



Building a better  
working world

# ¿Cómo pasar de una seguridad aislada a una integrada?

Cerrando la brecha de relaciones en la  
organización para construir un programa  
de seguridad alineado al negocio

Encuesta Global de Seguridad  
de la Información 2019-2020



The better the question. The better the answer.  
The better the world works.



## Contenido

---

Resumen ejecutivo	5
1. Un fallo sistemático de comunicación en la organización	13
2. Crear y mantener relaciones que aumenten la confianza y la colaboración	23
3. El CISO como agente de transformación	33
Ciberseguridad en tiempos de COVID en Latinoamérica	40
Conclusiones y siguientes pasos	48



**Marcelo Zanotti**  
Socio Consultoría en Riesgo

Bienvenidos a la 22a Encuesta anual global de Seguridad de la Información (GISS en inglés), la cual analiza los problemas de ciberseguridad más importantes a los que se enfrentan actualmente las organizaciones.

El estudio de este año nos encuentra en medio de una emergencia sanitaria inédita, que está desafiando a las organizaciones de todo el mundo a adaptarse y priorizar las funciones y procesos críticos.

Este escenario ha empujado a millones de personas a estructuras de trabajo remoto o a interacciones en línea entre clientes y empresas, dejando en evidencia muchas de las falencias y vulnerabilidades de las organizaciones. Este cambio conlleva riesgos adicionales de seguridad de la información para la confidencialidad, integridad y disponibilidad de los sistemas de información clave.

Todo esto da cuenta del nuevo foco que debe tener el oficial de seguridad de la información (CISO, por sus siglas en inglés), el que debe asumir un rol más central y liderar hacia la “nueva normalidad” que se perfila con la pandemia. Su función, debe conversar más con el resto de la organización, especialmente con el área comercial, y presentarse como un solucionador de problemas en este escenario de transformación.

Ahora más que nunca, la capacidad de una empresa para proteger a su fuerza de trabajo remota, activos de información valiosos y responder rápidamente a un incidente de ciberseguridad es vital para superar este período de incertidumbre.

La ciberseguridad no solo es un riesgo en constante evolución, sino que también debe ser confrontado en el contexto de la innovación y el cambio. “Security by Design” debe ser el objetivo de cada organización.

Una de las principales enseñanzas de la pandemia es que las organizaciones deben depender cada vez más de tecnologías nuevas y disruptivas. Las organizaciones que carecen de medidas de seguridad eficaces para ayudar a gestionar estos cambios se enfrentan a la ruptura de la confianza del mercado, con consecuencias como daño reputacional y pérdidas financieras significativas.

Las empresas deben adoptar una nueva perspectiva que garantice la resiliencia diaria, así como un enfoque proactivo, pragmático y estratégico que tenga en cuenta el riesgo y la seguridad desde el principio. Esto es Security by Design.

En lugar de evitar el riesgo por completo, Security by Design consiste en habilitar la confianza en los sistemas, diseños y datos para que las organizaciones puedan asumir más riesgos, liderar el cambio transformacional e innovar con seguridad.

Esperamos que esta publicación sea un aporte para su organización, la importancia de la ciberseguridad no puede ser subestimada en un mundo que, tras la pandemia, dio un salto gigante en las interacciones en línea.



# Resumen ejecutivo

---

Nunca antes se ha visto el nivel de amenazas a la ciberseguridad en el mundo como ahora, coincidiendo con la transformación de muchas industrias y organizaciones.

Hoy es fundamental que la organización en su conjunto (desde el Directorio, las gerencias y hasta los colaboradores) entiendan las amenazas y las medidas de respuesta orquestadas por el Oficial de Seguridad de Información, con el apoyo de todos.

Ciertamente, los equipos de ciberseguridad impulsan la prevención, respuesta y sostenibilidad de la seguridad de información y seguridad informática. En un contexto de prueba y error las empresas van tomando conciencia que tienen un rol crucial como habilitadores de la transformación desde el diseño: *Security by Design*. Sin embargo, hacer el cambio a dicha cultura es una responsabilidad compartida. Los CISOs deben tener espacio para construir relaciones en las áreas de negocio y en los Directorios para propiciar un trabajo conjunto, y para hacer frente a las amenazas y riesgos de ciberseguridad. Construir relaciones en base a la confianza basada en conocimiento, acciones conjuntas y resultados concretos.

Trabajar juntos de esta manera crea una oportunidad de oro para que las organizaciones coloquen la ciberseguridad en el centro de sus estrategias y así ganar ventaja competitiva y diferenciarse de los demás. Los CISOs deben comprometerse con las realidades comerciales que enfrentan sus organizaciones en un mercado disruptivo, a la vez que las demás áreas del negocio, desde los Directorios hasta los puestos con menos responsabilidades, se aseguren que la ciberseguridad es bienvenida en la mesa de liderazgo.

## Algunas recomendaciones

Según los hallazgos de la Encuesta Anual de Seguridad de la Información de EY (GISS por sus siglas en inglés) de este año, está claro que actualmente existe una oportunidad real para colocar la ciberseguridad en el centro de la innovación y transformación empresarial. No obstante, esto requerirá que los Directorios, los equipos de alta gerencia, los CISOs y los líderes de las empresas trabajen juntos para:

- 1. Establecer la ciberseguridad como un habilitador de valor clave en la transformación digital** - incorporar la ciberseguridad en la etapa de planificación de todas las nuevas iniciativas. Aprovechar el enfoque de *Security by Design* para navegar por los riesgos en la transformación, el diseño de productos o servicios desde el comienzo.
- 2. Construir relaciones de confianza con todas las áreas de la organización** - analizar los procesos de negocios clave junto con los equipos de ciberseguridad para entender cómo los riesgos cibernéticos los afectarían y cómo puede el equipo de ciberseguridad ayudar a mejorar la función de negocios que los rodea.
- 3. Implementar estructuras de gobierno que se ajusten al objetivo** - desarrollar un conjunto de indicadores clave de desempeño y de riesgo que puedan utilizarse para comunicar una perspectiva enfocada en riesgos en los informes ejecutivos y del Directorio.
- 4. Enfoque en la participación del Directorio** - comunicar de forma sencilla para que el Directorio pueda entender; considerar algún programa de medición de riesgos para comunicar de forma más efectiva aquellos aspectos relacionados con la ciberseguridad.
- 5. Evaluar la efectividad de la función de ciberseguridad para capacitar a los CISO con nuevas competencias** - determinar las fortalezas y debilidades de la función de ciberseguridad con el fin de entender lo que los CISO necesitan y la forma de hacerlo.

La encuesta de este año se concentró en la función evolutiva de la ciberseguridad y se divide en tres secciones:

# 1

## Un fallo sistemático de comunicación en la organización

El aumento de atacantes activistas (los cuales son la segunda fuente más común de violaciones graves o significativas según este informe) destaca la forma cómo la función de ciberseguridad necesita ser entendida en todos los niveles gerenciales de la empresa. No se puede gerenciar lo que no se conoce. El desdén por la seguridad de información de algunas gerencias motiva conductas en los colaboradores que propician el incremento de riesgos de ciberseguridad. Aquellos CISOs que no mantengan comunicación fluida para la coordinación de actividades conjuntas de prevención y mitigación de riesgos de ciberseguridad, no podrán cumplir con su labor. Pero la comunicación es en ambos sentidos, en consecuencia, las áreas de la organización deben también propiciar esta comunicación y trabajar conjuntamente en la prevención y respuesta de riesgos de ciberseguridad en el diseño de productos y en la operación diaria.

Hallazgos de la Encuesta Global de Riesgos del Directorio de EY mostraron la disrupción tecnológica como la mayor oportunidad estratégica para las organizaciones. El hecho de que muchas organizaciones estén aprovechando esta oportunidad para innovar y propiciar una transformación tecnológica, no puede ignorar los riesgos a la ciberseguridad asociados a esta disrupción y nuevas tecnologías. La cultura de *Security by Design* supone que todas las iniciativas comerciales y operativas consideren factores de riesgo de ciberseguridad los cuales puedan ser analizados por el CISO y entendidos por el Directorio y el *C-Suite* en la empresa.

- ▶ Las amenazas cibernéticas y de privacidad están aumentando y expandiéndose. Aproximadamente 6 de cada 10 organizaciones (59%) han enfrentado algún incidente significativo o grave en los últimos 12 meses y, según lo muestra nuestra Encuesta Global de Riesgos del Directorio, el 48% cree que los ataques cibernéticos y la violación de datos tendrán un impacto más que moderado en su negocio en los próximos 12 meses. Cerca de una quinta parte de estos ataques (21%) son causados por *hacktivistas* (es decir, activistas sociales, políticos, tecnológicamente capacitados), teniendo el segundo lugar después del crimen organizado (23%).
- ▶ Solo el 36% de las organizaciones afirmó que incluyen la ciberseguridad desde el inicio de la etapa de planificación de las nuevas iniciativas de negocio.
- ▶ Los gastos en cuanto a la ciberseguridad son impulsados por prioridades defensivas en lugar de la innovación y transformación: 77% de los gastos en nuevas iniciativas se enfocan en los riesgos o el cumplimiento en lugar de las oportunidades.
- ▶ Uno de cada cinco encuestados gasta 5% o menos de su presupuesto en apoyar nuevas iniciativas.

Global

Latam

36% 32%

Incluye al área de ciberseguridad desde la etapa de planificación en sus nuevas iniciativas empresariales

# 2

## Crear y mantener relaciones que aumenten la confianza y la colaboración

*Security by Design* es un concepto que considera la ciberseguridad desde el diseño de productos y servicios para clientes, o cambios en la infraestructura operativa de la empresa. Esta consideración previene la ocurrencia de problemas serios y reduce el costo en correcciones; además, el entendimiento en el Directorio motiva a las gerencias que lo apliquen y esto nutra el trabajo del CISO. La concienciación de todos es constante para entender las amenazas a la ciberseguridad y su evolución en el tiempo. *Security by Design* implica proteger la empresa, proteger los clientes y protegerse con terceros. Desarrollar iniciativas diferentes sin considerar los riesgos de seguridad de información, seguridad informática, o ciberseguridad es atentar contra la estabilidad del negocio.

Para crear y mantener relaciones de confianza con el Directorio y el *C-Suite*, el CISO debe entender el negocio y los riesgos de ciberseguridad que lo afectan, de manera de tener conversaciones en lenguaje de riesgos de negocio. El CISO debe demostrar conocimiento y capacidad de gestión. El Directorio y el *C-Suite* deben propiciar ambos la creación y mantenimiento de relaciones con el CISO. Esto es necesario para la sostenibilidad del negocio.

- ▶ 74% de las organizaciones dijeron que la relación entre la ciberseguridad y marketing, en el mejor de los casos, es neutral, desconfiada o inexistente; 64% dijo lo mismo sobre el equipo de investigación y desarrollo; y 59% sobre las líneas de negocios. Incluso los equipos de ciberseguridad dieron baja calificación a su relación con el departamento de finanzas, del cual depende la autorización de su presupuesto, donde el 57% de las compañías opinan que no es suficiente para sus iniciativas de ciberseguridad.
- ▶ Cerca de la mitad de los encuestados (48%) dijo que el Directorio todavía no entiende completamente los riesgos de ciberseguridad, mientras que el 43% dijo que el Directorio no entiende bien el valor y las necesidades del equipo de ciberseguridad.
- ▶ La encuesta realizada por EY sobre los Riesgos del Directorio muestra que los directores no confían en el departamento de ciberseguridad de su organización, con 50%, como mucho, diciendo que confían solo hasta cierto punto.
- ▶ Solamente el 54% de las organizaciones incluyen regularmente la ciberseguridad como un tema en la agenda del Directorio.
- ▶ Seis de cada diez organizaciones dijeron que no pueden cuantificar la efectividad de sus gastos en ciberseguridad ante el Directorio.

