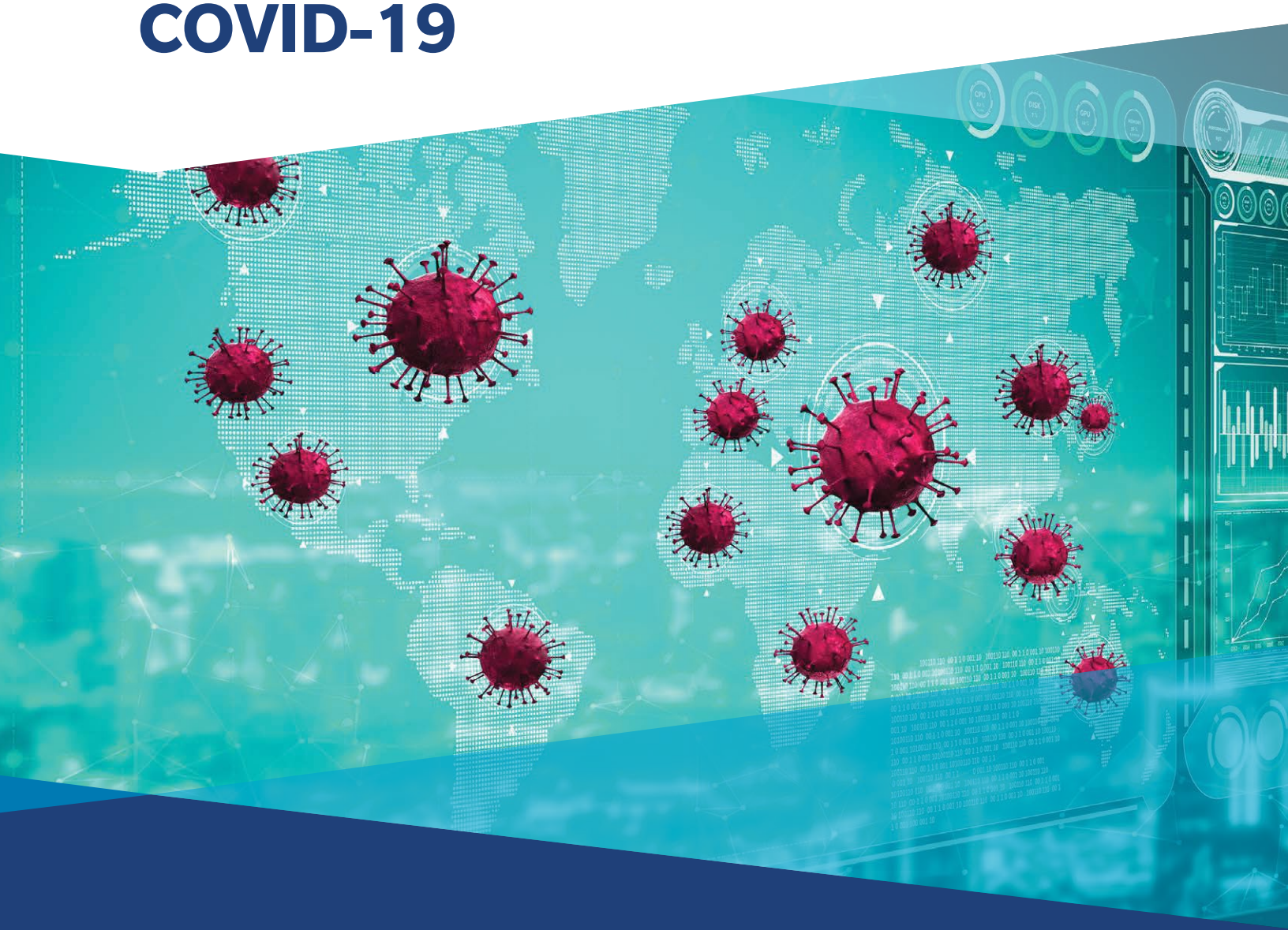
MARSH | Microsoft

PERSPECTIVAS | OCTUBRE 2020

Estado del Riesgo Cibernético en Latinoamérica en tiempos de COVID-19



MARSH & McLENNAN COMPANIES

Metodología

Alcance

Este informe se basa en los resultados de la Encuesta de Riesgo Cibernético en tiempos de COVID19 en Latinoamérica,

realizada en agosto de 2020 por Marsh y Microsoft, cuyo objetivo fue identificar el impacto que ha tenido el modelo de trabajo remoto, implementado como consecuencia del COVID19, en la gestión de la ciberseguridad en las empresas:

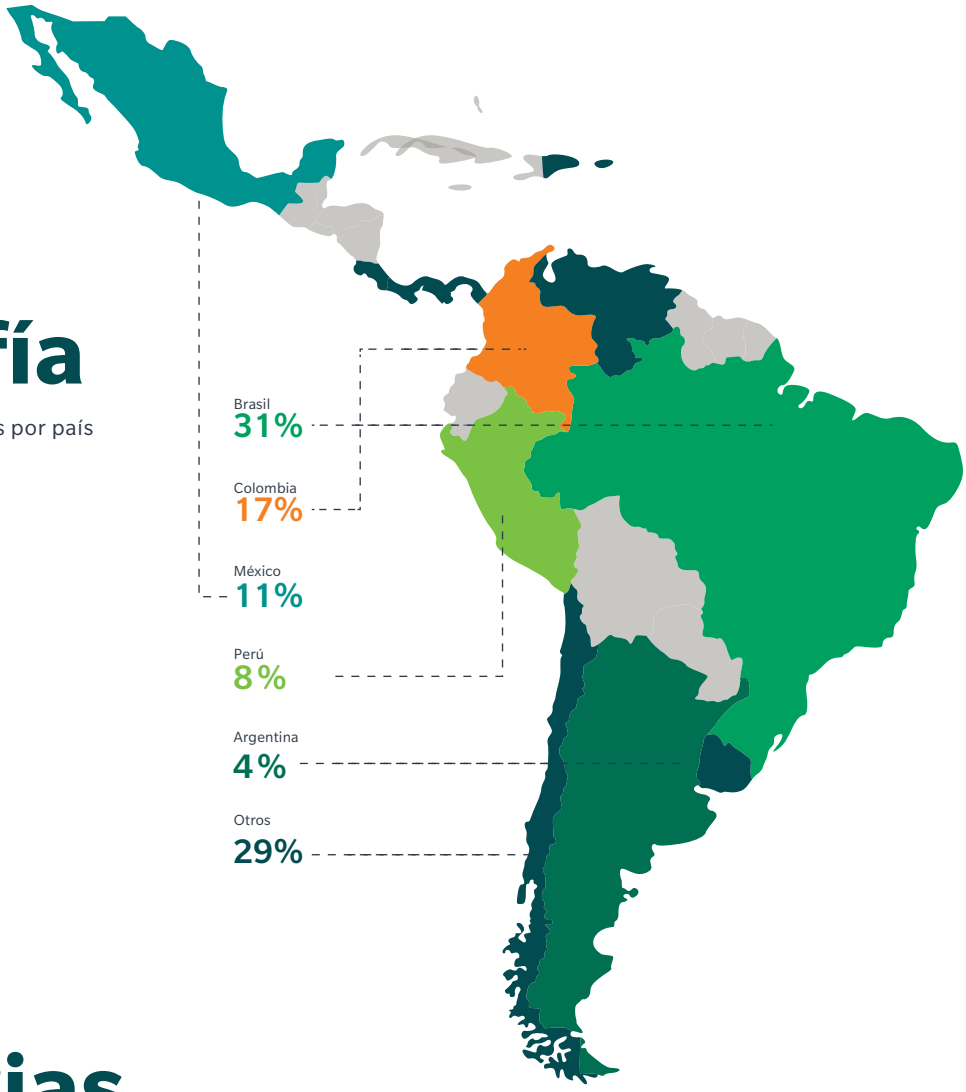
640
Empresas

+18
Países

+20
Industrias

Geografía

Distribución de los encuestados por país



Industrias

Sectores industriales en los que operan principalmente las empresas encuestadas

- Alimentos y bebidas
- Aviación / Aeroespacial
- Bienes raíces
- Comunicaciones, Medios de comunicación y Tecnología
- Construcción
- Educación
- Energía e hidrocarburos
- Entidades públicas/Sin fines de lucro
- Hotelería, alojamiento y restaurantes
- Industria financiera
- Manufactura/Automotriz
- Minería / Metales / Minerales
- Química
- Retail / Wholesale (minoristas y mayoristas)
- Servicios profesionales
- Transporte / Ferroviario / Marítimo
- Otras

