



Servicios de Consultoría

**Recuperando la  
ciberseguridad:  
prepárese para  
enfrentar  
los ataques  
cibernéticos**

Encuesta Global de Seguridad  
de la Información 2017-18



Building a better  
working world





# >Contenido

---



---

	<b>Bienvenida</b>	
<b>I</b>	<b>¿Está preparado para enfrentar los ataques cibernéticos?</b>	
	> Introducción	8
	> Sección 1: Enfrentando las amenazas cibernéticas	10
	> Sección 2: Comprendiendo el panorama de amenazas	13
	> Sección 3: Defendiéndose contra las amenazas	18
	> Sección 4: Servicio de emergencia: respondiendo a un ataque	28
	> Conclusión	32
	> Metodología	36
<b>II</b>	<b>Una visión integral para gestionar el riesgo cibernético</b>	
	> Ciberseguridad integral	40
	> Sección 1: Las 5 prioridades de la ciberseguridad	42
	> Sección 2: 10 cosas que debe hacer ahora	58
<b>III</b>	<b>Gestión de riesgos cibernéticos en todas las líneas de defensa</b>	
	> Las líneas de defensa	62
	> Sección 1: Plan de acción para un gobierno de riesgos cibernéticos en toda la empresa	66
	> Sección 2: Gobierno de riesgos cibernéticos	74
<b>IV</b>	<b>¿Cómo proteger a los robots de un ataque cibernético?</b>	
	> Sección 1: ¿A qué nos referimos con robótica?	81
	> Sección 2: Asegurando la RPA	84
	> Sección 3: Aprovechando la robótica para la ciberseguridad	88
	<b>Contactos EY Perú</b>	96



# > Bienvenida

---



Jorge Acosta  
Socio Líder de Consultoría

Presentamos nuestra **20ª Encuesta Global de Seguridad de Información 2017-2018 "Recuperando la ciberseguridad: prepárese para enfrentar los ataques cibernéticos."** Es así que, por cuarto año consecutivo en el Perú, tengo el agrado de presentar el informe de resultados de nuestra encuesta global, acompañado de los resultados locales. En esta edición nos ha complacido contar con casi 1,200 participantes a nivel mundial. Es invaluable la contribución de los representantes de las empresas peruanas, a quienes les hago presente nuestro más sincero agradecimiento.

Durante los últimos años, hemos visto como el mundo ha cambiado: los avances tecnológicos, la interconexión, el IoT, *blockchain*, la inteligencia artificial, la inteligencia cognitiva, la globalización de la economía, el desarrollo de los mercados, las telecomunicaciones, los dispositivos de telecomunicación, el comercio electrónico, la era digital, la innovación de los procesos y modelos

de negocio; no son solo conceptos, son una realidad, y con ello han aparecido nuevos y más riesgos de seguridad de información. Año a año observamos como la percepción de riesgo de seguridad ha ido incrementando, hemos visto la importancia de la Defensa Activa y la capacidad de desarrollar actividades de inteligencia avanzada sobre amenazas cibernéticas, y gestionar de forma proactiva esas amenazas. Hemos tomado consciencia de la importancia de la resiliencia cibernética y cómo debemos entender y desarrollar nuestras capacidades en nuestras empresas en sus tres áreas: sentir, resistir y reaccionar, y poder enfrentar a las crecientes amenazas cibernéticas. Sin embargo, la percepción de riesgos se sigue incrementando.

Si bien todos los enfoques pueden y deben seguir siendo aplicados, ahora somos más conscientes que debemos comprender el panorama de amenazas, defendernos y responder a un ataque.



Con la velocidad de los cambios en el entorno, es cada vez más difícil adelantarse a estas ciberamenazas.

En EY, tenemos una perspectiva integrada de todos los aspectos que representan riesgos en las organizaciones y somos líderes en el mercado en riesgos y controles y seguridad cibernética. Como líder en servicios de gestión de riesgos, EY trabaja de la mano con clientes de diversos tamaños y sectores de la economía, aportando conocimientos y experiencia en cada trabajo.

La presente publicación tiene como objetivo brindar un análisis y exponer estrategias innovadoras para que las distintas organizaciones del Perú puedan enfrentar los desafíos de seguridad de información en un mundo cambiante. El enfoque de nuestros servicios ha logrado integrar la gestión de la seguridad de información con la gestión de riesgos y la mejora de desempeño de nuestros clientes. Cuenten con nosotros como sus socios en su proceso de crecimiento sostenible. Nos ponemos a su disposición para asistirlos.

Atentamente,

**Jorge Acosta**







¿Está preparado para  
enfrentar los ataques  
cibernéticos?



# > Introducción

Bienvenidos a la 20ª Encuesta Global de Seguridad de la Información de EY (GISS, por sus siglas en inglés), la cual analiza los problemas de ciberseguridad más importantes que enfrentan las organizaciones hoy en día.

Dos décadas después de que EY publicara por primera vez encuestas anuales que detallaban las preocupaciones de las organizaciones con respecto a la ciberseguridad -así como sus esfuerzos para enfrentarlas-, la necesidad de una respuesta colaborativa y coherente a las nuevas

Si su organización está preocupada con respecto a la ciberseguridad, puede resultar reconfortante saber que no es la única.

amenazas no podría ser más apremiante. En nuestras conversaciones con organizaciones de todas las formas y tamaños, resulta claro que la ciberseguridad es un asunto prioritario desde el Comité hasta los demás niveles. Pero en un panorama complejo y en evolución, puede ser difícil ver la imagen completa: la amenaza de la ciberseguridad a menudo está bien camuflada, oculta a la vista.

Este año, estamos encantados de decir que casi 1,200 organizaciones pudieron participar en la encuesta. Hemos analizado las respuestas de directores de sistemas de la información, directores de seguridad de la información y otros ejecutivos, identificando fortalezas y debilidades a fin de generar una visión de la que todos podamos beneficiarnos. El informe GISS también se basa en nuestra amplia experiencia de trabajo con clientes a nivel mundial para mejorar su resiliencia en ciberseguridad.

La mayoría de las organizaciones sienten que están en mayor riesgo hoy que hace 12 meses. No es de extrañar: no solo los atacantes



cibernéticos se están volviendo más sofisticados, sino que las propias organizaciones están cada vez más hiperconectadas con oleadas de nuevas tecnologías que crean oportunidades y riesgos en toda la cadena de valor. Esta explosión de conectividad, impulsada por el crecimiento del Internet de las cosas (IoT, por sus siglas en inglés) y la cada vez mayor huella digital de muchas organizaciones, ha introducido nuevas vulnerabilidades que los atacantes pueden aprovechar. Es por eso que las empresas necesitan explorar los recursos digitales desde todos los ángulos, de modo que las ayuden a crecer y proteger sus organizaciones hoy, mañana y en el futuro.

Sin embargo, a pesar de los riesgos, también hay buenas noticias. Las organizaciones que enfrentan de manera adecuada el desafío de la ciberseguridad recuperarán el sentido del orden: no es posible repeler todas las amenazas, pero las organizaciones resilientes saben cómo protegerse, cómo detectar un problema cuando ocurre y cómo reaccionar de manera rápida y efectiva cuando surge un inconveniente.

Además, ahora tenemos una buena comprensión de los métodos de ataque más comunes y un gran aprecio por los componentes de una buena estructura de ciberseguridad, con los que la mayoría de estos ataques pueden derrotarse. Las estrategias de defensa activa y la inteligencia avanzada de amenazas proporcionan una base para resistir métodos de ataque más sofisticados y, si bien surgen nuevos métodos de ataque todo el tiempo, un buen gobierno de ciberseguridad y conceptos como “seguridad por diseño” dan a las organizaciones la oportunidad de luchar.

Trabajando juntos  
podemos recuperar la  
ciberseguridad.

## > Sección 1

---

# Enfrentando las amenazas cibernéticas

Hoy en día, todas las organizaciones son digitales por defecto. No todas las organizaciones ofrecen sus productos y servicios a través de canales digitales, pero todas operan con las culturas, la tecnología y los procesos de la era del Internet. Además, en el mundo conectado y convergente dado por el Internet de las cosas (IoT, por sus siglas en inglés), el panorama digital es vasto, y todos los activos utilizados por las organizaciones representan otro nodo en la red.

No es de extrañar que el Foro Económico Mundial considere que un fallo de ciberseguridad a gran escala es uno de los cinco riesgos más graves que enfrenta el mundo de hoy.<sup>1</sup> La escala de la amenaza se está expandiendo drásticamente: para el 2021, el costo global de las brechas en la ciberseguridad alcanzará los 6 billones de dólares según algunas estimaciones, el doble del total considerado para el 2015.<sup>2</sup>

Los ciberatacantes pueden tener un objetivo indiscriminado o altamente específico, y atacar organizaciones grandes o pequeñas ya sea del sector público o privado. Están bien camuflados: lograr exponer a los atacantes requiere defensas de ciberseguridad que identifiquen la amenaza,

---

<sup>1</sup> "Informe Global de Riesgos 2017", World Economic Forum, 11 de enero de 2017.

<sup>2</sup> "Edición 2017 del Informe del Cibercrimen", Cybersecurity Ventures, 19 de octubre de 2017.

incluso cuando adopte los colores de su entorno inmediato. Las organizaciones no siempre están preparadas para este escenario.

Solo este año, en el Reino Unido, el ataque *ransomware WannaCry* afectó una parte significativa del Servicio Nacional de Salud (NHS, por sus siglas en inglés).<sup>3</sup> En Francia, una brecha en la campaña presidencial de Emmanuel Macron amenazó con sumergir las elecciones en el caos.<sup>4</sup> En Estados Unidos, Yahoo reveló que una brecha vio comprometidas las cuentas de 3 mil millones de usuarios.<sup>5</sup> Y en India, un ataque paralizó el mayor puerto de contenedores de Mumbai.<sup>6</sup>

Al mismo tiempo, nunca ha sido más difícil para las organizaciones mapear el entorno digital en el que operan, o sus interacciones con él. La infraestructura tecnológica de cada organización es diferente y compleja, y abarca redes que constan de herramientas y tecnologías que pueden estar en las mismas instalaciones o en la nube. Además, cada vez es más difícil definir una “organización”, esto se debe a la proliferación de dispositivos pertenecientes a empleados, clientes y proveedores (incluyendo computadoras portátiles, tabletas, teléfonos móviles y más) con acceso a los sistemas de la organización, lo cual no permite definir con claridad el perímetro de seguridad. Las organizaciones se ven como pulpos con largos tentáculos que se arrastran en todas las direcciones.

Los dispositivos conectados se suman a esta complejidad. El IoT no es una colección de elementos pasivos, sino más bien una red de dispositivos conectados e interconectados que interactúan activa y constantemente. La convergencia de estas redes con sistemas que

alguna vez fueron separados y autónomos, y por lo tanto más manejables, representa un cambio fundamental.

Lo que está en juego no podría ser mayor. Las organizaciones son víctimas de un ataque cibernético corren el riesgo de sufrir una pérdida de reputación considerable así como los costos directos de la brecha, los cuales se estiman en US\$3.62m según el Instituto Ponemon.<sup>7</sup> También existe la posibilidad de enfrentamientos perjudiciales con las autoridades y las entidades reguladoras. El Reglamento General de Protección de Datos de la Unión Europea (RGPD), que entrará en vigor en el 2018, concede poderes a las entidades reguladoras para multar a las organizaciones con hasta 2% de su facturación anual global por fallas relacionadas con una brecha y 4% si la organización maneja su respuesta de manera incorrecta.<sup>8</sup>

Tampoco son solo los datos y la privacidad los que son vulnerables. El IoT expone las tecnologías operativas de las organizaciones a los atacantes, ofreciéndoles la oportunidad por ejemplo de apagar o sabotear sistemas de controles industriales. La amenaza puede ser incluso para la vida: imagine que el atacante tenga la capacidad de apagar los sistemas de soporte vital en los hospitales o de tomar el control de los automóviles conectados en la carretera.

Los crecientes niveles de amenazas requieren una respuesta más robusta, y el GISS de este año revela que muchas organizaciones continúan aumentando sus gastos de ciberseguridad. El 70% afirma que necesita hasta 25% más fondos, y el resto requiere incluso más que esto. Sin embargo, solo 12% espera recibir un aumento de más de 25%.

3 “Investigación: Ciberataque WannaCry y el NHS”, *National Audit Office*, 27 de octubre de 2017.

4 “Hackers golpean la campaña de Macron con ataque ‘masivo’”, *Financial Times*, 6 de mayo de 2017.

5 “Las 3 mil millones de cuentas de Yahoo fueron afectadas por el ataque del 2013”, *The New York Times*, 3 de octubre de 2017.

6 “Ciberataque Petya: India es la más afectada en Asia, Ucrania a nivel mundial”, *The Indian Express*, 29 de junio de 2017.

7 “Estudio del Costo de la Fuga de Información 2017”, *The Ponemon Institute*, junio de 2017.

8 “Portal RGPD: Visión general del sitio”, *European Union*, octubre de 2017.



de los encuestados afirma que su presupuesto ha aumentado en los últimos 12 meses



necesita hasta 50% más presupuesto



espera un aumento de más de 25 % en su presupuesto de ciberseguridad



de las organizaciones se sienten seguras de haber considerado plenamente las implicancias de seguridad de la información de su estrategia actual, y de haber incorporado y monitoreado en su panorama de riesgos las amenazas, vulnerabilidades y riesgos cibernéticos correspondientes.



Para muchas organizaciones tendría que pasar lo peor para que se cumplan estas demandas. Cuando se preguntó qué tipo de evento propiciaría el aumento de los presupuestos de ciberseguridad, 76% de los encuestados indicó que descubrir una brecha que causara daños, probablemente haría que se asignaran más recursos.

Por el contrario, 64% dijo que un ataque que no pareciera haber causado ningún daño, probablemente no provocaría un aumento en el presupuesto de ciberseguridad de la organización. Esta cifra es más alta que la reportada el año pasado, lo cual es preocupante dado que los ataques generalmente causan daño, aunque este no sea inmediatamente obvio. El fallo puede ser un ataque de prueba que expone la vulnerabilidad o una distracción diseñada para desviar la atención de otra amenaza más dañina; alternativamente, el atacante puede simplemente estar esperando un poco antes de aprovechar la brecha. Las organizaciones deben asumir que todos los ataques son dañinos y concluir que cuando no se ha identificado el daño, es simplemente porque aún no se ha descubierto.

En definitiva, a las organizaciones que no dedican los recursos necesarios para una ciberseguridad adecuada se les hará muy difícil gestionar los riesgos que enfrentan. Nuestra encuesta sugiere que las organizaciones lo reconocen cada vez más: 56% de los encuestados dice haber hecho cambios en sus estrategias y planes para tener en cuenta los riesgos generados por las ciberamenazas, o estar a punto de revisar la estrategia en este contexto. Sin embargo, solo 4% de las organizaciones se sienten seguras de haber considerado plenamente las implicaciones de seguridad de la información de su estrategia actual y de haber incorporado todos los riesgos y amenazas relevantes.

## > Sección 2

# Comprendiendo el panorama de amenazas

El primer paso para las organizaciones que buscan mejorar su capacidad de ciberseguridad, es desarrollar una mejor comprensión de la naturaleza de la amenaza. No será posible desarrollar una mayor resiliencia de ciberseguridad en la organización sin identificar primero las posibles causas de daño y cómo podrían manifestarse. Entender la situación es crucial: ¿Cuáles son las amenazas y qué significan para usted y su organización?

Además, el rango de ataques potenciales y de atacantes es amplio y lo es cada vez más con el pasar de los días. Las organizaciones pueden sentirse más seguras al enfrentar los tipos de ataques que se han vuelto conocidos en los últimos años, pero aún carecen de la capacidad para hacer frente a ataques más avanzados y selectivos; es posible que ni siquiera estén al tanto de los métodos de ataque que están surgiendo. Sin embargo, para ser ciber-resilientes, las organizaciones deben aumentar su comprensión rápidamente; es probable que enfrenten todas estas categorías de ataque en un momento u otro, y tal vez simultáneamente.

## &gt; El panorama de amenazas

	Ataques comunes	Ataques avanzados	Ataques emergentes
> ¿Qué son?	Son ataques que aprovechan vulnerabilidades conocidas utilizando herramientas de <i>hacking</i> de acceso libre, con poca experiencia requerida para tener éxito.	Son ataques que aprovechan vulnerabilidades complejas y algunas veces desconocidas ("día cero") utilizando herramientas y metodologías sofisticadas.	Son ataques que se centran en nuevos vectores de ataque y vulnerabilidades habilitadas por tecnologías emergentes, basándose en investigaciones específicas para identificar y aprovechar vulnerabilidades.
> Típicos actores de la amenaza	Atacantes poco sofisticados, como empleados descontentos, competidores, <i>hacktivistas</i> y algunos grupos de crimen organizado.	Atacantes sofisticados como grupos de crimen organizado, equipos de espionaje industrial, terroristas cibernéticos y estados nación.	Atacantes sofisticados como grupos de crimen organizado, equipos de espionaje industrial, terroristas cibernéticos y estados nación.
> Ejemplos	<ul style="list-style-type: none"> <li>▶ Aprovechar vulnerabilidad sin parche en un sitio web, utilizando un <i>exploit kit</i> de acceso libre.</li> <li>▶ Enviar un <i>malware</i> genérico a través de una campaña de <i>phishing</i>, permitiendo acceso remoto a un punto final.</li> <li>▶ Realizar ataque de denegación de servicio distribuido (<i>DDoS</i>) con una demanda aleatoria básica.</li> </ul>	<ul style="list-style-type: none"> <li>▶ Realizar ataque de <i>spear phishing</i> utilizando un <i>malware</i> personalizado.</li> <li>▶ Aprovechar vulnerabilidades de "día cero" utilizando un código de <i>exploit</i> personalizado.</li> <li>▶ Plantar empleados deshonestos para realizar un reconocimiento y/o espionaje profundo.</li> <li>▶ Usar vendedores y/o proveedores como una forma de obtener acceso a la organización.</li> </ul>	<ul style="list-style-type: none"> <li>▶ Aprovechar vulnerabilidades en dispositivos inteligentes para obtener acceso a datos y/o sistemas de control.</li> <li>▶ Usar brechas de seguridad creadas con la convergencia de dispositivos personales y corporativos en una red.</li> <li>▶ Usar técnicas avanzadas para evitar detección y/o evadir la defensa.</li> </ul>



Todas las organizaciones deben asumir que podría pasar lo peor: no hay excusa para suponer lo contrario. Ha habido demasiados ataques conocidos a nivel mundial como para que la despreocupación sea aceptable.

Tomemos el ejemplo del ataque *ransomware Petya* que afectó a decenas de miles de empresas del sector público y privado de todo el mundo a finales de junio de 2017. El vendedor había lanzado un parche para la debilidad, pero las organizaciones que no aplicaron esta actualización, tal vez porque no entendieron cuál era la amenaza para ellas, quedaron expuestas al ataque.

El ataque Mirai, por el contrario, es más sofisticado y subraya las vulnerabilidades más amplias que las organizaciones deben comprender y abordar. Uno de esos ataques contra Dyn, proveedor DNS, detuvo el año pasado gran parte de Internet, interrumpiendo

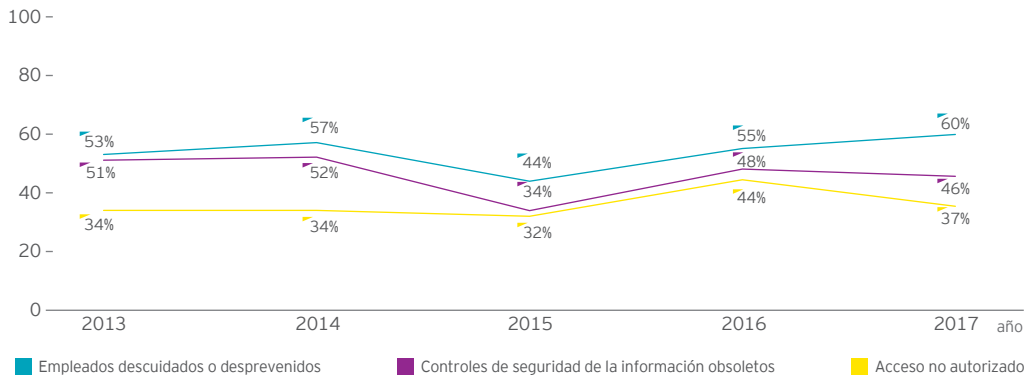
organizaciones como Twitter y Spotify,<sup>9</sup> entre otras. En ese ataque, Mirai apuntó a cámaras web no protegidas, pero también ha utilizado redes de cámaras CCTV, y en teoría podría apuntar a cualquier dispositivo inteligente que esté conectado a Internet. En este caso, la falta de comprensión o anticipación de la amenaza hizo que las organizaciones no se preocuparan en asegurarse de que las contraseñas de fábrica en todos los dispositivos inteligentes conectados a la red, se hayan actualizado.