Global

Latam

**59%** **59%**

Dice que la relación entre la ciberseguridad y las líneas de negocios es inexistente o neutral

La encuesta global realizada por EY sobre los riesgos del Directorio muestra que solo

**20%**

tienen extrema confianza en que las medidas de mitigación de los riesgos de ciberseguridad que se les presentaron pueden proteger a la organización de ataques cibernéticos mayores

# 3

## El CISO como agente de transformación

A través de relaciones más sólidas a nivel empresarial, un mejor entendimiento de las obligaciones comerciales de la organización y la habilidad de anticipar las amenazas cibernéticas en constante evolución, los CISO pueden convertirse en un factor central para la transformación de sus organizaciones.

Deberán tener una nueva mentalidad y nuevas habilidades en áreas como comunicación, negociación y colaboración. Aquellos CISO que se conviertan en poderosos agentes del cambio serán aquellos que, en lugar de decir "no" a las nuevas iniciativas, dirán "sí, pero...".

Contando con el apoyo del Directorio y del *C-Suite*, los CISOs deben orquestar en la organización junto con todas las áreas funcionales acciones concretas que van desde la concienciación, la coordinación, la colaboración, hasta el análisis y síntesis de situaciones diversas con recomendaciones fundamentadas en conocimiento, en análisis operativo, estadístico y financiero. Se convierte en alguien que inspira confianza porque sabe y tiene respuestas a las preguntas difíciles, organiza y dirige, delega y controla.

- ▶ Solo 7% de las organizaciones describiría al departamento de ciberseguridad como un habilitador de innovación; la mayoría escogió términos como “impulsado por el cumplimiento” y “adverso al riesgo”.
- ▶ Cerca de la mitad de las organizaciones (48%) dijo que el impulsor principal de los nuevos gastos es la reducción de riesgos y 29% citó los requisitos de cumplimiento. Solo 9% apunta a la habilitación de nuevas iniciativas de negocios.
- ▶ Seis de cada diez organizaciones no cuentan con un responsable de ciberseguridad que reporte al Directorio o se encuentre a nivel de gerencia ejecutiva.

Global

Latam

7%

4%

Describe al área de ciberseguridad como un habilitador de innovación

Global

Latam

60%

67%

No cuenta con un responsable de ciberseguridad que reporte al Directorio

# 1

*Un fallo  
sistemático de  
comunicación  
en la  
organización*

---



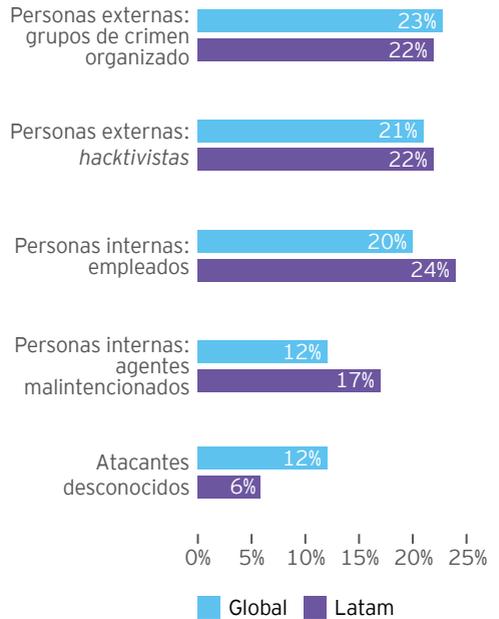
El arresto del activista de Internet, Julian Assange, por parte de la Policía Metropolitana de Londres en abril del 2019 provocó una respuesta furiosa en sus seguidores. En pocas horas, atacantes cibernéticos deshabilitaron el sitio web de la policía y afectaron los sitios web de casi 25 organismos de seguridad asociados.<sup>1</sup> Esto no fue un incidente aislado. En todo el mundo, *hacktivistas* utilizan los ataques cibernéticos como un arma contra las organizaciones, desde empresas hasta gobiernos, a las que se oponen.

La encuesta GISS de este año destacó esa tendencia. No solo se trata del aumento significativo en la cantidad de ataques destructivos que las organizaciones encuestadas enfrentan (aunque esto es bastante serio: 59% dijo que estos ataques se han vuelto más frecuentes en los últimos 12 meses, incluyendo 34% que reportaron un aumento de más de 10%), sino también del cambio del tipo de infractores. De acuerdo con las organizaciones encuestadas, los *hacktivistas* han lanzado más ataques que cualquier otro grupo, aparte de los del crimen organizado.

La amenaza de activistas ilustra uno de los desafíos que enfrentan los CISO. Después de combatir por muchos años las amenazas causadas por agentes malintencionados tradicionales (como el fraude, robo de datos o propiedad intelectual) y adaptarse a las técnicas de dichos atacantes (poner en peligro los correos electrónicos empresariales y el *ransomware* como ejemplos principales), las funciones de ciberseguridad ahora tienen que proteger a sus organizaciones de atacantes con motivaciones mucho más diversas. Por ejemplo, considere a un CISO que no se ha dado cuenta que las inversiones en minería de carbón que realiza su organización, o su registro sobre derechos humanos o divulgaciones sobre uno de sus ejecutivos, lo dejan en la mira de los *hacktivistas*. A menos que colaboren con sus colegas más allá de la función de ciberseguridad, los CISO son más propensos a no ver estas debilidades y, por lo tanto, las amenazas.

Figura 1

### Actores detrás de las brechas confirmadas



<sup>1</sup> *Hactivistas* atacan los sitios web de la policía del Reino Unido para protestar por el arresto de Julian Assange, DataBreaches.net, abril del 2019.

“No nos encontramos necesariamente por delante de la amenaza ya que no estamos construyendo la parte interna de la ciberseguridad”, explica Kris Lovejoy, Líder de Ciberseguridad de EY Global. “En el área cibernética, nos hemos enfocado en contrarrestar aquellas amenazas pensadas para robar datos, accesos y propiedad intelectual con el fin de obtener ganancias financieras. Ahora, debemos pensar en la ciberseguridad de forma muy diferente y protegernos de aquellas campañas realizadas por agentes con argumentos que requieren un nivel distinto de integración del negocio”.

En la actualidad, los equipos de ciberseguridad enfrentan una tormenta sin precedentes. En medio de crecientes ataques destructivos, incluidos los causados por activistas agresivos y bien organizados, los CISOs que están lejanos al negocio al que sirven y que no tienen la confianza de los demás colegas de la organización, tienen cada vez menos esperanza de proporcionar la protección requerida. Por esta razón, la seguridad y los CISOs deben evolucionar y pasar de ser tecnólogos introvertidos a socios continuos del negocio.

## La ciberseguridad todavía es una idea de último momento

La evidencia que nos deja el GISS de este año es que esta evolución (pasar de ser tecnólogos introvertidos a socios continuos del negocio) aún está por desarrollarse en muchas organizaciones. Crucialmente, solo el 36% dijo que su equipo de ciberseguridad está involucrado correctamente desde el inicio de una nueva iniciativa de negocios, es decir, siendo parte del proceso de planificación de los nuevos proyectos en lugar de empezar su participación solo como parte del equipo de diseño o incluso más adelante del proceso.

En otras palabras, muchos equipos de ciberseguridad trabajan para el negocio en lugar de hacerlo como parte del negocio. El resultado es que, en lugar de *Security by Design*, donde la ciberseguridad es una consideración central desde el comienzo de cada nuevo proyecto, la función se encuentra constantemente actualizando la protección, lo cual, a menudo, lleva a ofrecer soluciones imperfectas, costosas y poco prácticas.

En la era de transformación digital en la que nos encontramos, donde las organizaciones constantemente renuevan sus productos, servicios, procesos operativos y estructuras organizacionales, esto no es suficiente.

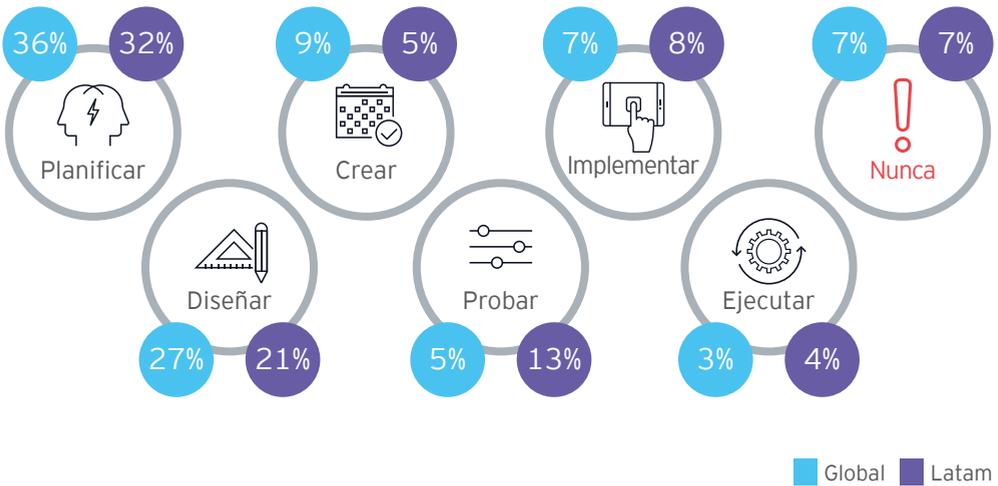
Actualmente nos encontramos en un ambiente en el que la tecnología evoluciona muy rápido; se están implementando iniciativas empresariales junto con estas nuevas capacidades habilitadoras de tecnología para que así las compañías puedan seguir siendo competitivas. Si la seguridad continúa siendo una idea de último momento, entonces siempre estaremos rezagados ante las amenazas.

Ahora que los activistas utilizan los ataques cibernéticos y la transformación empresarial impulsa la agenda corporativa, los equipos de ciberseguridad deben ir más allá del papel reactivo y defensivo que han tenido en el pasado. Solo involucrándose en la organización podrán integrar la agenda de seguridad en los programas de transformación digital desde el inicio y así anticiparse a la gran variedad de atacantes que podrían afectar la operativa del negocio.

Aquellas compañías que vemos triunfar han tenido un verdadero enfoque dedicado a impulsar programas de integración, velocidad y consistencia. Por lo contrario, a las que vemos fallar les ha faltado integración, simplificación y enfoque.

Figura 2

¿Cuándo los equipos de ciberseguridad se unen a las nuevas iniciativas de negocios?



An underwater photograph showing a diver in a black wetsuit and mask on the right, holding a black plastic basket. On the left, the head and open mouth of a shark are visible, swimming towards the diver. The water is clear blue, and the seabed is sandy with some green seagrass.

Global

Latam

86% 81%

Dice que la prevención de crisis y cumplimiento siguen siendo los impulsores principales para aumentar el presupuesto de ciberseguridad

## Las organizaciones están gastando en el negocio como siempre, no en nuevas iniciativas

Actualmente, las prioridades de gastos de muchas funciones de ciberseguridad muestran que hay mucho trabajo por hacer para incorporar la cultura de *Security by Design*. Ahora mismo, la mayoría (60%) de organizaciones afirman que donde hay un enfoque adicional y un gasto en ciberseguridad, se debe a la preocupación por el riesgo.

