El CEO ciberresiliente

Los CEO seguros de sí mismos asumen el control de la ciberseguridad

Voices of Change

De los insights a la acción, el camino hacia un valor extraordinario comienza aquí.

accenture

Los CEO son plenamente conscientes que los ciberataques son una amenaza para sus empresas. Sin embargo, nuestra investigación muestra que la mayoría de los CEO no confía en la capacidad de su organización para evitar o minimizar dichos ataques. Aprenden a ser ciberresilientes solo después de que su organización sufre alguna violación a la ciberseguridad. Esta forma reaccionaria de tratar la ciberseguridad se traduce en un mayor riesgo de ataques y mayores costos para remediarlos. Nuestra investigación revela que algunos escogen un camino mejor. En esta guía práctica, exploramos cómo los CEO están en mejor situación para poner en marcha cinco medidas que minimicen el riesgo y sitúen la ciberresiliencia en el centro de sus esfuerzos de reinvención.

Autores

Paolo Dal Cin
Senior Managing Director
Global Lead
Accenture Security

Paolo trabaja con ejecutivos de alto nivel, impulsando soluciones y servicios sobre estrategias de seguridad, resiliencia empresarial, ciberdefensa, inteligencia sobre amenazas y servicios gestionados.

Valerie Abend
Senior Managing Director
Global Cyber Strategy Lead
Accenture Security

Valerie dirige programas de seguridad y resiliencia en toda la empresa, y asesora a directivos, consejos de administración, reguladores y responsables políticos sobre la gestión del ciberriesgo.

Rachel Barton
Senior Managing Director
Europe Strategy Lead
Accenture Strategy

Rachel se especializa en estrategia de crecimiento, trabajando con altos ejecutivos y consejos de administración para ayudarlos a crecer de forma sostenible a través de un cambio audaz y transformador.

Yusof Seedat
Thought Leadership Director
Global Research Lead
Accenture Security

Yusof dirige la investigación sobre ciberseguridad, centrándose en dar forma a un liderazgo de pensamiento basado en datos para ayudar a orientar la toma de decisiones estratégicas y el posicionamiento en el mercado de las organizaciones a nivel mundial.

Agradecimientos

Los autores desean agradecer a Sarah Bird, Gargi Chakrabarty, Arlene Lehman, Eileen Moynihan, Manav Saxena, Ann Vander Hijde, Alissa Worley y Christine Yiannakis por sus contribuciones a este informe.

Índice

En Resumen

¿Es la ciberseguridad una prioridad de negocio? Debería serlo. Mantiene el buen funcionamiento de las operaciones de negocios, ayuda a las organizaciones a optimizar su rendimiento y asegura las relaciones con clientes y proveedores. Los CEO que dejan de lado la ciberseguridad exponen a sus organizaciones a más riesgos.

Fuerzas poderosas están multiplicando las vulnerabilidades digitales. La innovación tecnológica, incluida la IA generativa y la computación cuántica, los retos medioambientales, los cambios en las preferencias de los consumidores, las interrupciones en la cadena de suministro y la inestabilidad geopolítica están colisionando para alterar las agendas de los consejos de administración y hacer de la resiliencia en materia de ciberseguridad una prioridad absoluta.

Un puñado de organizaciones están tomando las riendas de su propia disrupción adoptando la Reinvención Total de la Empresa, una estrategia que conduce a una nueva frontera de desempeño. Su objetivo es reinventar cada parte de sus empresas a lo largo del tiempo, en torno a un núcleo digital y una cultura y capacidad centradas en la reinvención continua.

En el contexto de estos panoramas cambiantes, Accenture estudió las prácticas de ciberseguridad de 1.000 CEO de grandes organizaciones para comprender mejor lo que significa ser un líder ciberresiliente hoy en día. La investigación muestra que los CEO son plenamente conscientes de la ciberseguridad, y un 96% está de acuerdo en que es un factor clave para el crecimiento y la estabilidad de la organización. Sin embargo, el 74% está preocupado por la capacidad de su organización para evitar o minimizar los daños a la empresa derivados de un ciberataque. Se trata de una desconexión que pone de manifiesto que la mayoría de los CEO no confían en que sus organizaciones tengan realmente ciberresiliencia, y su incertidumbre se refleja en la forma en que priorizan sus inversiones en ciberseguridad.

Respaldados por nuestra amplia experiencia en ciberseguridad, en Accenture hemos identificado tres problemas que siguen suponiendo un reto para los CEO en la actualidad.

Comprensión limitada de la ciberseguridad y su relación con el negocio.
Los beneficios de la ciberseguridad son difíciles de cuantificar. Más de la mitad de los CEO afirman que el costo de implementación de la ciberseguridad es mucho mayor que el costo de sufrir un ciberataque, sin embargo, esto es lo contrario de la realidad. Como era de esperar, la falta de comprensión se traduce en un enfoque estratégico limitado; solo el 15% de los CEO afirmó haber dedicado reuniones del consejo de administración a debatir cuestiones de ciberseguridad.

Compartimentar los riesgos de ciberseguridad como cuestiones de cumplimiento.
Los riesgos de ciberseguridad se consideran cuestiones de cumplimiento (*compliance*) que deben ser abordadas por las funciones de control interno. Casi la mitad (44%) de los CEO no considera la ciberseguridad como una cuestión estratégica de negocio y afirma que requiere una intervención episódica en lugar de una atención continua, mientras que el 60% de los CEO afirma que sus organizaciones no introducen la "seguridad por diseño", es decir, que la ciberseguridad no se incorpora a las estrategias de negocios ni a servicios o productos específicos desde el principio.

Incapacidad de los líderes para seguir el ritmo del impacto empresarial de los riesgos en rápida evolución.
Solo el 33% de los CEO está totalmente de acuerdo en que conoce en profundidad el cambiante panorama de las amenazas a la ciberseguridad y el costo potencial que podría suponer para su negocio no comprender los nuevos riesgos y no actuar ante ellos. Tomemos como ejemplo la IA generativa, que está transformando todo rápidamente. Si no es segura, las organizaciones se enfrentan a un mayor riesgo de compromiso, incumplimiento normativo, daños a la reputación e incapacidad para mantener una ventaja competitiva. Limitar el alcance y la importancia de la ciberseguridad en la empresa puede ser una oportunidad perdida para los CEO. Por lo general, es solo después de sufrir un ciberataque cuando el CEO comprende la importancia de la ciberseguridad y comienza a dedicarle personalmente tiempo y esfuerzo. Este enfoque es arriesgado, dado el aumento exponencial de los ciberdelitos y el impacto potencial en la reputación y la marca.

Nuestra investigación muestra cómo los CEO pueden convertirse proactivamente en ciberresilientes y actuar con confianza.

Desarrollamos el índice de acciones del CEO ciberresiliente de Accenture para comparar 25 prácticas líderes que miden la resiliencia de la ciberseguridad. Utilizando este índice, encontramos un pequeño grupo (5%) de CEO que lideran la resiliencia en ciberseguridad.

A este grupo lo denominamos “los CEO ciberresilientes”, y notamos que utilizan una perspectiva más amplia para evaluar la ciberseguridad en sus organizaciones, inclusive el talento, la innovación, la sostenibilidad y los clientes.

Los CEO ciberresilientes no se basan en los requisitos en materia de violaciones a las normas o de cumplimiento para informar su visión de la ciberseguridad, sino que toman proactivamente las siguientes medidas:

1. **Incorporan la ciberresiliencia a la estrategia de negocio desde el principio.**
2. **Hacen que la ciberseguridad sea una responsabilidad compartida de toda la organización.**
3. **Protegen la base digital de la organización.**
4. **Extienden la ciberresiliencia más allá de los límites de la organización**
5. **Adoptan la ciberresiliencia continua para mantenerse a la vanguardia.**

Como resultado, estos líderes detectan, contienen y reparan las ciberamenazas más rápidamente que sus pares. Sus costos por incumplimientos son considerablemente más bajos y sus resultados financieros son mucho mejores que los del resto. En base al estudio de Accenture, este informe detalla los pasos prácticos que los CEO pueden dar para evaluar y mejorar la ciberresiliencia de su propia organización.

Complejidad de las ciberamenazas

Hoy en día, lo digital está en el centro de todo, desde la política y la estabilidad económica hasta la rentabilidad y el acceso a reservas continuas de talento.

Sin embargo, el rápido aumento de las ciberamenazas y los riesgos que se plantean cuando la seguridad no está integrada en a la base digital de una organización pueden obstaculizar la competitividad a nivel nacional y del negocio. Por ejemplo:

- La guerra contra Ucrania y la multipolarización geopolítica han amplificado muchas tendencias; en particular, se espera que los costos mundiales del ciberdelito alcancen los 10,5 billones de dólares anuales en 2025, frente a los 3 billones de 2015[1] y se prevé que el gasto mundial en ciberseguridad alcance los 300.000 millones de dólares en 2026.[2]

- Al mismo tiempo, garantizar la resiliencia de la infraestructura y las operaciones digitales requiere examinar creencias fundamentales en muchas industrias, lo que también afecta a habilitadores críticos como el Internet de las Cosas y los servicios de inteligencia artificial (IA) basados en la nube.

- La tecnología y los productos operativos son cada vez más vulnerables a los ciberataques y la seguridad de estos sistemas ciberfísicos sigue siendo un reto percibido como un factor que agrega tiempo, costos y complejidad.

- Es probable que la innovación digital, como la IA generativa, introduzca nuevas formas de complejidad. El 64% de los CEO afirmó que algunos perpetradores de amenazas ineficaces podrían utilizar la IA generativa para crear nuevos ciberataques sofisticados y difíciles de detectar.

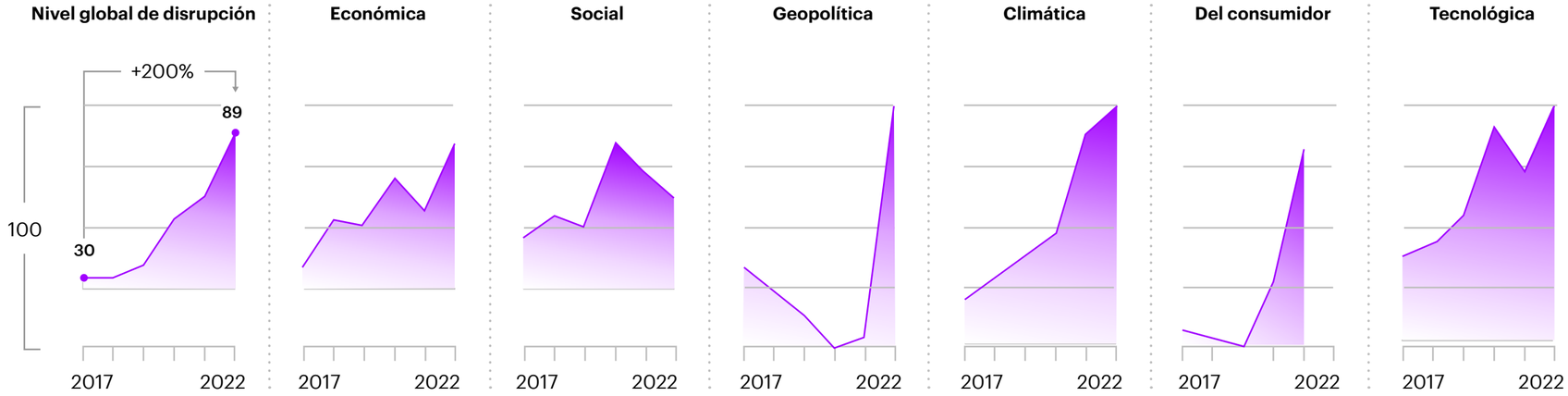
Hace diez años, Accenture preveía que todas las empresas se convertirían en empresas digitales y, hoy en día, todas las organizaciones son también organizaciones tecnológicas. Estas empresas están utilizando ampliamente las tecnologías digitales, como la nube, la computación de borde, 5G y ahora la IA generativa, para transformarse en un mundo cada vez más disruptivo. En nuestra investigación, el 96% de los CEO afirmó que la tecnología desempeña un papel fundamental en sus iniciativas de transformación y reinvención actuales y futuras.

