Building a better working world

Ciberseguridad: ¿cómo mantenerse a flote en medio de una tormenta?

Encuesta Global de Seguridad de la Información 2021

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

Haz clic en el título para ir directo al contenido

Contenido

	Bienvenida	03
	Introducción	06
01 |	Los CISO en encrucijada	08
02 |	Tres desafíos que detienen a los CISO	13
03 |	Conclusiones y próximos pasos	20
	Acerca de la encuesta	24
	Contactos	25

Bienvenida

Carlos López Cervantes
Socio Líder de Ciberseguridad para Consultoría
EY Latam Norte

Gustavo Díaz Rojas
Socio Líder de Ciberseguridad para Servicios Financieros
EY Latam Norte

Carlos López Cervantes
Socio Líder de Ciberseguridad para Consultoría
EY Latam Norte

Sin lugar a dudas, estamos viviendo uno los eventos más transformacionales en la historia de la humanidad derivado de la pandemia del COVID-19, los retos profesionales y personales que esta situación nos ha generado por la virtualidad que representa la "nueva normalidad", han acelerado de manera exponencial la transformación digital y la evolución de las empresas en esta nueva realidad.

Esta transformación y evolución acelerada está representando que no todos los componentes asociados están siendo cubiertos de manera adecuada. La ciberseguridad es uno de estos componentes, la cual es un factor de riesgo y de oportunidad.

Las organizaciones de todos los tamaños en Latinoamérica deben enfrentar este proceso evolutivo generando confianza en todos sus *stakeholders*, a través de la implementación de medidas eficientes que mitiguen los riesgos asociados a la ciberseguridad y que ayuden a materializar los beneficios de la transformación digital de sus negocios. Los eventos recientes en materia de ataques de ciberseguridad ponen de manifiesto lo urgente de implantar estas medidas.

Gustavo Díaz Rojas
Socio Líder de Ciberseguridad para Servicios Financieros
EY Latam Norte

Como en muchas otras industrias, las entidades del sector financiero están viviendo cambios significativos en su modelo de atención a los clientes, los productos y servicios ofrecidos a los mismos, así como en su modelo operativo y la arquitectura tecnológica que deben tener para soportar su operación.

Estos cambios han sido originados en gran parte por la denominada cuarta revolución industrial que busca la convergencia y aprovechamiento de las tecnologías digitales para mejorar y facilitar el desarrollo de las operaciones de las entidades, con un foco importante sobre la interacción que se tiene con los clientes, con el propósito que la misma sea cada vez más amigable, sencilla, ágil, personalizada y segura.

Por otra parte, la situación actual de la pandemia originada por COVID-19 ha impactado de manera radical la interacción de las entidades del sector financiero con sus clientes, haciendo que la experiencia presencial pierda importancia y la experiencia digital se vuelva un imperativo que marca la diferencia de un buen servicio, lo cual ha acelerado de manera exponencial la agenda de transformación digital que ya venían ejecutando las entidades.

Ahora bien, la introducción de todos estos cambios y la velocidad con que los mismos se están materializando en las entidades ha traído consigo nuevos retos a nivel de procesos, personas y la tecnología involucrada, generando un nuevo panorama de riesgos, para los cuales debemos estar preparados.

En este sentido, es importante mencionar que sí bien los ejecutivos de las entidades del sector financiero son cada vez más conscientes de los riesgos a los que se enfrentan en materia de ciberseguridad. En muchos casos la función de ciberseguridad no cuenta con los recursos y capacidades necesarias para proteger adecuadamente los activos de información que soportan las operaciones de negocio, así como tampoco para responder de manera oportuna a los cambios de los mismos.

Durante el último año hemos sido testigos del aumento significativo de ciberataques contra las organizaciones, que van desde el uso de métodos de ingeniería social, APT, *ransomware* y aprovechamiento vulnerabilidades presentes en sistemas desactualizados, entre otros, los cuales han generado verdaderos dolores de cabeza a las directivas y han retado la capacidad de detección, respuesta y recuperación.

Ante esta situación es importante que las entidades del sector continúen trabajando en el fortalecimiento y consolidación de la estrategia y programa de ciberseguridad pasando de un enfoque reactivo a proactivo basado en modelos flexibles que consideren la ciberseguridad desde el diseño en el negocio, el cual permita proteger de manera apropiada los activos de información críticos y se convierta en un habilitador de la estrategia de negocio.

Introducción

La Encuesta Global de Seguridad de la Información de EY 2021 encuentra a los oficiales de seguridad de la información (o CISO, por sus siglas en inglés) y líderes de seguridad luchando contra una nueva ola de amenazas desatadas por COVID-19.

La Encuesta Global de Seguridad de la Información de EY 2021 (GISS, por sus siglas en inglés) ilustra el impacto devastador y desproporcionado que la crisis ha tenido en una función que se esfuerza por posicionarse como un facilitador del crecimiento y un socio estratégico para el negocio.

A través de una encuesta global a más de 1,400 líderes de ciberseguridad, encontramos a los CISO lidiando con presupuestos inadecuados, luchando con la fragmentación regulatoria y sin encontrar un terreno común con las funciones que más los necesitan.

De hecho, la agitación de la pandemia mundial ha creado una tormenta perfecta de condiciones en las que los agentes de amenaza pueden actuar. Desde el estudio del año pasado, hemos identificado un aumento significativo en el número de ataques disruptivos y sofisticados, muchos de los cuales podrían haberse evitado si las empresas hubieran incorporado *Security by Design* en todo el negocio.

La relación de los CISO con las organizaciones también ha variado al agregar un componente de estrés coyuntural, y la consecuencia es una mayor exposición al riesgo cibernético. Además, las restricciones presupuestarias significan que los CISO están luchando por cerrar la brecha entre la necesidad y la financiación.

Es probable que la situación empeore antes de mejorar. Las organizaciones quieren invertir en tecnología e innovación para la era posterior a COVID, y deben garantizar la resiliencia para la próxima gran interrupción, pero muchos aún tienen que abordar primero los riesgos diferidos y las posibles vulnerabilidades que se introdujeron durante los esfuerzos de transformación en el punto álgido de la pandemia.

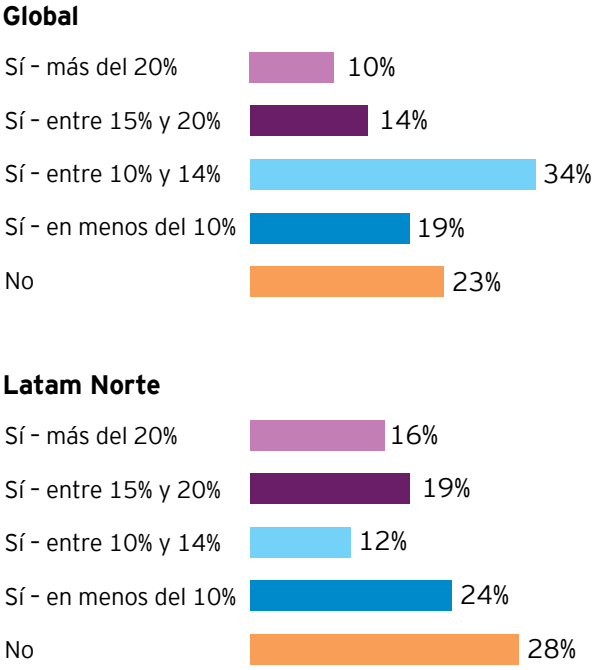
Los CISO se encuentran en una encrucijada. Para lidiar con los problemas complejos y agotadores que enfrentan, deben actuar con rapidez. Nuestro informe describe lo que los líderes en ciberseguridad necesitan saber ahora sobre su entorno operativo y lo que necesitan hacer para transformarlo.

1 Los CISO en encrucijada

Un momento de estrés, cambios y oportunidades

Figura 1: Los encuestados han visto un claro aumento de los ataques desde 2020

¿Ha visto un aumento en el número de ataques disruptivos en los últimos 12 meses?



Durante el último año, todas las organizaciones han tenido que adaptarse a los cambios e interrupciones de una forma u otra. En un intervalo de tiempo que hasta hace poco se hubiera pensado que era imposible, las organizaciones resilientes implementaron nuevas tecnologías orientadas al cliente y herramientas basadas en la nube que respaldaban el trabajo remoto y mantenían abierto el canal hacia el mercado.

Pero la velocidad del cambio vino con un alto precio. Muchas empresas no involucraron la ciberseguridad en el proceso de toma de decisiones, ya sea por supervisión o por la urgencia de moverse lo más rápido posible. Como resultado, nuevas vulnerabilidades ingresaron a un entorno el cual ya se movía rápidamente y continúan amenazando al negocio en la actualidad.

La transformación rápida trae nuevos riesgos

Mientras redactamos este documento, es posible que los CISO y sus equipos aún no hayan completado una evaluación a profundidad del impacto a largo plazo que tendrá la nueva tecnología en sus defensas. Mientras tanto, sus colegas continúan usando la nueva tecnología sin ningún impedimento.

