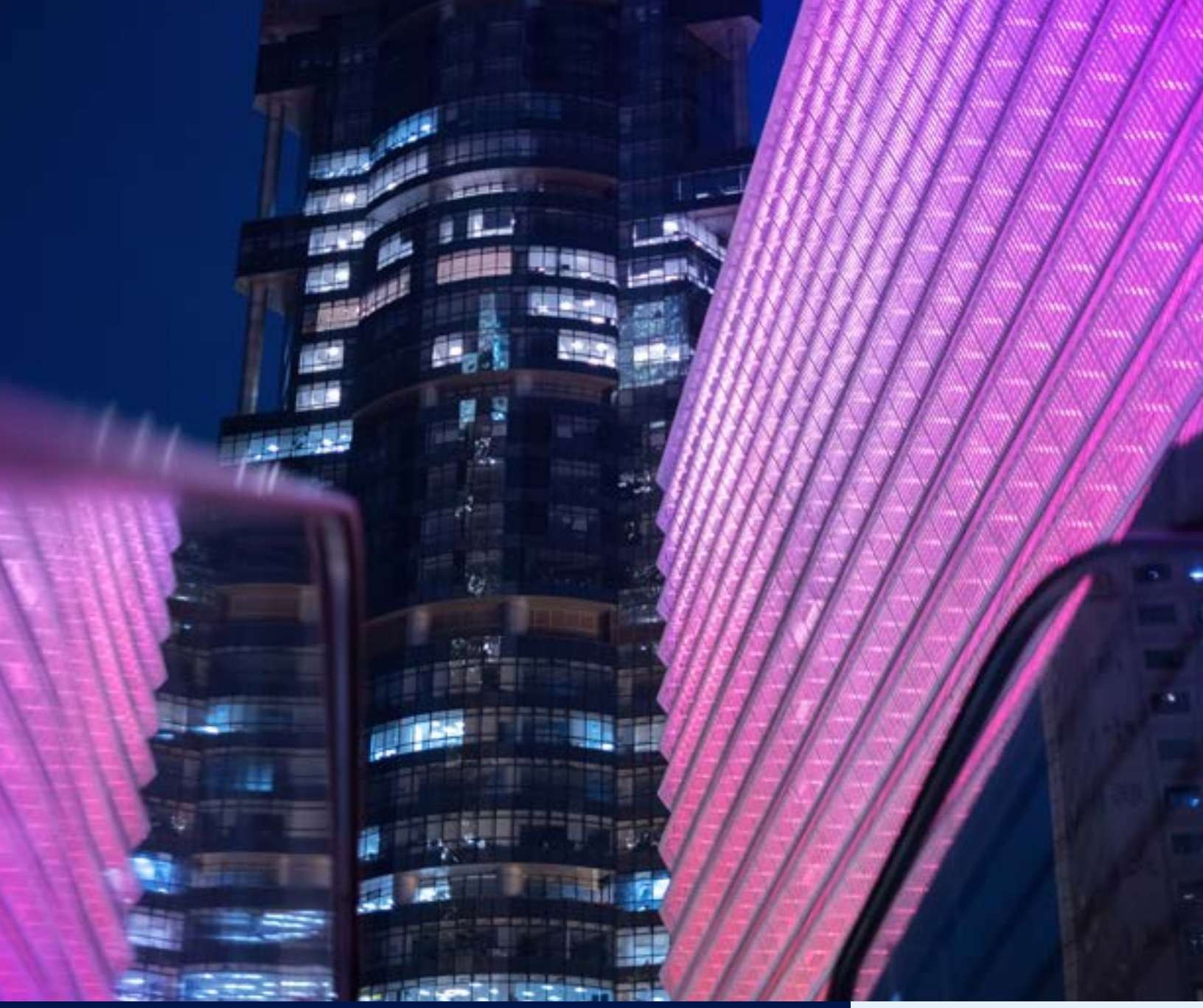

Zscaler Resilience™

Continuidad comercial ininterrumpida durante blackouts, brownouts y eventos catastróficos