Con tantas diferentes amenazas –y perpetradores, que podrían ser cualquiera, desde un empleador deshonesto hasta un grupo terrorista o un estado nación–, las organizaciones deben estar atentas en todos los ámbitos y estar bien familiarizadas con su propio panorama de amenazas. Sobre todo porque los atacantes tienen fácil acceso a los *malwares* y herramientas sofisticadas, e incluso pueden contratar ciberdelincuentes en línea.

## Amenazas y vulnerabilidades que han aumentado la exposición al riesgo de los encuestados, 2013-2017

### > Vulnerabilidades

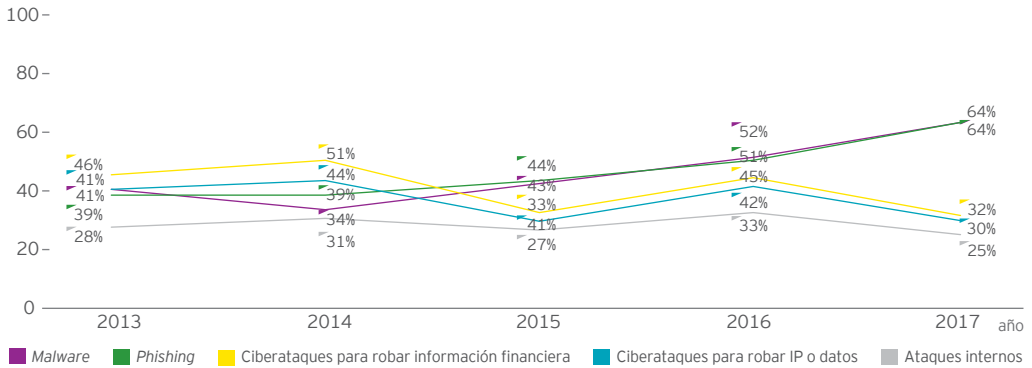
% de encuestados que indica lo siguiente como los principales elementos que aumentan la exposición al riesgo



9 "Corte de Internet afecta Twitter, Netflix, Paypal y muchas otras de las páginas web más visitadas," *The Independent*, 21 de octubre de 2016.

## > Amenazas

% de encuestados que indica lo siguiente como los principales elementos que aumentan la exposición al riesgo



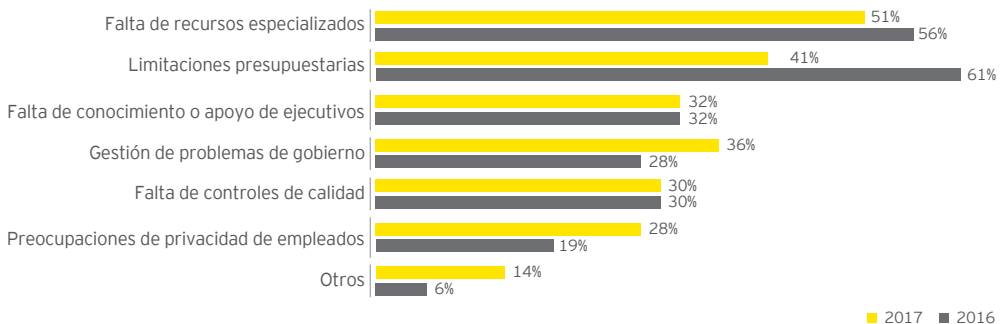
El gráfico anterior muestra cómo los empleados descuidados o desprevenidos aún son considerados un riesgo creciente, mientras que, curiosamente, el acceso no autorizado se ha reducido en gran medida como un riesgo percibido.

Los empleados y el crimen organizado son vistos como las mayores amenazas inmediatas. Para muchas organizaciones, el punto de debilidad más obvio vendrá de un empleado que es descuidado o deja de prestar atención a las pautas de ciberseguridad.

Las organizaciones también temen cada vez más a las vulnerabilidades dentro de los nuevos canales y herramientas. Por ejemplo, 77% de los encuestados sienten preocupación por el mal conocimiento y comportamiento del usuario que los expone al riesgo a través de un dispositivo móvil; la pérdida de dicho dispositivo y la posibilidad de pérdida de información y una violación de la identidad son una preocupación para el 50%.

Mientras tanto, el IoT es la fuente de una amplia gama de amenazas que muchas organizaciones ahora están esforzándose por comprender mejor. El siguiente gráfico describe algunos de los problemas relacionados con la integración del IoT.

## > Obstáculos que ralentizan la adopción de dispositivos del IoT (varias respuestas posibles)



## Entender el problema para abordar el desafío correcto

La historia de Santa Elena ofrece una buena metáfora de cómo algunas organizaciones todavía van por el camino equivocado con respecto a sus esfuerzos de ciberseguridad. Durante mucho tiempo, a Santa Elena, una isla remota en el Océano Atlántico Sur, se podía llegar después de un largo y difícil viaje por mar. Por ello, sus habitantes quedaron encantados cuando en el 2016 se completó un proyecto de US\$370 millones para construir una pista de aterrizaje. Lamentablemente, las aerolíneas comerciales inicialmente se negaron a utilizar la pista, la cual fue construida en el borde de un acantilado casi vertical de más de 300 metros, entre dos afloramientos rocosos que canalizan un viento feroz. Los pilotos advirtieron que era demasiado peligroso intentar un aterrizaje seguro.

El problema aquí es que aquellos detrás del proyecto se enfocaron en el problema equivocado: la falta de una pista en la isla. Ellos debieron haber pensado en la falta de un lugar seguro para aterrizar.

La aplicación de este ejemplo en la ciberseguridad es que mientras todas las organizaciones discuten sobre seguridad cibernética en sus salas de Comité, y a menudo hacen grandes inversiones, no siempre resulta claro qué problema están resolviendo. ¿Están enfocados simplemente en agregar más tecnología de ciberseguridad o en resolver la falta de resiliencia cibernética?

Claramente, este último debería ser el objetivo, pero para llegar allí, la organización necesita entender la relación entre resiliencia cibernética y los objetivos del negocio, así como la naturaleza de los riesgos a los que se enfrenta y el estado de la protección actual. Asimismo, debe evaluar cuánto riesgo está preparado para tomar, y definir cuál sería una pérdida aceptable. Solo cuando se hayan tomado estos pasos, la organización podrá hacer inversiones específicas y rentables en ciberseguridad.

Afortunadamente, los vuelos comerciales comenzaron en Santa Elena en octubre de 2017, y también estamos viendo que más Comités discuten y entienden sus riesgo cibernético así como la resiliencia cibernética deseada antes de asignar el presupuesto de ciberseguridad.

## > Sección 3

# Defendiéndose contra las amenazas

Es probable que las organizaciones se enfrenten a una ola de atacantes con distintos niveles de sofisticación, en donde deberán defenderse. La respuesta debe ser de varias capas: debe estar enfocada en repeler las amenazas o los ataques más comunes contra los cuales la organización se sienta más segura de defenderse, pero también debe ser consciente de que es necesario un enfoque más específico para lidiar con tipos de ataque avanzados y emergentes. Dado que algunos de estos ataques inevitablemente abrirán una brecha en las defensas de la organización, la atención debe estar en la rapidez con que se detectan y la eficacia con que se manejan.

## Defendiéndose contra los ataques más comunes

Las organizaciones deberían pensar en términos de cerrar la puerta a los tipos de ataque más comunes. Según Greg Young, Vicepresidente de Investigación de Gartner, "hasta el 2020, 99% de las vulnerabilidades aprovechadas continuarán siendo las que los profesionales de seguridad y TI ya habrán conocido por al menos un año"<sup>10</sup>. Por lo tanto, identificar y eliminar estas vulnerabilidades en su organización antes de que sean aprovechadas es crucial. De hecho, con una buena estrategia de ciberseguridad implementada

<sup>10</sup> "Cómo abordar amenazas en el actual panorama de seguridad", <https://www.gartner.com/smarterwithgartner/how-to-address-threats-in-todays-security-landscape/>, Gartner, 9 de mayo de 2017.

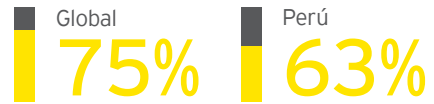
-incluso si esto es más fácil decirlo que hacerlo, debería ser posible evitar una proporción considerable de ataques comunes. En los próximos años, reparar las vulnerabilidades conocidas y eliminar las vulnerabilidades del servidor web podrían ser las acciones con mayor impacto para aumentar su ciberseguridad.

En este nivel de amenaza, las soluciones puntuales siguen siendo un elemento clave de resiliencia de ciberseguridad, con herramientas que incluyen *software* antivirus, detección de intrusos y sistemas de protección (IDS e IPS), gestión de parches compatibles y tecnologías de cifrado que protegen la integridad de los datos incluso si un atacante logra tener acceso a ella. La concientización de los empleados es también una importante defensa de primera línea, que desarrolla la percepción de la ciberseguridad y la disciplina de las contraseñas en toda la organización. Como los encuestados señalan, los comportamientos descuidados de los empleados representan un punto importante de debilidad para la mayoría de las organizaciones, así que abordar esta debilidad es vital.

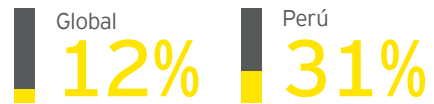
La madurez del enfoque de ciberseguridad de una organización determinará su efectividad. En la encuesta de este año, de todos los procesos de gestión de ciberseguridad discutidos, tres áreas se correlacionaron de manera especialmente estrecha con la confianza de las organizaciones en la detección de un ciberataque: privacidad, monitoreo de seguridad y gestión de terceros. Sin embargo, muchas organizaciones tienen serias dudas sobre la madurez actual de sus sistemas de ciberseguridad.

Para defenderse contra las amenazas comunes, las organizaciones deben asegurarse de que se hayan implementado lo básico que consta de 5 características estratégicas:

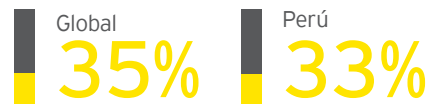
1. Centrada en el talento
2. Estratégica e innovadora
3. Enfocada en el riesgo
4. Inteligente y ágil
5. Resiliente y escalable



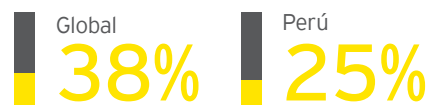
de los encuestados califican la madurez de su identificación de vulnerabilidades de baja a moderada



no tiene instalado un programa de detección de brechas



describe sus políticas de protección de datos como *ad-hoc* o inexistentes



no tiene programa de identidad o acceso o no han aprobado el programa formalmente

## Componentes requeridos para lograr la resiliencia de ciberseguridad

El constante cambio en un mundo cada vez más digitalizado, ha llevado a la convergencia de diferentes disciplinas de riesgo que se complementan entre sí para satisfacer las necesidades de sus clientes, reguladores y socios de negocio.

Colocar la ciberseguridad en el centro de la estrategia de una organización ayudará a mantener, e incluso mejorar, la confianza de los clientes, las entidades reguladoras y los medios. Para empezar, las altas gerencias ya no pueden asumir que la ciberseguridad es responsabilidad exclusiva del departamento de seguridad de la información o del departamento de tecnología de la información (TI). En cambio, las organizaciones deben hacer de la seguridad cibernética una parte central de la estrategia y cultura empresarial. Al hacerlo, pueden permitir a toda la organización comprender los riesgos que enfrentan, abrazar la innovación necesaria para contrarrestar esos riesgos. Tener la resiliencia para reagruparse y restaurar operaciones sin problemas y de manera eficiente ante una brecha cibernética.

Las organizaciones necesitan una visión de ciberseguridad integrada, que reúna las diversas funciones y dependencias con otras partes de la organización, con partes interesadas clave y con proveedores externos.



## Defendiéndose contra ataques avanzados

Si las organizaciones son lo suficientemente ambiciosas como para tratar de cerrar la puerta a tipos comunes de ataque cibernético, también deben ser lo suficientemente realistas como para aceptar que los atacantes avanzados lograrán ingresar en algún momento. En ese caso, es crucial poder identificar las intrusiones lo más rápido posible, y tener procesos que ciertamente proporcionen a la organización un medio efectivo para lidiar con la situación posterior a la brecha y poder expulsar a los atacantes.

Un Centro de Operaciones de Seguridad (SOC, por sus siglas en inglés) que se encuentre en la capacidad de detección de ciberamenazas de la organización es un excelente punto de partida, y proporciona un centro estructurado, coordinado y centralizado para todas las actividades de ciberseguridad. Los SOC son cada vez más comunes, pero 48% de los encuestados aún no cuenta con uno.

Esto no significa que un SOC tenga que desarrollar capacidades para todos los posibles aspectos de la estrategia y la práctica de ciberseguridad. Muchas organizaciones optan por externalizar algunas actividades en lugar de confiarlas al SOC interno: por ejemplo, 41% de los encuestados externalizó las pruebas de penetración, mientras 37% externaliza el monitoreo de la red en tiempo real.

Sin embargo, un SOC debe tener los medios para asegurar que puede mantenerse al tanto de las amenazas más recientes: los recursos de código abierto y de pago pueden proporcionar inteligencia valiosa, y 36% de los encuestados señala que su SOC colabora y comparte datos con pares de la industria.

Además, los SOC están pasando cada vez más frecuentemente de las prácticas de seguridad cibernética pasiva a la defensa activa: una campaña deliberadamente planificada y continuamente ejecutada busca identificar y eliminar atacantes ocultos y derrotar posibles escenarios de amenazas dirigidos a los activos más importantes de la organización. La defensa activa representa un avance crucial, ya que las organizaciones buscan contrarrestar a los atacantes avanzados, y puede considerarse como una estrategia que abarca al menos cuatro etapas:

### 1 | Priorizar lo más importante

En cualquier organización, ciertos activos, incluidas las personas, son particularmente valiosos y deben identificarse y protegerse de forma especial. Estos activos pueden estar relacionados con funciones comerciales importantes o bancos de datos particularmente confidenciales.

### 2 | Definir lo normal

Dado que la defensa activa depende de herramientas tales como el análisis de anomalías, es importante que las organizaciones comprendan cómo funcionan normalmente sus redes. Las herramientas de análisis de ciberseguridad utilizan el aprendizaje automático para definir lo "normal" y la inteligencia artificial para reconocer la potencial actividad maliciosa de forma más rápida y precisa.



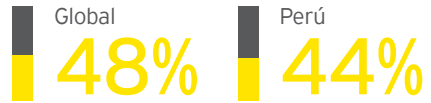
### 3 Inteligencia avanzada contra amenazas

Al trabajar estrechamente con proveedores de inteligencia de amenazas y desarrollar la capacidad de analistas internos, es posible que las organizaciones creen una imagen mucho más clara del panorama de amenazas, incluidas las identidades de los altos ejecutivos. Actualmente, sin embargo, 57% tiene muy poca gestión de inteligencia sobre las ciberamenazas.

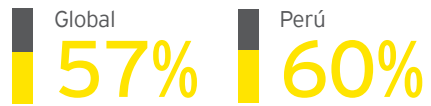
### 4 Misiones de defensa activa

Se trata de ejercicios planificados y ejecutados para vencer de forma proactiva escenarios de amenazas específicas y descubrir intrusos ocultos en la red. Requiere capacitación y pruebas personalizadas; por ejemplo, pruebas de *spear phishing* que identifican qué tan vulnerables son los empleados a las estafas de correo electrónico, pruebas de penetración que identifican las vulnerabilidades de la red, e incluso pruebas de equipo rojo a gran escala.

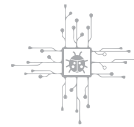
El empleo de estas estrategias puede aumentar la resiliencia cibernética de la organización y también reducir el “tiempo de permanencia” de la amenaza: la cantidad de tiempo que un atacante puede permanecer en el sistema sin ser detectado. Esto es crucial: solo 12% de los encuestados dice que es muy probable que detecten un ataque cibernético sofisticado dirigido a su organización. Entre las organizaciones que han experimentado algún incidente de seguridad cibernética, casi un tercio dice que el problema fue descubierto por su SOC.



de los encuestados no tiene un SOC



no tiene un programa de inteligencia de amenazas, o solo tiene uno informal



siente que es muy probable que detecten un ataque cibernético sofisticado

## No sea ingenuo con los edificios inteligentes

Los edificios de las organizaciones representan cada vez más una gran vulnerabilidad de ciberseguridad: el IoT y los avances en las tecnologías operativas pueden apuntar a una nueva generación de edificios inteligentes, pero también ofrecer a los atacantes cibernéticos un atractivo nuevo punto de entrada.

La naturaleza de la amenaza es amplia. Los atacantes pueden violentar los sistemas de control del edificio, poniendo en peligro la seguridad con ataques a los sistemas de protección contra incendios o los controles del elevador. Por ejemplo, incluso un breve apagado del sistema de aire acondicionado podría causar un colapso en un centro de datos. Alternativamente, los atacantes pueden apuntar a los sistemas conectados del edificio como una entrada a los sistemas más amplios de la empresa, por medio de enlaces remotos e interconectividad.

El alcance del daño de tales ataques es enorme. Se extiende desde la posibilidad de interrupciones del sistema hasta una fuga de datos a gran escala. Un *ransomware* puede volver inutilizable un edificio por un período. Las organizaciones en industrias reguladas, incluidos los servicios financieros, la salud y el sector público, pueden estar expuestas a sanciones de las autoridades pertinentes. El daño reputacional es muy probable. Las responsabilidades legales de los propietarios frente a sus inquilinos en tales eventos aún no se han analizado por completo. En un edificio como un hospital, la vida de las personas podría incluso estar en peligro.

Sin embargo, a pesar de estos riesgos, las organizaciones apenas están empezando a comprender las implicancias de ciberseguridad de su patrimonio físico. Hacerlo no es sencillo: muchas de las tecnologías operativas instaladas en los negocios se encuentran fuera de la función de TI, donde es más probable que la seguridad cibernética esté presente. A menudo se han agregado las conexiones poco a poco durante muchos años, añadiendo la funcionalidad de Internet a los sistemas históricos progresivamente, sin que una sola función o persona mantenga una visión general de todo el edificio; y gran parte de la conectividad agregada en años pasados tendrá poca o ninguna seguridad incorporada.

Los edificios inteligentes, en otras palabras, no son tan inteligentes desde la perspectiva de la ciberseguridad. Las últimas tecnologías, desde sistemas de iluminación inteligentes hasta controles de estacionamiento en garajes, pueden diseñarse e instalarse teniendo en cuenta la ciberseguridad, pero se están agregando a sistemas ya vulnerables.

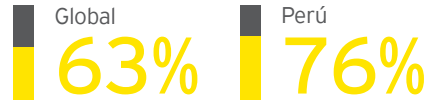
Las organizaciones ahora deben enfrentarse a este riesgo, identificando sus edificios más importantes -donde quizás residen sus activos más valiosos o sus sistemas más significativos para el negocio-, y trabajar rápidamente para mapear la conectividad con el fin de evaluar la ciberseguridad y mitigar el riesgo con las defensas adecuadas. Una vez que estos edificios prioritarios hayan sido protegidos, este enfoque debe extenderse al resto de la propiedad.

## Defendiéndose contra ataques emergentes

En la práctica, ninguna organización puede anticipar todas las amenazas que están surgiendo; la naturaleza de tales amenazas es que a menudo serán desconocidas, en cuyo caso, la puerta puede estar abierta a los perpetradores de dichos ataques. Sin embargo, las organizaciones innovadoras y capaces de ser imaginativas sobre la naturaleza de las posibles amenazas futuras, pueden generar agilidad en su ciberseguridad para poder avanzar rápidamente cuando llegue el momento. Además, las organizaciones con buenos procesos de gobierno que subyacen a su enfoque operativo pueden poner en práctica la seguridad por diseño, desarrollando sistemas y procesos capaces de responder a riesgos inesperados y peligros emergentes.

