Guardians of digital trust
Mes de Concienciación sobre la Ciberseguridad

Principales amenazas para la ciberseguridad y predicciones para 2025

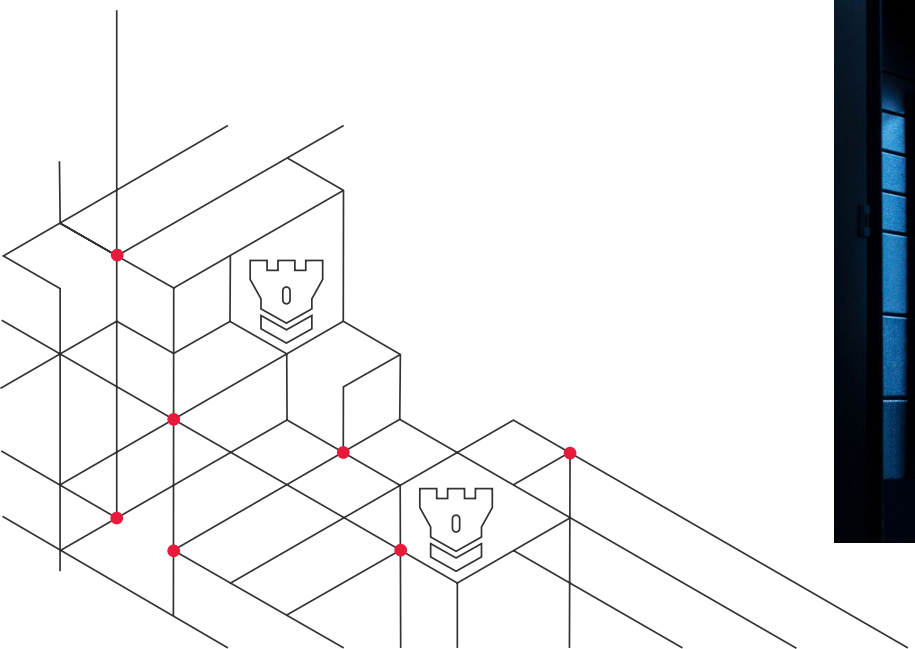
BDO

Principales amenazas para la ciberseguridad y predicciones para 2025

Las nuevas tecnologías han proporcionado a las empresas una mayor capacidad de análisis de datos, comunicación y eficiencia operativa. Sin embargo, también ha hecho más sofisticados a los actores de las amenazas, desde los agentes del estado-nación a los ciberdelincuentes. A medida que nuestro mundo está más interconectado digitalmente, asistimos a la integración de la inteligencia artificial en los ciberataques, lo que aumenta su gravedad.

Mantenerse un paso por delante en esta carrera digital exige adoptar medidas de vanguardia. Por ejemplo, aprovechar las soluciones de seguridad basadas en la IA Generativa puede mejorar drásticamente el funcionamiento de los equipos de seguridad, impulsando la eficiencia y reduciendo los riesgos. Las tecnologías de seguridad basadas en la IA Generativa pueden ayudar a hacer emerger los riesgos de mayor prioridad e impulsar procedimientos de respuesta automatizados. Estas soluciones pueden ayudar a su equipo de seguridad a liberar tiempo valioso, mejorar la detección e impulsar una respuesta y recuperación más rápidas para que su empresa siga prosperando.

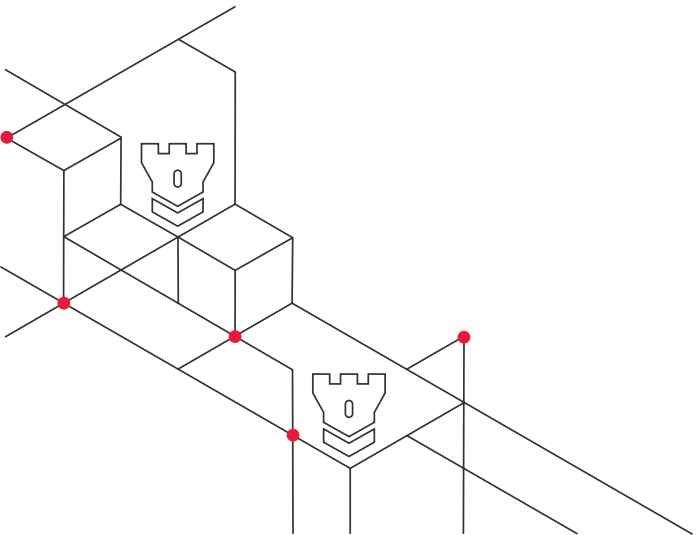
También es fundamental comprender las nuevas amenazas a las que se enfrentarán las empresas en 2025. En este artículo se analizan las mayores amenazas y las estrategias clave para ayudarle a mantenerse protegido.



