Estado de Resiliencia en materia de Ciberseguridad 2021

Cómo la alineación de la seguridad y el negocio crea ciberresiliencia

Índice

Sobre los autores

Kelly Bissell

Director Global de Accenture Security

Kelly lidera el negocio de Accenture Security a nivel global. Con más de 25 años de experiencia en el campo de la seguridad, Kelly ha prestado servicios a gobiernos y al sector privado en todas las áreas de ciberseguridad. Su papel como director de Accenture Security abarca desde consultoría estratégica, gestión proactiva de riesgos e identidad digital, hasta ciberdefensa, servicios de respuesta y remedio y servicios de seguridad gestionada en todos los sectores. Kelly también es socio de OASIS, un consorcio sin ánimo de lucro que promueve el desarrollo, la convergencia y la adopción de estándares abiertos para la Sociedad Mundial de la Información.

Jacky Fox

Directora de Tecnología del Grupo de Accenture Security

Jacky lidera la actividad de Accenture Security en Irlanda y ocupa un puesto en el equipo de liderazgo global como Directora de Tecnología del Grupo. Con más de 20 años de experiencia en consultoría tecnológica y de ciberseguridad, Jacky ha trabajado en múltiples sectores de la industria, está especializada en ayudar a las empresas a comprender y tratar sus ciberriesgos y tiene experiencia en la investigación de numerosas violaciones de seguridad nacionales e internacionales. También es vicepresidenta de la junta de Cyber Ireland y es profesora adjunta de investigación forense y seguridad en University College Dublin. Es una conferenciante habitual, con intervenciones en el Foro Económico Mundial, Interpol y Naciones Unidas.

Ryan M. LaSalle

Director General de Accenture Security

Ryan lidera la actividad de Accenture Security en Norteamérica. Es el responsable de apoyar a los equipos con talento que aportan soluciones revolucionadoras para defender y proteger mejor a nuestros clientes. A lo largo de casi dos décadas, ha trabajado con los clientes de Accenture en los sectores comerciales, públicos y sin ánimo de lucro, ayudándoles a identificar e implantar soluciones de tecnologías emergentes que satisfagan sus necesidades de negocio.
Ryan es socio del Ponemon Institute y participa activamente en la Cámara de Comercio de Greater Washington.

Paolo Dal Cin

Director General de Accenture Security

Paolo lidera la actividad de Accenture Security en Europa. Acumula 20 años de experiencia liderando proyectos complejos de los clientes de Accenture. Es un experto en estrategia de seguridad, resiliencia enpresarial, ciberdefensa y ciberofensa, protección de la nube, análisis de datos de seguridad, inteligencia en materia de amenazas, seguridad en aplicaciones, protección de datos y servicios de seguridad gestionada. Ha escrito varios libros sobre seguridad y es un ponente habitual en eventos de seguridad. Paolo enseñó seguridad de las tecnologías de la información y la comunicación en las universidades de Udine, Módena Milán, en Italia.

Agradecimientos

Los autores desean agradecer a Edward Blomquist, Julia Malinska, Anna Marszalik, Eileen Moynihan, Vincenzo Palermo y Ann Vander Hijde sus aportaciones a este informe.

Defendiendo la ciberseguridad

Defendiendo la ciberseguridad

En nuestra encuesta anual a 4.744 encuestados globales sobre el estado actual de resiliencia en materia de ciberseguridad, descubrimos que muchos Directores de Seguridad de la Información (CISO) creen que hace mucho tiempo que se debería haber reconocido su papel a la hora de llevar a cabo la estrategia empresarial. El 85% está de acuerdo o muy de acuerdo en que la estrategia de ciberseguridad se desarrolla teniendo en mente objetivos empresariales, tales como el crecimiento o la cuota de mercado.

Aún así, la mayoría de los directivos (78%) afirmaron que no saben cómo ni cuándo un incidente de ciberseguridad afectará a sus empresas. Es una opinión que continúa extendiéndose desde nuestro informe de 2020, cuando ya era alta con un 69%.

La mayoría de los encuestados (81%) declaró que «mantenerse un paso por delante de los atacantes es una batalla constante y el coste es insostenible», en comparación con el 69% de 2020. De hecho, descubrimos que los encuestados experimentaron un aumento del 32%, con respecto a 2020, en el número de ciberataques efectivos, mientras que algunos ataques, como los de ransomware, han sufrido un incremento mucho mayor.

Este año, continuamos con nuestro análisis de los líderes en ciberresiliencia. Debido al rápido aumento de los ataques de perfil alto y la total complejidad de la gestión de exigencias de ciberseguridad, hemos comprobado también la diferencia que suponía para la ciberresiliencia si existía una mayor alineación entre las prácticas de ciberseguridad y la estrategia empresarial.

¿Qué es la ciberresiliencia?

El negocio ciberresiliente aúna las capacidades de ciberseguridad, continuidad del negocio y resiliencia empresarial. Integra la seguridad en todo el ecosistema empresarial y aplica estrategias de seguridad para responder rápidamente a las amenazas, de manera que se pueda minimizar el daño y seguir operando ante un ataque. Como resultado, el negocio ciberresiliente puede introducir de manera segura ofertas y modelos de negocio innovadores en toda la cadena de valor, reforzar la confianza del cliente y crecer con seguridad.

Nuestra investigación identificó cuatro niveles de ciberresiliencia (Gráfica 1). Encabezando el conjunto se encuentra un grupo de 'ciber defensores', empresas que han encontrado el equilibrio, no solo destacando en ciberresiliencia, sino también en alineación con la estrategia de negocio para obtener mejores resultados empresariales. Tienen éxito en al menos tres de los cuatro criterios de rendimiento en ciberresiliencia: son mejores a la hora de detener ataques, detectar y remediar brechas de seguridad más rápidamente y reducir su impacto.

También identificamos dos nuevos grupos que reflejan diferentes enfoques sobre ciberresiliencia: 'Los obstaculizadores del negocio', que anteponen la ciberseguridad a la alineación con la estrategia empresarial, y 'los que asumen ciberriesgos', quienes anteponen la estrategia empresarial a la alineación con la ciberseguridad. El cuarto nivel de ciberresiliencia lo hemos identificado como 'los vulnerables'.

Es importante dónde se sitúan las empresas en este cibercuadrante; hay dinero en juego. 'los obstaculizadores del negocio' verían reducidos sus costes de violaciones de seguridad un 48%, 'los que asumen ciberriesgos', un 65%, y 'los vulnerables', un 71%, si aumentaran su rendimiento a los niveles de 'los ciberdefensores'.

El cibercuadrante

Gráfica 1. Cuatro niveles de ciberresiliencia

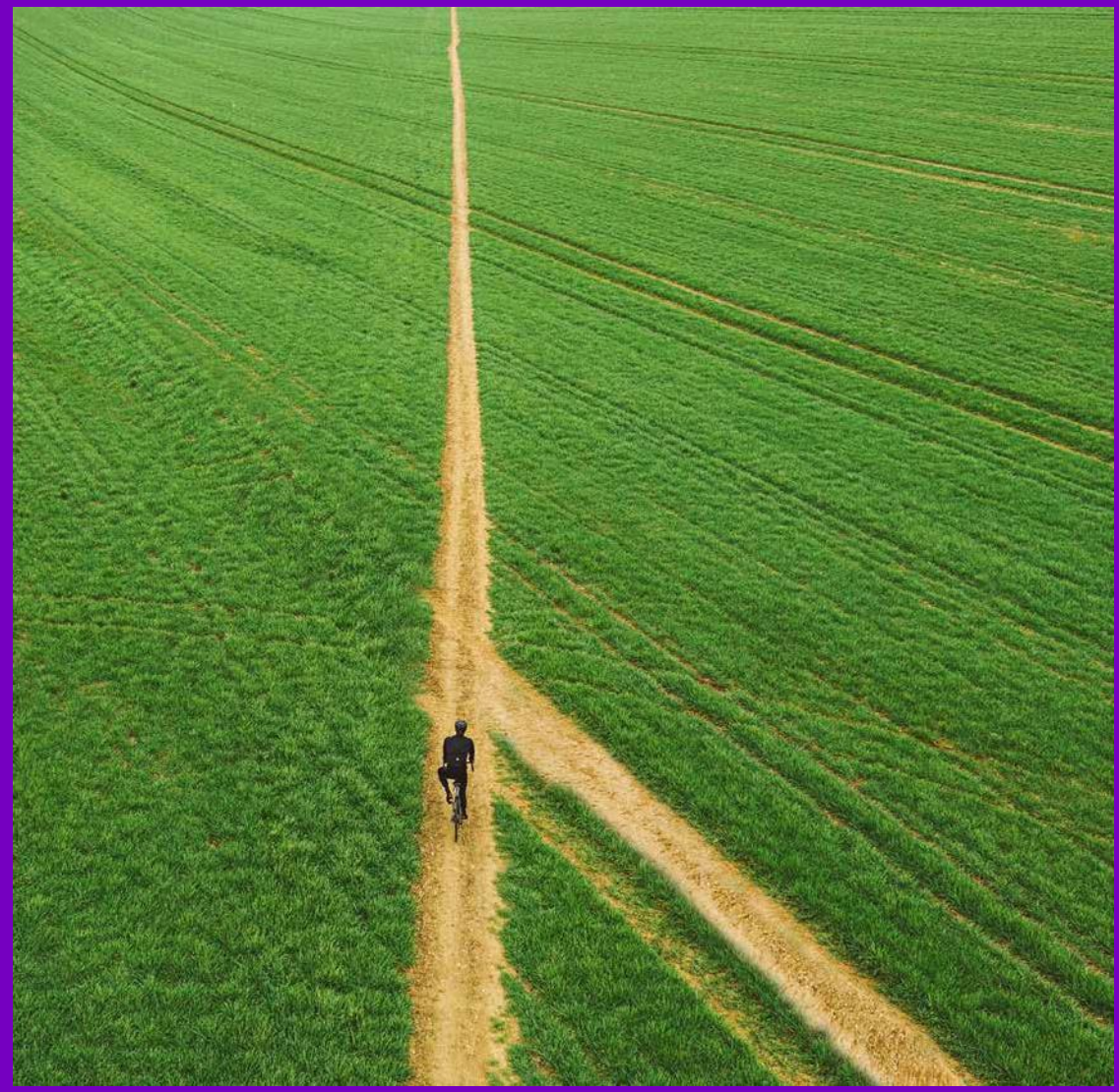
Nuestro informe muestra la diferencia de lo que supone un año y cómo las empresas líderes están demostrando su resiliencia en materia de ciberseguridad.