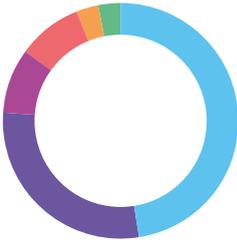
Al pedirles que identificaran las nuevas iniciativas empresariales o tecnológicas que están impulsando nuevos gastos, la regulación y los riesgos obtuvieron las calificaciones más altas. Aunque la transformación digital puede estar en el radar del 14% de las organizaciones, pocas destacan las tecnologías emergentes como un área de enfoque. Por ejemplo, a pesar de las muy publicitadas preocupaciones en los medios con respecto a las exposiciones que podrían causar los dispositivos conectados, solo 6% señaló las iniciativas relacionadas con el Internet de las cosas (IoT) como un impulsor de los nuevos gastos en ciberseguridad. A medida que la inteligencia artificial influye cada vez más en la forma cómo las organizaciones toman decisiones, ejecutan sus operaciones y se comunican con sus clientes, solo 5% mencionó aumentar su enfoque en dicha inteligencia.

La Figura 3 sugiere que los gastos de muchas funciones de ciberseguridad tienen un gran peso hacia los negocios como de costumbre, en lugar de hacia nuevas iniciativas. Cerca del 17% de las organizaciones gastan 5% o menos de su presupuesto de ciberseguridad en nuevas iniciativas; 44% gasta menos del 15%.

Figura 3

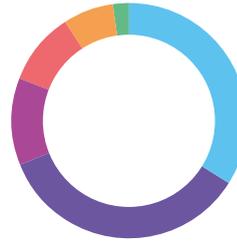
### Justificación para incrementos en el presupuesto de ciberseguridad

#### Global



- 48%** Reducción de riesgos (abordaje de amenazas emergentes)
- 29%** Requisitos de cumplimiento nuevos o cambiantes
- 9%** Crisis (por ej., incumplimiento)
- 9%** Habilitación de nuevas iniciativas de negocios
- 3%** Reducción de costos
- 3%** Otro

#### Latam



- 34%** Reducción de riesgos (abordaje de amenazas emergentes)
- 35%** Requisitos de cumplimiento nuevos o cambiantes
- 12%** Crisis (por ej., incumplimiento)
- 10%** Habilitación de nuevas iniciativas de negocios
- 7%** Reducción de costos
- 2%** Otro

Los CISO tampoco están necesariamente preparando y equipando sus funciones para futuros desafíos. La mayoría de las organizaciones (51%) que participaron en este informe gastan más de la mitad de sus presupuestos de ciberseguridad en operaciones; más de un tercio (43%) actualmente dedican menos de un cuarto de sus gastos en proyectos de capital e inversiones a largo plazo. Mientras tanto, en sectores más grandes como el capital privado, las organizaciones anticipan el aumento de la adopción tecnológica para realizar eficiencias operativas y el crecimiento y conocimiento del mercado (en la Encuesta global sobre capital privado de EY, por ejemplo, 75% de los CFO presionan a sus equipos a invertir más tiempo y aprovechar más la tecnología).

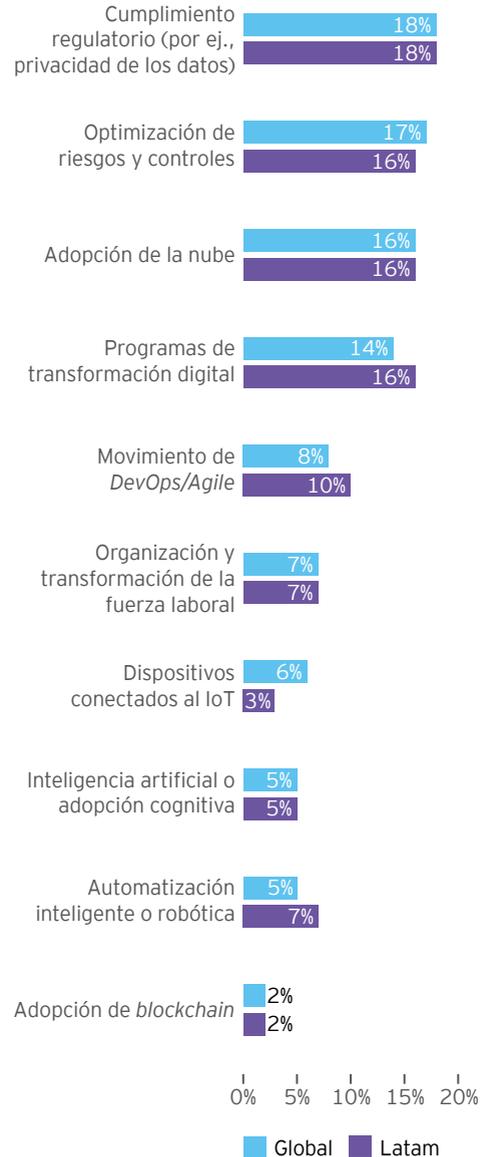
Lo que sorprende ahora es la existencia de tecnología que puede ser empleada directamente por las áreas usuarias, las cuales muchas veces contratan a terceros para servicios complementarios. Esto representa a la vez el progreso y la anarquía. Con innovaciones tecnológicas dirigidas a clientes con éxito y con posibles riesgos de ciberseguridad y privacidad de datos no atendidos se puede en un instante destruir la reputación de la empresa.

Es por esta razón que las gerencias comerciales, de ventas y de operaciones deben ser conscientes de los riesgos de seguridad de información y ciberseguridad; deben interactuar con el CISO y con el CIO para encontrar la viabilidad de la idea y operativizarla de una manera segura y sostenible.

No se puede tolerar la ignorancia y la omisión de los temas de seguridad de información y ciberseguridad en la marcha de los negocios y la construcción del futuro. Todos deben conducirse demostrando entendimiento de las bondades y riesgos de la tecnología de información y la transformación digital.

Figura 4

Uso del presupuesto para ciberseguridad



## Los CISOs deben prepararse para un nuevo rol

No será fácil llevar a cabo un cambio radical. Después de todo, las funciones de ciberseguridad continúan enfrentando cargas de trabajo significativas que requieren compromisos con las operaciones; y junto con la nueva necesidad de enfrentar una gama más amplia de atacantes y apoyar la innovación y la transformación, los desafíos más comunes no han desaparecido: los atacantes continúan apuntando a los datos de las organizaciones, y particularmente a los datos de sus clientes, lo que conlleva riesgos de reputación y regulatorios.

Muchas organizaciones todavía luchan para detectar y rechazar las violaciones de seguridad. Mientras que el 72% de los encuestados detectó su brecha más significativa de los últimos 12 meses en un mes, 28% dijo que les tomó más tiempo descubrir el problema y que son más vulnerables en algunas áreas que otras. Treinta y nueve por ciento (39%) de las organizaciones dijo que es probable que no detecten algún ataque de *malware*.

Por tanto, los CISOs deben evolucionar, madurar, y crecer para que su trabajo sea eficaz tanto para su aporte en el negocio como con la seguridad de información y ciberseguridad.

Crear confianza con el resultado de su trabajo siendo reconocido por las gerencias y el Directorio en su rol. La proactividad, innovación y conocimiento del CISO propiciará estar a la altura de las exigencias de la transformación en su organización y la respuesta a evolución de las amenazas.

Defender la organización y habilitar el cambio no es una tarea mutuamente excluyente: sin embargo, no es algo que dependa solo del CISO. Está basada en el trabajo colaborativo del CISO con las gerencias y con el Directorio. El entendimiento de los riesgos de seguridad de información y ciberseguridad propiciará la seguridad en el diseño, la prevención, detección y respuesta frente a brechas e incidentes: es una tarea conjunta y una responsabilidad operativa del CISO y una responsabilidad política de la Gerencia General; toda la organización debe estar alineada.

Al contar con una comprensión del negocio y los retos que enfrenta, el equipo de ciberseguridad estará en mejores condiciones de trabajar con las gerencias funcionales y anticipar conjuntamente nuevas amenazas y riesgos. Podrán responder con anticipación y mitigar riesgos de una manera más efectiva.

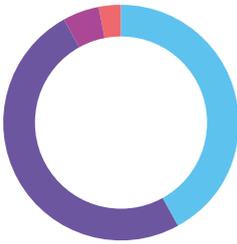
De esta manera el CISO será reconocido por el Directorio y por las gerencias en la organización por su sapiencia y proactividad; podrá orquestar iniciativas propias de su área y conjuntas con otras de la organización haciendo un trabajo efectivo y eficaz.

Ciberseguridad orquestada se convierte en tarea de todos.

Figura 5

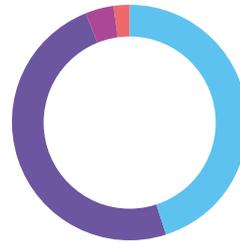
¿Cómo se percibe el nivel de compromiso del Directorio? Aprobando, gestionando y presupuestando los programas de medidas de la ciberseguridad

Global



- 42% Completamente involucrado
- 50% Involucrado de alguna forma
- 5% Ninguna participación
- 3% No lo sé

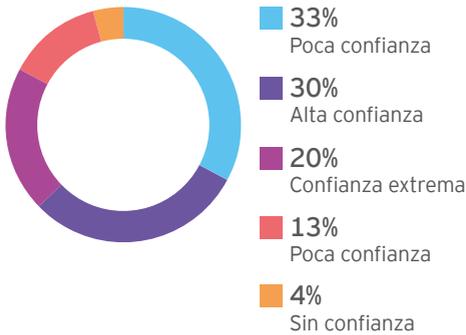
Latam



- 45% Completamente involucrado
- 49% Involucrado de alguna forma
- 4% Ninguna participación
- 2% No lo sé

Figura 6

**Grado de confianza del Directorio con respecto a la habilidad de su organización para protegerse de ataques cibernéticos graves**



Fuente: Encuesta global sobre los riesgos del Directorio de EY

Global	Latam
<b>59%</b>	<b>67%</b>

Ha experimentado un incidente significativo realizado por los empleados en los últimos 12 meses

Global	Latam
<b>14%</b>	<b>16%</b>

Del presupuesto de ciberseguridad es usado para programas de transformación digital

