zscaler

THE RESILIENCE FACTOR

La confianza empresarial global en la resiliencia cibernética es injustificada

Un nuevo informe de Zscaler, **Descubra el potencial de resiliencia: por qué "Resilient by Design" es el próximo imperativo de ciberseguridad**, destaca la necesidad de una mayor priorización e inversión para garantizar que las estrategias de ciberresiliencia estén preparadas para futuros escenarios en los que, inevitablemente, se producirán errores.

PRINCIPALES CONCLUSIONES

En un contexto de crecientes amenazas y un entorno operativo cada vez más volátil, la continuidad de la actividad empresarial está bajo ataque.

45 % de las organizaciones sufrieron un **fallo significativo** en los últimos 6 meses

60 % de las organizaciones esperan sufrir un fallo significativo en los **próximos 12 meses**

Los líderes de TI se sienten bien preparados para este tipo de escenarios de error.

49 % de los líderes de TI creen que su infraestructura de TI es **altamente resiliente**

78 % etiquetan el enfoque de su organización hacia la resiliencia cibernética de forma **madura**

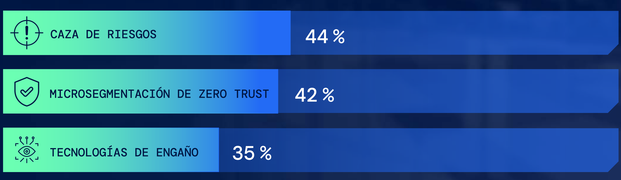
94 % creen que sus medidas actuales de resiliencia cibernética son **eficaces**

Pero un examen más detallado revela inconsistencias, lagunas e ineficiencias

SOLO **45 %** de los líderes de TI dicen que su estrategia de resiliencia cibernética está **al día** en respuesta al auge de la IA

40 % admiten **no haber revisado** su estrategia de ciberresiliencia en los últimos 6 meses

Menos de la mitad de las organizaciones utilizan cada una de las siguientes herramientas de seguridad proactiva



La falta de inversión en liderazgo se identifica como un punto de fricción

SÓLO EL 39 % de los líderes de TI cree que la ciberresiliencia es una prioridad máxima para el liderazgo

El 49 % está de acuerdo en que el presupuesto asignado a la ciberresiliencia no satisface la creciente necesidad

SÓLO EL 36 % dice que la estrategia de resiliencia cibernética está incluida dentro de la estrategia de resiliencia general de su organización.

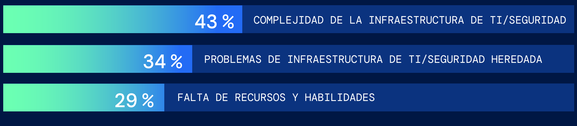
SÓLO EL 44 % dice que el CISO participa activamente en la planificación de la resiliencia

Se requiere un cambio de mentalidad a fin de superar las barreras clave para implementar una estrategia potente en relación a la resiliencia cibernética

El 60 % de los líderes de TI creen que su organización da demasiado prioridad a la prevención en su estrategia de ciberseguridad

El 57 % afirma que sus líderes continúan definiendo el fallo de seguridad cibernética como el acceso inicial (por parte de un autor de amenazas)

Las tres principales barreras para volverse más resiliente:



Incorporar la ciberresiliencia a la estrategia empresarial desde el principio

Los líderes de TI pueden ver la correlación entre una estrategia sólida de resiliencia cibernética y un desempeño comercial más fuerte, pero están teniendo serias dificultades para lograr resultados con los esfuerzos actuales.

56 % están siendo testigos de una **reducción** en la pérdida de datos

53 % están experimentando una recuperación de incidentes **más rápida**

49 % Indican una mayor celeridad en la detección y la contención de incidentes

El contexto empresarial actual exige que las organizaciones presten más atención a la resiliencia cibernética: que la financien mejor, la revisen con mayor frecuencia y aumenten sus expectativas al respecto. Es necesario un cambio fundamental en el enfoque y la mentalidad para que la resiliencia cibernética sea una parte vital de la estrategia de seguridad desde la base, lo que se conoce como **« Resilient by Design ».**

Obtenga más información sobre cómo adoptar un enfoque con « Resilient by Design », habilitado por la plataforma Zero Trust Exchange, aquí. Lea el informe

METODOLOGÍA

En diciembre de 2024, Zscaler encargó a Sapio Research que realizara una encuesta a 1700 ejecutivos encargados de la toma de decisiones de TI (líderes de TI) en 12 mercados (Australia, Francia, Alemania, India, Italia, Japón, Países Bajos, Singapur, España, Suecia, Reino Unido e Irlanda, EE. UU.). Estos líderes de TI trabajan en empresas con más de 500 empleados y en sectores diferentes.

ACERCA DE ZSCALER

Zscaler acelera la transformación digital para que los clientes puedan ser más ágiles, eficientes, resilientes y seguros. Zero Trust Exchange de Zscaler protege a miles de clientes de ciberataques y de la pérdida de datos gracias a la conexión segura de los usuarios, dispositivos y aplicaciones ubicados en cualquier lugar. Distribuido en más de 160 centros de datos en todo el mundo, Zero Trust Exchange basado en SSE es la mayor plataforma de seguridad en línea en la nube del mundo.

zscaler