Ciberseguridad

¿Es su red de seguridad lo suficientemente fuerte?

mazars

Contenido

Prólogo
Ciberseguridad: un delicado equilibrio

Las ciberamenazas nos rodean. No se trata de paranoia, sino de una desafortunada realidad: cada día se producen nuevos hackeos, nuevas filtraciones de datos, nuevas situaciones embarazosas... y nuevos costos nadie se libra. Los ataques se dirigen a empresas grandes y pequeñas, así como a instituciones del sector público y privados. Colectivamente, estamos mejorando en la prevención y detección de las intrusiones cibernéticas y limitar sus daños, gracias en parte a las soluciones tecnológicas, pero también a una mayor concienciación sobre los peligros del phishing y otras técnicas clásicas de hacking. Sin embargo, ningún sistema es infalible. Los avances tecnológicos que pueden protegernos también proporcionan a los ciberdelincuentes herramientas más avanzadas, incluida la inteligencia artificial, que pueden mantenerlos varios pasos por delante de las organizaciones a las que se dirigen.

En este contexto, el presente informe toma como punto de partida la inevitabilidad de sufrir un ataque. La ciberseguridad ya no es una cuestión de "si", sino de "cuándo". Esto puede suponer un cambio de mentalidad para muchos líderes empresariales, pero creemos que es importante hacerlo. En nuestra opinión, el realismo de mirada fría es la mejor estrategia de defensa cibernética, ya que informará a cada uno de los cinco aspectos operativos clave que deben estar en su posición para salvaguardar los datos de la empresa. Estos cinco pilares son: identificación, prevención, detección, respuesta y recuperación.

Una prueba de fuego para la resistencia de las organizaciones

Una encuesta que realizamos a más de 1.000 ejecutivos de todo el mundo el pasado mes de diciembre para nuestro barómetro anual de la alta dirección puso de relieve cómo la ciberseguridad es ahora una de las principales preocupaciones de los líderes empresariales. Más de la mitad de los encuestados nos dijeron que los riesgos cibernéticos han aumentado en el último año, y más de un tercio se preparan para sufrir filtraciones de datos en los próximos 12 meses. Sin embargo, la misma encuesta mostró que los altos directivos tienen un nivel de confianza en su propia empresa para resistir ataques que pueden parecer sorprendentes, incluso paradójicos. ¿Saben algo que sus propios departamentos informáticos ignoran? Probablemente no. Sin embargo, estos resultados sugieren que la ciberseguridad se ha convertido en un delicado acto de equilibrio para muchas empresas, similar a caminar por la cuerda floja: sí, es peligroso, pero lo importante es construir una sólida red de seguridad que pueda amortiguar cualquier posible caída.

Muchas herramientas que pueden ayudar a identificar, prevenir y detectar violaciones cibernéticas están ahora fácilmente disponibles. Los CEO pueden poner cifras a los presupuestos de sus juntas directivas, así como ejemplos que ilustren su supuesto grado de preparación. La respuesta y la recuperación después de un ataque son mucho más difíciles, dado que cada vulneración puede ser diferente. Sin embargo, la forma en que una empresa o una institución del sector público o privado reacciona ante los ciberataques es una prueba esencial de estrategia y liderazgo. Esperar a que se produzca una crisis para elaborar un plan de respuesta eficaz es como intentar colgar la red de seguridad mientras se tropieza. Y la capacidad de una organización para recuperarse de un colapso cibernético puede ser difícil de calibrar antes de que se ponga a prueba en la vida real.

En ese sentido, la ciberseguridad es un indicador revelador de la salud de la organización. Las competencias necesarias para hacer frente a las ciber amenazas no se limitan a los equipos de TI o de comunicaciones, sino que se extienden a toda la organización, y si la respuesta a una brecha está bien planificada y ejecutada, lo más probable es que la organización esté más sana y sea más resistente en su conjunto. Encontrar el equilibrio en ciberseguridad es bueno para el negocio en general.

Resumen ejecutivo

Las empresas de todo el mundo se preparan para los ciberataques, pero confían en poder resistirlos

Más de la mitad de los directivos encuestados en nuestro barómetro anual de la alta dirección perciben un aumento de las ciber amenazas en el último año, y el 35% espera una violación de datos significativa en su propia empresa en el próximo año. La preocupación es global, aunque más pronunciada en las grandes empresas con más de 1.000 millones de dólares de ingresos anuales. No obstante, la mayoría de las empresas parecen confiar en su capacidad para hacer frente a los ataques: a nivel mundial, el 68% de los líderes empresariales considera que los datos de su empresa están "completamente protegidos". En Estados Unidos, esa cifra asciende hasta el 80%.

Las pérdidas financieras son el mayor riesgo percibido

Más de la mitad de los líderes empresariales encuestados sitúan las pérdidas financieras a la cabeza de la lista de los mayores riesgos para la protección de datos, seguidos de el riesgo de cumplimiento (44%). Sólo un tercio mencionó la preocupación por la reputación y la continuidad de la actividad empresarial. Los niveles de preocupación y confianza varían de un sector a otro, siendo las empresas financieras, tecnológicas y de consumo las más seguras, posiblemente porque son las más expuestas debido a que manejan datos sensibles de los consumidores.

La ciberseguridad va mucho más allá del cumplimiento de las normas.

Los escenarios de crisis deben probarse, volver a probarse y mejorarse continuamente.

Una ciberdefensa eficaz se basa en cinco pilares: identificación, prevención, detección, respuesta y recuperación

Cada uno tiene un componente tecnológico importante, pero igualmente cada uno tiene un componente humano crítico. Conocer las vulnerabilidades del propio sistema y ser capaz de detectar patrones inusuales es un punto de partida tanto para la prevención como para la detección. Las soluciones tecnológicas pueden incluir la segmentación de las redes informáticas para poner capas adicionales de seguridad en torno a los datos más sensibles y amplias copias de seguridad fuera de línea, pero todo el mundo, desde la alta dirección hasta el personal a tiempo parcial, debe recibir formación y recordatorios frecuentes de los riesgos. Un plan de comunicación detallado y probarlo es esencial para una respuesta eficaz, tanto para uso interno como para llegar a clientes, proveedores, reguladores y cualquier persona de su ecosistema de datos.

Los planes de continuidad de la actividad deben haber sido minuciosamente elaborados y ampliamente probados para que puedan ser adoptados sin problemas por toda la organización.

