Resumen de la solución

# Zscaler Resilience™

## Continuidad empresarial ininterrumpida durante blackouts, brownouts y eventos catastróficos

## La continuidad de la actividad es fundamental para los responsables de TI

Nuestro modo de trabajar ha cambiado y, con este cambio, la continuidad empresarial se ha convertido en una prioridad absoluta para los responsables de TI. Ahora, los responsables de TI deben centrarse en prevenir las interrupciones de los servicios de misión crítica y facilitar la continuidad de la productividad como si se tratara de la actividad habitual. Con las herramientas, los procesos y la tecnología adecuados, los equipos de TI pueden restablecer rápida y fácilmente la funcionalidad total de sus organizaciones, incluso en caso de desastres.

El cambio hacia los servicios prestados en la nube para el almacenamiento, la informática y la seguridad ha aportado a las organizaciones sistemas flexibles y escalables, mejor continuidad empresarial, reducción de los costos de TI y menor complejidad. Incluso con estas ventajas, las organizaciones buscan optimizar la continuidad empresarial ante eventos catastróficos como desastres naturales, ataques físicos o amenazas de estados–nación.

Zscaler Resilience es un conjunto completo de capacidades que garantiza la continuidad empresarial sin interrupciones para los clientes durante blackouts, brownouts y eventos catastróficos. Está construido sobre la arquitectura avanzada de Zscaler Zero Trust Exchange™ y potenciado por la excelencia operativa para ofrecer alta disponibilidad y capacidad de servicio a los clientes en todo momento. Las capacidades de recuperación de desastres controladas por el cliente de Zscaler, en combinación con un sólido conjunto de opciones de migración tras error, respaldan los esfuerzos de planificación de continuidad de la actividad de los clientes en todos los escenarios posibles de fallo. Este amplio conjunto de capacidades de recuperación convierte a la nube de seguridad Zscaler en la nube más segura y resistente del sector.

## Resiliencia en la nube: ¿Por qué es necesaria?

Los líderes empresariales se focalizan en proporcionar un entorno que propicie la máxima productividad. Los equipos de TI deben permitir la continuidad empresarial y la productividad incluso cuando los problemas de conectividad, los eventos de escalado o los fallos del servicio interrumpan la normalidad de la actividad empresarial.

El tráfico de usuarios a aplicaciones de misión crítica, tanto SaaS como internas y privadas, debe circular siempre para garantizar la continuidad empresarial. Las interrupciones pueden provenir de una falla en la nube o en la conectividad con las aplicaciones. La resiliencia de la nube reúne ambas cosas: la resiliencia de la nube y la resiliencia a la nube.

**Resiliencia de la nube**

La resiliencia de la nube garantiza que la propia nube esté construida sobre una infraestructura eficaz y cuente con procesos operativos sólidos para las funciones empresariales cotidianas. La nube de Zscaler gestiona de forma autónoma muchos fallos menores (caída de nodos, problemas de disco, etc.) sin ninguna interacción con el cliente, pérdida de conectividad o caída del rendimiento. Nuestros sólidos sistemas de hardware construidos a medida constan de una capacidad de procesamiento y redundancia mucho mayor a la necesaria, sentando las bases de una gran capacidad de recuperación.

**Resiliencia a la nube**

La resiliencia a la nube es un aspecto esencial de una solución integral de resiliencia a la nube. La conectividad a la nube depende de su disponibilidad y de los medios de conexión para que los usuarios puedan acceder a las aplicaciones o a los datos. Cuando se interrumpe el acceso a la nube, es necesario encontrar una vía alternativa y óptima para las aplicaciones. Esta optimización representa un conjunto de acciones manuales o autónomas que pueden aplicarse para hacer frente a fallos que van desde una caída en el rendimiento de la red hasta interrupciones totales. Zscaler Resilience es un conjunto completo de capacidades que garantiza la continuidad ininterrumpida de la actividad empresarial ante cualquier tipo de fallo, desde fallos menores hasta fallos catastróficos.