Resumen de la solución

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 de la actividad empresarial 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 en periodos de normalidad empresarial. 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 la continuidad de la actividad empresarial ininterrumpida para los clientes durante blackouts, brownouts y eventos catastróficos. Se basa en la arquitectura avanzada de Zscaler Zero Trust Exchange™ y se optimiza con excelencia operativa para ofrecer alta disponibilidad y capacidad de servicio a los clientes en todo momento. Las capacidades de recuperación ante desastres de Zscaler, controladas por el cliente, junto con un potente conjunto de opciones de conmutación por error, respaldan los esfuerzos de planificación de la continuidad de la actividad empresarial de los clientes en todos los escenarios de fallo. Este completo conjunto de capacidades de resiliencia convierte a Zscaler en la nube de seguridad más segura y resiliente 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 nube misma se construya sobre una infraestructura eficaz y cuente con sólidos procesos operativos para las funciones empresariales diarias. La nube de Zscaler gestiona de forma autónoma numerosos fallos menores (caídas de nodos, problemas de disco, etc.) sin interacción alguna por parte del cliente, pérdida de conectividad ni disminución del rendimiento. Nuestros robustos sistemas de hardware, diseñados específicamente para este fin, con sobreaprovisionamiento de capacidad de procesamiento y redundancia, sientan las bases para una alta resiliencia.

Resiliencia en 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 de los medios para que los usuarios puedan acceder a las aplicaciones o los datos. Cuando se interrumpe el acceso a la nube, es necesario encontrar una ruta alternativa óptima para las aplicaciones. Esta optimización representa un conjunto de acciones manuales o autónomas que se pueden aplicar para abordar fallos que van desde una caída en el rendimiento de la red hasta interrupciones totales del servicio. Zscaler Resilience es un conjunto completo de capacidades que garantiza la continuidad de la actividad empresarial ininterrumpida ante cualquier tipo de fallo, desde eventos menores hasta fallos catastróficos.

Garantizar la resiliencia a la nube en escenarios de error

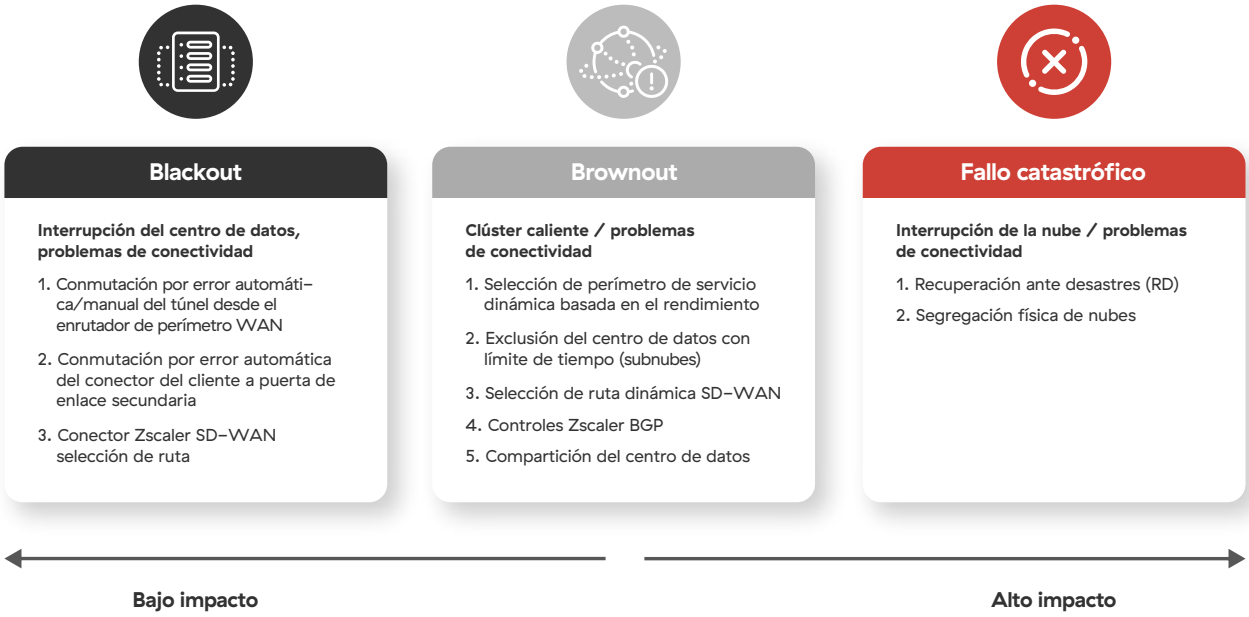

Figura 1: Múltiples opciones para responder a escenarios de error

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 esenciales mientras otorga acceso zero trust a Internet, SaaS y aplicaciones privadas, incluso durante desastres.