Contenido

01

Introducción

La enfermedad por coronavirus 2019 (COVID-19) fue conocida por primera vez en Wuhan, China, y posteriormente se extendió por todo el mundo, convirtiéndose en una pandemia global que ha puesto en cuarentena a prácticamente todos los países, llevando a los sistemas de salud al límite y generado que la economía mundial haya entrado en una recesión sin precedentes.

El COVID19 ha dejado a las empresas frente a una interrupción inesperada de sus operaciones, lo que las ha llevado a migrar a un ambiente de trabajo remoto y, por consecuencia, a incrementar su exposición al Riesgo Cibernético de manera constante, de la mano de la evolución de la pandemia.

Los resultados de la Encuesta de Marsh y Microsoft sobre Riesgo Cibernético en tiempos de COVID19 en Latinoamérica, muestra cómo se ha adaptado la gestión de la ciberseguridad en las empresas, como resultado de la pandemia. Nuestros hallazgos se centran en cuatro importantes aspectos que muestran el impacto del Riesgo Cibernético en el panorama actual de COVID19:

A pesar de que el Riesgo Cibernético se ha vuelto más complejo y desafiante a raíz de la pandemia, los resultados de la encuesta muestran que algunas empresas son conscientes del incremento en los ciberataques y, en algunos casos, han realizado esfuerzos adicionales, e incluso incrementado sus presupuestos con el fin de implementar controles que les permitieran mitigar dichos riesgos.

No obstante, se siguen observando empresas en las que esta situación no se ha manifestado y, consecuentemente, no perciben un incremento de los ciberataques. Esta situación podría deberse a la falta de mecanismos y procedimientos necesarios para detectar situaciones sospechosas que puedan sugerir un ataque, de manera oportuna.

La pandemia ha llevado a algunas empresas a realizar ajustes a sus presupuestos, incluyendo aquellos relacionados con seguridad de la información y ciberseguridad. Esta situación, podría haber limitado la capacidad de estas organizaciones para detectar y responder ante ciberincidentes de manera oportuna, principalmente en una realidad en la que los ciberataques se han incrementado de una manera tan significativa.

En algunas industrias se puede observar un mayor grado de adopción del seguro de Riesgo Cibernético como un medio para transferir este tipo de riesgos y como consecuencia de la pandemia, incluso, han considerado ampliar el límite asegurado o coberturas contratadas. Aún resulta preocupante que muchas compañías no cuenten con este tipo de seguro como parte de su gestión del Riesgo Cibernético; sin embargo, con el paso de la pandemia han cambiado su percepción sobre la posibilidad de adquirir uno.

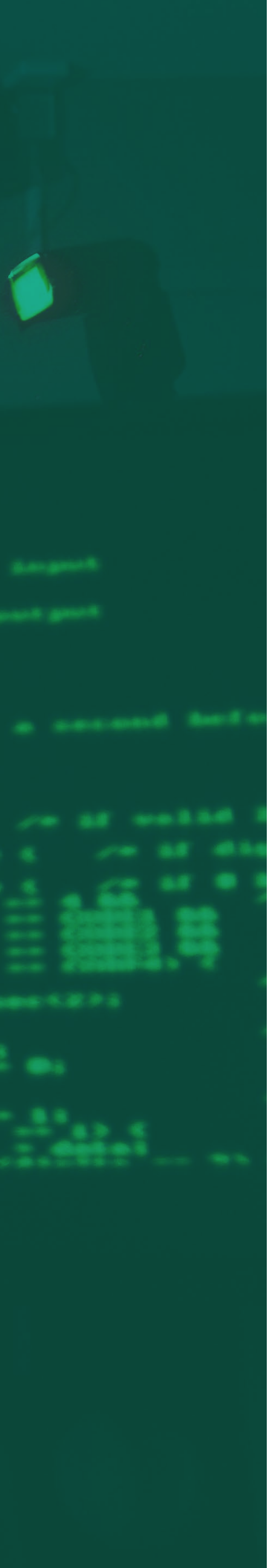
Las compañías han reevaluado sus prioridades de ciberseguridad con el fin de enfocar sus esfuerzos en implementar controles para mejorar la protección de datos, la seguridad de acceso remoto, la continuidad del negocio y la concientización en seguridad. Ahora más que nunca, y no solo como consecuencia de la pandemia, será importante para el funcionamiento de cualquier organización, mejorar su nivel de madurez en la implementación de dichos controles y cualquier otro que les permita mitigar los riesgos cibernéticos.

02

Aspectos destacados de la encuesta

La Encuesta de Marsh y Microsoft sobre Riesgo Cibernético en tiempos de COVID19 en Latinoamérica, busca identificar cómo se ha visto afectada la gestión de la ciberseguridad en las empresas debido a la pandemia, qué decisiones se tomaron para hacer una distribución más efectiva del presupuesto asignado a la gestión de la seguridad de la información y ciberseguridad, y qué acciones se llevarán a cabo en esta "nueva normalidad".

Los resultados de la encuesta muestran cómo las prioridades en ciberseguridad fueron reevaluadas, así como la importancia de analizar otras opciones como parte de una mejor gestión del Riesgo Cibernético.



Ciberataques en tiempos de pandemia

Dar continuidad a las operaciones críticas fue la prioridad de las organizaciones con la llegada de la pandemia. Para esto, fue necesario dar lugar al trabajo remoto y, en muchos casos, al uso de dispositivos personales.

- En el 70% de las empresas encuestadas, un grupo de sus empleados ha estado trabajando con sus dispositivos personales, llegando, en algunos casos, a más del 75% del total de su fuerza laboral.
- Solo el 27% de las compañías encuestadas afirmaron que sus empleados están trabajando exclusivamente con los dispositivos propios de la organización.
- El 31% de los encuestados han percibido un incremento en los ciberataques como consecuencia de la pandemia, siendo la principal amenaza los eventos de Ingeniería Social, como el Phishing.

Presupuesto de ciberseguridad

La asignación del presupuesto de tecnología y el porcentaje de los ingresos anuales que se invierten para la gestión de TI y ciberseguridad, varían mucho dependiendo de la industria, el tamaño de la empresa y, por supuesto, el apetito al riesgo de la organización.

- El 50% de los encuestados indicaron que el porcentaje de los ingresos anuales de la compañía invertidos en TI es menor al 5%. El 18% mencionaron que este porcentaje se encuentra entre el 5% y 15%. Solo el 5% manifestó que este porcentaje es mayor al 15%.
- Con relación al porcentaje del presupuesto de TI que se dedica a la seguridad de la información y ciberseguridad, se identifica que en la mitad de las empresas encuestadas este porcentaje es menor al 5%, seguido por un porcentaje del 16% de los encuestados que invierten entre el 5% y 15%. Solo el 7% de las empresas encuestadas invierten más del 15%.
- El 24% de los encuestados indicó que, como consecuencia de la pandemia, se incrementó el presupuesto de seguridad de la información y/o ciberseguridad.