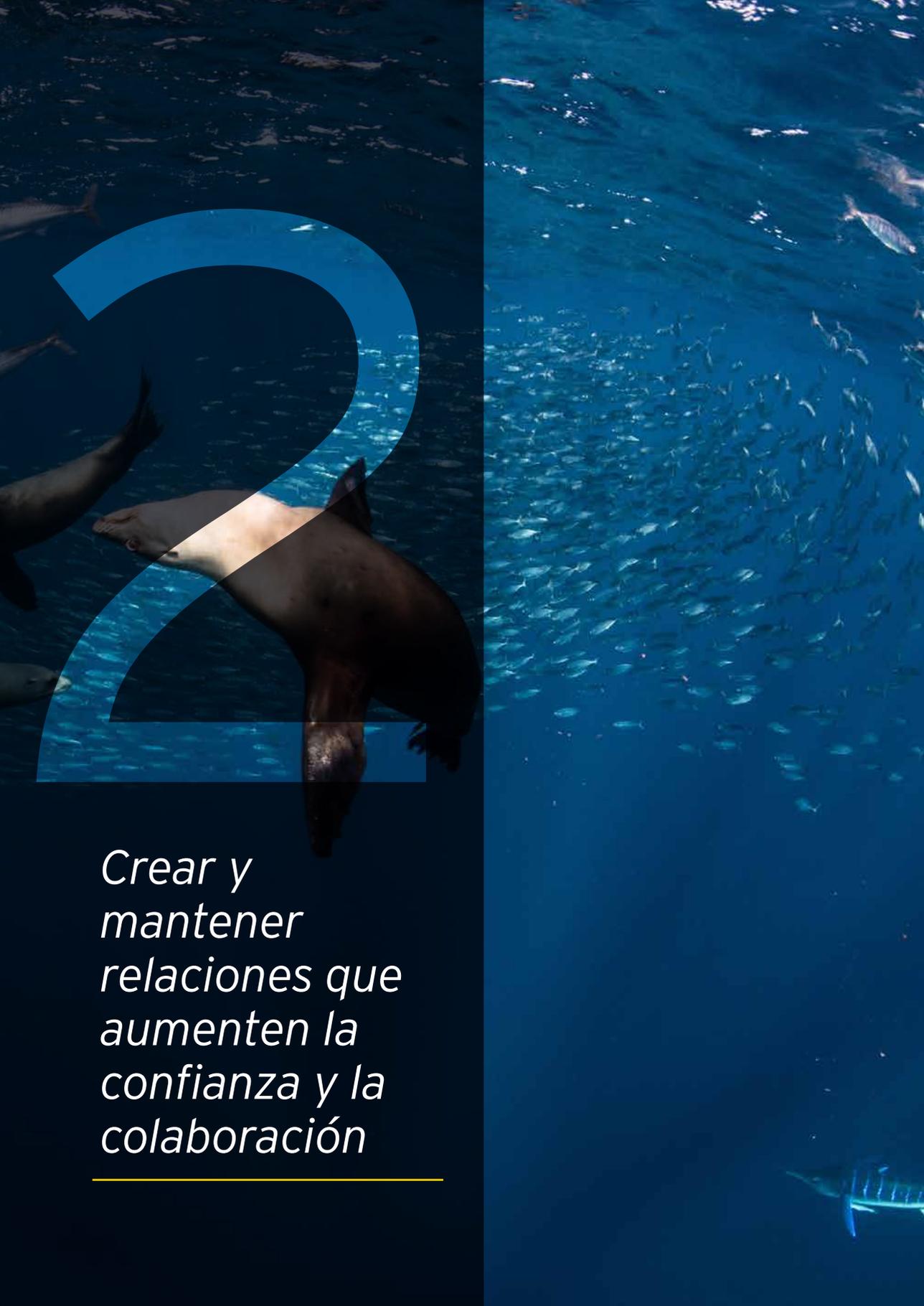
Global	Latam
<b>92%</b>	<b>94%</b>

De los Directorios están involucrados en la dirección y estrategia de ciberseguridad

y solo el

Global	Latam
<b>4%</b>	<b>7%</b>

Tiene extrema confianza en las medidas de mitigación de ataques cibernéticos



*Crear y  
mantener  
relaciones que  
aumenten la  
confianza y la  
colaboración*

---

Muchas organizaciones sienten que sus funciones de ciberseguridad están estancadas. Esto se puede deber a varios factores, entre ellos, la falta de contratación de recursos para esta función, ausencia de presupuesto de capacitación y herramientas, y el no entendimiento de la organización de lo que hace el CISO y por qué es importante. Por otro lado, el CISO puede no tener competencias o capacidades necesarias para desempeñar su papel y conectar con la organización.

Lo más serio es la falta de entendimiento y atención de la organización en todo nivel de lo que representa la seguridad de información y la ciberseguridad y porqué es importante. Si no hay este entendimiento no puede haber una relación real con el CISO, confianza en su trabajo, o un trabajo colaborativo. Una relación implica conocerse entre las partes y buscar objetivos comunes.

### ¿Por qué la colaboración es tan crucial?

Un imperativo es llegar a las funciones de todo el negocio para trabajar más de cerca que nunca. Según la Figura 7, actualmente, el equipo de ciberseguridad de muchas organizaciones tiene poca o ninguna relación con otras funciones clave, especialmente aquellas involucradas en las actividades de innovación, desarrollo de productos y servicio al cliente.

Casi dos tercios (74%) de las organizaciones dijeron que la relación entre ciberseguridad y marketing no es mejor que neutral y, en muchos casos, la describen como desconfiada o inexistente. Cerca del 64% dijo lo mismo sobre la relación de la función con los equipos de desarrollo de productos e I&D. Solo cuando se refiere a las funciones de TI, riesgos y legal es donde el papel tradicionalmente defensivo e impulsado por el cumplimiento de ciberseguridad se ajusta mejor; un número significativo de empresas describe la relación como confiable y cooperativa (ver Figura 7). En muchas empresas, aun la relación con finanzas es difícil, con más de un cuarto de los encuestados que la describen como desconfiada o inexistente.

Sin la confianza y el apoyo de la gerencia general y la organización en su conjunto, la misión del CISO termina siendo limitada y su rol cuestionado. Solo se pueden crear relaciones de confianza si ambas partes deciden iniciar esta relación y sostenerla sobre la base de comunicación abierta, entendimiento de las amenazas de ciberseguridad por la gerencia, y por el CISO conocimiento y capacidad de gestión e integración con la organización. Sin estas relaciones de confianza mutua la ciberseguridad no será considerada oportunamente en las iniciativas de negocio, no podrá estar a la altura de las circunstancias anticipando las amenazas en el mercado y la respuesta frente a éstas.

Por esta razón, las relaciones entre el CISO y la organización en su conjunto son vital. Los mejores CISOs han logrado un entendimiento profundo del negocio, lo que les permite analizar y navegar los riesgos de ciberseguridad durante el desarrollo de iniciativas del negocio. Para que sea sostenible en el tiempo, el CISO y la organización deben mantenerse comunicados y actualizados sobre la evolución del negocio y la ciberseguridad.

Se trata de una inversión clave del CISO en la creación de capacidades y competencias que le permitan construir y mantener relaciones de confianza y el apoyo de la gerencia en sus iniciativas. Estas capacidades le permitirán contribuir de manera efectiva con el desarrollo del negocio y la mitigación de riesgos de ciberseguridad. Mientras que el 20% de los encuestados dijo que asocian la función con la idea de proteger a la empresa, solo 7% estuvo de acuerdo con que la función "habilita la innovación con confianza".

El cambio de esta percepción demanda por un lado la concienciación de la organización a todo nivel sobre los riesgos de ciberseguridad y su impacto en el negocio. Por otro lado, la evolución del CISO a partir de la asimilación de capacidades y competencias que le permitan crear una relación de confianza sobre la base de conocimiento, credibilidad y resultados. De otra manera la organización quedará expuesta riesgos que puedan atentar contra sus clientes y su reputación. Ganarse el respeto de todos es una necesidad del CISO hoy.

Global

Latam

54% 43%

Incluye regularmente temas de ciberseguridad en la agenda del Directorio

## Crear compromiso del Directorio a través de una mejor comunicación

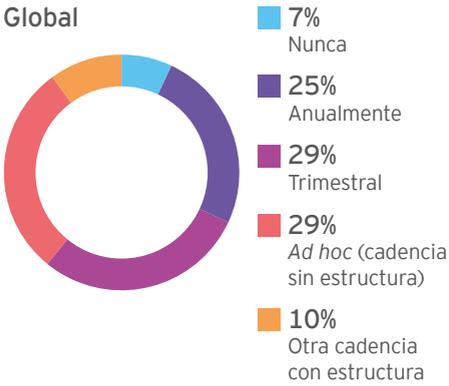
Estas relaciones multifuncionales no son los únicos vínculos en los que debe trabajar el equipo de ciberseguridad: muchas empresas también han informado acerca de la desconexión entre los Directorios y la función de ciberseguridad. Esto genera preocupación debido a que dicha desconexión socava la habilidad de la ciberseguridad para conectarse mejor con otros departamentos: si el Directorio no respalda a la función de ciberseguridad, tampoco lo hará ninguna otra área del negocio. Ellas también serán una amenaza para la habilidad de los CISOs de asegurar los recursos que necesitan.

Uno de los mantras de la ciberseguridad siempre ha sido: 'El Directorio no nos entiende'. En realidad, los altos funcionarios en la mayoría de organizaciones sí reconocen parcialmente la amenaza, pero este reconocimiento no permite la asignación de recursos necesarios para la labor del CISO y su equipo, limitando sus capacidades. Sin el apoyo de altos funcionarios, el CISO termina actuando en respuesta a incidentes sin poder anticiparlos.

Figura 7

### ¿Cada cuánto tiempo la ciberseguridad está en la agenda del Directorio?

#### Global



#### Latam

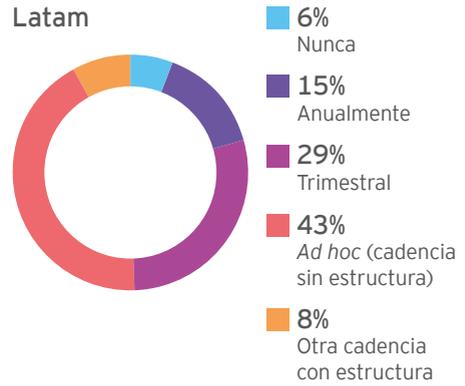
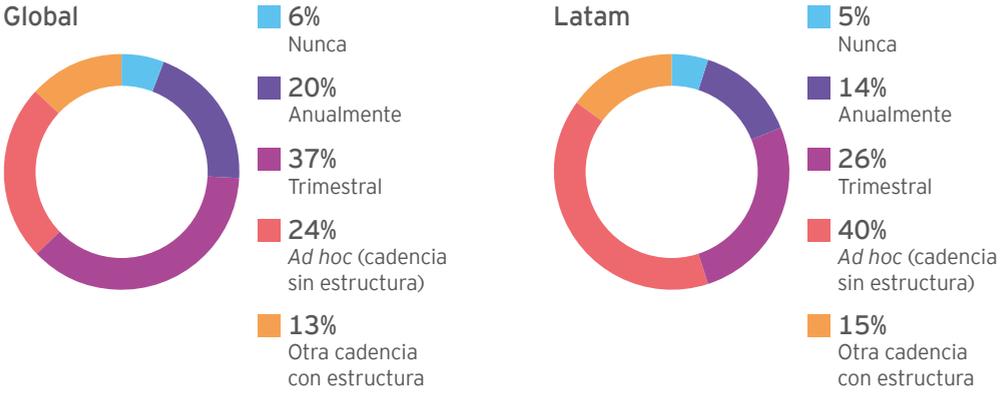


Figura 8

¿Cada cuánto tiempo la ciberseguridad está sujeto a un subcomité o auditoría del Directorio?



El problema no está en que los Directorios no reconozcan la importancia de comprometerse con la ciberseguridad. De hecho, una investigación realizada por EY mostró que actualmente los CEO creen que los ataques cibernéticos corporativos y nacionales son la mayor amenaza que la economía mundial enfrentará en los próximos 10 años<sup>2</sup>. Por su parte, el GISS de este año reveló que 72% de las organizaciones aceptan que los Directorios perciben a los riesgos cibernéticos como algo “significativo”. Desde la perspectiva de los Directorios, éstos esperan que los riesgos cibernéticos tengan un impacto significativo en sus empresas en los siguientes 12 meses: 50% de los directores indicaron esto en los hallazgos tempranos de la Encuesta Global realizada por EY sobre los Riesgos del Directorio.

En cambio, se trata de la comprensión del tema por parte del Directorio. Solo 48% de los encuestados respondió que el Directorio y equipos de gerencia ejecutiva comprenden que deben evaluar completamente los riesgos cibernéticos y las medidas que están implementando para defenderse de ellos. De manera similar, 42% se quejó acerca de que el Directorio no comprende bien el valor del equipo de ciberseguridad y sus necesidades.