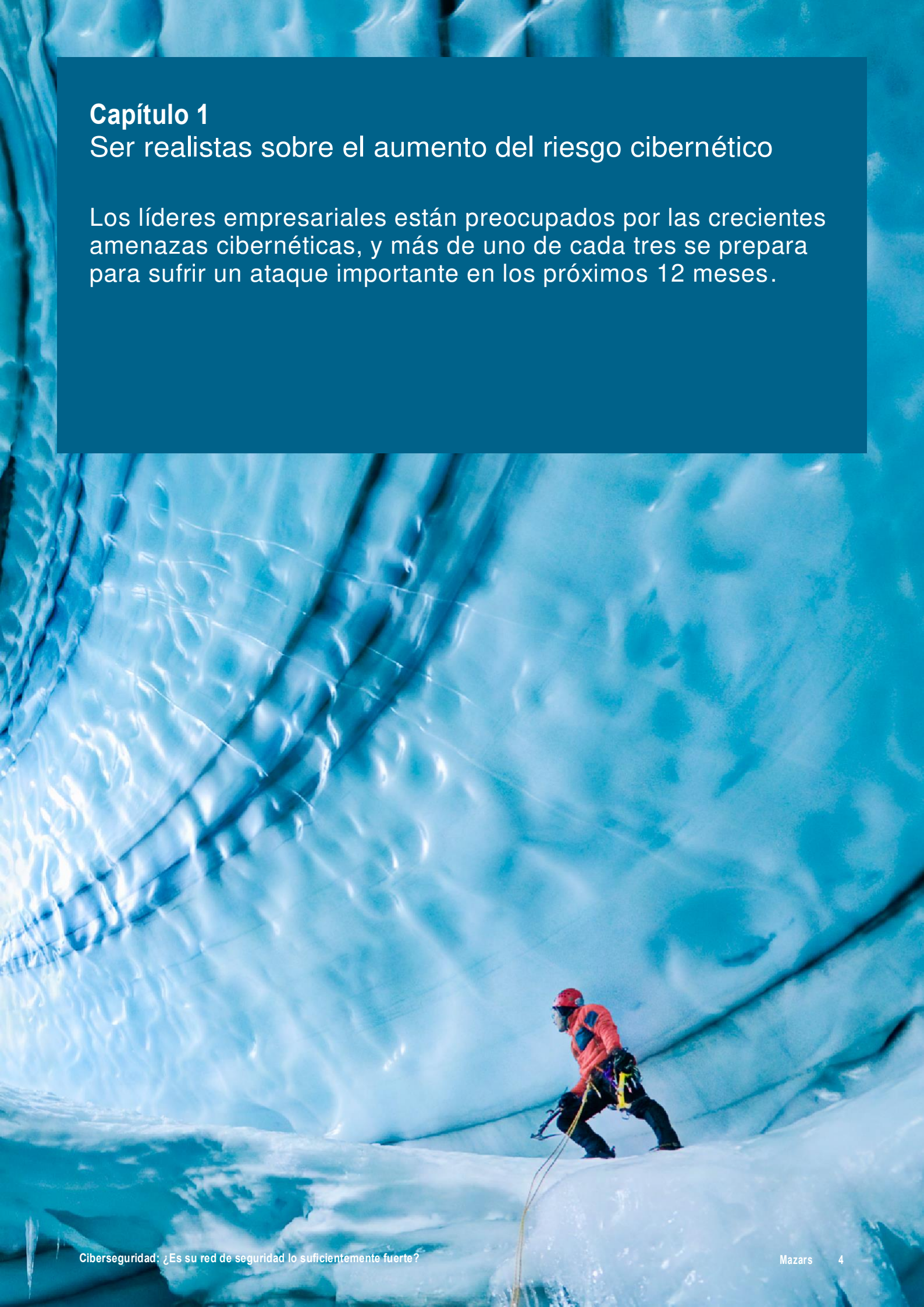
La mejor defensa es cambiar de mentalidad y prepararse para lo peor

La ciberseguridad es un campo en rápida evolución, con atacantes ahora fuertemente armados (incluso Auditoría Interna) y a menudo dos pasos por delante de las organizaciones en su punto de mira. La vigilancia tecnológica, combinada con los esfuerzos de educación continua y los juegos de guerra permanentes de escenarios puede evitar algunos de los problemas. La regulación es cada vez mayor; cada vez más, las empresas de muchos sectores tienen la obligación de informar sobre sobre su preparación cibernética y notificar las vulneraciones. Pero la ciberseguridad va mucho más allá del cumplimiento de la normativa.

Los escenarios de crisis deben probarse, volver a probarse y mejorarse continuamente. Aceptar que se producirán violaciones de datos y disponer de planes sólidos para gestionarlas es la mejor garantía de que la respuesta será rápida, la recuperación eficaz y los costos limitados.

Capítulo 1
Ser realistas sobre el aumento del riesgo cibernético

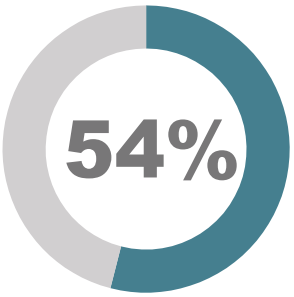
Los líderes empresariales están preocupados por las crecientes amenazas cibernéticas, y más de uno de cada tres se prepara para sufrir un ataque importante en los próximos 12 meses.



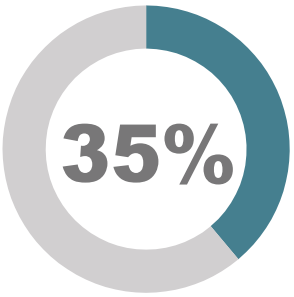
Ser realistas sobre el aumento del riesgo cibernético

Las ciberamenazas son reales, peligrosas y cada vez más graves. Los directivos de las empresas son conscientes de ello. Nuestro barómetro de directivos muestra que más de la mitad de los encuestados creen que las amenazas cibernéticas para sus organizaciones han aumentado en los últimos doce meses, y el 35% espera una vulneración de datos significativa en el próximo año.

Estas cifras globales ocultan diferencias significativas según el tamaño y la ubicación de la empresa. Las grandes empresas con más de 1.000 millones de dólares de ingresos anuales son las más preocupadas: dos tercios de ellas perciben un aumento de las amenazas, en comparación con algo menos de la mitad de las empresas de entre 1 y 100 millones de dólares. millones de dólares. Y la sensibilización ante los riesgos es mayor tanto en Estados Unidos como en Europa, donde más del 60% ve peligros crecientes.

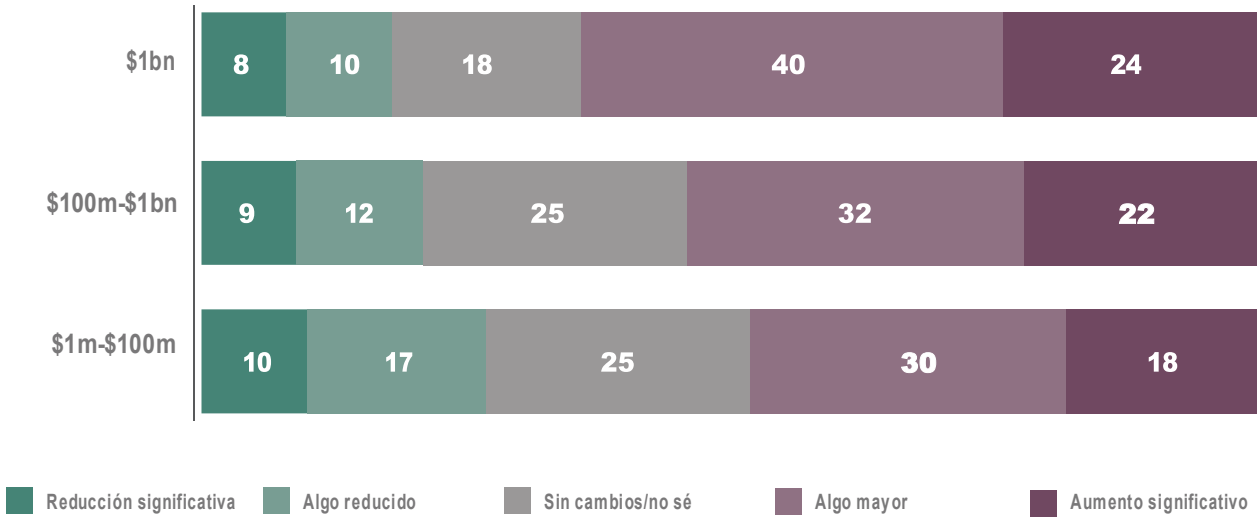


Más de la mitad de los encuestados cree que el riesgo de ciberseguridad para su organización ha aumentado en los últimos 12 meses.



Más de un tercio cree que es probable que se produzca una vulneración.

Cambio en el riesgo de ciberseguridad
Porcentaje de encuestados por banda de ingresos



Pregunta: ¿Cómo ha cambiado el riesgo de ciberseguridad para su organización en los últimos 12 meses?
Entre 1 y 100 millones de dólares, n=432; entre 100 y 1.000 millones de dólares, n=350; más de 1.000 millones de dólares.

Ser realistas sobre el aumento del riesgo cibernético

Pequeñas empresas, grandes amenazas

Que usted sea una pequeña empresa no significa que sus riesgos de ciberataques sean menos importantes que los de las grandes compañías. Las ciberamenazas no funcionan así. Los delincuentes que atacan su sistema informático no discriminan: sondean a todo el mundo en busca de vulnerabilidades, independientemente de su tamaño. Y, en cierto modo, las pequeñas empresas corren más riesgos. Suelen tener menos personal con capacidades de ciberseguridad para ayudar a proteger sus sistemas y pueden carecer de los rigurosos controles internos para identificar y detectar amenazas que muchas organizaciones más grandes tienen en marcha.