## Garantiza la resiliencia de la nube frente a escenarios de fallo

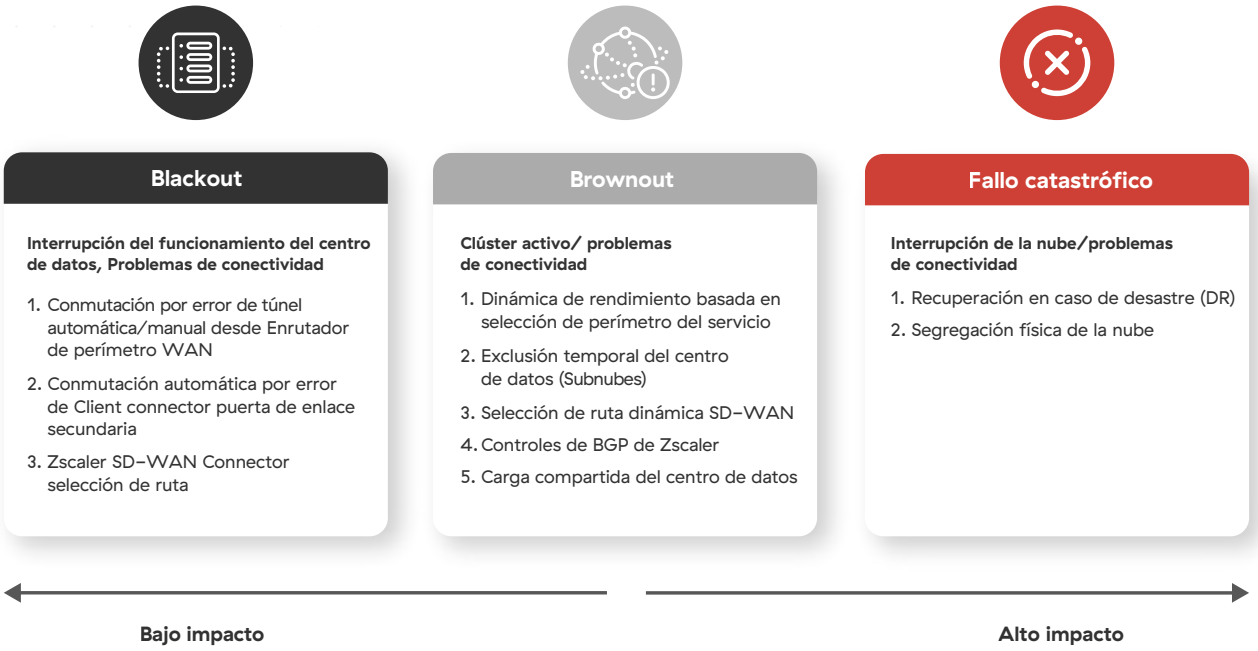


*Figura 1: Múltiples opciones para responder a escenarios de fallo*

## Fallos menores

Los fallos menores incluyen fallos de rendimiento, problemas de compatibilidad y problemas operativos o de calidad que no son fallos graves o críticos, las caídas de nodos o los problemas de disco podrían ser las razones principales de fallos aislados. Los fallos menores son los más frecuentes y suelen pasar desapercibidos. Estos fallos pueden provocar ralentizaciones, problemas operativos y pueden frustrar a los usuarios. La resiliente arquitectura en la nube de Zscaler y la excelencia operativa pueden evitarlos. Los fallos menores se gestionan en segundo plano con una interacción mínima con el cliente, al tiempo que se garantiza una productividad continua.

## Beneficios clave de Zscaler Resilience

### Continuidad empresarial con seguridad ininterrumpida

Aplique políticas de seguridad críticas al tiempo que garantiza un acceso a confianza cero a internet, SaaS y privado incluso durante desastres.