Pero los cambios drásticos provocados por estos esfuerzos de transformación y reinvención digital también introducen nuevas vías para los ciberataques que no solo proliferan, sino que también modifican drásticamente los planes de negocio. El Índice de Disrupción Global de Accenture (Figura 1)—una medida compuesta que abarca la disrupción económica, social, geopolítica, climática, del consumidor y tecnológica- muestra que los niveles de disrupción aumentaron un 200% de 2017 a 2022.[3]

Figura 1. Índice de disrupción global de Accenture

Los niveles de disrupción aumentaron un 200% de 2017 a 2022

Medida global de disrupción basada en la media de 6 subcomponentes, cada uno de los cuales se basa en puntuaciones indexadas de un conjunto de indicadores.



Fuente: Accenture, Reinvención Total de la Empresa, 2023

Cuando consultamos a los CEO sobre qué fuerzas disruptivas están creando vulnerabilidades cibernéticas para sus organizaciones, identificaron los siguientes factores:

52%

Innovación tecnológica

Más de la mitad (52%) clasificó el ritmo acelerado de la innovación tecnológica como el principal riesgo de ciberataques y el 86% considera que la ciberconfianza y la resiliencia de las tecnologías emergentes, como la IA generativa y la computación cuántica, son muy importantes para sus organizaciones.

51%

Interrupción de la cadena de suministro

Alrededor de la mitad (51%) de los CEO clasificaron la cadena de suministro como el segundo mayor riesgo externo, lo que subraya las vulnerabilidades de las organizaciones globales a lo largo de sus cadenas de valor repartidas por diferentes lugares.

90%

Vulnerabilidades medioambientales

Los retos medioambientales son otros riesgos externos mejor valorados por los CEO, y un 90% reconoce la relación y la vulnerabilidad de los cambios e iniciativas medioambientales.

Los CEO también clasificaron el cambio en las preferencias de los consumidores y la tensión geopolítica entre los 10 principales factores externos que más influyen en el panorama de las ciberamenazas, y el 90% prevé una ciberamenaza catastrófica dentro de dos años.[4]

Todos estos factores han reconfigurado el panorama de las ciberamenazas, haciendo de la ciberseguridad un factor clave para impulsar el valor de negocio con seguridad, confianza y resiliencia.

Tamaño y escala

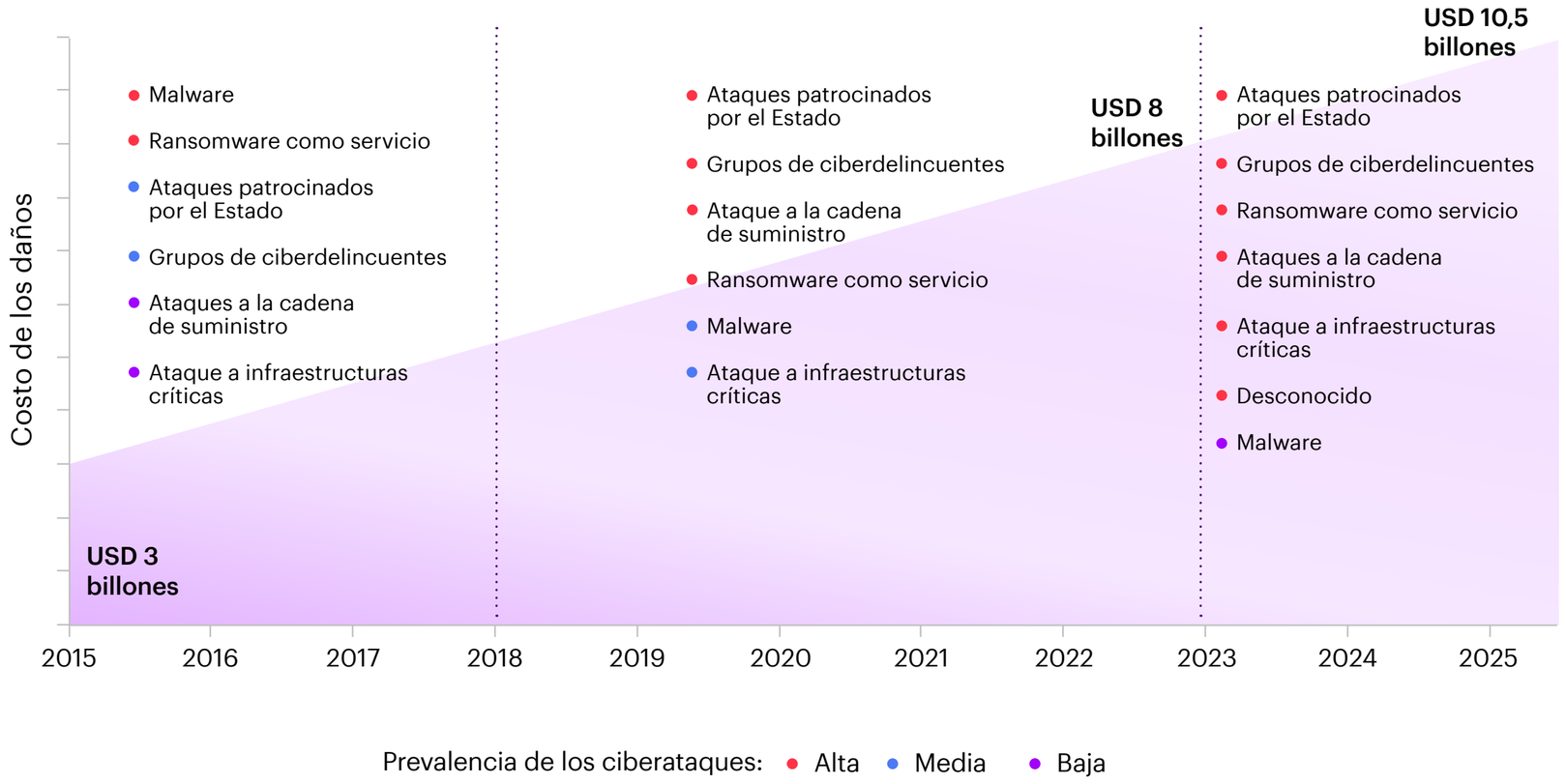
Las pérdidas por el cibercrimen pasaron de ser USD 3 billones en 2015 a USD 8 billones en 2023, y se prevé que alcancen los USD 10,5 billones en 2025, el tamaño de la tercera economía más grande del mundo después de Estados Unidos y China, según una investigación publicada por Cybersecurity Ventures.[5]

Los ciberataques son cada vez más complejos y frecuentes y pueden paralizar rápidamente las operaciones de las empresas, incluso de las grandes compañías globales con operaciones sofisticadas (Figura 2).

Tomemos el ejemplo de la empresa naviera y de logística danesa Maersk. Un ataque de ransomware NotPetya sirvió como llamada de atención para reforzar su preparación en ciberseguridad. El impacto en los sistemas de TI fue inmediato: casi 50.000 computadoras fueron infectadas en 600 sitios de 130 países.

El impacto en el negocio fue inmediato. La indisponibilidad de los sistemas provocó la paralización de buques y envíos críticos en los puertos. Las pérdidas ascendieron a USD 300 millones, afectando aproximadamente 90.000 trabajadores, además de infraestructuras portuarias, empresas y consumidores que se vieron afectados por la interrupción del transporte a nivel mundial. El ataque de ransomware provocó una caída del 20% en los volúmenes de negocios.[6]

Figura 2. Costos y complejidad de los daños causados por el cibercrimen



Fuente: Análisis de Accenture Research, Cybersecurity Ventures

Riesgo y recompensa

Los CEO hoy prestan más atención al riesgo de ciberseguridad. El reconocimiento de las pérdidas financieras, el daño a la reputación y las interrupciones operativas que pueden derivarse de los ciberataques está alimentando un creciente sentido de urgencia y es una fuerza impulsora detrás de un cambio en su mentalidad.

Una mayoría del 96% de los CEO comprende la importancia de la ciberseguridad y reconoce que es un factor clave para el crecimiento, la estabilidad y la competitividad de las organizaciones.

Nuestro análisis de las transcripciones de las declaraciones de resultados de las grandes empresas respalda esta creciente concienciación: encontramos un aumento de 6 veces el número de menciones de las palabras ciberriesgo, ciberseguridad y ciberataques por parte de los CEO desde 2017 hasta 2022.[7] Es más, el 90% de los CEO afirmaron que consideran la ciberseguridad como un factor diferenciador de sus productos o servicios para ayudarlos a generar confianza entre los clientes.

96%

de los CEO comprende la importancia de la ciberseguridad y reconoce que es un factor clave para el crecimiento, la estabilidad y la competitividad de las organizaciones.

Preparación contra el riesgo

En un panorama de ciberamenazas en rápida evolución, el conocimiento es poder. Sin embargo, existe una brecha cada vez mayor entre la creciente concienciación de los CEO sobre el valor de negocio de la ciberseguridad y lo que entienden sobre los perpetradores de amenazas emergentes, lo que, a su vez, reduce su confianza para evitar o mitigar los ciberataques.

En pocas palabras, las empresas aún no son ciberresilientes y los CEO no están seguros de cómo medir la ciberresiliencia o asegurarse de que sus empresas van por buen camino. Pero dado que el mundo digital lo conecta todo, la protección es esencial, especialmente a medida que aumentan la exposición y las vulnerabilidades digitales.

Solo el 33% de los CEO están totalmente de acuerdo en que tienen un conocimiento profundo de la evolución del panorama de las ciberamenazas, lo que deja a muchos sin claridad sobre cómo abordar los riesgos. Como era de esperar, al 74% le preocupa la capacidad de su organización para evitar o minimizar los daños a la empresa derivados de un ciberataque. Alrededor del 60% de los CEO encuestados afirmaron que llevan a cabo prácticas comunes de ciberresiliencia, pero reconocen que esto no es suficiente. Además, casi la mitad cree que la ciberseguridad requiere una intervención episódica, en lugar de considerarla un elemento clave del negocio que requiere atención continua.

Esta mentalidad reactiva también se pone de manifiesto en el escaso tiempo que los CEO dedican personalmente a abordar la ciberseguridad; solo el 15% dedica reuniones del consejo de administración a debatir cuestiones de ciberseguridad. Y el hecho de que la ciberseguridad sea difícil de cuantificar hace que sea más fácil pasarla por alto: el 54% considera que el costo de implementar la ciberseguridad es mucho mayor que el costo de un ciberataque. Sin embargo, nuestro estudio muestra que las empresas que dan prioridad a las inversiones en ciberseguridad experimentan costos de violación cibernética hasta tres veces inferiores en comparación con sus pares.

33% de los CEO están totalmente de acuerdo en que tiene un profundo conocimiento de la evolución del panorama de las ciberamenazas

74% están preocupados por la capacidad de su organización para evitar o minimizar las pérdidas de negocio derivadas de un ciberataque

60% de los CEO afirmaron que llevan a cabo prácticas comunes de ciberresiliencia, pero reconocen que no es suficiente

15% realizan reuniones del consejo dedicadas a debatir cuestiones de ciberseguridad

54% creen que el costo de la implementación de la ciberseguridad es mucho mayor que el costo de un ciberataque

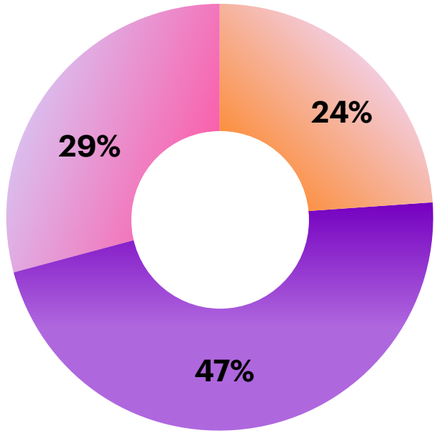
El resultado es que muchos CEO tienden a tratar la ciberseguridad como una función técnica que se rige por los incidentes y el cumplimiento de las normativas.