¿Cómo puede el Directorio y la Gerencia General tomar decisiones sobre cosas que no conoce? Como ha ocurrido en diversas empresas, es posible que este tema sea mejor comprendido cuando la empresa sufra eventualmente un problema serio que la afecte tanto que no quiera repetirlo nunca más.



Global	Latam
32%	32%

De los líderes de ciberseguridad utilizan el tiempo con el Directorio para discutir temas futuros que impulsen cambios

<sup>2</sup> Cómo la ciberseguridad se convirtió en la amenaza número uno para la economía global de los CEO, EY, octubre del 2019.

¿De qué manera las organizaciones pueden mejorar esta situación? Una tarea importante para los CISO es pensar más detalladamente acerca de la forma cómo se comunican con el Directorio. Por ejemplo, solo 25% de los encuestados dijo que pueden cuantificar, en términos financieros, la efectividad de sus gastos de ciberseguridad para abordar los riesgos que el negocio enfrenta. La Encuesta global realizada por EY sobre los Riesgos del Directorio sugiere que solo 20% confía en gran manera en que el equipo de ciberseguridad es efectivo. No sorprende porqué muchos CISO luchan para asegurar los recursos que necesitan.

Muchos de ellos se preocupan porque su Directorio no tiene ninguna estructura para revisar los riesgos cibernéticos. Solo 54% de las organizaciones incluyen regularmente la ciberseguridad como un tema de la agenda del Directorio, y solo 57% incluye regularmente este tema en la agenda de uno de los sub-comités. Esto podría ser un síntoma de la forma cómo la función de ciberseguridad elige comunicarse con el Directorio, es decir, se enfoca en el estatus de la seguridad, los resultados de auditoría, entre otros, en lugar de enfocarse en el desempeño o la innovación (ver Figura 9).

Figura 9

**¿Qué reportan los CISOs al Directorio?**

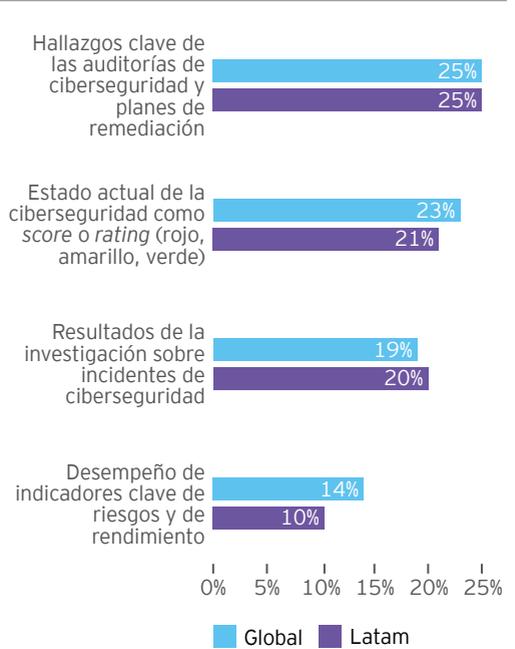
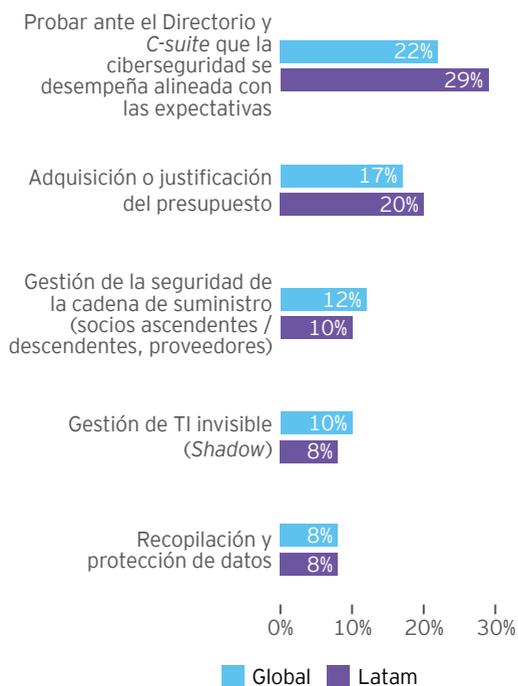


Figura 10

### Desafíos apremiantes de la ciberseguridad



Global Latam

**25%** **25%**

Son capaces de cuantificar en términos financieros, la efectividad de gastos en ciberseguridad





Ante la falta de una conversación más profunda con el Directorio y los equipos gerenciales con respecto al valor que tiene la ciberseguridad, es muy probable que no se logre un mayor compromiso de parte del negocio.

Muchos CISOs mencionan que el aspecto más desafiante de su función es asignar el valor de lo que hacen y asegurar el presupuesto que consideran necesario (ver Figura 10). Para muchos, esto es mucho más difícil que gestionar la seguridad, sobre todo cuando se trata de tecnologías y nuevas amenazas.

Kris Lovejoy, Líder de Ciberseguridad Global de EY, cree que esta es otra razón para reformular la mentalidad sobre la ciberseguridad: “¿En qué gastan su dinero las funciones de ciberseguridad? Lo gastan en la mitigación de riesgos y optimización de controles de riesgos y controles. ¿A quién le presentan sus informes? A menudo, lo hacen al comité de auditoría. ¿Qué es lo que están entregando al comité de auditoría? Entregan resultados de *benchmarking* con respecto a su estado sobre la optimización de riesgos y controles”, afirma.

“La forma en que hemos organizado la ciberseguridad es como una función retrospectiva, cuando es capaz de ser una función prospectiva y de valor agregado. Cuando la función de ciberseguridad hable el idioma del negocio, dará el primer paso crítico para ser escuchada y entendida. Comenzará a demostrar valor porque podrá unir directamente los impulsores de negocios con lo que la ciberseguridad hace para habilitarlos, justificando sus gastos y efectividad. Esto ayudará a que se consoliden relaciones positivas fuera de las líneas tradicionales, y cambie la conversación de ‘¿por qué no podemos?’ a ‘¿cómo podemos?’ Esto mueve el debate de la reducción de riesgos a la innovación”.

Figura 11

La experiencia en la industria y las calificaciones del equipo son el primer factor citado para ayudar a aumentar los niveles de confianza en un proveedor de ciberseguridad

-  Experiencia en la industria, calificaciones del equipo  
Buenas referencias
-  Buena experiencia del cliente  
Términos y condiciones fáciles de entender
-  Información de los productos y servicios fácil de encontrar  
Precios fáciles de entender

### ¿Cuál es la función de los terceros?

¿Pueden los proveedores externos ayudar a los CISOs a mejorar el desempeño de ciberseguridad y acercarse más al negocio? Actualmente, existe cierto escepticismo con respecto al valor que los proveedores de la industria pueden agregar genuinamente. Solo 10% de los encuestados dijo que confía en las afirmaciones de mercadeo de los vendedores de ciberseguridad aunque otro 69% dice que depende del proveedor en cuestión. Casi una cuarta parte dijo que los proveedores fallan por una entrega inconsistente (24%) o en productos y servicios confusos (20%).

No obstante, con tres cuartas partes de las organizaciones utilizando hasta 20 productos o herramientas de ciberseguridad (y algunas que usan aún más), existe un margen para impulsar el rendimiento a través de una colaboración más cercana con un grupo seleccionado de los proveedores de mayor confianza. Los CISOs se enfocan en la experiencia en la industria y el servicio al cliente como cualidades clave.

Según Mike Maddison, líder de ciberseguridad de EY EMEA, “los CISO se preguntan cómo pueden optimizar y simplificar. Una opción es reducir la cantidad de actividades que tienen o traer un tipo particular de proveedores de *software* para así reducir los gastos generales de administración al moverse hacia acuerdos empresariales más amplios para obtener el mayor consumo posible de un proveedor”.

# 3

*El CISO  
como agente de  
transformación*

---

Global

7%

Latam

9%

De los líderes de ciberseguridad tienen la capacidad de cuantificar financieramente el impacto de los incidentes

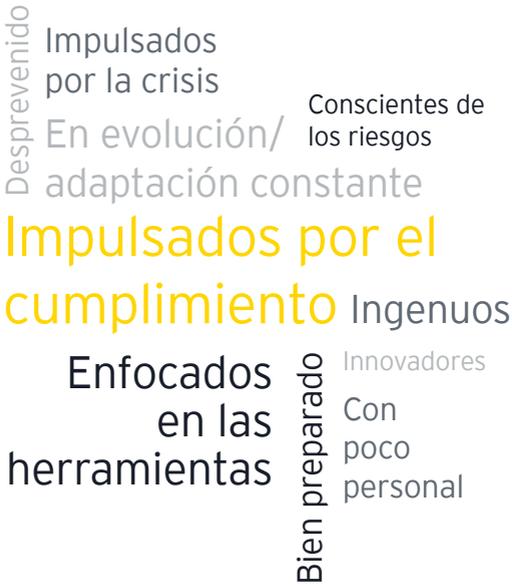
“

Hemos hablado sobre los habilitadores cibernéticos durante algún tiempo, y esta idea será más importante debido al énfasis en la optimización y el crecimiento.

Mike Maddison

Líder de Ciberseguridad de EY EMEA

Figura 12: A las percepciones les falta mucho camino  
**¿Cómo se perciben los CISOs?**



Muchos CISO ahora se encuentran en una encrucijada. Hasta ahora, se han centrado en mejorar las defensas de su organización y protegerla de los ciberatacantes. Ese desafío persiste, pero ahora existe una oportunidad para que los CISO pasen a la vanguardia y se conviertan en agentes de cambio que son figuras cruciales en los esfuerzos de sus organizaciones para transformar sus negocios.

Construirán funciones de ciberseguridad que operarán como habilitadores de innovación y que colaborarán con otras funciones más de cerca de lo que lo han hecho antes. Además, aprovecharán estas relaciones para anticipar las amenazas emergentes y disruptivas en constante cambio causadas por agentes malintencionados con un amplio rango de motivaciones.

Aquellos que no aprovechen la oportunidad verán a sus funciones estancarse cada vez más. “Hemos estado hablando de habilitadores cibernéticos por algún tiempo, y esta idea se ha vuelto más importante debido al énfasis que se le ha dado a la optimización y al crecimiento”, explica Mike Maddison, Líder de Ciberseguridad de Consultoría de EY EMEA. “No obstante, muchas organizaciones realmente están luchando para que los líderes de seguridad den un paso adelante”.

Esta nueva oportunidad creará CISOs muy diferentes, requerirá que toda la función de ciberseguridad se adapte a las nuevas formas de trabajo. Estos importantes cambios valdrán la pena: esta es una oportunidad para que la ciberseguridad se convierta en un socio comercial confiable en el centro de la cadena de valor de la organización, impulsando la transformación y demostrando su valía.

Actualmente, se considera a la industria de la ciberseguridad como impulsada por el cumplimiento, configurada para responder a las crisis y centrada en las herramientas que tiene a su disposición (ver Figura 12). Solo el 13% de los encuestados describe el sector como en constante evolución y adaptación; y aún menos usan la palabra "innovación" al hablar de ciberseguridad.

## El CISO futuro: nuevas habilidades, nuevas estructuras, nuevo estado

Una pregunta importante para los CISOs es si actualmente tienen las habilidades y la experiencia adecuadas para trabajar de esta nueva manera y liderar una función que sea más proactiva y con visión de futuro. Sus considerables habilidades técnicas, obtenidas durante su carrera para gestionar las funciones de ciberseguridad, no serán suficientes. El nuevo rol de CISO requerirá experiencia comercial, fuertes habilidades de comunicación y la capacidad de trabajar en equipo con otras áreas de negocio.