Seguro de riesgo cibernético antes y después del COVID19

A medida que la percepción del Riesgo Cibernético aumenta en Latinoamérica, las organizaciones son cada vez más conscientes de la necesidad de gestionar de una manera integral este riesgo. Sin embargo, la penetración de este tipo de seguros en la región aún es muy baja, aunque cada año su contratación aumenta de manera exponencial y las organizaciones lo convierten en parte fundamental de su estrategia de gestión del riesgo.

- El 17% de las compañías encuestadas manifestaron que cuentan con un seguro de Riesgo Cibernético. El sector Financiero y el sector retail/wholesale son las industrias con el mayor porcentaje de contratación de esta cobertura.
- 23% de las empresas encuestadas han incrementado su percepción acerca de la importancia de la contratación de un seguro cibernético.

Prioridades de ciberseguridad

Las prioridades en ciberseguridad se han reevaluado en el trascurso del año debido a la pandemia, lo cual ha llevado a las compañías a enfocar sus esfuerzos de seguridad de la información y ciberseguridad, en la protección de datos y la seguridad en acceso remoto.

- El 14% de los encuestados manifestaron que la protección de datos es su prioridad número uno en materia de seguridad.
- La seguridad en acceso remoto es la primera prioridad para el 12% de los encuestados, y la segunda para el 7% de los encuestados.
- Solo para el 6% de los encuestados la concientización y entrenamiento de sus empleados es su principal prioridad.

03

Ciberataques en tiempos de pandemia y trabajo remoto

Con la llegada de la pandemia y, consecuentemente, el trabajo remoto, las organizaciones enfocaron sus esfuerzos en dar continuidad al negocio, permitiendo, en muchos casos, el uso de dispositivos personales para el desarrollo de sus operaciones.

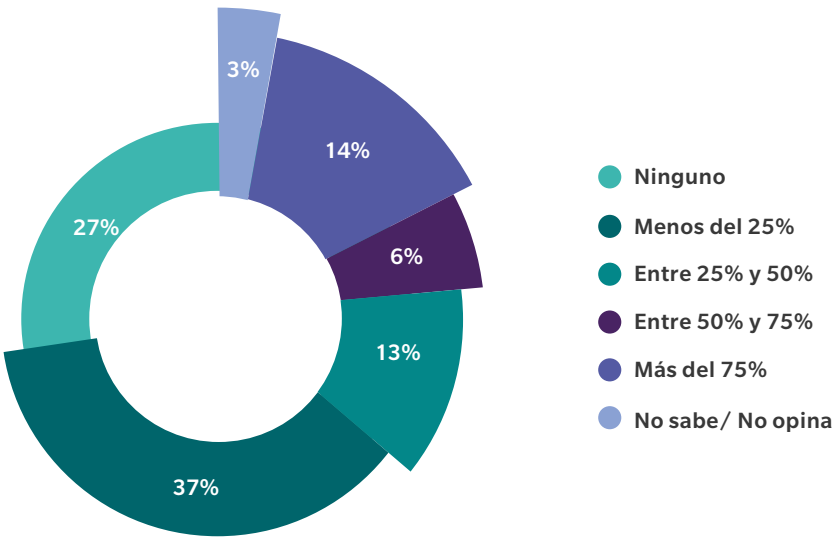
Sin embargo, sus consecuencias no se hicieron esperar y desde el inicio de la pandemia se ha presentado un incremento significativo en los ciberataques, especialmente los de ingeniería social.

Trabajo remoto y uso de dispositivos personales

Con la llegada de la pandemia, la prioridad de las compañías se enfocó en dar continuidad a las operaciones críticas del negocio con el fin de poder subsistir en la situación actual y mantener la generación de ingresos. Sin embargo, como consecuencia de lo anterior, las empresas se vieron obligadas a enviar a sus empleados a trabajar de manera remota desde sus hogares. Con este nuevo modelo de trabajo, se empezaron a observar excepciones a los estándares de seguridad definidos en la organización, particularmente en el uso de dispositivos personales y de redes no seguras, con un nivel de protección de seguridad menor a los requeridos.

En la mayoría de las empresas encuestadas, un grupo de sus empleados han estado trabajando con sus dispositivos personales, llegando, en algunos casos, a más del 75% de ellos. Solamente en el 27% de las compañías, los empleados están trabajando exclusivamente con los dispositivos otorgados por la organización.

¿Qué porcentaje del total de empleados de la compañía está trabajando con sus dispositivos personales y no con los que son propiedad de la organización (ej. laptops, smartphone, tablet)?

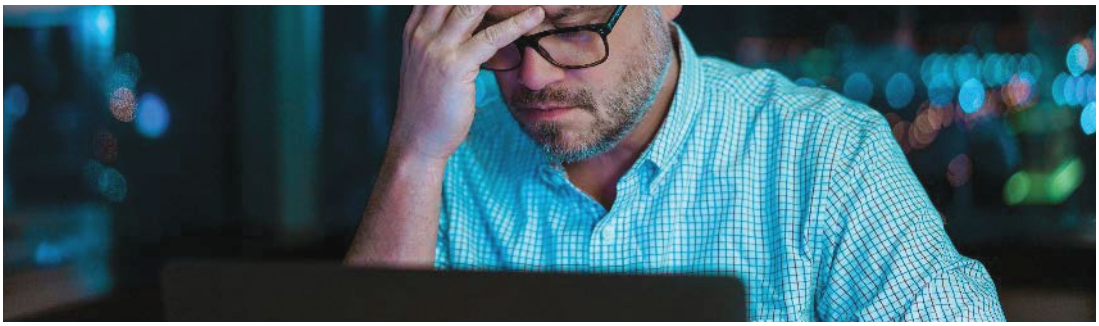


Con el uso de dispositivos personales que no están adecuadamente configurados ni monitoreados y, a través de los cuales se otorgó acceso a información confidencial y a los sistemas de las compañías, se incrementó exponencialmente la exposición al Riesgo Cibernético.

Lo anterior podría resultar en una potencial divulgación de información confidencial, intrusión por parte de individuos no autorizados, multas regulatorias, afectación a la continuidad de la operación, impactos reputacionales y, por su puesto, otorgar un mayor espectro de ataque para los cibercriminales.

Por otro lado, el trabajo remoto puso a prueba la capacidad de las compañías para identificar amenazas asociadas a este tipo de trabajo y su capacidad para aislar, proteger y, cuando sea necesario, restaurar la información y los servicios después de un ataque.

Todos estos cambios modificarían la postura de riesgo de la organización, pero lo más preocupante es que, a la fecha, muchas organizaciones no han evaluado qué tan expuestas están a los ciberataques bajo este nuevo panorama. Tampoco se han revisado las políticas y lineamientos de seguridad, las cuales, en algunos casos, ya no se pueden aplicar en este nuevo modelo de trabajo.



