Guardians of digital trust
Mes de Concientización sobre la Ciberseguridad

La creciente brecha entre organizaciones ciberresilientes y no resilientes y cómo BDO puede ayudar a reducirla

BDO

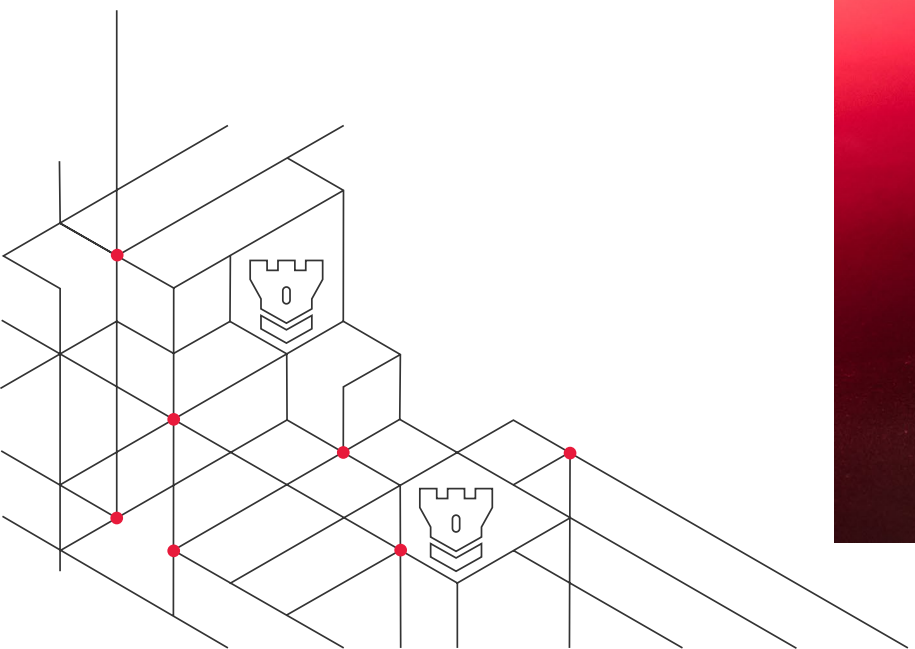
La creciente brecha entre organizaciones ciberresilientes y no resilientes y cómo BDO puede ayudar a reducirla

A lo largo de 2024, ciberataques de interrupción de negocio como el ransomware han afectado a organizaciones de sectores como la danesa WS Audiology, Transport for London, la estadounidense Dicks Sporting Goods, el aeropuerto SeaTac de Seattle y cientos más.

Frente a esta creciente amenaza, la ciberresiliencia -la capacidad de mantener las operaciones a pesar de los ciberataques- se ha vuelto crucial.

Con amenazas cibernéticas cada vez más complejas y frecuentes, la brecha entre organizaciones resilientes y no resilientes se está ampliando. Incidentes recientes destacan los importantes efectos de los ciberataques en la reputación, las finanzas, las operaciones y las partes interesadas.

El Foro Económico Mundial incluye los ciberataques entre los principales riesgos mundiales, y la pandemia COVID-19 ha aumentado la exposición de las organizaciones a estos riesgos.



Comprendiendo la ciberresiliencia

La ciberresiliencia va más allá de la ciberseguridad tradicional, que se centra principalmente en la prevención de ataques. En su lugar, abarca un enfoque holístico que incluye la capacidad de prepararse, responder y recuperarse de los incidentes cibernéticos. Una organización ciberresiliente no sólo es capaz de defenderse de los ataques, sino también de garantizar la continuidad y la rápida recuperación cuando se producen vulneraciones.

La ciberresiliencia comienza mucho antes de que se produzca un posible incidente y requiere una gestión informada del riesgo, tomando decisiones basadas en un conocimiento profundo de los riesgos. La gestión informada del riesgo implica recopilar y analizar toda la información pertinente, aprender de los incidentes y tomar decisiones bien fundadas que minimicen los posibles efectos negativos en la organización.

Los elementos esenciales de una gestión informada del riesgo son:

01

Identificación de riesgos
Reconocer los riesgos potenciales que pueden afectar a la organización

02

Evaluación de riesgos
Evaluar la probabilidad y el impacto de esos riesgos

03

Priorización de riesgos
Determinar qué riesgos requieren atención inmediata en función de su impacto potencial

04

Reducción de riesgos
Aplicar una estrategia para reducir o gestionar los riesgos identificados

05

Control continuo
Control continuo, revisar y actualizar periódicamente la estrategia de gestión de riesgos elegida para adaptar la nueva información o las circunstancias cambiantes.