¿Dónde estamos ahora?

Los ciberataques están en alza

La inversión en seguridad continúa aumentando

La nube todavía mantiene una relación compleja con la seguridad



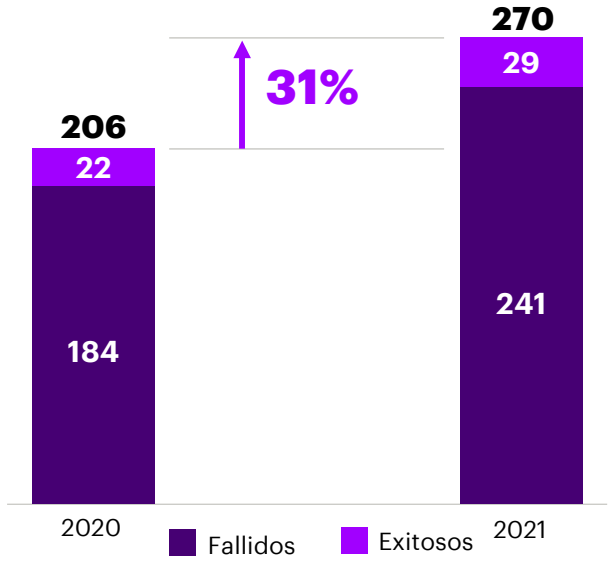
Los ciberataques están en alza

Ni siquiera una pandemia mundial puede frenar a los ciberdelincuentes; en todo caso, la vulnerabilidad y la incertidumbre fueron un caldo de cultivo para nuevos ataques. Hubo una media de 270 ataques (accesos no autorizados a datos, aplicaciones, servicios, redes o dispositivos) por empresa a lo largo del año, un aumento del 31% en comparación con 2020 (Gráfica 2).

El riesgo de terceros sigue predominando. Los ataques indirectos, es decir, las violaciones efectivas contra la empresa a través de la cadena de valor, han crecido de un 44% a un 61%.

Y el impacto de la ciberseguridad ha entrado con fuerza en el consejo de administración. En un análisis de los informes de ingresos de 2020 de más de 500 compañías, ha habido un incremento de los debates legales (23%), económicos (16%) e internos (10%) sobre las consecuencias de la ciberseguridad con respecto a 2019, lo que sugiere un aumento de la priorización del tema.[1]

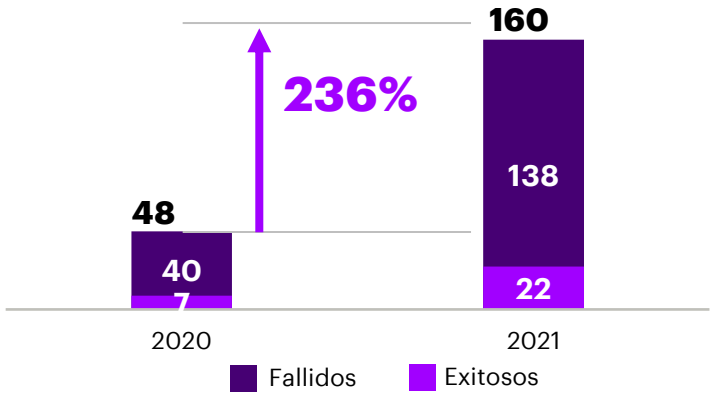
Gráfica 2. La media de ataques por empresa ha aumentado un 31 %. Muestra global.



Fuente: Encuestas de Accenture sobre el Estado de la Ciberseguridad Informe Wave 3 publicado en enero de 2020 (N=4.644) e informe Wave 4 publicado en noviembre de 2021 (N=4.744)

Si observamos los resultados de la muestra efectuada en España, el incremento de los ciberataques fue de un 260% respecto a 2020. Respecto al resto de porcentajes, la media en España se encuentra dentro del rango de resultados que muestra la encuesta global.

Gráfica 2.1 La media de ataques por empresa en España ha aumentado un 236 %. Muestra local.



Fuente: Encuestas de Accenture sobre el Estado de la Ciberseguridad Informe Wave 3 publicado en enero de 2020 (N=4.644) e informe Wave 4 publicado en noviembre de 2021 (N=4.744) Spain N=251

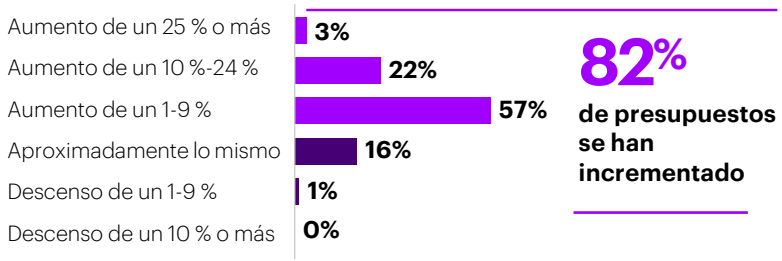
La inversión en seguridad continúa aumentando

Los presupuestos de seguridad de TI están elevándose, con más de un 82% de los encuestados de nuestro estudio afirmando que sus presupuestos han aumentado en el último año (Gráfica 3). Los presupuestos de seguridad de TI alcanzan ahora hasta un 15% del gasto total en TI, 5 puntos porcentuales más que el gasto declarado en 2020.[2]

Esto puede deberse al cambio provocado por la COVID-19, el giro rápido y masivo en la manera de gestionar los negocios y el aumento de las exigencias de seguridad; no sabremos hasta el próximo año si este tipo de inversión se mantendrá, pero sí sabemos que los presupuestos siempre están en el punto de mira. La rápida adopción de la nube también puede contribuir a este aumento de la inversión, ya que muchas herramientas de seguridad deben actualizarse para alojar la nube o se necesita una seguridad más sólida en un mundo digital.

Quizás este aumento del gasto ha favorecido el optimismo. De media, un 70% cree que su empresa está activamente protegida por su programa de ciberseguridad, en comparación con el 60% de 2020. También se sienten más confiados con respecto el panorama general: el 67% considera que sus ecosistemas son seguros, en comparación con el 60% de 2020.

Gráfica 3. Aumento del gasto en ciberseguridad de 2021 comparado con el de 2020



Fuente: Estado de Resiliencia en materia de Ciberseguridad de Accenture 2021 (N=4.744)

«Durante mi mandato de cuatro años, triplicamos, o puede que cuadruplicáramos, el presupuesto de seguridad. Empezamos de cero, así que tuvimos que sobreinvertir en sistemas e infraestructuras de seguridad para llegar al nivel en el que teníamos que estar.»

Director Global de TI, empresa farmacéutica

La nube todavía mantiene una relación compleja con la seguridad

Entre los próximos tres a cinco años, más de dos tercios de las cargas de trabajo se transferirán a la nube, con alrededor de un tercio de empresas transfiriendo más de un 75% a la nube en la mayoría de regiones del mundo.[3]

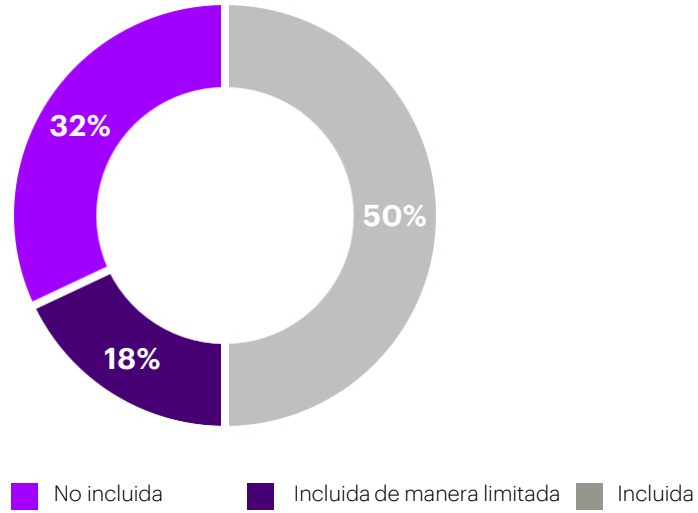
De esto se hace eco nuestra reciente investigación sobre estrategias de innovación tecnológica, que concluyó que el 10% de los encuestados de la parte superior de la tabla duplicaron su inversión en tecnología durante la pandemia, mientras que un 72% aceleró la inversión en seguridad.[4]

Los encuestados de nuestro estudio sobre ciberresiliencia afirman que han migrado sus operaciones a la nube ya que reconocen sus beneficios cómo costes más bajos, operaciones más resilientes y acceso a tecnología más avanzada.

Con todo, a pesar de que la mayoría de los encuestados de nuestro estudio creen que las aplicaciones y las operaciones en la nube son más seguras que las alojadas en las propias instalaciones, casi un tercio (32%) afirma que la seguridad no ha sido parte del debate sobre la nube desde el principio y que su empresa está intentando ponerse al día (Gráfica 4).

Y los motivos que impiden que la nube despegue giran alrededor de cuestiones de seguridad: alrededor de un tercio de los encuestados declararon que un gobierno y unas prácticas de cumplimiento deficientes en lo que respecta a la seguridad de la nube, constituyen un problema, que la seguridad de la nube es demasiado compleja y que no tienen las habilidades a nivel interno para estructurar un marco adecuado de seguridad de la nube.

