Resumen de la solución

Zscaler Resilience™

Continuidad comercial ininterrumpida durante apagones, caídas de tensión y eventos catastróficos

La continuidad del negocio es lo más importante para los líderes de TI

La forma en que trabajamos ha cambiado y, con este cambio, la continuidad del negocio se ha convertido en una prioridad fundamental para los líderes de TI. Ahora, los líderes de TI deben centrarse en evitar interrupciones en los servicios esenciales y facilitar la productividad continua como si todo transcurriera con normalidad. Con las herramientas, los procesos y la tecnología adecuados, los equipos de TI pueden restaurar rápida y fácilmente la funcionalidad completa de sus organizaciones, incluso en caso de desastre

El paso a los servicios prestados en la nube para el almacenamiento, la computación y la seguridad ha brindado a las organizaciones sistemas flexibles y escalables, una mejor continuidad del negocio, menores costes de TI y menor complejidad. Incluso con estas ventajas, las organizaciones buscan optimizar la continuidad del negocio frente a eventos desastrosos como desastres naturales, ataques físicos o amenazas de estados–nación.

Zscaler Resilience es un conjunto completo de capacidades de resiliencia que garantiza una continuidad comercial ininterrumpida para los clientes durante apagones, caídas de tensión y eventos catastróficos. Se basa en la arquitectura avanzada de Zscaler Zero Trust ExchangeTM y está mejorado por excelencia operativa para ofrecer alta disponibilidad y capacidad de servicio a los clientes en todo momento. Las capacidades de recuperación ante desastres controladas por el cliente de Zscaler, en combinación con un sólido conjunto de opciones de conmutación por error, respaldan los esfuerzos de planificación de la continuidad del negocio de los clientes en todos los escenarios de error. Este conjunto integral de capacidades de resiliencia hace que la nube de seguridad de Zscaler sea la nube más segura y resistente del sector.

Resiliencia de la nube: ¿Por qué es necesaria?

Los líderes empresariales se centran en proporcionar un entorno favorable para lograr la máxima productividad. Los equipos de TI deben permitir la continuidad del negocio y la productividad incluso cuando los problemas de conectividad, los eventos de escalado o los errores de servicio interrumpen la actividad comercial normal.

El tráfico de usuarios a aplicaciones esenciales (SaaS, internas y privadas por igual) siempre debe fluir para garantizar la continuidad del negocio. Las interrupciones pueden provenir de un error en la nube o en la conectividad a las aplicaciones. La resiliencia de la nube abarca tanto la resiliencia de la nube como la resiliencia a la nube.

Resiliencia de la nube
La resiliencia de la nube garantiza que la propia nube se base en una infraestructura eficaz y tenga procesos operativos sólidos para las funciones empresariales cotidianas. La nube de Zscaler maneja de manera autónoma muchos errores menores (caída del nodo, problemas de disco, etc.) sin ninguna interacción con el cliente, pérdida de conectividad o caída del rendimiento. Nuestros sólidos sistemas de hardware especialmente diseñados con sobreaprovisionamiento de capacidad de procesamiento y redundancia proporcionan la base para una alta resiliencia.

Resiliencia a la nube
La resiliencia a la nube es un aspecto esencial de una solución integral de resiliencia en la nube. La conectividad a la nube depende de su disponibilidad y los medios para conectarse para que los usuarios puedan acceder a aplicaciones o datos. Cuando se interrumpe el acceso a la nube, es necesario encontrar una ruta óptima y alternativa para acceder a las aplicaciones. Esta optimización representa una colección de acciones manuales o autónomas que se pueden aplicar para abordar errores que van desde una caída en el rendimiento de la red hasta interrupciones completas. Zscaler Resilience es un conjunto completo de capacidades que garantiza la continuidad comercial ininterrumpida sin importar el tipo de error que se dé, desde fallos menores hasta fallos catastróficos.