El estudio muestra que los presupuestos de ciberseguridad son más altos en organizaciones que:

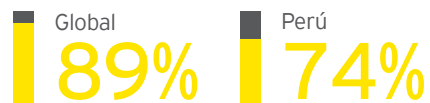
- ▶ Colocan oficiales de seguridad especiales en líneas de negocios clave.
- ▶ Envían informes sobre ciberseguridad al Comité y al Comité de auditoría al menos dos veces al año.
- ▶ Identifican específicamente los activos más importantes para la organización (no TI) y los protegen diferencialmente.



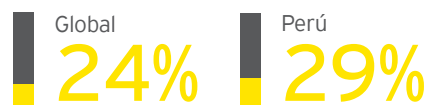
de las organizaciones aún tiene una función de ciberseguridad que reporta a TI



le reporta al Comité regularmente



afirma que la función de ciberseguridad no cumple plenamente las necesidades de su organización



Comenta que el responsable de la ciberseguridad participa en su Comité

Para mejorar las posibilidades de defenderse contra los atacantes cibernéticos, las organizaciones tendrán que superar las barreras que actualmente dificultan que las operaciones de ciberseguridad agreguen valor. Por ejemplo, 59% de los encuestados menciona limitaciones presupuestarias, mientras que 58% lamenta la falta de recursos especializados, y 29% se queja de la falta de conocimiento o apoyo de los ejecutivos.



de los Comités tiene suficiente conocimiento de seguridad de la información para evaluar plenamente la efectividad de los riesgos que la organización está afrontando y las medidas que se están tomando.



## Ciberseguridad para la seguridad vial

El automóvil conectado ya es una realidad. La constante evolución del sector automotriz hacia vehículos cada vez más autónomos depende de las tecnologías operativas que brindan acceso remoto a sistemas de vehículos, las cuales van desde la navegación hasta los controles de seguridad básicos. Además, los principales fabricantes ahora ven la tecnología de programación inalámbrica como la opción predeterminada para mantener, reparar y actualizar los vehículos que ya se vendieron a los conductores. Esas actualizaciones abarcarán todos los aspectos del vehículo, desde información y entretenimiento, hasta telemática y unidades de control.

En este contexto -el rápido cambio de redes cerradas a abiertas que rigen el comportamiento y el rendimiento de los vehículos-, la ciberseguridad es una consideración crucial. Los riesgos generados por atacantes cibernéticos capaces de tomar el control de un vehículo a través de una conectividad poco protegida no podrían ser más graves. Un atacante tiene la capacidad de poner en riesgo la vida de los habitantes del vehículo y de otros usuarios de la carretera, incluso de convertir el vehículo en una arma para apuntar deliberadamente a otros.

Sin embargo, así como muchos otros aspectos de las tecnologías operativas y las aplicaciones del IoT, se están desarrollando tecnologías de cuidado conectado. La madurez de tomar en cuenta los riesgos cibernéticos y su mitigación está creciendo. Los innovadores que han hecho ese buen trabajo en tantas áreas de la tecnología automotriz necesitan ganar aún más experiencia práctica para enfrentar amenazas cibernéticas.

Cada vez más, los Fabricantes de Equipos Originales (OEM, por sus siglas en inglés) entienden este problema y están priorizando la ciberseguridad, y están intentando integrar la ciberseguridad en los proveedores de componentes.

Se está haciendo un gran esfuerzo para cerrar esta brecha en el sector automotriz, y se está progresando. El deseo de innovar y desplegar nuevas tecnologías debe ser moderado por la comprensión de las vulnerabilidades de ciberseguridad que pueden crear, especialmente en las empresas automotrices tradicionales que ahora están redefiniendo sus procesos de diseño para una nueva generación de vehículos inteligentes. Esto requiere mayores niveles de cooperación y colaboración entre los innovadores y los expertos en ciberseguridad, incorporando desde el inicio conceptos como privacidad y seguridad por diseño.

## > Sección 4

---

# Servicio de emergencia: respondiendo a un ataque

Las organizaciones serán prudentes si operan sobre la base de que solo es cuestión de tiempo antes de que sufran un ataque, el cual abrirá con éxito una brecha en sus defensas. Tener un Plan de Respuesta a la Brecha Cibernética (PRBC) que se active automáticamente cuando se identifique la brecha, es la mejor oportunidad de una organización para minimizar el impacto. Pero un PRBC debe abarcar toda la organización y debe ser dirigido por alguien con la experiencia y el conocimiento para gestionar la respuesta operativa y estratégica de la organización.

El marco del PRBC abarcará:



## Ciberseguridad

¿Cómo se asegurará la organización de resistir el ataque, aislar y evaluar el daño infligido, y respaldar las defensas para evitar brechas similares en el futuro?



## Planificación de la continuidad del negocio

¿Cómo continuará operando normalmente la organización mientras se resuelve el ataque?



## Cumplimiento

¿Cuáles son los deberes de la organización para informar sobre la brecha a las autoridades correspondientes, incluidas agencias de seguridad y cómo se cumplirán?



## Seguro

¿La organización tiene un seguro cibernético y este incidente está cubierto? En ese caso, ¿qué se puede reclamar?



## Relaciones públicas y comunicaciones

¿Cómo se comunicará la organización de forma clara y efectiva con todas las partes interesadas, incluidos empleados, clientes, proveedores e inversionistas, tanto directamente como a través de los medios de comunicación?



## Litigio

¿Cómo evaluará la organización a qué potencial litigio la deja vulnerable el ataque, o incluso si recurre a la acción legal? ¿Cómo registrará y mantendrá legalmente la evidencia para uso de las agencias de seguridad?



de los encuestados no tiene implementado un plan o estrategia de comunicaciones en caso de un ataque significativo



haría una declaración pública a los medios dentro del mes en que se produzca una brecha que comprometa información



En la práctica, el PRBC es efectivamente un plan de gestión de crisis. Se requiere proporcionar orientación a cada función de la organización involucrada en la respuesta, establecer un nivel de entendimiento sobre qué información es importante que conozcan los altos ejecutivos –así como cuándo y cómo expresarla–, y respaldar la precisión y la velocidad de la reacción continua de la organización mientras la brecha continúe desarrollándose posiblemente durante días, semanas o incluso meses.

Esta encuesta sugiere diferentes niveles de preparación entre las organizaciones. Muchas organizaciones pueden estar confundidas sobre sus responsabilidades legales; 17% de los encuestados dice que no notificarían a todos los clientes, incluso si la brecha afectara la información del cliente; 10% ni siquiera notificaría a los clientes afectados. Dado que el Reglamento General de Protección de Datos de la Unión Europea ocupa un lugar preponderante, dichas posturas no serán justificables.

En general, mientras que 69% de los encuestados tiene alguna forma de capacidad formal de respuesta a incidentes, solo 8% describe su plan como uno robusto que abarca terceros y la aplicación de la ley.



## Lidiando con la nube y la convergencia

El pensamiento tradicional sobre las estructuras de TI parece cada vez más obsoleto: un gran número de organizaciones ahora depende de infraestructura de TI, tanto *software* como *hardware*, que está alojada de forma remota en la nube y no en las mismas instalaciones. Asimismo, la distinción entre TI y las tecnologías de operación (TO) está desapareciendo rápidamente a medida que las organizaciones vinculan las dos. La convergencia y la conectividad se han convertido en la norma.

Hay buenas razones para esto. En el entorno virtual de la nube, no hay restricciones de límites físicos para los usuarios, y la infraestructura se adapta y escala fácilmente. La conexión entre TI y TO puede impulsar procesos de extremo a extremo que transforman la productividad en cada área de la organización.

Sin embargo, estos temas presentan un problema de ciberseguridad. Dado que las organizaciones mantienen estructuras virtuales compuestas por entidades múltiples, ninguna configuración puede ser más segura que su enlace más débil, y cada vez hay más enlaces que proteger. Un ataque a un enlace, además, se convierte rápidamente en un ataque contra toda la organización. Las organizaciones ahora deben comprender esta realidad y tomar medidas para mitigar los riesgos generados. En particular, el concepto de zonificación es crucial aquí: inevitablemente, en una gran red de sistemas conectados, algunas áreas serán más vulnerables que otras, y algunas contendrán activos y sistemas más valiosos. Identificar y luego proteger estas zonas con seguridad mejorada debe ser una prioridad.

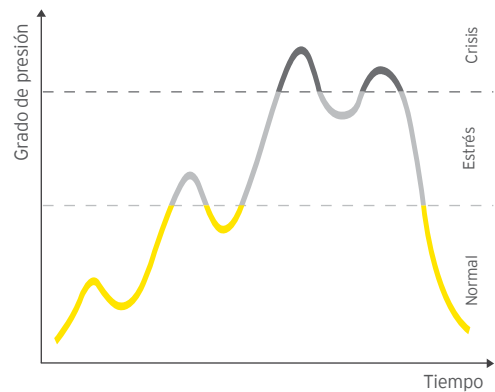
El objetivo es construir *firebreaks* entre diferentes áreas de la red para garantizar que la convergencia dentro de la organización no proporcione conveniencia a los atacantes cibernéticos. El hecho de que un atacante sea capaz de penetrar en una zona no significa que el acceso a todas las demás zonas sea sencillo, y en particular que no exista riesgo adicional de comprometer a áreas de alto valor.

# > Conclusión

En ediciones anteriores de esta encuesta, se ha resaltado la necesidad de estructurar la resiliencia de ciberseguridad en torno a los principios de detectar, proteger y reaccionar. Estos imperativos son más importantes que nunca: las organizaciones que entiendan el panorama de amenazas y que cuenten con fuertes defensas, tendrán más posibilidades de repeler ataques e identificar a los atacantes que logren ingresar; aquellas con la capacidad de defenderse limitarán el daño que puedan hacer los atacantes actuando rápidamente.

Puede resultar útil pensar en seguridad cibernética en el contexto de la gestión de crisis. Como lo demuestra el cuadro, las organizaciones que enfrentan eventos o incidentes importantes deben manejar picos de presión a medida que los problemas aumentan los niveles de estrés y desencadenan una crisis a gran escala.<sup>11</sup>

## > El patrón de intensidad de una crisis



<sup>11</sup> "Informe sobre Cooperación y Gestión de Ciber crisis", European Union Agency for Network and Information Security, noviembre de 2014.



> Acciones que todas las organizaciones deberían considerar

Tipo de amenaza	Estrategia	Ejemplo de acciones
> Ataques comunes	Las organizaciones deben ser capaces de prevenir este tipo de ataques a través de un buen esquema de ciberseguridad básica.	<ul style="list-style-type: none"> <li>▶ <b>Establecer el gobierno y la organización:</b> comprender los impulsores clave del negocio y obtener el apoyo de los altos ejecutivos para un sólido programa de ciberseguridad; establecer roles y responsabilidades; acordar una estrategia; desarrollar políticas y normas; habilitar informes.</li> <li>▶ <b>Identificar lo que más importa:</b> mapear los objetivos, productos y servicios del negocio para respaldar personas, procesos, tecnología e infraestructura de datos, y clasificarlos por importancia para su negocio. Esto incluye la cadena de suministro y el ecosistema en la que opera: tanto los terceros que le suministran como a los que usted suministra.</li> <li>▶ <b>Comprender las amenazas:</b> comprender quién podría querer atacarlo, por qué y cómo podría llevar a cabo un ataque; enfocar sus esfuerzos en cómo responder a las amenazas más probables.</li> <li>▶ <b>Definir su apetito de riesgo:</b> comprender cuánto le costarían a su empresa los ciberataques más probables a través de una cuantificación simplificada del riesgo cibernético, junto con un marco de gestión del riesgo cibernético, lo cual forma parte de sus procesos generales de gestión del riesgo operacional; establecer su apetito al riesgo y los mecanismos de informe para garantizar que usted opera dentro de él.</li> </ul>

>>>

&gt;&gt;&gt;

Tipo de amenaza	Estrategia	Ejemplo de acciones
> Ataques comunes	Las organizaciones deben ser capaces de prevenir este tipo de ataques a través de un buen esquema de ciberseguridad básica.	<ul style="list-style-type: none"> <li>▶ <b>Enfocarse en la educación y la concientización:</b> establecer un programa de educación y concientización, garantizando que todos los empleados, proveedores y terceros puedan identificar un ciberataque y conozcan el papel que desempeñan en la defensa de su negocio.</li> <li>▶ <b>Implementar protecciones básicas:</b> proteger su negocio a nivel tecnológico mediante la implementación de protecciones básicas que incluyen configuración segura, administración de parches, <i>firewalls</i>, <i>antimalware</i>, controles de medios extraíbles, controles de acceso remoto y encriptación; establecer un programa de Gestión de Vulnerabilidades (VM, por sus siglas en inglés) que gestione las vulnerabilidades desde la identificación hasta la remediación; establecer un programa efectivo de Gestión de Acceso e Identidad (IAM, por sus siglas en inglés) para controlar el acceso a su información; enfocarse en la protección de datos y la privacidad (técnica y de cumplimiento), así como en la gestión de terceros que tienen acceso o control de sus datos.</li> </ul>
> Ataques avanzados	Las organizaciones deben evitar algunos de estos ataques, y deben enfocarse en su capacidad para detectar y responder a los ataques más sofisticados y peligrosos.	<ul style="list-style-type: none"> <li>▶ <b>Ser capaz de detectar un ataque:</b> establecer una capacidad de monitoreo de seguridad que pueda detectar un ataque a través de la supervisión en varios niveles dentro de su negocio; por ejemplo, un sistema básico mediante el cual se genera y se envía por correo electrónico una alerta cuando se detecta actividad sospechosa en un <i>firewall</i>, a través de un SOC 24x7x365 que monitoree redes, sistemas operativos, aplicaciones y usuarios finales.</li> <li>▶ <b>Prepararse para reaccionar:</b> establecer un equipo formal de gestión de incidentes cibernéticos que haya sido capacitado y esté siguiendo un plan documentado que se pruebe al menos una vez al año.</li> <li>▶ <b>Adoptar un enfoque basado en el riesgo para la resiliencia:</b> establecer planes de recuperación (incluidas copias de seguridad completas) para todos los procesos y tecnologías de apoyo según su importancia para la supervivencia del negocio.</li> <li>▶ <b>Implementar protecciones automáticas adicionales:</b> madurar las capacidades existentes (por ejemplo, automatizar los procesos de VM e IAM usando tecnología específica), además de implementar capacidades y tecnologías complementarias como Sistemas de Prevención de Intrusiones (IPS), Sistemas de Detección de Intrusiones (IDS), <i>Firewalls</i> de Aplicación Web (WAF) y Sistemas de Prevención de Pérdida de Datos (DLP).</li> </ul>

&gt;&gt;&gt;

>>>

Tipo de amenaza	Estrategia	Ejemplo de acciones
> Ataques avanzados	Las organizaciones deben evitar algunos de estos ataques, y deben enfocarse en su capacidad para detectar y responder a los ataques más sofisticados y peligrosos.	<ul style="list-style-type: none"> <li>▶ <b>Desafiar y probar regularmente:</b> llevar a cabo un ejercicio de simulación de incidentes cibernéticos para evaluar la capacidad de su gestión ejecutiva para manejar la respuesta a un ciberataque significativo; llevar a cabo un ejercicio inicial de equipo rojo (un ataque planificado, llevado a cabo por <i>hackers</i> profesionales éticos) para probar su capacidad técnica para detectar y responder a ataques sofisticados.</li> <li>▶ <b>Crear un ciclo de vida de gestión del riesgo cibernético:</b> reflexionar sobre todas las áreas de su programa de gestión del riesgo cibernético e identificar áreas para la mejora continua; repetir las evaluaciones de riesgo regularmente; considerar el cumplimiento de las regulaciones correspondientes.</li> </ul>
> Ataques emergentes	Las organizaciones necesitan comprender las amenazas emergentes y entender cómo deberían influenciar la toma de decisiones estratégicas, mientras realizan inversiones enfocadas en los controles de ciberseguridad.	<ul style="list-style-type: none"> <li>▶ <b>Desarrollar seguridad en el ciclo de vida del desarrollo:</b> garantizar que el riesgo cibernético esté considerado en todos los productos, servicios, emprendimientos comerciales nuevos, etc., completando evaluaciones de riesgos según sea necesario y gestionándolas dentro del apetito de riesgo acordado.</li> <li>▶ <b>Mejorar el monitoreo de amenazas:</b> usar la inteligencia de amenazas con visión de futuro para identificar y rastrear amenazas emergentes.</li> </ul>

Comprender el panorama de las amenazas -detectando los riesgos potenciales a la vista- es la base de una buena ciberseguridad. Permite a las organizaciones limitar el tiempo que pasan fuera de la normalidad, comprender cuándo y por qué han pasado hacia el estrés, y por lo tanto adelantarse al desarrollo de una crisis completa. Defenderse –protegiendo a la organización del riesgo cibernético– se fundamenta en esta base. Brinda a la organización las habilidades y la confianza para lidiar con el estrés y la crisis de manera más efectiva, con herramientas y procesos que proporcionan un marco para responder a los atacantes.

La capacidad de responder a un ataque – reaccionar rápida y efectivamente cuando se produce una brecha– es la pieza final del rompecabezas. Tal brecha, ya sea que comprometa datos o ataque los sistemas de

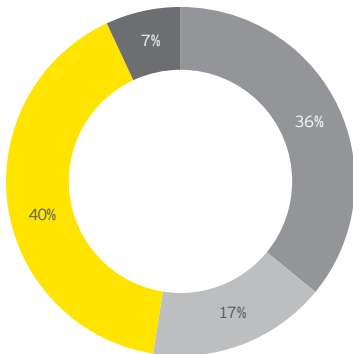
control de una organización, casi seguramente representará una crisis a gran escala. Pero las organizaciones capaces de actuar con calma, empleando un plan de respuesta a la brecha cibernética bien pensado y probado en el que todos entiendan sus responsabilidades, podrán reducir la escala de la crisis mucho más rápidamente.

Al unir estos aspectos de ciberseguridad, las organizaciones avanzarán hacia una mayor resiliencia, incluso ante el riesgo cada vez mayor que generan los diferentes y a menudo sofisticados ciberatacantes. Las herramientas y tecnologías requeridas para enfrentar la amenaza ya están disponibles y muchas organizaciones han desarrollado políticas y procesos innovadores para hacer mejor uso de ellas. Ahora, esta buena práctica debe convertirse en estándar para todas las organizaciones.

# > Metodología

La 20ª Encuesta Global de Seguridad de la Información de EY reúne las respuestas de casi 1200 altos ejecutivos y gerentes de seguridad de la información y tecnología de la información, los cuales representan a muchas de las organizaciones más grandes y reconocidas a nivel mundial. La investigación se realizó entre junio y septiembre de 2017.

## > Encuestados por área



- Europa, Medio Oriente, India y África
- Japón
- Américas
- Asia Pacífico

## > Encuestados por número de empleados

Menos de 500	30%
501-1,000	11%
1,001-2,000	12%
2,001-3,000	6%
3,001-4,000	5%
4,001-5,000	5%
5,001-8,000	7%
8,001-10,000	4%
10,001-15,000	5%
15,001-20,000	2%
20,001-30,000	4%
30,001-40,000	2%
40,001-50,000	1%
50,001-75,000	2%
75,001-100,000	1%
100,001-150,000	1%
Más de 150,000	1%



### > Encuestados por total de ingresos anuales (en USD)

Menos de 1 millón	■	4%
1 millón-5 millones	■	5%
5 millones-10 millones	■	3%
10 millones-50 millones	■	7%
50 millones-100 millones	■	6%
100 millones-500 millones	■	18%
500 millones-1 mil millones	■	12%
1 mil millones-1.5 mil millones	■	4%
1.5 mil millones-2 mil millones	■	5%
2 mil millones-5 mil millones	■	14%
5 mil millones-10 mil millones	■	8%
Más de 10 mil millones	■	14%

### > Encuestados por sector industrial

Banca y mercado de capitales	■	14%
Consumo masivo y <i>retail</i>	■	12%
Gobierno y sector público	■	7%
Seguros	■	7%
Automotriz y transporte	■	6%
Productos industriales diversos	■	6%
Tecnología	■	6%
Energía y servicios públicos	■	5%
Petróleo y gas	■	4%
Telecomunicaciones	■	4%
Bienes raíces	■	3%
Firmas y servicios profesionales	■	3%
Gestión de patrimonio y activos	■	3%
Medios de comunicación y entretenimiento	■	3%
Minería y metales	■	3%
Salud	■	3%
Ciencias de la vida	■	2%
Aeroespacial y defensa	■	1%
Químicos	■	1%
Otros	■	8%







Una visión integral  
para gestionar el  
riesgo cibernético



# > Ciberseguridad integral

---

Los ciberataques de hoy en día se están volviendo más numerosos, más frecuentes y, en la práctica, más amenazantes que nunca. La motivación de la nueva generación de atacantes no es solo robar fondos y secuestrar la información de las compañías; en su lugar, el objetivo puede ser infiltrarse y manipular no solo una empresa sino todo el ecosistema al que ésta pertenece.