El coste creciente de los ciberataques y la importancia de la resistencia

Según el Informe de IBM 2024 sobre el coste de una filtración de datos, los costes de las filtraciones aumentaron un 10% con respecto al año anterior, el mayor incremento anual desde la pandemia. Además, un 26% más de organizaciones se enfrentaron a graves carencias de personal en comparación con el año anterior y observaron un aumento medio de 1,76 millones de dólares en los costes de las infracciones, en comparación con las que no tenían problemas de personal de seguridad o tenían un nivel bajo. Este hallazgo resalta la alarmante brecha existente en la capacidad de las organizaciones para identificar, detectar y responder a las ciberamenazas antes de que la organización sienta su impacto. Sin embargo, hay algunas buenas noticias. El informe también revela que el 42% de las filtraciones de datos fueron descubiertas por los equipos de seguridad, lo que supone una mejora del 9% con respecto al año pasado. Este aumento se atribuye a una mayor inversión en planificación cibernética y detección de amenazas, así como a la adopción de tecnología de IA para colmar las lagunas de recursos.

Aunque estas mejoras son prometedoras, aún queda mucho por hacer. La evolución del panorama de las amenazas, alimentada por las tensiones geopolíticas y los métodos de ataque innovadores, resalta la necesidad de que las organizaciones desarrollen y sometan periódicamente a pruebas de resistencia sus planes de ciberresiliencia. Aprovechar las herramientas de IA puede liberar un tiempo valioso para que los equipos de seguridad se centren en la mejora continua de sus programas. Dotar a los equipos de herramientas y estrategias para lograr más con recursos limitados sigue siendo un reto fundamental.



¿Cuáles son las principales amenazas para la ciberseguridad de las empresas?

Su postura en materia de ciberseguridad no es sólo una preocupación informática, sino un aspecto fundamental de su estrategia y resistencia empresariales globales. La capacidad de navegar por la compleja red de amenazas a la ciberseguridad ya no es una cuestión de ventaja competitiva, sino una obligación legal y ética. Se han promulgado leyes y normativas estrictas que obligan a las empresas a mantenerse vigilantes y proactivas en la protección de sus datos para preservar su integridad y mantener la confianza y privacidad de sus clientes y socios.

Para mitigar eficazmente los riesgos, las organizaciones deben identificar y abordar las siguientes amenazas en 2025:

Actores estatales

Los actores estatales se encuentran entre los grupos más organizados y capaces del panorama de las ciberamenazas. Estos actores de amenazas invierten significativamente en capacidades cibernéticas, tanto ofensivas como defensivas, para obtener ventajas geopolíticas. Sus actividades dictan a menudo las tendencias generales de la ciberseguridad. Con las actuales tensiones geopolíticas en Europa del Este y el Pacífico Occidental, estos grupos seguirán marcando las nuevas tendencias en ciberseguridad.

Desde el punto de vista ofensivo, los actores estatales desarrollan plataformas y herramientas de ciberataque a menudo muy sensibles y secretas, destinadas a ser utilizadas de forma sigilosa en el momento y lugar de su elección. A veces, estos sistemas se hacen públicos o son expuestos y utilizados deliberadamente por bandas criminales o incluso aprovechados por otros actores estatales.

En el lado defensivo, organismos gubernamentales como la Securities and Exchange Commission (SEC) de Estados Unidos están endureciendo las normas de ciberseguridad para las empresas, en parte como respuesta a las sofisticadas amenazas que plantean los actores estatales. En este caso, los directivos de las empresas son directamente responsables de las medidas de ciberseguridad en las que invierten o dejan de invertir.