"La urgencia de la crisis significó que se pasó por alto la seguridad cibernética incluso cuando las organizaciones abrían sistemas que nunca antes habían estado abiertos", reflexiona Richard Watson, Líder de Ciberseguridad para Consultoría en EY Asia-Pacífico. "No todas las organizaciones reconocen que ahora deben volver atrás y abordar esos problemas".

Sin embargo, los riesgos de seguir adelante sin evaluar estos problemas son muy reales y cada vez más urgentes. Tres de cada cuatro (77%) encuestados mundiales del GISS de este año advierten que han visto un aumento en el número de ataques disruptivos, como *ransomware*, en los últimos 12 meses. Por el contrario, solo 59% registró un aumento en los 12 meses anteriores (ver figura 1).

> "Me enfoco en entender las implicaciones de las amenazas existentes y desconocidas, y luego agrego velocidad, seguridad y privacidad de diseño en el producto a medida que se construye.

Roland Cloutier
Director Global de Seguridad de la Información de Tik Tok

Global

43%

Latam Norte

57%

está más preocupado que nunca por la capacidad de su empresa para gestionar las amenazas cibernéticas.

Sin embargo, los CISO están luchando por hacerse oír. La mayoría de los encuestados (56%) admitió que los equipos de ciberseguridad no reciben consultas de otras áreas o se les consulta demasiado tarde cuando se toman decisiones estratégicas urgentes. Si bien algunos sostienen que esto no sucede "muy a menudo", solo es necesario que suceda una vez para que los actores de amenazas exploten una falla en las defensas (ver figura 2).

El resultado es ansiedad por lo que depara el futuro. "Nos esforzamos por asegurar la seguridad como un facilitador", dice Richard Watson. "Pero todavía hay organizaciones que lanzan proyectos sin considerar la seguridad antes de ponerlos en marcha".

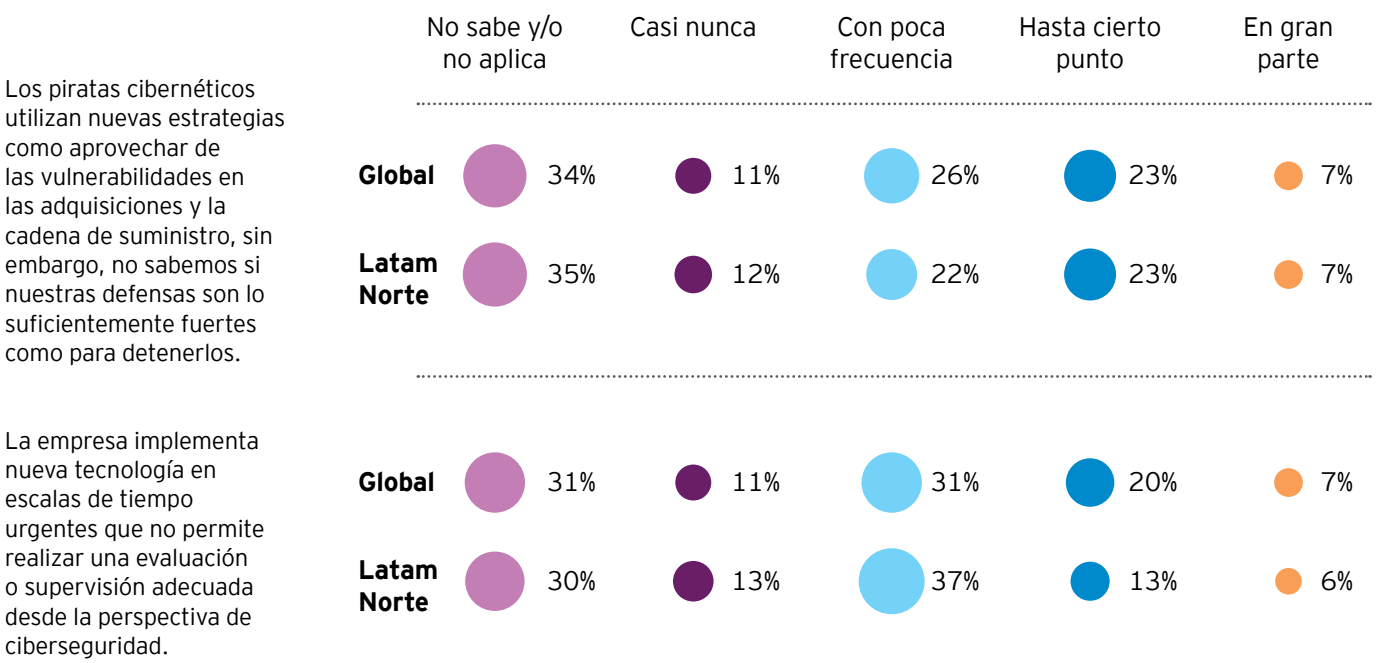
En el peor de los casos, los CISO descubren que sus advertencias son ignoradas. En el GISS de este año, 43% dice que está más preocupado que nunca por la capacidad de su empresa para gestionar las amenazas cibernéticas. Pero no tiene que ser de esta manera.

TikTok: *Security by design*, a gran velocidad

Roland Cloutier, Director Global de Seguridad de la Información en la plataforma de entretenimiento y video de formato corto TikTok, está profundamente involucrado en la toma de decisiones estratégicas de forma iterativa, semana a semana. "Puede variar desde una estrategia para el crecimiento de usuarios hasta un nuevo tipo de monetización o producto musical", dice. "Todos involucran la construcción y distribución de nueva tecnología. Me concentro en comprender las implicaciones de las amenazas existentes y desconocidas, y luego agrego velocidad, seguridad y privacidad por diseño en el producto a medida que se construye. Luego preparo a la organización para la nueva información que llega. ¿Cómo hacemos eso tanto a la velocidad de internet como a la velocidad de la cultura? Eso es lo que hace que este trabajo sea tan divertido ".

Figura 2: Los equipos de ciberseguridad están excluidos de la toma de decisiones en las empresas

¿En qué medida ocurre lo siguiente en su negocio?



Global

47%

Latam Norte

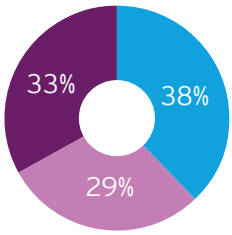
46%

indicó que comprenden y pueden anticipar las estrategias que utilizan los atacantes.

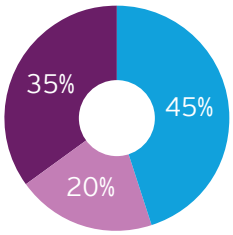
Figura 3: Los CISO carecen de confianza cuando se enfrentan a los causantes de amenazas

¿Qué tan seguro está de las habilidades de su equipo para garantizar que toda la cadena de suministro sea capaz de defenderse contra las amenazas y recuperarse de ellas?

Global



Latam Norte



Me siento seguro

Para nada o no muy seguro

No sabe y/o no aplica

Los atacantes han alcanzado un nuevo nivel de madurez

Durante el último año, los causantes de amenazas han adoptado nuevas estrategias, ya sea dirigiéndose a empresas con campañas de phishing que contienen *software* malicioso que se reenvía por parte de los empleados, o incorporando un código de puerta trasera (*backdoor code*) que les permite explotar el *software* comercial después de que los clientes lo hayan adquirido.

"La realidad es que hoy se manifiestan más amenazas de las que jamás hayamos visto", dice Dave Burg, Líder de Ciberseguridad en EY Americas. "Ha sido impulsado por el modelo de negocio de *ransomware*, que está demostrando ser muy eficaz".

Los riesgos no podrían ser mayores. Los piratas informáticos que cerraron el Oleoducto Colonial de EE. UU. en mayo de 2021 utilizaron *ransomware* como servicio que otros pueden obtener a través de la *dark web*, lo que representa riesgos críticos para las organizaciones. la economía y la sociedad en general. Al mismo tiempo, las personas que se infiltraron en *SolarWinds* durante varios meses en el año 2020, lo hicieron a través de un sofisticado ataque a la cadena de suministro que en gran medida no era familiar para los equipos de seguridad.

Los atacantes tienen como objetivo el crecimiento del alcance de sus ataques y sus tácticas son cada vez más impredecibles. Solo uno de cada tres encuestados confía en su capacidad para hacer que la cadena de suministro sea suficientemente sólida (ver figura 3), lo que destaca la importancia de trabajar en estrecha colaboración con colegas en adquisiciones y operaciones. Menos de la mitad (47%) dice que comprenden y pueden anticipar las estrategias que usan los atacantes, un problema que ha sido ilustrado por incidentes en los que los atacantes se infiltran en el *software* que luego se vende a los clientes.