Gráfica 4. Casi un tercio de los encuestados afirman que la seguridad no es parte del debate sobre la nube



Source: Accenture State of Cybersecurity Resilience 2021 (N=4,744)

¿Por qué es importante la alineación?

¿Por qué es importante la alineación?

La investigación de este año siguió explorando cómo abordan las empresas exitosas la ciberresiliencia, evaluando sus respuestas a partir de las siguientes medidas claves de ciberresiliencia: detienen más ataques, detectan y remedian violaciones de seguridad más rápido y reducen su impacto.

También observamos el impacto que tiene sobre la ciberresiliencia estar alineado con la estrategia de negocio e identificamos cuatro niveles de ciberresiliencia: 'los ciberdefensores', 'los obstaculizadores del negocio', 'los que asumen ciberriesgos'y 'los vulnerables' (Gráfica 5).

Examinemos las diferencias en las posiciones del cibercuadrante y las implicaciones para el rendimiento del negocio y la ciberresiliencia.

Gráfica 5. Medidas claves de ciberresiliencia

	'Los ciberdefensores'	'Los obstaculizadores del negocio'	'Los que asumen ciberriesgos'	'Los vulnerables'
Detienes más ataques: Número de ataques que violan la seguridad	**1 de 4**	**1 de 4**	**1 de 2**	**1 de 2,3**
Detectan violaciones más rápido: % violaciones detectadas en < 1 día	**55%**	**50%**	**11%**	**15%**
Remedian violaciones más rápido: % remediadas en 15 días o menos	**100%**	**96%**	**30%**	**30%**
Reducen el impacto de las violaciones: % violaciones sin impacto	**72%**	**64%**	**23%**	**24%**

Fuente: Estado de Resiliencia en materia de Ciberseguridad de Accenture 2021, ejecutivos de seguridad (=3.455: 'los ciberdefensores' N=172, '"Los obstaculizadores del negocio'"N=522, 'los que asumen ciberriesgos'N=885, 'Los vulnerables' N=1.876)

Los obstaculizadores del negocio

‘Los obstaculizadores del negocio’ adoptan un enfoque que prioriza la seguridad y ponen menos énfasis en la alineación con la estrategia de negocio. A veces se perciben como un obstáculo para los objetivos empresariales.

¿Por qué es importante la alineación?

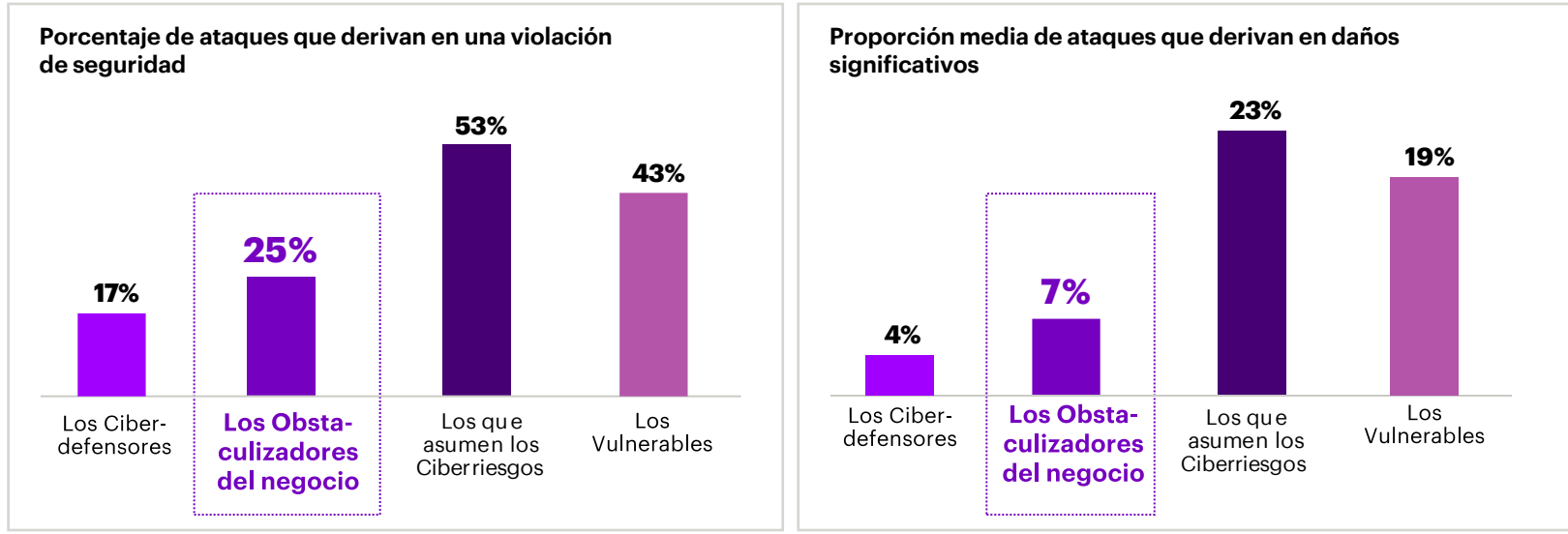
‘Los obstaculizadores del negocio’ superan a 'los que asumen ciberriesgos’ y a ‘los vulnerables', pero van a la zaga de 'los ciberdefensores' en todas las medidas claves de ciberresiliencia. Tal y como ilustra la Gráfica 6, sufren menos violaciones que 'los que asumen ciberriesgos' y ‘los vulnerables', pero 8 puntos porcentuales más que ‘los ciberdefensores' (17%).

En lo que respecta a la proporción de ataques significativos, con un impacto grave, a largo plazo y de perfil alto sobre el negocio o la misión de la empresa, experimentan menos que 'los que asumen ciberriesgos'y ‘los vulnerables', pero casi más del doble que ‘los ciberdefensores’.

Y cuando los ataques logran abrirse paso, ‘los obstaculizadores del negocio’ los detectan y los remedian más rápido que ‘los que asumen ciberriesgos' y ‘los vulnerables’, pero van un día por detrás de 'los ciberdefensores' en ambas medidas.

'Los obstaculizadores del negocio’ también tienen el porcentaje más alto de CISOs con autoridad plena para aprobar presupuestos (32%) en comparación con ‘los ciberdefensores' (21%), 'los que asumen ciberriesgos' (21%) y ‘los vulnerables' (16%). La autonomía de los CISOs a la hora de decidir el gasto puede explicar el foco creciente en la ciberseguridad por encima de la estrategia empresarial.

Gráfica 6. Impacto de las violaciones de seguridad sobre ‘Los obstaculizadores del negocio'



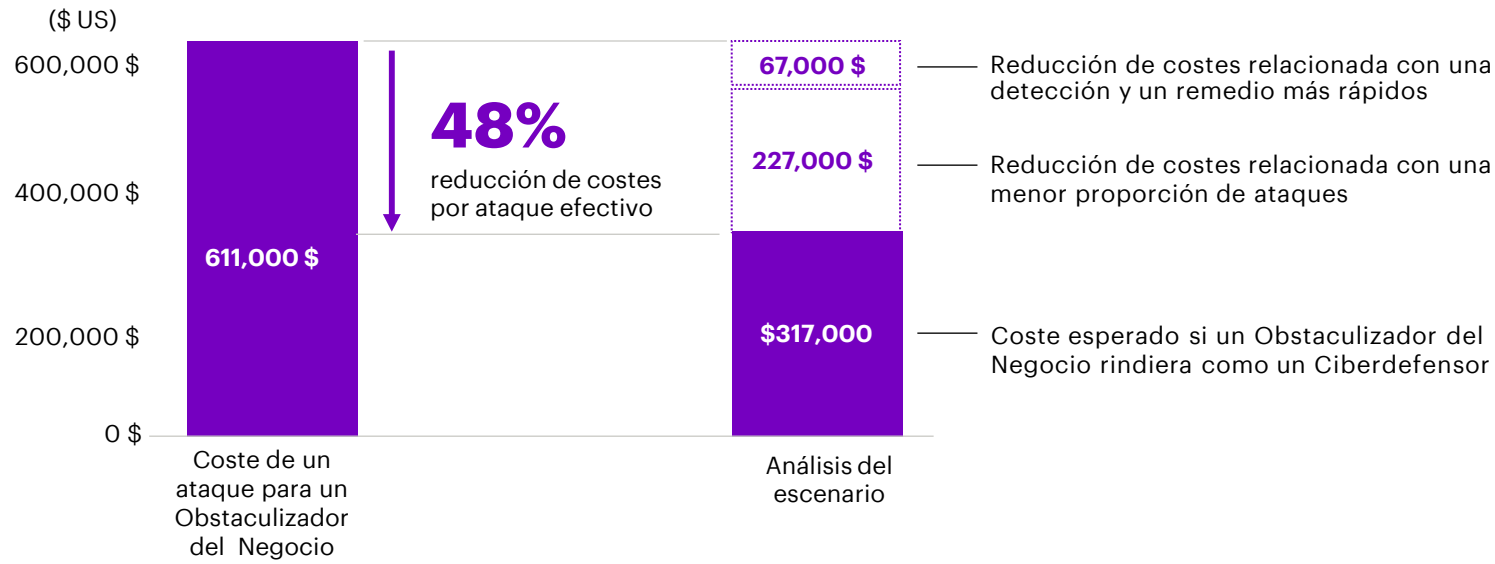
Fuente: Estado de Resiliencia en materia de Ciberseguridad de Accenture 2021, ejecutivos de seguridad
(N=3.455: "los ciberdefensores" N=172, "'Los obstaculizadores del negocio'"N=522, 'los que asumen ciberriesgos'N=885, 'Los vulnerables' N=1.876)

¿Por qué es importante la alineación?