El doble papel de los actores estatales en el avance de las tecnologías cibernéticas ofensivas y defensivas puede tener un impacto desigual en las empresas.

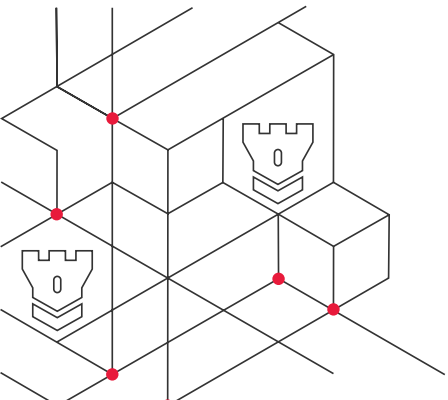
Ciberdelincuentes

Los grupos de ciberdelincuentes se centran a menudo en el beneficio económico y van desde sofisticados conjuntos, que a veces operan con cierto grado de respaldo estatal (para actuar como representantes), hasta equipos menos organizados pero altamente cualificados. Además, las herramientas utilizadas por los agentes estatales a veces caen en manos de estos delincuentes, deliberada o inadvertidamente, lo que aumenta aún más los riesgos.

Hackers individuales

En el otro extremo del espectro se encuentran los hackers individuales y los pequeños grupos, a menudo denominados hackers aficionados. Aunque sus motivos varían desde el activismo hasta el beneficio económico o la notoriedad, presentan retos organizativos diferentes. Las tecnologías que permiten el hacking son cada vez más accesibles a través de plataformas que «hackean como servicio», lo que permite incluso a individuos menos experimentados plantear un riesgo significativo.

MÁS INFORMACIÓN SOBRE LAS CIBERAMENAZAS A LAS MATERIAS PRIMAS



Comprender el panorama de las ciberamenazas: ¿Quiénes son los actores de la amenaza?

En el mundo interconectado de hoy en día, ninguna organización está completamente a salvo de las ciberamenazas, por lo que es imperativo que las empresas comprendan el cambiante panorama de las amenazas. Este ecosistema es una compleja red de diversos actores, cada uno con motivaciones y capacidades únicas, que plantean una serie de riesgos para la integridad financiera y operativa de las organizaciones.

Ciberespionaje

Esta amenaza encubierta implica el acceso no autorizado a sistemas y redes informáticos con la intención de recabar información sensible, lo que puede tener graves consecuencias. Pueden ir desde la pérdida de la reputación de una empresa o de una ventaja competitiva hasta el riesgo para la seguridad nacional. En este contexto, comprender las tácticas habituales de ciberespionaje es fundamental para aplicar contramedidas eficaces.

Compromiso del correo electrónico empresarial

Caracterizados por su engañosa sencillez, los ataques al correo electrónico empresarial consisten en hacerse pasar por una persona o entidad de confianza a través de la comunicación por correo electrónico para manipular a empleados, clientes o consumidores con el fin de que revelen información sensible o ejecuten transacciones financieras fraudulentas. A menudo, esto puede dar lugar a importantes pérdidas económicas y daños a la reputación.

Suplantación de credenciales

Los agentes de la amenazas utilizan nombres de usuario y contraseñas robados de un sitio web o servicio para acceder a otras cuentas, aprovechándose de personas que utilizan las mismas credenciales de inicio de sesión en varias plataformas. Esta táctica se basa en contraseñas reutilizadas, lo que la convierte en un método eficaz para comprometer cuentas y acceder a información confidencial.

Amenazas internas

Según un informe reciente de Verizon, la amenaza externa media compromete unos 200 millones de registros, mientras que los incidentes en los que interviene un actor interno han dado lugar a la exposición de 1.000 millones de registros o más. Se trata de una importante táctica de ciberamenaza en la que individuos con acceso autorizado a los sistemas y datos de una organización aprovechan su posición. Estas personas pueden ser empleados, contratistas o socios comerciales.