Se debe tener en cuenta que un 76% de los CEO afirmaron que solo implementan controles de seguridad para funciones críticas o los despliegan una vez finalizada la transformación o cuando se detectan vulnerabilidades. La mayoría (91%) afirma que la ciberseguridad es una función técnica responsabilidad del CIO o CISO, y el 95% afirma que el cumplimiento es uno de los principales impulsores de su estrategia de ciberseguridad (Figura 3).

Figura 3. Los CEO consideran la ciberseguridad como una función técnica aislada que se rige por los incidentes y el cumplimiento de las normativas.

7 in 10

Los CEO implementan controles de seguridad para funciones críticas o los despliegan una vez finalizada la transformación y detectadas las vulnerabilidades



- Incorporan controles de seguridad en todas las iniciativas de transformación desde el principio.
- Implementan controles de seguridad solo para las funciones críticas, equilibrando la velocidad y la gestión de riesgos.
- Implantan la seguridad una vez finalizada la transformación solo si se detectan vulnerabilidades, garantizando que se pueda avanzar en la transformación lo más rápido posible.

~50%

de los CEO afirman que la ciberseguridad requiere una **intervención episódica** en lugar de una atención continua.

91%

de los CEO afirmaron que la ciberseguridad es **una función técnica** y que confían en la experiencia de su CIO o CISO para dirigirla con eficacia.

95%

de los CEO afirman que el **cumplimiento de las normativas impulsa su estrategia de ciberseguridad** para garantizar que sus organizaciones cumplan las normas y los requisitos reglamentarios.

Fuente: Encuesta 2023 de Accenture a CEO ciberresilientes (n = 1.000)

Desafortunadamente, a menudo es solo después de que los CEO viven un incidente cibernético material que invierten proactivamente tiempo, recursos y amplían las expectativas más allá del CISO y las funciones tecnológicas.

Un ciberataque a Colonial Pipeline en mayo de 2021 ilustra cómo a muchos CEO se les pide que manejen este cambio masivo en las vulnerabilidades cibernéticas mientras aún no están seguros de su capacidad para seguir el ritmo de los cambios. El ataque no solo perturbó el funcionamiento de la empresa, sino que también interrumpió el suministro de combustible al sureste de Estados Unidos, lo que provocó compras de pánico y un aumento de los precios de la nafta. Los atacantes robaron 100 gigabytes de datos en un plazo de dos horas. Infectaron con ransomware los sistemas de TI de la empresa, incluidos los de facturación y contabilidad.

En respuesta, Colonial Pipeline cerró el oleoducto para evitar la propagación del ransomware, lo que provocó una crisis de suministro en el mercado. El CEO aceptó en una comparecencia ante el Senado que la empresa no disponía de un plan para prevenir un ataque de ransomware. Tras el ataque, la empresa renovó su equipo de seguridad, contrató a su primer Director de Seguridad de la Información (CISO) y comenzó a reconstruir su programa de ciberseguridad.[8]

Cinco medidas de ciberresiliencia

Para los CEO, cerrar la brecha de ciberresiliencia es una prioridad de negocio.

Nuestro índice de acciones de CEO ciberresilientes, que comprende 25 prácticas que miden la ciberresiliencia (véase Acerca de la investigación), identificó las prácticas que los CEO que dan prioridad a la ciberseguridad llevan a cabo para impulsar el valor de negocio con seguridad, confianza y resiliencia.

Agrupamos estas prácticas en cinco medidas generales:

01 **Incorporar la ciberresiliencia a la estrategia de negocio desde el principio.**

02 **Hacer que la ciberseguridad sea una responsabilidad compartida de toda la organización**

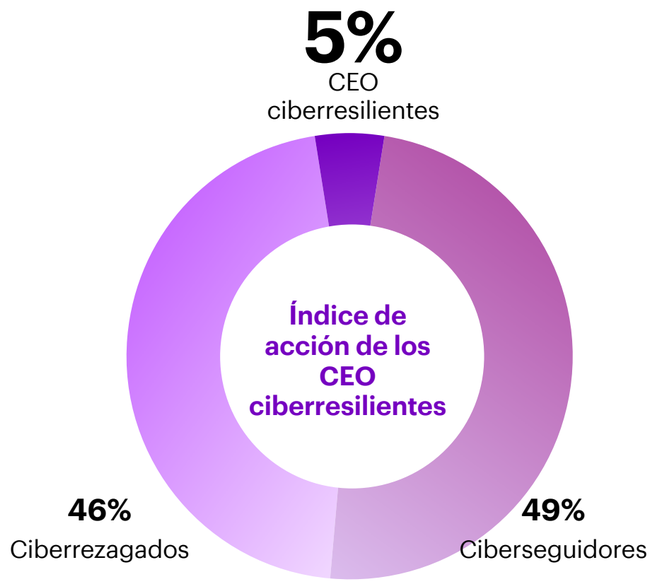
03 **Proteger la base digital de la organización.**

04 **Extender la ciberresiliencia más allá de los límites de la organización.**

05 **Adoptar la ciberresiliencia continua para mantenerse a la vanguardia.**

Utilizando el índice, descubrimos que solo el 5% de los CEO son líderes en ciberresiliencia. Estos CEO ciberresilientes adoptan sistemáticamente tres o más de estas medidas, sin esperar a que se produzca una violación o un plazo de cumplimiento.

En el siguiente nivel se encuentran los ciberseguidores. Siendo un 49%, estos CEO siguen rigurosamente al menos dos de las cinco medidas y adoptan algunas prácticas de las restantes. Los ciberrezagados, el 46% de nuestra muestra, no llevan a cabo ninguna de las acciones de forma coherente o rigurosa y suelen quedarse en un modo reaccionario.



¿Qué aspecto tiene un CEO ciberresiliente?

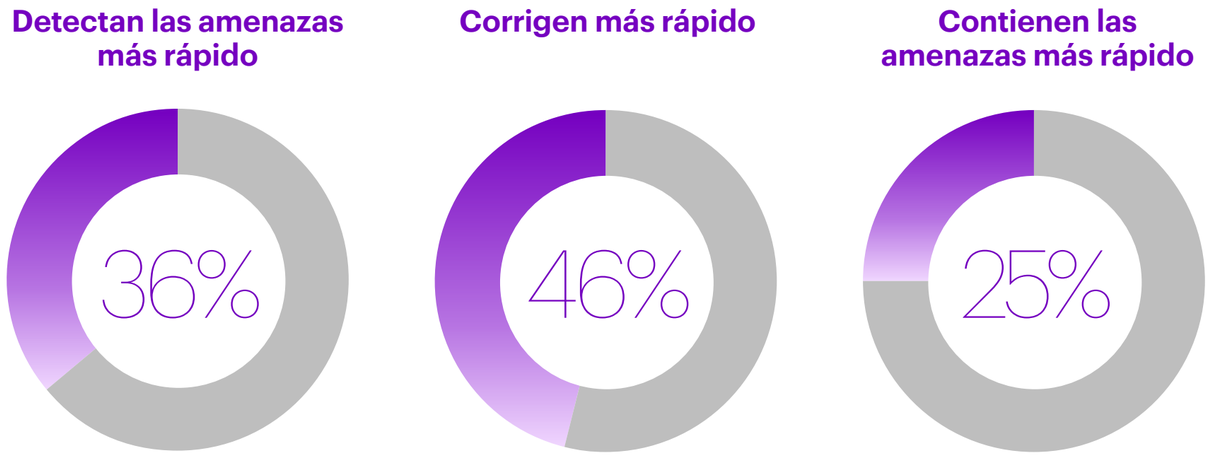
La investigación muestra que los CEO ciberresilientes:

Actúan con confianza

Están más seguros de que sus organizaciones son ciberresilientes: el 60% de ellos afirma que son ciberresilientes, frente al 24% de los ciberseguidores y ciberrezagados combinados. Y sus afirmaciones se ven respaldadas por su capacidad para detectar, contener y corregir las amenazas con mayor rapidez (Figura 4) y por el hecho de que los costos de las violaciones son casi 2 veces inferiores a los de los ciberseguidores y 3 veces inferiores a los de los ciberrezagados.

A pesar de sufrir un 25% más de intentos de intrusión en 2022 con respecto a 2021, la tasa de éxito de las violaciones para los CEO ciberresilientes (violaciones totales exitosas como porcentaje de las violaciones totales intentadas) es menor en comparación con los ciberrezagados (un 14% menos) y los ciberseguidores (un 6% menos).

Figura 4. Los CEO ciberresilientes actúan



Fuente: Encuesta 2023 a CEO ciberresilientes de Accenture (n = 1.000)
Los porcentajes representan a los CEO ciberresilientes frente a los ciberrezagados.

Adoptar la reinvención

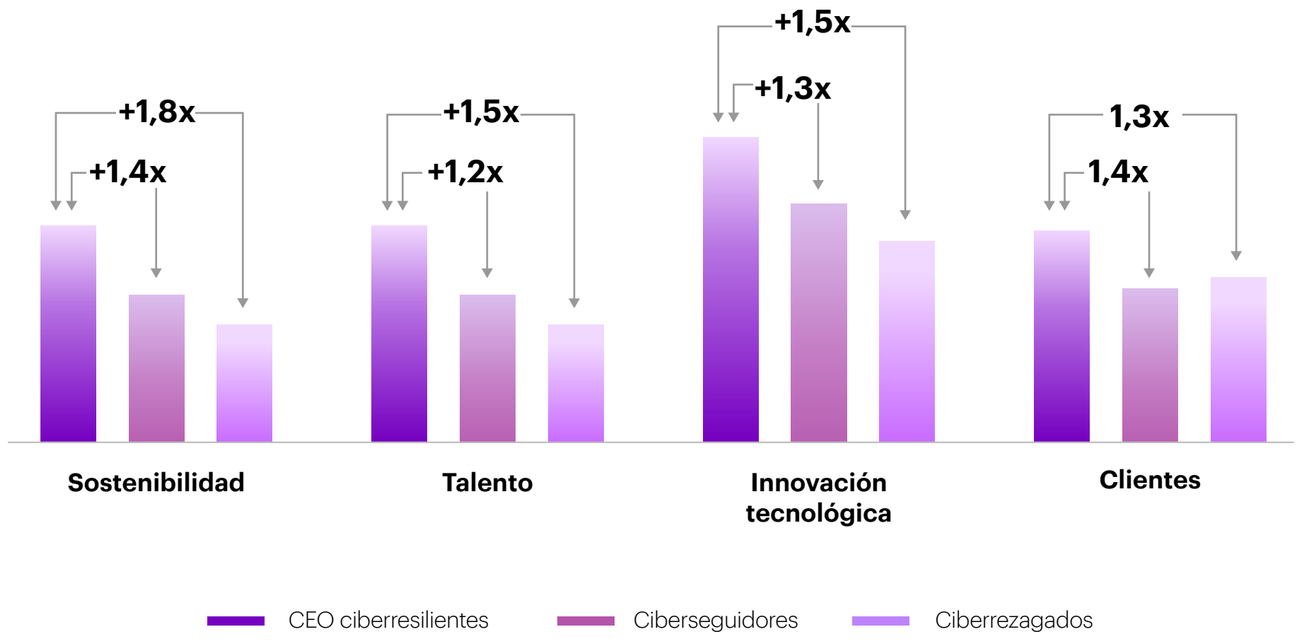
Todos los CEO ciberresilientes encuestados adoptan estrategias empresariales para reinventar sus funciones y unidades de negocio, creando capacidades que trascienden los silos funcionales y departamentales y estableciendo nuevas fronteras de desempeño. Además, adoptan una visión holística de la ciberseguridad, integrándola en sus estrategias desde el principio.