Garantizar la resiliencia a la nube en escenarios de error

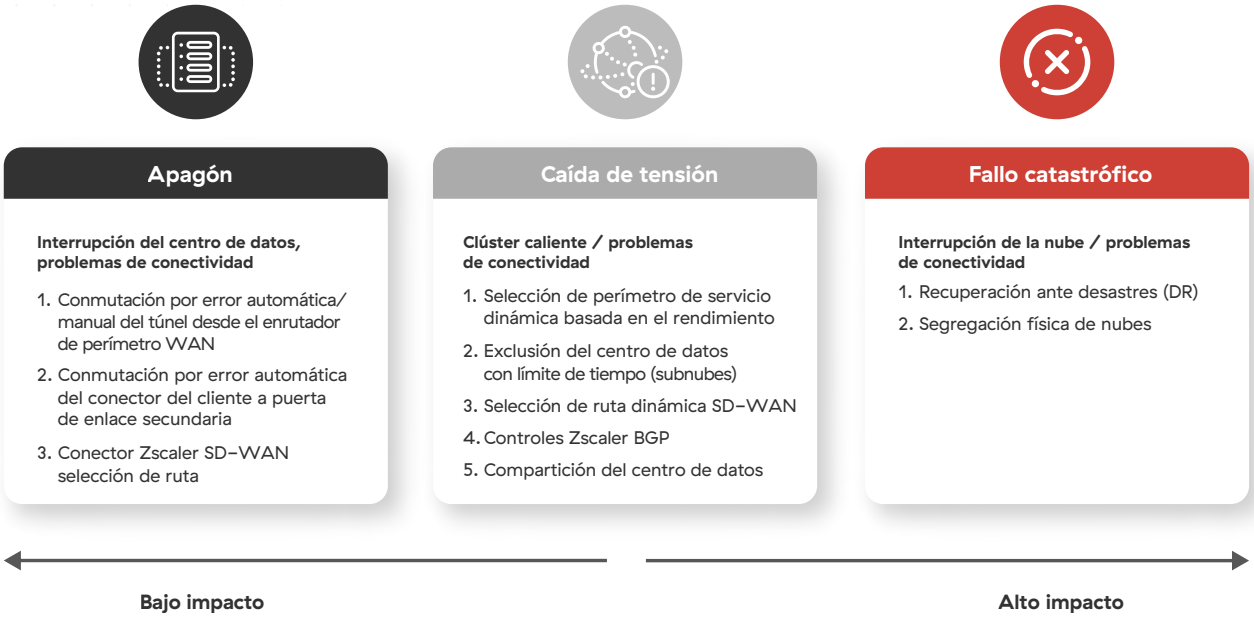

Figura 1: Múltiples opciones para responder a escenarios de error

Fallos menores

Los fallos menores incluyen errores de rendimiento, problemas de compatibilidad y problemas operativos o de calidad que no son fallos graves o críticos; los errores de los nodos o los problemas del disco pueden ser las razones principales de los fallos aislados. Los fallos menores ocurren con mayor frecuencia y, a menudo, pasan desapercibidos. Estos fallos pueden generar ralentización, problemas operativos y frustración del usuario. La arquitectura de nube resiliente y la excelencia operativa de Zscaler pueden prevenirlos. Los fallos menores se gestionan en segundo plano con una interacción mínima con el cliente y, al mismo tiempo, se garantiza una productividad continua.

Beneficios clave de Zscaler Resilience

Continuidad del negocio con seguridad ininterrumpida

Aplique políticas de seguridad críticas al tiempo que otorga acceso de confianza cero a Internet, SaaS y aplicaciones privadas, incluso durante desastres.

Experiencias fluidas en todos los escenarios de fallo

Handle blackouts, brownouts, and catastrophic failures with ease by leveraging the best-in-class architecture and operational excellence of the Zscaler Zero Trust Exchange.

Costes reducidos y complejidad

Evite las interrupciones del negocio y las pérdidas de productividad causadas por la falta de acceso a aplicaciones críticas mientras elimina los costes de la infraestructura de copia de seguridad heredada y las VPN locales.