Ataques a la cadena de suministro

En estos ataques, los actores intentan comprometer a terceros vendedores o proveedores para acceder a los sistemas o datos de la organización objetivo. A continuación, pueden vulnerar la seguridad de toda la cadena de suministro, lo que puede dar lugar a filtraciones de datos, sistemas comprometidos u otras consecuencias adversas. La mitigación proactiva del riesgo es esencial para contrarrestar esta amenaza de múltiples capas y en constante evolución.

Cibersabotaje

Esta campaña implica actos deliberados para perturbar la infraestructura digital con la intención de comprometer la integridad, confidencialidad o reputación de la empresa objetivo por motivos ideológicos, personales o competitivos. Es crucial comprender qué tácticas hay que tener en cuenta a la hora de desarrollar estrategias de defensa eficaces contra el cibersabotaje. Familiarícese con las siguientes tácticas:

Ransomware

El Informe de Defensa Digital 2023 de Microsoft indica que las organizaciones se enfrentan a un aumento del índice de ataques de ransomware con respecto al año anterior: el número de ataques de ransomware perpetrados por personas aumentó en más de un 200 %. El ransomware se caracteriza por el cifrado o, en ocasiones, la modificación de datos críticos para exigir un rescate a las víctimas. Los ciberdelincuentes colaboran cada vez más, comparten herramientas y tácticas y tienden una red más amplia para atacar a organizaciones de todos los tamaños. Estos factores han contribuido a la creciente frecuencia y sofisticación de los incidentes de ransomware, lo que supone un riesgo significativo para las empresas y las infraestructuras críticas de todo el mundo.

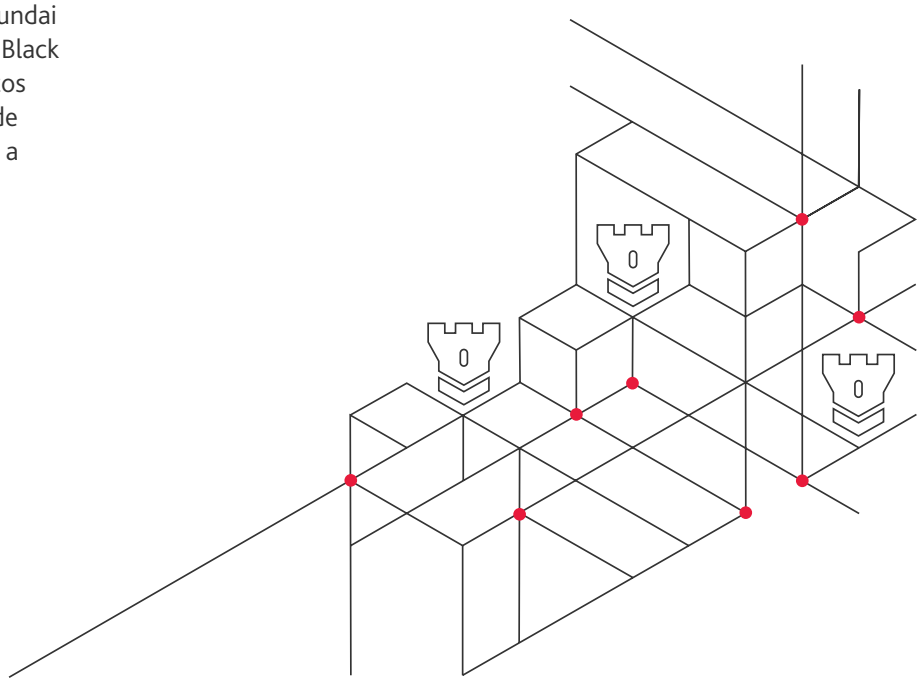
En octubre de 2023, la Biblioteca Pública de Toronto, la mayor red de bibliotecas de Canadá, fue víctima de un ataque de ransomware. Los ciberdelincuentes cifraron los sistemas informáticos de la biblioteca y robaron datos de los empleados, causando una interrupción generalizada de los servicios. En mayo de 2024, Ascension, uno de los mayores sistemas sanitarios sin ánimo de lucro de Estados Unidos, sufrió un ataque de ransomware que interrumpió sus operaciones durante semanas. Y en febrero, Hyundai Motor Europe sufrió un ataque de ransomware Black Basta en el que se robaron tres terabytes de datos corporativos. Estos son solo algunos ejemplos de incidentes que han afectado significativamente a organizaciones y personas de todo el mundo.