Evaluar holísticamente

Los CEO ciberresilientes utilizan una perspectiva más amplia de 360 grados al considerar su postura de ciberseguridad—hasta 1,8 veces más que sus pares—en acciones o financieras, como la sostenibilidad, el talento, la innovación tecnológica y los clientes (Figura 5).

Figura 5. Los CEO ciberresilientes adoptan un enfoque de 360 grados respecto a la ciberseguridad

Las puntuaciones de 360˚de ciberseguridad evalúan el grado en que los CEO perciben y asocian la ciberseguridad a través de acciones no financieras



Fuente: Encuesta 2023 de Accenture a CEO ciberresilientes (n = 1.000)

Como resultado, en promedio, los CEO ciberresilientes están logrando un mayor valor de negocio que sus pares.

Figura 6. Los CEO ciberresilientes superan financieramente a sus pares

+16% Mayor crecimiento de los ingresos

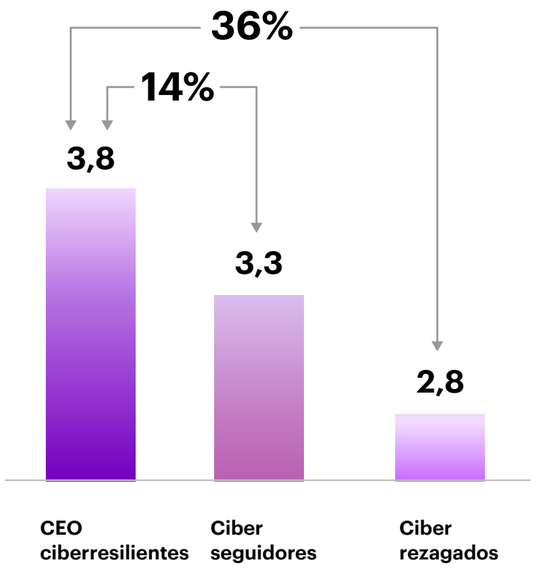
+21% Más mejoras de reducción de costos

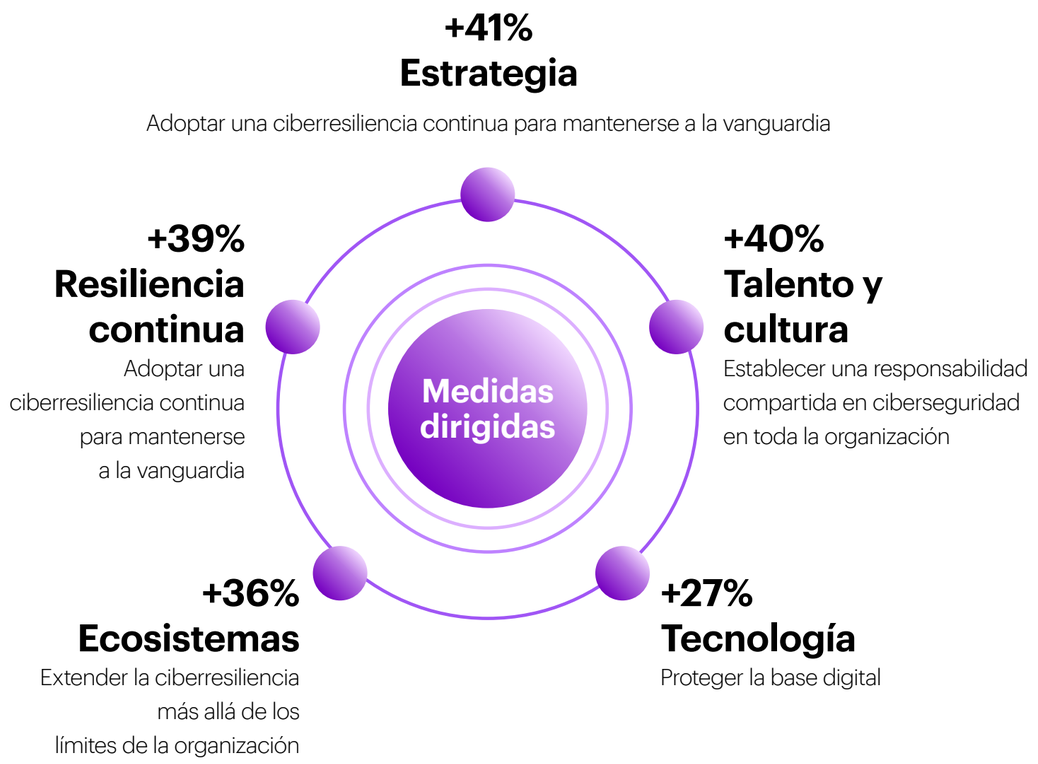
+19% Mejoras en el balance

Fuente: Encuesta 2023 de Accenture a CEO ciberresilientes (n = 1.000)

En general, los CEO ciberresilientes superan a sus pares en cada una de las cinco medidas de nuestro índice—estrategia, talento y cultura, tecnología, ecosistemas y resiliencia continua—superando a los ciberseguidores en 14 puntos porcentuales y a los ciberrezagados en 36 puntos porcentuales (Figura 7).

Figura 7. Los CEO ciberresilientes superan a sus pares en el índice de acciones del CEO





CEOs ciberresilientes frente a ciberrezagados

Fuente: Encuesta 2023 de Accenture a CEO ciberresilientes (n = 1.000)

El manual del CEO ciberresiliente

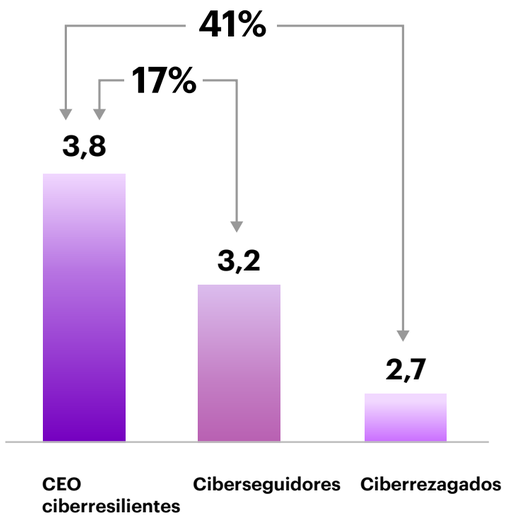
Mediante la aplicación de las cinco medidas, los CEO pueden dejar de ver la ciberseguridad como una función puramente técnica—de la que solo se ocupa el departamento de TI—y convertirla en una prioridad para toda la organización, estableciendo procesos de información y rendición de cuentas desde la alta dirección hasta el consejo de administración.

Incorporar la ciberresiliencia a la estrategia de negocio desde el principio

Para las organizaciones ciberresilientes una visión audaz de la ciberseguridad integrada en la estrategia de negocio es un diferenciador competitivo clave.

En la dimensión de **estrategia** del índice de acción del CEO, los CEO ciberresilientes superan a sus pares. Se destacan en la integración de la ciberresiliencia en sus estrategias de negocio desde el principio, con una puntuación de 3,8 puntos. Este desempeño es significativamente superior, con una ventaja del 41% sobre los ciberrezagados y una notable ventaja del 17% sobre los ciberseguidores. Al integrar la ciberresiliencia en su enfoque estratégico, los CEO ciberresilientes demuestran su compromiso con la protección de sus organizaciones frente a las ciberamenazas en evolución y el mantenimiento de una postura de seguridad sólida (Figura 8).

Figura 8. Los CEO ciberresilientes integran la ciberresiliencia en la estrategia de negocio



Fuente: Encuesta 2023 de Accenture a CEO ciberresilientes (n = 1.000)

Pasos prácticos: Estrategia

1. Respaldar la ciberseguridad como habilitador de negocio estratégico para identificar nuevo valor.

Incorporar la ciberresiliencia en la estrategia del negocio, tratándola como un factor estratégico desde el principio. Esto implica que los CEO aprueben y defiendan un marco para evaluar los riesgos cibernéticos y obliguen a utilizarlo para fundamentar las decisiones e inversiones estratégicas de negocio. Cuando los líderes empresariales tienen una justificación económica sólida y entienden por qué y cómo la gestión de los riesgos cibernéticos es un elemento facilitador del negocio, es más probable que incorporen prácticas sólidas desde el principio. Los CEO ciberresilientes (casi el 70% frente al 38% de los ciberrezagados) se distinguen por impulsar esta práctica líder. El valor potencial es convincente; nuestra investigación anterior ha demostrado que las organizaciones que alinean estrechamente los programas de ciberseguridad con los objetivos de negocio tienen un 18% más de probabilidades de lograr el crecimiento de ingresos y la cuota de mercado objetivo, mejorar la satisfacción y la confianza de los clientes y obtener una mayor productividad de los empleados.

2. Tratar el desempeño cibernético como desempeño financiero, vinculado a los resultados del desempeño personal de los ejecutivos.

Garantizar que los líderes adopten la ciberseguridad como parte integral de los procesos de toma de decisiones, desde la planificación estratégica hasta la elaboración de presupuestos, permitiendo una gestión eficaz del riesgo y estrategias de mitigación. Esto demuestra el compromiso de la organización con la protección de datos confidenciales, el mantenimiento de la continuidad operativa y la salvaguarda de la confianza de los clientes, lo que, en última instancia, aumenta la resistencia frente a la evolución de las ciberamenazas. El 60% de los CEO ciberresilientes gestionan el desempeño cibernético de la misma forma que gestionan el desempeño financiero, en comparación con un tercio de los ciberrezagados. Se ha de considerar cómo los ejecutivos integran la ciberseguridad en sus estrategias de negocio y en la toma de decisiones. Se los debe hacer responsables del volumen y la gravedad de las excepciones de riesgo cuando no cumplan las políticas y normas alineadas con el apetito de riesgo de la empresa.

3. Revisar las evaluaciones de riesgos cibernéticos a lo largo de la vida de todas las iniciativas críticas.

Tanto si se lanzan nuevos productos, se amplían servicios, se realizan adquisiciones o se establecen operaciones en nuevos sitios, la integración continua de la gestión del ciberriesgo permite a las empresas cuantificar y abordar las complejidades potenciales de la ciberseguridad en sus estrategias de negocio. Los CEO deben establecer objetivos claros y solicitar informes sobre cómo, cuándo y dónde se ha consultado a los responsables de seguridad, identificando los riesgos y aportando soluciones a lo largo de la planificación estratégica, la implementación y la vida útil de una iniciativa de negocio. Cerca del 70% de los CEO ciberresilientes, frente al 41% de los ciberrezagados hacen esto.

Pasos prácticos: Estrategia

4. Reducir la complejidad organizativa y tecnológica

La complejidad organizativa y tecnológica introduce el ciberriesgo. Al simplificar las complejas jerarquías organizativas, los procesos de toma de decisiones y los flujos de trabajo operativos, los CEO permiten responder mejor a riesgos y a posibles violaciones, además de brindar una mayor visibilidad y control de las medidas de ciberseguridad. Esto mejora la capacidad de un CISO para detectar, responder y mitigar las ciberamenazas más rápidamente y con mayor fiabilidad. Esta simplificación estructural permite una mejor coordinación, una toma de decisiones más rápida y una implementación más eficaz de las medidas de seguridad, mejorando en última instancia la ciberresiliencia general.