### Experiencias sin fisuras en todos los escenarios de fallo

Gestione blackouts, brownouts y fallos catastróficos con facilidad aprovechando la mejor arquitectura y excelencia operativa de su clase de Zscaler Zero Trust Exchange.

### Reducción de costos y complejidad

Evite las interrupciones de la actividad empresarial y las pérdidas de productividad causadas por la falta de acceso a las aplicaciones críticas, al tiempo que elimina los costes de las infraestructuras de respaldo heredadas y las VPN locales.

## Blackouts

Las interrupciones de los centros de datos (por ejemplo, la interrupción de enero de 2022 en las instalaciones de Interxion en Londres) o los problemas graves de conectividad, como la interrupción de los proveedores de transporte/tránsito, se consideran escenarios de apagón en los que las organizaciones no pueden reenviar tráfico al centro de datos de Zscaler afectado. Nuestra arquitectura redundante; centros de datos neutrales en cuanto al operador con múltiples proveedores e intercambio de Internet (IX), es muy eficaz para minimizar las interrupciones en caso de pérdida de un único operador y otros problemas de conectividad. Independientemente del tiempo de restablecimiento, el problema para nuestros clientes es la imposibilidad de seguir utilizando los servicios del centro de datos afectado.

Para continuar con la actividad, los clientes deben redirigir el tráfico a un centro de datos secundario cercano de Zscaler. Utilizamos una combinación de operadores y proveedores de centros de datos para mitigar eficazmente las interrupciones de cualquier distribuidor, garantizando que el centro de datos secundario esté disponible. También aprovisionamos más de lo necesario y mantenemos capacidad de reserva en el centro de datos para soportar carga transitoria adicional.

**Adoptar la continuidad empresarial consiste en pensar y planificar diferentes escenarios posibles de fallos. La infraestructura de Zscaler es de clase mundial y está diseñada para ofrecer una disponibilidad del 100%.**

**Tráfico desde la oficina utilizando el dispositivo SD-WAN**

Cuando se envía tráfico desde una oficina utilizando un dispositivo de enrutamiento/SD-WAN, los clientes deben seguir las mejores prácticas de implementación de Zscaler teniendo un túnel IPsec/GRE de respaldo listo para funcionar cuando no se puede acceder al primario. La forma en que se activa la conmutación por error depende de las capacidades del dispositivo y del diseño de la red. Por ejemplo, una SD-WAN con circuitos de Internet duales podría conmutar automáticamente al túnel de respaldo en un circuito secundario cuando el túnel activo sea inalcanzable o supere un umbral de latencia (con las comprobaciones de estado L7 activadas). Con dispositivos más primitivos, los clientes tendrían que habilitar manualmente el túnel de respaldo. Una vez que el centro de datos primario vuelve a funcionar, es responsabilidad del cliente volver a hacer el cambio.

**Tráfico a través Zscaler Client Connector**

Cuando se envía tráfico utilizando Zscaler Client Connector, Zscaler controla ambos extremos del túnel y conmutará automáticamente de la puerta de enlace primaria a la secundaria utilizando la lógica del archivo PAC de App Profile. Zscaler Client Connector (ZCC) volverá a la puerta de enlace primaria una vez que sea accesible. En ciertos casos, los clientes pueden optar por modificar manualmente los archivos PAC para activar una conmutación por error.

## Brownouts

Una caída involuntaria o inesperada de la calidad del servicio de la red suele constituir una brownout. La mala gestión de una brownout puede resultar costosa, tanto en términos de pérdida de ingresos como de productividad: si los usuarios alertan de una brownout antes de que el equipo de TI la haya descubierto y haya empezado a trabajar para resolverla, se puede producir una gran frustración en los usuarios, lo que ralentiza todo. Además de las formas de solucionar los blackouts, Zscaler ayuda a mitigar las brownouts de otras maneras que se mencionan a continuación.