Denegación de servicio

Los ataques de denegación de servicio (DoS) tienen como objetivo interrumpir la disponibilidad de los servicios en línea o sitios web abrumando sus servidores con una avalancha de tráfico, haciéndolos inaccesibles para los usuarios legítimos. Para ello se suelen utilizar múltiples dispositivos comprometidos o una red de bots para generar peticiones o tráfico excesivos. El objetivo principal no es robar datos, sino causar trastornos operativos a la organización atacada.

Sabotaje del proceso

Estos ataques se centran en procesos dependientes de datos esenciales para el buen funcionamiento. Al alterar o borrar datos críticos, los ataques hacen que los protocolos operativos pierdan su eficacia. Por ejemplo, considere una flota de vehículos que operan bajo un estricto programa de mantenimiento. Si los registros de mantenimiento fueran manipulados o borrados, la disponibilidad de los vehículos podría verse comprometida, interrumpiendo toda la cadena logística.



Fraude cibernético

El ciberfraude, una amenaza omnipresente y en constante evolución, es un término genérico que engloba una amplia gama de actividades ilícitas cuyo objetivo es obtener beneficios económicos o comprometer datos. Las tácticas implican el uso de correos electrónicos y técnicas de ingeniería social para explotar las vulnerabilidades de una organización, lo que a menudo tiene consecuencias perjudiciales. Las contramedidas deben incluir protocolos de autenticación robustos, programas de concienciación de los empleados y sistemas de vigilancia para detectar actividades inusuales.

Exposición de credenciales

Tal vez una de las formas más elementales de fraude cibernético, la exposición de credenciales a menudo se manifiesta a través de intentos de phishing por correo electrónico, llamadas telefónicas o incluso mensajes de texto. Normalmente, la narración implica un requerimiento urgente de verificación de cuenta o un proceso de reembolso. La concienciación es la primera línea de defensa en este caso: saber, por ejemplo, que las instituciones financieras u organismos gubernamentales legítimos nunca solicitarán información personal a través de comunicaciones no solicitadas.

Adquisición de cuentas

La apropiación de cuentas (ATO) se produce cuando un actor malicioso obtiene el control de una cuenta legítima (bancaria, de correo electrónico, redes sociales) sin el permiso del propietario. A menudo es posible aprovechando puntos débiles en la autenticación o en las medidas de seguridad. La inercia humana en torno a los cambios de contraseña juega a favor de los estafadores. La ATO puede ser especialmente perjudicial para las organizaciones en las que los perfiles de los clientes en aplicaciones externas pueden monetizarse, como en los programas de fidelización.

Fraude en pagos

A menudo interconectado con el compromiso del correo electrónico empresarial, el fraude en los pagos tiene como objetivo iniciar transacciones financieras no autorizadas. Suele consistir en hacerse pasar por una entidad de confianza y solicitar a un responsable de cuentas por pagar que modifique los datos bancarios de un pago pendiente. El momento suele planificarse meticulosamente para que coincida con periodos en los que la vigilancia puede ser menor, como el fin de semana o cuando la alta dirección está fuera de la oficina.

Desinformación

Se trata de una potente forma de ataque digital que implica la difusión deliberada de información falsa o engañosa con la intención de engañar, manipular o causar confusión. Estas campañas utilizan a menudo canales en línea como las redes sociales, el correo electrónico y los sitios web, lo que subraya la importancia de la alfabetización mediática, el pensamiento crítico y la comprobación de los hechos.