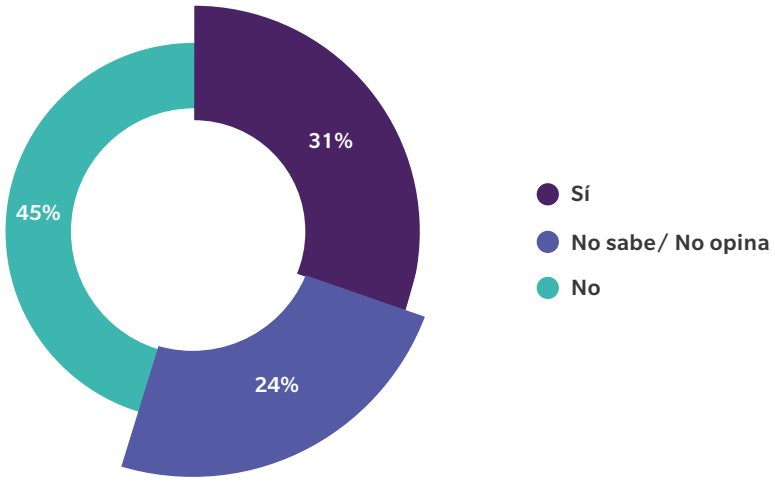
Ciberataques en tiempos de pandemia

Desde el inicio de la pandemia se ha reportado un incremento significativo en ciberataques, particularmente en el envío de emails maliciosos. Estos mensajes usan información relacionada con el COVID19, herramientas de comunicación y aprovechándose de la incertidumbre, el miedo y la situación económica de las personas, las engañan para que ingresen a enlaces sospechosos o descarguen archivos que están adjuntos en los correos y que incluyen diferentes tipos de malware, destacando los casos de ransomware y de troyanos. Todo esto con el fin de robar información personal que permita a los atacantes acceder a las cuentas personales o empresariales, acceder a sus archivos y redes, o realizar extorsiones.

Con relación al aumento en los ciberataques, el 31% de los encuestados ha percibido un incremento de este tipo de incidentes. Sin embargo, casi la mitad de los encuestados consideran que no ha habido un incremento. Esta última cifra puede obedecer a los siguientes factores:

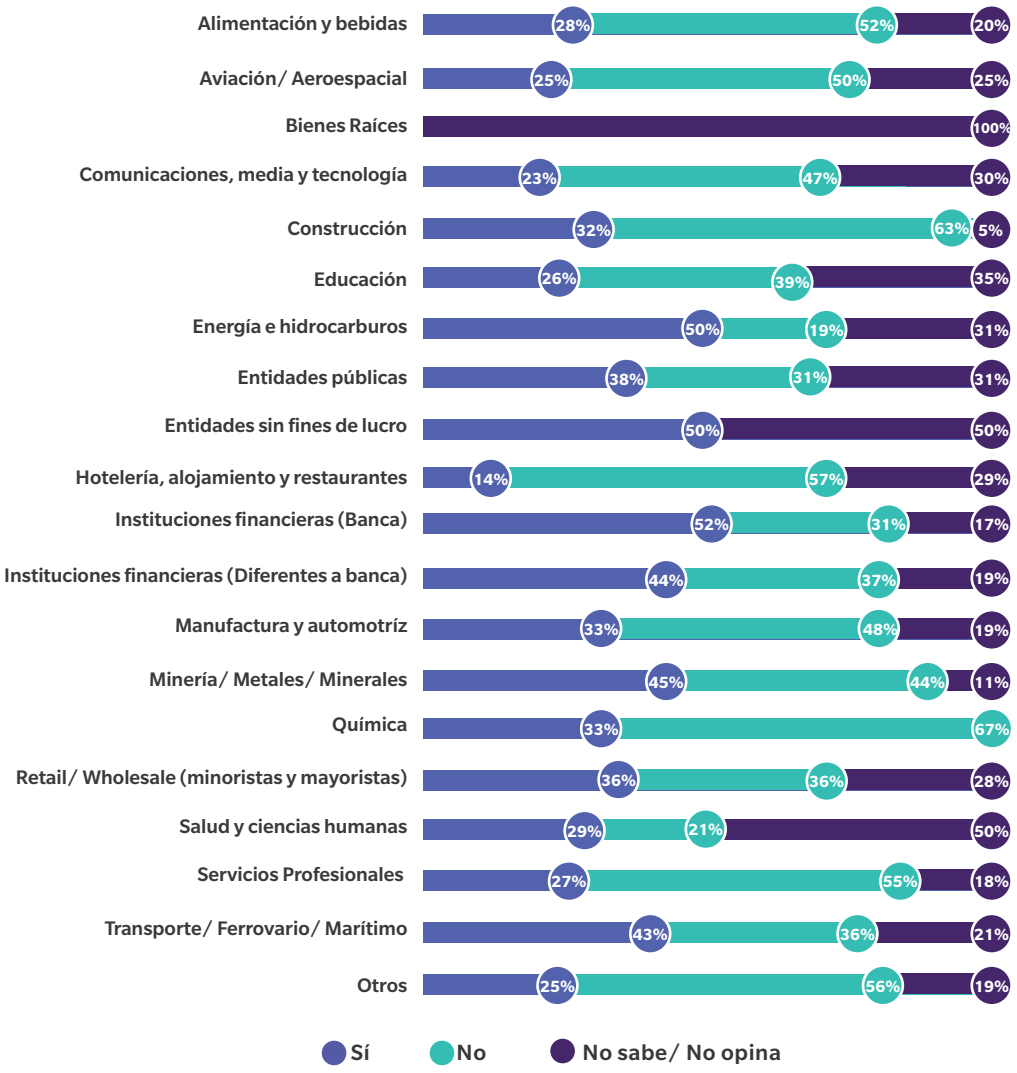
- Ausencia de adecuados mecanismos y procedimientos para detectar patrones sospechosos en la red de manera oportuna.
- Los sistemas de información y los activos críticos no son monitoreados periódicamente para identificar comportamientos inusuales que puedan evidenciar ciberataques contra la entidad.
- No se lleva un registro de los incidentes de ciberseguridad que han afectado a la organización, antes y durante la pandemia.
- Ausencia de revisiones de seguridad que permitan detectar debilidades que podrían ser o que ya hayan sido explotadas por ciberatacantes.

¿Su compañía percibe un incremento de ciberataques como consecuencia de la pandemia?



Con relación a las industrias que más han percibido un incremento en los ciberataques, encontramos las siguientes: financiera, energía e hidrocarburos, minería y transporte. Las industrias que no percibieron un incremento en ciberataques o que no saben si lo hubo, son: bienes raíces, organizaciones sin fines de lucro, hotelería, comunicaciones y tecnología, aviación, educación, servicios profesionales, salud y química.
Si bien no haber percibido un incremento en ciberataques puede estar asociado a los factores mencionados anteriormente, sí se ha podido observar durante la pandemia que hay industrias más afectadas que otras por los ciberataques.

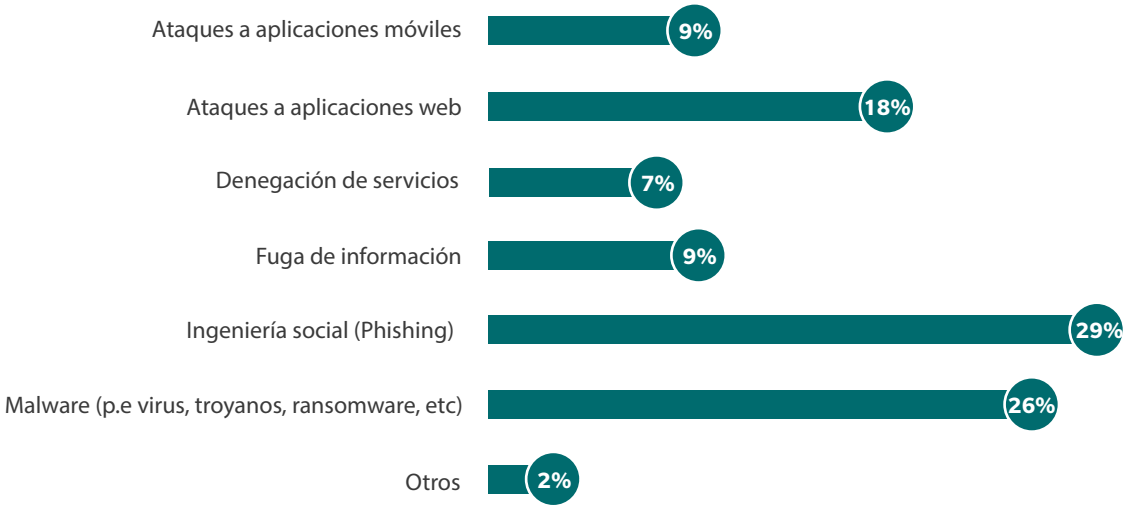
¿Su compañía percibe un incremento de ciberataques como consecuencia de la pandemia?