Si ‘los obstaculizadores del negocio' añadieran la alineación a su ya sólida base de ciberseguridad, tendrían una ciberresiliencia todavía mayor sin sacrificar los resultados empresariales.

‘Los obstaculizadores del negocio’ podrían reducir sus costes un 48% por ataque efectivo si aumentaran su rendimiento hasta los niveles de 'los ciberdefensores', con un ahorro de aproximadamente 294.000 $ US por ataque (Gráfica 7).

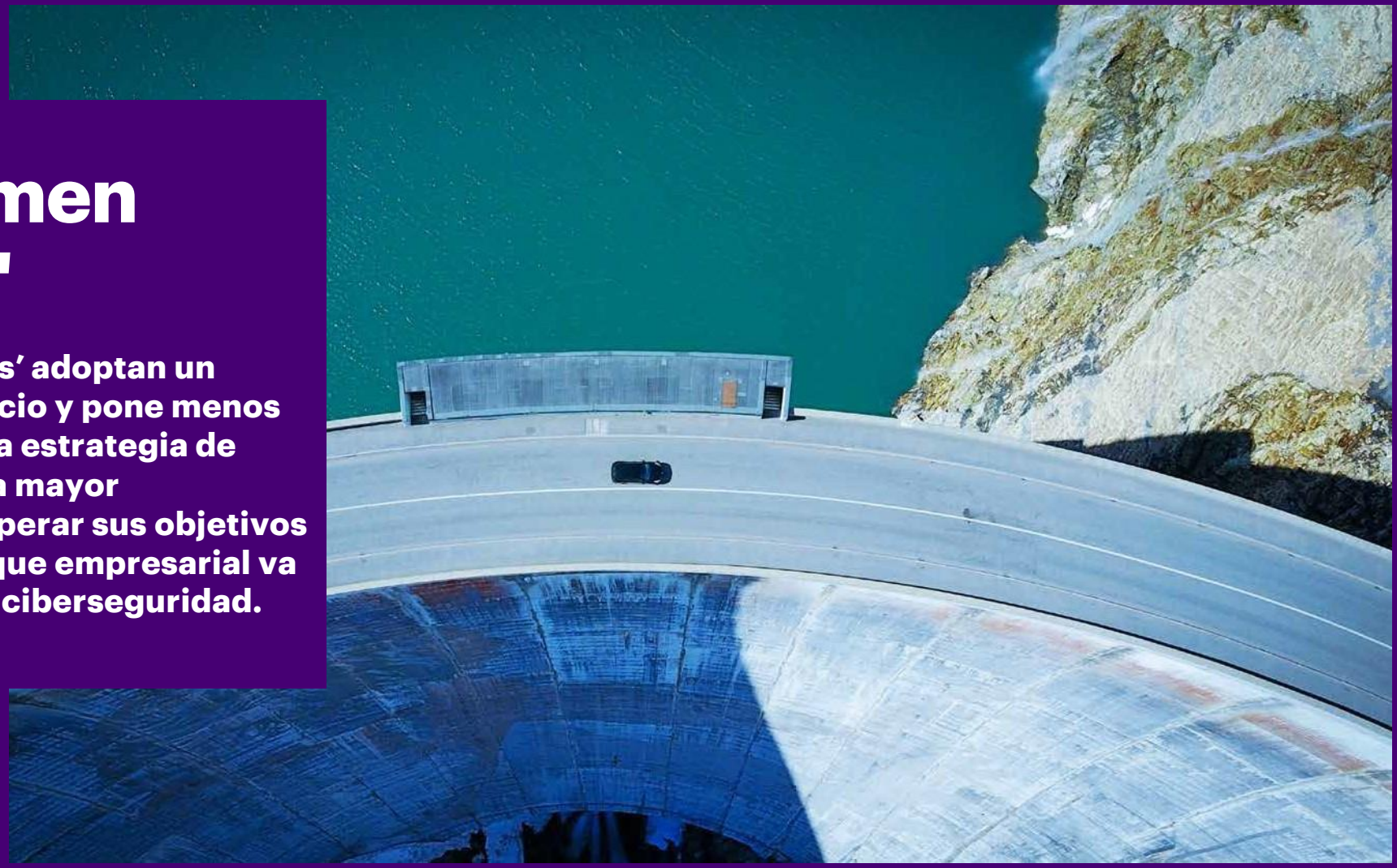
Gráfica 7. Valor en juego si ‘los obstaculizadores del negocio’ rindieran como ‘los ciberdefensores'



Nota: Asignamos el mismo nivel de rendimiento a '"Los obstaculizadores del negocio"'que a las empresas Ciberdefensoras en todas las métricas de ciberresiliencia, como la velocidad de detección/remedio y la proporción de ataques significativos, y simulamos los resultados de costes. N=522

'Los que asumen ciberriesgos'

'Los que asumen ciberriesgos' adoptan un enfoque que prioriza el negocio y pone menos énfasis en la alineación con la estrategia de ciberseguridad. Refieren una mayor probabilidad de cumplir o superar sus objetivos empresariales, pero su enfoque empresarial va en detrimento de su éxito en ciberseguridad.



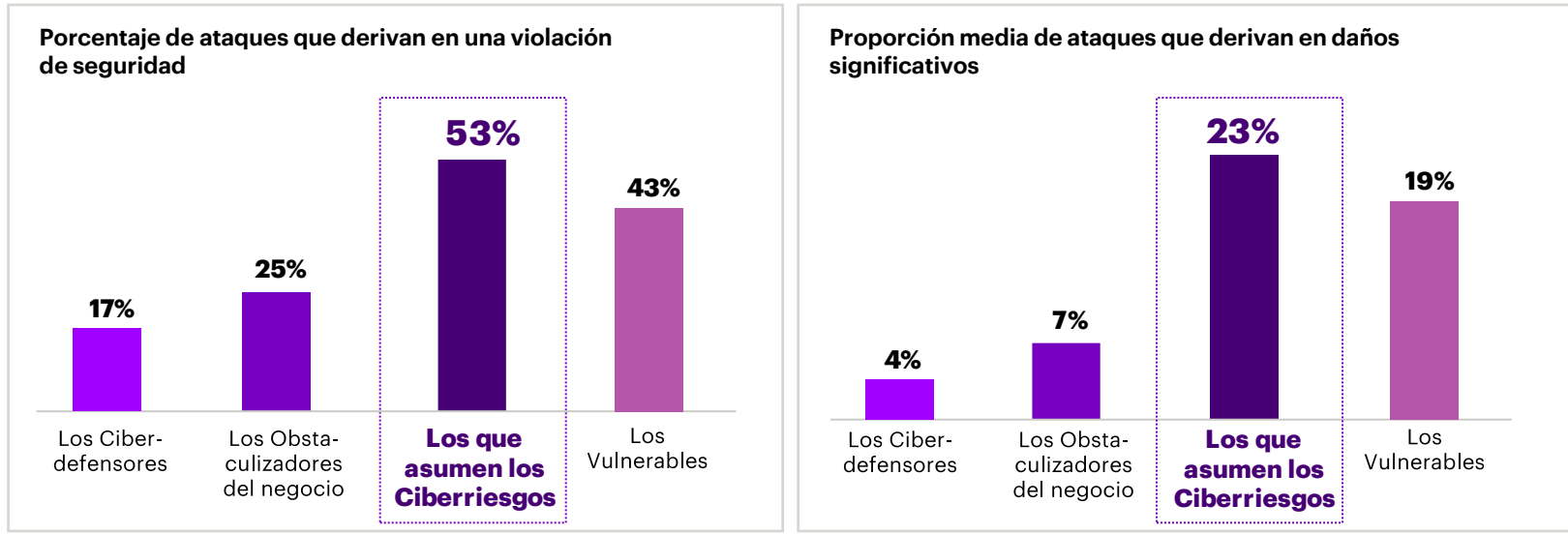
¿Por qué es importante la alineación?

'Los que asumen ciberriesgos' son líderes en la obtención de resultados empresariales en ocho áreas de negocio de nuestro estudio, incluyendo reducción de costes, crecimiento empresarial, comercialización más rápida, obtención de cuota de mercado, desarrollo de nuevos productos/servicios, penetración en nuevos mercados, mayor satisfacción del cliente y experiencia del usuario sin fricciones.

De manera significativa, 'los que asumen ciberriesgos' asignan a la ciberseguridad un presupuesto más alto y, aún así, la cifra de violaciones efectivas es el doble de alta que la de 'los obstaculizadores del negocio' y 10 puntos porcentuales más alta que la de 'los vulnerables'. Asignar un presupuesto más elevado no se traduce en una mejor ciberresiliencia.

A pesar de centrarse en los objetivos empresariales, el rendimiento de 'los que asumen ciberriesgos' se encuentra entre los más bajos en lo que se refiere a la media de violaciones efectivas y la de ataques significativos (Gráfica 8).