Experiencias perfectas en todos los escenarios de errores

Gestione blackouts, caídas de tensión y errores catastróficos con facilidad aprovechando la mejor arquitectura de su clase y la excelencia operativa de Zero Trust Exchange.

Costes y complejidad reducidos

Evite las interrupciones de la actividad empresarial y las pérdidas de productividad que causa el no poder acceder a aplicaciones críticas y, al mismo tiempo, elimine los costes de la infraestructura de respaldo heredada y las VPN locales.

Blackouts

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 un 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 disponiendo de un túnel IPsec/GRE de respaldo listo para funcionar cuando el principal sea inaccesible. La activación de 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 se vuelve inaccesible o supera un umbral de latencia (con las comprobaciones de estado de L7 habilitadas). Con dispositivos más básicos, los clientes tendrían que habilitar manualmente el túnel de respaldo. Una vez que el centro de datos principal esté operativo, es responsabilidad del cliente volver a conmutar.

Tráfico Zscaler Client Connector: al enviar tráfico mediante Zscaler Client Connector, Zscaler controla ambos extremos del túnel y realiza una conmutación por error automática de la puerta de enlace principal a la secundaria mediante la lógica del archivo PAC del Perfil de Aplicación. Zscaler Client Connector (ZCC) revertirá a la puerta de enlace principal una vez que sea accesible. En ciertos casos, los clientes pueden modificar manualmente los archivos PAC para activar una conmutación por error.

Brownouts

Una caída involuntaria o inesperada en la calidad del servicio de red generalmente constituye una brownout. La mala gestión de una brownout puede ser cara, tanto en términos de pérdida de ingresos como de productividad: si los usuarios detectan una brownout antes de que el equipo de TI la haya descubierto y comenzado a trabajar para resolverla, puede generarse una gran frustración en los usuarios, haciendo que todo se ralentice. Además de las formas que Zscaler tiene de abordar los blackouts, también ayuda a mitigar las caídas de tensión de otras maneras que se mencionan a continuación.

Selección dinámica de borde de servicio basada en el rendimiento de Zscaler
El conector de cliente de Zscaler selecciona la ruta óptima entre el borde de servicio ZIA principal y el secundario, independientemente de la proximidad geográfica, y se basa en el estado de cada borde de servicio ZIA, como se muestra en la figura 2. Una conexión HTTP de extremo a extremo calcula la latencia mediante un ping continuo a ambas puertas de enlace. Con esto, Zscaler ofrece una selección de centro de datos basada en la latencia para abordar eficazmente las caídas de tensión.

Exclusión de centros de datos controlada por el cliente
Otra forma de mantener la continuidad de la actividad empresarial durante caídas de tensión 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 emparejamiento de aplicaciones SaaS en LAX (que podría tardar horas en solucionarse),