La crisis generada como consecuencia de la pandemia ha hecho que las estrategias que usan los ciberdelincuentes, especialmente los ataques de ingeniería social, sean cada día más sofisticados y efectivos, aprovechando las vulnerabilidades a nivel de la tecnología y de la cultura de ciberseguridad que enfrentan las empresas para trabajar remotamente.

Entre el 2019 y lo corrido de 2020 fueron evaluados más de 6 billones de correos electrónicos y fueron bloqueados más de 13.000 millones de correos maliciosos y sospechosos en la plataforma de Microsoft, de los cuales más de 1.000 millones fueron URLs configuradas con el propósito explícito de lanzar un ataque de phishing, tratando de robar la credencial de acceso y la identidad del usuario. Los grupos criminales son hábiles e implacables y se observó que aprovechan el miedo y la incertidumbre asociados con COVID-19 con gran éxito. El seguimiento de los ataques temáticos COVID-19 en el estudio de Microsoft muestra la rapidez con la que los ciberdelincuentes se mueven para adaptar sus acciones a los temas del día.

¿Qué tipo de ciberataques considera que se han incrementado?



Además de los ataques de phishing, los cibercriminales han creado aplicaciones o páginas web que aparentan entregar a los usuarios información relacionada con el virus, como datos actualizados en línea sobre la cantidad de contagios o síntomas y avances en el desarrollo de la vacuna, con el fin de llevar a las personas a descargar programas maliciosos.

Finalmente, es importante tener presente que todos estos ciberataques que hemos mencionado seguirán en aumento porque generalmente son muy rentables para los cibercriminales. Lo anterior debido a que estos ataques a menudo carecen de sofisticación para ser ejecutados, no siempre requieren muchos recursos financieros y son difíciles de atribuir a alguna persona o grupo en particular. Es por esto que las capacidades que tengan las empresas y sus trabajadores para identificar vulnerabilidades y detectar amenazas oportunamente, serán fundamentales para el funcionamiento de cualquier empresa en el entorno actual.

04

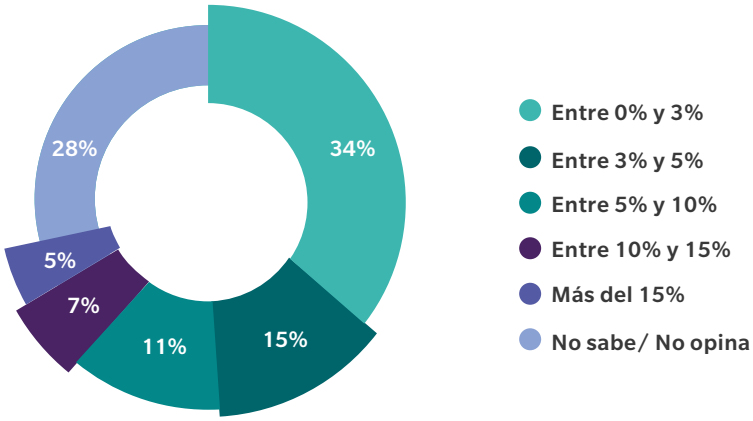
La evolución del presupuesto de ciberseguridad

La transformación digital, el panorama de las amenazas cibernéticas y, por supuesto, la pandemia, son algunos de los factores que tienen un alto impacto al momento de decidir cuánto debería asignarse a los presupuestos de seguridad de la información y ciberseguridad en las empresas; sin embargo, ¿sabemos qué tanto impacto ha tenido la pandemia sobre el presupuesto que había sido destinado a temas de seguridad de la información y ciberseguridad para este 2020?

Los presupuestos para gestionar la seguridad de la información y la ciberseguridad dependen de varios factores y no hay respuestas únicas que permitan determinar exactamente cuánto debería destinarse a estos presupuestos. Las consideraciones a tener en cuenta varían según la industria, el tamaño de la empresa, el nivel de exposición y, por supuesto, el apetito al riesgo de la organización.

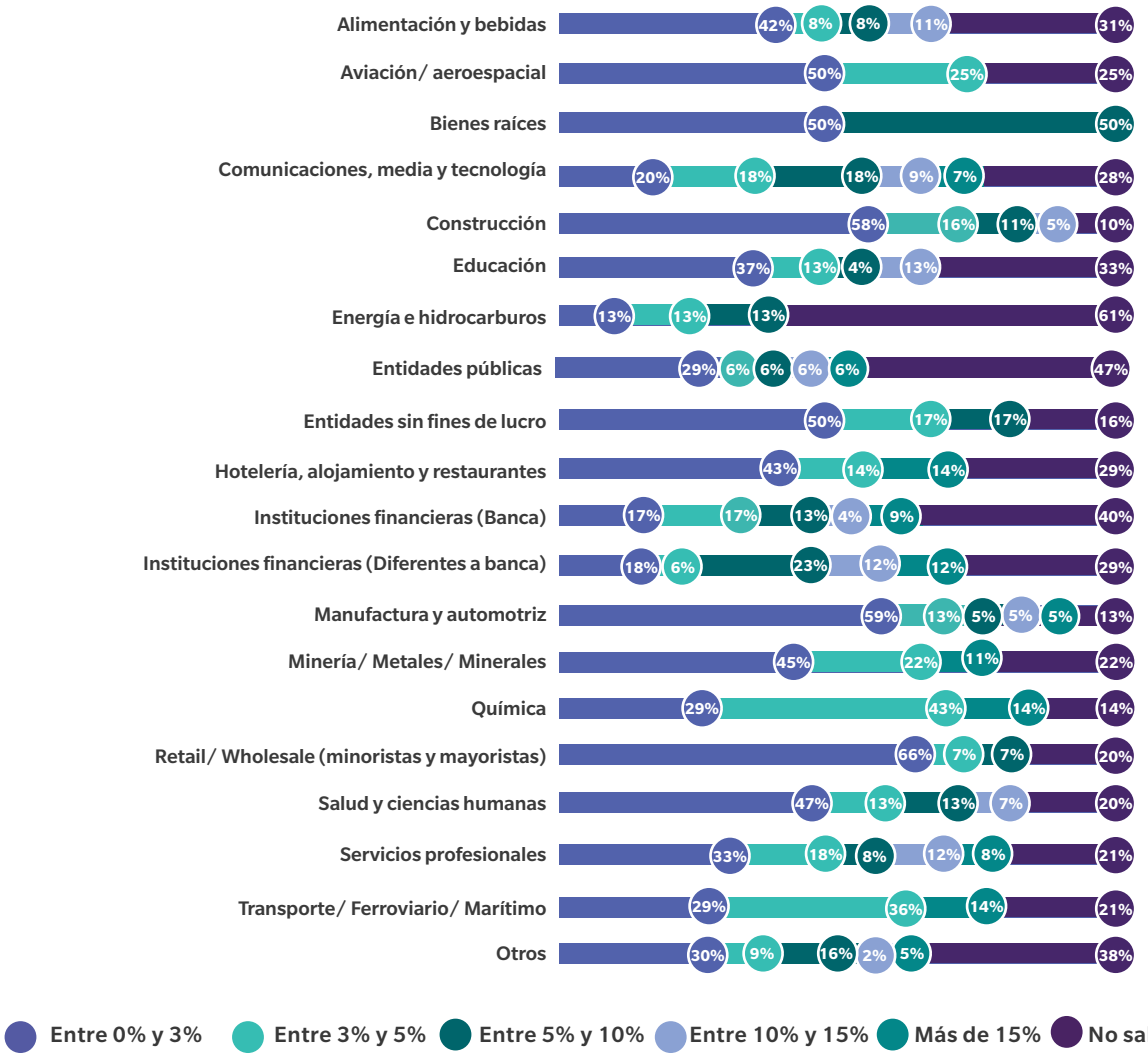
A pesar de ello, en este estudio quisimos brindar un benchmark del nivel de inversión del total de los ingresos de la organización en TI y, como una medida referencial, el porcentaje del presupuesto de TI invertido en Seguridad. Como resultado de la encuesta se observa que la mitad de los encuestados indican que este porcentaje de los ingresos anuales de la organización invertido en TI es menor al 5%, seguido por un 18% de las empresas que indican que este porcentaje se encuentra entre el 5% y 15%. Solo el 5%, indica que este porcentaje es mayor al 15%.