Sin embargo, la naturaleza de la desestabilización puede ser diferente para las empresas más pequeñas. Los ataques de ransomware -que bloquean a los usuarios de un sistema hasta que se paga- tienden a centrarse en grandes corporaciones o instituciones, incluido el sector público. Del mismo modo, los ataques de denegación de servicio (DoS), que inundan los objetivos con tráfico o provocan una caída con una sobrecarga de información, tienden a dirigirse a los actores más grandes. Sin embargo, el phishing clásico y el fraude del CEO, o "whale phishing", que consiste en que un hacker se hace pasar por un alto ejecutivo con la esperanza de persuadir a un empleado o contratista para que divulgue información valiosa por correo electrónico, son comunes a todas las empresas, pequeñas y grandes.

En cierto modo, las pequeñas empresas corren más riesgos, ya que cuentan con menos personal capacitado en ciberseguridad y pueden carecer de los controles internos necesarios para identificar y detectar amenazas.

Las tecnologías digitales, y especialmente las plataformas digitales como las que operan Amazon, Facebook y otras, han permitido a las pequeñas empresas extender su alcance por todo el mundo. Estas plataformas pueden proporcionar una mayor protección cibernética a las empresas en sus plataformas de lo que muchas empresas pueden llegar a poner en marcha por sí mismas. Pero, desde luego, no garantizan la inmunidad. Para todas las empresas, la TI más vulnerable que tienen es el sistema que utilizan para conectarse con el mundo exterior. Y en un mundo que gira en torno a la relevancia, la puntualidad en el mercado y la innovación, las pequeñas empresas tienen que encontrar un difícil equilibrio: cómo actualizar y cambiar sus sistemas informáticos para seguir el ritmo de los requisitos de marketing sin crear innecesariamente nuevas vulnerabilidades.

Ser realistas sobre el aumento del riesgo cibernético
Pequeñas empresas, grandes amenazas

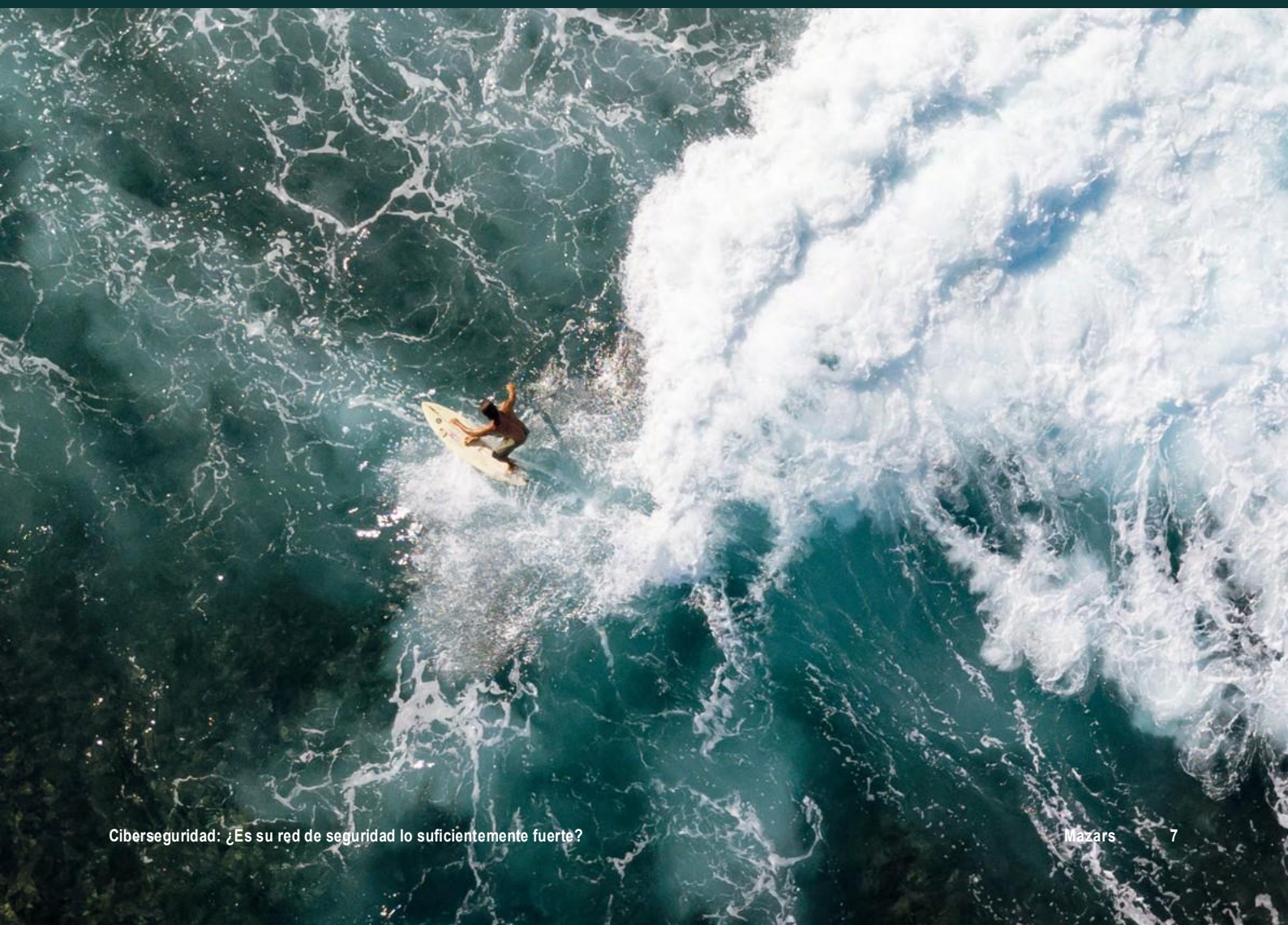
Entonces, ¿qué pueden hacer las empresas más pequeñas para protegerse dadas sus limitaciones de tamaño? Sus posibilidades son intrínsecamente más limitadas, porque las pequeñas empresas tienen menos recursos que las grandes, tanto en términos de dinero como de experiencia cibernética. Esto hace que sea primordial que las empresas más pequeñas se centren en las medidas más sólidas, pero también las más sencillas posibles. Destacan tres:

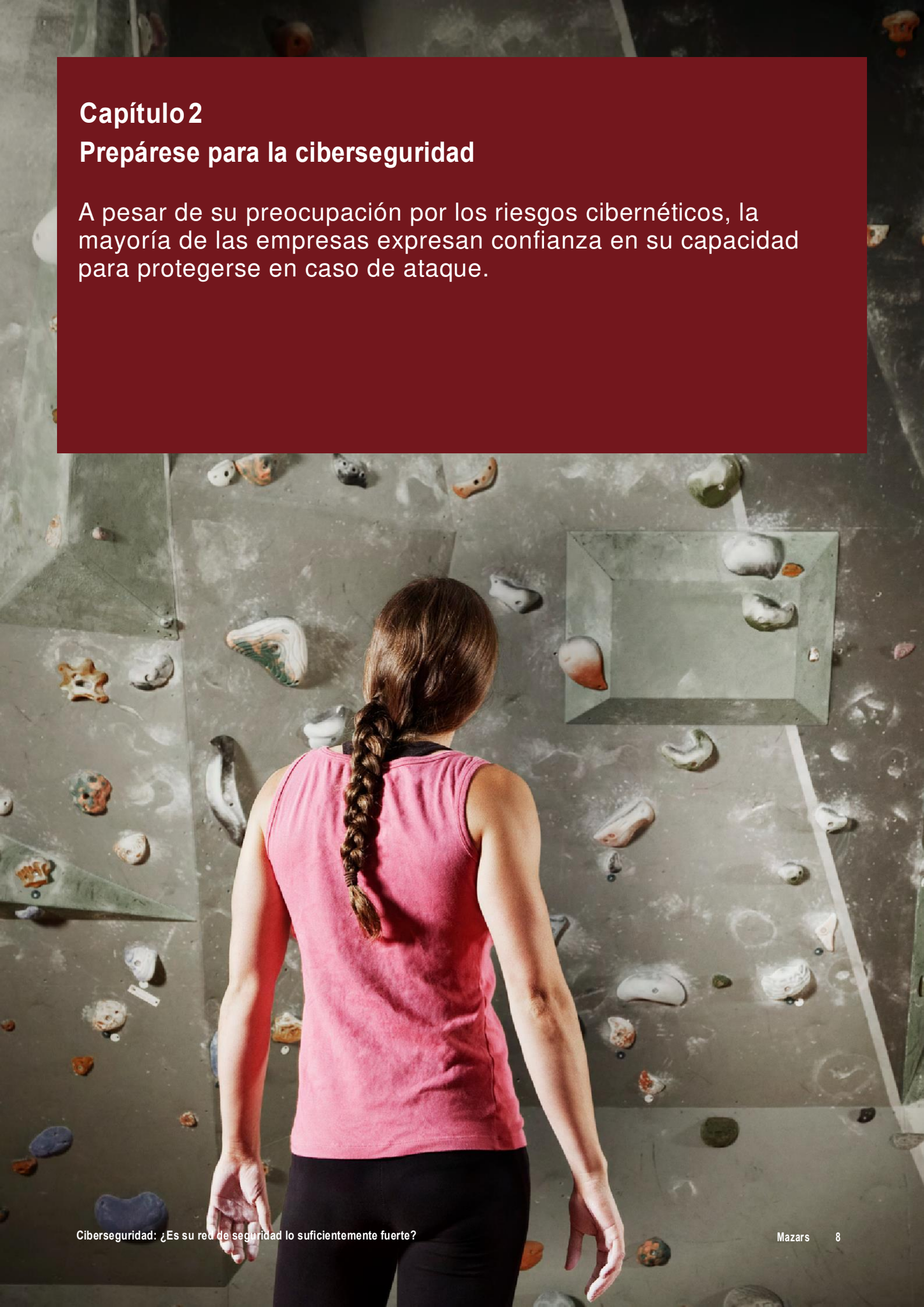
En primer lugar, sea a la antigua escuela: haga una muy buena copia de seguridad de sus datos con un espacio de aire. En otras palabras, almacena una copia completa de tus datos clave fuera de línea, en algún lugar seguro, para que puedas recuperarlos en caso de un ataque debilitador.

En segundo lugar, segmenta los datos en sub-sectores para evitar que una intrusión en tu sistema contamine todos tus datos. La segmentación no es un remedio costoso para los sistemas informáticos, pero es muy importante para las pequeñas empresas.

Por último, manténgase informado y flexible. Algunas pequeñas empresas piensan que pueden implantar un sistema de ciberseguridad y dejar de preocuparse. Es un planteamiento equivocado: todas las empresas deben mantenerse alerta. Es imprescindible organizar comunicaciones con los proveedores informáticos y las partes interesadas cuando usted o ellos tengan un incidente. Y es esencial mantenerse informado sobre las nuevas amenazas y riesgos cibernéticos.

En el mundo de la ciberseguridad, no es imposible protegerse si se es pequeño. Pero hay que actuar con mucho cuidado.





Capítulo 2

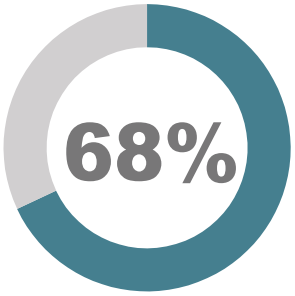
Prepárese para la ciberseguridad

A pesar de su preocupación por los riesgos cibernéticos, la mayoría de las empresas expresan confianza en su capacidad para protegerse en caso de ataque.

Medir la preparación para la ciberseguridad

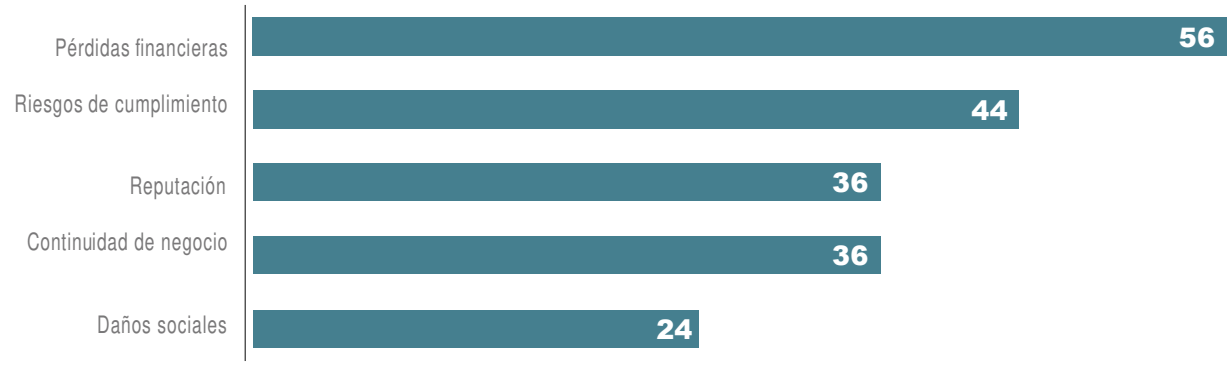
Para los altos ejecutivos de todo el mundo, el riesgo cibernético se traduce en gran medida en miedo al riesgo financiero. Más de la mitad de los líderes empresariales encuestados sitúan las pérdidas financieras a la cabeza de la lista de los mayores riesgos para la protección de datos, seguidas del riesgo de cumplimiento (44%). Sólo un tercio citó la preocupación por la reputación y la continuidad del negocio.

Al mismo tiempo, la confianza en poder resistir los ciberataques es alta, con más de dos tercios de los líderes empresariales -el 68%- diciéndonos que sienten que los datos de su organización están "completamente protegidos". Un corte geográfico de los resultados de la encuesta muestra que la confianza es mayor en Estados Unidos, donde el 80% de los encuestados cree que sus datos están completamente protegidos.



Más de dos tercios confían en que sus datos están completamente protegidos. Otro 29% afirma que sus datos están parcialmente protegidos.

Mayores riesgos de ciberseguridad y protección de datos
Porcentaje de encuestados



Pregunta: ¿Cuáles son los DOS mayores riesgos para su organización en materia de ciberseguridad y protección de datos?

Medir la preparación para la ciberseguridad

Mantener las luces encendidas: preparación cibernética del sector público

Los peligros cibernéticos que acechan en la sombra a las empresas del sector privado no son una amenaza menor para las administraciones nacionales y locales y otras organizaciones del sector público, y en algunos aspectos lo son aún más. Los datos que guardan estas organizaciones son a menudo muy privados y confidenciales, y van desde datos de la seguridad social y declaraciones de impuestos hasta información sobre educación, registros sanitarios, salud y justicia penal. En casos extremos, la seguridad nacional puede verse comprometida si se atacan infraestructuras claves como centrales eléctricas o incluso instalaciones de defensa. Dicho sin rodeos, cuando se trata de riesgos del sector público, sólo se está a un paso de quedarse sin luz.

Los ataques cibernéticos a organizaciones locales o nacionales que han recibido gran publicidad en muchos países en los últimos años han aumentado la concienciación sobre los riesgos a los que se enfrentan las instituciones del sector público. Uno de ellos es el "ransomware", un tipo de software malicioso que cifra los archivos de un dispositivo o una red, dejándolos inutilizables. Sus autores exigen un pago a cambio del descifrado, a menudo amenazando con vender o filtrar datos o información de autenticación si no se paga el rescate. Pagar o no pagar es un malabarismo imposible para la organización afectada: ¿cómo reaccionaría el público ante la idea de recompensar a los delincuentes con el dinero de los contribuyentes?