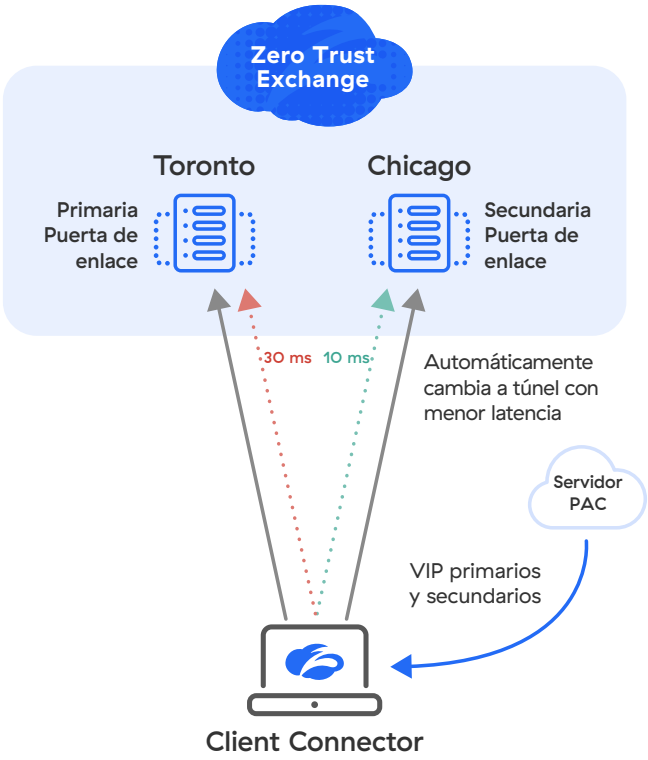

Figura 2: La selección dinámica de servicio perimetral basada en el rendimiento

dicho centro de datos puede excluirse de la nube secundaria en el portal de administración. Zscaler Client Connector obtiene entonces la nueva puerta de enlace principal y secundaria, y establece un túnel Z a un nuevo centro de datos. Esta exclusión de centro de datos controlada por el cliente tiene un límite de tiempo y vuelve al centro de datos seleccionado originalmente después de un tiempo predeterminado.

Conmutación por error de túnel desde dispositivos de enrutamiento que detectan caídas de tensión
Al enviar tráfico desde una oficina utilizando un dispositivo de enrutado/SD-WAN sobre el que Zscaler no tiene control directo, las opciones del cliente dependen de las capacidades del dispositivo perimetral. Por ejemplo, un enrutador SD-WAN puede detectar la degradación del servicio mediante algoritmos propietarios basados en comprobaciones de estado de L7 para los terminales sondeo de Zscaler. Al detectar una posible brownout, el dispositivo SD-WAN puede conmutar 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 ofrezcan mejores resultados.

Controles BGP de Zscaler
Nuestra arquitectura redundante (centros de datos neutrales con múltiples proveedores e intercambio de internet [IX]) es muy eficaz para minimizar caídas de tensión, congestión u otros problemas con un solo proveedor. Cuando Zscaler CloudOps detecta que un ISP ascendente ofrece un enrutamiento deficiente, podemos redirigir el tráfico a través de un ISP secundario mientras trabajamos con el principal para resolver el problema.

Envío de carga de centro de datos de 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.