5. Liderar con transparencia con todas las partes interesadas

Más de dos tercios de los CEO ciberresilientes dan prioridad a la transparencia, revelando abiertamente a las partes interesadas los intentos de ciberataque y las medidas correspondientes para abordarlos. Esto incluye a las partes interesadas internas y externas que puedan verse afectadas por la ciberseguridad de la organización o que tengan interés en su postura de seguridad, como clientes, proveedores o reguladores. Al compartir abiertamente información sobre ciberincidentes, las organizaciones demuestran su compromiso con la transparencia y sus esfuerzos proactivos para hacer frente a las ciberamenazas, manteniendo al mismo tiempo relaciones sólidas con las partes interesadas.

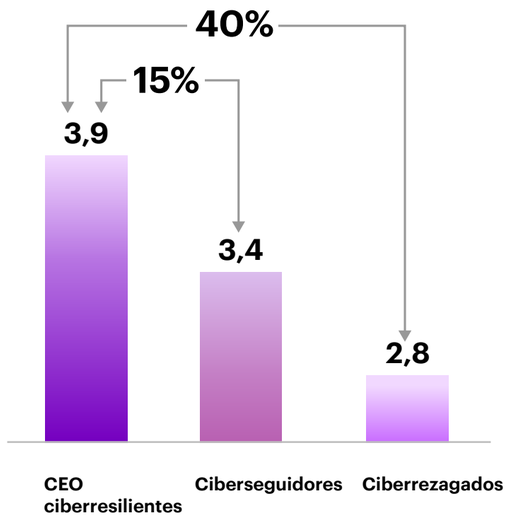
Además, las organizaciones tienen cada vez más interdependencias con sus partes interesadas, por lo que liderar con transparencia y establecer expectativas para que los socios del ecosistema hagan lo mismo mejora la ciberresiliencia. Las últimas normativas de la *United States Securities and Exchange Commission* (SEC) para mejorar la transparencia de la gestión del ciberriesgo son una llamada a la acción en pos de un mayor intercambio de información, no solo para satisfacer las expectativas basadas en el cumplimiento, sino también para mejorar la participación de las partes interesadas y la ciberresiliencia en todos los ecosistemas.

Hacer que la ciberseguridad sea una responsabilidad compartida de toda la organización

Los CEO ciberresilientes reconocen que una cultura orientada a la seguridad comienza con conocimiento en los niveles más altos e incluye a todos los integrantes de la organización.

En la dimensión del **talento y la cultura** del índice de acciones del CEO, se evaluó el desempeño del CEO sobre la base de su adopción de prácticas de seguridad que promuevan la responsabilidad compartida en materia de ciberseguridad en toda la organización. Los CEO ciberresilientes alcanzaron un puntaje de 3,9, superando a los rezagados en un 40% y a los aficionados en un 15%. Los CEO ciberresilientes son más proactivos al fijar una cultura de ciberseguridad que involucre a los empleados de todos los niveles (Figura 9).

Figura 9. Los CEO ciberresilientes son más proactivos al fijar una cultura de ciberseguridad



Fuente: Encuesta de Accenture 2023 a CEO ciberresilientes (n=1.000)

Pasos prácticos: Talento y cultura

1. Infundir una cultura de responsabilidad compartida en el nivel superior de la empresa

Establecer una cultura de responsabilidad compartida, que inspire a los líderes de negocios a considerar a la ciberseguridad como un elemento de diferenciación competitiva que permite la innovación al tiempo que se asegura la seguridad. Dos tercios de los CEO ciberresilientes manifestaron haber establecido una relación más sólida con el CISO para alentar y dar el ejemplo a otros líderes. La responsabilidad requiere la alineación de los incentivos para los directivos de la empresa y sus equipos de liderazgo por parte del CEO. Por ejemplo, los incentivos actuales para el liderazgo de tecnología casi siempre ponen el acento en la velocidad de las actualizaciones, los nuevos lanzamientos tecnológicos y los incentivos de seguridad para eliminar vulnerabilidades que pudieran causar incumplimientos. Pero con incentivos de negocios compartidos, los equipos de liderazgo pueden avanzar en sintonía con la responsabilidad compartida y las prácticas sólidas de gestión de riesgos.

Casi 70% de los CEO ciberresilientes adoptan la responsabilidad compartida, a diferencia del 37% de los ciberrezagados. Los CEO deben infundir la responsabilidad compartida en materia de ciberseguridad dentro de sus equipos de liderazgo, utilizando ambos incentivos y sus consecuencias para dar impulso a la eficiencia. Esto incluye medir la responsabilidad de directivos y líderes en función de sus roles específicos y empoderar a las organizaciones para que respalden estas responsabilidades. Por ejemplo, tomemos a los CFO/COO. Ellos deben dirigir el libro de prácticas y el proceso para determinar e informar la relevancia financiera de los incidentes de ciberseguridad. Para ello se necesita información de otros líderes dentro de la organización, como los jefes de negocios, que conocen de cerca los volúmenes de transacciones y el impacto de las pérdidas comerciales, o los líderes de TI, que conocen las interdependencias específicas de aplicaciones, infraestructura y procesos. De manera similar, el CHRO debe liderar la búsqueda y la formación del cibertalento en un mercado competitivo y asociarse para garantizar que la organización cuente con enfoques continuos de seguridad y conocimientos que aborden el factor del riesgo humano de la ciberseguridad. Si bien es fundamental elevar la relación de los directivos con el CISO, los CEO deben asegurar que las responsabilidades comunes permitan resultados ciberresilientes.

2. Construir una cultura que considere la ciberseguridad en primer lugar para toda la empresa

Los CEO pueden desempeñar un rol crítico en la construcción de una cultura en la cual la ciberseguridad es primordial dentro de la organización al poner énfasis en la importancia de una conducta de conocimiento de informática en todos los niveles. Los CEO deben guiar con su ejemplo, pronunciándose a favor de la importancia de la ciberseguridad y demostrando que se esfuerzan para ampliar su conocimiento personal en materia de ciberseguridad. Tienen el poder de sentar las pautas para sus empleados y transparentar su responsabilidad en la gestión de riesgos cibernéticos hacia los líderes, de manera que se filtre a cada uno de los miembros del equipo ejecutivo. Debemos destacar que los CEO ciberresilientes tienen 62% más posibilidades de cultivar activamente esta cultura con preponderancia de la ciberseguridad, a diferencia de los ciberrezagados. Al hacerlo, pueden inculcar la práctica de hábitos digitales seguros en todas las funciones y operaciones, desde la nómina, pasando por la cadena de suministros, hasta la relación con el cliente.

Pasos prácticos: Talento y cultura

3. Conducir el llamado a la acción para impulsar la innovación y la resiliencia

La innovación nunca ha sido tan accesible. La amplia disponibilidad de IA, en particular IA generativa, presenta desafíos de ciberseguridad y oportunidades significativas para que las organizaciones optimicen y automaticen sus procesos de seguridad. Colaborar con los CISO para explorar en forma proactiva tanto los riesgos como los casos de uso para la IA generativa. Al aprovechar el poder de la IA generativa, las organizaciones pueden ser eficaces en la gestión de sus cargas de trabajo, la eliminación de tareas laboriosas y la ampliación de sus capacidades de ciberdefensa. Los CEO ciberresilientes indicaron que la detección automática de amenazas, los escenarios de simulacros de ciberataques y el aumento de las tareas manuales de seguridad constituyen los usos clave de IA generativa para ciberdefensa. Más de la mitad de los CEO ciberresilientes trabajan en conjunto con sus CISOs para evaluar y gestionar los riesgos de la IA generativa, asegurando que la tecnología sea utilizada de manera segura y eficaz, comparado con el 33% de los ciberrezagados.

Por ejemplo, Accenture ha adoptado la IA y la automatización a través de nuestra Intelligent Application Security Platform. Al utilizar las mejores herramientas de análisis comerciales y la inteligencia artificial para identificar, verificar y reducir vulnerabilidades a escala, los equipos de aplicaciones ahorraron miles de horas y mejoraron la reducción de riesgos.

4. Respaldar los esfuerzos para cerrar la brecha de talentos en materia de seguridad

Cerrar la creciente brecha de talentos de seguridad al invertir en desarrollo de talentos junto a los esfuerzos de contratación Identificar los roles que pueden automatizarse o aumentarse con IA generativa. Pasar de ser un consumidor de talentos a un creador de talentos al contratar personas que posean rasgos tales como curiosidad, pensamiento crítico y habilidades de resolución de problemas, al tiempo que se ofrece capacitación para ocupar cualquier ausencia de competencias. Casi el 64% de los CEO ciberresilientes planea aumentar sus inversiones en formación y reciclaje laboral para sus equipos de ciberseguridad en los próximos tres años, comparado con el 38% de los ciberrezagados.

5. Adoptar la Ciberseguridad como un Servicio (CaaS) para las áreas de seguridad muy críticas

Prácticamente el 60% de los CEO ciberresilientes priorizan esta práctica. La mayoría concuerda en que CaaS a menudo ofrece beneficios tales como la reducción de costos, la consolidación de proveedores y al abordaje de la brecha de talentos.

Por ejemplo, cuando una cadena minorista norteamericana puso sus acciones en venta como corporación independiente, se vio obligada a repensar sus operaciones de TI. Accenture fue contratada para dar soporte al equipo de seguridad de la información del minorista con la incorporación de la ciberseguridad como un servicio, inicialmente haciéndose cargo de las operaciones de seguridad de la compañía, incluyendo inteligencia de amenazas y un Security Operations Center (SOC). En la actualidad, Accenture brinda protección de datos, gestión de identidades, seguridad de redes, gestión de vulnerabilidades y concientización sobre seguridad y gestión de riesgos como un servicio, mejorando la ciberresiliencia y los resultados comerciales del minorista por ser una empresa segura desde el inicio.

Proteger la base digital de la organización

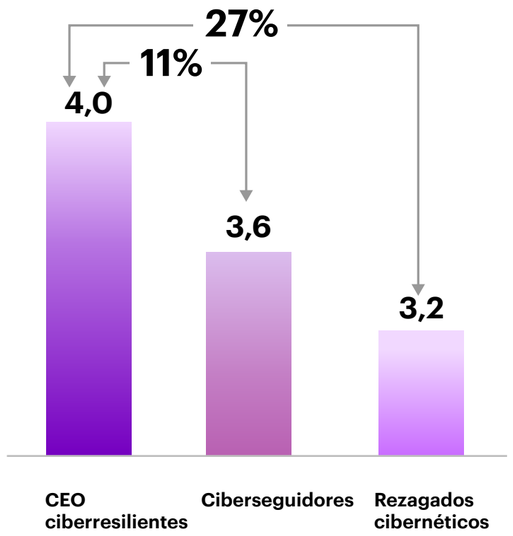
Los CEO deben prepararse ahora para un futuro en el cual los actores de las amenazas usen nuevas tecnologías tales como la computación cuántica para descifrar la mayoría de los algoritmos de codificación (con claves públicas) y decodificar la información confidencial del negocio y las personas, creando un enorme riesgo para la confidencialidad y la privacidad de los datos.

Nuestra investigación muestra que los CEO ciberresilientes garantizan que sus equipos aseguren el núcleo digital que consiste en tres capas: una capa de infraestructura y seguridad, una de datos e IA y una de aplicaciones y plataformas. Crean y sostienen un ambiente de confianza para clientes, empleados y socios de la cadena de suministros y están mejor preparados para reinventarse.

En la dimensión de **Tecnología** del índice de acciones del CEO, se evaluó el desempeño de los CEO sobre la base de su adopción de prácticas relativas a la seguridad para salvaguardar el núcleo digital. Los CEO ciberresilientes alcanzaron un puntaje de 4,0, superando a los rezagados en un 27% y a los aficionados en un 11%.

Los CEO ciberresilientes son más proactivos en la adopción de prácticas de seguridad que amplíen la seguridad de su infraestructura digital (Figura 10).