Los riesgos cibernéticos se intensifican a medida que las empresas transforman sus operaciones mediante nuevos canales digitales, la automatización y otras tecnologías avanzadas.

Las compañías continúan destinando grandes inversiones a cerrar las brechas en sus marcos internos, en la red y digitales; debido a aquellos que quieren sacar provecho de esas debilidades; pues se están volviendo más inteligentes, hábiles y destructivos. En respuesta, las entidades reguladoras se están enfocando principalmente en manejar el riesgo cibernético sistémico y los posibles contagios entre organizaciones y terceros.



Las nuevas amenazas plantean serias preguntas sobre la preparación que tienen las organizaciones para recuperarse de una brecha. Según la Encuesta Global de Seguridad de la Información (GISS) 2017-2018, 6% de los encuestados piensa que su función de seguridad de la información satisface sus necesidades organizacionales. Para que la confianza aumente, la ciberseguridad debe ser responsabilidad de todos los empleados, ya que se extiende al ecosistema de los clientes, proveedores y vendedores de la organización.

Para negocios individuales, se necesita claramente una nueva estrategia para abordar la ciberseguridad. En EY, llamamos a un enfoque de gestión de riesgos de ciberseguridad integral, el cual debe incluir los recursos y las actividades de toda la organización.

Esta no es una tarea fácil pero se puede lograr si las compañías priorizan las siguientes cinco áreas: centrada en el talento, estratégica e innovadora, enfocada en riesgos, inteligente y ágil, resiliente y adaptable.

La ciberseguridad actual es más que solo proteger información y sistemas sensibles contra ataques externos: abarca proteger la identidad, la privacidad de datos y la gestión de vulnerabilidades a gran escala.

## > Sección 1

# Las 5 prioridades de la ciberseguridad



## 1. Centrada en el talento: generando consciencia sobre la ciberseguridad en los trabajadores

77% de los encuestados ven a los empleados como la mayor vulnerabilidad interna de ciberseguridad ya que -por lo general, son ellos quienes dan clic a un enlace y causan el problema-. Sin embargo, la realidad es que cada vez se hace más difícil diferenciar las fuentes de información legítimas de las ilegítimas.

Actualmente, hay una verdadera escasez de habilidades en ciberseguridad. Algunas estadísticas sugieren que habrá más de un millón de empleos de ciberseguridad desocupados en todo el mundo para el 2019.<sup>12</sup> Pero el problema

---

<sup>12</sup> "La falta de competencias en ciberseguridad vuelve a las compañías vulnerables," *Information Week*: [www.informationweek.com/strategic-cio/security-and-risk-strategy/cyber-security-skills-shortage-leaves-companies-vulnerable](http://www.informationweek.com/strategic-cio/security-and-risk-strategy/cyber-security-skills-shortage-leaves-companies-vulnerable).

es mucho más grande que la falta de expertos en ciberseguridad. En todos los niveles, no hay capacitaciones sobre cómo se debe manejar los riesgos cibernéticos cotidianamente en el negocio.

Las compañías necesitan incrementar las capacitaciones sobre conocimientos de ciberseguridad, pero también necesitan enseñar cómo los riesgos cibernéticos impactan en diferentes funciones y proyectos individuales, así como en el negocio en general.

En otras palabras, si las empresas quieren abordar los riesgos existenciales provocados por los riesgos cibernéticos, deben inculcar responsabilidad y acción frente a la ciberseguridad a nivel individual. Todos los empleados, desde los nuevos hasta los gerentes, deben darse cuenta de cómo un ciberataque puede mermar la confianza en la organización, y cuán dañinas y trascendentales pueden ser las consecuencias

## La cambiante función del CISO

Para alcanzar ese nivel de competencia en toda la compañía, los Comités van a necesitar informes sobre riesgos de ciberseguridad más audaces e integrales, así como informes que sean relevantes para el Comité.

Reestructurar la función del director de seguridad de la información (CISO, por sus siglas en inglés) es un paso importante. Al igual que las organizaciones necesitan integrar la ciberseguridad como parte de su estrategia de negocio, también necesitan expandir el alcance e influencia del CISO, el cual debería guiar toda la estrategia de ciberseguridad, y ayudar al Comité a entender y graduar su apetito al riesgo cibernético. Debe ayudar a comprender cuáles son los activos más importantes para asegurar y asesorar cómo destinar el dinero.

77% de los encuestados ven a los empleados como la mayor vulnerabilidad interna de ciberseguridad.

Además, debe asegurarse que la inversión se destine a las partes adecuadas del negocio, en equilibrio con el nivel de riesgo cibernético.

Algunas empresas con más experiencia en asuntos cibernéticos ya están haciendo esto. Están moviendo al CISO fuera de su línea jerárquica tradicional, pasando de reportar generalmente al director de sistemas de información (CIO) a reportar al director de riesgos (CRO). Esto manda la señal clara a toda la organización de que la ciberseguridad no es solo un asunto tecnológico.

El segundo cambio es que las funciones del CISO están comenzando a dividirse en dos, un reconocimiento tácito de la gran cantidad de trabajo constante que demanda la ciberseguridad. Una de las dos funciones emergentes es el reflejo del CISO tradicional: velar por el desarrollo y la ejecución de los proyectos de ciberseguridad. El segundo rol es nuevo y se enfoca en la estrategia, la política y el gobierno, así como también en la cooperación con entidades reguladoras externas.

Replantear el rol del CISO no solo tiene sentido en términos de estrategia, es gestión inteligente para una posición ejecutiva que se convierte en pararrayos cuando algo sale mal. Los CISO saben que cargarán con la culpa cuando ocurran brechas de ciberseguridad, pero si las compañías les brindan gran apoyo, financiamiento y compromiso, no solo la organización será más segura, sino también será posible retener la experiencia y pericia en el tema que el CISO desarrolla en su trabajo.

### ***Calls to action***

- Revise su actual modelo de organización y operación de riesgo cibernético y responda estas preguntas: ¿Cuál es la función y línea jerárquica del CISO?
- Use ejercicios de ingeniería social junto con capacitación (enfocada en todos los empleados, y capacitación específica para empleados de alto riesgo como ejecutivos y administradores de TI) para concientizar sobre las funciones individuales en la estrategias de ciberseguridad de la organización.
- Asegúrese de que se implemente un programa de gestión de identidad y acceso para limitar el acceso solo a los que lo necesitan, además de herramientas de monitoreo en tiempo real que permitan identificar comportamientos anormales rápidamente.



## 2. Estratégica e innovadora: integrando la ciberseguridad en la organización

La ciberseguridad debería ser tratada como otro riesgo operativo que debe enmarcarse en la gestión de riesgos de la organización. Los Comités ya discuten sin problema el riesgo de mercado, el riesgo de crédito y el riesgo operativo. Ha llegado la hora de considerar la ciberseguridad como otro riesgo no financiero que debe ser evaluado y cuestionado.

El aumento de la frecuencia y del alcance de los ciberataques, combinado con una nueva regulación en curso, ha provocado que algunas de las más grandes empresas del sector revisen sus ciberdefensas. 59% de los encuestados reveló que su presupuesto de ciberseguridad ha incrementado durante el año pasado. Sin embargo, esto es solo el comienzo de lo que el sector, en general, requiere.

Las compañías necesitan integrar la ciberseguridad en toda la estructura, estrategia y cultura corporativa para que todos los empleados (hasta los contratistas) participen activamente en la defensa del negocio contra los ciberataques. Esto comienza con un Comité que incorpore una estrategia cibernética que tome en consideración la amplitud del negocio. Frecuentemente, los Comités tienen un panorama limitado en cuanto a ciberseguridad, y destinan recursos a la seguridad perimetral y a programas de monitoreo,

sin considerar las implicaciones comerciales para las otras áreas, incluyendo la legal, la de cumplimiento regulatorio, la de servicio al cliente, y hasta la de marketing y comunicaciones corporativas.

Antes, puede que el área de TI se haya desvelado una noche protegiéndose contra una brecha cibernética, pero ahora estas amenazas tienen un efecto directo e inmediato en la reputación corporativa, las nuevas adquisiciones del negocio y la retención de clientes.

Tener a alguien en el Comité que esté informado sobre ciberseguridad y tenga una conexión directa con el director de riesgos y los comités de riesgo operativo debería ser, como mínimo, una de las buenas prácticas de esta nueva era cibernética. De esta forma, el Comité estará capacitado para tomar buenas decisiones sobre las necesidades de financiamiento del CISO y dónde se está gastando el dinero.

Actualmente, el CISO forma parte del Comité en 24% de las organizaciones, según los encuestados.

## > ¿Quiénes son las típicas partes interesadas en la ciberseguridad?

El público de la ciberseguridad es más grande y amplio que solo el CISO y debe ser integrado en diferentes partes de las organizaciones de nuestros clientes.



Fuente: "Quiénes son las típicas partes interesadas de la ciberseguridad" modelo de EY, 2017.

\*Cómo desarrollar ciberseguridad en estas transformaciones y cómo los riesgos cibernéticos las aceleran.

\*\*Cómo desarrollar ciberseguridad en la innovación y cómo la ciberseguridad debería seguir siendo innovadora.



## Innovación que mejora la seguridad

A medida que las organizaciones aumentan el ritmo en que adoptan y se integran a soluciones de tecnología financiera o *FinTech*, necesitan asegurarse de que su innovación tecnológica también se extienda a la infraestructura de ciberseguridad.

Integrar a las *FinTech* puede significar crear nuevas funciones disruptivas en las organizaciones existentes. Las “soluciones” *FinTech* que prometen optimizar y automatizar muchas partes del sector, sea la interacción frontal con el consumidor o las operaciones administrativas, aumentan los riesgos cibernéticos. Sin embargo, también pueden mejorar la seguridad, siempre que las compañías incluyan la estrategia de ciberseguridad en sus planes *FinTech* desde el comienzo.

Los macrodatos o *Big Data* jugarán un rol cada vez más importante, particularmente en la forma de analítica cibernética. Como lo sugiere su nombre, la analítica cibernética cubre el modelo estadístico que busca comportamiento anormal en conjuntos de macrodatos provenientes del lado del usuario final, de dentro de la red o de otras partes de la infraestructura de la TI.

La analítica cibernética a esta escala puede brindar un enfoque más inteligente y más informado para investigar cómo los ciberataques afectan los sistemas. Dar clic en un enlace en un correo de *spear phishing*, por ejemplo, puede descargar *malware* en la computadora e infectar la red de una organización. Ese *malware* desencadenará ciertos comportamientos en la red que son anormales. La analítica cibernética puede ayudar a los expertos a ubicar esas anomalías y reaccionar más rápido que las tradicionales defensas de marca o basadas en reglas.

La analítica cibernética puede brindar un enfoque más inteligente y más informado para investigar cómo los ciberataques afectan los sistemas.

El *blockchain* es mencionado usualmente como la próxima gran herramienta tecnológica que cambiará las reglas del juego para los negocios y los servicios financieros, en particular. Su conjunto integrado de cuentas y balances digitales, a través de una lista descentralizada de transacciones, ofrece una forma segura y transparente de proteger pagos digitales y la privacidad de datos. Potencialmente, las cuentas y balances del *blockchain* se pueden aplicar a todo, desde la gestión de acceso de identidad hasta funciones de auditoría y servicios TPRM.

La inteligencia artificial (IA) también podría ayudar a contrarrestar el cibercrimen. La agencia de investigación del Departamento de Defensa de los Estados Unidos (DARPA, por sus siglas en inglés) ha hecho experimentos con “*hackeo robótico*” para ver cómo es que computadoras conectadas se pueden defender de ciberataques.<sup>13</sup>

Un área donde la IA parece preparada para tener un impacto real es en el protocolo de intervención y respuesta o “área de reacción” de centros operacionales de seguridad. Actualmente, ese trabajo es hecho por personas, pero, como los atacantes hacen uso de la IA y así los ataques aumentan y mutan rápidamente, las compañías necesitarán su propia IA para contrarrestar esa amenaza. Los humanos no serán capaces de seguir el ritmo de ese volumen de datos que será la marca distintiva de estos ataques.

Se necesitará que se haga una transferencia de confianza y de toma de decisiones a la IA; esto representa un gran cambio para la actualidad, donde los humanos determinan si cierran un segmento de la red o cambian las configuraciones del *firewall* para evitar lo que parece ser un ataque en particular.

## **Calls to action: estratégicas e innovadoras**

- ▶ Implemente barreras que hagan que se tomen en cuenta y autoricen los riesgos cibernéticos desde el comienzo y en los puntos clave de todas las nuevas iniciativas comerciales; todo desde *FinTech* y desarrollo de nuevos productos hasta actividades de fusiones y adquisiciones (M&A).
- ▶ Considere fusionar la analítica cibernética con modelos existentes de centros operacionales de ciberseguridad para identificar brechas muy sofisticadas y difíciles de detectar.
- ▶ Revise regularmente las áreas que desarrollan robótica e IA, y busque oportunidades ventajosas para su experimentación en ambientes controlados.

<sup>13</sup> “Los hackers robóticos podrían ser el futuro de la ciberseguridad,” página web de *Scientific American*, agosto de 2016, [www.scientificamerican.com/article/robot-hackers-could-be-the-future-of-cybersecurity](http://www.scientificamerican.com/article/robot-hackers-could-be-the-future-of-cybersecurity).



### 3. Enfocada en el riesgo: priorizando lo esencial

La naturaleza rápidamente evolutiva del mundo de los riesgos cibernéticos hace que sea cada vez más importante que las compañías adopten un enfoque de ciberseguridad basado en riesgos. Las empresas simplemente no pueden protegerlo todo en la misma medida. Las prioridades importan.

El primer paso es corregir el gobierno de riesgos cibernéticos. Los Comités entienden que la ciberseguridad es un riesgo importante, tal vez incluso el riesgo número uno. Ellas saben que el riesgo cambia rápido y que es complicado seguirle el paso. Aún así tienen problemas para decidir cómo debería evolucionar ese gobierno. En la práctica, un conjunto más amplio de tendencias influirá en el futuro diseño de gobierno de riesgos cibernéticos. Estas incluyen nuevas leyes de privacidad y de datos, la implementación de la ciberseguridad de las 3LoD, la necesidad de desarrollar ciberseguridad en la innovación, y el cumplimiento de nuevas regulaciones y mayores expectativas de supervisión. Es importante realizar un análisis de estas tendencias para diseñar mejor la forma de gobierno.<sup>14</sup>

El enfoque de gestión del riesgo cibernético también es importante. Depender única o principalmente del equipo de ciberseguridad de primera línea ya no es aceptable. Ese grupo necesita ser dotado de buenos recursos, además de estar enfocado e integrado. Pero los líderes de negocios de primera línea tienen que asumir los riesgos cibernéticos, así como mantener y probar los controles que sean necesarios. Después de todo, ellos deberían asumir y manejar todos los riesgos relacionados con su negocio.



<sup>14</sup> *Gobernando riesgos cibernéticos en instituciones financieras*, EY, julio de 2017, [www.ey.com/gl/en/industries/financial-services/ey-governing-cyber-risks-financial-services](http://www.ey.com/gl/en/industries/financial-services/ey-governing-cyber-risks-financial-services).

## &gt; La función de la ciberseguridad de las 3 líneas de defensa (3LoD)

	¿Quiénes son?	¿Cuál es su rol en la ciberseguridad?	¿Cuál es su desafío?
> Primera línea	Unidades de negocio y equipos de seguridad de la información con responsabilidad directa para asumir, comprender y gestionar riesgos cibernéticos.	<ul style="list-style-type: none"> <li>▶ Medir, monitorear, gestionar y mitigar riesgos cibernéticos y vulnerabilidades dentro de la tolerancia aprobada por el Comité, si las unidades de primera línea están trabajando con equipos de seguridad de la información y equipos de ciberseguridad.</li> <li>▶ Definir los riesgos cibernéticos y exposiciones que enfrenta cada línea de negocio.</li> <li>▶ Preparar normas y procedimientos que complementen el marco de riesgos cibernéticos de la segunda línea en el contexto de riesgos de negocio específicos.</li> </ul>	<ul style="list-style-type: none"> <li>▶ Lograr que el pensamiento sobre ciberseguridad esté enmarcado en las operaciones diarias.</li> <li>▶ Lograr que la primera línea (no el equipo de ciberseguridad) identifique los riesgos cibernéticos correctamente, y desarrolle y mantenga controles sólidos.</li> </ul>
> Segunda línea	Gerentes de riesgos responsables de los riesgos cibernéticos de toda la empresa, con autoridad independiente para cuestionar, con eficacia, el enfoque de riesgos cibernéticos de la primera línea.	<ul style="list-style-type: none"> <li>▶ Desarrollar un marco de riesgos cibernéticos y cuestionar su implementación por parte de la primera línea.</li> <li>▶ Desarrollar el apetito al riesgo cibernético de la empresa y monitorear su cumplimiento.</li> <li>▶ Informar sobre los riesgos cibernéticos de toda la empresa.</li> </ul>	<ul style="list-style-type: none"> <li>▶ Desarrollar a profundidad un conjunto de métricas de ciberseguridad para toda la empresa.</li> <li>▶ Alinear el marco de gestión de riesgos cibernéticos con el de los riesgos generales.</li> <li>▶ Encontrar talento que sepa de riesgos y ciberseguridad.</li> </ul>
> Tercera línea	Equipo de auditoría interna que asegure todo el gobierno de riesgo cibernético de la empresa.	<ul style="list-style-type: none"> <li>▶ Auditar los elementos cibernéticos esenciales, ya sea como auditorías individuales (por ejemplo, en controles de acceso) o auditorías específicas correspondiente (por ejemplo, gestión de riesgos de los vendedores).</li> <li>▶ Evaluar el diseño general y la eficiencia operativa de la gestión de riesgos cibernéticos en la primera y segunda línea.</li> </ul>	<ul style="list-style-type: none"> <li>▶ Brindar conocimiento que mejore materialmente la calidad de los controles cibernéticos.</li> <li>▶ Determinar el mejor enfoque para evaluar el marco de riesgos cibernéticos de forma independiente.</li> </ul>

La función de riesgo de la segunda línea tiene que desarrollar sus capacidades. Los riesgos cibernéticos deben estar completamente considerados dentro del marco de apetito de riesgo de toda la empresa, de modo que el Comité apruebe formalmente su apetito de riesgo cibernético y monitoree que la empresa se mantenga dentro de esa tolerancia. El marco de la gestión de riesgos cibernéticos debe estar totalmente incorporado en un enfoque de gestión de riesgos más amplio, y estar bien alineado con los marcos de la TI, riesgos de seguridad y riesgos operativos.

La tercera línea (auditoría interna) necesitará un enfoque más sólido en la ciberseguridad, así como personal nuevo, o competencias obtenidas fuera y una perspectiva más independiente sobre qué tan bien el Comité, la primera línea y la segunda línea supervisan, evalúan y gestionan los riesgos cibernéticos.

Un desafío muy grande para las tres líneas es gestionar los riesgos cibernéticos asociados con terceros. Las entidades reguladoras insisten cada vez más en la supervisión permanente y detallada de terceros, particularmente, cuando se trata de ciberseguridad, resiliencia y protección de datos.

En esencia, es necesario un enfoque de 3 líneas de defensa totalmente funcional para la gestión de riesgos cibernéticos<sup>15</sup>. La industria se está moviendo rápidamente para adoptar esa estrategia integral. Al hacerlo, las empresas de servicios financieros ahora están teniendo que desarrollar su estrategia de talento cibernético, como ya se ha mencionado.