Con este planteamiento de gestión de riesgos, el programa de seguridad desarrollada funciona de forma continua en toda la organización, incluyendo:

01

Prevención

Implantar medidas sólidas de ciberseguridad para frustrar los ataques.

02

Detección

Identificar y evaluar rápidamente las ciberamenazas.

03

Respuesta

Gestionar y mitigar eficazmente el impacto de los incidentes cibernéticos..

04

Recuperación

Restablecer rápidamente la normalidad y aprender de los incidentes para mejorar la capacidad de resiliencia en el futuro.

¿Qué diferencia hay entre organizaciones ciberresistentes y no ciberresistentes?

Según el último informe del Foro Económico Mundial[1], cada vez es mayor la brecha entre las organizaciones ciberresilientes y las que aún no han adoptado las medidas adecuadas. Panorama mundial de la ciberseguridad.

El informe constata un aumento de la desigualdad cibernética. El 90% de los ejecutivos encuestados en la Reunión Anual del Foro Económico Mundial sobre Ciberseguridad para 2023, declaró que era necesario actuar urgentemente para hacer frente a la brecha.

Algunas organizaciones están más preparadas y son más proactivas que otras a la hora de hacer frente a los ciberriesgos y crear ciberresiliencia. Según el informe, sólo el 17% de las organizaciones se consideran líderes en ciberresiliencia, mientras que el 74% son todavía novatas en este campo. Los líderes ciberresilientes tienen una estrategia cibernética clara y completa, una cultura cibernética fuerte y solidaria, la capacidad de atraer talento, una capacidad tecnológica cibernética sólida y ágil, y un programa de gobernanza cibernética eficaz y responsable. Por otro lado, los novatos en ciberresiliencia carecen de una o más de estas dimensiones y son más propensos a sufrir infracciones, interrupciones y pérdidas cibernéticas.

El auge de las nuevas tecnologías amplificará los retos ya existentes, al igual que la creciente brecha en las competencias cibernéticas y la escasez de talentos. La IA generativa sin duda hará avanzar los ciberataques en los próximos años; pero al mismo tiempo puede ayudar a las organizaciones a protegerse mejor.

[1] Las tendencias en ciberseguridad que los líderes deberán afrontar en 2024 | Foro Económico Mundial (weforum.org)

La importancia de la ciberresiliencia

Nunca se insistirá lo suficiente en la importancia de la ciberresiliencia en un mundo en el que los avances tecnológicos se adoptan a un ritmo acelerado y en el que las ciberamenazas son omnipresentes y cada vez más sofisticadas. Las consecuencias de los incidentes cibernéticos pueden ser graves, desde pérdidas financieras y trastornos operativos hasta daños a la reputación y sanciones reglamentarias.

01

Protección financiera

Los ciberataques pueden provocar importantes pérdidas económicas. Las organizaciones ciberresilientes están mejor posicionadas para mitigar estos costes mediante una rápida recuperación y la continuación de sus operaciones.

02

Continuidad operativa

Mantener las operaciones empresariales durante y después de un ciberataque es crucial. La ciberresiliencia garantiza la continuidad de las funciones críticas, minimizando el tiempo de inactividad y las interrupciones.

03

Integridad reputacional

La confianza es un activo valioso. Las organizaciones que demuestran una sólida ciberresiliencia tienen más probabilidades de mantener la confianza de sus clientes.

04

Cumplimiento normativo

Muchas industrias están sujetas a normativas estrictas en materia de protección de datos y ciberseguridad. Las organizaciones con ciberresiliencia están mejor preparadas para cumplir estas normativas y evitar sanciones.

Perspectivas mundiales de la ciberresiliencia

Instituciones mundiales como los gobiernos y el Foro Económico Mundial (FEM) reconocen la necesidad crítica de ciberresiliencia y ofrecen asesoramiento para ayudar a las organizaciones a reforzar sus defensas.