68% de los gerentes generales globalmente está planeando una importante inversión en tecnología en los próximos 12 meses.

No es que haya pasado la necesidad de una transformación rápida. Mientras se redacta este estudio, se ha logrado un progreso significativo en la contención de COVID-19, pero la crisis pasará por varias etapas antes de que las empresas vuelvan a la "normalidad".

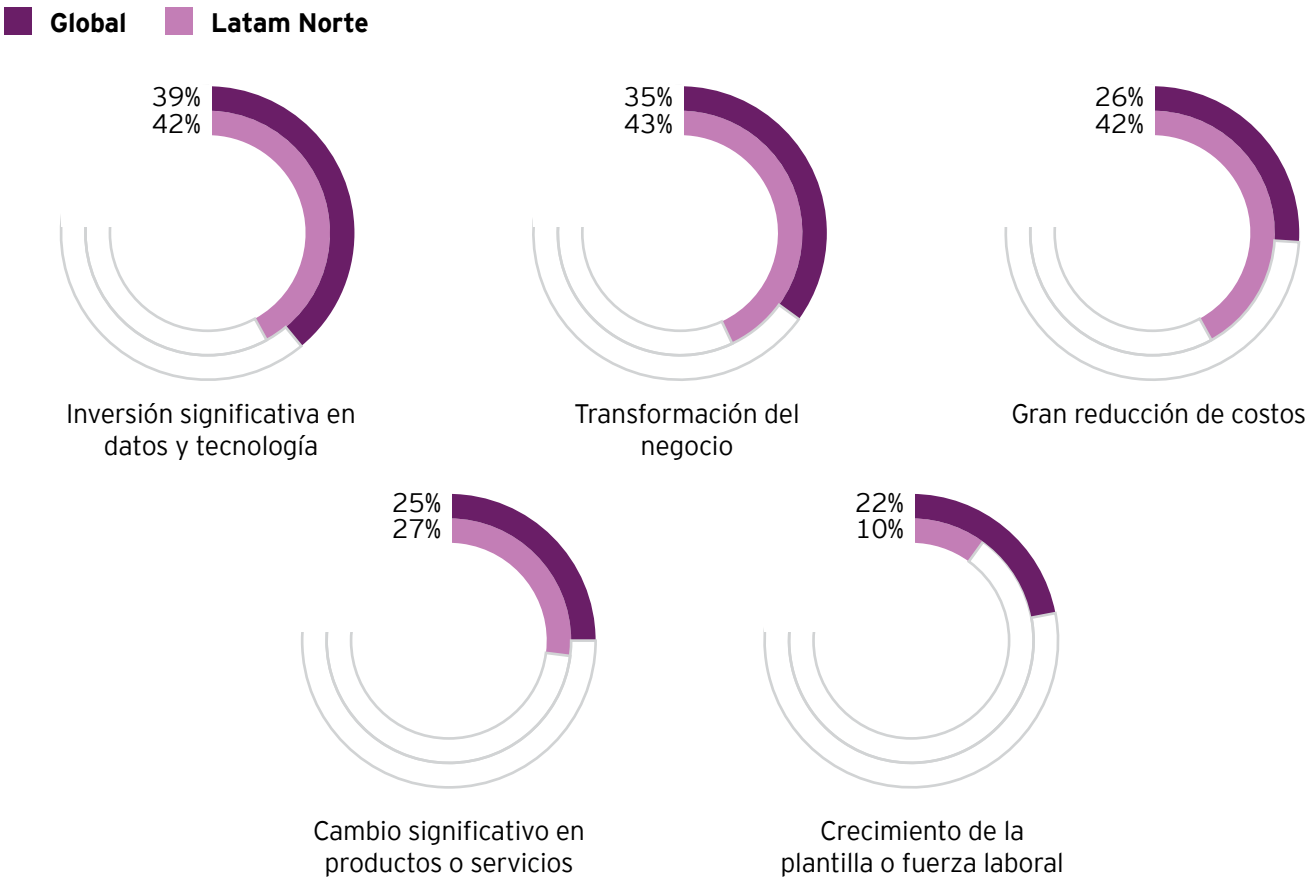
Los empleadores, por ejemplo, buscan respaldar modelos de trabajo híbridos, al mismo tiempo que desbloquean el crecimiento en una economía en recuperación. Un estudio reciente de EY, *Work Reimagined* 2021, encontró que 54% de los encuestados considerarían la renuncia si sus empleadores les negaran la flexibilidad que estaban buscando. Los CISO también deben ser conscientes de que la mitad de los empleados (48%) desean invertir en nueva tecnología para el trabajo virtual, lo que abre la posibilidad de una mayor exposición si las empresas no pueden abordar la seguridad desde el diseño.

Todos los ojos están puestos en los CISO

Los CISO se enfrentan a un momento crítico. Si pueden respaldar la transformación digital desde la etapa de planificación, en un momento cuando el 68% de los gerentes generales están planificando una importante inversión en datos y tecnología en los próximos 12 meses según el estudio EY CEO *Imperative* 2021, realmente se convertirán en un habilitador estratégico del crecimiento. Si no pueden desempeñar un papel más activo en la transformación, las amenazas a la seguridad se acelerarán y su posición en las sesiones de los Directorios disminuirá.

Figura 4: Las cinco principales prioridades estratégicas de las empresas sugieren un enfoque continuo en la transformación

¿Cuáles de las siguientes acciones prevé que llevará a cabo su organización en los próximos 12 meses?



Más de la mitad:

Global

55%

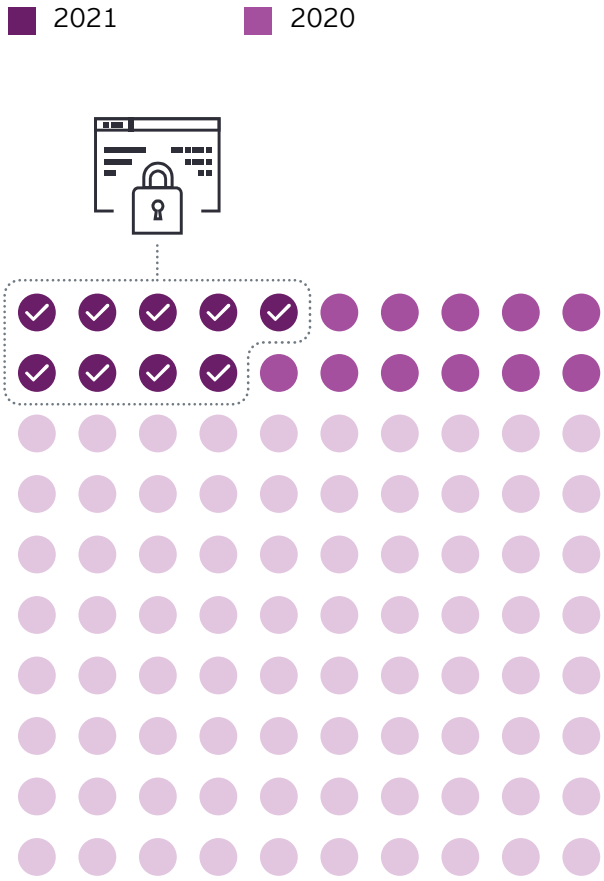
Latam Norte

72%

de los encuestados dice que ahora la ciberseguridad está siendo analizada detenidamente más que en cualquier otro momento de sus carreras.

Figura 5: La erosión de la confianza

Solo el 9% de los Directorios siente confianza plena en las medidas de mitigación de riesgos de ciberseguridad de su organización, una clara disminución con respecto al año pasado.



El equipo senior de liderazgo se encuentra preocupado por la capacidad de la función de seguridad para proteger a sus organizaciones. Más de la mitad (55%) de los encuestados dice que la ciberseguridad está siendo objeto de más escrutinio hoy que en cualquier otro momento de sus carreras. Cuatro en diez (39%) organizaciones incluyen la ciberseguridad en las agendas de los Directorios trimestralmente, frente a la cifra 29% del año 2020.

Y, sin embargo, en el Estudio EY *Global Board Risk* 2021, solo 9% de los Directorios se declararon extremadamente confiados en las medidas de mitigación de riesgos de ciberseguridad de su organización, en comparación con el 20% del año anterior.

Una oportunidad en crisis

Los CISO que pueden mitigar el riesgo, mientras habilitan las ambiciones de crecimiento y tecnología de sus negocios, tienen un futuro brillante. La mayoría reconoce esto: 57% cree que la crisis brinda una oportunidad para que la ciberseguridad destaque.

Dave Burg insta a los CISO a capitalizar su mayor visibilidad. "Conozco a muchos directores de seguridad a quienes se les consideraba 'súper estrellas', y a ellos los queremos al frente de la innovación.", dice.