Reconociendo esto, algunas organizaciones ya están contratando más CISOs con una visión más allá de la función de ciberseguridad. Están eligiendo ejecutivos que han servido en otras áreas del negocio, particularmente en roles más comerciales. No será necesario ser tecnólogo para ser un buen CISO. Al final del día, el trabajo consiste en gestionar el riesgo, por lo que los mejores CISOs son los que entienden mejor el lenguaje del riesgo.

Otras organizaciones preferirán seguir con los CISO que tienen antecedentes más convencionales, al mismo tiempo que tratarán de construir procesos organizativos que mejoren las relaciones entre la ciberseguridad, el Directorio, la *C-suite* y el resto del negocio. "Tenemos que ser mentores de la función, así como crear estructuras de gestión y gobierno más formales que permitan que la ciberseguridad se comunique dentro de un contexto empresarial", dice Kris Lovejoy, Líder de Ciberseguridad de EY Global. Esencialmente, necesitamos el lenguaje y los mecanismos para conectar entre esa función, el Directorio, la *C-suite* y otras funciones.

El cambio se puede resumir sucintamente en tener que pasar de un CISO que dice 'no' a uno que dice 'Sí, pero...' En otras palabras, los CISO no pueden permitirse ser vistos como bloqueadores de la innovación; deben ser identificados como quienes solucionan problemas: habilitadores que promueven *Security by Design* y permiten que sus organizaciones se transformen de manera segura.

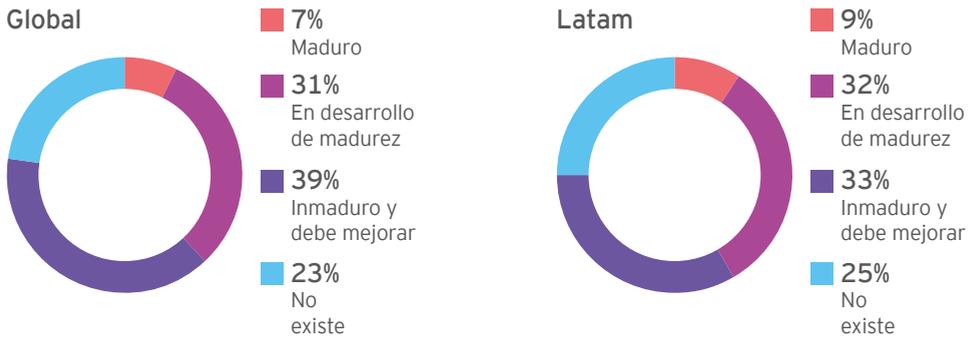
Sin embargo, dado que los CISO contemplan este tipo diferente de función, ¿son adecuadas las estructuras de informes de hoy para su propósito? Actualmente, solo el 36% de los CISO se sienta en el Directorio de su organización u opera como miembros del equipo de gerencia ejecutiva. Si el trabajo del CISO se va a ampliar, y las relaciones más estrechas con los líderes superiores y otras funciones comerciales se vuelven más vitales, es posible que más organizaciones necesiten elevar el estatus del rol del CISO.

Tomando las estructuras de reportes: los encuestados nos dicen que los CISOs tienen más probabilidades de reportar al CIO de la organización. Esto podría dejar a la ciberseguridad a un paso del resto del negocio, y el CIO deberá actuar como un conductor.

Eso tendrá que cambiar si la ciberseguridad va a desempeñar un papel habilitador en la transformación empresarial, con estas organizaciones siguiendo el ejemplo del 18% cuyo CISO informa directamente al CEO. La pequeña minoría de organizaciones cuyos CISO reportan a áreas de riesgos, finanzas o asuntos legales, podrán notar que estas estructuras ya no funcionan.

Figura 12

¿Los líderes de seguridad (CISOs) tienen las habilidades para cuantificar el impacto financiero de las brechas en la ciberseguridad?



## Caso de estudio

# AXA

Arnaud Tanguy se convirtió en el director de seguridad del Grupo de la compañía de seguros francesa AXA, en octubre de 2018, como parte de una reorganización que reunió a equipos previamente separados responsables de la ciberseguridad, la seguridad física y la capacidad de recuperación operativa como una sola función de seguridad. "Este enfoque integral de la seguridad a nivel mundial refleja que las amenazas también están convergiendo".

La reorganización no solo ha puesto a la función de seguridad en una posición más sólida para proteger el negocio y sus clientes, sino que también le ha permitido jugar a un nivel estratégico. Entendemos el negocio y estamos cerca de él, pero eso no es suficiente. Somos parte de una empresa que está trabajando para transformar la experiencia de nuestros clientes. Estamos aquí para que demuestren que somos seguros y resistentes en un mundo competitivo. La convergencia de nuestra función nos permite pensar en la seguridad de manera integral: aplicar *Security by Design* en todo lo que hacemos.

Este rol habilitador está respaldado por una estrecha relación entre los equipos de seguridad de AXA y los principales líderes de la compañía. El director de seguridad del grupo reporta directamente al director de operaciones del grupo, el cual forma parte del comité de administración de AXA. "Esto significa que la seguridad es parte de las decisiones estratégicas de AXA", agrega Arnaud. "Realmente, estamos aquí para apoyar la estrategia del grupo, enfocándonos en nuestros clientes en una compañía liderada por la tecnología para proteger nuestro negocio".

**Arnaud Tanguy**  
Director de Seguridad del  
Grupo AXA

## Señales alentadoras, pero aun con barreras

La ciberseguridad no puede cumplir su potencial para agregar valor si se mantiene a distancia del resto de la organización. Las organizaciones que realmente presionan por esa participación proactiva de la seguridad verán beneficios comerciales muy significativos tanto a corto como a largo plazo.

Existen algunos signos alentadores. Por ejemplo, el 50% de las organizaciones dicen que están articulando el riesgo cibernético, y su tolerancia al riesgo, en el contexto del riesgo comercial u operativo. Dos tercios (67%) de las organizaciones esperan que la función de seguridad proporcione gobierno a medida que se desarrolla la nueva propiedad intelectual; solo un poco menos (61%) dice lo mismo de las tecnologías operativas.

Esto es prometedor, pero las organizaciones encontrarán obstáculos cuando intenten integrar la ciberseguridad con otras funciones.

La asignación del presupuesto, en particular, puede representar un desafío. En muchas organizaciones, el presupuesto para la ciberseguridad ya se deriva de varias fuentes, incluido el dinero de otras líneas de negocios y funciones comerciales. Casi un tercio de los encuestados (32%) dice que su presupuesto proviene de más de una fuente, y es probable que esto crezca a medida que aumenta la colaboración. ¿Quién debería ser responsable de controlar esos fondos? Casi las tres cuartas partes (68%) de las organizaciones dicen que hay un "propietario" centralizado de abastecimiento y desembolso, pero esta será una pregunta que se mantendrá en el tiempo.

Se trata de cuestiones estructurales y operativas que deben sopesarse en lugar de ser consideradas barreras importantes para una nueva forma de trabajar. Los beneficios de una mayor integración tanto para el negocio como para la ciberseguridad superan estos obstáculos y deberían persuadir a las organizaciones para que hagan todo lo posible para resolverlos.

## ¿Los Centros de Operaciones de Seguridad (SOC en inglés) son adecuados para el objetivo requerido?

El GISS de este año considera que el desempeño de los SOC de muchas organizaciones han sido decepcionante. Los encuestados informan que gastan el 28% de sus presupuestos de ciberseguridad en sus SOC y asignan el 27% del tiempo de los empleados para operarlos; sin embargo, solo el 26% dice que su SOC identificó su brecha más significativa en los últimos 12 meses.

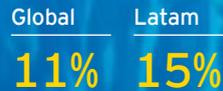
Esto podría deberse a que muchas organizaciones continúan operando con SOC de primera generación que requieren importante intervención manual, en particular dada la renuencia (o incapacidad) para invertir en pruebas a futuro. Actualmente, solo el 19% del presupuesto se destina a arquitectura e ingeniería. ¿Están los SOC reteniendo las funciones de ciberseguridad?

Los SOC que operan con tecnologías estandarizadas son reactivos en su enfoque y altamente manuales, y dependen del ojo humano para detectar anomalías. La próxima generación de SOC tienen casos de uso comunes, como la remediación de *phishing*, automatizada. Son de naturaleza proactiva y utilizan *analytics* para detectar anomalías. Están basados en la nube y están diseñados específicamente para el cliente al que sirven.

Eso significa que actualizar el SOC ahora podría generar dividendos significativos. No solo mejorará la capacidad de la organización para identificar amenazas e infracciones, sino que también liberará recursos a través de una mayor automatización. Las organizaciones que pueden reducir la cantidad de tiempo requerido por los empleados para operar los SOC pueden redistribuir al personal de ciberseguridad en actividades comerciales.

## #1

La categoría en ciberseguridad que tiene más asignación de presupuesto es el SOC en Latinoamérica y a nivel mundial



De las infracciones fueron detectadas por un SOC en los últimos 12 meses



# Ciberseguridad en tiempos de COVID en Latinoamérica

---

Si bien nuestra encuesta de Seguridad de la Información hace mención a algunas iniciativas de ciberseguridad en las compañías, la actual pandemia de COVID-19 está poniendo a prueba las formas de trabajo que conocíamos hasta hace algunas semanas. Estamos frente a una gran ejecución de trabajo a distancia y con ello surgen una serie de alteraciones a protocolos ya establecidos dentro del espectro seguro que significaba trabajar desde una oficina, conectados a una red segura, monitoreada normalmente por el área de sistemas o por alguna otra área de control. Nos referimos a los ciberataques, un escenario bastante peligroso que enfrentamos, hoy más que nunca, en casa u oficina.

## Una amenaza latente en plena pandemia

El COVID-19 nos trajo un duro golpe de realidad, haciéndonos conscientes de lo vulnerables que somos y de lo rápido que pueden cambiar las circunstancias en nuestro entorno, sin embargo, no es la única pandemia o riesgo potencial que tenemos por delante.

La dependencia de la tecnología ha ido en aumento en los últimos años, pero ha sido vital en los últimos meses. El confinamiento impuesto por el COVID-19 en varios países, además del uso de plataformas digitales, ventas en línea, seguimiento del estado de salud de empleados y terceros, y el regreso a una nueva normalidad, ha provocado que centros de monitoreo de seguridad en áreas afectadas hayan cerrado, comprometiendo la seguridad de varias compañías. Este es el escenario ideal para que los ciberdelincuentes lancen sus ataques y comprometan la seguridad de los datos confidenciales, así como la continuidad operativa de las organizaciones. Sabiendo que hoy en día estamos a la expectativa de toda nueva información sobre la pandemia, los ciberdelincuentes, disfrazados de representantes de la Organización Mundial de la Salud (OMS), envían actualizaciones falsas de correo electrónico a los usuarios y roban información confidencial. Lamentablemente en la mayoría de los casos somos reactivos frente a la ciberdelincuencia.

Por otro lado, las organizaciones, empresas y personas se enfrentan día a día a una amplia gama de ciberamenazas y ciberataques cada vez más evolucionada y compleja de detectar, contener y resolver. Es claro ver que el cibercrimen se ha vuelto una de las actividades más lucrativas en los últimos años, incrementándose exponencialmente.

Los cibercriminales están aprovechando la situación sin mostrar escrúpulos. Están tomando ventaja sobre personas y organizaciones que se enfrentan a condiciones nunca vistas, que han llevado a las empresas a reaccionar en forma improvisada y muchas veces descuidada para ofrecer continuidad a sus operaciones de negocio. Establecer un enfoque holístico es lo primero que debe entender toda organización en este proceso para combatir los ataques cibernéticos. Aquí listamos 10 pasos que pueden ser implementados por las compañías para enfrentar la ciberdelincuencia:

1

Integrar la ciberseguridad en la estrategia de talento.