Apagones

Las interrupciones del centro de datos (p. ej., la interrupción de enero de 2022 en las instalaciones de Interxion en Londres) o los problemas graves de conectividad, como las interrupciones de proveedores de servicios de operador/transporte, se consideran escenarios de interrupción en los que las organizaciones no pueden reenviar el tráfico al centro de datos Zscaler afectado. Nuestra arquitectura redundante (centros de datos independientes del operador con múltiples proveedores e intercambio de Internet [IX]) es muy eficaz para minimizar las interrupciones en caso de pérdida de un solo operador y otros problemas de conectividad. Independientemente del tiempo de restauración, el impacto en nuestros clientes es la incapacidad 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 Zscaler secundario cercano. Utilizamos una combinación de operadores y proveedores de centros de datos para mitigar eficazmente las interrupciones de cualquier proveedor determinado, lo que garantiza que el centro de datos secundario estará disponible. También sobreaprovisionamos y mantenemos capacidad de reserva en el centro de datos para tramitar cargas transitorias adicionales.

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

Tráfico desde la oficina mediante dispositivo SD-WAN

Al enviar tráfico desde una oficina mediante un dispositivo de enrutamiento/SD-WAN, los clientes deben seguir las mejores prácticas de implementación de Zscaler y tener un túnel IPsec/GRE de respaldo listo para usar cuando no se puede acceder al principal. 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 por error automáticamente al túnel de respaldo en un circuito secundario cuando el túnel activo se vuelva inalcanzable o supere un umbral de latencia (con las comprobaciones de estado de L7 habilitadas). Con dispositivos más primitivos, los clientes tendrían que habilitar manualmente el túnel de respaldo. Una vez que el centro de datos principal está en funcionamiento, es responsabilidad del cliente volver a cambiar.

Tráfico utilizando Zscaler Client Connector

Al enviar tráfico mediante Zscaler Client Connector, Zscaler controla ambos perímetros del túnel y conmutará automáticamente desde la puerta de enlace principal a la secundaria mediante la lógica del archivo PAC del perfil de la aplicación. Zscaler Client Connector (ZCC) regresará a la puerta de enlace principal una vez que sea accesible. En ciertos casos, los clientes pueden optar por modificar manualmente los archivos PAC para activar una conmutación por error.

Caídas de tensión

Una caída involuntaria o inesperada en la calidad del servicio de red generalmente constituye una caída de tensión. La mala gestión de una caída de tensión puede resultar costosa, tanto en términos de pérdida de ingresos como de productividad; si los usuarios notifican una caída de tensión antes de que el equipo de TI la haya descubierto y haya comenzado a trabajar para resolverla, puede provocar una gran frustración del usuario, lo que ralentiza todo. Además de las formas que Zscaler tiene de abordar los apagones, también ayuda a mitigar las caídas de tensión de otras maneras que se mencionan a continuación.

Selección dinámica de servicios perimetrales basada en el rendimiento de Zscaler
Zscaler Client Connector elige la ruta óptima entre el ZIA Service Edge primario y secundario, independientemente de la proximidad geográfica, en lugar de confiar en el estado de cada ZIA Service Edge, como se muestra en la figura 2. Una conexión HTTP de extremo a extremo calcula la latencia haciendo ping continuamente en ambas puertas de enlace para determinar la latencia. Con esta información, Zscaler proporciona una selección de centros de datos basada en la latencia para abordar escenarios de caídas de tensión de manera efectiva.

Exclusión del centro de datos controlada por el cliente
AnOtra forma de mantener la continuidad empresarial durante las caídas de tensión es a través de la selección del centro 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 emparejamiento de aplicaciones SaaS en LAX (que podría tardar horas en solucionarse), dicho centro de datos se puede excluir de la subnube en el portal de administración. Luego, 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 tiene un límite de tiempo y vuelve a la selección original del centro de datos después de un tiempo predeterminado.