## Cuidando lo que es esencial

Al final, las empresas tienen que priorizar sus esfuerzos.

En primer lugar, tienen que identificar los procesos y activos del negocio que son más importantes para ellos, e implementar un enfoque diferenciado para protegerlos. Eso requiere que las empresas mapeen los procesos comerciales en aplicaciones e infraestructura, e incluyan flujos de datos y dependencias previas y posteriores. De esa forma, las empresas conocen el universo de lo que es esencial.

En segundo lugar, deben determinar cómo segmentarán o pondrán en cuarentena a los activos esenciales. Muchas veces, los ciberataques acceden a procesos esenciales a través de activos menos protegidos.

Finalmente, deben determinar los terceros que son esenciales para esos procesos. Los vendedores esenciales deben ser evaluados y monitoreados más rigurosamente. Si es posible, las empresas deberían tener vendedores alternativos a quienes llamar en caso de que los vendedores existentes sufran ciberataques, brechas cibernéticas o fallas tecnológicas materiales. La resiliencia cibernética se está convirtiendo en un asunto de gran trascendencia en la industria, por encima de los terceros.

<sup>15</sup> *Gestión de riesgos cibernéticos en las tres líneas de defensa*, EY, abril de 2017, [www.ey.com/Publication/vwLUAssets/ey-cyber-risk-management/\\$File/ey-cyber-risk-management.pdf](http://www.ey.com/Publication/vwLUAssets/ey-cyber-risk-management/$File/ey-cyber-risk-management.pdf).

## Un desafío regulador cada vez más grande

En respuesta a las crecientes amenazas cibernéticas específicamente en el sector de servicios financiero, las entidades reguladoras alrededor del mundo están ejerciendo presión para que más empresas se responsabilicen de la ciberseguridad, a través de regulaciones más severas y mayores expectativas de supervisión.

En líneas generales, la regulación cibernética cubre dos áreas principales: proteger la privacidad del consumidor y proteger el sistema de servicios financieros en general.

El Reglamento General de Protección de Datos de la UE (RGPD) se enfoca principalmente en la privacidad del consumidor, tal como lo sugiere su nombre. Exige que las empresas reporten brechas cibernéticas en cualquier parte de su ecosistema, incluyendo contratistas, vendedores externos y afiliados.

Los Estados Unidos está reforzando la regulación cibernética en una serie de aspectos. La Corporación Federal de Seguro de Depósitos (FDIC, por sus siglas en inglés), la Oficina del Contralor de la Moneda (OCC, por sus siglas en inglés) y el Comité de la Reserva Federal (FRB, por sus siglas en inglés) han propuesto normas más sólidas para el manejo de riesgos cibernéticos para las instituciones financieras. El periodo de observación para la Notificación Previa a la Propuesta de Reglamentación (ANPR, por sus siglas en inglés) se ha completado y la legislación propuesta está pendiente de notificación.

La ANPR está dirigida principalmente al riesgo sistemático al interior de las empresas y del sector en general. De hecho, su meta general es la de proteger todo el sistema financiero. Es considerada como el más significativo y exigente conjunto de normas relacionadas con

la ciberseguridad aplicadas a grandes compañías de servicios financieros que operan en Estados Unidos. Uno de sus puntos de referencia es que las empresas desarrollen y mantengan una estrategia de gestión de riesgos cibernéticos escrita, aprobada por el Comité e integrada en los planes estratégicos de toda la empresa. En resumen, la ANPR señala que la ciberseguridad es la parte central de la estrategia comercial y del ecosistema más amplio de servicios financieros, incluyendo terceros.

Otras entidades reguladoras también se están enfrentando al desafío cara a cara, incluyendo las autoridades monetarias de Singapur y Hong Kong. Otras regulaciones que se acercan rápidamente están relacionadas con la seguridad de la red y de la información y con los sistemas de pago.

La escala y alcance de las nuevas regulaciones de ciberseguridad que pronto estarán vigentes significan un claro desafío de cumplimiento para las compañías de servicios financieros, en particular porque una gran parte del mercado de servicios financieros consiste en organizaciones con presencia en el mercado global, o con clientes distribuidos en diferentes mercados. Estos actores globales van a tener que cumplir con las diferentes regulaciones alrededor del mundo.

### **Calls to action: enfocadas en el riesgo**

- ▶ Evalúe el gobierno de riesgos cibernéticos para determinar qué mejoras se necesitan para que el Comité tenga una mayor supervisión de los riesgos cibernéticos.
- ▶ Establezca una estrategia para implementar un enfoque de las 3LoD para la gestión de riesgos cibernéticos, con mayor énfasis en la articulación clara de las funciones y responsabilidad en toda y dentro de las tres líneas, y en los procesos, activos y vendedores esenciales del negocio.
- ▶ Desarrolle un enfoque de gestión de riesgos cibernéticos de segunda línea, desarrollado en torno a una declaración sobre el apetito de riesgo cibernético bien articulada y aprobada por el Comité, y respaldada por una métrica de riesgo cibernético precisa y oportuna.
- ▶ Establezca una competencia de cumplimiento de regulaciones cibernéticas que combine todos los requerimientos normativos competentes y concernientes; esto asegurará que la organización tenga un panorama completo de las actividades que involucrarán una o más regulaciones.

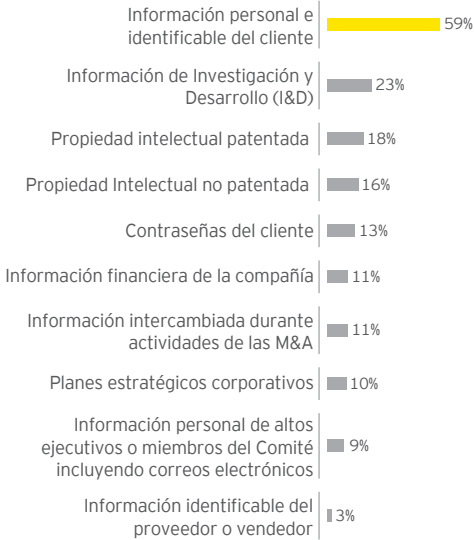


## 4. Inteligente y ágil: protegiendo lo esencial

Decidir lo que es esencial puede ser un reto para cualquier organización grande, particularmente porque los ataques son cada vez más sofisticados y las líneas de ataque cambian a diario. Diferentes partes del negocio pueden dar argumentos convincentes de por qué sus activos son fundamentales y deben ser protegidos. Sin embargo, la realidad dicta que ninguna organización puede protegerse completamente de un ciberataque. Eso significa que la pregunta real es: ¿cuál es el apetito al riesgo para proteger los activos esenciales? Esto dependerá tanto de la naturaleza de los propios activos lo cual determina su vulnerabilidad inherente y de las prioridades de la organización. Por ejemplo, puede ser mejor aceptar ciertos riesgos con el fin de asignar recursos a la gestión de la reputación.

Entonces, ¿cuáles son los activos críticos que son realmente importantes para su negocio? Para muchas empresas es la información de sus clientes; 59% de los encuestados dijo que la información personal e identificable de sus clientes era el activo más importante que debían proteger, mientras que un 13% mencionó las contraseñas de los clientes. Para otras compañías, podría ser la información financiera, los planes estratégicos corporativos, los datos personales relacionados con el Comité o la información sobre la actividad de las M&A.

> La información del cliente se considera el activo más valioso que debe protegerse



Fuente "La información del cliente es considerada con mucho el activo más valioso que debe protegerse", Encuesta Global de Seguridad de la Información de EY 2017-2018

Finalmente, a medida que las organizaciones buscan proteger lo esencial, deben sopesar el costo económico de un ciberataque. El impacto económico de los ataques e incidentes cibernéticos es casi siempre significativamente más alto que el valor nominal de la pérdida directa.

Esto se debe a que las pérdidas globales incluyen costos indirectos relacionados con la investigación y corrección del problema, daños a la reputación y pérdida de clientes, obligaciones legales, potenciales multas por incumplimiento normativo e impacto en el precio de las acciones. Las empresas pueden evaluar el valor de la resiliencia cibernética de su organización mediante herramientas económicas hechas a medida.

> ¿Cómo manejar el riesgo informático desde su hoja de balance?





Aplicar un modelo cibereconómico puede ayudar a identificar los activos más importantes que necesitan protección y a cuantificar la pérdida económica tras un ciberataque. Por ejemplo, ¿cuál sería la pérdida cuantificada para un banco si perdiera los datos de un millón de clientes, y esa pérdida se hiciera pública? Al emplear este modelo, usted puede planificar cómo el valor en riesgo comenzará a disminuir a medida que aumenta sus controles de defensa para prevenir los ataques correspondientes a esos escenarios de pérdida cibereconómica.

### ***Calls to action:*** **inteligentes y hábiles**

- Haga un inventario de sus activos y procesos clave para identificar cuáles son considerados fundamentales.
- Identifique quién los amenazaría, por qué y qué métodos de ataque implementarían; utilice esta inteligencia de amenazas de manera permanente para mejorar y mantener actualizadas sus evaluaciones de amenazas.
- Evalúe qué tan vulnerables son sus activos más importantes basándose en su análisis de amenazas, y enfóquese en el esfuerzo y la inversión al manejar estas vulnerabilidades.
- Desarrolle un modelo cibereconómico, incorporando sus evaluaciones de amenazas y vulnerabilidades, para identificar las potenciales pérdidas de dinero si sus activos esenciales son atacados con éxito (esto dará información sobre los presupuestos de inversión y el Comité tendrá un caso más cuantificado).



## 5. Resiliente y escalable: recuperándose y protegiendo el ecosistema

Si aceptamos que ser víctima de un ciberataque es inevitable, entonces se vuelve aún más importante para la organización tener sistemas y estrategias disponibles para restablecer el negocio de la manera más rápida posible. Aprender de lo que sucedió, y adaptar y remodelar la organización para optimizar el avance de la resiliencia cibernética.

Esto exige un Programa de Respuesta a Brechas Cibernéticas (PRBC) centralizado para toda la empresa que pueda unir a la amplia variedad de partes interesadas que deben colaborar para resolver una brecha. El PRBC necesita ser liderado por alguien que tenga experiencia en tecnología, y que sea capaz de manejar la respuesta operativa y táctica del día a día. Ese líder debería también contar con amplia experiencia en el ámbito legal y regulatorio, ya que cualquier brecha cibernética puede desencadenar problemas legales y normativos complejos con impacto en los estados financieros.

La crisis económica del 2008 destacó el grado al que el sector de servicios financieros está interconectado. Desde entonces, la red de conectividad ha incrementado, ya que las compañías han buscado tercerizar incluso más partes de su negocio. Actualmente, un banco global puede tener hasta 6 mil vendedores. Eso significa grandes desafíos al intentar asegurarse de que cada vendedor tenga los controles de ciberseguridad adecuados.

71% de los encuestados no incrementaría sus gastos en seguridad de la información, aunque un proveedor fuera atacado; a pesar que esta sea la ruta directa a la organización para el atacante.

Ahora las compañías necesitan respaldar todo su ecosistema de vendedores y socios con la misma intensidad que preparan a su fuerza laboral con herramientas y habilidades para protegerse frente a ciberataques.

Tener confianza en el ecosistema de la compañía requerirá de una estrategia de proveedores que, en primera instancia, puede parecer exageradamente cautelosa, pero que, de hecho, es fundamental dado que la mayor amenaza de la seguridad proviene a menudo de las conexiones de terceros. Las compañías de grandes y medianas han notado esto y han invertido tiempo priorizando a sus vendedores en los últimos años mediante una combinación de cuestionarios y evaluaciones remotas e *in situ*, además de revisiones.

Las empresas tendrán que seguir adoptando un enfoque adaptado a los riesgos para socios y proveedores, a los cuales deberá categorizar en base a una serie de criterios de riesgo que se alineen con la estrategia general de ciberseguridad. Los programas de inteligencia de amenazas pueden ayudar a las empresas a tener una mayor comprensión de las vulnerabilidades de los proveedores, mientras que las evaluaciones de riesgos de los vendedores deberán ser actualizadas y adecuadas para corregir todas las brechas de ciberseguridad que existen actualmente.

Adoptar una postura firme con los socios subcontratados es importante porque una gran parte de las actividades de una organización generalmente están en manos de terceros. ¿Realmente es el vendedor quien está procesando sus datos o ha tercerizado el servicio a otra compañía? ¿Está convencido de que está actuando de manera segura y que cuenta con un programa para asegurar que sus empleados estén protegiendo sus datos adecuadamente?

El proceso de evaluación de riesgos puede tener como consecuencia una reducción del número de vendedores en los que la empresa confía. De ser así, las empresas pueden incentivar el cumplimiento en sus proveedores y hacerlos más fáciles de monitorear en el futuro.

### **Calls to action: escalables y resilientes**

- ▶ Confirme que cuenta con un PRBC documentado que incluya a todas las partes interesadas (desde el Comité y altos ejecutivos hasta el área legal, de recursos humanos, de riesgos, de relaciones públicas, de comunicaciones, TI, unidades de negocio, etc.).
- ▶ Verifique que todas las partes interesadas hayan sido capacitadas en el plan, y lo más importante, que hayan participado en un simulacro de incidente cibernético, para cuestionar y evaluar su capacidad de respuesta.
- ▶ Reexamine el plan de comunicación de crisis y asegúrese de que no solo cubra partes interesadas externas clave, como organizaciones de seguridad, entidades regulatorias, clientes y medios de comunicación, sino también los diferentes escenarios en los que se necesita comunicación con las partes interesadas, logrando encontrar el balance correcto entre informar demasiado pronto y demasiado tarde.
- ▶ Implemente un programa centralizado de gestión de terceros en torno al registro de todos los terceros, incluyendo información sobre si un tercero administra sus datos o tiene accesos a sus sistemas. Si cuenta con la supervisión adecuada, incluyendo auditorías de ciberseguridad *in situ*, podrá entonces centrarse en los vendedores que representen mayor riesgo.

## > Sección 2

---

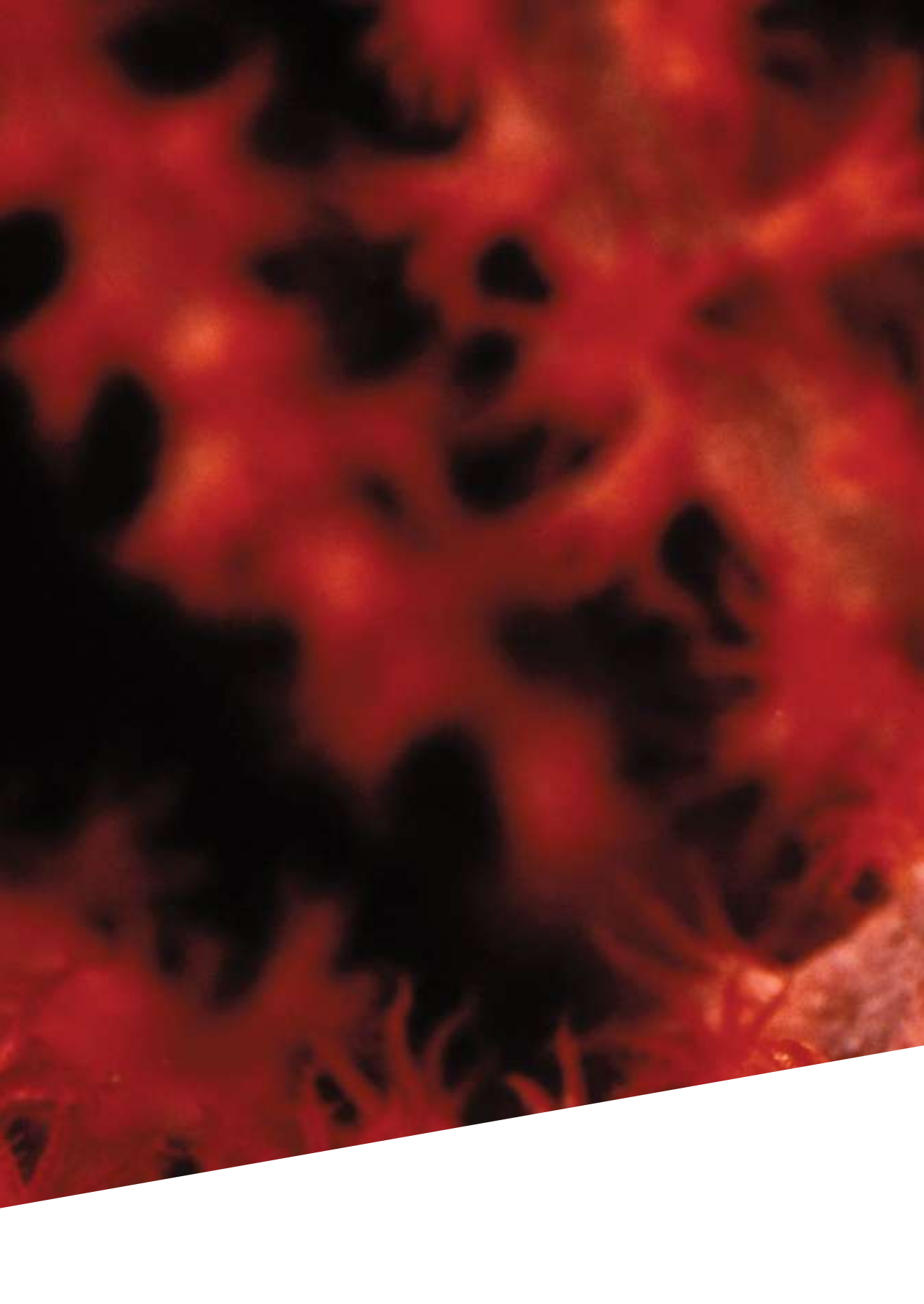
# 10 cosas que debe hacer ahora

Implementar un enfoque holístico orientado al negocio para combatir ciberataques puede resultar un poco abrumador cuando su organización ya está enfrentando una crisis en diferentes frentes.

Sin embargo, la ciberseguridad debe ser una prioridad en el negocio y una preocupación para todos los empleados en las organizaciones modernas.

**A continuación presentamos 10 cosas que usted puede hacer para que esto suceda:**

- 1 Integre la ciberseguridad a la estrategia de talento y cree una función de CISO que se adecúe al propósito de su organización.
- 2 Defina claramente las responsabilidades de ciberseguridad en su organización.
- 3 Coloque la ciberseguridad al frente de una estrategia de negocios multifuncional. No debe concebirse como un problema de la TI.
- 4 Asegúrese de que la ciberseguridad esté en el centro de la innovación digital y que represente una ayuda, no un obstáculo.
- 5 Observe el impacto que tiene la regulación en su negocio global, y trabaje con las entidades reguladoras, ya que estas también desean lograr un sólido sector.
- 6 Analice el riesgo de todos sus activos clave y determine un enfoque de protección para cada uno, poniendo énfasis en los más esenciales.
- 7 Desarrolle un modelo ágil y dinámico de gestión de riesgos cibernéticos para permitir que su organización se adapte si hay un incremento de riesgos externos o una decisión que cambiará el apetito al riesgo de la empresa.
- 8 Integre el cumplimiento regulatorio en su estrategia de ciberseguridad, de manera que toda inversión económica hecha en el cumplimiento devuelva valor al negocio al brindar una defensa adecuada para la organización.
- 9 Fortalezca la resiliencia con planes de acción y comunicación de crisis claros para cuando las cosas salgan mal, de manera que la gestión de crisis y de continuidad pueda ser analizada concienzudamente y practicada en todos los niveles de la organización.
- 10 Colabore con sus pares para buscar más soluciones intersectoriales. Los riesgos cibernéticos actuales amenazan todo el sistema, y el error de un actor clave podría perjudicar la reputación de toda una industria.





Gestión de riesgos  
cibernéticos en todas  
las líneas de defensa



# > Las líneas de defensa

---



¿Recuerda el tiempo en el que el robo de los números de las tarjetas de crédito era lo más sofisticado en crímenes cibernéticos? Ese tiempo ha quedado atrás. Actualmente, los ataques complejos y difíciles de detectar podrían traer abajo no solo a una empresa, sino también a grandes regiones del internet y los mercados financieros.

Por lo tanto, la ciberseguridad ya no es cuestión de evitar a los atacantes; ahora se trata de descubrir cómo manejar y adelantarse a estos intrusos que ya se encuentran dentro de la organización.