2

Definir claramente las responsabilidades de ciberseguridad en su organización.

3

Establecer protocolos de ciberseguridad y confirmar de manera periódica su cumplimiento.

4

Asegurarse que la ciberseguridad esté en el corazón de la innovación digital de la empresa.

5

Comprender cómo la regulación afecta su negocio global y trabajar con los reguladores, ya que ellos también quieren un sector de servicios sólido.

6

Evaluar el riesgo de todos los activos clave y determinar un enfoque de protección para cada uno, con prioridad en los más críticos.

7

Desarrollar un modelo dinámico y ágil de gestión de riesgo de ciberseguridad para permitir a la organización crecer de manera ordenada.

8

Integrar el *compliance* en su estrategia de ciberseguridad, de modo que cualquier dinero invertido devuelva valor al negocio proporcionando una defensa adecuada para la organización.

9

Fortalecer la resiliencia teniendo un área de gestión de crisis y comunicaciones que pueda ser implementada y practicada en todos los niveles de la organización.

10

Colaborar con sus pares para buscar más soluciones intrasectoriales; los riesgos cibernéticos actuales amenazan a todas las industrias y no solo al sistema financiero, y la falla de un jugador clave podría dañar la reputación de toda una industria.

## El Centro de Operaciones de Ciberseguridad de EY

Estos pasos deben estar integrados en un programa de seguridad y protección de datos adecuado las condiciones de cada empresa para poder enfrentar efectivamente esta ciberamenaza creciente; como un sistema inmunológico, donde sus diferentes componentes trabajen en forma orquestada para poder prevenir, detectar, responder y recuperarse ante los diferentes tipos y formas de ciberataques o vulneraciones.

Un Centro de Operaciones de Ciberseguridad se establece como el corazón del sistema de ciberdefensa. Sin embargo, su implementación requiere no solo una gran inversión en tecnología, sino contar con habilidades especializadas y experiencia para responder efectiva, preventiva y proactivamente ante los riesgos en materia de ciberseguridad.

A inicios de este año, inauguramos en México el decimosexto Centro Avanzado de Ciberseguridad EY a nivel mundial, con el objetivo de ayudar a las empresas en el monitoreo, la detección, respuesta y recuperación ante ciberamenazas y así proteger efectivamente sus activos críticos de negocio.

Hoy que la confianza es más importante que nunca, el CiberSOC de EY ofrece a las organizaciones protección diferenciada basada en ciberinteligencia y tecnología de punta para detectar oportunamente amenazas y saber responder de forma efectiva y orquestada, basada en analítica e inteligencia artificial. La tecnología del centro permite identificar y anticipar la materialización de un ataque y responder a estos de la forma más efectiva en el menor tiempo para lograr reducir su impacto en la organización.

Con este nuevo recurso, EY pretende poner al servicio de la región conocimiento, tecnología y estrategia de un equipo que globalmente, día a día, busca comprender mejor los riesgos tecnológicos de las organizaciones y en consecuencia trabajan sin descanso por estar un paso más adelante que los principales grupos de crimen cibernético.



## México:

### Una nueva superficie de riesgos

Para los mexicanos, hablar de pandemia no es un tema nuevo, pero tampoco es que estén acostumbrados a sobrellevarlas. La pandemia que se vive hoy en día inició como una alarma a la que varios gobiernos no pusieron mucha atención y las medidas tomadas en su momento no eran suficientes para enfrentar la situación actual.

El país tomó medidas de confinamiento con su programa “quédate en casa”, incentivando que las personas permanecieran en sus hogares, y salieran exclusivamente a labores de vital importancia. Es aquí donde el teletrabajo toma vital importancia. México, es uno de los países líderes<sup>3</sup> en relación con el teletrabajo, según algunas cifras, llegó a ocupar el segundo puesto como país en la implementación del teletrabajo con cerca del 30% de los trabajadores en esta modalidad o con permiso para trabajar bajo esta modalidad.

Sin embargo, esta situación de confinamiento nos tomó por sorpresa a todos, y México al igual que otros países tuvo que empezar a funcionar de una manera diferente; los modelos de ciberseguridad de las organizaciones, en el mejor de los casos, tuvieron que adaptarse al cambio, en otros, la rigidez del modelo de ciberseguridad establecido no permitió más opción que asimilar el riesgo y aceptar que su modelo era poco o nada flexible.

El país no ha sido invulnerable ante los ciberataques, según Banxico<sup>4</sup>, en abril de este año, México sufrió un ataque por ransomware, que según reportes no generó pérdidas económicas, pero sí evidenció que los atacantes están a la vuelta de la esquina esperando que su presa se adapte a la nueva normalidad y se establezcan los nuevos escenarios de amenazas para cada una de las organizaciones.

Teniendo al enemigo al acecho, las organizaciones de toda la región, y de México en este caso, deben más que nunca adaptarse a la nueva normal de una manera coordinada, estratégica y flexible que permita tener en cuenta las nuevas fronteras y los nuevos escenarios de amenazas a los que se verá expuesta la información de las organizaciones; un escenario donde más que nunca las áreas de ciberseguridad jugarán un papel estratégico y pasarán a tener mayor visibilidad en Directorio y *C-Level* de las organizaciones, además que se volverán no sólo habilitadores de las estrategias digitales sino habilitadores de la operación bajo la nueva normal.

No se puede decir que sea el momento de la ciberseguridad, pero sí se puede decir que ciberseguridad pasará a tener gran protagonismo en la operación de las organizaciones, pasará de ser el “NO” ante muchas iniciativas, a ser el proponente de los nuevos modelos de operación ante la nueva normal.

El mundo anticipaba las vulnerabilidades en seguridad como una amenaza por el paso acelerado con el que ocurrían la evolución tecnológica y la globalización; hoy la pandemia global acentúa esta realidad y plantea con carácter de urgencia el movimiento del foco de atención hacia el cuidado de la seguridad de la operación y de los datos a nivel mundial.

---

<sup>3</sup> <https://teletrabajo.gov.co/622/w3-article-27303.html>

<sup>4</sup> <https://www.banxico.org.mx/sistema-financiero/seguridad-informacion-banco.html>

## Colombia: Sacando lo mejor de lo inesperado

Hay muchas mejoras que se plantean desde el esquema de teletrabajo, pero sin duda, estos esquemas no son del gusto de muchas organizaciones; sin embargo, ante las situaciones que se han venido presentando por el confinamiento, muchas se vieron obligadas a permitir que sus trabajadores ejecutaran el trabajo de manera remota; y en algunos casos de manera más improvisada que otras.

Para algunas organizaciones fue simplemente que sus empleados empezarán a trabajar desde sus equipos de cómputo en sus casas, y eso fue lo que se imaginaron en primera instancia, pero empezaron a aparecer amenazas y riesgos colaterales sobre los activos de las organizaciones; redes WiFi compartidas con otros dispositivos o servicios, situaciones en la cuáles se debió emplear el equipo personal para poder acceder y manipular la información de la organización y finalmente, las herramientas de videoconferencia o chat, que antes no estaban contempladas en el modelo de riesgos de la organización porque simplemente el esquema de teletrabajo no estaba previsto dentro de las normales de la organización.

Ante esta situación es momento para que las organizaciones replanteen y actualicen su modelo operativo, y esto nos lleva a que el modelo de ciberseguridad de las organizaciones pase de ser estático a dinámico y mucho más proactivo que reactivo. Tradicionalmente los modelos de ciberseguridad son estáticos, esto quiere decir que funcionan y mantienen su eficiencia debido a que en todo momento saben dónde están las joyas de la corona, y sobre éstas hacen sus esfuerzos

de control y ante los cambios de patrones se activan las alertas. La situación que se está viviendo, evidencia que estos modelos deben ser más flexibles que nunca. Empezando porque las joyas de la corona pueden estar en cualquier lugar y en cualquier momento, y eso lo saben las organizaciones, y los atacantes.

Ante esta omnipresencia de la información, los modelos de ciberseguridad, deben adaptarse a esa nueva normalidad, y tener en cuenta que el modelo de operación no volverá a ser estático; por el contrario, será más dinámico que nunca, y muchas organizaciones aprenderán que podrán seguir operando, de manera segura y confiable, sin tener a sus trabajadores confinados en un espacio físico; además, podría ser el momento de plantearse varias interrogantes, ¿es más eficiente la organización en esquema de teletrabajo?, ¿cómo puedo ayudar a que ciberseguridad se convierta en un habilitador del teletrabajo en las nuevas fronteras y bajo la nueva normal?

Será muy interesante conocer las respuestas a las anteriores interrogantes y observar cómo la nueva normal obligará a las organizaciones y a sus modelos de ciberseguridad a transformarse en elementos más dinámicos y resilientes.

## Perú:

### Primeros pasos hacia una ciberseguridad robusta

La ciberseguridad en el Perú está empezando a ser considerada en los diferentes sectores de la industria, ya no solo para el sector financiero. Esto como consecuencia de los incidentes que se vienen suscitando a nivel mundial tales como ataques continuos y la posibilidad de ver afectadas las operaciones de las compañías, lo cual representa una oportunidad y un reto importante en las actuales circunstancias.

Es así que, las partes interesadas como Directorios y comités de gerencia, han considerado las amenazas reales para ponerse a trabajar de manera efectiva en la búsqueda de soluciones apropiadas que les permita estar mejor preparados, sobre todo en esta época de pandemia. Se están empezando a aplicar medidas de control efectivas, para anticiparse a incidentes que afecten la continuidad de sus operaciones, los cuales forman parte de un programa o plan de ciberseguridad formal que les permitirá actuar de manera apropiada.

Con este liderazgo se han venido ejecutando proyectos en algunas compañías con la finalidad de determinar el grado de madurez en el cual se encuentran y realizar las mejoras y adecuaciones requeridas para proteger la información de clientes, productos y servicios que usan en el ciberespacio.

Respecto a los ciber-riesgos, también se vienen reforzando los aspectos metodológicos para incorporar en las matrices correspondientes las referidas a este contexto, con una orientación a incorporar de manera integral en la agenda de trabajo del año en curso, reformulando los ya existentes.

Adicionalmente, los profesionales de la comunidad de negocios se encuentran capacitando de manera constante en modelos y marcos de trabajos considerados buenas prácticas que les permitan aplicar las acciones apropiadas en sus organizaciones, de tal manera de manejar este proceso de manera ordenada y que les permita uniformizar las medidas a adoptar.

En general, en el país se vienen incrementando de manera gradual los planes e iniciativas de ciberseguridad, adecuando las estrategias de negocio y preocupándose de los impactos que puede generar el no tomar acción oportuna.

## Chile: Enfrentando importantes transformaciones

Chile, como país, ha enfrentado un escenario complejo en los últimos 10 meses, iniciándose con el estallido social del 18 de octubre de 2019, el cual ha condicionado la economía, la seguridad y, de forma significativa, la productividad y el comercio. Si bien, apenas se lograron establecer acuerdos transversales a nivel social, el país debió enfrentar un nuevo desafío en marzo de este año con la pandemia de COVID-19, por la cual las autoridades adoptaron medidas para su control que incluyeron diferentes herramientas y estrategias basadas en el equilibrio entre la salud pública y la actividad económica.

En el ámbito de privacidad se ha discutido bastante sobre la facultad de las organizaciones para compartir los datos de los contagiados por COVID-19 y hacer uso de la información para aplicar políticas públicas y estrategias de protección a la ciudadanía por parte de las alcaldías, contando con la negativa del gobierno para su utilización.