**Selección de perímetro basada en rendimiento dinámico de Zscaler**
Zscaler Client Connector elige la ruta óptima entre el perímetro de servicio ZIA primario y secundario independientemente de la proximidad geográfica, confiando en cambio en el estado de cada perímetro de servicio ZIA, como se muestra en la figura 2. Una conexión HTTP de extremo a extremo calcula la latencia, haciendo ping continuamente a ambas puertas de enlace para conocer la latencia. De este modo, Zscaler proporciona una selección de centros de datos basada en la latencia para hacer frente a los escenarios de brownouts de forma eficaz.

**Exclusión del centro de datos controlada por el cliente**
Otra forma de mantener la continuidad empresarial durante las brownouts es mediante la selección de centros de datos controlada por el cliente, como se muestra en la figura 3. Cuando un cliente experimenta problemas de capacidad en un centro de datos, como un problema de interconexión de aplicaciones SaaS en LAX (que podría tardar horas en solucionarse), ese centro de datos puede excluirse de la subnube en el portal de gestión. Posteriormente Zscaler Client Connector obtiene la nueva puerta de enlace primaria y secundaria y establece un túnel Z a un nuevo centro de datos. Esta exclusión del centro de datos controlada por el cliente está limitada en el tiempo y vuelve a la selección original del centro de datos después de un tiempo predeterminado.

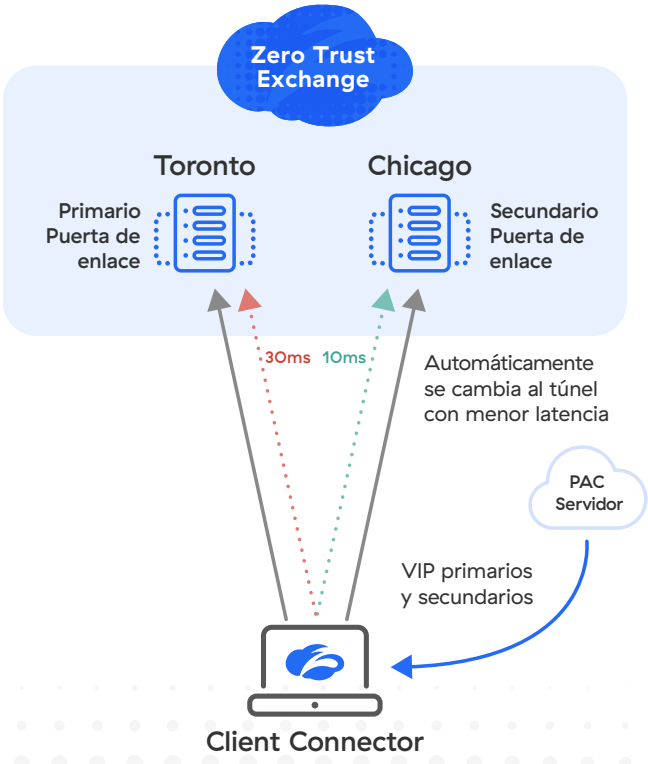


*Figura 2: Selección dinámica del perímetro de servicio basada en el rendimiento*

**Conmutación por error del túnel desde dispositivos de enrutamiento que detectan las brownouts**
Cuando se envía tráfico desde una oficina utilizando un dispositivo de enrutamiento/SD-WAN sobre el que Zscaler no tiene control directo, las opciones del cliente están limitadas a las capacidades del dispositivo de perímetro. Por ejemplo, un enrutador SD-WAN puede detectar la degradación del servicio utilizando algoritmos propios basados en comprobaciones de estado L7 a puntos finales de Zscaler. Una vez detectada una posible caída de tensión, el dispositivo SD-WAN puede conmutar automáticamente a un túnel de reserva en el mismo enlace o en un enlace secundario. El dispositivo volverá al túnel primario una vez que las comprobaciones de estado ofrezcan mejores resultados.