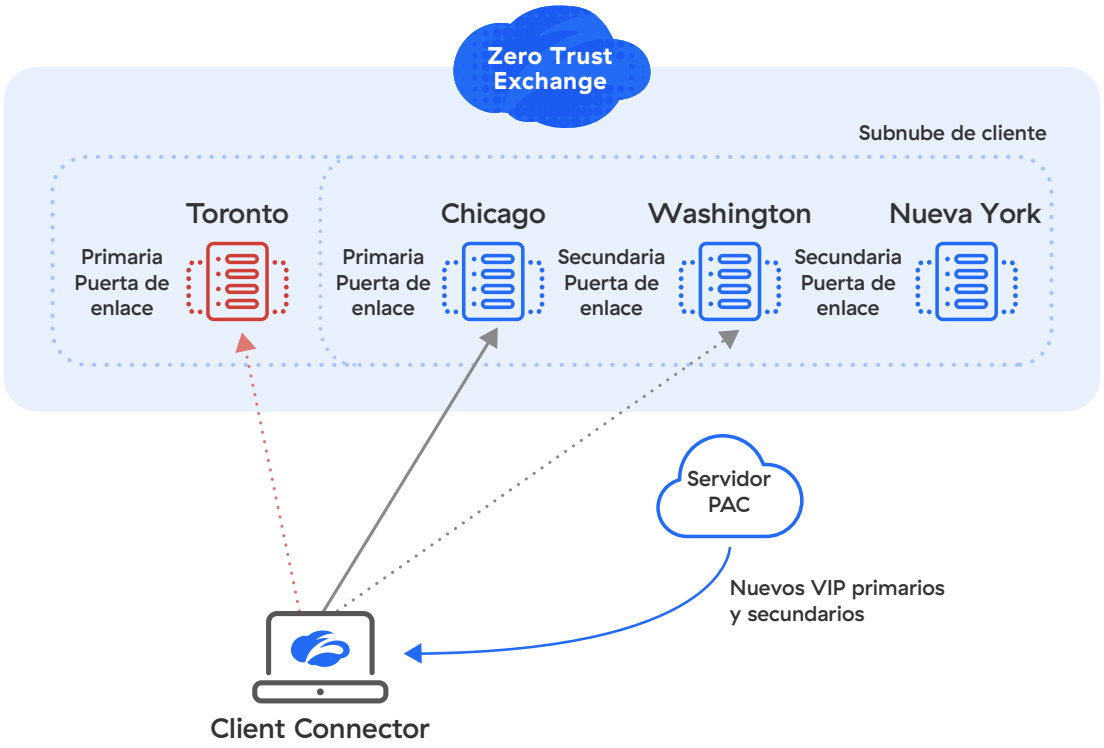

Figura 3: Exclusión del centro de datos controlada por el cliente

Fallos catastróficos

Zscaler Business Continuity para ZIA/ZPA

Zscaler Business Continuity 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.

Las organizaciones necesitan acceso ininterrumpido a las aplicaciones, sin comprometer la seguridad zero trust durante desastres o períodos de acceso degradado a la infraestructura. Además, en muchos sectores es necesario cumplir con los estándares regulatorios y de cumplimiento para la continuidad de la actividad empresarial.

Para satisfacer estas necesidades, Zscaler ofrece la opción de una nube privada de continuidad empresarial para mantener a las organizaciones operativas, incluso durante un evento catastrófico que pueda afectar la nube pública de Zscaler.

Si la nube pública de Zscaler no está disponible o no se puede acceder a ella, los clientes pueden cambiar al modo de continuidad de la actividad empresarial. En este estado, las políticas y la autenticación de usuarios continúan siendo aplicadas por los servicios de Zscaler, que se ejecutan en una máquina virtual alojada por el cliente.

Continuidad de la actividad empresarial para ZIA

Para brindar acceso ininterrumpido a Internet y a las aplicaciones SaaS, y mantener el cumplimiento, Zscaler ofrece la capacidad de realizar una conmutación por error a una nube de continuidad comercial privada que incluye perímetros de servicio privados ZIA alojados por el cliente y memorias caché de políticas privadas.

Los PSE brindan un procesamiento de tráfico consistente y son compatibles con funciones como inspección de tráfico y cortafuegos para los usuarios que ejecutan Zscaler Client Connector. En caso de interrupción, estos perímetros de servicio privados están respaldados por una memoria caché de política privada que contiene una copia en memoria caché de la configuración del cliente.

Para los clientes que no desean implementar capacidades autohospedadas, la solución de continuidad de la actividad empresarial estándar de Zscaler permite el acceso continuo a la web y a las aplicaciones SaaS en caso de una interrupción. Los clientes pueden elegir una de tres opciones en este escenario:

Fallo abierto: acceso a Internet sin restricciones de seguridad

Lista de permitidos predefinida: acceso sin restricciones a un conjunto limitado de aplicaciones comunes

Fallo cerrado: todo acceso a Internet queda bloqueado mientras dure la interrupción.

Continuidad empresarial para ZPA

Para tener acceso ininterrumpido a aplicaciones privadas durante una interrupción, los clientes pueden optar por implementar su propia nube privada de continuidad de la actividad empresarial, que son agrupaciones lógicas de los siguientes componentes, cada uno de los cuales se puede implementar en un grupo para redundancia adicional:

Controladores de nube privada que sincronizan continuamente la configuración y las políticas con la nube Zscaler

Perímetros de servicio privados ZPA que proporcionan funcionalidad ZPA pública en el entorno de una organización

Conectores de aplicaciones para acceso seguro a servicios privados

Receptores de registro para capturar salidas de registro de otros componentes

En el caso de una interrupción catastrófica o si la nube Zscaler se vuelve inaccesible, los usuarios se conectarán automáticamente a los controladores de nube privada para su autenticación y redirección a los perímetros de servicio privado ZPA. Una vez conectado al PSE, el canal de control y datos será con el PSE ZPA.