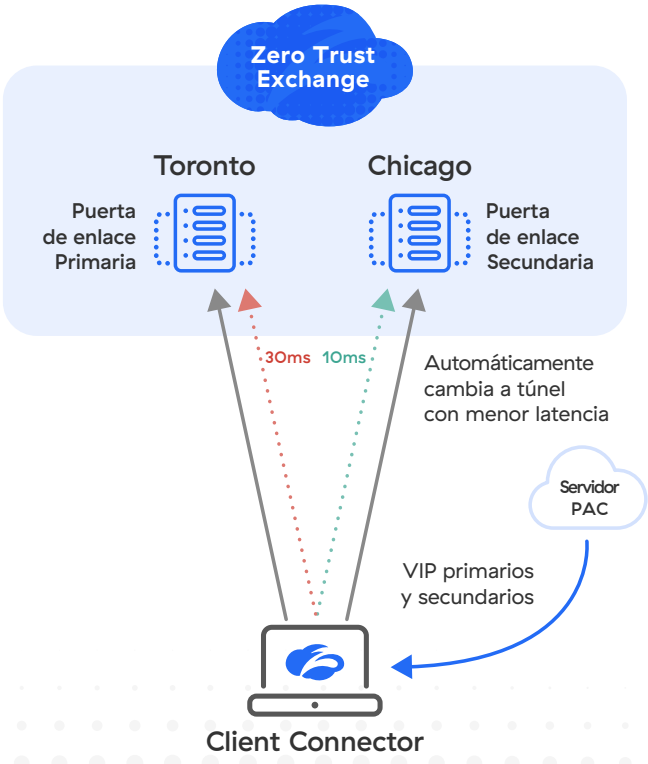

Figura 2: La selección dinámica de servicio perimetral basada en el rendimiento

Conmutación por error del túnel desde dispositivos de enrutamiento que detectan caídas de tensión
Cuando se envía tráfico desde una oficina mediante un dispositivo de enrutamiento/SD-WAN sobre el cual Zscaler no tiene control directo, las opciones de un cliente están vinculadas a las capacidades del dispositivo perimetral. Por ejemplo, un enrutador SD-WAN puede detectar la degradación del servicio utilizando algoritmos patentados basados en comprobaciones de estado L7 para los puntos finales de la sonda Zscaler. Una vez que se detecta una posible caída de tensión, el dispositivo SD-WAN puede conmutar por error automáticamente a un túnel de respaldo en el mismo enlace o en un enlace secundario. El dispositivo volverá al túnel principal una vez que las comprobaciones de estado proporcionen mejores resultados.

Controles Zscaler BGP
Nuestra arquitectura redundante (centros de datos independientes del operador con múltiples proveedores e intercambio de Internet [IX]) es muy eficaz para minimizar las caídas de tensión, la congestión u otros problemas con un solo operador. Cuando Zscaler CloudOps descubre que un ISP ascendente proporciona un enrutamiento subóptimo, podemos redirigir el tráfico a través de un ISP secundario mientras trabajamos con el principal para resolver el problema.

Compartición de centros de datos Zscaler
En caso de congestión de la red u otros problemas de conectividad en un centro de datos en particular, Zscaler puede redirigir proactivamente a los clientes que ejecutan Zscaler Client Connector a centros de datos secundarios que estén próximos geográficamente sin usar un método estadístico.