Por otro lado, las medidas de confinamiento que se han establecido para la población han generado una alta demanda en el comercio electrónico, compras *online* y *delivery*, los cuales han tenido que enfrentar el gran desafío de abastecer a toda la demanda en tiempo y ha puesto a prueba la efectividad de los procesos de atención a clientes de forma remota. Adicionalmente, se han registrado casos de estafas por medio de ingeniería social ya sea mediante la utilización de técnicas de *phishing* o *pharming*, suplantaciones de identidad y vulneración de apps para servicios bancarios, entre otros.

Desde la mirada de las empresas, el confinamiento obligó a trasladar la operación de sus colaboradores a la modalidad de teletrabajo y se encontraron con diversos escenarios de riesgo. Para ello, las organizaciones se vieron con el reto de proveer accesos remotos a su personal de manera significativa, debiéndose priorizar la operación de sus recursos por sobre los niveles

seguridad exigidos. Adicionalmente, la exposición de información desde los hogares ciertamente es un ambiente menos controlado que su red interna y sus respectivas capas de protección. Hoy, las empresas deben confiar en la “seguridad” de cada hogar, ya sea a en configuraciones de seguridad establecidas por los proveedores de servicio de internet y a las herramientas de protección para sus propias estaciones de trabajo.

Todos estos escenarios están develando cuáles de los planes de respuesta ante incidentes y de continuidad han sido efectivos, versus los que no obtuvieron los resultados esperados. Esto ha generado que las empresas tengan que reevaluar sus procesos para fortalecerlos pensando que este nuevo escenario llegó para quedarse por largo tiempo.

En materia política, hubo ciertos avances, como la aprobación de la ley 21.220 que modifica el código del trabajo en materia de teletrabajo y trabajo a distancia. También el Gobierno estableció convenios de colaboración con el objetivo de intercambiar información relativa a alertas, amenazas e incidentes de seguridad informática y cooperar en la prevención y detección de incidentes de ciberseguridad<sup>5</sup>. El tema que aún queda por resolver es poder contar con una legislación robusta en materia de protección de datos personales. Creemos que el escenario actual pone presión a esta necesidad y esperamos que en el corto plazo el borrador de la ley vea la luz y pueda ser reglamentado.

A la fecha, no podemos negar que los desafíos han sido bastantes y que hay mucho trabajo por realizar, sin embargo, creemos que, para avanzar en estos nuevos escenarios, es necesario poder ver el estado actual de nuestra seguridad de la información, proyectarnos en el futuro para establecer un camino de prioridades que podamos lograr de acuerdo a los recursos disponibles para mitigar los riesgos.

<sup>5</sup> <https://www.csirt.gob.cl/noticias/gobierno-y-sector-privado-reafirman-compromiso-con-la-ciberseguridad>

## Centroamérica: Trabajando en una nueva normal sin siquiera estar preparados

Gran parte del tiempo de las áreas de ciberseguridad de las organizaciones se emplea en diseñar, desarrollar y poner en operación un modelo de ciberseguridad, muchas veces sin los recursos requeridos y de manera reactiva antes que proactiva. Así mismo, los ejecutivos en las organizaciones están empezando a tener un cambio importante pasando de un modelo donde ciberseguridad es visto como un gasto, a un modelo en el que es visto como un habilitador estratégico en las transformaciones digitales. En este sentido los equipos deben enfocarse en ser más estratégicos, de tal manera que se puedan anticipar a los nuevos modelos de amenazas a los que se ven expuestas las iniciativas digitales y que en gran medida pueden impactar las organizaciones.

Sin embargo, por más estratégico que pueda ser, se presentan eventos para los cuáles no se tenían antecedentes y no se estaba preparado; este año, un evento nos llevó a un confinamiento que impacta a la humanidad y a las economías de todos los países; un evento para lo cual no habían modelos establecidos dentro de las organizaciones y que llevó a éstas a activar sus modelos de resiliencia de manera masiva y en algunas ocasiones improvisadamente para poder soportar la continuidad del negocio por medio de esquemas de teletrabajo.

Por ejemplo, el teletrabajo, apenas estaba pasando de ser algo más que una palabra comúnmente usada a la práctica bajo esquemas regulados; algunos datos de teletrabajo en Centroamérica nos indican que desde septiembre de 2019 Costa Rica cuenta con la ley de teletrabajo<sup>6</sup>, con

la cual el gobierno buscaba reducir al menos 60 toneladas de emisiones de CO<sub>2</sub>, 350.000 litros de combustible y mitigar el ajetreteado transporte de 1100 automóviles diarios en San José. Otros países como Guatemala<sup>7</sup> y Panamá<sup>8</sup> han presentado recientemente las iniciativas de legislación del teletrabajo en abril y febrero de este año respectivamente.

La mezcla de las situaciones antes descritas y la incertidumbre que aún se tiene sobre la pandemia obligó a las compañías a poner a prueba su modelo de ciberseguridad ante la nueva normalidad, enfrentándose a nuevos escenarios de amenazas que no estaban dentro de la ecuación de operación y ante las cuales debieron adaptarse. Pasando de un modelo naturalmente inflexible a un modelo que funcionara fuera de las fronteras físicas de la organización.

Con base en lo anterior, ¿será interesante saber cómo las cifras de operación en teletrabajo cambiarán? ¿cómo la nueva normalidad cambiará la estrategia? y ¿cómo sobre estos cambios se plantearán los nuevos modelos de ciberseguridad? Sin lugar a duda, las siguientes ediciones del presente estudio serán de gran valor y contarán mejor esta historia aún por escribir.

<sup>6</sup> [http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm\\_texto\\_completo.aspx?param1=NRTC&nValor1=1&nValor2=89753](http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=89753)

<sup>7</sup> <https://elperiodico.com.gt/nacion/2020/04/20/presentan-iniciativa-de-ley-para-regular-la-aplicacion-del-teletrabajo-en-el-pais/>

<sup>8</sup> <https://www.presidencia.gob.pa/Noticias/Presidente-sanciona-ley-que-regula-el-teletrabajo-en-Panamá>

# Conclusiones y siguientes pasos

La Encuesta Global de Seguridad de la Información de EY de este año analiza el progreso realizado por las organizaciones al intentar posicionar la ciberseguridad en el corazón de la transformación empresarial, construida sobre la base de *Security by Design*.

Aquí hay una oportunidad significativa para que los CISO, el Directorio, las *C-suites* y el resto del negocio trabajen juntos para reposicionar la función de ciberseguridad. Las organizaciones que tienen éxito en este esfuerzo pueden garantizar que la función de ciberseguridad se convierta en un agente clave de cambio, permitiendo que la transformación que sus negocios deben experimentar, se mantenga competitiva. Las organizaciones también descubrirán que la ciberseguridad se vuelve más efectiva en su rol defensivo tradicional, capaz de anticipar nuevas amenazas a medida que evoluciona con una comprensión más amplia del riesgo potencial que representan por ejemplo, los *hacktivistas*. Además, con relaciones más fuertes entre el Directorio y los CISOs logrados por un nuevo estilo de reporte y comunicación, las viejas batallas por los recursos y el valor desaparecerán.

Hacer esta transición no es sencillo, ni es igual para todos. Lo que las organizaciones hagan a continuación (sus CISO, el Directorio, *C-suites* y funciones individuales) dependerá del estado actual de sus funciones de ciberseguridad y de las características y objetivos de sus organizaciones. Sin embargo, hay cinco acciones que cada organización puede priorizar para aprovechar al máximo la oportunidad:

## 1

### Evaluar la efectividad de la función de ciberseguridad para capacitar a los CISOs en nuevas competencias

Integrar la ciberseguridad en los procesos comerciales utilizando un enfoque de *Security by Design*. Llevar la ciberseguridad a la etapa de planificación de cada nueva iniciativa empresarial es el modelo óptimo, ya que reduce la energía y el gasto de resolver problemas después del hecho y genera confianza en un producto o servicio desde el principio. Se requiere de la ciberseguridad para ser mucho más integrado y colaborativo.

## 2

### Construir relaciones de confianza con cada área de la organización

Cuando la ciberseguridad está integrada en el negocio, los CISOs estarán en una posición sólida para ayudar a impulsar la innovación y estar mejor informados de las amenazas que enfrenta la organización. Una forma de hacer esto es utilizando los datos existentes para modelar los procesos comerciales y los controles asociados, y se colabora con los CISO para comprender los verdaderos impactos de la ciberseguridad en estos procesos comerciales.

A medida que la evidencia se vuelve clara para todos, las funciones comerciales obtienen una visión en tiempo real de la seguridad de sus procesos y se genera confianza. Los CISOs obtienen visibilidad sobre posibles riesgos y amenazas adicionales, y cómo ayudar a la empresa a controlar o innovar alrededor de estos.

## 3 Implementar estructuras de gobernanza que sean aptas para el propósito

---

Los Directorios y líderes del *C-suite* deberían considerar las líneas de reporte, el control del presupuesto y la rendición de cuentas para reflejar el nuevo rol de la ciberseguridad en el corazón de la innovación. Una vez establecido, se deberían desarrollar los indicadores clave de desempeño y de riesgos que serán usados para comunicar una vista centrada en el riesgo, en los reportes al Directorio.

## 4 Enfocarse en la participación del Directorio

---

Es vital que las organizaciones desarrollen estructuras de informes y formas de cuantificar el valor de la ciberseguridad que sea comprendido por el Directorio. Un paso clave es implementar un programa de cuantificación de los riesgos cibernéticos para comunicarlos de manera más efectiva y en términos comerciales al Directorio.

## 5 Evaluar la efectividad de la ciberseguridad para capacitar a los CISOs en nuevas competencias

---

Los líderes de ciberseguridad deben tener sentido comercial, la capacidad de comunicarse en un lenguaje que comprenda la empresa y la voluntad de encontrar soluciones a los problemas de seguridad en lugar de decir "no". Esto comienza con la comprensión de las fortalezas y debilidades de la función de ciberseguridad para identificar cuánto espacio tiene un CISO para maniobrar. Determinar si los servicios gestionados se están utilizando de manera apropiada para entregar a escala, a un costo competitivo y con resultados efectivos. Evaluar las capacidades de automatización y orquestación para reducir el esfuerzo manual de la función de ciberseguridad y liberarlas para respaldar el negocio de una manera que genere mayor valor agregado.

Los líderes de ciberseguridad deben tener sentido comercial, la capacidad de comunicarse en un lenguaje que comprenda la empresa y la voluntad de encontrar soluciones a los problemas de seguridad en lugar de decir "no".



# Contacto

---



**Marcelo Zanotti**

Socio Consultoría en Riesgo

+56226761147

[marcelo.zanotti@cl.ey.com](mailto:marcelo.zanotti@cl.ey.com)

# 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.



EY | Assurance | Impuestos | Consultoría |  
Estrategia y Transacciones | Legal | Outsourcing

### Acerca de EY

EY es la firma líder 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/cl](http://ey.com/cl)

© 2020 EY  
All Rights Reserved.

### Sobre este informe

La Encuesta Global de Seguridad de la Información de este año se basa en una encuesta de líderes de alto nivel en casi 1.300 organizaciones realizada por EY entre agosto y octubre de 2019.

Esta fue una encuesta global con Europa, Medio Oriente, India y África (EMEIA) que representa el 47% de los encuestados, las Américas, el 29%, y la región de Asia y el Pacífico, el 24%. Los encuestados incluyeron a los CISO o sus equivalentes de todos los sectores de la industria.