Para defenderse, las organizaciones del sector público necesitan reforzar los mismos cinco pilares que el sector privado, a saber, identificación, detección, prevención, respuesta y recuperación. Sin embargo, el sector público se enfrenta a algunos retos particulares para hacerlo.

En primer lugar, los propios sistemas pueden ser muy vulnerables. Para muchas organizaciones del sector público, los sistemas informáticos son un mosaico de viejos y nuevos, y los sistemas heredados son los más vulnerables al ransomware y otros ataques.

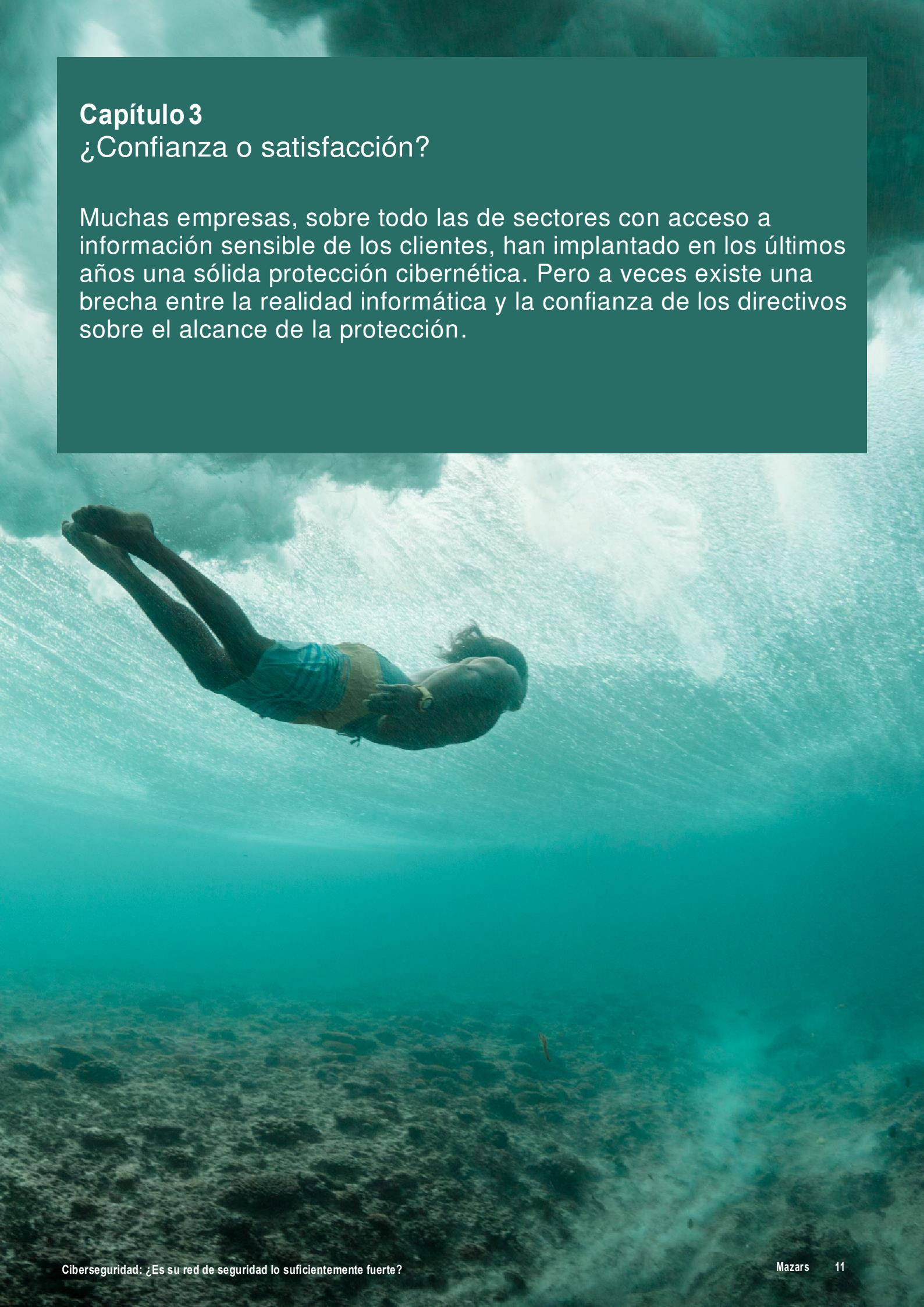
Al mismo tiempo, estas organizaciones no suelen disponer de fondos para actualizar todo a la tecnología más reciente.

Una segunda desventaja es que incluso las organizaciones del sector público más conscientes de los riesgos y que tratan de construir defensas más sólidas pueden tener dificultades para contratar a los expertos cibernéticos que necesitan para poner en práctica sus deseos. Los especialistas cibernéticos tienen un valor de mercado considerable en todas partes, a menudo muy por encima del alcance de los presupuestos públicos e incluso si una organización contrata o forma a personas competentes, a menudo son cazadas furtivamente.

Se puede hacer mucho, y se está haciendo, con un uso cuidadoso de los recursos. Las organizaciones cibernéticas nacionales comparten buenas prácticas y mucho más. En el Reino Unido, por ejemplo, el Centro Nacional de Seguridad Cibernética ofrece herramientas de ciberseguridad y muchos otros recursos para ayudar a las organizaciones del sector público a prepararse. Los altos ejecutivos de la administración pública son ahora muy conscientes del riesgo cibernético y hacen más por evaluar las vulnerabilidades, probar los sistemas y recurrir a ayuda externa cuando es necesario para mejorar estas eventualidades. La concienciación de todo el personal se ha intensificado. En algunos países, la planificación de la respuesta instantánea está muy avanzada y existen planes de recuperación de desastres y continuidad de la actividad, al menos sobre el papel. Sin embargo, como siguen demostrando las continuas brechas cibernéticas en instituciones públicas de todo el mundo, nunca es suficiente. Mantener las luces encendidas sigue siendo una cuestión de vigilancia intensificada, más recursos, más formación y ciclos interminables de pruebas.

Capítulo 3
¿Confianza o satisfacción?

Muchas empresas, sobre todo las de sectores con acceso a información sensible de los clientes, han implantado en los últimos años una sólida protección cibernética. Pero a veces existe una brecha entre la realidad informática y la confianza de los directivos sobre el alcance de la protección.



¿Confianza o satisfacción?

¿Cómo explicar la aparente desconexión en la alta dirección entre el creciente temor a las ciberamenazas y la aparentemente sólida confianza entre los líderes de negocio de que sus empresas están bien protegidas? Observamos una desconexión similar en una encuesta sobre datos que realizamos el año pasado: cuatro de cada cinco ejecutivos a cargo de la gobernanza de los datos afirmaban que su empresa era más madura en materia de datos que sus competidores. Al mismo tiempo, muchas de esas empresas simplemente no cumplían las mejores prácticas que sustentan la madurez de los datos, en particular en lo que respecta a la calidad de los datos, un ingrediente esencial para la ventaja digital.

El día a día de los departamentos de TI es cada vez más complejo y arriesgado.

Es posible que en las empresas se esté configurando un universo paralelo: mientras los altos directivos elaboran planes de gobernanza en la creencia de que pueden alcanzar o han alcanzado un alto nivel de cumplimiento en materia de seguridad, la realidad cotidiana en los departamentos de TI es cada vez más compleja y está plagada de riesgos. La tecnología y la pandemia de Covid-19 ayudan a explicar este último estado de cosas: si en 2019 el mantra de la oficina era "trae tu propio dispositivo", hoy -en parte debido a la tendencia de trabajar desde casa- eso ha cambiado a "trae tu propia nube".

Al mismo tiempo, un número cada vez mayor de empresas, especialmente en los sectores más expuestos, como la banca y el comercio minorista, han acumulado un profundo conocimiento tanto de los riesgos como de las amenazas necesarias para hacer frente con eficacia a las ciberamenazas. En este sentido, están surgiendo buenas prácticas que sirven de base a las conclusiones de este informe.