**Controles de BGP de Zscaler**
Nuestra arquitectura redundante; centros de datos neutrales con múltiples proveedores e intercambio de Internet (IX), es muy eficaz para minimizar las brownouts, congestión y otros problemas con operadores únicos. Cuando Zscaler CloudOps detecta que un ISP de la cadena ascendente proporciona un enrutamiento subóptimo, podemos redirigir el tráfico a través de un ISP secundario mientras trabajamos con el principal para resolver el problema.

**Reparto de la carga del centro de datos Zscaler**
En caso de congestión de la red u otros problemas de conectividad a un centro de datos en particular, Zscaler puede redirigir proactivamente a los clientes que ejecutan Zscaler Client Connector a centros de datos secundarios cercanos geográficamente sin utilizar un método estadístico.

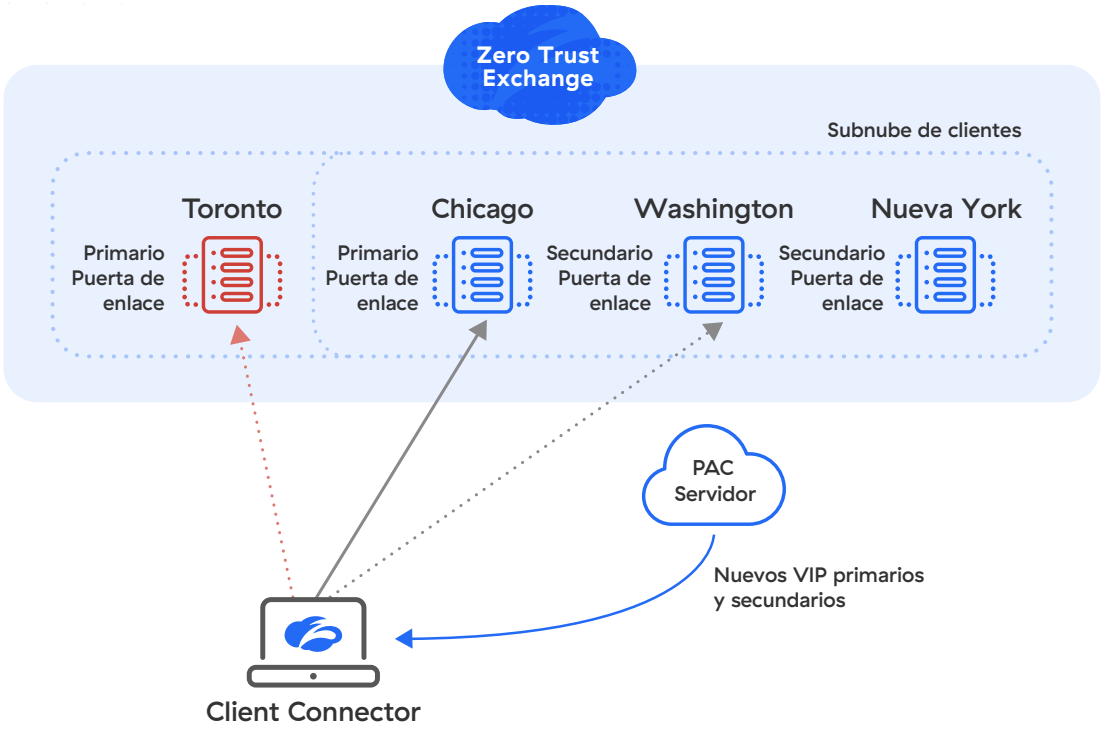


*Figura 3: Exclusión del centro de datos controlada por el cliente*

## Fallas catastróficas

**Capacidad de recuperación ante desastres de Zscaler para ZIA/ZPA**

La recuperación ante desastres (DR) de Zscaler para la nube garantiza operaciones ininterrumpidas para los usuarios, asegurando que puedan acceder a las aplicaciones de misión crítica incluso durante un suceso inesperado.

La recuperación ante desastres de Zscaler es una solución para la continuidad empresarial controlada por el cliente para mantener operativas a las organizaciones incluso durante un accidente catastrófico que pueda afectar a la nube de Zscaler.