Entonces, ¿están los CISO listos para aprovechar la oportunidad de un nuevo rol como habilitador del crecimiento? ¿Pueden incorporar resiliencia antes de la próxima gran disrupción empresarial? La respuesta es sí, pero solo si primero pueden abordar tres desafíos críticos e interrelacionados que se interponen en su camino:

1. La organización de la ciberseguridad está muy mal financiada y dicho financiamiento se necesita ahora más que nunca.
2. La fragmentación regulatoria ha sido un dolor de cabeza, generando más trabajo y problemas de abastecimiento.
3. Las relaciones de los CISO con otras áreas son débiles, exactamente cuando más se necesitan conexiones sólidas.

"Hoy más que nunca los CISO deben ser vistos como un habilitador y aliado del negocio a través del fortalecimiento de los asuntos clave en materia de gobierno de cibersecuridad, identificando los actores clave que deben estar involucrados en dicho gobierno y sus responsabilidades, potencializando su relación con el CISO.

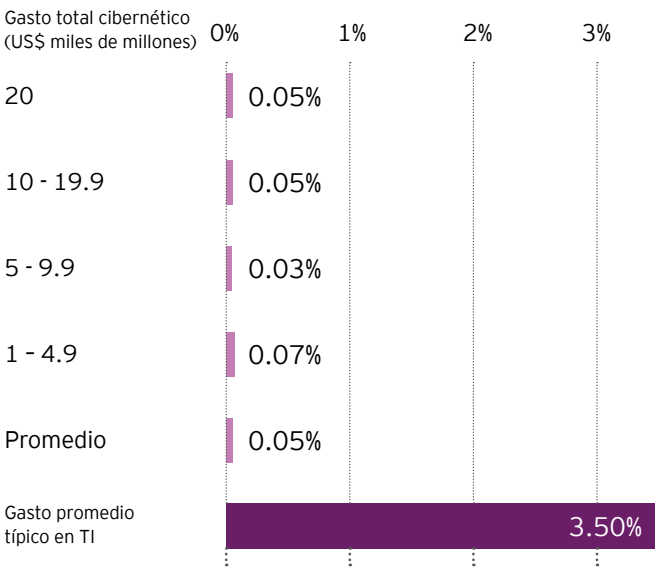
Gustavo Díaz
Socio Líder de Ciberseguridad para Servicios Financieros de EY Latam Norte

2 Tres desafíos que detienen a los CISO

La tormenta perfecta para la ciberseguridad

Figura 6: Gasto en tecnologías de la información y ciberseguridad, con un desglose de la empresa por tamaño para el gasto cibernético. El gráfico asume que el gasto en TI está entre el 2% y el 5%, de acuerdo con los informes de la industria.

¿Cuál es su gasto anual en ciberseguridad, a proporción de los ingresos?



Global

61%

Latam Norte

59%

de los encuestados dice que sus presupuestos de seguridad forman parte de un gasto corporativo mayor, como TI.

1. La organización actual de ciberseguridad no cuenta con fondos suficientes

A pesar de la creciente amenaza de ciberataque, el presupuesto de ciberseguridad es bajo en relación con el gasto total en el área de tecnología de información. Los datos de la encuesta también sugieren que los procesos de asignación presupuestaria son en gran medida inflexibles, a pesar de la necesidad de respuestas ágiles frente a la volatilidad de la era de la pandemia y la perspectiva de interrupciones futuras.

"Los modelos de financiación actuales son simplemente inadecuados para lo que, de hecho, es un riesgo existencial", dice Kris Lovejoy, Líder Global de Ciberseguridad para Consultoría de EY. "También es sintomático de la poca comprensión que muchas empresas tienen de los problemas cibernéticos y su incapacidad para implementar una cultura de seguridad por diseño".

Los presupuestos no están sincronizados con las necesidades

En la elaboración de este informe, EY realizó entrevistas cualitativas con tres responsables de ciberseguridad y encuestó a más de 1.000 profesionales dentro de ciberseguridad. Aproximadamente, los encuestados obtuvieron ingresos promedio de US$11 mil millones el año pasado, mientras que gastaron un promedio de solo US$5.28 millones, o 0.05% del total, en ciberseguridad.

La imagen varía de un sector a otro. En un extremo, en los sectores de tecnología y servicios financieros, medios y entretenimiento, y telecomunicaciones (TMT), el encuestado promedio de GISS gastó un promedio de US$9.43 millones y US$9,62 millones respectivamente en ciberseguridad el año pasado. En el otro extremo del espectro, las empresas de energía gastaron solo US$2,17 millones en promedio. También encontramos diferencias por tamaño de empresa, con las empresas más pequeñas gastando una mayor proporción.

Un problema se relaciona con la forma de planificar y asignar el presupuesto. Aproximadamente seis de cada 10 (61%) encuestados dicen que su presupuesto de seguridad forma parte de un gasto corporativo más grande, como TI, y 19% informa que esto es fijo y definido cíclicamente. Más de un tercio (37%) dice que los costos de ciberseguridad se comparten en toda la organización, pero solo 15% lo hacen de manera dinámica, dependiendo de cómo se utilicen los recursos.

Global **Latam Norte**

36% 39%

de los encuestados piensa que enfrentará una amenaza mayor a corto plazo, la cual podría haber sido eliminada con inversión apropiada.

En otras palabras, muy pocas organizaciones definen sus presupuestos de seguridad como un costo variable y contingente de hacer negocios. En efecto, los CISO pueden tener dificultades para escalar los esfuerzos de sus funciones en el contexto de iniciativas comerciales específicas y de rápida evolución.

La reducción de costos crea nuevas debilidades

Los CISO son muy conscientes de las vulnerabilidades que enfrentan sus organizaciones debido a presupuestos inflexibles e insuficientes.

Cuatro de cada 10 encuestados (39%) señala que los gastos de ciberseguridad no se tienen en cuenta de manera adecuada en el costo de las inversiones estratégicas, como una transformación de la cadena de suministro de TI. Más de un tercio (36%) dice que es sólo cuestión de tiempo hasta que enfrenten una brecha mayor que podría haberse evitado mediante una inversión más adecuada en las defensas de la ciberseguridad.

Dado que las organizaciones se han apresurado en transformar sus operaciones frente a la disrupción, podríamos esperar que el problema se intensifique a medida que las empresas continúan la inversión para respaldar el crecimiento. Cuatro de cada 10 encuestados (39%) advierte que el presupuesto de su organización está por debajo de lo requerido para gestionar los nuevos desafíos que han surgido en los últimos 12 meses.

Un resultado inevitable de las restricciones presupuestarias es que los CISO toman decisiones difíciles y cancelan algunas de las actividades estratégicas que se habían puesto en marcha antes de que comenzara la crisis. Más de la mitad de empresas (56%) con presupuestos insuficientes nos dicen que han tenido que reajustar sus requisitos de ciberseguridad, y 44%dice que se han visto obligados a reducir costos al centrarse en su arquitectura y sistemas heredados.

Sin embargo, una minoría de organizaciones adopta un enfoque más estratégico para la financiación de la ciberseguridad. En Assicurazioni Generali, una de las aseguradoras líderes del mundo, el Director de Seguridad del grupo, Remo Marini, dice que la empresa adopta un enfoque basado en el riesgo a la financiación de la ciberseguridad. "Construimos un vínculo directo entre las inversiones en seguridad, el valor comercial y la reducción de riesgos", dice. "Nuestro presupuesto refleja una actividad de planificación sofisticada que comienza con la definición de nuestra estrategia, por lo general con un horizonte de tres años, y recopila aportaciones de todas las partes interesadas internas y externas relevantes".

"

Nosotros construimos un vínculo directo entre inversiones en seguridad, valor comercial y reducción de riesgos.

Remo Marini
Director de Seguridad del Grupo Assicurazioni Generali

Global **Latam Norte**

42% 46%

El presupuesto forma parte de un gasto corporativo y/o organizacional mayor (por ejemplo, el de TI y/o tecnología) y se define de manera dinámica.

Global **Latam Norte**

22% 14%

El gasto en ciberseguridad es fijo, se comparte con todas las unidades de negocios y se define por ciclos.

Global **Latam Norte**

19% 13%

El presupuesto es una parte fija de un gasto corporativo/organizacional mayor (por ejemplo, el 5% de TI y/o tecnología) y se define por ciclos.

Global **Latam Norte**

15% 18%

El gasto en ciberseguridad se comparte con todas las unidades de negocios, las cuales definen su contribución de forma dinámica con base en el uso.

Global

56%

Latam Norte

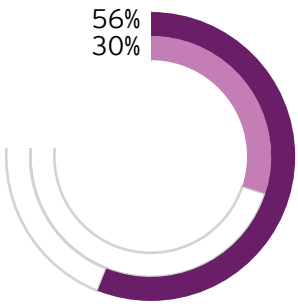
30%

de los encuestados con presupuestos insuficientes ha tenido que realinear sus requisitos de ciberseguridad para satisfacer mejor las cambiantes necesidades del negocio.