¿Confianza o satisfacción?
Minoristas: confianza prudente tras años de experiencia

"Cuando manejas datos privados de clientes, incluidos números de tarjetas de crédito, tienes que estar muy seguro de ti mismo. Y los minoristas se toman la ciberseguridad muy en serio: llevan años haciéndolo. Por eso parecen confiados.

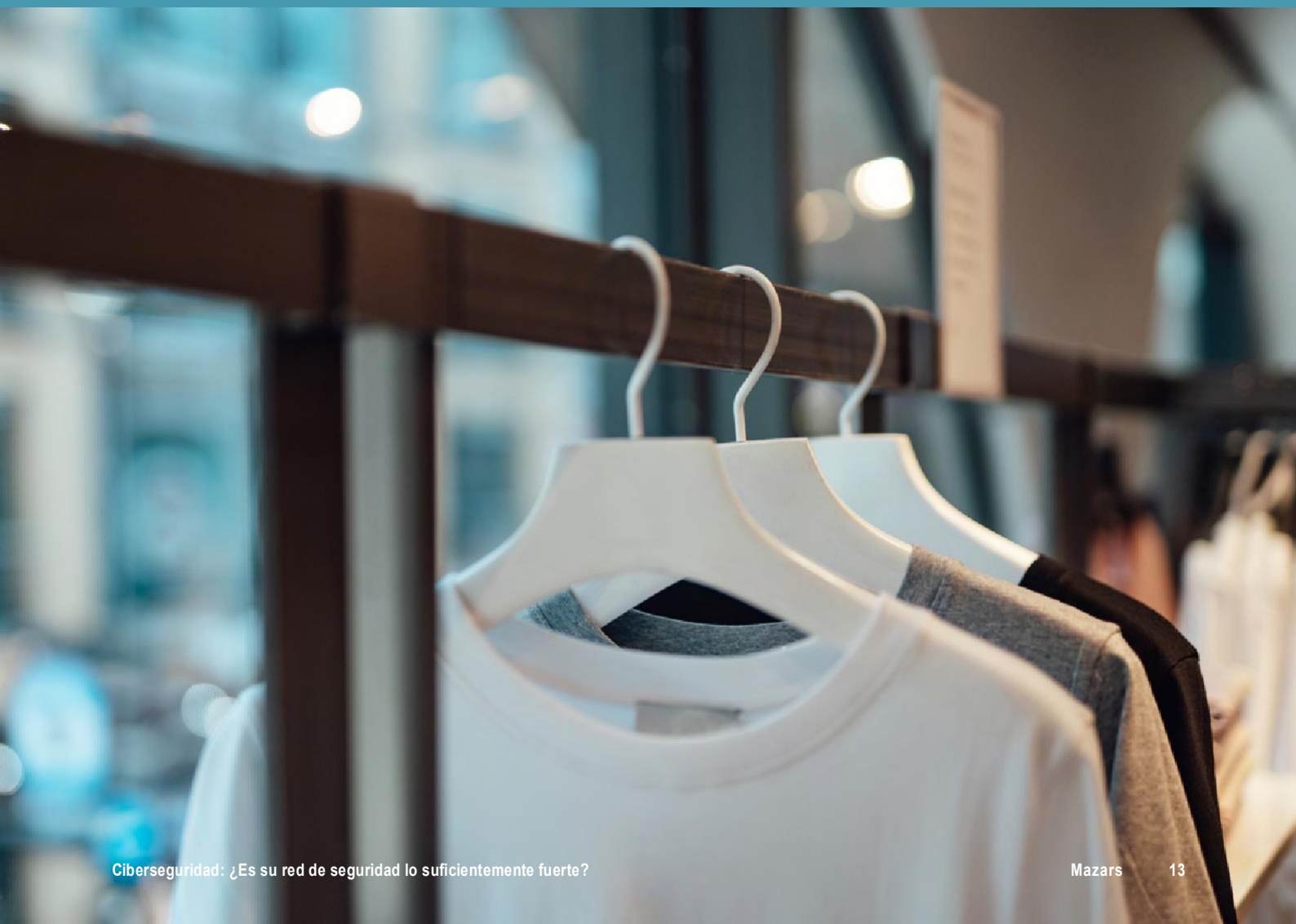
El riesgo cibernético en el comercio minorista aumentó durante la pandemia debido al gran incremento del comercio electrónico. Al mismo tiempo, también aumentaron la importancia y la intensidad del cuidado que los minoristas prestan a los datos. Todos los grandes minoristas cuentan ahora con especialistas en ciberseguridad y su inversión en seguridad se ha acelerado en los últimos dos o tres años. Así que, aunque los riesgos aumentan, la forma de afrontarlos ha mejorado.

Lo importante es tener un plan global. Siempre es un golpe cuando te atacan, pero no debe ser algo que te paralice, porque te has preparado para ello.

No sólo hay que estar preparado desde el punto de vista tecnológico. Necesitas un plan B para la continuidad de la empresa.necesitas un buen plan de comunicación, sobre todo si los datos de los clientes se ven comprometidos, ya que eso puede poner en peligro tu imagen. Si alguna vez ocurre, necesitas las palabras adecuadas. Tienes que ser lo más transparente posible.

Eso es cierto para el sector en su conjunto, pero hay diferencias. A veces es una cuestión de escala y otras de generación. Si eres un empresario nativo digital, todos tus sistemas se han creado para ser seguros y pueden ampliarse de forma segura. Es muy diferente si eres un minorista clásico y necesitas entrar en el mundo digital.

Nuestra conclusión es que nunca se sabe, así que prepárense. Este es un sector en riesgo todo el tiempo".



Capítulo 4
No sí, pero cuando: los cinco pilares de la defensa

Una defensa sólida contra los ciberataques depende de su capacidad para identificar, prevenir y, posteriormente, detectar los ataques. La respuesta y la recuperación tras un ataque deben planificarse cuidadosamente y probarse exhaustivamente.

No sí, pero cuándo
Cinco pilares de defensa

La defensa inteligente contra las ciberamenazas tiene cinco pilares: identificación, prevención, detección, respuesta y recuperación. Cada uno de estos pilares contribuye al equilibrio general de la ciberseguridad de una empresa, ayudándola a gestionar el riesgo mediante la organización de la información, permitiendo la toma de decisiones de gestión del riesgo, haciendo frente a las amenazas, aprendiendo de las actividades anteriores... y consiguiendo como resultado ser más resistente. Cada uno de los pilares tiene un componente tecnológico importante, pero igualmente cada uno tiene un componente humano crítico. La realidad tecnológica de las TI y los factores humanos van de la mano. Ambos requieren paciencia, formación, inversión y pruebas exhaustivas.

Pilar 1: Identificación

Desarrollar la comprensión organizativa que le permitirá gestionar los riesgos de ciberseguridad para los sistemas, activos, datos y capacidades.

Un primer paso fundamental para una empresa es conocerse a sí misma. Gran parte del trabajo pesado aquí debe ser realizado por el equipo de TI: identificar y mapear todas las fuentes de datos, el grado de sensibilidad en torno a estos datos y todas las vulnerabilidades potenciales del sistema que podrían exponerlos. sensibilidad que rodea a estos datos, y todas las vulnerabilidades potenciales del sistema que podrían exponerlos. El mapa interno es sólo el principio: debe complementarse con un conocimiento detallado de las fuentes externas de contagio potencial, procedentes de proveedores y otras partes interesadas a lo largo de toda la operación.

Más allá de disponer de la infraestructura informática adecuada, el mapeo requerirá conocimientos humanos. ¿Dispone de las personas adecuadas en su equipo de TI para llevarlo a cabo? ¿Y qué tipo de información sobre los riesgos y amenazas cotidianos debe transmitirse a la dirección? Éstas son las preguntas esenciales que toda empresa debe plantearse.

