una serie de prácticas básicas recomendadas de ciberhigiene, a saber, los principios Zero Trust, las actualizaciones de software, la configuración de dispositivos, la segmentación de la red, la gestión de identidades y accesos o la concienciación de los usuarios, y la formación del personal y la concienciación sobre ciberamenazas, phishing o técnicas de ingeniería social. El Considerando 89 también insta a las entidades a implementar tecnologías que mejoren la ciberseguridad, como la inteligencia artificial (IA) o los sistemas de aprendizaje automático (AA), para optimizar sus capacidades y la seguridad de las redes y los sistemas de información.

Cómo puede ayudarle Zscaler: A continuación, describimos en general cómo Zscaler puede ayudar a las entidades a cumplir con aspectos específicos de estas disposiciones. Para obtener un mapa detallado de las soluciones y herramientas específicas de Zscaler que respaldan estas disposiciones, comuníquese con su representante local de Zscaler. Puede encontrar contenido general y documentos técnicos sobre las soluciones de Zscaler en https://www.zscaler.com/es/resources?type=white-papers.

Gobernanza y gestión de riesgos de la Directiva NIS2

La Directiva NIS2 atribuye la máxima responsabilidad a la dirección de la empresa. La gerencia debe aprobar y supervisar la implementación de las medidas de gestión de riesgos de ciberseguridad de la entidad. La dirección también debe seguir la formación en ciberseguridad y ofrecer formación similar a sus empleados de forma regular, para que adquieran conocimientos y habilidades suficientes que les permitan identificar riesgos y evaluar las prácticas de gestión de riesgos de ciberseguridad y su impacto en los servicios de la entidad.

Cómo puede ayudarle Zscaler: Zscaler ofrece funciones de seguridad integrales en su conjunto de servicios, diseñadas para ayudar a las organizaciones a minimizar su superficie de ataque y garantizar la eficacia de los controles de seguridad aplicados en el programa de gestión de riesgos y gobernanza del cliente.

Zscaler Resilience™ es un conjunto completo de capacidades que garantiza la continuidad del negocio ininterrumpida durante apagones, caídas de tensión o eventos catastróficos de cisne negro.

Zscaler Internet Access (ZIA) y Zscaler Private Access (ZPA) refuerzan los flujos de tráfico y proporcionan registros de eventos y transacciones de seguridad para correlación y gestión, lo que permite a las organizaciones supervisar y mitigar amenazas potenciales de manera efectiva.

Zero Trust Exchange™ de Zscaler garantiza que los usuarios no queden en la red y las aplicaciones nunca queden expuestas a Internet, lo que reduce significativamente la superficie de ataque. La solución también permite a las organizaciones crear y aplicar políticas en torno a los sitios de IA generativa con los que los usuarios pueden interactuar para garantizar la protección de datos confidenciales.

Las capacidades de inspección SSL de Zscaler mejoran aún más la seguridad al descifrar el tráfico HTTPS para detectar y bloquear contenido malicioso.

Las ofertas Risk360™ y Zscaler Posture Control (ZPC) de Zscaler permiten la supervisión continua y la detección de vulnerabilidades, lo que permite a las organizaciones abordar de manera proactiva los riesgos de seguridad.

Zscaler Digital Experience (ZDX) proporciona seguimiento del inventario dedispositivos, lo que garantiza que los componentes del servicio se identifiquen adecuadamente y se retiren de forma segura cuando sea necesario, lo que contribuye a minimizar la superficie de ataque.

El servicio de transmisión Nanolog (NSS) de Zscaler facilita una comunicación fluida entre la nube de Zscaler y los dispositivos de soluciones de seguridad de terceros, lo que permite la transmisión en tiempo real de registros a los sistemas SIEM de los clientes a través de opciones NSS basadas en VM o en la nube.

El servicio de prevención de intrusiones en la nube Zscaler (IPS), integrado con tecnologías como firewalls y sandboxes, brinda protección integral contra diversos ataques, aprovechando firmas personalizadas y líderes en la industria para la supervisión en tiempo real y la aplicación de políticas. Además, las organizaciones pueden identificar y remediar vulnerabilidades de manera proactiva utilizando las capacidades de Zscaler, como las políticas de protección contra amenazas avanzadas y protección contra malware móvil de ZIA, mientras que Risk360 ofrece información sobre la superficie de ataque externa y el riesgo de propagación lateral, lo que permite tomar decisiones informadas para mejorar la postura de seguridad de una organización y reducir su tiempo medio de respuesta (MTTR).

Por último, todos los clientes pueden registrarse en ZScaler Trust Portal para notificar incidentes o sospechas de incidentes.