Los atacantes modernos normalmente no buscan resultados rápidos; ellos intentan infiltrarse sigilosamente en las redes de una organización para buscar puntos vulnerables, con el fin de esperar el momento oportuno para atacar a sus blancos o utilizar las conexiones confiables del servidor para infiltrarse en otras empresas desprevenidas. Usualmente, estos ataques duran varios meses o incluso años.





Las organizaciones deben hacer frente a estos criminales que están desarrollando continuamente nuevos métodos y técnicas para lograr sus objetivos. Algunas de las miles de motivaciones de estos criminales cibernéticos se relacionan con querer dañar la reputación o marcas de sus blancos u obtener información confidencial de los clientes para poner en riesgo o robar distintos tipos de activos, mientras que otras razones son más difíciles de determinar.

La reciente preocupación sobre las amenazas cibernéticas sistemáticas ha elevado la importancia de los riesgos cibernéticos en la agenda política y regulatoria. Después de algunos ataques cibernéticos recientes, la industria ha comenzado a considerar seriamente en el riesgo real de los atacantes cibernéticos y cómo pueden afectar los sistemas más grandes en vez de dañar solo empresas individuales. Un ataque de tal magnitud podría afectar considerablemente las transacciones financieras, parar mercados enteros y socavar la estabilidad y confianza en el sector.

Para estar seguros no solo se necesita evitar a los atacantes, sino adelantarse a ellos, pues ya se encuentran dentro de la misma organización.

Esto ha sido un llamado de atención para aplicar un mejor enfoque de manejo de riesgos cibernéticos, el cual no constituye la única preocupación de seguridad informática. Para este fin, las organizaciones se han embarcado en un viaje para implementar el modelo de “tres líneas de defensa” (3LoD) para manejar riesgos cibernéticos, el cual incluye lo siguiente:

**Primera línea:** Unidades de negocio y equipos de seguridad informática responsables directamente de identificar, comprender y manejar los riesgos cibernéticos.

**Segunda línea:** Gestores de riesgos responsables de los riesgos cibernéticos globales para toda la institución, quienes tienen autoridad independiente para cuestionar efectivamente el enfoque empleado por la primera línea para enfrentar riesgos cibernéticos.

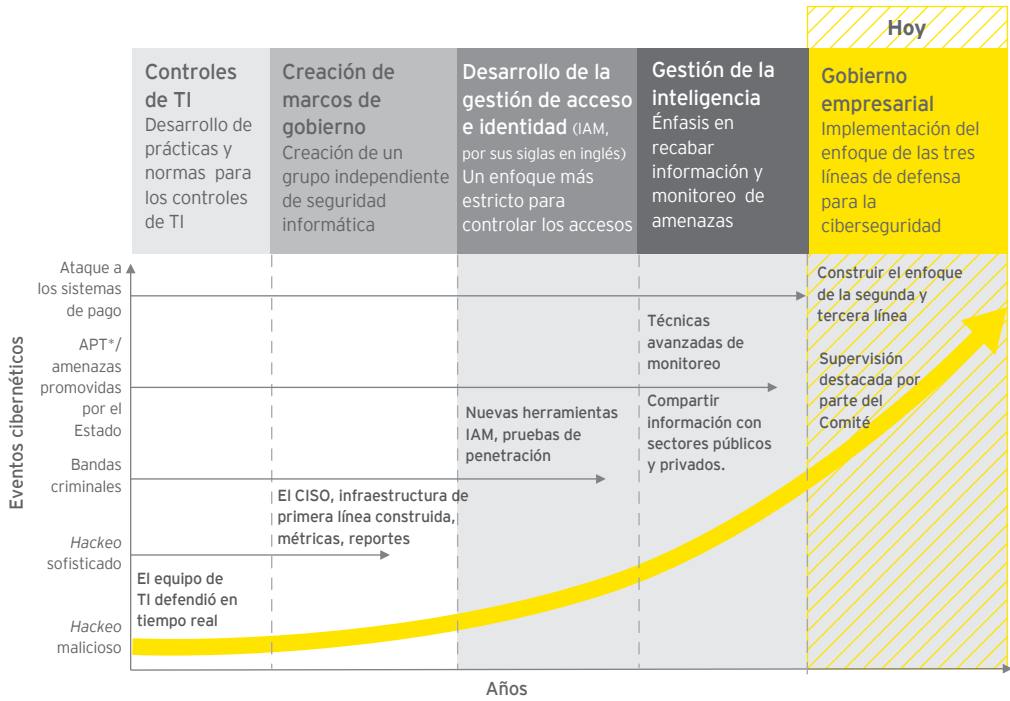
**Tercera línea:** Equipo de auditoría interna que asegure el gobierno de riesgos cibernéticos de la empresa.

Un Comité activo, calificado y comprometido guía estas tres líneas de defensa y aprueba y supervisa el enfoque de ciberseguridad de la empresa, mientras que logra un alineamiento al presentar un equilibrio efectivo y creíble para la gestión.

Un Comité activo,  
calificado y  
comprometido,  
guía estas tres  
líneas de defensa,  
aprueba y supervisa  
el enfoque de  
ciberseguridad de  
la empresa.



➤ Evolución de la gestión de riesgos cibernéticos



\*Amenazas avanzadas persistentes  
Fuente: EY



## > Sección 1

# Plan de acción para un gobierno de riesgos cibernéticos en toda la empresa

Establecer un enfoque de tres líneas de defensa para afrontar los riesgos cibernéticos no es una tarea sencilla. Las empresas aún tienen dificultades para decidir cuál es el mejor modelo de riesgos no financieros que deben implementar en sus negocios, por lo tanto, agregar el componente de gestión de riesgos cibernéticos al modelo de las 3LoD, implicaría un reto incluso mayor para las organizaciones.

Se conoce muy bien el concepto general; el problema es su implementación. Algunas de las preguntas frecuentes son las siguientes:

- ▶ Contar con responsables de primera línea para todos los riesgos tiene sentido, pero ¿qué se debe hacer para que los líderes tecnológicos y empresariales de primera línea cumplan con sus obligaciones relacionadas con los riesgos?

Estas nuevas responsabilidades implicarán una inversión significativa en recursos humanos y herramientas, incluyendo mejoras en las competencias de monitoreo y análisis para poder elaborar evaluaciones más precisas de los niveles de riesgo cibernético existentes.

- ▶ La supervisión de segunda línea de riesgos globales es importante sin lugar a duda, pero ¿cómo la segunda línea puede tomar este rol sin dar la impresión de que está despojando de su labor a la primera línea, sabiendo que la segunda línea está ahí?
- ▶ La seguridad de tercera línea actúa como un importante respaldo, pero ¿cómo la auditoría interna puede comprometerse lo suficiente para mejorar el gobierno de riesgos cibernéticos sin socavar su independencia?

Un factor clave de éxito será entender la función de cada línea y contar con una buena supervisión del Comité durante la implementación del modelo de las tres líneas de defensa para afrontar riesgos cibernéticos.



## Primera línea: fortalezca las competencias de la ciberseguridad y comience el negocio

Las unidades de primera línea que trabajan con la seguridad informática y los equipos de seguridad informática; deben medir, monitorear y mitigar los riesgos cibernéticos dentro de la tolerancia aprobada por el Comité.

Una primera línea fuerte de ciberseguridad requiere un esfuerzo significativo dentro de las líneas del negocio. Ya sea dentro de un banco comercial, banco de inversiones, banco corporativo, banco privado o cualquier otra área, las cabezas de las empresas deberán realizar un examen exhaustivo para determinar si su organización está dedicando todos los esfuerzos necesarios para manejar los riesgos cibernéticos. Los grupos de seguridad informática no pueden seguir dando las mismas soluciones para toda la empresa. Por el contrario, cada línea de negocio deberá definir cuidadosamente los riesgos cibernéticos y su exposición hacia ellos. Los riesgos cibernéticos se deben insertar en la autoevaluación de controles y riesgos de la primera línea al igual que en la gestión de crisis; fraudes y en los procesos de resiliencia del negocio.

Esto requerirá que las empresas logren una mejor comprensión de la relación entre sus actividades y los riesgos cibernéticos. Las líneas de negocios deberán monitorear activamente los riesgos de exposición, áreas vulnerables, amenazas y los riesgos propios de sus actividades existentes y futuros.

## Alcanzar el nivel de seguridad adecuado

Apoyar una gestión de riesgos cibernéticos efectiva y sólida para toda la empresa consiste en una serie de capacidades básicas fundamentales. Como referencia, la Encuesta Global de Seguridad de la Información (GISS) de 2016-2017 elaborada por EY destacó el hecho que pocas empresas piensan que han alcanzado un nivel alto de madurez en estos temas.

Por ejemplo:

- ▶ Solo 7% de bancos y 6% de aseguradoras creen que cuentan con una gestión avanzada de vulnerabilidades, incluyendo la capacidad de realizar evaluaciones de riesgos durante todo el año que lleven a planes acordados de corrección entre su negocio y la función de riesgos.
- ▶ Solo 3% de bancos y 2% de aseguradoras cuentan con procesos formales de recolección, difusión, integración, respuesta y progresión de amenazas, así como de predicción de ataques.
- ▶ Solo 9% de bancos y 3% de aseguradoras cuentan con un sólido programa de incidencias que incluye a terceros y a las fuerzas del orden, se integra a una función más amplia de gestión de vulnerabilidades y amenazas, y da respuesta a potenciales incidentes siguiendo manuales evaluados periódicamente.

A fin de cuentas, es la misma empresa que conoce sus flujos de datos y procesos empresariales. Por eso, las empresas deben determinar, de la mano con la tecnología, cómo podrían impactar los riesgos cibernéticos en sus clientes, procesos operativos y estrategias.

Estas nuevas responsabilidades implicarán una inversión significativa en recursos humanos y herramientas, incluyendo mejoras en las competencias de monitoreo y análisis para poder elaborar evaluaciones más precisas de los niveles de riesgo cibernético existentes.



## Segunda línea: incorpore a los gestores de riesgos cibernéticos en las operaciones

Los riesgos cibernéticos no deben aislarse como una función de riesgos independiente. Estos deben incluirse en el marco general de gestión de la segunda línea de riesgos. Los gestores de riesgos de las empresas necesitan comparar los riesgos cibernéticos con otros riesgos, empleando los mismos puntos de referencia financieros y de probabilidades, con el fin de considerar, al mismo tiempo, la inversión en prevención y corrección de riesgos cibernéticos, así como otros riesgos urgentes para la empresa.

La gestión de riesgos de la segunda línea cumple un papel fundamental para el manejo de riesgos cibernéticos. Como guardián de los niveles de tolerancia de riesgos aprobados por el Comité, determina cómo medir adecuadamente los riesgos cibernéticos, incorporando umbrales cuantitativos y cualitativos (por ejemplo: la reputación) para los riesgos cibernéticos en la declaración de la tolerancia a riesgos cibernéticos de la empresa. Además, este apetito y los umbrales de tolerancia claramente establecidos, deben transmitirse a las operaciones de cada línea de negocio.

Otras actividades básicas de los gestores de riesgos deben extenderse a manejar los riesgos cibernéticos de la misma manera en que se gestionan los riesgos operativos o riesgos de mercado. Para hacer esto, se deben integrar

firmemente los riesgos cibernéticos en los procesos de control de riesgos y en la taxonomía de riesgos de toda la empresa, incluyendo un marco definido de gestión de riesgos cibernéticos que cubra tantos los riesgos internos y externos como las dependencias. Basados en este marco, los gestores de riesgos de la segunda línea deben desarrollar un panorama integral de los riesgos, las vulnerabilidades y la exposición frente a riesgos cibernéticos, y luego generar métricas sólidas para informar el proceso de toma de decisiones y establecer la relación riesgo-beneficio que implica la inversión en ciberseguridad. Asimismo, los gestores de riesgos deben monitorear las líneas de negocio para verificar si hay una adecuada adherencia al apetito de riesgos cibernéticos de la empresa.

Los datos de pérdidas relacionadas con los riesgos cibernéticos se convertirán inevitablemente en un factor más importante en las decisiones de inversión al igual que las pruebas de resistencia de liquidez y capital.

Tradicionalmente, los datos de pérdidas simplemente reflejan el costo de corregir violaciones de seguridad y no los costos de haber perdido negocios o la erosión de la confianza de los clientes y del valor de la marca. Al incluir estos factores en una perspectiva más amplia de lo que constituye una pérdida por riesgos cibernéticos, los gestores serán capaces de mejorar su capacidad global de toma de decisiones.

El director de riesgos (CRO) juega un importante papel en el liderazgo del equipo de gestión de riesgos cibernéticos de la segunda línea, llevando a cabo acciones como las siguientes:

- **Gestión y supervisión:** propiciar el diálogo con el Comité principal y los comités de auditoría y riesgos.

- ▶ **Estructura organizacional:** establecer las relaciones de subordinación con los jefes de información, los CISO, los jefes de protección de datos y jefes de cumplimiento regulatorio.
- ▶ **Marco de riesgos:** insertar los riesgos cibernéticos en los marcos de gestión de riesgos de toda la empresa, incluyendo al gobierno de riesgos, al reporte de riesgos y métricas, y progresión de riesgos.
- ▶ **Evaluación de impactos:** calificar los potenciales impactos a la liquidez, capital y ganancias causados por un evento de ciberseguridad.
- ▶ **Preparación:** probar la efectividad de los esfuerzos de recuperación de desastres y continuidad del negocio frente a amenazas cibernéticas, así como el grado en que la planificación de recuperación y resolución se incorporan adecuadamente con los riesgos cibernéticos.
- ▶ **Seguros:** evaluar el riesgo cibernético residual y decidir qué riesgos serán cubiertos por seguros (externos o seguros propios).

Los CRO deben reportar directamente al gerente general y al Comité, según corresponda, cuando sus evaluaciones de riesgos cibernéticos difieran de las evaluaciones realizadas por las unidades de negocio de la primera línea o cuando una unidad haya sobrepasado la tolerancia a riesgos cibernéticos establecida por la entidad. Estos reportes se darán adicionalmente a los informes elaborados por los profesionales de seguridad informática de la primera línea.

Debido a que la aplicación del modelo de las tres líneas de defensa es relativamente reciente para afrontar riesgos cibernéticos, la mayoría de las primeras y segundas líneas se enfocan en gestionar más efectivamente estos riesgos en vez de concentrarse en temas más específicos como el cumplimiento regulatorio. No obstante, dado el volumen creciente de asesoramiento normativo y normas obligatorias que surgen, al igual que las normas regulatorias y profesionales, el tema cibernético constituirá progresivamente un riesgo de cumplimiento importante. Por ende, las empresas deberán integrar el cumplimiento regulatorio de riesgos cibernéticos en la gestión de riesgos de la segunda línea.





## Tercera línea: amplíe el mandato de las auditorías internas para que cubran la ciberseguridad y los ataques cibernéticos

Por lo general, el papel fundamental de la tercera línea de defensa radica en evaluar de forma independiente el entorno de control y riesgos de la empresa y en potenciar la efectividad del enfoque de gobierno de riesgos. Lo que se preguntan ahora los reguladores es cuán efectivo e independiente puede ser un equipo de auditoría interna con respecto a la revisión del enfoque de ciberseguridad de la empresa.

Como punto base, el equipo de auditoría interna deberá incluir en su plan global de auditorías, una evaluación de la efectividad del diseño y operatividad de su gestión de riesgos cibernéticos a través de la primera y la segunda línea. Por lo general, las normas de la industria (como el Marco de Ciberseguridad elaborado por el Instituto Nacional de Estándares y Tecnología) se han empleado como puntos de referencia para evaluar la efectividad de una empresa. Por otro lado, los equipos de auditoría interna podrían requerir la creación de sus propios marcos o la aplicación de múltiples marcos de la industria. Al hacerlo, los auditores mantendrán una mayor independencia para evaluar la efectividad de la gestión de riesgos cibernéticos, eliminando así el riesgo de potenciales puntos ciegos que podrían resultar del uso de un estándar general a través de las tres líneas de defensa.

Bajo el modelo de las tres líneas de defensa, los auditores internos harán lo siguiente:

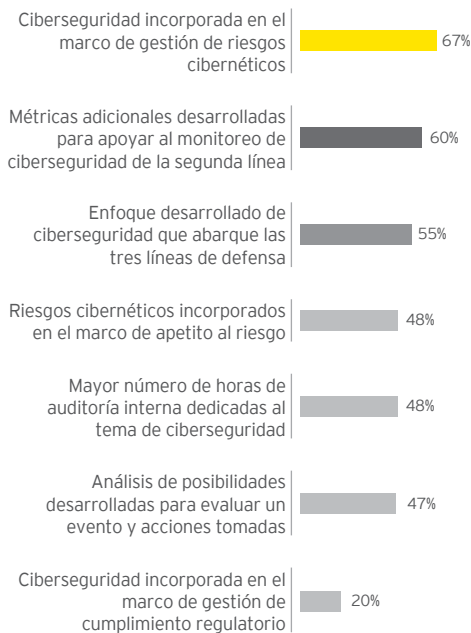
- ▶ **Realizar evaluaciones de rendimiento:** informar acerca de cuán bien se adhieren la primera y la segunda línea de defensa al marco de gestión de riesgos cibernéticos; comparar la exposición actual a riesgos cibernéticos con la tolerancia y el apetito de riesgo aprobados; y evaluar las competencias de la empresa para adaptarse a amenazas y vulnerabilidades cambiantes.
- ▶ **Validar aplicaciones y conexiones:** validar independientemente el inventario de aplicaciones de la empresa a través de su catálogo de aplicaciones internas, infraestructura tecnológica, procesos de negocio y proveedores; monitorear las conexiones y dependencias tanto internamente como externamente de otras organizaciones que le comparten información.
- ▶ **Evaluar los riesgos de terceros:** con base en un mayor énfasis en los proveedores y “nodos” críticos dentro del sistema, la auditoría interna podría necesitar reforzar su evaluación de proveedores críticos a través de, por ejemplo, mejores técnicas de monitoreo continuo o un mayor número de revisiones *in situ*. Por su lado, los terceros deberían incrementar el grado en que emiten sus informes testimoniales, por ejemplo, sus informes de SOCs 2, para proporcionar suficiente información a sus clientes sobre su enfoque de gestión de riesgos cibernéticos.

► **Llevar a cabo pruebas de penetración y evaluaciones de vulnerabilidades independientes:** el equipo de auditoría interna deberá, como mínimo, mejorar la manera en que valida independientemente el alcance, la calidad y las acciones correctivas asociadas con las pruebas de penetración y evaluaciones de vulnerabilidades de la primera línea. Sin embargo, con el tiempo, esto no será suficiente. El equipo de auditoría interna podría realizar sus propias pruebas y evaluaciones. Las evaluaciones, propias o realizadas por la primera línea, deben ser capaces de adaptarse al entorno cambiante de amenazas. Esto podría requerir una rotación periódica de terceros que realicen estas evaluaciones.

► **Mejorar los procedimientos regulares de auditoría aplicando consideraciones sobre los riesgos cibernéticos:** los factores relevantes para hacer frente a riesgos cibernéticos deberán incorporarse en las auditorías regulares realizadas a lo largo del año. Por ejemplo, como parte de las auditorías de rutina, los auditores internos deberán revisar también lo siguiente: los planes de continuidad de negocio y de recuperación después de desastres; escenarios de prueba de resistencia de liquidez y capital (que incluye diversos escenarios relacionados con ataques cibernéticos); planes de resolución y recuperación (en especial para los proveedores más importantes y servicios internos compartidos); tecnología de la información y gestión de riesgos de seguridad; y evaluaciones de impactos relacionados con la adopción de nuevas tecnologías o plataformas digitales disruptivas.

► **Mantenerse actualizado sobre las amenazas:** para alinear las actividades de auditoría con las prioridades corporativas basándose en riesgos y amenazas activas, los auditores internos deberán colaborar con la primera línea para recibir información y análisis sobre las amenazas.

## > Reforzando la gestión de riesgos cibernéticos



Fuente: Séptima Encuesta Global Anual de Gestión de Riesgos Bancarios, EY y el Instituto de Finanzas Internacionales, Octubre de 2016

## Los bancos ya están adoptando el modelo de las tres líneas de defensa

Por más que el énfasis regulatorio en el modelo de riesgos cibernéticos de las tres líneas de defensa es relativamente reciente, se pueden observar señales claras de que la industria bancaria ya está abordando por sí misma los riesgos a través de estas tres líneas. En una serie de planes de acción para el éxito, la séptima Encuesta Global Anual de Gestión de Riesgos Bancarios realizada por EY y el Instituto de Finanzas Internacionales, la ciberseguridad se ubicó segunda en una lista de las cinco mayores preocupaciones de los jefes de riesgos y más de la mitad de ellos (51%) la puso como prioridad, situación diferente en 2015 (22%) y 2014 (10%).