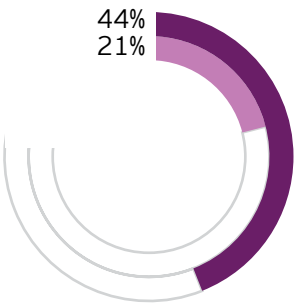
Figura 8: Los CISO con presupuestos insuficientes se han visto obligados a reducir el trabajo de seguridad esencial

¿Qué acciones ha realizado para gestionar presupuestos insuficientes?

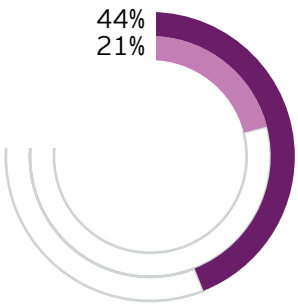
Global **Latam Norte**



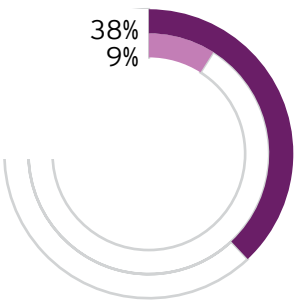
Realineación de los requisitos de ciberseguridad para satisfacer mejor las cambiantes necesidades del negocio



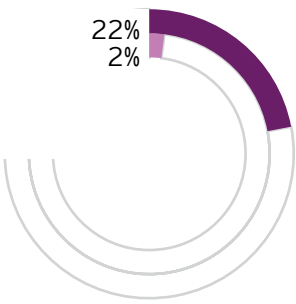
Revisión de la arquitectura heredada para oportunidades de reducción de costos



Incremento en la dependencia de proveedores externos



Reducción de la actividad de innovación para enfocarse en tareas básicas no estratégicas



Reducción de planilla o fuerza laboral

Global

49%

Latam Norte

50%

dice que garantizar el cumplimiento en el panorama regulatorio actual puede ser la parte más estresante de su trabajo.

2. La fragmentación regulatoria es un dolor de cabeza creciente para los CISO

El entorno de cumplimiento global es cada vez más complejo, con regímenes que operan a niveles regionales y nacionales. Las organizaciones en ciertos sectores deben manejar las regulaciones específicas de cada industria.

Mike Maddison, Líder de Cberseguridad para Consultoría en EY EMEIA, cree que la regulación es una preocupación creciente. "Si su organización es internacional, la forma como usted maneje la superposición de estas regulaciones es todo un desafío, particularmente a medida que la información se vuelve ubicua y viaja internacionalmente".

Una pérdida de tiempo y recursos valiosos

La regulación está reclamando tiempo que los CISO no tienen para dar. Uno de cada dos (49%) advierte que garantizar el cumplimiento puede ser la parte más estresante de su trabajo. Seis de cada 10 (57%) predice que la regulación se volverá más heterogénea, consumirá más tiempo y, algunos podrían decir, será caótica en los próximos años. Mientras los CISO luchan por asegurar los recursos que necesitan, es comprensible un impacto en sus niveles de estrés.

"La agenda regulatoria está cada vez más apretada a medida que los reguladores locales e internacionales intensifican su enfoque", confirma Marini de Assicurazioni Generali. "Estamos viendo una proliferación de regulaciones que plantean dificultades, en particular para los grupos internacionales. Un marco común y estandarizado sería más eficiente".

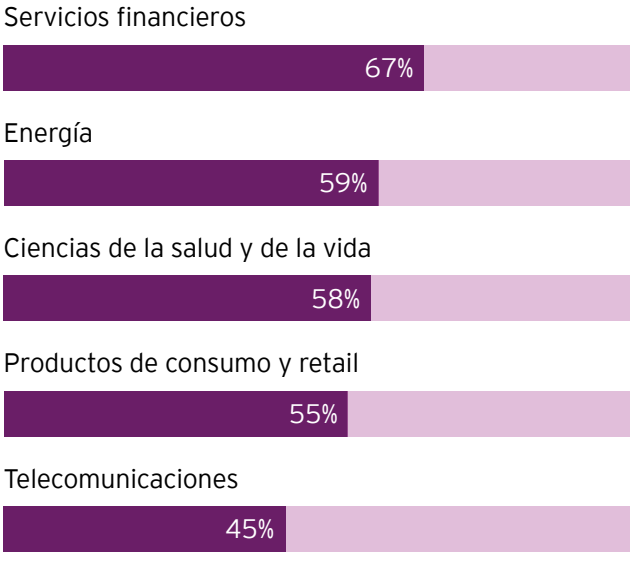
Una preocupación adicional, al menos en Estados Unidos, es que el Departamento de Justicia ha elevado los ataques de *ransomware* al mismo nivel de prioridad que el terrorismo y está coordinando investigaciones a través de un grupo de trabajo en Washington. Mientras este estudio se redactaba, no estaba claro todavía qué recursos se pondrán a disposición de las organizaciones del sector privado si son víctimas de ataques.

Kris Lovejoy cree que ha habido un cambio fundamental en la forma en que los CISO consideran el cumplimiento, lo que tiene implicaciones preocupantes en la relación con el regulador. "Los CISO aún se mostraban positivos sobre el papel del cumplimiento el año pasado", dice. "Este año, reconocen que el cumplimiento ha cambiado. Se ha vuelto tan fragmentado y tan complejo que ahora es una distracción. El cumplimiento ya no es amigo del CISO, en el sentido de que ya no justifica los presupuestos de la forma en la que lo hizo. El cumplimiento se ha convertido en su enemigo".

Para Lovejoy, este año los CISO tienen menos confianza en que la regulación apoye la mejora de los estándares de ciberseguridad en las organizaciones. La investigación de EY también encuentra que el cumplimiento ni siquiera proporciona los medios para asegurar fondos adicionales que una vez lo hizo, lo que, a la luz de las limitaciones presupuestarias, antes se había considerado un rayo de luz.

Figura 9: Los CISO en servicios financieros están más preocupados por la nueva regulación compleja

¿Está de acuerdo en que la regulación se volverá más fragmentada y difícil de gestionar en los próximos años?



Global

35%

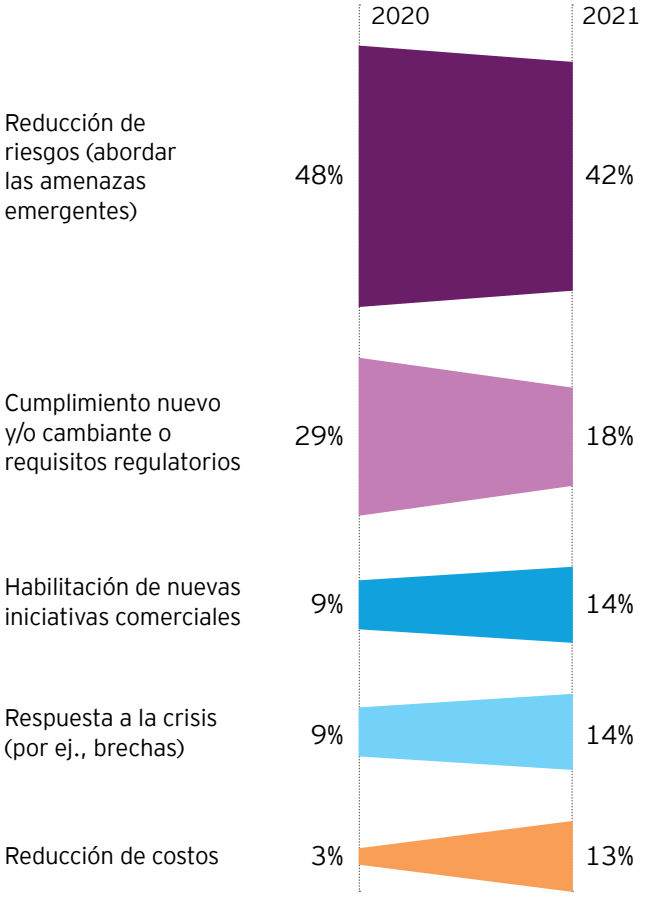
Latam Norte

90%

de los encuestados cree que los requisitos del cumplimiento de la ciberseguridad impulsan los comportamientos correctos.

Figura 10: La regulación obtiene puntuaciones relativamente bajas como justificación presupuestaria

¿Cuál es el impulsor primario de los gastos nuevos o aumentados en ciberseguridad?



> En el entorno dinámico durante COVID, existía una gran necesidad de velocidad y las organizaciones cuestionaron si los equipos de ciberseguridad tenían las habilidades adecuadas.
>
> Mike Maddison
> Líder de Ciberseguridad para Consultoría en EY EMEIA

En el estudio del año pasado, el 46% de los encuestados pensaba que el cumplimiento impulsaba el enfoque y los comportamientos correctos dentro de su negocio. En 2021, esta cifra ha bajado a 35%. Al mismo tiempo, menos de uno de cada cinco (18%) encuestados describen la regulación como una forma efectiva de presentar sus argumentos a sus juntas para obtener un presupuesto adicional, en comparación con 29% del año 2020 (ver figura 10).