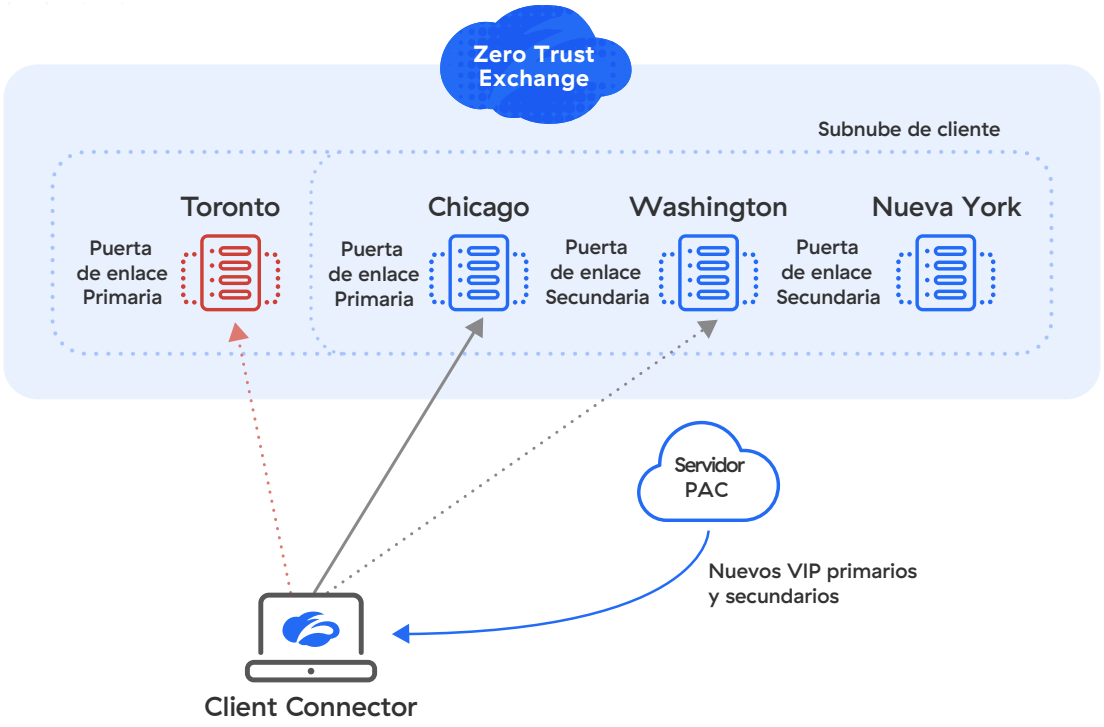

Figura 3: Exclusión del centro de datos controlada por el cliente

Fallos catastróficos

Capacidad de recuperación ante desastres de Zscaler para ZIA/ZPA

La recuperación ante desastres (DR) de Zscaler para la nube proporciona operaciones ininterrumpidas para los usuarios, lo que garantiza que puedan acceder a aplicaciones esenciales incluso durante un evento de cisne negro.

La recuperación ante desastres de Zscaler es una solución de continuidad comercial controlada por el cliente para mantener las organizaciones operativas incluso durante un evento catastrófico que pueda afectar 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 se conecten desde cualquier lugar para acceder a aplicaciones SaaS y privadas de misión crítica e Internet, como se muestra en la figura 4. Con la recuperación ante desastres de Zscaler, los clientes tienen el control sobre a qué aplicaciones SaaS o privadas críticas para la actividad empresarial pueden acceder los usuarios durante una interrupción de la nube global de Zscaler.

Los usuarios se conectan a aplicaciones privadas críticas a través del perímetro del servicio privado Zscaler Private Access™ (ZPA™), una versión implementada localmente de la nube de Zscaler, y a aplicaciones SaaS críticas e Internet definidas por políticas guardadas en la instancia de AWS S3. Cualquier cliente que tenga instalado Zscaler Client Connector puede usar la recuperación ante desastres de Zscaler. A través del activador DR basado en DNS iniciado por el cliente, los clientes pueden determinar y controlar cuándo activar la recuperación ante desastres.

Para un acceso seguro a aplicaciones privadas, los administradores pueden configurar la DR en el portal de administración de Zscaler para segmentos de aplicaciones críticas, grupos de conectores de aplicaciones y grupos de perímetro de servicio privado de ZPA para garantizar la continuidad de la actividad empresarial en caso de un desastre que afecte la infraestructura global de la nube de ZPA.

Acceso a aplicaciones críticas identificadas por el cliente

En el tablero de la interfaz de usuario de ZPA, los clientes pueden identificar previamente las aplicaciones críticas para la continuidad de la actividad empresarial durante un desastre para asegurarse de que los usuarios tengan acceso a esas aplicaciones durante un evento de recuperación ante desastres (DR).

Para un 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 ante desastres (estos controles se proporcionan a través de Zscaler Client Connector y se configuran en Zscaler Portal):

- **Fallo abierto:** en el improbable caso de una interrupción de la nube de Zscaler, los usuarios van directamente a Internet. Sin embargo, esto conlleva el riesgo de dar a todos los usuarios acceso ilimitado a cualquier sitio web en 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 en la web (Office 365, Google Workspace, etc.). Zscaler mantiene esta lista, alojada en AWS, para que esté disponible mientras la nube de Zscaler se recupera de una interrupción. Los clientes pueden agregar su propia lista de sitios web de Internet a esta lista y cualquier sitio web que no esté en la lista se bloqueará. Esta decisión se aplicará en el extremo del usuario a través de Zscaler Client Connector. Zscaler Client Connector descargará periódicamente esta lista para mantenerla actualizada y precisa.
- **Fallo cerrado:** los clientes que son muy conscientes de la seguridad y que no desean que los usuarios accedan a nada en Internet sin ZIA pueden detener todo acceso.