Otras diversas funciones o grupos de gobierno han incrementado su atención hacia la ciberseguridad durante el año pasado, incluyendo a directores (80%), gerentes de líneas de negocio (71%), auditoría interna (66%) y cumplimiento regulatorio (42%).

Al establecer el modelo de riesgos de las tres líneas de defensa, los bancos han diseñado más roles para abordar la ciberseguridad en los grupos de riesgos de la segunda línea y de cumplimiento regulatorio. Asimismo, han dedicado más empleados (75%), designado roles específicos para la ciberseguridad (55%) y creado una posición similar a la de un jefe de seguridad informática (32%). Estos profesionales sirven como complemento, más que como reemplazo, de los roles ya existentes de la primera línea.

Además, como se muestra en la figura anterior, a través de las tres líneas, los bancos han estado mejorando el grado en que insertan los riesgos cibernéticos en sus modelos de operaciones de riesgos, incluyendo en el marco de gestión de riesgos, el plan de auditoría y el cumplimiento regulatorio.

## > Sección 2

# Gobierno de riesgos cibernéticos

El Comité es responsable en última instancia de verificar que las gerencias implementen un enfoque de tres líneas de defensa efectivo para hacer frente a riesgos cibernéticos. Los Comités -incluyendo el de auditoría, riesgos y, en algunos casos, tecnología- deben validar la definición de responsabilidades de gestión de riesgos y supervisión de seguridad informática en la gestión de riesgos, el control interno y la auditoría interna. Ellos deberían supervisar firmemente y cuestionar efectivamente la gestión.

El Comité supervisa la estrategia de gestión de riesgos cibernéticos para toda la empresa, que incluye un apetito al riesgo establecido apropiadamente. Asimismo, debe validar que las estrategias de gestión de riesgos cibernéticos y el apetito al riesgo que se haya integrado en planes estratégicos y estructuras de gestión de riesgos en otras áreas de la empresa.

La estrategia de gestión de riesgos cibernéticos debe abordar los siguientes puntos:

- ▶ Manejar los riesgos cibernéticos residuales inherentes o acumulados, en otras palabras, los riesgos antes y después de los controles de mitigación.
- ▶ Mantener la resiliencia continuamente.

- ▶ Identificar y evaluar actividades, exposición y recursos que involucren riesgos cibernéticos.
- ▶ Establecer políticas para identificar incidentes de ciberseguridad, abordar deficiencias y responder a incidentes y amenazas de seguridad informática.
- ▶ Hacer pruebas y medir la protección, detección y respuestas de la ciberseguridad.

Progresivamente, los reguladores esperarán que los Comités validen que las estrategias de gestión de riesgos cibernéticos consideren la posición global, importancia e interconectividad de la empresa dentro del mercado financiero a mayor escala. Una perspectiva interna ya no será suficiente.

Los Comités deben confirmar que la gerencia cuente con métricas claras para el éxito. Esto incluye tener métricas absolutas para realizar comparaciones de año a año; métricas basadas en metas que evalúen cuán bien la empresa se desempeñó con respecto a objetivos establecidos (por ejemplo, si la meta era lograr “ningún tiempo muerto mayor de una hora”, verificar cuán seguido esto sucedía); métricas basadas en capacidades que describan las nuevas capacidades que la empresa no solía tener en un periodo anterior; y análisis de pares empleando información y encuestas a nivel empresarial.

Cuando los Comités actualizan los puestos y responsabilidades de supervisión de seguridad informática, es importante que evalúen si sus miembros tienen experiencia suficiente en ciberseguridad. Como mínimo, necesitan acceso a personal con dicha experiencia o pueden apoyarse contratando a terceros. Adicionalmente, uno o más miembros del Comité debería tener conocimientos técnicos suficientes para permitir responsabilizarse por el desarrollo e implementación de la estrategia de riesgos cibernéticos y manejar la empresa en niveles de riesgos cibernéticos aprobados por el Comité.

Los Comités  
-incluyendo el de  
auditoría, riesgos y,  
en algunos casos,  
tecnología- deben  
validar la definición  
de responsabilidades  
de gestión de riesgos  
y supervisión de  
seguridad informática  
en la gestión de  
riesgos, el control  
interno y la auditoría  
interna.

## Incorporar la ciberseguridad en toda la organización

En la medida que las empresas midan y gestionen con mayor precisión los riesgos cibernéticos, estas necesitarán integrar un análisis de ciberseguridad más sofisticado para ciertas actividades, incluyendo lo siguiente:

- ▶ **Estrategia, fusiones y adquisiciones:** Los riesgos cibernéticos deben considerarse en los planes estratégicos globales y en los procesos estratégicos de gestión de riesgos. Especialmente, en la debida diligencia y análisis del desarrollo y fusiones empresariales, adquisiciones y disposiciones, y dentro de relaciones con socios aliados.
- ▶ **Innovación:** Mientras que nuevas innovaciones traen consigo crecimiento y rentabilidad para la empresa, estas también pueden generar nuevos riesgos cibernéticos. Se deberá entonces considerar a los riesgos cibernéticos con más detenimiento en el proceso de aprobación de nuevos productos, en iniciativas y adquisición de tecnologías financieras y en la adopción de nuevas tecnologías y plataformas digitales.
- ▶ **Gestión del talento:** Inevitablemente, las empresas al armar su modelo de gestión de riesgos cibernéticos de las tres líneas de defensa, tendrán que poner a prueba su estrategia de retención y adquisición de talento humano. Las empresas deberán validar que cuentan con las competencias y habilidades correctas a lo largo de sus

tres líneas de defensa. De acuerdo con la Encuesta Global de Seguridad de la Información (GISS) 2016-2017 realizada por EY, 51% de los bancos y 59% de las aseguradoras señalan que la falta de habilidades es una de las mayores preocupaciones en sus programas de ciberseguridad. La competencia por talentos se intensificará mientras más instituciones financieras implementen nuevos y más estrictos requisitos regulatorios.

- ▶ **Capacitación de empleados:** Una capacitación efectiva es esencial, ya que la mejor línea de defensa son los empleados de la propia empresa. Como referencia, según la GISS 2016-2017 realizada por EY, 67% de bancos y 82% de aseguradoras afirma que la fuente más significativa de ataques proviene de empleados negligentes. Por lo tanto, la capacitación debe ser personalizada para el puesto y aplicada en general. Todo el personal, incluyendo contratistas terceros, debe asistir frecuentemente a sesiones de capacitación y sensibilización sobre seguridad informática, cuyo contenido debe actualizarse constantemente para reflejar los nuevos riesgos identificados en la evaluación anual de riesgos de la empresa. Asimismo, todo el personal de ciberseguridad debe participar en sesiones periódicas de capacitación y actualización sobre ciberseguridad, y el personal clave debe adicionalmente actualizarse de las nuevas amenazas y contramedidas de ciberseguridad. Se deberían desarrollar y emplear métricas para monitorear la comprensión de los empleados.



## Todos estamos juntos en esta tarea

Los reguladores están imponiendo el modelo de tres líneas de defensa para obligar a las empresas, principalmente a los bancos, a mejorar su gestión de riesgos en respuesta a fallas ocurridas antes y después de la crisis financiera. Las empresas han implementado exitosamente el modelo en el área de riesgos financieros, créditos y liquidez. El área que más retos presupone a la industria es la de riesgos no financieros, que incluye los riesgos cibernéticos.

Los reguladores han concluido claramente que el modelo de ciberseguridad de tres líneas de defensa es crucial. Los riesgos cibernéticos ya no se pueden considerar como riesgos informáticos que los profesionales de seguridad puedan manejar por sí solos. Ellos aún tienen un rol fundamental en la gestión de riesgos cibernéticos trabajando mano a mano con la gestión de primera línea de la empresa. Al mismo tiempo, la segunda y la tercera línea tienen roles independientes que desempeñar supervisados por un Comité comprometido y efectivo.

Encontrar el balance perfecto tomará un tiempo. No obstante, considerando los riesgos cibernéticos para todo el sistema, la industria necesita moverse rápido para poner en marcha los aspectos fundamentales para que, en conjunto, las empresas individuales y la industria en general estén mejor protegidas y sean más resilientes y capaces de responder rápida y eficazmente a los inevitables ataques cada vez más potentes que la industria sufrirá en los próximos años.







¿Cómo proteger  
a los robots de un  
ataque cibernético?

IV

---

## El panorama de la robótica en la ciberseguridad

Un aumento de los ciberataques, combinado con el cambio hacia la automatización de los procesos de negocios mediante la Automatización Robótica de Procesos (RPA, por sus siglas en inglés), trae nuevos riesgos que deben abordarse para proteger los datos confidenciales e infundir confianza en sus plataformas de robótica.

Además, la brecha de talento en la ciberseguridad, junto con las presiones para administrar los costos, hace que la orquestación y el aprendizaje cognitivo sean una opción atractiva para muchas organizaciones con el fin de mejorar su postura de seguridad de manera más eficiente.



## > Sección 1

---

# ¿A qué nos referimos con robótica?

La Automatización de Tecnologías de la Información (ITA, por sus siglas en inglés) y la Automatización de Procesos Comerciales (BPA, por sus siglas en inglés) han existido durante décadas, ¿en qué consiste toda esta exaltación sobre la robótica? Recientemente hemos respondido a diversas preguntas sobre si la robótica es realmente diferente de la ITA y la BPA tradicional. Desde nuestra perspectiva, la respuesta es un rotundo "sí". Si bien el objetivo principal de automatizar un proceso es compartido, quien construye y mantiene la ITA y BPA, generalmente es un equipo pequeño, técnicamente preparado y centralizado. La robótica inversamente coloca gran parte del control de la automatización en las manos de los usuarios y las personas con menor conocimiento técnico. En segundo lugar, la ITA y la BPA son conocidos por tardar meses y, a veces, años en implementarse. Con la robótica, las tareas se pueden automatizar en cuestión de semanas debido al desarrollo limitado de códigos y capacidades de lectura de pantalla de aplicaciones inteligentes.

Vemos que la robótica gana interés rápidamente en organizaciones de diferentes industrias y sectores. Los usuarios empresariales están empleando la Automatización Robótica de Procesos (RPA) para automatizar rápida y fácilmente los procesos repetitivos que consumen mucho tiempo. Los grupos de TI y ciberseguridad están aprovechando la capacidad de las plataformas de robótica para orquestar flujos de trabajo y realizar funciones de aprendizaje cognitivo. Como tal, a menudo hay un poco de confusión sobre lo que alguien quiere decir cuando dice "robótica".

En EY, generalmente vemos las siguientes tres formas de robótica:

## 1 Automatización Robótica de Procesos (RPA)

Aprovecha aplicaciones fáciles de usar para configurar robots de *software*, que se pueden entrenar e implementar rápidamente para automatizar tareas manuales en varios procesos comerciales que abarcan múltiples sistemas. Las actividades típicas consideradas para la RPA incluyen la entrada de datos, migración de datos a través de múltiples sistemas, manipulación de datos, reconciliación de datos y toma de decisiones basadas en reglas en procesos comerciales. Estos robots de *software* están entrenados para interactuar directamente con una interfaz de usuario sin necesidad de desarrollar códigos para automatizar tareas individuales las cuales ayudan al personal humano.

## 2 Orquestación (OR)

A menudo se usa en operaciones de gestión de servicios de TI y ciberseguridad para actividades como aprovisionamiento y desaprovisionamiento de usuarios, gestión de *tickets* y clasificación de incidentes de ciberseguridad. Esta forma de robótica se centra en la codificación de acciones de automatización y módulos de actores que se pueden aplicar a muchos sistemas, con el objetivo de optimizar flujos de trabajo complejos y automatizar tareas que requieren de mucho tiempo. La robótica sigue un conjunto de reglas predefinidas que describen tareas y toman decisiones basadas en criterios predefinidos. Estas soluciones interactúan con las Interfaces de Programación de Aplicaciones (APIs, por sus siglas en inglés), bases de datos y servidores *back-end*, que a menudo requieren un desarrollo de código significativo para configurar los módulos necesarios con la capacidad de aprovechar estos módulos en un momento posterior con menos necesidad de habilidades de desarrollo de código.

Atributo clave de la robótica	RPA	OR	CL
Interactúa con la interfaz de usuario	✓		
Scraping de pantalla inteligente	✓		
Entrenado por usuarios de negocios	✓		
Toma de decisiones basada en reglas	✓	✓	
Entrenado por el administrador de TI y los analistas de seguridad de TI			✓
Interactúa con APIs y bases de datos directamente		✓	✓
Requiere un desarrollo de código significativo		✓	✓
Entrenado por programadores / desarrolladores expertos			✓
Inteligencia Artificial / aprendizaje automático			✓

## 3 Aprendizaje Cognitivo (AC)

Esta forma de robótica va más allá de la toma de decisiones basada en reglas para procesar datos estructurados y no estructurados. Incorpora el aprendizaje automático y la inteligencia artificial mediante la aplicación de algoritmos y análisis avanzados. El aprendizaje cognitivo tiene como objetivo pensar y actuar de la misma manera que los humanos para realizar tareas complejas sin interacción humana. Esto requiere una extensa programación y modelado de algoritmos de máquina y autoaprendizaje.

## Un marco de ciberseguridad para la robótica

El entorno empresarial actual cuenta con una necesidad apremiante por digitalizar; por este motivo, la robótica es un componente crítico en la estrategia digital de una empresa. Dado que la robótica se aplica a varias facetas de una empresa, un programa debería abordar

el riesgo cibernético asegurando plataformas robóticas y se debería aprovechar para permitir la ejecución de operaciones cibernéticas más efectivas y eficientes. Creemos que los seis dominios cibernéticos descritos a continuación, desempeñan los roles más críticos en robótica. A lo largo de este capítulo, estos seis dominios servirán como un lente para visualizar la seguridad de la robótica.



## > Sección 2

# Asegurando la RPA

## ¿Cuáles son los riesgos cibernéticos asociados con la RPA?

La RPA introduce una nueva superficie de ataque que puede ser aprovechado para divulgar, robar, destruir o modificar datos confidenciales y/o información de alto valor, acceder a aplicaciones y sistemas no autorizados, además de explotar vulnerabilidades para obtener más acceso a una organización.

Una de las preguntas más populares que escuchamos en la actualidad es: "¿Qué riesgos cibernéticos debería considerar en mis capacidades de robótica?" En esta sección, nos centramos en los riesgos cibernéticos de la RPA, dejando algunas consideraciones específicas sobre el aprendizaje cognitivo para ser abordadas en otro momento.

En EY, creemos que las organizaciones deben generar confianza en sus plataformas de RPA para abordar diversas formas de riesgo, incluido el riesgo cibernético. Algunos ejemplos sobre riesgos cibernéticos, que las organizaciones relacionadas con la robótica deberían considerar para asegurar sus implementaciones de robótica, incluyen:

### Creador de bot

Entrena a los bots para automatizar tareas

### Gestor de bot

Gestiona la ejecución simultánea de muchos bots

### Ejecutor de bot

Ejecuta tareas automáticas



### > ¿Cuáles son los riesgos cibernéticos asociados con la RPA?

Riesgo cibernético	Escenario
> Abuso de acceso privilegiado	<ul style="list-style-type: none"> <li>▶ Un atacante compromete una cuenta de usuario robótica altamente privilegiada utilizada por algunos <i>bots</i> para obtener acceso a datos confidenciales y moverse dentro de una red.</li> <li>▶ Un interno malicioso entrena un robot para destruir datos de alto valor, interrumpiendo procesos comerciales clave, como clientes que generan pedidos.</li> </ul>
> Divulgación de datos confidenciales	<ul style="list-style-type: none"> <li>▶ Un creador de <i>bot</i> entrena por error a un <i>bot</i> para cargar información de tarjetas de crédito a una base de datos accesible a través de la web.</li> <li>▶ Un creador de <i>bot</i> aprovecha una cuenta genérica para robar propiedad intelectual sensible, dejándolo difícil, si no imposible, para identificar la verdadera fuente de la fuga.</li> </ul>
> Vulnerabilidades de seguridad	<ul style="list-style-type: none"> <li>▶ Existe una vulnerabilidad en el <i>software</i> de robótica que proporciona a los atacantes acceso remoto a la red de una organización.</li> <li>▶ Un creador de <i>bot</i> entrena a un <i>bot</i> para manejar datos confidenciales de clientes pero no protege ni encripta la transmisión de esos datos a la nube.</li> </ul>
> Negación de servicio	<ul style="list-style-type: none"> <li>▶ Está previsto que un <i>bot</i> ejecute en una secuencia rápida, lo que agota todos los recursos disponibles del sistema y detiene todas las actividades de los <i>bot</i>.</li> <li>▶ El gestor de <i>bot</i> es interrumpido debido a una red no planificada, servicio o corte del sistema que resulta en una pérdida de productividad, la cual no se reemplaza fácilmente con mano de obra humana.</li> </ul>

## ¿Cómo puedo proteger mi ecosistema de RPA?

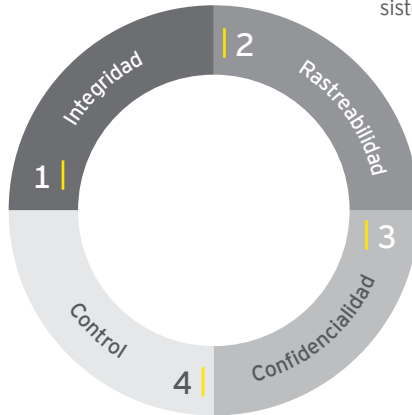
Cuando se trata de asegurar las implementaciones de RPA, una organización debe considerar los elementos técnicos, de proceso y humanos de todo el ecosistema de robótica. Un diseño seguro debe incluir todo el ciclo de vida del producto a partir de los requisitos, la selección, la arquitectura, la implementación y las operaciones continuas. Para generar confianza dentro de una plataforma robótica, creemos que su enfoque debería proporcionar lo siguiente:

### 1 | Integridad

¿Puedo confiar en que los datos y resultados que obtengo de mis *bots* no hayan sido modificados o alterados?

### 2 | Rastreabilidad

¿Puedo monitorear y rastrear actividades de *bots* para identificar el mal uso de la robótica que afecta confidencialmente, la integridad o la disponibilidad de otros sistemas y/o datos?



### 4 | Control

¿Estoy controlando el acceso y protegiendo las cuentas privilegiadas aprovechadas por el sistema robótico y los usuarios?

### 3 | Confidencialidad

¿Puedo proteger los datos confidenciales para que no los revelen intencionalmente o accidentalmente los gestores de *bots* y ejecutores de *bots*?

Aprovechando el marco de seguridad cibernética para la robótica descrito anteriormente, nos gustaría analizar las consideraciones de control de seguridad para cada dominio cibernético.