Pilar 2: Prevención

Desarrollar y aplicar salvaguardias adecuadas para garantizar la prestación de servicios de infraestructuras críticas.

Existen múltiples soluciones técnicas para ayudar a proteger los sistemas informáticos y garantizar que sigan funcionando con normalidad incluso frente a los ataques. Estas soluciones pueden incluir estrategias de segmentación que consisten en dividir las redes informáticas en subsecciones para evitar el contagio del sistema. En el marco de una estrategia de segmentación, se pueden aislar los datos más importantes.

Sensibilizar a las personas sobre los riesgos cotidianos es un aspecto no menos esencial que puede lograrse mediante programas de educación y pruebas periódicas de "phishing" y otras pruebas internas. La autenticación de múltiples factores para los usuarios es una herramienta valiosa que permite a las empresas redoblar la lucha contra el fraude de los usuarios y, al mismo tiempo, mejorar la ciber higiene de los empleados.

No sí, pero cuándo
Cinco pilares de defensa

Pilar 3: Detección

Desarrollar y aplicar actividades adecuadas para identificar cuándo se ha producido una violación de la ciberseguridad.

Las auditorías de ciberseguridad pueden proporcionar perspectivas externas útiles sobre la eficacia de las salvaguardias del sistema. Los requisitos incluyen comprender la exposición potencial de su empresa, disponer de las herramientas para supervisar la actividad de la red y ser capaz de detectar anomalías en tiempo real y escalarlas cuando sea necesario.

No basta con que el personal informático participe en estos esfuerzos: se necesitan gestores bien formados a todos los niveles, capaces de detectar los problemas y saber a quién alertar.

Las auditorías de ciberseguridad pueden aportar perspectivas externas útiles sobre la eficacia de salvaguardias del sistema.

No sí, pero cuándo
Cinco pilares de defensa

Pilar 4: Respuesta

Desarrollar y aplicar las medidas adecuadas en caso de que se detecte una vulneración de la ciberseguridad.

Una vez detectada una intrusión, la respuesta técnica para aislarla y neutralizarla debe ser extremadamente rápida. Una estrategia de segmentación eficaz limitará los daños protegiendo los datos más esenciales de la contaminación. Ya en esta primera fase, comprender qué datos y sistemas se han visto comprometidos es un requisito imprescindible que informará de los pasos siguientes.

Inevitablemente, el objetivo inicial es reparar los daños informáticos, pero hay que dar muchos otros pasos... en una sucesión rápida y cuidadosamente planificada. La comunicación es clave: los líderes de negocio tienen que llegar a la alta dirección y al personal, a los clientes, a los proveedores y a otros en su ecosistema de datos, y -cada vez más- a los reguladores, y, cada vez más, a los reguladores. De hecho, la rápida evolución de la normativa a ambos lados del Atlántico está exigiendo a las empresas de diversos sectores no sólo informen de las vulneraciones cibernéticas, sino que muestren el alcance de su red de seguridad cibernética y permitan que se ponga a prueba. Dado que las redes son el núcleo de nuestra economía cada vez más digital, no es de extrañar: una brecha cibernética nunca es un hecho aislado, sino que puede propagarse rápidamente a otras. Nadie vuela solo en el mundo digital: un solo trapecista que pierda el control puede desequilibrar a todo el equipo.

Pilar 5: Recuperación

Desarrollar y aplicar las medidas adecuadas que permitan volver a la normalidad tras una vulneración de la ciberseguridad.

En cierto modo, la recuperación es lo más difícil de planificar y probar por adelantado, ya que depende mucho del alcance de la vulneración cibernética y del daño que cause a los datos, a los clientes y a la reputación. Sin embargo, podría decirse que es también la más importante: poder reanudar la actividad con normalidad es fundamental. También en este caso, la tecnología ofrece algunas soluciones. Entre ellas, los sistemas de copia de seguridad offline que pueden activarse rápidamente para restablecer el funcionamiento normal de las TI. Muchas otras partes de la empresa deben unirse en torno a un plan de recuperación probado. La continuidad de la empresa es la consigna. recuperar el equilibrio en la cuerda floja si un ciberataque le hace caer temporalmente de ella. Los planes de continuidad de la actividad variarán de un sector a otro y de una empresa a otra, y sólo pueden funcionar bien si se han probado y vuelto a probar cuidadosamente con mucha antelación, no sólo desde el punto de vista de los sistemas, sino también desde el punto de vista humano. Los responsables deberán ser capaces de pasar al Plan B sin el menor contratiempo o problema. Cada vez más, los reguladores exigen que se demuestre que se puede sobrevivir a los ciberataques y seguir funcionando.

No sí, pero cuándo
Regulación de la ciberseguridad: un campo en rápida evolución

La ciberseguridad no es sólo una cuestión de empresa a empresa. Cada vez está más sujeta a normativas, tanto nacionales como internacionales, que abarcan cuestiones que van desde la gestión de riesgos hasta la notificación obligatoria de incidentes cibernéticos. A medida que aumentan los riesgos cibernéticos, esa normativa evoluciona. A continuación, analizamos las principales novedades legislativas a ambos lados del Atlántico.

EU: NIS2 Directive

La primera Directiva de Seguridad de las Redes y de la Información (SRI) de la UE se adoptó en 2016. Se centraba en reforzar las capacidades nacionales de ciberseguridad, establecer una colaboración transfronteriza y poner en marcha una supervisión nacional de la ciberseguridad en sectores críticos como la energía, el transporte, el agua, la salud, las infraestructuras digitales y el sector financiero. En 2021, la Comisión Europea propuso sustituirla por una versión actualizada destinada a responder a las crecientes amenazas. La NIS2 aborda la seguridad de las operaciones y pretende racionalizar las obligaciones de información e introducir medidas de supervisión más estrictas y requisitos de aplicación más rigurosos, incluidas sanciones armonizadas en toda la UE.

EU: Digital Operational Resilience Act (DORA)

Este nuevo Reglamento, que entrará en vigor en los Estados miembros de la UE en 2022, constituye un marco detallado y completo para los bancos y otras entidades financieras destinado a mejorar su ciberseguridad. Fundamentalmente, también cubre la gestión de riesgos de los proveedores de servicios TIC con los que trabajan estas instituciones financieras. Estos proveedores estarán incluidos en el ámbito de aplicación del DORA, al igual que las grandes y pequeñas empresas financieras. El amplio alcance de la normativa abarca las empresas de inversión alternativa, los proveedores de servicios de criptoactivos, los proveedores de servicios de financiación colectiva (crowdfunding) y otros.

Como consecuencia de ello, los organismos de supervisión tendrán que desempeñar un papel más importante y aumentar su propia concienciación cibernética. La Comisión de la UE propuso por primera vez este Reglamento en 2019. Entre tanto, se ha sometido a varias rondas de consultas. La idea era llenar un vacío: la ausencia de normas a escala de la UE sobre la resiliencia operativa digital que había dado lugar a la proliferación de iniciativas reguladoras nacionales.

Estas normas nacionales eran a veces incoherentes o duplicadas y traían consigo costos administrativos y de cumplimiento adicionales

.

US: Strengthening American Cybersecurity Act

El 15 de marzo de 2022, el presidente Biden promulgó esta ley. Utilizando el lenguaje de otros proyectos de ley, la Ley exige a los operadores de infraestructuras críticas que informen de "incidentes cibernéticos sustanciales" a la Agencia de Ciberseguridad y Seguridad de Infraestructuras (CISA) en un plazo de 72 horas e informen del pago de ransomware en 24 horas. El proyecto de ley contiene otras disposiciones para reforzar la ciberseguridad, incluida la obligación de todos los organismos federales de notificar a la CISA los ciberincidentes importantes cibernéticos sustanciales a la CISA, convirtiendo a esta agencia en la principal organización gubernamental para ayudar a los operadores de infraestructuras críticas a responder y recuperarse de las principales violaciones de la red.