Si bien los altos ejecutivos pueden haberse vuelto más receptivos a los casos comerciales que vinculan el aumento del gasto en ciberseguridad con la transformación, parecen menos conmovidos por las advertencias de los CISO sobre la creciente carga de acciones de cumplimiento.

No todos los líderes en ciberseguridad son pesimistas sobre la regulación. Roland Cloutier de TikTok dice que la regulación está consumiendo "al menos 50% o 60%" de su tiempo, pero sigue siendo positivo en general." "Nuestros programas de seguridad estratégica se basan en el requisito de la próxima generación en torno a consideraciones regulatorias y protección al consumidor. Eso es genial. Permitimos que nuestros productos estén listos para el futuro. Nos está ayudando a crear el concepto líder en la industria de cómo operar como una empresa dedicada a proteger la seguridad y la privacidad de nuestros usuarios en todo el mundo".

3. Las relaciones de ciberseguridad con otros líderes se están deteriorando.

Para gestionar el riesgo cibernético asociado a la transformación estratégica, los CISO deben brindar asesoramiento en las primeras etapas de la toma de decisiones de inversión. Pero las relaciones entre ciberseguridad y otras áreas en el negocio, que son fundamentales para que dichas consultas se lleven a cabo, carecen de positividad y fuerza.

Los líderes empresariales excluyen al CISO

Las relaciones débiles han sido durante mucho tiempo una preocupación para los CISO, pero el GISS de este año sugiere que el problema está cada vez más pronunciado. Según la encuesta, los líderes empresariales están eliminando la ciberseguridad de las conversaciones vitales. Alrededor de seis de cada 10 (58%) dice que sus organizaciones a veces implementan nueva tecnología con escalas de tiempo que no permiten una evaluación o supervisión adecuada de la ciberseguridad.

Dan Higgins, Líder Global de Tecnología para Consultoría de EY, dice que es preocupante que los CISO estén involucrados al final del proceso de Implementar nuevas tecnologías y soluciones de datos. "Es imperativo que los CISO establezcan su lugar en la mesa en las fases de arquitectura de estrategias y soluciones de la transformación digital, cuando estos riesgos se pueden abordar y evitar de manera proactiva", dice.

Es una tendencia que puede ser impulsada desde la cima del negocio. Según el estudio EY *CEO Imperative* 2021, los gerentes generales ya no describen la ciberseguridad como su principal preocupación, como lo hicieron en el 2020.

En cambio, este año su enfoque está centrado en los desafíos relacionados con la adopción de nuevas tecnologías.

La pandemia está empeorando las cosas: el 81% de las organizaciones eludieron los procesos cibernéticos y no consultaron a los equipos de ciberseguridad en las etapas de planificación de nuevas iniciativas comerciales.

"En el entorno dinámico que vimos durante COVID, existía una gran necesidad de velocidad y las organizaciones cuestionaron si los equipos de ciberseguridad tenían las habilidades adecuadas", dice Mike Maddison. "¿Se los veía como un paso que impedía la agilidad o como personas que ofrecían soluciones efectivas? Cuando las respuestas a esas preguntas estaban en duda, otras partes de la organización lo hacían solas sin el equipo cibernético".

Las relaciones son más débiles donde deben ser fuertes

El problema es más agudo entre las funciones que se implementarán y escalarán la nueva tecnología basada en la nube en los próximos meses y que, por lo tanto, corren un gran riesgo de verse comprometidas por los piratas informáticos que implementan *ransomware*.

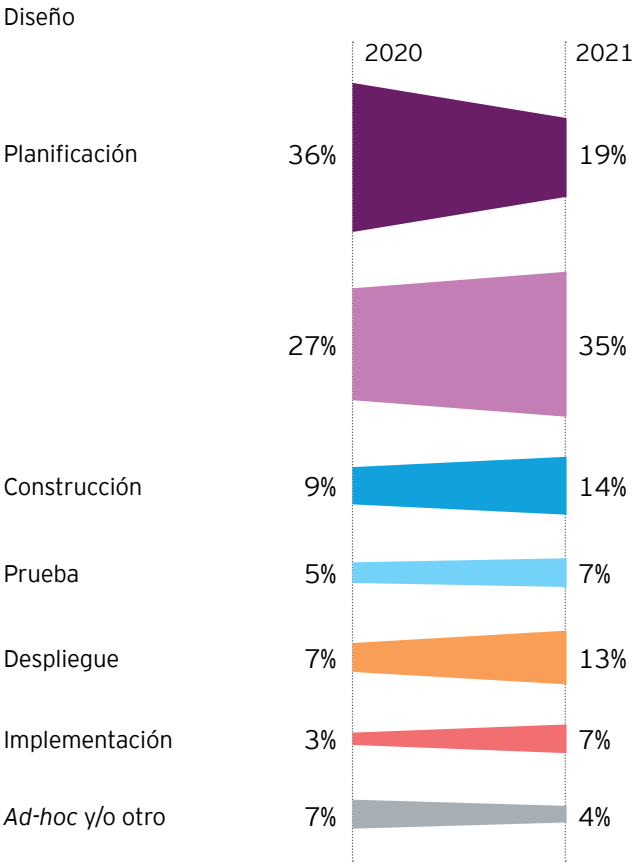
En el estudio de este año, el 41% de los encuestados describe su relación con la función de marketing como negativa, frente al 36% que dijo lo mismo hace un año. Al mismo tiempo, 28% dijo que su relación con los dueños de negocios es deficiente, en comparación con 23% hace un año.

El resultado es que, si bien más de un tercio de los encuestados en 2020 (36%) confiaban en que se estaba consultando a los equipos de ciberseguridad en la etapa de planificación de nuevas iniciativas comerciales, esta cifra se redujo a 19% en el 2021.

"La relación de la ciberseguridad con las líneas de negocio, el desarrollo de productos y el marketing son negativas, mientras que sus interacciones con riesgo, legal y TI son positivas", dice Kris Lovejoy. "Esencialmente, las relaciones se vuelven más positivas cuanto más se aleja del ciclo de planificación, lo cual es un problema. Donde más se necesita involucrar al equipo de ciberseguridad, no se les invita a la fiesta ".

Figura 11: Es menos probable que los equipos de ciberseguridad pasen a las primeras etapas de desarrollo

¿En qué etapa se incorpora la ciberseguridad a una nueva iniciativa empresarial?



Falla de comunicación

La mala comunicación entre equipos es una barrera para el progreso. Los CISO nos comentan que luchan por lograr que su gente articule la necesidad de la consulta cibernética en términos comerciales. Además, la empresa puede reconocer las fortalezas tradicionales de la ciberseguridad, como el control del riesgo, pero no siempre percibe la ciberseguridad como un socio estratégico.

"En toda la industria, he visto un cambio de mentalidad positivo con los Directorios que reconocen que la ciberseguridad es un riesgo", dice Darren Kane, Director de Seguridad de NBN Co en Australia, que participó en una entrevista cualitativa para este informe pero no en la encuesta.

"Pero los CISO aún tienen trabajo por hacer para derribar las barreras de comunicación al hablar en un lenguaje menos técnico, para que los Directorios comprendan mejor los riesgos comerciales potenciales".

Menos de la mitad de los encuestados (44%) confían en la capacidad de su equipo para hablar el mismo idioma que sus compañeros, y solo el 26% cree que los líderes usarían términos técnicos para describir la función. Solo uno de cada cuatro (25%) cree que los líderes empresariales de alto nivel describirían la ciberseguridad como comercial.

Los encuestados admiten que es más probable que el resto de la organización describa la ciberseguridad como la protección del negocio y la respuesta rápida a las crisis. Si bien estas son cualidades admirables en sí mismas, deben equilibrarse con la capacidad de comunicarse, persuadir y generar confianza.

"Los resultados en Latam Norte no difieren de los resultados globales en la encuesta, el fortalecimiento de la función de ciberseguridad a través de un mayor y mejor financiamiento es vital para garantizar que los riesgos a los que se enfrenta el CISO son abordados de manera adecuada, las organizaciones de todos los tamaños y de todos los giros deben invertir en proveer a las CISOs los recursos necesarios para proteger los activos de información clave de sus compañías.