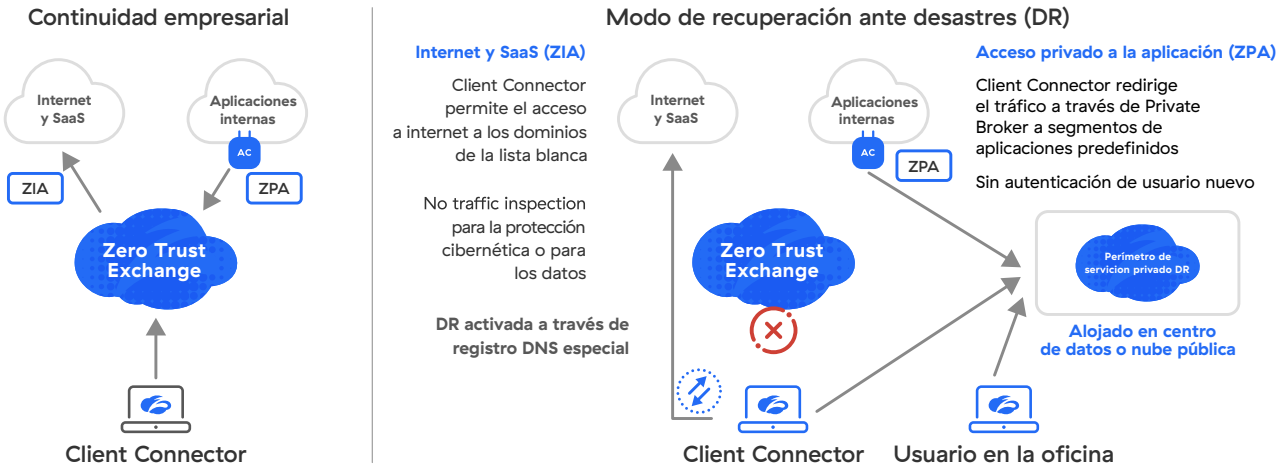

Figura 4: Recuperación ante desastres para los servicios de misión crítica de Zscaler

La habilitación de la recuperación ante desastres garantiza la continuidad de la actividad empresarial en caso de un escenario de desastre que afecte la infraestructura global de la nube de Zscaler. Esta implementación permite un acceso continuo y sin fisuras a aplicaciones críticas para usuarios desde cualquier parte del mundo.

Durante las operaciones normales, el acceso a las aplicaciones de misión crítica se negocia a través de Zero Trust Exchange. En caso de desastre, todas las conexiones a aplicaciones privadas se gestionarán a través de 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 aplicaciones SaaS se aplican a través de políticas guardadas en el depósito de AWS S3. Esto da como resultado una experiencia de usuario perfecta durante una situación de desastre. Tras la restauración de la funcionalidad de la nube de Zscaler, el producto puede volver a su funcionamiento normal para aprovechar al máximo la seguridad y la conectividad de confianza cero a través de Zero Trust Exchange. Zscaler Digital Experience detecta errores menores, apagones y caídas de tensión para ayudar a los clientes a abordarlos antes de que afecten drásticamente a los usuarios. La plataforma Zscaler brinda total flexibilidad para la continuidad de la actividad empresarial con una seguridad inigualable y una experiencia de usuario perfecta

Zscaler Resilience, como parte de la plataforma general, brinda a nuestros clientes redundancia dentro de la plataforma sin necesidad de servicios externos adicionales. Zscaler se compromete a brindar una experiencia continua y sin problemas para los usuarios y los equipos de TI mediante la inversión continua en las soluciones Zscaler Resilience.

Para conocer las últimas novedades sobre Zscaler Resilience, visite zscaler.es/resilience.

Beneficios clave de la recuperación ante desastres de Zscaler

- Interrupción mínima de las operaciones de los clientes durante un evento de desastre
- Acceso a aplicaciones de misión crítica incluso durante un evento de cisne negro • Mayor confiabilidad de la solución para el acceso a la aplicación con Zscaler
- Ahorro de costes al tener una plataforma para administrar el acceso a la aplicación durante el funcionamiento normal y en casos de DR
- Ahorros potenciales al evitar la pérdida de productividad debido a brechas durante un desastre

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