01

Iniciativas gubernamentales:

- Marco de ciberseguridad del NIST: El Instituto Nacional de Normas y Tecnología de Estados Unidos (NIST) ofrece un marco completo para mejorar las prácticas de ciberseguridad, ampliamente adoptado en todos los sectores.
- Directiva de la UE sobre seguridad de las infraestructuras de red y de los sistemas de información (NIS2): Las organizaciones de sectores críticos como la energía, el transporte, la banca y la salud van a tener que aplicar medidas adecuadas y proporcionales para gestionar los riesgos para la seguridad.
- Ley sobre ciberseguridad de la UE: La Ley de Ciberseguridad de la Unión Europea pretende reforzar la seguridad de los productos y servicios digitales, promoviendo un alto nivel de ciberresiliencia en todos los Estados miembros.
- La ASEAN aún no cuenta con una ley o directiva única y unificada sobre ciberseguridad. Sin embargo, ha desarrollado una estrategia integral de cooperación en ciberseguridad para 2021-2025, centrada en avanzar en la preparación cibernética, armonizar las ciberpolíticas regionales, aumentar la confianza en el ciberespacio y crear capacidad regional.
- La Comisión Económica para América Latina y el Caribe de las Naciones Unidas (CEPAL) ha integrado la ciberseguridad en su Agenda Digital.

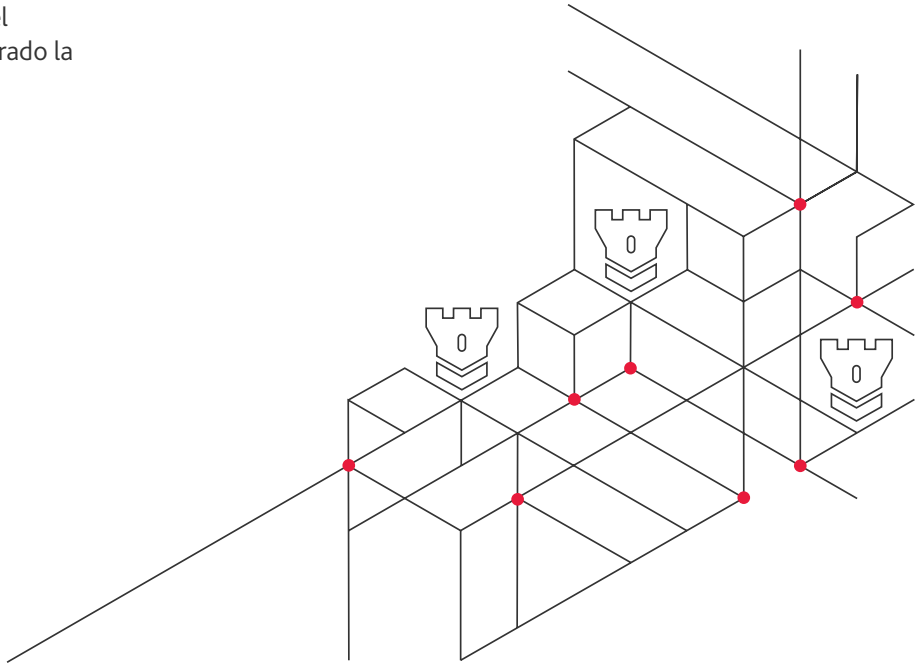
02

Foro Económico Mundial (FEM):

- El FEM subraya la importancia de las asociaciones público-privadas para mejorar la ciberresiliencia. Sus informes destacan la necesidad de un enfoque colaborativo para hacer frente a las ciberamenazas y recomiendan las mejores prácticas para aumentar la resiliencia.
- El Centro de Ciberseguridad del FEM aboga por la cooperación mundial y ofrece recursos y foros para que las organizaciones compartan conocimientos y estrategias sobre ciberresiliencia.

La nueva directiva europea Network and Information Security Directive 2 (NIS2) entrará en vigor en octubre de 2024. BDO ha desarrollado una clara herramienta de evaluación de NIS2 que puede proporcionarle una visión inmediata de su situación actual. Puede acceder a esta herramienta a través del siguiente botón.

WWW.NIS2SURE.COM



Estrategias para reforzar la Ciberresiliencia

Para salvar la creciente brecha, las organizaciones pueden tomar varias medidas proactivas, como:

01

Desarrollar un plan de ciberresiliencia

Cree un plan integral que describa las medidas preventivas, los protocolos de respuesta a incidentes y las estrategias de recuperación. Asegúrese de que el plan está en línea con la estrategia y los objetivos de la empresa; revíselo y actualícelo periódicamente para reflejar los cambios en el panorama cibernético y las necesidades de la empresa.