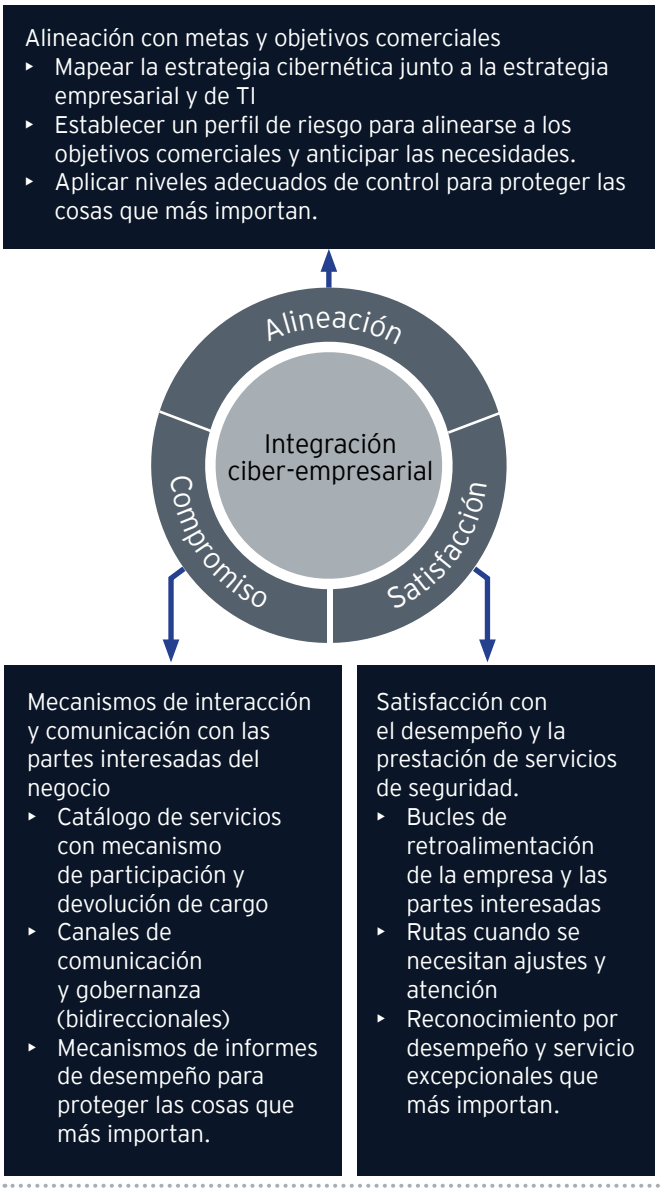
Gustavo Díaz
Socio Líder de Ciberseguridad para Servicios Financieros de EY Latam Norte

3 Conclusiones y próximos pasos

El CISO como habilitador de valor

> Los CISO son fundamentales en la transformación de una organización al ofrecer valor a largo plazo.
>
> Errol Gardner
> Vicepresidente Global de Consultoría en EY

Figura 12: Tres elementos críticos para la integración de negocios cibernéticos.



¿Cómo deben responder los CISO a los desafíos centrales descritos en el GISS de este año? Deberían jugar un papel más estratégico y comercial en sus organizaciones, reinventando el rol de sus equipos como facilitadores de la transformación.

"Los CISO son fundamentales para los esfuerzos de las organizaciones en transformarse y ofrecer valor a largo plazo", dice Errol Gardner, Vicepresidente Global de Consultoría en EY. Al discutir cómo los CISO deben posicionarse como facilitadores de la transformación, Gardner agrega: "Si bien los CEO están en el camino de hacer realidad su visión y transformar con éxito sus negocios a través de la tecnología, no pueden permitirse el lujo de hacer la vista gorda ante los riesgos cibernéticos que esto plantea."

"Al mismo tiempo, corresponde a los CISO garantizar que los gerentes generales comprendan correctamente el valor que aporta la inversión en ciberseguridad y que lo reconozcan como parte integral del viaje de transformación. Invertir en la construcción de una relación estratégica entre los CISO, los CEO y el resto de la C-suite ayudará a garantizar que los programas de transformación no solo sean exitosos, sino que también se implementen de una manera cibersegura para la organización y su gente".

Pero la capacidad de los ejecutivos de ciberseguridad para ejercer influencia y garantizar que el negocio en general apoye su creciente función, está lejos de ser segura. Ocho de cada diez Directorios creen que la gestión de riesgos será fundamental para proteger y generar valor, según el Estudio EY *Global Board Risk Study* 2021, pero esperamos que la contribución del CISO sea menos reconocida en la actualidad.

Nuestros hallazgos sugieren que los CISO deberían considerar tres acciones centrales para fortalecer su posición dentro del negocio:

- Reevaluar su alineación con el negocio
- Revisar el perfil de talento
- Centrarse en cuatro stakeholders clave

Vale la pena señalar que estas acciones son consistentes con la orientación que brindamos en nuestro informe de 2020, aunque con cierta evolución en el proceso de pensamiento subyacente. Los eventos de la crisis solo han enfatizado su urgencia y resaltado la importancia de hacerlo bien.

<< No existe un perfil de ciberseguridad "estándar"

1

Llegue a la "verdad fundamental": reevalúe su alineación con la empresa

Los equipos de ciberseguridad han sido tradicionalmente más fuertes cuando se trata de evaluar sus capacidades, identificar riesgos y construir hojas de ruta para el futuro.

Los CISO deben centrar su atención en los elementos de la ciberseguridad que han sido más débiles en el pasado. Específicamente, deben buscar fortalecer su compromiso con las partes interesadas, garantizar su alineación con las metas y objetivos comerciales centrales y evaluar la satisfacción de sus socios comerciales con el desempeño y la entrega de servicios de seguridad (ver figura 12).

Dado que las relaciones con los socios comerciales se han deteriorado en los últimos años, los CISO pueden carecer de la visibilidad que necesitan para operar en sincronización con otras funciones y seguir una estrategia que se alinee con el negocio.

2

Revise el perfil necesario, pero no espere lo imposible

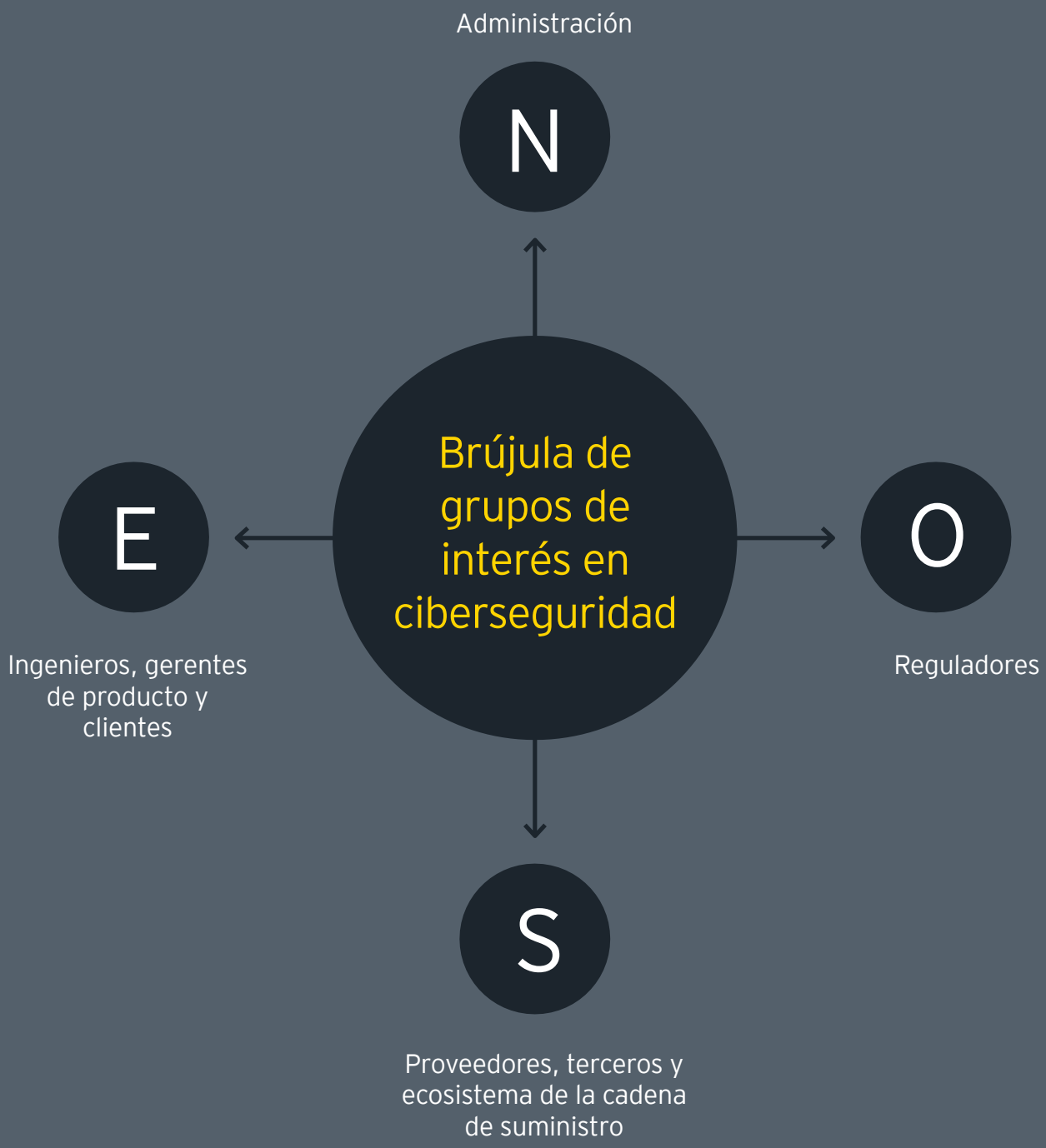
Para responder a los desafíos organizacionales destacados por la encuesta, así como a la naturaleza sofisticada de los recientes ataques de alto perfil, los CISO necesitan el apoyo de profesionales versátiles y con múltiples habilidades.