¿Cuál es el porcentaje de los ingresos anuales de la compañía invertidos en TI?



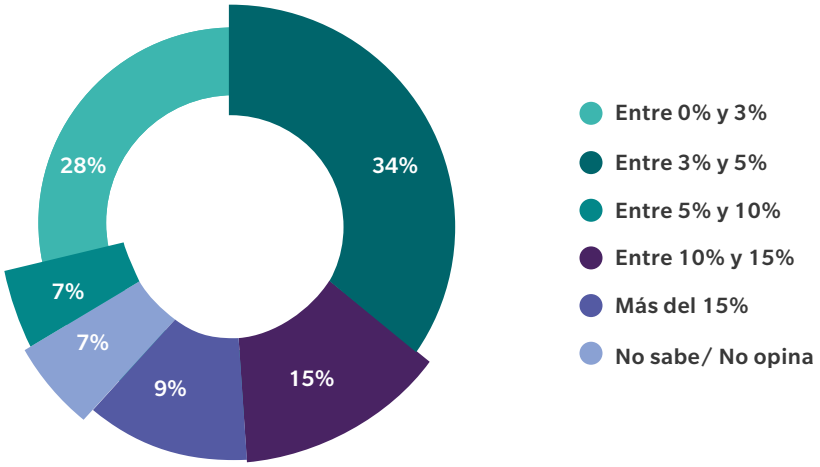
Podemos identificar que las industrias cuyo porcentaje de ingresos anuales invertidos en TI es menor al 5% son: aviación, retail/wholesale, construcción, manufactura y automotriz y química, seguidas por la industria financiera que invierten entre el 5% y 15% de sus ingresos anuales. Finalmente, se puede evidenciar que algunas empresas del sector hotelero, financiero (diferentes a banca) y minería, asignan más del 15% del porcentaje de los ingresos anuales de la compañía a este concepto.

¿Cuál es el porcentaje de los ingresos anuales de la compañía invertidos en TI?



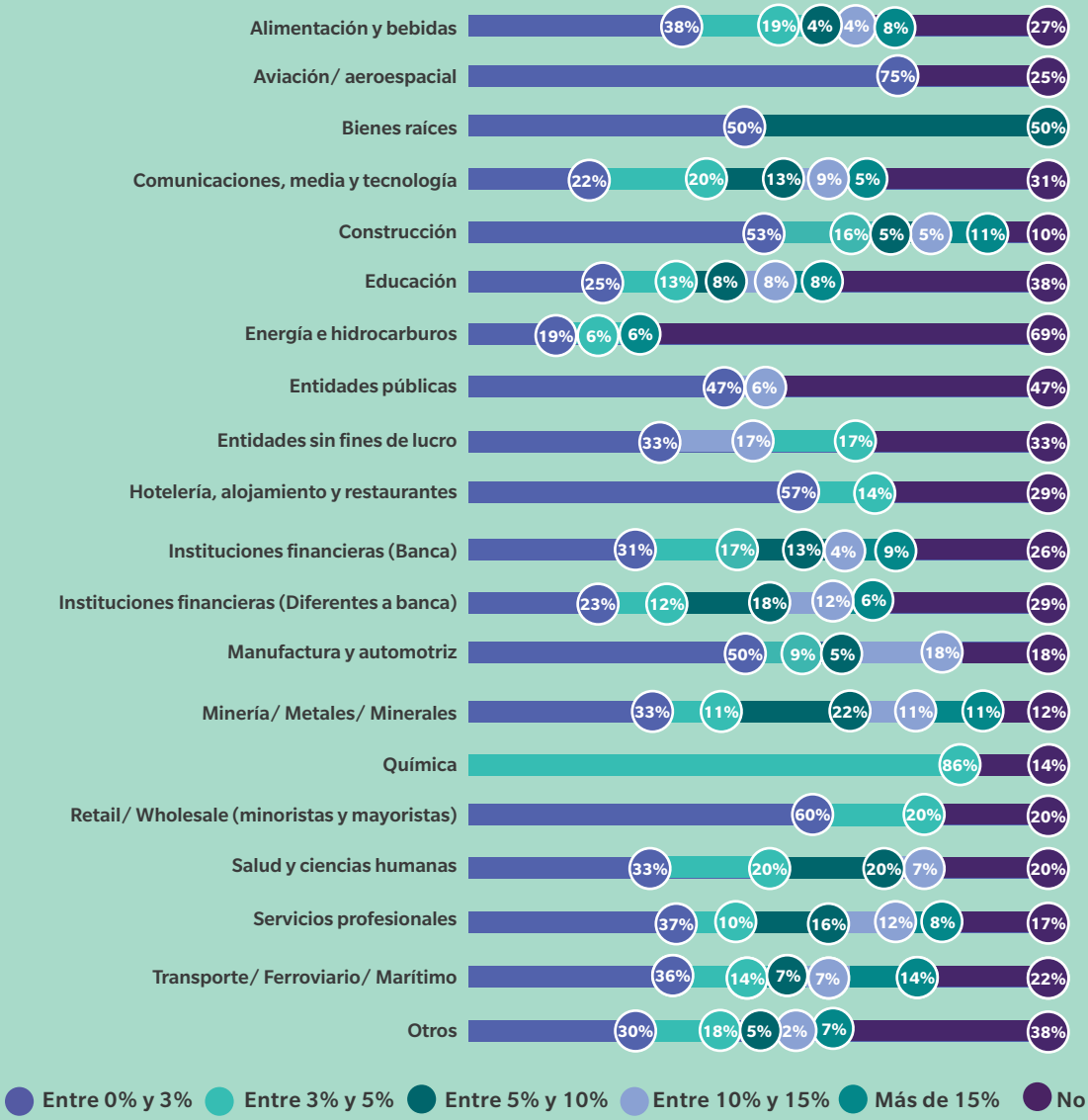
Por otro lado, al revisar qué porcentaje del presupuesto de TI se dedica a la seguridad de la información y ciberseguridad, identificamos que en la mitad de las empresas encuestadas este porcentaje es menor al 5%, seguido por un porcentaje del 16% de los encuestados que invierten entre el 5% y 15%, y solo el 7% de las empresas encuestadas invierten más del 15%.