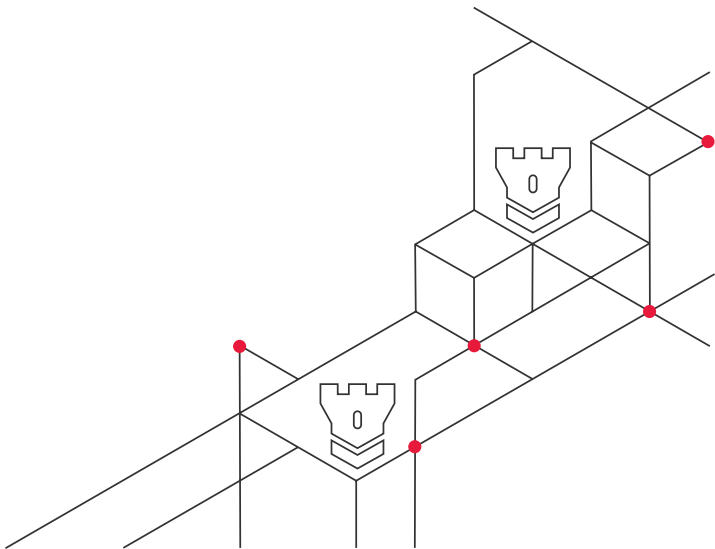
Las repercusiones de la desinformación son enormes, y van desde la pérdida de confianza y credibilidad del público hasta perjuicios económicos o sociales reales. Combatirla exige un planteamiento polifacético que implica vigilancia individual y acción colectiva. Utilizando las capacidades de protección contra riesgos digitales de su organización, como la inteligencia sobre ciberamenazas, puede detectar la desinformación a tiempo y acabar con ella para minimizar su impacto en la marca y el público. Los principales tipos de tácticas de desinformación son:

Mal uso de la marca

Los ciberdelincuentes o los actores maliciosos pueden utilizar la desinformación para empañar la reputación de una marca. Esto puede ir desde la difusión de reseñas e información falsas, la creación de cuentas falsas en redes sociales que suplanten la identidad de la marca o la creación de sitios web fraudulentos como si fueran legítimos. Estas tácticas pueden confundir a los clientes, perjudicar a la marca e incluso provocar pérdidas económicas.