Gráfica 8. Impacto de las violaciones de seguridad sobre 'los que asumen ciberriesgos'



Fuente: Estado de Resiliencia en materia de Ciberseguridad de Accenture 2021, ejecutivos de seguridad
(N=3.455: 'los ciberdefensores' N=172, '"Los obstaculizadores del negocio'"N=522, 'los que asumen ciberriesgos'N=885, 'Los vulnerables' N=1.876)

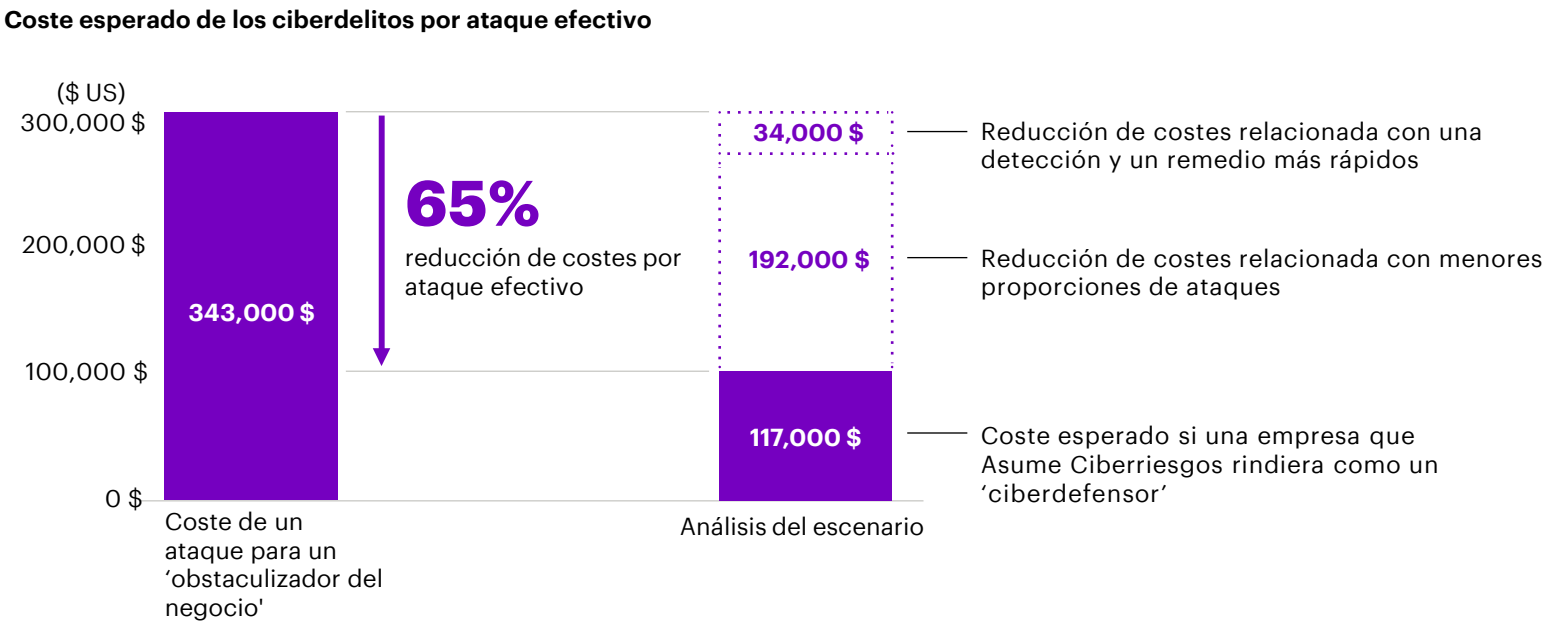
¿Por qué es importante la alineación?

Y tienen un problema de asignación de recursos. Les falta visibilidad, toman decisiones de inversión con retraso y con métricas poco claras, demuestran una asignación de fondos deficiente. Con menos CISOs autorizando el presupuesto de seguridad, puede ser que 'los que asumen ciberriesgos' sean ricos en efectivo, pero pobres en conocimientos sobre cómo gastar sus presupuestos de ciberseguridad.

Si bien poner el foco únicamente sobre la alineación puede acarrear potenciales y significativos beneficios empresariales, sin una base de ciberresiliencia, las empresas estarán expuestas a un mayor riesgo y tendrán costes de ciberseguridad más elevados.

'Los que asumen ciberriesgos' podrían reducir sus costes un 65% por ataque efectivo si aumentaran su rendimiento a los niveles de 'los ciberdefensores', con ahorros de alrededor de 226.000 $ US por ataque (Gráfica 9).

Gráfica 9. Valor en juego si 'los que asumen ciberriesgos' rindieran como 'los ciberdefensores'



Nota: Asignamos el mismo nivel de rendimiento a 'los que asumen ciberriesgos'que a 'los ciberdefensores' en todas las métricas de ciberresiliencia, como la velocidad de detección/remedio y la proporción de ataques significativos, y simulamos los resultados de costes. N=885

'Los ciberdefensores'

'Los ciberdefensores' son lo mejor de lo mejor. Al igual que 'los obstaculizadores del negocio', 'los ciberdefensores' están entre el 30 % de la parte alta de la tabla en al menos tres de los cuatro criterios de ciberresiliencia.
Lo que les diferencia es su estrecha alineación con la estrategia de negocio.

¿Por qué es importante la alineación?

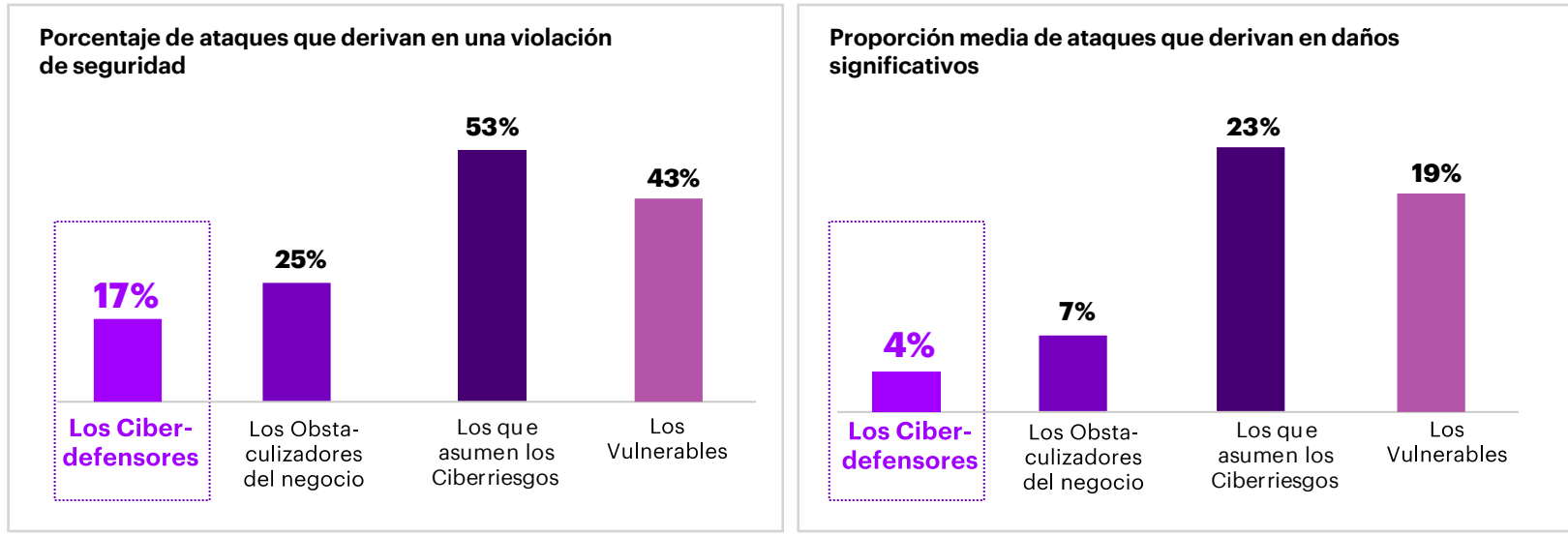
El número de violaciones efectivas sufridas por 'los ciberdefensores' es 8 puntos porcentuales más bajo que el de 'los obstaculizadores del negocio' y 36 puntos más bajo que 'los que asumen ciberriesgos' y, además, reciben menos ataques significativos (Gráfica 10).

'Los ciberdefensores' tienen una respuesta de detección y remedio más ágil: un día extra de plena operatividad puede marcar toda la diferencia.

'Los ciberdefensores' son más capaces de protegerse frente a la pérdida de datos; alrededor de un 4 % de 'los ciberdefensores' pierden más de 500.000 registros, 6,5 veces menos que 'los que asumen ciberriesgos' situados en el 27 %.

Parte del éxito de 'los ciberdefensores' en la alineación con el negocio puede ser resultado de que tienen una mayor proporción de líderes de unidades empresariales a cargo de la ciberseguridad, casi el doble (1,9 veces) que 'los que asumen ciberriesgos'.

Gráfica 10. Impacto de las violaciones de seguridad sobre 'los ciberdefensores'

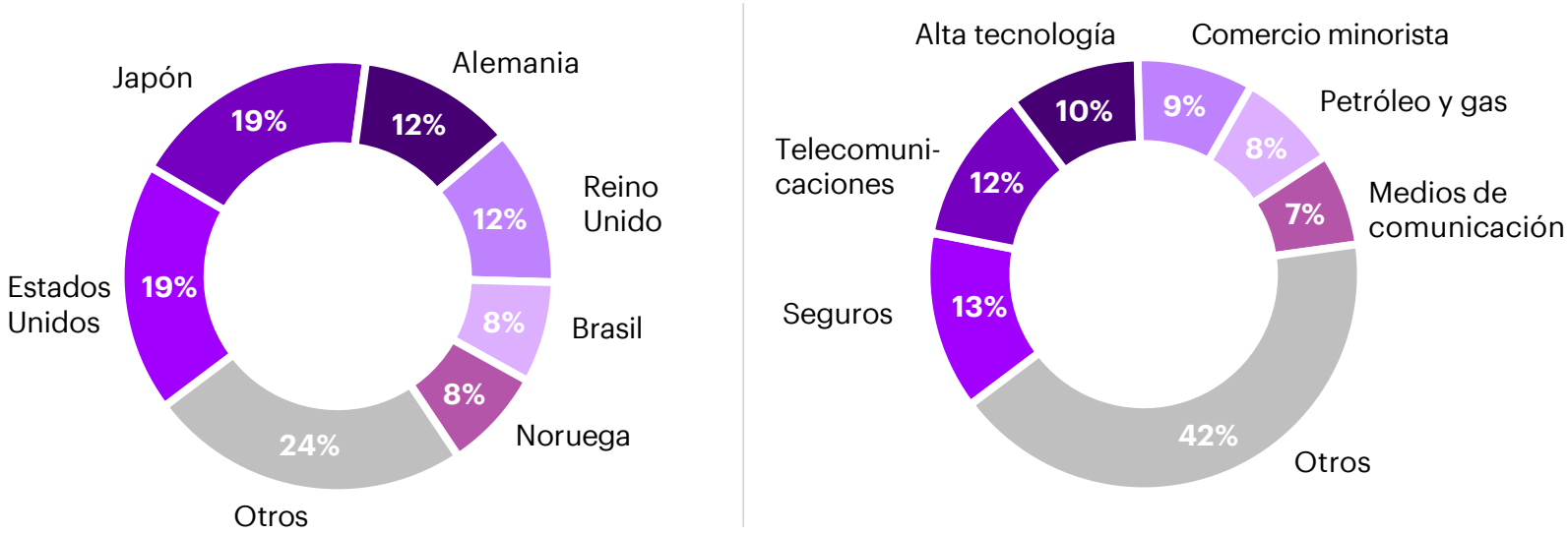


Fuente: Estado de Resiliencia en materia de Ciberseguridad de Accenture 2021, ejecutivos de seguridad
(N=3.455: 'los ciberdefensores' N=172, 'Los obstaculizadores del negocio'N=522, 'los que asumen ciberriesgos'N=885, 'los vulnerables' N=1.876)

¿Por qué es importante la alineación?