## > ¿Cómo puedo proteger mi ecosistema de RPA?

Control	Detalles de la robótica
> Gobernanza	<ul style="list-style-type: none"> <li>▶ Establecer un marco de gobernanza con roles y responsabilidades para asegurar la robótica.</li> <li>▶ Desarrollar los requisitos de seguridad y estrategia para la RPA dentro de las políticas y supervisar el cumplimiento de las políticas de seguridad relacionadas con la RPA.</li> <li>▶ Administrar los riesgos de la RPA identificados a través de un programa formal de gestión de riesgos y aumentar la conciencia acerca de los riesgos de la RPA entre los creadores de <i>bot</i> y los usuarios empresariales.</li> </ul>
> <i>Software</i> y seguridad del producto	<ul style="list-style-type: none"> <li>▶ Realizar un análisis de riesgo en la arquitectura de seguridad de las soluciones de la RPA elegidas, incluida la creación, la gestión y la ejecución de bots. Identificar fallas de la arquitectura de seguridad en productos subyacentes para conexiones en varios entornos, uso de metodologías de virtualización y fallas de autorización.</li> <li>▶ Llevar a cabo una revisión de diseño segura, que incluya un análisis de flujo de datos para verificar que los controles en torno a la seguridad estén integrados en la autenticación de <i>bot</i>, autorización y validación de entrada.</li> <li>▶ Integrar herramientas de escaneo de seguridad como parte del proceso de creación de <i>bot</i> para escanear el código creado en el <i>back-end</i> para vulnerabilidades de seguridad.</li> <li>▶ Escanear el <i>bot</i> creado para encontrar vulnerabilidades de seguridad usando pruebas dinámicas o tecnología <i>fuzzing</i> de seguridad para determinar fallas.</li> <li>▶ Asegurar que el esquema de implementación del <i>bot</i> tenga en cuenta consideraciones de seguridad.</li> </ul>
> Identidad digital y gestión de accesos	<ul style="list-style-type: none"> <li>▶ Mejorar la auditabilidad (cada paso podría registrarse) y controlar las actividades manuales propensas a errores que podrían elevar el riesgo y el incumplimiento.</li> <li>▶ Administrar privilegios de acceso de usuarios y/o separar los riesgos de tareas; por ejemplo, el uso de una matriz de seguridad especializada autoriza a los bots a realizar solo las tareas asignadas a ellos.</li> <li>▶ Implementar controles de seguridad para proteger las credenciales durante el tiempo de ejecución de la sesión robótica; por ejemplo, si el uso del inicio de sesión único (SSO, por sus siglas en inglés) con el protocolo de acceso ligero a directorios (LDAP, por sus siglas en inglés) es compatible con el inicio de sesión protegido a la interfaz RPA.</li> <li>▶ Reforzar contraseñas a través de sesiones robóticas, centralizar la identidad robótica y el proceso de administración de acceso; aprovechar los administradores de credenciales encriptados para evitar la fuga de credenciales.</li> </ul>
> Identificación y protección de datos	<ul style="list-style-type: none"> <li>▶ Llevar a cabo una evaluación del cumplimiento de regulaciones de datos para el uso de la robótica y la automatización.</li> <li>▶ Monitorear de datos confidenciales procesados y automatizados por la robótica, para verificar el cumplimiento de las políticas de uso.</li> <li>▶ Comprobar la integridad de robótica y el código de automatización.</li> </ul>
> Operaciones de seguridad	<ul style="list-style-type: none"> <li>▶ Consolidar los datos de registro de los ejecutores y gestores de bots para proporcionar un seguimiento de las actividades de auditoría, el control de picos anormales en la actividad, el acceso de los sistemas y el uso de cuentas privilegiadas.</li> <li>▶ Realizar un escaneo de vulnerabilidad en la plataforma de robótica y ejecutar ejercicios de modelado de amenazas de sesiones de robótica para determinar debilidades técnicas o brechas del proceso.</li> </ul>

## > Sección 3

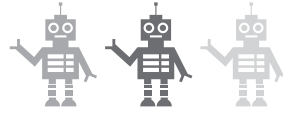
# Aprovechando la robótica para la ciberseguridad

## ¿Cómo puede la automatización y la orquestación robótica mejorar la seguridad en su organización?

Muchos directores de sistemas (CIO), directores de seguridad de la información (CISO) y los directores de tecnología digital (CDO) son desafiados por decenas y, a menudo, cientos de tecnologías y aplicaciones heredadas que no funcionan bien entre sí. Esto implica que empleados recopilen datos manualmente de múltiples sistemas, copien información de un sistema a otro y aplicaciones para completar una sola tarea. Para solucionar esto, una nueva categoría de capacidades se está volviendo más popular en el dominio de seguridad cibernética.

Las organizaciones están utilizando estas formas de robótica para:

- ▶ Reducir el tiempo para detectar y responder incidentes, ayudando a minimizar la exposición de riesgo en un ataque.
- ▶ Cerrar la brecha de talento a través de la automatización de tareas de uso intensivo de recursos, ayudando a las organizaciones a administrar los gastos operativos.
- ▶ Reducir al mínimo la rotación de personal debido a la falta de retos o línea de carrera, al permitir que los empleados se centren en tareas de mayor valor.
- ▶ Implementar automáticamente controles de seguridad que den como resultado una superficie de ataque reducida cuando se descubran vulnerabilidades o excepciones de cumplimiento.
- ▶ Tomar decisiones inteligentes rápidamente, dando resultados consistentes y de alta calidad.



EY cree que la robótica ayudará a llenar la escasez de talento a 1,5 millones de profesionales de ciberseguridad para 2019.<sup>16</sup>



Para EY, la robótica puede ayudar a reducir significativamente el tiempo promedio de detección, de los actuales 205 días<sup>17</sup>, a semanas o incluso días.



El 74% de los profesionales de seguridad de la información están preocupados por las amenazas internas.<sup>18</sup> EY cree que la robótica puede ayudar a reducir la exposición de los empleados a datos confidenciales.

<sup>16</sup> (ISC)

<sup>17</sup> Reporte de Gartner Inc. "Market Share Analysis: IT Services, Worldwide 2016"

<sup>18</sup> SANS

## Casos ilustrativos para aplicar la robótica en la ciberseguridad

Anteriormente se discutió sobre las posibles preocupaciones de seguridad asociadas con la robótica; sin embargo, también hay varias oportunidades para aprovechar la robótica, con el fin de mejorar la estrategia digital y potenciar las operaciones de seguridad.

Se utilizará el marco de seguridad cibernética para la robótica, presentado previamente, con el fin de ilustrar posibles casos de uso beneficiosos:

### > Casos ilustrativos para aplicar la robótica en la ciberseguridad

Dominio de ciberseguridad	Casos ilustrativos
> Gobernanza	<p><b>Gobierno del programa de seguridad</b></p> <p>La robótica puede mejorar la calidad, la puntualidad y el rendimiento de los informes de seguridad. Por ejemplo, las pruebas de postura de seguridad automáticas y periódicas, se pueden alimentar a un proceso integral de informes impulsado por la robótica, proporcionando paneles de mandos y áreas de preocupación destacadas (independientemente de las tolerancias y métricas establecidas por la administración).</p> <p><b>Seguimiento de controles de seguridad</b></p> <p>La robótica puede ayudar a conducir pruebas automatizadas dentro del espacio de seguridad de la información. Por ejemplo, dentro de su configuración, la robótica podría permitir pruebas de cumplimiento más rápidas y eficientes para asegurar ajustes en servidores, <i>firewalls</i>, <i>routers</i> y aplicaciones. Las pruebas se pueden llevar a cabo de forma periódica y se pueden enviar a informes automáticos al tablero de embarque, entre otros.</p>
> Software y seguridad del producto	<p><b>Seguimiento del inventario de aplicaciones</b></p> <p>La robótica puede ser aprovechada para automatizar las aplicaciones de detección e inventario en la empresa. Una vez descubierto, el aprendizaje cognitivo se puede utilizar para automatizar la clasificación de riesgos de la aplicación en función a los datos y controles detectados. Además, los <i>bots</i> se pueden implementar para descubrir y actualizar continuamente el inventario y controles asociados.</p> <p><b>Puertas de desarrollo seguras</b></p> <p>El aprendizaje cognitivo se puede utilizar para realizar verificaciones de puertas en las actividades de seguridad del ciclo de vida de desarrollo del software (SDLC, por sus siglas en inglés). Los <i>bots</i> pueden recopilar información de cada herramienta de gestión de proyectos o a través de sistemas automatizados para identificar cuándo una base de códigos se está moviendo a la siguiente fase del SDLC. Las reglas se pueden configurar y enviar a informes automáticos para el tablero de embarque, entre otros, para comprender si la deuda de seguridad de una aplicación debe remediarse.</p> <p style="text-align: right;">&gt;&gt;&gt;</p>

&gt;&gt;&gt;

Dominio de ciberseguridad	Casos ilustrativos
<p>&gt; <i>Software</i> y seguridad del producto</p>	<p><b>Validación y remediación de seguridad</b></p> <p>La robótica se puede utilizar para recopilar información automatizada sobre las URL y el código, los cuales deben probarse para permitir un análisis eficiente en las vulnerabilidades de las aplicaciones. Los <i>bots</i> pueden permitir la escalabilidad de múltiples aplicaciones al mismo tiempo y completar las vulnerabilidades descubiertas del triaje <i>Tier</i> 1. Asimismo, los resultados de las pruebas se pueden integrar con las plataformas de desarrolladores existentes para repararse a través de robots de aprendizaje cognitivo.</p>
<p>&gt; Identidad digital y acceso</p>	<p><b>Cumplimiento de acceso</b></p> <p>La robótica puede ayudar a reducir la dependencia de grandes equipos de soporte y operaciones al automatizar la mayoría de las tareas de aprovisionamiento y/o desaproveccionamiento. Puede ofrecer una mejora de hasta 8 veces en los marcos de tiempo de cumplimiento de solicitud automática en comparación con el procesamiento manual.</p> <p><b>Certificación de acceso</b></p> <p>Los <i>bots</i> pueden ser entrenados para alcanzar hasta 45% de ganancias operativas y de eficiencia de costos al automatizar las verificaciones de validación de datos de precertificación manual. Pueden ser entrenados también para la administración de configuración de certificación, verificaciones manuales de campaña durante certificaciones y/o revisiones de acceso, reconciliación e informes posteriores a la certificación.</p> <p><b>Comprobación de la adecuación de acceso manual y notificaciones de alerta automáticas</b></p> <p>La robótica puede ayudar a mejorar la eficacia y la calidad de la validación de los datos de acceso, lo que permite a los administradores centrarse en las cuestiones de acceso de mayor riesgo durante el proceso de revisión. También se puede capacitar para redactar y enviar notificaciones de confirmación a los usuarios si se detectan anomalías al realizar validaciones de datos.</p>

&gt;&gt;&gt;

&gt;&gt;&gt;

**Dominio de ciberseguridad****Casos ilustrativos**

## &gt; Identificación y protección de datos

**Detección de datos, clasificación y remediación**

La robótica se puede aprovechar para automatizar la detección y el inventario de datos confidenciales. Una vez descubierto, el aprendizaje cognitivo se puede utilizar para automatizar la clasificación de datos confidenciales. Además, los *bots* se pueden implementar para detectar, validar y eliminar datos confidenciales almacenados en lugares no autorizados.

**Detección y corrección de pérdida de datos**

El aprendizaje cognitivo se puede aplicar para mejorar la precisión de la amenaza interna y el control de la pérdida de datos. Una vez que se descubren los problemas a través de la monitorización de pérdida de datos, los controles de seguridad de datos pueden implementarse automáticamente para remediar los sistemas infractores y evitar problemas futuros.

## &gt; Operaciones de seguridad

**Detección de amenazas y respuesta**

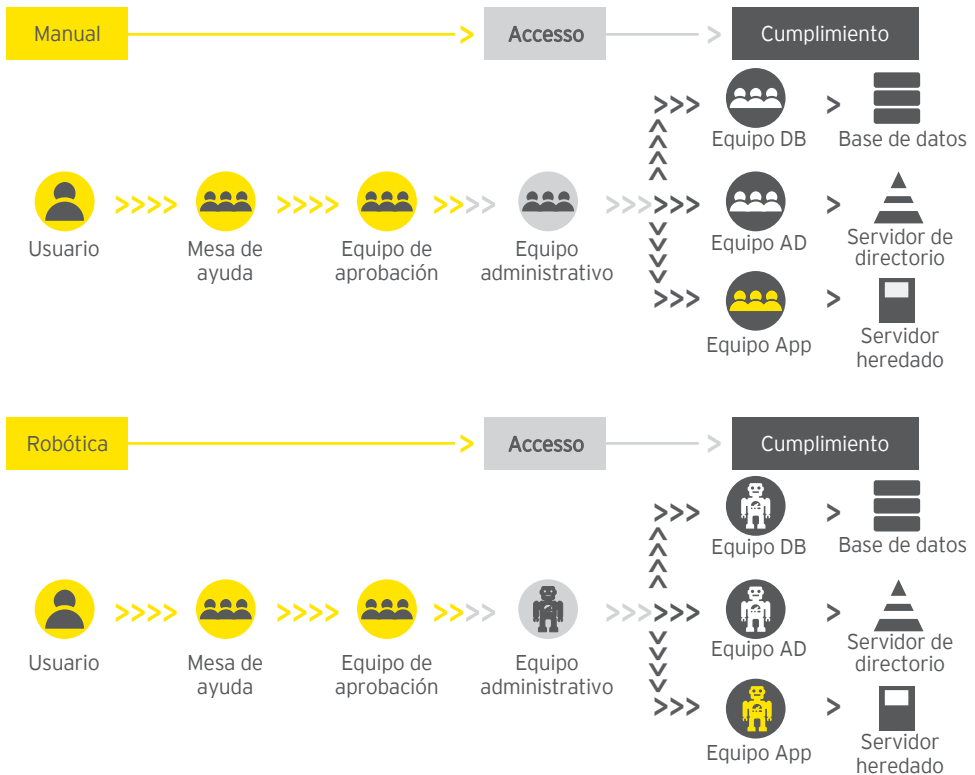
La robótica se puede utilizar para recopilar información relevante sobre amenazas y datos técnicos para permitir el análisis rápido y eficiente de *malware* y alertas de amenazas. Una vez recopilados, la robótica puede ayudar a automatizar el proceso de clasificación del *Tier 1* para tomar decisiones sobre cuándo y cómo responder. Además, se pueden tomar acciones automatizadas para coordinar la corrección de incidentes.

**Exposición a amenazas y manejo de vulnerabilidades**

La robótica puede mejorar la eficiencia y la calidad del programa de amenazas y brechas, ayudando a comprender las vulnerabilidades empresariales y priorizando las actividades de remediación. Luego se puede aprovechar para notificar automáticamente a los administradores de sistemas y aplicaciones de las actividades de remediación y realizar la validación para rastrear el cumplimiento.

## Caso de cumplimiento de accesos para la automatización de procesos robóticos

Los robots se pueden crear para recopilar la información del trabajo manual, desde la solución de Gestión de Acceso a la Identidad (IAM) hasta automatizar la ejecución de tareas de cumplimiento de acceso en los sistemas finales.



### Beneficios de la robótica:

- ▶ Mejora de **6x-8x** tomando un proceso manual de 6-8 minutos y reduciendo a ~1 minuto.
- ▶ Los robots pueden proporcionar una **cobertura 24/7** y manejar tareas por sí mismos.

- ▶ **Lógica de gestión de excepciones** para excepciones comerciales, del sistema y validaciones de datos.
- ▶ Capacidad de **revisar registros de auditoría, programar y manejar tareas** por sí mismo.
- ▶ Se pueden implementar múltiples robots para manejar **actividades paralelas** basadas en los volúmenes de transacción.

## Caso de *phishing* para la orquestación de la robótica

Los ataques de *phishing* son una de las amenazas más comunes que enfrentan las organizaciones hoy en día. El análisis y una respuesta adecuada a un correo de *phishing*, se convierte en un proceso que requiere mucho tiempo. Esto hace que el

proceso de respuesta sea un candidato excelente para la automatización.

Las organizaciones, mediante la automatización de casi todo el proceso de recopilación de datos, pueden estar más alertas de manera más efectiva, ayudando a mejorar la gestión de riesgos y reducir la superficie de ataque.

	Recopilación de datos	Análisis	Remediación
> Actividades	<ul style="list-style-type: none"> <li>▸ Extraer indicadores (URL o IP) del mensaje</li> <li>▸ Comparar fuentes de datos con inteligencia de amenazas</li> <li>▸ Generar informes</li> <li>▸ Crear <i>tickets</i> con información relevante</li> </ul>	<ul style="list-style-type: none"> <li>▸ Inspeccionar los encabezados de los mensajes</li> <li>▸ URL de referencia cruzada, dominio, dirección IP con inteligencia de amenaza</li> <li>▸ Leer gramática sospechosa</li> <li>▸ Escanear adjuntos para <i>malware</i></li> <li>▸ Extraer indicadores de <i>malware</i>: IP, URL, <i>Hash</i>, procesos</li> <li>▸ Consultar la información de seguridad y gestión de eventos (SIEM, por sus siglas en inglés)</li> <li>▸ Soluciones de <i>pivot to point</i></li> <li>▸ Validar autenticación de registros</li> </ul>	<ul style="list-style-type: none"> <li>▸ Ejecutar un análisis antivirus</li> <li>▸ Ejecutar procedimientos de respuesta o pasos de respuesta de precarga en soluciones puntuales</li> <li>▸ Actualizar filtro de <i>firewall</i>, <i>spam</i></li> <li>▸ Desactivar cuentas de usuario</li> <li>▸ Eliminar el servidor de correo electrónico</li> <li>▸ Actualizar el sistema de <i>tickets</i></li> <li>▸ Notificar a las partes afectadas</li> </ul>
> Tiempo (pre-automatización)	10 minutos	10 minutos	20 minutos
> Tiempo (post-automatización)	~4 minutos	~4 minutos	~4 minutos

**50% a 75% de reducción en el tiempo para detectar y responder a un ataque de *phishing***



# ¿Tu negocio está preparado para lo que aún no existe?

Navega la Era de la Transformación  
de la mano de los consultores mejor  
conectados.



# > Contactos

---

## EY Perú

**Paulo Pantigoso**  
Country Managing Partner  
paulo.pantigoso@pe.ey.com

## > Consultoría

---

**Jorge Acosta**  
Socio Líder de Consultoría  
jorge.acosta@pe.ey.com

**Elder Cama**  
elder.cama@pe.ey.com

**Fabiola Juscamaita**  
fabiola.juscamaita@pe.ey.com

**Cecilia Ota**  
cecilia.ota@pe.ey.com

**Giuliana Guerrero**  
giuliana.guerrero@pe.ey.com

**Geraldine Mouchard**  
geraldine.mouchard@pe.ey.com

**Renato Urdaneta**  
renato.urdaneta@pe.ey.com

## > Consultoría para la Industria Financiera

---

**José Carlos Bellina**  
Socio Líder de Consultoría para la Industria Financiera  
jose.bellina@pe.ey.com

**Numa Arellano**  
numa.arellano@pe.ey.com

**Alejandro Magdits**  
alejandro.magdits@pe.ey.com

## > Oficinas

---

**Lima**  
Av. Víctor Andrés Belaúnde 171,  
San Isidro - Lima 27  
Telf: +51 1 411 4444

**Arequipa**  
Av. Bolognesi 407,  
Yanahuara - Arequipa  
Telf: +51 54 484 470

**Chiclayo**  
Av. Federico Villarreal 115,  
Salón Cinto,  
Chiclayo - Lambayeque  
Telf: +51 74 227 424

**Trujillo**  
Av. El Golf 591, Urb. Del Golf  
II Etapa.  
Víctor Larco Herrera 13009,  
Sala Puémape, Trujillo - La Libertad  
Telf: +51 44 608 830

Av. Jorge Basadre 330,  
San Isidro - Lima 27  
Telf: +51 1 411 4444



## Declaración

---

Esta publicación contiene información en forma resumida y está pensada solamente como una guía general de referencia y de facilitación de acceso a información. Este documento, de ninguna manera, pretende sustituir cualquier investigación exhaustiva o la aplicación del criterio y conocimiento profesional. Asimismo, la constante dinámica de los mercados y su información resultante puede ocasionar la necesidad de una actualización de la información incluida en este documento. EY no se hace responsable por los resultados económicos que alguna persona, empresa o negocio pretenda atribuir a la consulta de esta publicación. Para cualquier tema de negocios y asesoría en particular, le recomendamos contactarnos.

### Acerca de EY

EY es el líder global en servicios de auditoría, impuestos, transacciones y consultoría. La calidad de servicio y conocimientos que aportamos ayudan a brindar confianza en los mercados de capitales y en las economías del mundo. Desarrollamos líderes excepcionales que trabajan en equipo para cumplir nuestro compromiso con nuestros stakeholders. Así, jugamos un rol fundamental en la construcción de un mundo mejor para nuestra gente, nuestros clientes y nuestras comunidades.

Para más información visite [ey.com/pe](http://ey.com/pe)

© 2018 EY  
All Rights Reserved.




Descarga nuestras  
publicaciones y guías en:  
[ey.com/PE/EYPeruLibrary](http://ey.com/PE/EYPeruLibrary)

 /EYPeru

 @EYPeru

 /company/ernstandyoung

 @ey\_peru

 /EYPeru

 [perspectivasperu.ey.com](http://perspectivasperu.ey.com)

 [ey.com/pe](http://ey.com/pe)