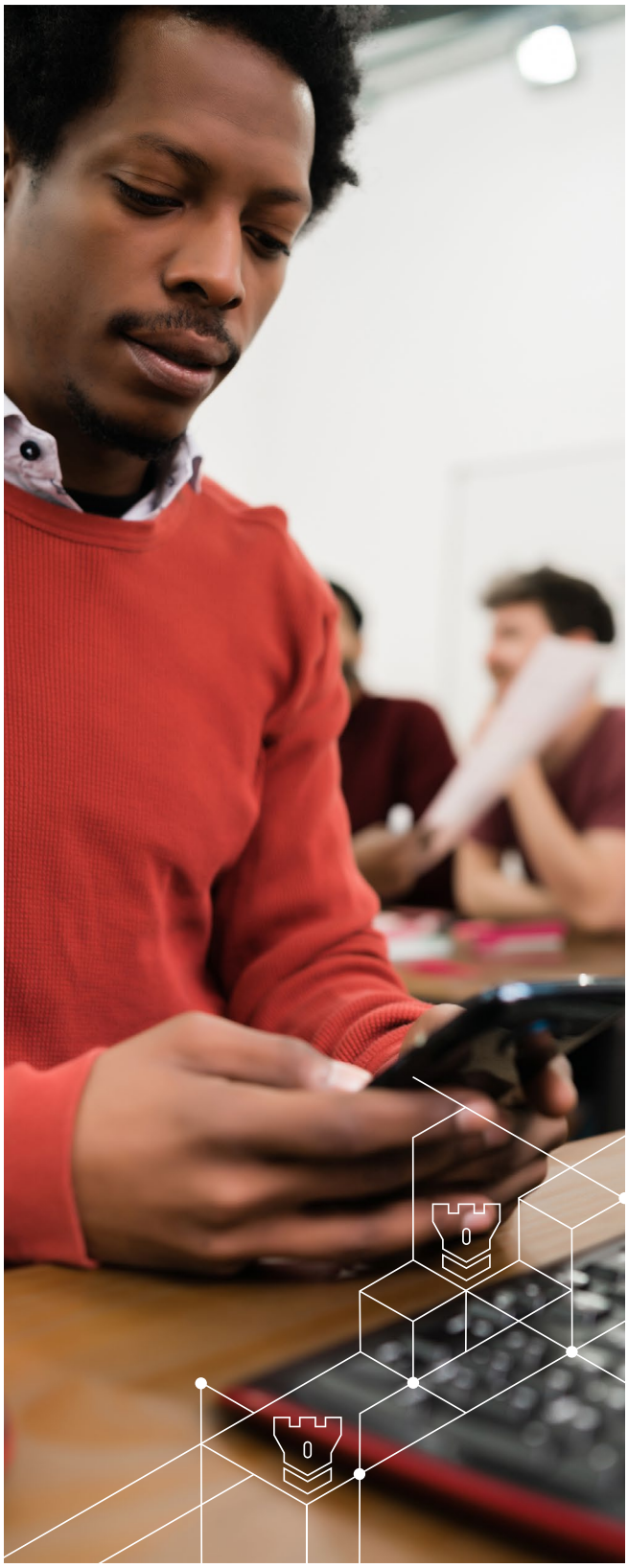
Fraude electoral

La desinformación también puede utilizarse como arma para perturbar el proceso democrático. Pueden distribuirse falsas narrativas o materiales manipulados para confundir a los votantes, debilitar a los candidatos o manipular los resultados electorales.



Buenas prácticas adicionales de ciberseguridad para las empresas

- Conocer los riesgos e identificar los puntos ciegos es el primer paso hacia la protección. Aplique medidas específicas para proteger los activos digitales de su organización detectando las vulnerabilidades y las posibles deficiencias de su infraestructura de seguridad.
- Supervise su exposición aprovechando la inteligencia para la detección temprana de amenazas, como la vigilancia de mercados y foros en línea ilícitos en los que los ciberdelincuentes suelen comerciar con datos robados.
- Supervise y gestione los comportamientos de la red 24 horas al día, 7 días a la semana, para impedir la entrada no autorizada en su infraestructura digital, reduciendo el riesgo de ciberamenazas y filtraciones de datos.
- Cumpla la normativa sobre privacidad y seguridad en constante evolución, para evitar repercusiones legales y financieras.
- Realice una evaluación de la continuidad y resistencia de su empresa. Evalúe la capacidad de su empresa y de sus proveedores para mantener las operaciones durante las interrupciones, a fin de garantizar la continuidad ininterrumpida del negocio frente a posibles ciberamenazas.
- Alinee los riesgos cibernéticos con su estrategia empresarial general, para ayudar a los consejos de administración y a los inversores a tomar decisiones informadas y asignar recursos de forma eficaz. Lea nuestro primer artículo de la serie: Cómo pueden los consejos mejorar sus conocimientos sobre ciberseguridad: seis estrategias para proteger a su organización de las ciberamenazas.
- La intrincada naturaleza del panorama de las ciberamenazas demuestra que abordar la ciberseguridad no es dominio exclusivo de los departamentos de TI. Por el contrario, se trata de una responsabilidad compartida que requiere estrategias integrales de gestión de riesgos en las que participen múltiples partes interesadas, incluidos los responsables de la toma de decisiones financieras, como los directores financieros.



Cómo BDO puede ayudarle

El equipo de ciberseguridad de BDO entiende los riesgos asociados a la tecnología disruptiva y ofrece un conjunto completo de servicios de ciberseguridad diseñados para salvaguardar su organización. Nuestro enfoque incluye la evaluación exhaustiva de su nivel de madurez de ciberseguridad, la comprobación de las vulnerabilidades de su red y la evaluación exhaustiva del riesgo. Concierte hoy mismo una consulta con nuestro equipo para revisar su estructura organizativa en busca de problemas de seguridad.

BDO es Socio Global de Seguridad del Año de Microsoft y proveedor líder de soluciones de ciberseguridad para empresas. Proporcionamos soluciones integrales aprovechando las capacidades avanzadas de seguridad e identidad de Microsoft 365 y Microsoft Azure Security.

CIBERSEGURIDAD AVANZADA PARA SU ORGANIZACIÓN | BDO-BDO

Rocco Galletto
Global Cybersecurity Leader