Los controladores de nube privada, implementados como una máquina virtual, brindan funciones críticas en caso de interrupción:

- Redirección de autenticación
- Redirección de usuarios
- Servicio de transmisión de registros
- Sincronización de la configuración del cliente
- Sincronización de políticas de clientes

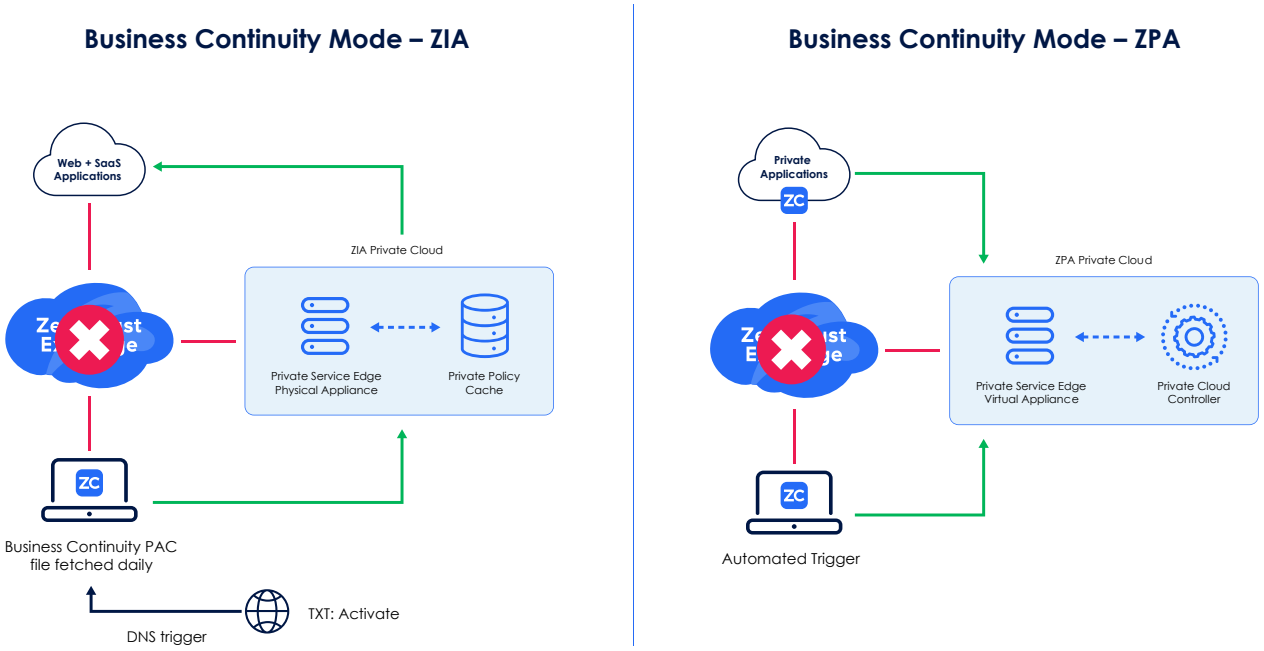

Figura 4: Nubes privadas de continuidad empresarial para acceder a todas las aplicaciones con total seguridad

Continuidad de la actividad empresarial para terminales

Otro problema que puede resultar catastrófico para una organización es la incapacidad de usar sus terminales habituales (ordenadores portátiles, ordenadores de sobremesa, etc.) cuando estos no están disponibles por cualquier motivo: fallan, faltan o están comprometidos. Para abordar este escenario, se puede implementar Zscaler Cloud Browser Isolation para brindar acceso seguro basado en navegador a aplicaciones privadas, web o SaaS desde terminales no administrados (como dispositivos propios del usuario), sin riesgo de pérdida de datos.

Zscaler Business Continuity, en conclusión

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 zero trust a través de Zero Trust Exchange. Zscaler Digital Experience detecta errores menores, blackouts 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 Business Continuity, como parte de la plataforma general Zscaler, brinda a los clientes redundancia dentro de la plataforma sin la necesidad de soluciones adicionales de terceros. Zscaler se compromete a brindar una experiencia continua y sin fisuras para los usuarios y los equipos de TI mediante la inversión continua en las soluciones de resiliencia Zscaler.

Beneficios clave de las soluciones de continuidad de la actividad empresarial de Zscaler

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

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

zscaler™ | Experience your world, secured.™

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