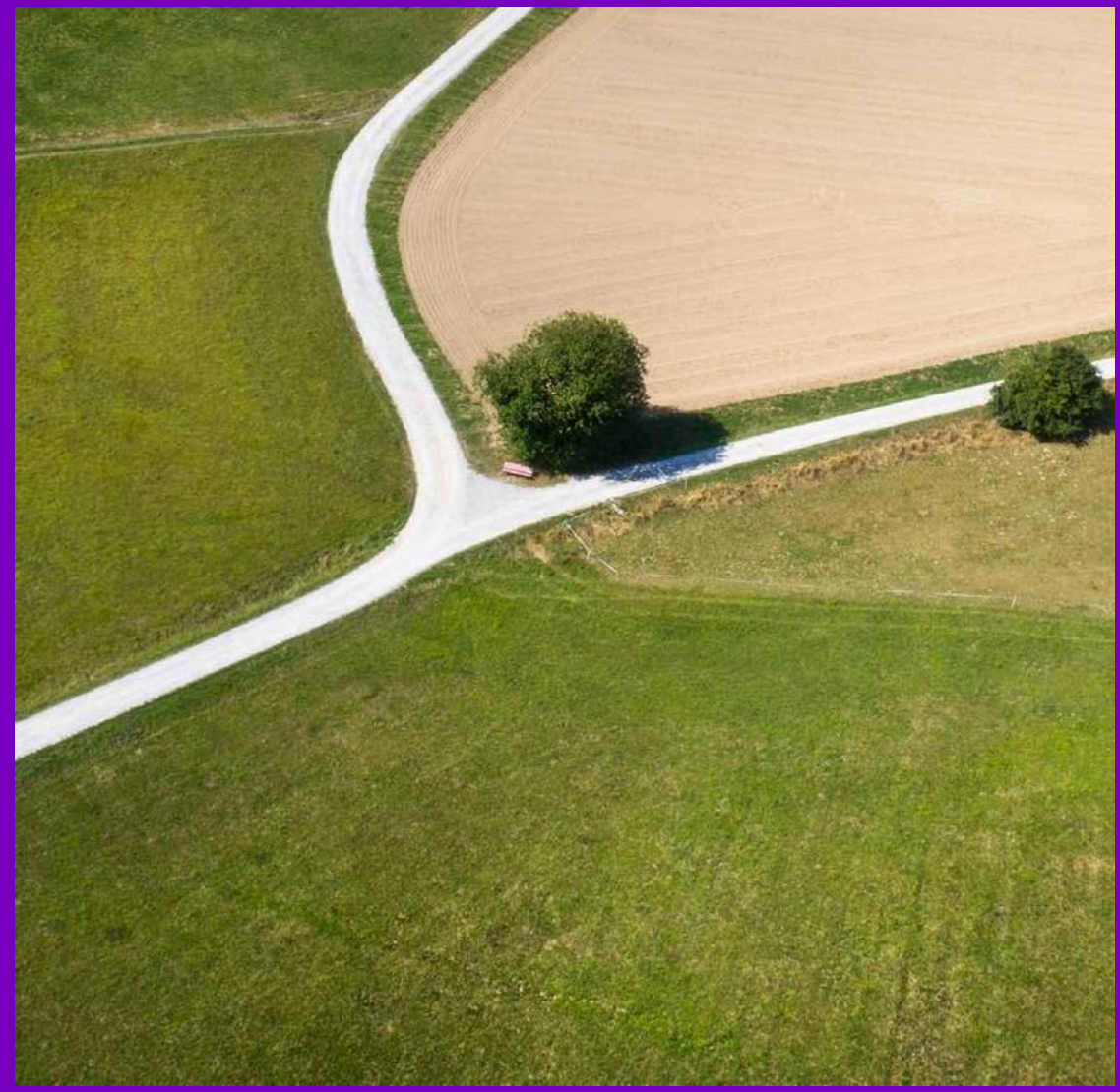
Los principales países y sectores representados en 'los ciberdefensores' incluyen Estados Unidos, Japón, Reino Unido y Alemania y seguros, telecomunicaciones, alta tecnología y comercio minorista, respectivamente. (Gráfica 11).

Gráfica 11. Ciberdefensores, principales países y sectores representados



Fuente: Estado de Resiliencia en materia de Ciberseguridad de Accenture 2021, 'los ciberdefensores' (N=172)

Cómo convertirse en un 'ciberdefensor'



Ofrecer a los CISOs un sitio en el consejo directivo.

Centrarse en las amenazas y estar alineado con el negocio.

Sacarle el máximo partido a una nube segura.

Ofrecer a los CISOs un sitio en el consejo directivo

Los CISOs deben alejarse de los silos centrados en la seguridad y colaborar con los ejecutivos adecuados de la organización para comprender los riesgos y las prioridades empresariales. Sirviéndose de la experiencia y los conocimientos del equipo ejecutivo, los CISOs pueden obtener una perspectiva más amplia que funcione bien para toda la empresa.

Descubrimos que 'los ciberdefensores' se distinguen del resto en lo que se refiere a sus estructuras jerárquicas. Alrededor de un 70% del grupo responden ante el CEO y el Consejo y demuestran tener una relación mucho más estrecha con el CFO (la presentación de informes es 7 veces más alta que en otros grupos).

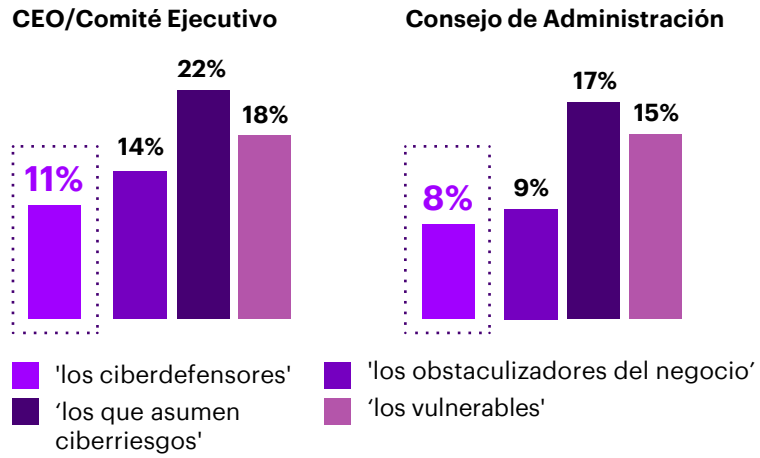
'Los ciberdefensores' sacan partido de estas relaciones a la hora de definir la estrategia. Consultan principalmente al CEO (51%) y al CFO (49%) para desarrollar la estrategia de ciberseguridad de su empresa, casi el doble que 'los obstaculizadores del negocio'.

En lo que se refiere a autorización de presupuestos, los CEOs o el Consejo solo autorizan los presupuestos en el 19% para 'los ciberdefensores', en comparación con el 23% de 'los obstaculizadores del negocio' y el 39% de 'los que asumen ciberriesgos' (Gráfica 12). Esto sugiere que 'los ciberdefensores' tienen más autonomía en lo que respecta a las finanzas y dependen menos del CEO y el Consejo para obtener autorización.

«El negocio está extremadamente alineado con el CISO. La razón es muy simple. La ciberseguridad es una de las tres principales prioridades comunicadas por nuestro presidente y la alta dirección. Si no tienes el visto bueno de ciberseguridad, el producto simplemente no sale adelante.»

CISO, banco regional estadounidense

Gráfica 12. 'los ciberdefensores' tienen más autonomía: solo un 19% tiene su presupuesto autorizado por el CEO o el Consejo



Fuente: Estado de Resiliencia en materia de Ciberseguridad de Accenture 2021, ejecutivos de seguridad (=3.455: 'los ciberdefensores' N=172, 'los obstaculizadores del negocio' N=522, 'los que asumen ciberriesgos' N=885, 'los vulnerables' N=1.876)

Centrarse en las amenazas y estar alineado con el negocio

Los CISOs solo tienen que pensar en el aumento interanual del 160% en incidencias de ransomware en 2020 para darse cuenta de que los ciberataques están provocando un enfoque de «mejor prevenir que curar».[5]

Dado que el remedio puede alcanzar 30 veces el coste de la prevención, una vez que se produce un ataque de ransomware, uno de los mayores retos cuando dañan un entorno empresarial es entender las prioridades. ¿Cuál es el sistema más importante de su red que hay que recuperar? ¿De qué dependen sus ingresos? ¿Qué es lo más crítico para sus operaciones?