Figura 10. Los CEO ciberresilientes garantizan que sus equipos protejan la base digital



Fuente: Encuesta de Accenture 2023 a CEO ciberresilientes (n=1.000)

Pasos prácticos: Tecnología

1. Priorizar y promover la seguridad por diseño

Apoyar los esfuerzos del liderazgo para construir e implementar estrategias de seguridad ágiles que puedan responder rápidamente para minimizar el impacto de los ataques. Al hacerlo, las organizaciones pueden asegurar operaciones ininterrumpidas incluso ante un ciberataque. Para crecer con confianza, la competitividad del negocio requiere más digitalización y mejor ciberresiliencia. Como resultado, es fundamental reconocer que la deuda en materia de alta tecnología no debe producir una reducción en la inversión en seguridad. Más digitalización puede producir más resiliencia si no se trata a la ciberseguridad como una idea tardía. Cabe destacar que uno de cada dos CEO ciberresilientes incorpora la ciberseguridad a su núcleo digital desde el inicio. A modo de ejemplo, un importante banco minorista y comercial introdujo la toma de decisiones ágil en materia de ciberseguridad al inicio de su proceso de transformación digital para reducir riesgos y vulnerabilidades, mejorar la protección de datos y mejorar su posición general en cuanto a la seguridad. Más aún, el banco ha reducido costos y tiempo muerto al tiempo que mejoró el cumplimiento... y su reputación como una organización segura y confiable. Por otro lado, un estudio reciente reveló que descubrir un error causado por una mala seguridad de aplicaciones en la fase de codificación de la aplicación, y no en la planificación inicial, resulta cinco veces más caro de reparar, y eleva hasta 30 veces el costo posterior al lanzamiento.

2. Defender el enfoque de cero confianza

A la vanguardia de las responsabilidades del CEO se encuentra el rol clave de defender las estrategias de preparación para el futuro: en especial, la adopción proactiva de un marco de cero confianza. Este enfoque estratégico no solo redefine los paradigmas convencionales de la seguridad, sino que también funciona como catalizador del cultivo de resiliencia al tiempo que lidera la transformación del núcleo digital. La incorporación de una mentalidad de cero confianza implica un cambio fundamental en la manera de percibir y materializar la seguridad dentro de la organización. Supone tratar a cada intento de acceso como potencialmente no autorizado, independientemente del origen del usuario o la ubicación de la red. Al defender la verificación continua de las identidades de usuario, los atributos del dispositivo y los componentes de la red, los CEO sientan las bases de una cultura de mayor conciencia sobre seguridad.

La importancia de este enfoque se extiende más allá del refuerzo a las prácticas de seguridad. Al adoptar y defender los principios de cero confianza, los CEO activan la transformación integral de la arquitectura digital de la organización. Incluye recalibrar los controles de acceso a datos, implementar mecanismos robustos de encriptación e instalar sistemas de monitoreo y detección de anomalías de vanguardia en tiempo real. Este enfoque holístico y proactivo no solo asegura que los CEO posicionen a sus organizaciones a la vanguardia de la transformación digital segura sino que también cultiva la resiliencia al empoderar a sus equipos para que naveguen a través del escenario de las amenazas con confianza y agilidad. El setenta por ciento de los CEO ciberresilientes ya han adoptado el enfoque de cero confianza, comparado con solo el 41% de los demás.

Pasos prácticos: Tecnología

3. Priorizar la construcción de confianza digital

Colaborar con el Chief Data Officer y el CISO para asegurar que implementen medidas robustas de gobierno y protección de datos para los datos y la información confidencial de los clientes. Más de la mitad de los CEO ciberresilientes han adoptado este enfoque.

Los consumidores han dejado en claro que la confianza es importante; están dispuestos a abandonar a las marcas que no respalden a sus renovados valores. Estar listos para el cambio constante a medida que se generalizan las nuevas tecnologías. Por ejemplo, para asegurar la seguridad a largo plazo ante los avances en computación cuántica, se deberá adoptar la codificación cripto-ágil. Es fundamental tomar conciencia de los riesgos potenciales e implementar ahora algoritmos resistentes a lo cuántico para asegurar los sistemas y proteger los datos del cliente en el futuro.

4. Asegurar las tecnologías emergentes

Promover un sentido de responsabilidad en todos los equipos en relación con el desarrollo y el uso de tecnologías emergentes. Asignar más recursos al presupuesto de ciberseguridad a medida que avanzan en el viaje hacia la adopción y la implementación de tecnologías emergentes. Es notable que el 76% de los CEO ciberresilientes (contra el 41% de los ciberrezagados) tienen la intención de aumentar su presupuesto de ciberseguridad a medida que se intensifique la adopción de tecnologías emergentes.

La mitad de los CEO ciberresilientes considera que la IA generativa es una tecnología central de ciberdefensa que pueden usar para mejorar la ciberresiliencia. Evaluar y gestionar los riesgos asociados con la IA generativa y hacer que todos los miembros de la organización asuman responsabilidad por su uso seguro y eficaz, trabajando en conjunto con el CISO. Desarrollar un marco de seguridad con lineamientos, protocolos y parámetros de cumplimiento e incorporarlo a la IA generativa y los sistemas cuánticos desde el inicio. La IA generativa y el machine learning (ML) pueden potencialmente detectar y responder a amenazas de seguridad tales como malware, phishing y ataques de distributed denial-of-service (DDoS) en tiempo real, ampliar la automatización de la seguridad y analizar amplias hojas de datos para identificar patrones, anomalías y tendencias que indiquen fallas de seguridad. No obstante, la adopción de IA generativa debe encararse con precaución, y debe estar acompañada de estándares de gobierno y controles claramente definidos.

Extender la ciberresiliencia más allá de los límites de la organización

La ciberresiliencia es una meta más amplia que la mejora a la madurez de la función de seguridad de la información. Si bien los equipos de seguridad de la información deben constantemente mejorar las capacidades para contrarrestar un cambiante escenario de amenazas, si el énfasis del CEO está puesto solamente en hacer que el CISO asuma la responsabilidad, el resultado será una capacidad estanca que no se alinea con los riesgos comerciales de la compañía.

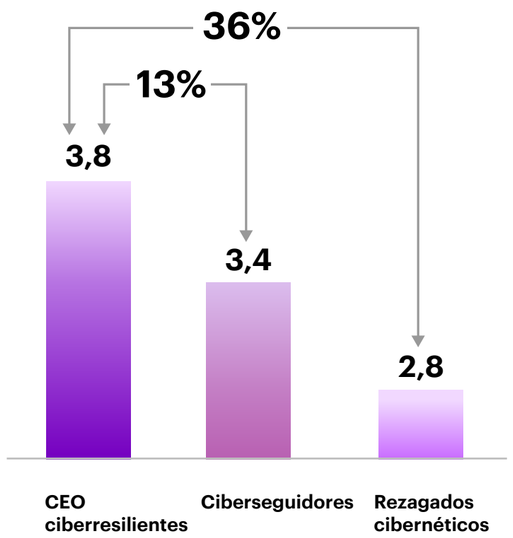
Debido a que el riesgo cibernético se ha convertido en uno de los principales riesgos comerciales, los CEO deben asegurar que la dirección ejecutiva evalúe y aborde los riesgos como parte de la Gestión de Riesgos Empresariales (ERM) general de la compañía. Esto queda reforzado por las disposiciones de la Comisión de Bolsa y Valores (SEC) recientemente adoptadas, que exigen que las empresas que cotizan en bolsa informen las competencias de ciberseguridad de sus directores, con lo cual la ciberseguridad pasa oficialmente al directorio.

Los riesgos cibernéticos aumentan en todas las áreas de la empresa, incluyendo los ambientes cibernéticos y físicos tales como fábrica o distribución, infraestructuras digitales tales como las plataformas offshore, productos digitales inteligentes tales como dispositivos médicos y cadenas de suministro y terceros.

Los ataques recientes han demostrado de qué manera una mayor interconectividad, el acceso a la red y las vulnerabilidades en la cadena de suministro y el ecosistema pueden afectar hasta a los negocios más seguros. Los CEO ciberresilientes establecen activamente un ambiente de confianza y preparan a sus organizaciones para futuras amenazas.

En la dimensión de los **ecosistemas** interno y externo del índice de acciones del CEO, los CEO ciberresilientes son proactivos en la protección de sus ecosistemas contra las vulnerabilidades. Los CEO ciberresilientes alcanzaron un puntaje de 3,8, que muestra una mejora en el desempeño del orden del 36% por sobre los ciberrezagados, y de un 13% por sobre los ciberseguidores (Figura 11).

Figura 11. Los CEO ciberresilientes son más proactivos a proteger sus ecosistemas



Fuente: Encuesta de Accenture 2023 a CEO ciberresilientes (n=1.000)

Pasos prácticos: Ecosistemas

1. Fijar la expectativa de que las sociedades estratégicas vuelven más resilientes a las cadenas de suministros

Reconocer el rol fundamental de la cadena de suministros en cada negocio y priorizar las sociedades con empresas que tengan sólidas posturas en materia de ciberresiliencia. Implementar políticas y controles personalizados para terceros e involucrarlos en evaluaciones compartidas, las preparaciones y los simulacros de las cibercrisis. Los CEO ciberresilientes superan a los ciberrezagados en un 40% en lo referente a la posibilidad de implementar políticas y controles específicos para terceros.

2. Colaborar abiertamente para contener ciberataques sorpresivos

Fomentar ambientes transparentes y colaborativos para contener ciberataques sorpresivos y minimizar su impacto. Comenzar con prácticas de compras transparentes que prioricen la ciberseguridad como un valor compartido en toda la cadena de suministros. Construir relaciones sólidas con las partes interesadas internas que tengan conocimientos de ciberseguridad. Además, participar en iniciativas de conocimientos compartidos con pares de la industria y socios en otras industrias. Estas iniciativas facilitan el intercambio de inteligencia oportuna y practicable, que incluye indicadores de compromiso y las principales prácticas para la identificación de actores maliciosos, que permiten a la empresa estar un paso adelante de las amenazas que surjan. Alrededor del 86% de los CEO ciberresilientes reconoce el valor que tiene contratar a proveedores de servicios de ciberseguridad para obtener conocimientos de los riesgos de ciberseguridad en todo el sector.

3. Interactuar proactivamente con entes reguladores y asociaciones público-privadas (PPPs) para mejorar la ciberresiliencia

La colaboración entre los entes gubernamentales y el sector privado es crucial para abordar los riesgos cibernéticos y salvaguardar la economía digital. Los organismos reguladores siguen ampliando y profundizando sus acercamientos a la ciberresiliencia ante fallas cada vez mayores que impactan en los consumidores y la infraestructura crítica. Los CEO deben interactuar proactivamente con los entes reguladores para alentar un acercamiento a la resiliencia basado e los riesgos y adoptar una nube basada en la confianza o en datos como por ejemplo, la nube híbrida o soberana. Además, los CEO que participan en PPPs facilitan un mayor uso compartido de la información, un mayor desarrollo tecnológico y esfuerzos conjuntos para combatir las ciberamenazas. Para lograrlo se debe:

- **Fomentar la colaboración**: Trabajar dentro de las empresas y en las sociedades público-privadas para reforzar la ciberdefensa y resiliencia. Colaborar con los gobiernos y las entidades del sector privado para establecer marcos de ciberseguridad y regulaciones específicas para el sector

Pasos prácticos: Ecosistemas

- **Participar en alianzas globales**: Participar en colaboraciones internacionales, como las que se realizan entre los Estados Unidos de América y la Unión Europea, con el fin de abordar eficientemente las ciberamenazas internacionales. La participación en foros, iniciativas y acuerdos internacionales facilita la cooperación, el uso compartido de las principales prácticas, la armonización de los estándares de ciberseguridad y el establecimiento de normas de conducta responsables en el ciberespacio. Además, se debe promover la colaboración y el uso compartido de la información dentro de y entre los países para reforzar las capacidades colectivas de ciberdefensa.
- **Colaboración bilateral específica para la industria**: Compartir de manera pública la inteligencia oportuna y practicable, que incluye indicadores de compromiso, tácticas, técnicas y las principales prácticas para identificar a los ciberdelincuentes conocidos, incluyendo el monitoreo continuo y la inteligencia contra amenazas.