No sí, pero cuándo
El factor humano: una vulnerabilidad clave

"La educación y la concienciación son imprescindibles. Al final, la ciberseguridad tiene que ver sobre todo con el factor humano. No es ético dar a los humanos sistemas mal protegidos, pero los humanos tienen que entender cuáles son los riesgos.

El personal informático necesita suficientes capacidades de ciberseguridad, ya que muchos riesgos pueden derivarse de una mala programación. Es necesario comprender cómo desarrollar un sistema maduro. Pero los usuarios finales también deben entender los riesgos y cómo evitarlos.

Debe saber qué contienen los datos que comparte con terceros y que ellos comparten con usted.

A estas alturas, todo el mundo sabe lo que son las contraseñas y la importancia de no utilizar contraseñas obvias o de reutilizar la misma contraseña para varias aplicaciones en el trabajo y en casa. Pero también hay que saber qué contienen los datos que compartimos con otras personas, y que ellas comparten con nosotros.

Hay muchas cosas que se pueden hacer para reforzar la ciberseguridad. A menudo realizamos ejercicios de phishing e informamos de quién cae en ellos. Esto sensibiliza a la gente, pero debe ir acompañado de una formación básica para todos los empleados. ¿Cómo detectar un falso? ¿Cómo reconozco que alguien está utilizando mis credenciales? En la mayoría de las empresas, este aspecto aún está en fase de desarrollo. Hay una mayor concienciación, pero aún no hemos llegado a ese punto""

Capítulo 5
Reforzar la red de ciberseguridad

Mejorar la ciberseguridad de su organización va mucho más allá de la preparación técnica. Sobrevivir a los ataques y prosperar frente a ellos exige cambios de mentalidad y comportamiento.

Reforzar la red de ciberseguridad
Principales conclusiones

Las ciberamenazas han llegado para quedarse y van a empeorar. Esa es la sobria realidad de la opinión de los altos ejecutivos, tal y como refleja nuestro barómetro anual. Los líderes empresariales no tienen más remedio que vivir con esa realidad y afrontarla lo mejor que puedan. Muchos confían en poder resistir ataques importantes, pero ¿por qué tentar a la suerte?

Todo el mundo necesita una red de seguridad cibernética, y cuanto más fuerte, mejor. Esta sección final contiene seis consejos para sobrevivir y prosperar en un mundo cibernéticamente aterrador. Se trata de principios diseñados para estimular la acción, con relevancia no sólo para los líderes empresariales y los equipos de TI, sino también para todos los empleados.

Cambie de mentalidad

Prepárate para lo peor. No te confíes ni te acomodes demasiado con la idea del riesgo al que te enfrentas. Si ataca, y cuando lo haga, puede sorprenderle por su virulencia, y probablemente lo hará. La consigna es la vigilancia. Hay que estar siempre alerta, atento a los cambios de las técnicas, a las nuevas vulnerabilidades y a la evolución de las condiciones del mercado, así como a las amenazas.

Conozca sus sistemas, sus aplicaciones de datos y sus vulnerabilidades

En muchas empresas hay dos realidades: una realidad informática y una evaluación de esa realidad informática por parte de la alta dirección. La primera, la realidad informática, tiene que ver con la sofisticación operativa. ¿Hasta qué punto es buena la programación? ¿Hasta qué punto son seguras las nuevas impresoras que acabamos de conectar o el nuevo software de marketing que hemos integrado? La segunda, la realidad de la administración, se refiere con demasiada frecuencia al cumplimiento de las normas: ¿disponemos de un proceso para hacer frente a una vulneración? ¿una violación? Es necesario cerrar esa brecha de conocimiento, con una mejor comunicación y una mayor comprensión de las dos realidades, por ambas partes.

Centrarse en el riesgo externo

No olvide incluir la exposición de su operación la evaluación de riesgos externos. Puede ser fácilmente causa de contagio. ¿Con qué cuidado gestionan sus sistemas los proveedores, especialmente si les ha subcontratado alguna parte de su operación? El riesgo de terceros se convierte rápidamente en su riesgo en caso de vulneración.

Aprender, enseñar y educar

No subestime la importancia del factor humano como causa principal de las crisis cibernéticas. Un miembro del personal que hace clic en un enlace de aspecto inocente en un momento de olvido puede tener consecuencias en cascada y, a veces, devastadoras. La ciberseguridad debe ser un programa de aprendizaje obligatorio para todas las empresas, y un programa en constante evolución.

Probar, probar y volver a probar

Su plan de gestión de crisis es tan bueno como la última vez que lo puso a prueba. A medida que las ciberamenazas crecen y evolucionan, es necesario afinar las respuestas a una serie de escenarios para garantizar que todos en la empresa -no sólo los departamentos de TI y comunicaciones- sepan qué hacer para poner en marcha los planes de recuperación más sencillos posibles en lo que seguramente serán condiciones muy difíciles.

No se trata sólo de un ejercicio de cumplimiento

Sí, los reguladores se están implicando cada vez más. Aun así, es esencial ver la ciberseguridad como lo que realmente es: no sólo una cuestión de cumplimiento, sino una preocupación común, un riesgo compartido para los individuos, las empresas y las sociedades en general. Todos podemos infectarnos unos a otros a través de errores involuntarios, pero también podemos protegernos unos a otros a través de decisiones conscientes, especialmente cuando se trata de la divulgación completa después de un ataque. Dicho sin rodeos, en un mundo donde no hay ciberseguridad, no hay negocio. Así pues, una respuesta y una recuperación eficaces no son sólo asunto de las empresas, sino que conciernen a toda la sociedad.

Metodología

El barómetro de nuestros Socios de Mazars fue diseñado y realizado por GQR Research, en colaboración con Mazars. Los datos se recopilaron a través de una encuesta online entre el 24 de septiembre de 2022 y el 25 de octubre de 2022. La muestra total es de 1.130, de los cuales 1.096 proceden de grupos online y 34 han sido invitados por correo electrónico directamente por Mazars.

Función		Industria		Ingresos Anuales (USD)	
Director General, Presidente, Consejo	706	Servicios financieros	219	$1m-$100m	432
Otras "C-suite" ejecutivas	423	Tecnología y telecomunicaciones	178	$100m - $1bn	350
		Minoristas y productos de consumo	149	$1bn+	348
		Automotriz y manufactura	166		

Región	País	Muestra		Región	País	Muestra	
África y Oriente Medio	Egipto	20	135	Norteamérica	Canada	53	108
	Kenia	20			Estados Unidos de América	55	
	Marruecos	20		Latinoamérica	Argentina	10	171
	Nigeria	20			Brazil	25	
	Sudáfrica	35			Chile	29	
	Emiratos Árabes Unidos	20			Colombia	30	
Asia-Pacífico	Australia	23	198		Mexico	72	
	China	20			Uruguay	5	
	Hong Kong	20		Europa	Francia	50	354
	Indonesia	20			Alemania	60	
	Japón	20			Irlanda	15	
	Malasia	15			Italia	53	
	Filipinas	20			Países Bajos	51	
	Singapur	20			España	50	
	Corea del Sur	20			Suiza	22	
	Vietnam	20			Reino Unido	50	
Europa Central y Oriental	Austria	9	164		Turquía	3	
	Polonia	36		Total	39 países	1,130	
	Rumanía	48					
	Rusia	43					
	Eslovaquia	12					
	Ucrania	16					

Contacto

Yonson Velandia Alvarado
Socio Líder de Consultoría, Mazars
yonson.velandia@mazars.com.co

Andrés Velasco Pacheco
Gerente de Consultoría, Mazars
andres.velasco@mazars.com.co

Mazars es una sociedad internacional integrada, especializada en auditoría, contabilidad, asesoramiento, fiscalidad y servicios jurídicos*. Presentes en más de 90 países y territorios de todo el mundo, contamos con la experiencia de más de 44.000 profesionales -más de 28.000 en la asociación integrada de Mazars y más de 16.000 a través de la Mazars North America Alliance- para ayudar a clientes de todos los tamaños en cada etapa de su desarrollo.

Siempre que lo permita la legislación nacional aplicable

mazars