Un desafío es que la amplitud de habilidades necesarias en la función actual se está expandiendo en varias direcciones a la vez. No existe un perfil de ciberseguridad "estándar". Los CISO necesitan personas con habilidades técnicas avanzadas, así como con la capacidad de construir relaciones interdepartamentales. Necesitan personas apasionadas por la innovación y el crecimiento, que también puedan detectar amenazas emergentes y encontrar fallas en las defensas.

Figura 13: Múltiples perfiles en la función de ciberseguridad actual

Perfil ejecutivo de ciberseguridad	Área de enfoque	Fortalezas	Debilidades
Experto en seguridad	Seguridad en general	Amplio conocimiento del tema	Falta de visión para el negocio
Defensor tecnológico	Herramientas y soluciones tecnológicas	Orientado a la tecnología	Mentalidad en silos
Pros regulatorios y de riesgos	Riesgos, controles y cumplimiento	Bueno para los sectores altamente regulados	Falta de visión tecnológica
Trasplantes de negocios	Integración de negocios	Conectividad de negocios	Falta de visión de seguridad y tecnología
Trabajadores a tiempo parcial y asignación de trabajos	División entre roles de ciberseguridad y otras funciones primarias	Ahorro en costos	"Aprendiz de todo, maestro de nada"

Figura 14: El CISO en el centro de cuatro grupos de interés



> Los CISO conocen el principio de "desplazamiento a la izquierda" y se esfuerzan por involucrar la ciberseguridad en una etapa más temprana de la transformación.

3

En la figura 13, describimos algunos de los perfiles ejecutivos de ciberseguridad que han surgido en los últimos años, a pesar de la relativa novedad de la profesión. Cada perfil tiene su propia área de enfoque, se basa en su propia gama de habilidades sociales, calificaciones profesionales y desempeña un papel importante en la satisfacción de las necesidades cambiantes de la empresa.

Sin embargo, intentar encontrar una persona que tenga todos estos talentos es como intentar reclutar un unicornio. Un mejor enfoque es construir un equipo que equilibre una combinación de disciplinas amplias, entendiendo que cada una tiene sus propias fortalezas y debilidades.

Con respecto a la construcción de relaciones, los CISO deben asegurarse de que su gente tenga una mayor exposición a funciones como marketing, innovación y otras unidades comerciales relevantes. "La gente cibernética ha tenido la reputación de ocupar los niveles del sótano de un edificio de oficinas", dice Darren Kane. "Pero dado que el riesgo cibernético es ahora uno de los principales riesgos operativos de cualquier empresa, los equipos cibernéticos deberían salir más y tener una mayor exposición a otras partes del negocio".

Cambie en todas partes: adopte una nueva brújula para los grupos de interés

Los CISO están familiarizados con el principio de "desplazarse a la izquierda", esforzándose por involucrar la ciberseguridad en una etapa más temprana del ciclo de vida de transformación y desarrollo de productos.

Los desafíos de COVID-19 indican, sin embargo, que cambiar a la izquierda ya no es todo lo que se requiere. Nuestra sugerencia a los CISO es que se desplacen hacia el norte, este, sur y oeste. En la práctica, esto significa navegar por cuatro grupos de interés clave, como se ilustra en la figura 14.

Abordar las preocupaciones de la administración, en el "norte", significa centrarse en la presentación de informes y la rendición de cuentas, así como en la asignación de recursos y presupuestos. Cambiar el enfoque "hacia el este", a los reguladores, es un caso de priorizar las certificaciones y atestaciones, junto con el mapeo regulatorio. Cambiar al sur consiste en mejorar los estándares y las pruebas. Y cambiar al oeste implica centrarse en la seguridad y la privacidad por diseño, junto con certificaciones y pruebas continuas.

Si los CISO pueden posicionarse en el centro de estas cuatro partes interesadas vitales, estarán en el lugar correcto para llevar su función al siguiente nivel de influencia estratégica.

> "Aún y cuando los requerimientos regulatorios en materia de Ciberseguridad varían de país a país, el común denominador en estas regulaciones es que requieren un esfuerzo significativo para dar cumplimiento cabal a las disposiciones emitidas por los diferentes reguladores. Los CISOs deben estar conscientes que estos requerimientos son ineludibles y que se deben habilitar los recursos materiales, humanos y tecnológicos necesarios para que las organizaciones den cumplimiento a estos requerimientos.
>
> Carlos López Cervantes
> Socio Líder de Ciberseguridad para Consultoría en EY Latam Norte

Más allá de la tormenta

La crisis de COVID-19 ha sido una llamada de atención para los CISO. La empresa ha recurrido al equipo de ciberseguridad para proteger a la organización de una ciberamenaza en evolución, al tiempo que permite una transformación tecnológica urgente y un nuevo crecimiento.

No hay duda de que muchos CISO se han enfrentado al desafío y hoy pueden demostrar la creciente importancia estratégica de su función. Pero también sería justo señalar que la crisis ha puesto de relieve las debilidades en la ciberseguridad y las áreas en las que se requiere una mejora. Específicamente, los CISO deben acelerar sus esfuerzos para abordar la seguridad desde el diseño mientras construyen relaciones más sólidas y basadas en la confianza con sus pares *C-suite*.

No es una iniciativa sencilla ni una ambición que se pueda lograr en un año, pero el negocio está mirando. Los CISO deben participar cuando se planifican inversiones estratégicas. Depende de ellos asegurar un asiento en la mesa.

Acerca de la encuesta

La Encuesta Global de Seguridad de Información 2021 de EY se fundamenta en información obtenida de más de 1.400 directores de seguridad de la información (CISO, en inglés) y altos ejecutivos de seguridad. Esta encuesta explora los desafíos que enfrentan en su puesto como habilitadores de crecimiento y socios estratégicos. Los CISO y otros profesionales de alto nivel comprendieron el 50% de los encuestados; los otros eran profesionales de ciberseguridad C-1. Las encuestas se realizaron principalmente por teléfono, y una minoría se completó en línea.

Se trata de una encuesta global con Europa, Oriente Medio, India y África (EMEIA) que representa el 45% de los encuestados, las Américas 36%, y la región de Asia y el Pacífico, 18%. Los encuestados son CISO o sus equivalentes de los servicios financieros, productos de consumo y retail, salud y ciencias de la vida, energía, gobierno y tecnología, medios y entretenimiento y telecomunicaciones. Cada negocio incluido en los datos de este informe tuvo ingresos anuales superiores a US$1 mil millones. Los países que componen Latam Norte son México, Colombia, Perú, Centroamérica, Panamá, República Dominicana, Ecuador y Venezuela.

Las comparaciones con 2020 representan una instantánea en el tiempo durante 2020 y 2021, basadas en perfiles de muestra similares año tras año. Empresas con ingresos anuales inferiores a 1.000 millones de dólares se incluyeron en 2020 pero no en el año 2021.

Además de la investigación cuantitativa, EY llevó a cabo una serie de discusiones en profundidad con líderes de opinión en ciberseguridad entre abril y junio de 2021.

Contactos

Carlos López Cervantes
Socio Líder de Ciberseguridad
para Consultoría
carlos.lopez2@mx.ey.com

Gustavo Díaz Rojas
Socio Líder de Ciberseguridad para
Servicios Financieros
gustavo.diaz@co.ey.com

EY México
Juan Fernández
Juan.Fernandez@mx.ey.com

Carlos López
Carlos.Lopez2@mx.ey.com

EY Colombia
Gustavo Díaz
gustavo.diaz@co.ey.com

Conchita Jaimes
Conchita.Jaimes@co.ey.com

EY Centroamérica, Panamá y Rep. Dominicana
Miguel Caldentey
miguel.caldentey@pa.ey.com

EY Ecuador
Diego León
diego.leon@ec.ey.com

EY Venezuela
Juan Fernández
juan.fernandez@ve.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.

Todas las imágenes: Shutterstock, Freepik, Unsplash

EY | Auditoría | Consultoría | Impuestos | Estrategias y Transacciones

Acerca de EY
EY es la firma líder en servicios de auditoría, impuestos, estrategia, 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