4. Contratar empresas líderes en la protección del mundo ciberfísico

Las organizaciones amplían su huella global mediante la construcción de nuevas sucursales, fábricas y centros de entrega. Con mayores puntos de encuentro entre los mundos físico y cibernético y el uso expansivo de la tecnología operacional (OT), se deben proteger las nuevas operaciones de los ataques que intentan interrumpir las operaciones directamente o a través de nuevas cadenas de suministros específicas de la geografía.

5. Abordar y reconocer los vínculos y la exposición a vulnerabilidades entre las medidas ambientales y la resiliencia en materia de ciberseguridad

Abordar y reconocer la interconexión entre la creciente importancia de las iniciativas ambientales y la ciberresiliencia. A medida que las organizaciones reducen su dependencia de los combustibles fósiles—por ejemplo, al migrar hacia una red eléctrica más distribuida vía parques eólicos y proyectos de energía solar, cada uno con sistemas de control conectados y protocolos más complejos—podríamos quedar expuestos a nuevos desafíos en materia de ciberseguridad. Muchos de estos activos no fueron diseñados desde el inicio tomando en cuenta la ciberseguridad. Es fundamental asociar la resiliencia y sustentabilidad climática con la resiliencia en ciberseguridad. De no hacerlo, podrían aparecer más vulnerabilidades. Los CEO ciberresilientes tienen un 61% más de posibilidades de reconocer vulnerabilidades en materia de ciberseguridad dentro de las iniciativas ambientales, comparado con los ciberrezagados.

Pasos prácticos: Ecosistemas

6. Evaluar la ciberresiliencia más allá de la madurez cibernética de la seguridad de la Información

Si bien es importante evaluar la madurez cibernética de la empresa, la simple revisión de las capacidades de la función de seguridad de la información resulta insuficiente para alcanzar ciberresiliencia. En cambio, los CEO deben comprender y asegurar que estas capacidades se entrecrucen con la resiliencia general del negocio. Esto significa contar con un marco para evaluar y medir la penetración y efectividad de los controles en todas las funciones críticas de las cadenas de valor del negocio, asegurando que puedan operar a escala y con la velocidad requerida para respaldar la reinvención del negocio y atravesar las disrupciones. En muchos casos, las empresas aún no son capaces de articular qué es lo más importante para ellas y dónde se sienten que están en riesgo. Para alcanzar la resiliencia en el trabajo, debe existir una clara alineación de la estrategia, los riesgos y la asignación de recursos con el negocio, la tecnología y la seguridad de la información, así como con terceros.

7. Destacarse en la integración de la ciberseguridad y la gestión de riesgos

Integrar un marco basado en ciberriesgos al programa de gestión de riesgos de la empresa. Alinear las operaciones de ciberseguridad y el liderazgo ejecutivo para consensuar la prioridad de los activos y las operaciones que se deben proteger. Considerar en gran medida el riesgo de ciberseguridad al momento de evaluar el riesgo general de la empresa. Los CEO ciberresilientes promueven un enfoque de evaluación de riesgos en toda la empresa (64% de los CEO ciberresilientes contra 41% de los ciberrezagados) que trascienda unidades de negocios y funciones. Esta visión integral permite comprender de manera holística las vulnerabilidades, las fortalezas y la capacidad de la organización para defenderse de las ciberamenazas en forma proactiva.

Por ejemplo, cuando decidió integrar el riesgo de ciberseguridad al marco más amplio de gestión de riesgos empresariales, una compañía global de viajes pudo mejorar su gestión de riesgos, el cumplimiento de los requisitos regulatorios y la protección del negocio y sus clientes. Más aún, los CEO ciberresilientes priorizan la verificación de sus operaciones cibernéticas en toda la organización. Al realizar evaluaciones periódicas para detectar vulnerabilidades, minimizan el elemento sorpresa de los ciberataques.

Este enfoque proactivo les permite identificar y abordar las potenciales debilidades, reduciendo así el impacto de los ciberincidentes. El 70% de los CEO ciberresilientes aplican esta práctica, comparado con el 36% de los ciberrezagados.

Adoptar la ciberresiliencia continua para mantenerse a la vanguardia

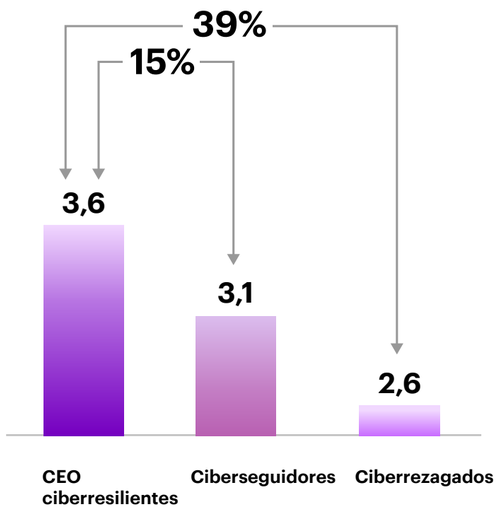
Los CEO ciberresilientes se comprometen con la implementación de prácticas que promueven un ambiente seguro dentro de sus organizaciones y ecosistemas.

Comprenden que la ciberseguridad no es una iniciativa única y reconocen la necesidad de realizar esfuerzos continuos para reforzar sus defensas y adaptarse a fin de permanecer a la vanguardia.

En la dimensión de **resiliencia continua** del índice de acciones del CEO, los CEO ciberresilientes superan a los ciberrezagados en un 39% y a los ciberseguidores en un 15%.

Figura 12.

Los CEO ciberresilientes reconocen a la ciberseguridad como un esfuerzo continuo



Fuente: Encuesta de Accenture 2023 a CEO ciberresilientes (n=1.000)

Pasos prácticos: Resiliencia continua

1. Redefinir el perfil de riesgos

Comprometerse a establecer constantemente medidas de ciberseguridad líderes en la industria que tomen en cuenta el cambiante panorama de riesgos y se alineen con las prioridades de negocios. Los CEO ciberresilientes amplían continuamente sus referencias de desempeño cibernético para ir al compás del cambiante escenario de amenazas. Al ampliar las definiciones de riesgo y tolerancia, 60% de los CEO ciberresilientes se distinguen al adoptar este enfoque proactivo, comparado con solo 34% de los ciberrezagados.

2. Realizar revisiones independientes y evaluaciones de mejora continua de los programas de seguridad

Evaluar el programa de seguridad de la organización mediante revisiones externas e implementar las mejoras para alinearse con el cambiante escenario de amenazas. Casi dos tercios de los CEO ciberresilientes adoptan esta práctica y así superan a los rezagados por un substancial margen de 27 puntos porcentuales.

3. Construir la preparación para apagones en materia de ciberseguridad

Crear e implementar un libro de prácticas de respuestas integrales a las cibercrisis que incluyan aspectos clave tales como la toma de decisiones a nivel ejecutivo, los protocolos de comunicación interna y externa, y la colaboración con asesores legales externos, agencias de seguridad y equipos externos de respuesta a incidentes de ciberseguridad. El libro de prácticas asegura una respuesta eficaz a escenarios graves como los ataques generalizados de ransomware, los ataques específicos o las vulnerabilidades de día cero. Más aún, las organizaciones deben aislar las copias de respaldo de las aplicaciones críticas dentro de una bóveda de ciberseguridad, para poder reiniciar las operaciones mientras se reconstruyen los sistemas de producción.

4. Defender la IA y el ML avanzado para alcanzar una protección proactiva contra las amenazas

Indicar a los ejecutivos que aprovechen el poder de los datos, las IA generativa y el *machine learning* avanzado para ser proactivos en la preparación, predicción y protección contra las ciberamenazas. La integración revoluciona la ciberresiliencia, permitiendo la detección de amenazas proactiva, la respuesta automática a los incidentes, la defensa adaptable, las analíticas predictivas y las medidas de seguridad ampliadas. Todos los CEO ciberresilientes planean liderar y dirigir a sus empleados en el uso de datos, IA generativa y *machine learning* avanzado para detectar y protegerse de los ciberataques antes de su ocurrencia, ganando de este modo una ventaja competitiva.

Lista de verificación del CEO ciberresiliente

Estrategia

- Establecer una estrategia de protección cibernética diseñada para proteger las iniciativas estratégicas y el valor corporativo
- La ciberseguridad debe reducir el riesgo y optimizar las capacidades de las organizaciones, y debería recibir el mismo nivel de importancia que el desempeño financiero.

Talento y cultura

- Exigir la implementación de ciberseguridad por parte de los líderes de negocios en sus respectivos departamentos y ofrecer capacitación en ciberseguridad a los empleados.
- Promover una cultura de expertos en ciberseguridad en todos los niveles.
- Llevar a cabo las capacitaciones necesarias para mejorar las capacidades del equipo y, de ser necesario, incorporar a proveedores de servicios de seguridad gestionados.

Tecnología

- El diseño de la base digital debe incluir la seguridad y dicha base debe contar con un acceso seguro.
- Los datos del cliente son clave para la construcción de la confianza digital y es importante que las organizaciones lo aseguren.

Ecosistemas

- Comprender y gestionar los riesgos externos para ayudar a reducir la exposición a los ataques.
- La evaluación de ciberriesgos no debe limitarse a departamentos o funciones específicas, sino que debe convertirse en un ejercicio de toda la empresa.
- Realizar simulacros de ataques para probar la ciberresiliencia.
- Monitorear de cerca el tiempo necesario para detectar y para contener las amenazas.

Resiliencia continua

- Usar los contactos que hayan experimentado un incidente grave para ayudar a educarse y a prepararse para potenciales ataques.
- Desarrollar ahora una relación de colaboración para hacer un uso compartido de la inteligencia contra amenazas y dar forma a las políticas de ciberseguridad a nivel nacional e internacional.
- Elaborar referencias de seguridad líderes en la industria y usar la tecnología para prever amenazas antes de su ocurrencia.

Acerca de la investigación

Adoptamos un enfoque de métodos múltiples

La encuesta a CEO ciberresilientes de Accenture se realizó en junio de 2023 y contó con la participación de 1.000 CEO globales de 19 industrias en 15 países. Los participantes respondieron preguntas que ayudaron a determinar su conocimiento y comprensión de la ciberseguridad y su ciberresiliencia, así como el enfoque de sus organizaciones hacia las prácticas de negocios en materia de ciberseguridad.

Los participantes representan a organizaciones con ingresos anuales de US$ 1.000 millones* o más en América del Norte y del Sur, Europa, la región de Asia Pacífico y Medio Oriente.

1,000 CEO participantes

15 países

Australia (68)
Brasil (67)
Canadá (67)
Francia (67)
Alemania (68)
Irlanda (68)
Italia (65)
Japón (66)
Países Bajos (66)
Noruega (66)
Arabia Saudita (63)
España (67)
Emiratos Árabes Unidos (64)
Reino Unido (67)
Estados Unidos de América (71)

USD 1.000 M+ de ingresos

19 industrias

Industria aeroespacial (55)
Automotriz (52)
Banca (53)
Mercados de Capitales (53)
Productos químicos (53)
Bienes y Servicios de Consumo (53)
Energía – Petróleo y Gas (54)
Pagadores de Salud (52)
Proveedores de Salud (52)
Alta Tecnología (52)
Industrial (53)
Seguros (53)
Ciencias de la Vida (51)
Satención al Público (47)
Minorista (54)
Software y Plataformas (54)
Telecomunicaciones (52)
Viajes (54)
Servicios públicos (53)

*<1% de la muestra *<1% de la muestra debe tener ingresos de entre US$ 500 millones y US$ 1.000 millones para cumplir con el cupo de la encuesta

Índice de acciones del CEO ciberresiliente

En un estudio de 25 prácticas de CEO relacionadas con la ciberseguridad, identificamos cinco temas de acción principales. Estos temas de acción pueden ayudar a las organizaciones a evaluar y redefinir sus estrategias para sentar las bases de la resiliencia en ciberseguridad de primera línea.