¿Qué porcentaje del presupuesto de TI se dedica a seguridad de la información y/o ciberseguridad en la compañía?



Las industrias que menor porcentaje del presupuesto de TI dedican a la seguridad de la información y ciberseguridad son: química, retail/whosale, hotelería y construcción. Las industrias de bienes raíces, minería, financieras (diferentes a Banca) y de servicios profesionales, asignan entre el 5% y 15% del presupuesto de TI. Finalmente, algunas entidades sin ánimo de lucro y de transporte asignan más del 15%.

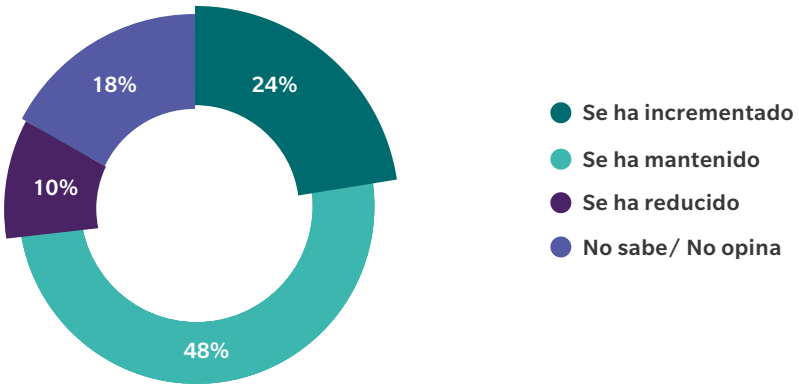
¿Qué porcentaje del presupuesto de TI se dedica a seguridad de la información y/o ciberseguridad en la compañía?



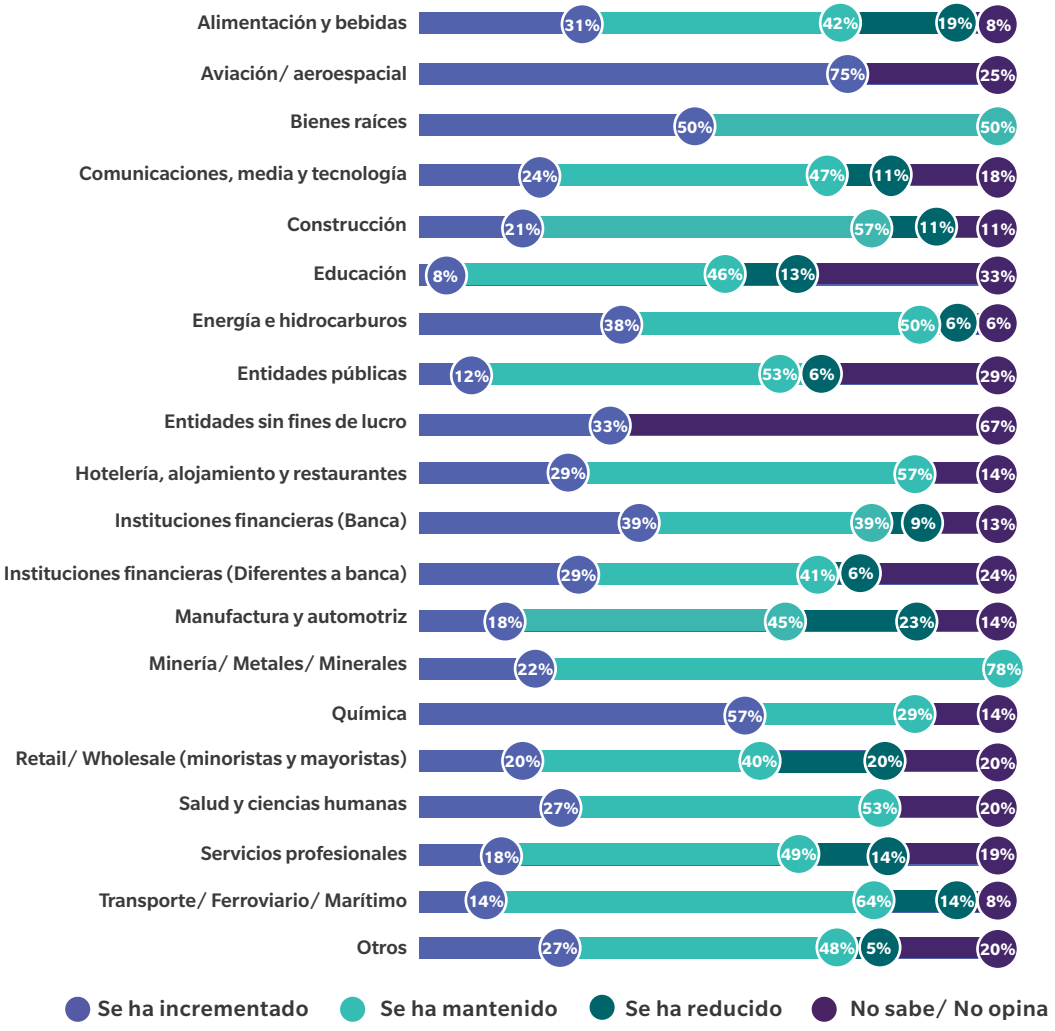
Factores como la transformación digital y el panorama de las amenazas cibernéticas tienen un impacto sobre cuánto debería asignarse a los presupuestos de ciberseguridad en las empresas. Sin embargo, la pandemia ha sido un factor relevante durante este año y, en algunos casos, ha llevado a las empresas a modificar su presupuesto de seguridad de la información y ciberseguridad. Esta modificación en el 24% de los encuestados, implicó un incremento en el presupuesto, posiblemente para implementar controles para el trabajo remoto y los riesgos asociados.

A pesar de la pandemia, la mitad de los encuestados indican que mantuvieron su presupuesto, y un 10% indica que fue reducido. De las industrias que incrementaron su presupuesto se encuentran: química, bienes raíces, financiero (Banca), y energía e hidrocarburos. En contraste, las industrias que decidieron reducir su presupuesto son: manufactura y automotriz, retail/whosale, y alimentos y bebidas.

¿Cómo se ha modificado el presupuesto de seguridad de la información y/o ciberseguridad en la compañía a partir de la pandemia?



¿Cómo se ha modificado el presupuesto de seguridad de la información y/o ciberseguridad en la compañía a partir de la pandemia?