02

Invertir en cibertecnología

Como la gestión de la superficie de ataque y la postura, los controles de seguridad de datos, la IA centrada en la seguridad y el aprendizaje automático- que sea adecuada para el propósito, escalable, resiliente y segura, y que permita a la organización detectar, responder y recuperarse de las amenazas e incidentes cibernéticos, al tiempo que proporciona a los recursos valiosos la capacidad de descargar y automatizar ciertas tareas.

03

Fomentar una cultura de ciberseguridad

Fomentar una cultura de ciberseguridad: Alentar una cultura en la que la ciberseguridad sea una responsabilidad compartida, que faculte a todos los niveles de la organización.

04

Impartir formación periódica

Educar a los empleados sobre las mejores prácticas de ciberseguridad y la importancia de su papel en el mantenimiento de la ciberresiliencia. El 95 % de los ciberataques se deben a errores humanos, lo que subraya la enorme necesidad de formación y desarrollo internos a todos los niveles.

05

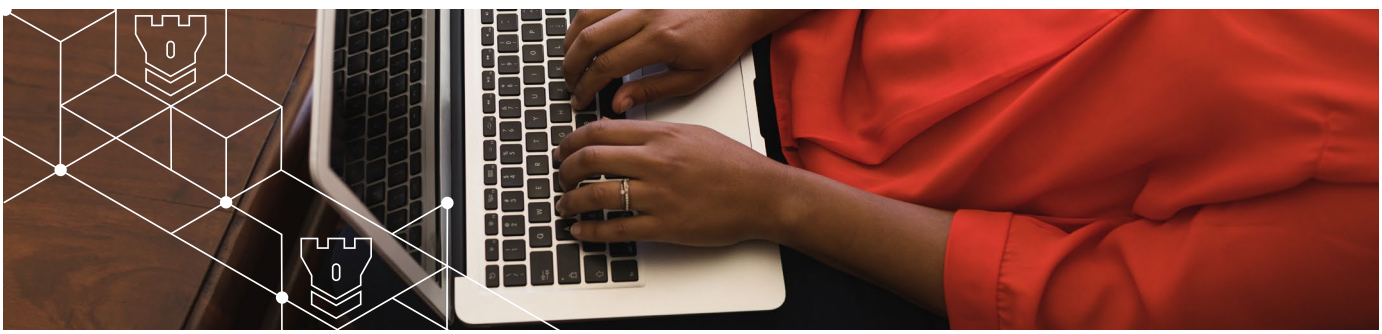
La creciente brecha entre organizaciones ciberresilientes y no ciberresilientes

Establecer una cibergobernanza que defina las funciones, responsabilidades y rendición de cuentas del consejo de administración, la dirección y el personal, y que proporcione políticas, normas y procedimientos claros y coherentes para la gestión del ciberriesgo y la supervisión, notificación y actuación en materia de cumplimiento.

06

Realizar auditorías y evaluaciones periódicas

Evaluar continuamente las medidas de ciberseguridad y las estrategias de resistencia para identificar y abordar las vulnerabilidades.



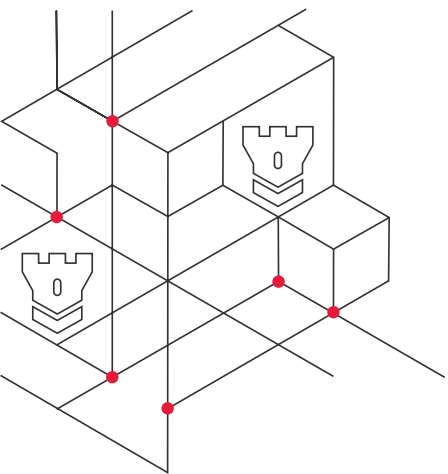
Conclusión

La creciente brecha entre organizaciones ciberresilientes y no ciberresilientes subraya la urgente necesidad de dar prioridad a la ciberresiliencia. Comprendiendo su importancia, aprovechando los conocimientos globales y aplicando medidas estratégicas, las organizaciones pueden salvaguardar sus activos, mantener la continuidad operativa y generar confianza en un mundo cada vez más digital.

Cultivar las mejores prácticas, atraer el talento adecuado e implantar tecnología a medida ayudará a crear la resiliencia necesaria.

Ya no se trata de si su organización estará en peligro, sino de cuándo lo estará. Ningún país u organización se librará de la ciberdelincuencia, por lo que es crucial que las partes interesadas de todo el mundo colaboren para ayudar a cerrar la brecha.

A medida que las ciberamenazas siguen evolucionando, también deben hacerlo nuestros planteamientos de resiliencia, garantizando que siempre estemos un paso por delante en el panorama de la ciberseguridad.