Mantener a los atacantes fuera de su entorno depende de que los líderes de seguridad estén estrechamente alineados con el negocio colaborando para reducir el riesgo. Esta alineación ayuda a integrar la seguridad en las prioridades empresariales.

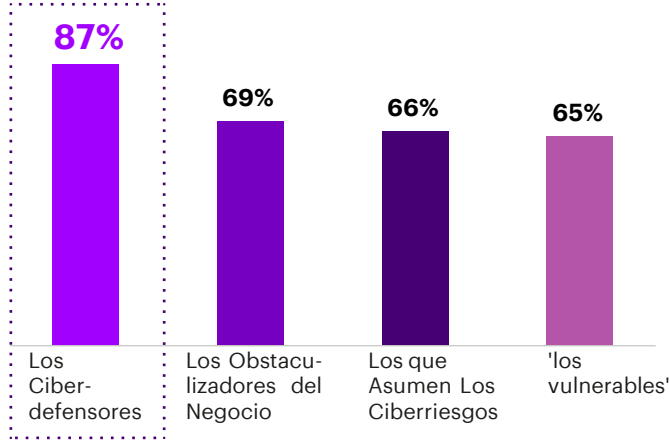
'Los ciberdefensores' entienden la importancia del equilibrio entre la seguridad y el negocio; miden y supervisan su estado con frecuencia para mejorar de manera continua su función de seguridad y que el negocio pueda gestionar el riesgo.

Descubrimos que casi el 90% de 'los ciberdefensores' miden la madurez de su programa de ciberseguridad al menos una vez al año o con mayor frecuencia, un 18 % más que 'los obstaculizadores del negocio' (Gráfica 13). Esto indica que 'los ciberdefensores' entienden claramente los riesgos, mientras que para 'los obstaculizadores del negocio' pueden pasar desapercibidos.

Midiendo y supervisando sus perfiles de riesgo y poniendo los datos a disposición de la dirección, los CISOs pueden alinearse mejor con el negocio.

> «Hacemos un seguimiento de los datos en cuatro áreas: efectividad de la ciberseguridad, cibercultura de la empresa, preparación de ciberseguridad y resiliencia de ciberseguridad. Supervisamos la eficacia con la que alineamos nuestros planes con los procesos clave y lo que sucede en el negocio.»
>
> CISO, gran empresa del sector minero

Gráfica 13. 'los ciberdefensores' miden la madurez de la ciberseguridad con frecuencia



Fuente: Accenture State of Cybersecurity Resilience 2021, ejecutivos de segurid (N=3.455: 'los ciberdefensores' N=172, 'los obstaculizadores del negocio' N=522 'los que asumen ciberriesgos' N=885, 'los vulnerables' N=1.876)

Sacarle el máximo partido a una nube segura

La seguridad debería estar integrada sistemáticamente en la nube. Con demasiada frecuencia, la seguridad se añade al final del camino hacia el cloud-first, lo que puede retrasar los resultados empresariales o incluso obligar a repetir todo el trabajo con un coste elevado.

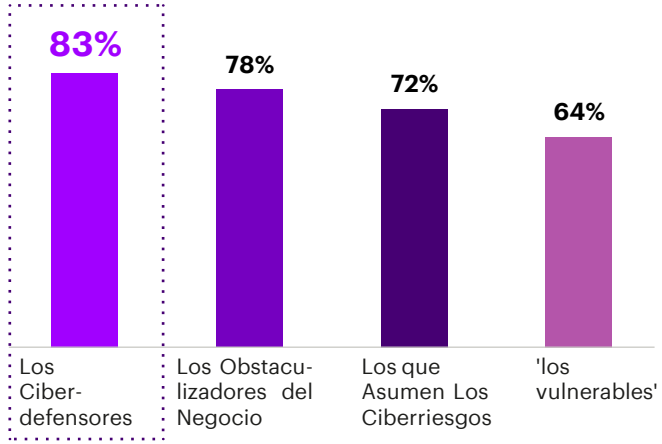
La seguridad en la nube puede permitir obtener mejores resultados empresariales gracias a su rapidez, su ausencia de fricciones, su carácter escalable, proactivo y rentable respecto a los costes.[6]

Con un cambio acelerado hacia el uso de la nube, es importante sacarle el máximo partido. Cuando migran a la nube, las empresas deberían aprovechar la oportunidad para reajustar su postura en términos de seguridad, de manera más temprana y efectiva, tal y como hacen nuestros 'ciberdefensores'.

La mayoría de 'los ciberdefensores' (83%) afirman que la seguridad es un factor muy importante a la hora de transferir operaciones a la nube, frente al 70% de la muestra general. 'Los ciberdefensores' son mejores en lo que respecta a incluir la seguridad en sus iniciativas de la nube; no perciben la implicación de la seguridad como un impedimento significativo para los debates sobre la nube (Gráfica 14).

'Los ciberdefensores' saben lo que hacen: trabajan estrechamente alineados con el negocio para realizar la migración a la nube de manera más segura.

Gráfica 14. 'los ciberdefensores' migran a la nube con la seguridad en mente



Fuente: Estado de Resiliencia en materia de Ciberseguridad de Accenture 2021, ejecutivos de seguridad (=3.455: 'los ciberdefensores' N=172, '"los obstaculizadores del negocio' N=522, 'los que asumen ciberriesgos' N=885, 'los vulnerables' N=1.876)

¿Están los ejecutivos de seguridad y los ajenos a seguridad en la misma página?

Nuestro estudio más reciente demuestra que todavía hay diferencias en cómo ven las cosas los ejecutivos de seguridad y los ejecutivos ajenos a seguridad. En conjunto, sus respuestas ponen de manifiesto la brecha entre los ejecutivos de seguridad y los ajenos a seguridad en lo que respecta a cómo perciben la efectividad de la seguridad, su presupuesto y los riesgos de ataques (Gráfica 15).

Cuando preguntamos sobre los obstáculos que impiden a sus empresas cumplir sus objetivos de ciberseguridad, hubo una diferencia media de 14 puntos porcentuales entre las respuestas de los de seguridad y las de los ajenos a seguridad en siete factores significativos. En particular, estaban en desacuerdo sobre la implicación de la seguridad en los debates sobre la nube: el 43 % de los ejecutivos ajenos a seguridad, frente al 31 % de los de seguridad, afirmaron que la seguridad no formaba parte del debate y que ahora estaban intentando ponerse al día.

Estas diferencias de opinión pueden reflejar una mayor confianza por parte de los ejecutivos de seguridad por su ciberresiliencia. O pueden indicar que los ejecutivos de seguridad necesitan trabajar más en integrarse en el negocio para que las prioridades sean acordadas y claras. De cualquier manera, es importante que los ejecutivos de seguridad y del negocio se alineen mejor para que se puedan establecer, medir y cumplir los resultados empresariales.

Gráfica 15. Diferencias de opinión entre los ejecutivos de seguridad y los ejecutivos ajenos a seguridad

	Ejecutivos de seguridad	Ejecutivos ajenos a seguridad
Efectividad de la seguridad: Mi empresa está bien protegida frente a las ciberamenazas.	52%	38%
Gasto: Porcentaje estimado del presupuesto de TI gastado en seguridad en mi empresa.	15%	26%
Ataques en mi empresa		
• Número de tentativas de violaciones de seguridad	270	180
• Número de tentativas de ataques de *ransomware*	180	300

Fuente: Estado de Resiliencia en materia de Ciberseguridad de Accenture 2021, ejecutivos de seguridad (N=4.244) y ejecutivos ajenos a seguridad (N=500)

El camino a la ciberresiliencia

Aunque este ha sido un año como ningún otro, ha puesto de manifiesto el papel crítico de la ciberseguridad dentro de la empresa y la importancia de que la ciberseguridad y las estrategias de negocio estén alineadas.

Estamos observando retos conocidos que ya habíamos percibido en el pasado; los ciberataques están disparándose, las inversiones en seguridad siguen en alza y la relación de la seguridad con la nube continúa siendo un reto.

Incluso la relevancia de los CISOs en la empresa ha crecido, con más CISOs que nunca respondiendo directamente ante el CEO o el Consejo (72% en 2021, comparado con el 59 % de 2020) y consiguiendo más control directo sobre sus presupuestos.

En este escenario, en el que el cambio es la palabra clave, buscar la mejor manera de gestionar las operaciones de seguridad puede marcar toda la diferencia. No es un proceso unidireccional.

Como hemos visto en este informe, las empresas que se centran únicamente en el crecimiento empresarial están perdiéndose los beneficios de la ciberresiliencia. Y existen beneficios para las empresas que buscan proactivamente la sinergia entre la seguridad y el negocio.

Al alinear sus esfuerzos en ciberseguridad con la estrategia de negocio, las empresas pueden no solo obtener mejores resultados empresariales, sino también aprovecharse de una ventaja en la carrera hacia la ciberresiliencia.

«La Dirección está ahora muy implicada en temas como la ciberresiliencia; existe una buena disposición para invertir más dinero en ello. Es una conversación que se está teniendo en este momento y es mejor de lo que nunca ha sido.»

CISO, gran empresa del sector minero

Sobre la investigación

Datos demográficos

El estudio de estado sobre resiliencia en Ciberseguridad 2021 encuestó a 4.744 ejecutivos en marzo y abril de 2021 para entender hasta que punto las organizaciones priorizan la seguridad, el grado de seguridad y cuán completos son sus planes y cómo están funcionando sus inversiones en seguridad.

Los ejecutivos representan a organizaciones con ingresos anuales de 1.000 millones de dólares o más, de 18 países y 23 de sectores de América de Norte, América del Sur, Europa y Asia-Pacífico.