Cómo lo hicimos

Con el fin de identificar las principales 25 prácticas de ciberseguridad en las organizaciones ciberresilientes, emprendimos un extenso trabajo de investigación en el cual revisamos la literatura empírica sobre ciberseguridad, obtuvimos información de expertos internos y externos en el tema y aprovechamos nuestra propia experiencia de trabajo con organizaciones de alto desempeño. Luego, agrupamos estas 25 prácticas en cinco temas de acción y desarrollamos un activo de diagnóstico: el índice de acciones del CEO ciberresiliente. Este índice compara y calcula el puntaje de adopción de acciones de seguridad de una compañía. Definimos un índice como la medición del desempeño de las compañías en un continuo. El continuo utilizado en este estudio se basó en cinco puntos. El índice se utiliza para comparar a las empresas con el fin de comprender cómo califican en relación con las demás dentro de este continuo. Para determinar el mecanismo de puntuación, se otorgó un puntaje en el índice a cada una de las preguntas.

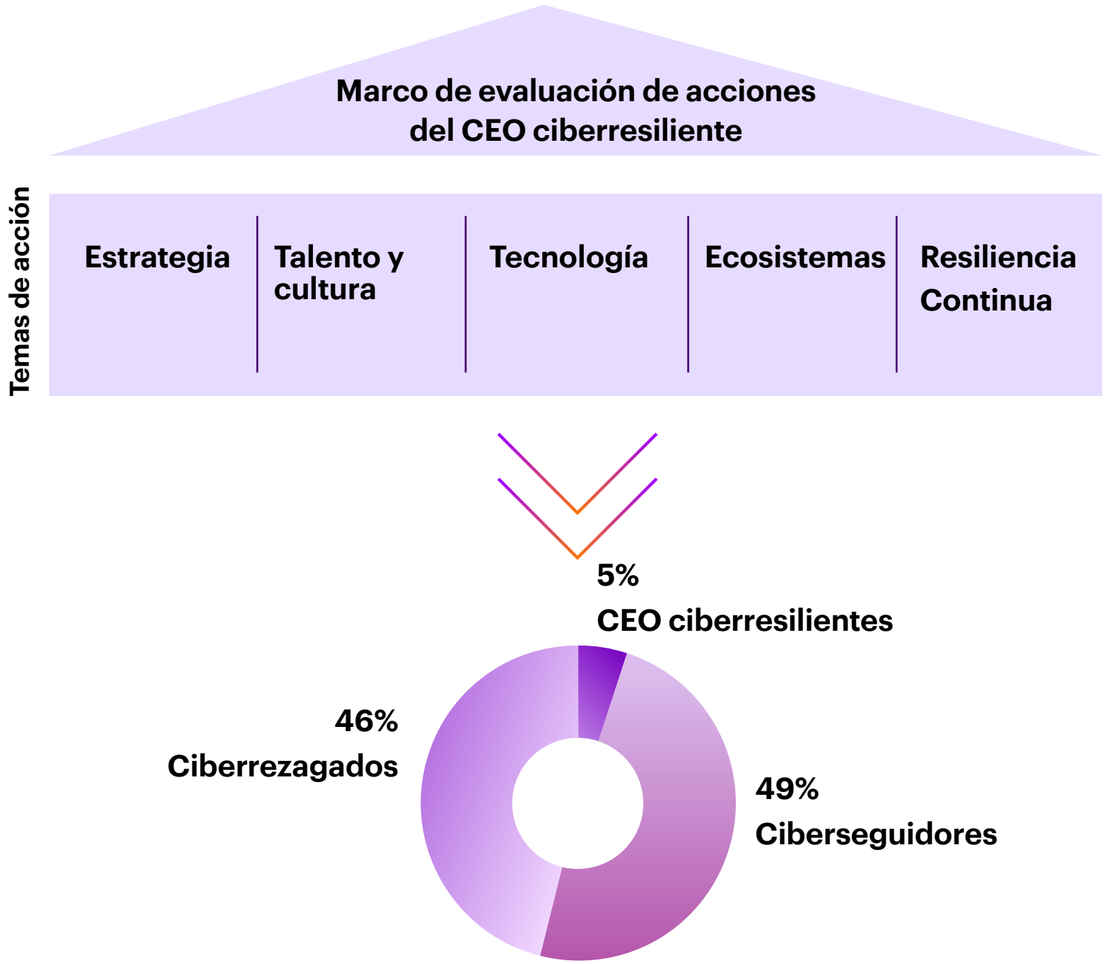
Para validar el índice, analizamos y probamos estadísticamente la adopción de las 25 prácticas en los cinco temas de acción con 1.000 CEO de grandes empresas de todo el mundo.

Como resultado, identificamos tres arquetipos de CEO:

- **Ciberresilientes**: Representando solo el 5% de nuestra muestra de 1.000, estas empresas mostraron un desvío estándar por sobre el puntaje medio en el índice y han adoptado por lo menos 60% de las acciones o más.

- **Ciberseguidores**: Estas empresas mostraron un desvío estándar por sobre el puntaje medio del índice pero han adoptado menos del 60% de las cinco medidas. Representan el 49% de la muestra.

- **Ciberrezagados**: El 46% de la muestra que no mostró un desvío estándar por sobre el valor medio del índice en ninguna de las acciones.



Índice de disrupción global de Acccenture

Creamos una medición general de disrupción para evaluar el nivel de volatilidad y cambio en el ambiente de negocios externo. El índice se basa en el promedio de seis subcomponentes que abarcan los ámbitos económico, social, geopolítico, ambiental, de consumo y tecnológico. Cada subcomponente se basa en un conjunto de puntajes clasificados para una variedad de indicadores. El componente económico se basa en los puntajes de riesgo económico. El Índice de Volatilidad (VIX), Producto Bruto Interno (PBI), la volatilidad y la volatilidad de la inflación. La geopolítica se basa en el riesgo de inestabilidad geopolítica. El componente social releja el descontento social y la falta de participación en el mercado laboral. El componente ambiental refleja la frecuencia de las catástrofes relacionadas con el clima y el riesgo impulsado por el clima. El componente de consumo refleja el pesimismo a nivel global, y es inverso al Índice de Confianza del Consumidor de OECD. Por último, el componente tecnológico se basa en un índice que consta de 24 indicadores, que utilizan la presencia de elementos disruptores y el desempeño de los actores tradicionales para representar el nivel de innovación disruptiva en las industrias.

Análisis de las comunicaciones de los inversores según la ciencia de datos

Usamos ingeniería rápida y GPT3.5 para analizar los *earning call transcripts* de las principales 2.000 compañías entre 2017 y 2022. Analizamos los comentarios de los CEO para verificar la frecuencia de uso de palabras clave relacionadas con ciberriesgo, ciberseguridad y estrategia cibernética. Este ejercicio nos ayudó a comprender la creciente conciencia acerca de la ciberseguridad en los CEO.

Puntajes de ciberconocimiento en 360°

Usamos nuestra encuesta para evaluar y calificar de qué manera los Ceo perciben y asocian la ciberseguridad con los siguientes parámetros:

- **Sustentabilidad**: ¿Desarrollaron los CEO una perspectiva más amplia de iniciativas de sustentabilidad en la cual ven a la ciberseguridad como parte central de sus metas ambientales?
- **Talento**: ¿En qué medida los CEO reconocieron la importancia de abordar la brecha de talento en la ciberseguridad?
- **Innovación tecnológica**: Los CEO, ¿adoptaron e implementaron la tecnología emergente en forma segura?
- **Confianza del cliente**: ¿Comprendieron los CEO que un ciberataque tendría un impacto negativo sobre la confianza del cliente y podría generar desgaste en los clientes?

Por último, complementamos el estudio con un análisis de estudios de casos, así como revisiones escritas e investigaciones secundarias de varias fuentes.

Referencias

1 Cybercrime To Cost The World $10.5 Trillion Annually By 2025, Cyber Crime Magazine, Noviembre de 2020, https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

2 Global cybersecurity spending to top $219B this year: IDC, Cybersecurity Dive, Marzo de 2023, https://www.cybersecuritydive.com/news/cybersecurity-spending-increase-idc/645338/#:~:text=Global%20security%20spending%20will%20reach,an%20IDC%20forecast%20released%20Thursday

3 Accenture, Total Enterprise Reinvention, 2023, https://www.accenture.com/us-en/insights/consulting/total-enterprise-reinvention

4 Foro Económico Mundial y Accenture, Global Cybersecurity Outlook 2023, https://www.weforum.org/reports/global-cybersecurity-outlook-2023/

5 Cybercrime To Cost The World $10.5 Trillion Annually By 2025, Cyber Crime Magazine, Noviembre de 2020, https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

6 NonPetya ransomware forced Maersk to reinstall 4000 servers, 45000 PCs, ZDNet, Enero de 26, 2018, https://www.zdnet.com/article/maersk-forced-to-reinstall-4000-servers-45000-pcs-due-to-notpetya-attack/

7 Análisis de Accenture de la transcripción de NLP de las Principales 2000 empresas mundiales, 2017 a 2022

8 Colonial Pipeline CEO acknowledges paying hackers to restore pipeline, Reuters, 7 de Junio de 2021, https://www.reuters.com/business/energy/colonial-pipeline-ceo-paid-ransom-swiftly-restart-pipeline-testimony-2021-06-07/

Acerca de Accenture

Accenture es una compañía global líder en servicios profesionales que ayuda a las principales empresas, gobiernos y organizaciones a construir sus núcleos digitales, optimizar sus operaciones, acelerar el crecimiento de ingresos y ampliar los servicios a los ciudadanos, creando valor tangible rápidamente y a escala. Somos una empresa guiada por el talento y la innovación con 733.000 empleados que atienden en más de 120 países. La tecnología se encuentra en el centro del cambio actual y somos uno de las empresas líderes a nivel mundial que ayudan a impulsar el cambio, con fuertes relaciones con los ecosistemas. Combinamos nuestra fortaleza en tecnología con experiencia sin igual en la industria, pericia funcional y capacidad de entrega global. Tenemos la exclusiva capacidad de producir resultados tangibles debido a nuestra amplia variedad de servicios, soluciones y activos en Estrategia y Consultoría, Tecnología, Operaciones, Industria

X y Accenture Song. Estas capacidades, junto con nuestra cultura de éxito y compromiso compartidos con la creación de valor de 360°, nos permite ayudar a nuestros clientes a alcanzar el éxito y construir relaciones de confianza duraderas. Medimos el éxito con el valor de 360° que creamos para nuestros clientes, cada uno de nosotros, nuestros accionistas, nuestros socios y las comunidades.

Visítenos en www.accenture.com/cloud

Acerca de Accenture Research

Accenture Research genera liderazgo de pensamiento sobre los problemas de negocios más acuciantes que enfrentan las organizaciones. Combinando técnicas de investigación innovadoras, tales como el análisis guiado por la ciencia de datos, con nuestra profunda comprensión de la industria y la tecnología, nuestro equipo de 300 investigadores en 20 países publica cientos de informes, artículos y puntos de vista por año. Nuestra investigación –que invita a la reflexión– desarrollada con organizaciones líderes en todo el mundo, ayuda a nuestros clientes a adoptar el cambio, crear valor y cumplir con el poder de la tecnología y el ingenio humano.

Para más información, visite **www.accenture.com/research**