La recuperación ante desastres de Zscaler se inicia actualizando el registro DNS TXT. Cuando se inicia la conmutación por error de DR, la recuperación ante desastres de Zscaler proporciona una ruta para que los usuarios que se conectan desde cualquier lugar puedan acceder a las aplicaciones privadas y SaaS de misión crítica y a Internet, como se muestra en la figura 4. Con la recuperación ante desastres de Zscaler, los clientes tienen el control sobre a qué aplicaciones privadas o SaaS críticas para la empresa pueden acceder los usuarios durante una interrupción de la nube global de Zscaler.

Los usuarios se conectan a aplicaciones privadas críticas a través de Zscaler Private Access™ (ZPA™) Private Service Edge, una versión local de la nube de Zscaler, y a aplicaciones SaaS críticas e Internet definidas por políticas guardadas en la instancia S3 de AWS. Cualquier cliente que tenga instalado Zscaler Client Connector puede utilizar la recuperación ante desastres de Zscaler. Mediante la activación de la recuperación ante desastres iniciada por el cliente y basada en DNS, los clientes pueden determinar y controlar cuándo activar la recuperación ante desastres.

Para un acceso seguro a las aplicaciones privadas, los administradores pueden configurar DR en el portal de administración de Zscaler para segmentos de aplicaciones críticas, grupos App Connector y grupos ZPA Private Service Edge para garantizar la continuidad empresarial en caso de que sucedan incidentes que afecten a la infraestructura global de la nube ZPA.

**Acceso a aplicaciones críticas identificadas por el cliente**

En el panel de control de la interfaz de usuario de ZPA, los clientes pueden identificar previamente las aplicaciones críticas para necesarias para la continuidad empresarial durante un incidente y así poder asegurar que los usuarios tengan acceso a esas aplicaciones durante un evento de DR.

Para el acceso seguro a las aplicaciones en Internet a través de Zscaler Internet Access™ (ZIA™), los administradores pueden elegir entre las siguientes opciones para la recuperación de desastres (estos controles se proporcionan a través de Zscaler Client Connector y se configuran en el Zscaler Portal):

- **Fallo abierto:** En el improbable caso de una interrupción de Zscaler Cloud, los usuarios pasan directamente a Internet. Sin embargo, esto conlleva el riesgo de dar a todos los usuarios acceso sin limitaciones a cualquier sitio web de Internet sin restricciones de seguridad.
- **Fallo abierto controlado—acceso a la lista de destinos de Internet definida por Zscaler:** Los usuarios tienen acceso a las aplicaciones más comunes y críticas de la web (Office 365, Google Workspace, etc.). Zscaler conserva esta lista, alojada en AWS, para que esté disponible mientras Zscaler Cloud se recupera de una interrupción. Los clientes pueden añadir su propia lista de sitios web de Internet a esta lista, y cualquier sitio web que no esté en la lista será bloqueado, aplicado en el punto final del usuario a través de Zscaler Client Connector. Zscaler Client Connector descargará periódicamente esta lista para mantenerla actualizada y precisa.
- **Fallo cerrado:** Los clientes muy preocupados por la seguridad y que no desean que los usuarios accedan a nada en Internet sin ZIA pueden detener todo tipo de acceso.