4º
Estudio Anual de Investigación

1.000 millones USD
Ingresos

4.744
Encuestados

4.244 Encuestados
500 Encuestados de seguridad ajenos a seguridad

18
Países

- Austria (50)
- Australia (372)
- Brasil (177)
- Canada (194)
- France (369)
- Alemania (364)
- Irlanda (100)
- Italia (307)
- Japón (388)
- Paises Bajos (118)
- Noruega (124)
- Portugal (100)
- Arabia Saudí (111)
- Singapur (102)
- España (251)
- Suiza (50)
- Reino Unido (489)
- Estados Unidos (1,078)

23
Sectores

- Aeroespacial y defensa (101)
- Automoción (101)
- Banca (345)
- Biotecnología (11)
- Mercados de capital (121)
- Químico (200)
- Bienes de consumo y servicios (440)
- Energía (210)
- Pagadores servicios sanitarios (102)
- Proveedores de servicios sanitarios (102)
- Alta tecnología (343)
- Equipos industriales (434)
- Seguros (456)
- Ciencias biológicas (139)
- Medios de comunicación (222)
- Metalurgia y minería (100)
- Farmacéutica (49)
- Servicios federales estadounidenses (100)
- Comercio minorista (438)
- Software y plataformas (220)
- Telecomunicaciones (207)
- Viajes y hostelería (93)
- Servicios públicos (210)

Nuestra metodología

Retomando nuestro enfoque de años anteriores, primero definimos a los **líderes en ciberresiliencia** como aquellos que muestran un rendimiento alto (20% superior de la muestra) en al menos tres de los siguientes cuatro criterios de rendimiento:

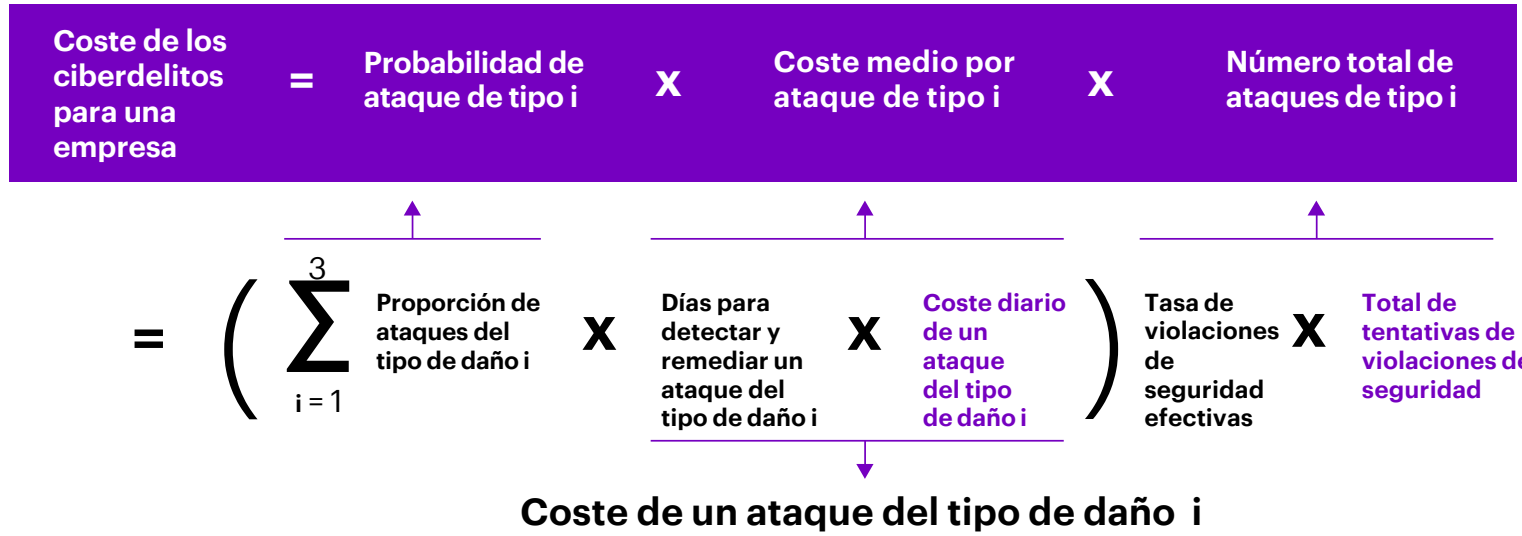
- Detienen más ataques
- Detectan violaciones de seguridad más rápido
- Remedian violaciones de seguridad más rápido
- Reducen el impacto de las violaciones de seguridad.

Realizamos entonces una serie de experimentos «y si...» para explorar el rendimiento de la inversión en la mejora de estas prácticas de ciberseguridad.

Creamos una fórmula para calcular el coste de los ciberdelitos para una empresa: el coste medio por ataque, multiplicado por el número total de ataques.

El coste medio por ataque fue la suma del producto del coste diario de un ataque por el tipo de daño, los días para detectar y remediar un ataque de este tipo de daño y la proporción. de ataques para este tipo de daño. El número total de ataques fue el producto de la tasa de violaciones de seguridad y el número total de tentativas de violaciones (Gráfica 16).

Gráfica 16. Fórmula modelo para valorar el coste de los ciberdelitos



Nota: Para los ejercicios de modelización, realizamos nuestro análisis en una muestra de 3.455 empresas que respondieron a todos los elementos claves del modelo de costes de los ciberdelitos. Asumimos las variables en morado para permanecer constantes en la serie de experimentos «y si...» que llevamos a cabo. Los tipos de daño incluyen ataques que son: (1) Significativos, (2) Moderados, (3) Menores y (4) Sin repercusión.

Sobre la investigación

Realizamos nuestro análisis de modelización en un subconjunto de muestra de 3.455 empresas que respondieron a todos los elementos claves del modelo de costes de los ciberdelitos.

A continuación, examinamos **cómo la intensidad de la alineación entre la estrategia de ciberseguridad y la estrategia de negocio afectaba a la ciberresiliencia.** La intensidad de la alineación se definió a partir de los siguientes elementos:

1. La medida en la que los objetivos empresariales (por ej., reducción de costes, crecimiento del negocio, satisfacción del cliente) son una prioridad para la estrategia de negocio general de la empresa y la medida en la que se consulta a ciberseguridad a la hora de planificar estas áreas comerciales.

2. La medida en la que los encuestados estaban de acuerdo o en desacuerdo con las declaraciones sobre alineación (por ej., implicación de toda la empresa en la comprensión y mitigación de los ciberriesgos e implicación de la dirección en el establecimiento de estrategias y presupuestos de ciberseguridad.)

Ambos elementos se reclasifican en una escala de 0 a 100 y se hace la media para obtener una puntuación final de alineación. Partiendo de estas definiciones de ciberresiliencia y alineación, dividimos nuestra muestra en cuatro niveles de ciberresiliencia:

'Los obstaculizadores del negocio'

15% de la muestra de la encuesta

522 encuestados

'Los ciberdefensores'

5% de la muestra de la encuesta

172 encuestados

'Los vulnerables'

55% de la muestra de la encuesta

1,876 encuestados

'Los que asumen ciberriesgos'

25% de la muestra de la encuesta

885 encuestados

Continuamos entonces con nuestros experimentos «y si...» utilizando la ecuación presentada en la página 30 para estudiar el rendimiento de las inversiones derivado de la alineación.

Referencias

1. Análisis de Accenture Research de 1.548 informes trimestrales 10-K de la Securities & Exchange Commission sobre 500 empresas de 2017 a 2020

2. Tercer Estado de Ciberresiliencia Anual, Accenture 2020

3. La progresión del Cloud, Accenture 2021

4. Da el salto, asume el liderazgo, Accenture 2021

5. Respuesta y recuperación en casos de *ransomware,* Accenture 2021

6. Seguridad en la nube, Accenture 2021

Sobre Accenture

Accenture es una compañía global líder en servicios profesionales digitales, de la nube y de seguridad. Gracias a la combinación de una experiencia inigualable y habilidades especializadas en más de 40 sectores, ofrecemos servicios de estrategia y consultoría, interactivos, de tecnología y de operaciones, todos ellos impulsados por la red más grande del mundo de centros de tecnología avanzada y operaciones Nuestros 624.000 trabajadores hacen realidad la promesa de la tecnología y el ingenio humano todos los días y dan servicio a clientes de más de 120 países. Adoptamos el poder del cambio para crear valor y compartimos el éxito con nuestros clientes, trabajadores, accionistas, socios y comunidades.
Visita www.accenture.com

Sobre Accenture Security

Accenture Security es un proveedor líder de servicios de ciberseguridad de extremo a extremo, que incluyen ciberdefensa avanzada, soluciones de ciberseguridad aplicadas y operaciones de seguridad gestionada. Ofrecemos innovación en seguridad, además de una escala global y una capacidad de entrega a nivel mundial a través de nuestra red de centros de tecnología avanzada y operaciones inteligentes. Con la ayuda de nuestro equipo de profesionales altamente capacitados, ayudamos a nuestros clientes a innovar de manera segura, desarrollar la resiliencia cibernética y crecer con confianza.

Sigue nuestra cuenta **@AccentureSecure** en Twitter o visita nuestra página web
www.accenture.com/security

Sobre Accenture Research

Accenture Research da forma a las tendencias y elabora enfoques a partir de datos sobre las cuestiones más acuciantes a las que se enfrentan las empresas globales. Combinando el poder de técnicas de investigación innovadoras con un profundo conocimiento de los sectores de nuestros clientes, nuestro equipo de 300 investigadores y analistas se extiende a lo largo de 20 países y cada año publica cientos de informes, artículos y opiniones. Nuestra estimulante investigación, respaldada por datos propios y colaboraciones con organizaciones líderes, como el MIT y Harvard, guía nuestras innovaciones y nos permite transformar las teorías y
las ideas nuevas en soluciones para nuestros clientes que sean aptas para el mundo. Para más información, visita
www.accenture.com/research.

12460920

210573