Requisitos de notificación de incidentes de NIS2 (artículo 23)

Las entidades deben notificar a las autoridades cualquier incidente que tenga un impacto significativo en la prestación de sus servicios. Cuando corresponda, las entidades también deben notificar a los destinatarios de sus servicios incidentes significativos que puedan afectar negativamente la prestación del servicio. La Directiva NIS2 define un incidente significativo como aquel que ha causado o es capaz de causar una interrupción operativa grave de los servicios o una pérdida financiera para la entidad en cuestión, o ha afectado o es capaz de afectar a otras personas físicas o jurídicas causándoles un daño material o inmaterial considerable.

El cronograma de informes de incidentes es el siguiente:

- Una "alerta temprana" dentro de las 24 horas siguientes a tener conocimiento del incidente significativo;
- Una notificación formal del incidente dentro de las 72 horas de tomar conocimiento del incidente significativo, proporcionando una evaluación inicial del incidente, incluyendo su gravedad e impacto, así como (cuando estén disponibles) indicadores de compromiso;
- Un informe final dentro de un mes que detalle el incidente, incluyendo su gravedad e impacto; el tipo de amenaza o causa raíz que probablemente haya desencadenado el incidente; las medidas de mitigación aplicadas y en curso; y (cuando corresponda) los impactos transfronterizos.
- Durante este proceso las autoridades pueden solicitar un informe intermedio sobre actualizaciones de estado relevantes.

Cómo puede ayudarle Zscaler: Las soluciones de seguridad en la nube de Zscaler ofrecen capacidades de detección y mitigación de amenazas en tiempo real, lo que garantiza que las organizaciones puedan identificar y mitigar las amenazas rápidamente. Además, al priorizar las defensas perimetrales tradicionales en favor de la verificación y autorización de identidad continuas, la arquitectura Zero Trust de Zscaler ayuda a prevenir el movimiento lateral que podría agravar la vulnerabilidad en caso de una brecha de seguridad. Al evaluar cada solicitud de acceso en función de la identidad, la autorización y el contexto circundante, todo el entorno está mejor protegido contra ciberincidentes.

Supervisión y ejecución de la Directiva NIS2 (artículos 32 y 33)

Los Estados miembros de la UE pueden ejercer poderes de supervisión y ejecución sobre las entidades que incumplan las medidas de gestión de riesgos de ciberseguridad y las obligaciones de presentación de informes de la Directiva NIS2. Los regímenes de supervisión y ejecución de las entidades esenciales e importantes están ligeramente diferenciados: para las entidades esenciales la supervisión es ex ante, mientras que para las entidades importantes es ex post (cuando hay evidencia, indicación o información de que una entidad no cumple con la Directiva NIS2).
En general, las autoridades pueden someter a las entidades cubiertas de cualquiera de las categorías a:

- Inspecciones in situ y supervisión externa
- Auditorías de seguridad específicas realizadas por un organismo independiente o una autoridad competente
- Análisis de seguridad
- Solicitudes de información necesarias para evaluar las medidas de gestión de riesgos de ciberseguridad adoptadas, incluidas las políticas de ciberseguridad documentadas
- Solicitudes de acceso a datos, documentos e información necesarios para la supervisión
- Solicitudes de evidencia de implementación de políticas de ciberseguridad

La Directiva NIS2 también establece que la dirección puede ser considerada personalmente responsable por las infracciones de la Directiva NIS2, incluidas posibles prohibiciones temporales de ocupar puestos directivos y, como último recurso, las autoridades tienen el poder de suspender temporalmente una certificación o autorización relacionada con los servicios relevantes prestados o las actividades realizadas por la entidad.

Los Estados miembros de la UE también pueden imponer multas administrativas en caso de incumplimiento del NIS. Para las entidades esenciales, las multas administrativas pueden alcanzar los 10 millones de euros o 2 % del volumen de negocio anual total mundial del ejercicio anterior, el que sea mayor. Para las entidades importantes, las multas pueden alcanzar los 7 millones de euros o 1,4 % del volumen de negocio anual total mundial del ejercicio anterior, el que sea mayor.

Cómo puede ayudarle Zscaler: Zscaler ayuda a las organizaciones a prepararse y responder a auditorías y escrutinios regulatorio a través de registros exhaustivos, aplicación constante de políticas e informes detallados.

Para obtener más información sobre las capacidades de NIS2 y Zscaler, póngase en contacto con su representante local de Zscaler.

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 los ciberataques y la pérdida de datos mediante la conexión segura de usuarios, dispositivos y aplicaciones en cualquier lugar. Distribuida en más de 150 centros de datos en todo el mundo, Zero Trust Exchange basada en SASE es la mayor plataforma de seguridad en la nube en línea del mundo. Obtenga más información en **zscaler.com/es** o síganos en Twitter **@zscaler**.

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