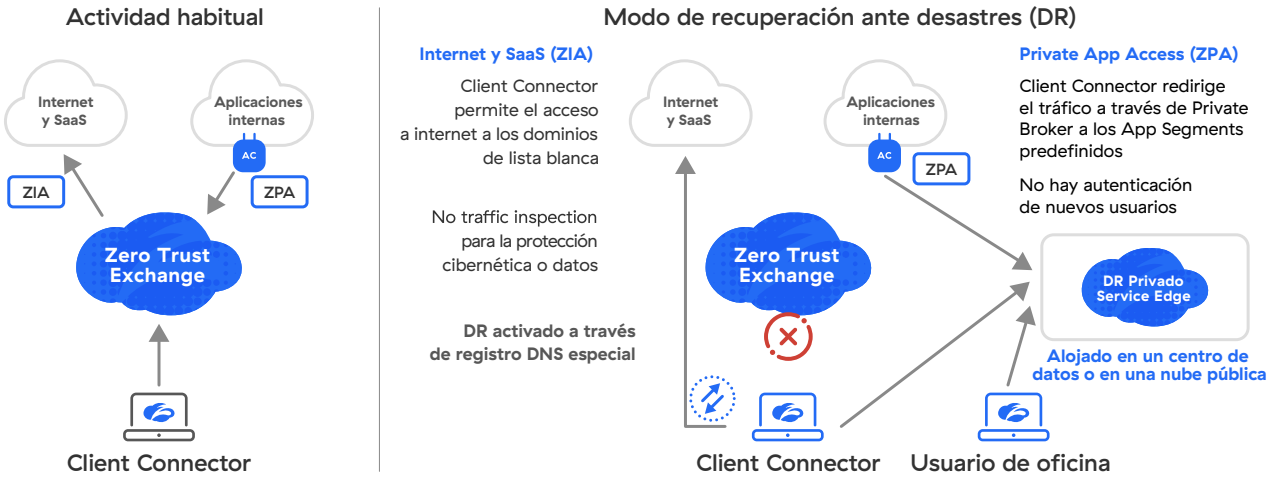


*Figura 4: Recuperación ante desastres para el servicio de misión crítica de Zscaler*

Habilitar la recuperación ante incidentes garantiza la continuidad empresarial en caso de un escenario de desastre que afecte a la infraestructura global de la nube de Zscaler. Esta medida permite a los usuarios seguir accediendo sin problemas a las aplicaciones críticas desde cualquier lugar del mundo.

Durante las operaciones normales, el acceso a las aplicaciones de misión crítica se realiza a través de Zero Trust Exchange. En un escenario de desastre, todas las conexiones a las aplicaciones privadas se gestionarán a través del ZPA Private Service Edge, que se instala localmente en el centro de datos del cliente o en la nube privada, y todas las conexiones a Internet y a las aplicaciones SaaS se aplican a través de políticas guardadas en el compartimiento S3 de AWS. El resultado es una experiencia de usuario sin fisuras durante un desastre. Una vez restablecida la funcionalidad de Zscaler Cloud, el producto puede volver al funcionamiento normal para aprovechar al máximo la seguridad y la conectividad de confianza cero a través de Zero Trust Exchange. Zscaler Digital Experience detecta fallos menores, brownouts y blackouts para ayudar a los clientes a solucionarlos antes de que afecten drásticamente a los usuarios. La plataforma Zscaler proporciona una flexibilidad total para la continuidad empresarial con una seguridad inigualable y una experiencia de usuario sin fisuras.

El hecho de que Zscaler Resilience forme parte de la plataforma general ofrece a nuestros clientes redundancia dentro de la plataforma sin necesidad de servicios externos adicionales. Zscaler se compromete a proporcionar una experiencia fluida y continua para los usuarios y los equipos de TI con inversiones continuas en las soluciones Zscaler Resilience.

Para conocer las novedades sobre Zscaler Resilience visite zscaler.com/mx/resilience.

## Principales ventajas de la recuperación ante desastres de Zscaler

- Interrupción mínima de las operaciones para los clientes durante un desastre
- Acceso a aplicaciones de misión crítica incluso durante un evento inesperado • Mayor confiabilidad de la solución para el acceso a aplicaciones con Zscaler
- Ahorro de costos al disponer de una única plataforma para gestionar el acceso a las aplicaciones tanto durante el funcionamiento normal como durante el DR
- Ahorro potencial al evitar la pérdida de productividad por interrupciones durante un desastre

zscaler™ | Experience your world, secured.™



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