¿Cómo puede ayudar BDO?

Los fundamentos que los ciberprofesionales han puesto en marcha están funcionando. Práctica global de ciberseguridad de BDO está formado por profesionales de diversos ámbitos, incluidos consultores experimentados en TI, operaciones y privacidad de datos, así como profesionales de la tecnología forense, el asesoramiento empresarial y la contabilidad.

Estamos hechos para prestar servicios integrales y personalizados a cada cliente, centrándonos en su modelo operativo específico, sus exigencias técnicas, su entorno normativo y la dinámica del sector.

Ya se trate de servicios financieros, salud, comercio minorista, recursos naturales o cualquier otro sector, nosotros entendemos sus necesidades. Nuestra huella global se extiende a todos los rincones del planeta, al igual que la ciberdelincuencia. Permítanos ayudar a su organización, esté donde esté, a mitigar los riesgos cibernéticos a los que se enfrenta.

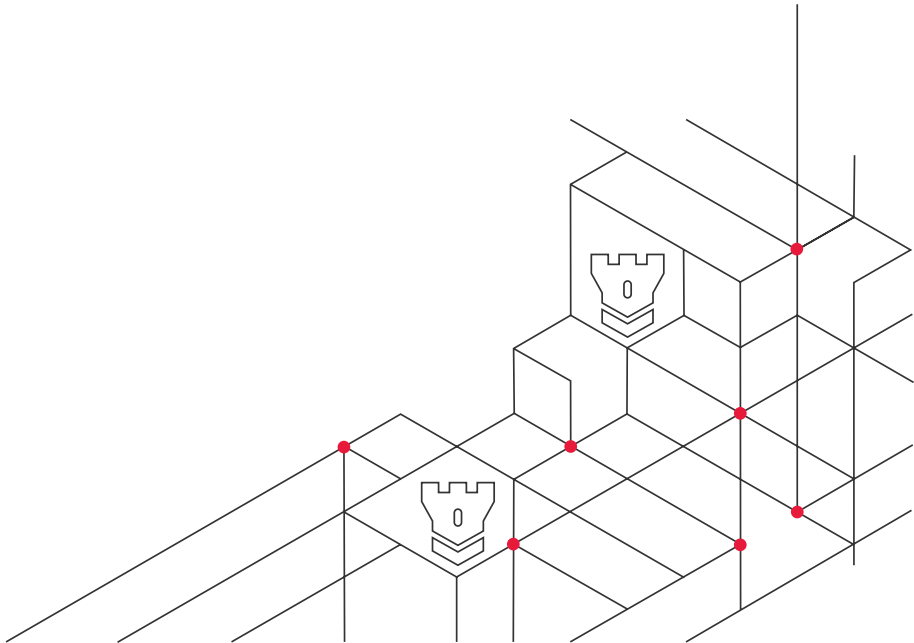
Rocco Galletto
Global Cybersecurity Leader

$9.22 billones de dólares
coste de la ciberdelincuencia mundial en 2023

Se prevé que el coste mundial de la ciberdelincuencia aumente hasta los **$23.84 billones de dólares en 2027,**
frente a los 8,44 billones de 2022 (Statista).

46%
porcentaje de organizaciones que pagan un rescate tras un ataque de ransomware

1.9 millones
número global de amenazas únicas reportadas por los usuarios finales en 2023



'BDO', 'we', 'us', and 'our' refer to one or more of BDO International Limited, its network of independent member firms ('the BDO network'), and their related entities.

The BDO network is an international network of independent public accounting, tax and advisory firms which are members of BDO International Limited and perform professional services under the name and style of BDO (hereafter: 'BDO member firms'). BDO International Limited is a UK company limited by guarantee. It is the governing entity of the BDO network.

Service provision within the BDO network is coordinated by Brussels Worldwide Services BV, a limited liability company incorporated in Belgium.

Each of BDO International Limited, Brussels Worldwide Services BV and the BDO member firms is a separate legal entity and has no liability for another entity's acts or omissions. Nothing in the arrangements or rules of the BDO network shall constitute or imply an agency relationship or a partnership between BDO International Limited, Brussels Worldwide Services BV and/or the

BDO member firms. Neither BDO International Limited nor any other central entities of the BDO network provide services to clients.

BDO is the brand name for the BDO network and for each of the BDO member firms.

© Brussels Worldwide Services BV October 2024