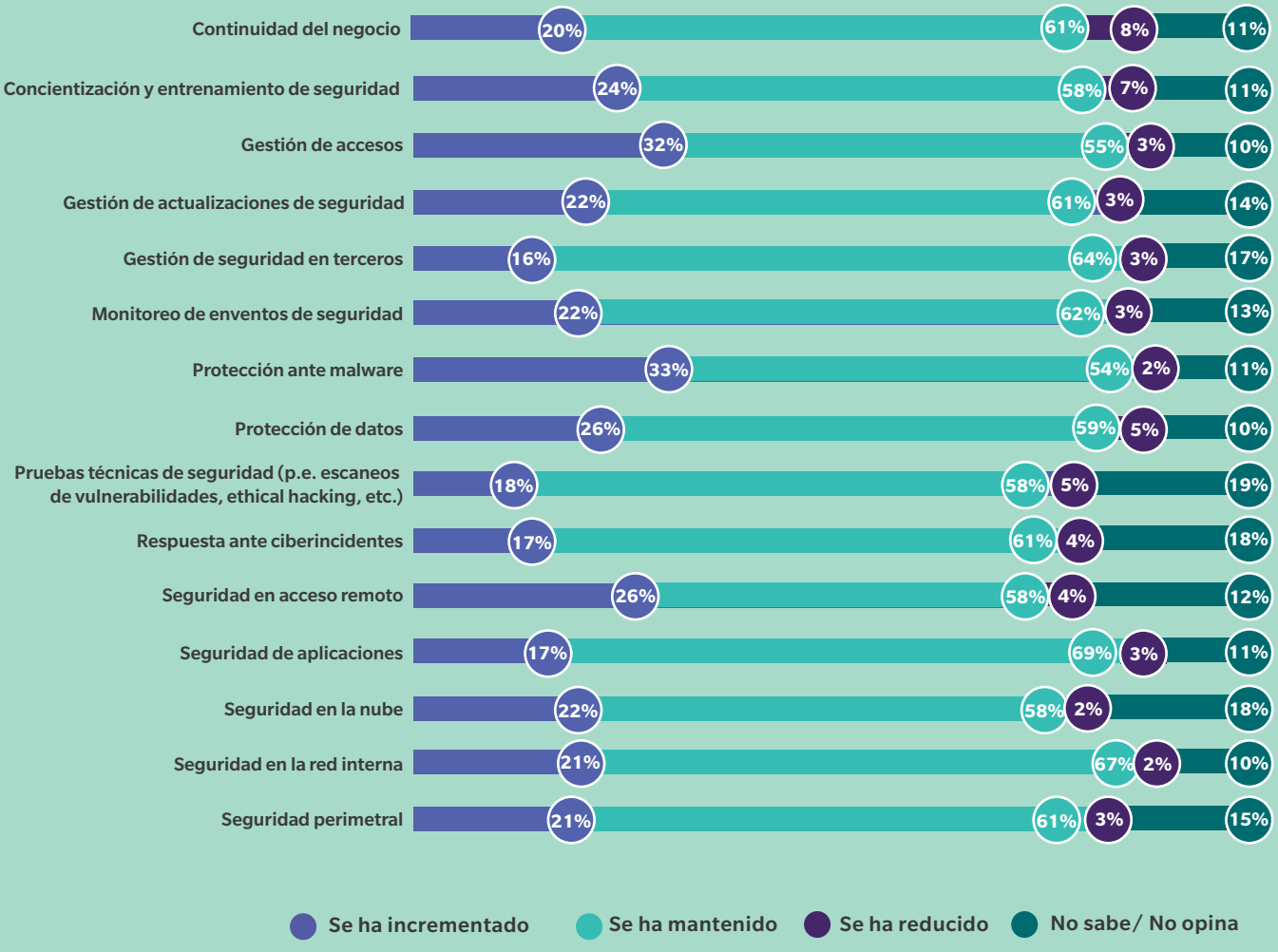


Independientemente de las decisiones tomadas con relación al presupuesto, muchas de las industrias mencionadas se han visto fuertemente afectadas por la pandemia. A la fecha, en varios países, apenas un porcentaje menor de empleados están regresando a las oficinas, se han activado solo algunos vuelos nacionales e internacionales, y el número de clientes que va a los restaurantes es reducido, por citar algunos ejemplos de las consecuencias de la pandemia.

Si bien es cierto que los gerentes o directivos de una organización tienen muy poco control sobre la propagación de la pandemia, sí son responsables del manejo que les den a los riesgos a los que se están enfrentando como consecuencia de la misma. Es por esto que un aspecto a tener en cuenta cuando se hace necesario realizar una reducción del presupuesto, es hacer un análisis y cuantificación de la exposición de la compañía a los riesgos que enfrenta, de modo que se definan estrategias efectivas en cuanto a la mitigación y la transferencia del riesgo.

Finalmente, como consecuencia de la pandemia, las empresas se han visto obligadas a repensar la manera en la que destinan su presupuesto de seguridad. Entre los principales aspectos en los que se ha visto un incremento del presupuesto, se encuentra la protección ante malware, gestión de accesos, seguridad en acceso remoto y protección de datos. Sin embargo, un número menor de encuestados indican que se ha reducido el presupuesto para temas de continuidad del negocio, así como de concientización y entrenamiento de seguridad.

Como consecuencia de la pandemia ¿Cómo ha variado el presupuesto de seguridad de la información y/o ciberseguridad para los siguientes aspectos?



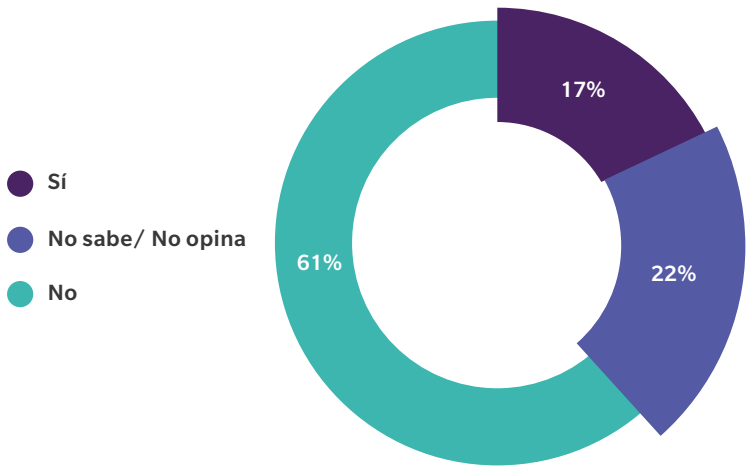
05

Seguro de riesgo cibernético antes y después del COVID19

A medida que la percepción del riesgo aumenta en Latinoamérica, las organizaciones son cada vez más conscientes de la necesidad de gestionar de una manera integral el Riesgo Cibernético. La transformación digital, la dependencia de la tecnología y, actualmente, la pandemia, han llevado a que las compañías consideren la contratación de seguros de Riesgo Cibernético como una parte fundamental de esta gestión.

A través de este tipo de seguros se transfiere el impacto financiero que una compañía puede sufrir como consecuencia de una afectación a su información (bases de datos, información confidencial de terceros, entre otra), su infraestructura tecnológica y sistemas de información (diseñados para almacenar, procesar, recuperar y distribuir información) y sus redes OT (tecnología operacional que permite detectar o cambiar los procesos físicos a través del monitoreo y control de dispositivos).

¿Su organización cuenta con un seguro de riesgo cibernético?



El bien que se busca proteger es un activo intangible (activos digitales) cuya afectación puede ocasionar, como ya se anticipó, un impacto financiero al asegurado, que se refleja en una pérdida de ingresos (lucro cesante sin daño material), incurrir en costos adicionales (costos para la reconstrucción de activos digitales, contratación de especialistas de cómputo forense, costos de expertos en relaciones públicas, entre otros) y, por último, daños a terceros (por ejemplo, por la divulgación de información confidencial o la infección de sistemas).

La penetración de este tipo de seguros aún es muy baja en Latinoamérica, como se evidencia en los resultados de la encuesta, donde solo el 17% de los encuestados afirman contar con este tipo de cobertura, versus un 61% que manifiesta no contar con la misma. No se puede perder de vista el alto porcentaje de encuestados, 22% del total de los participantes, que afirman desconocer si la organización cuenta o no con un seguro de Riesgo Cibernético. Este resultado puede ser la consecuencia de la falta de alineación entre las diferentes áreas de la organización en la gestión de este riesgo y la evidencia de que sigue siendo manejado por silos por parte de las diferentes áreas de la organización, sin contar con una gestión integral que incluya a todas las áreas de la compañía.

> No obstante la baja penetración de estos seguros, en los últimos años se ha incrementado de manera exponencial el número de colocaciones de este tipo en Latinoamérica, especialmente en países como Brasil, Colombia y México.

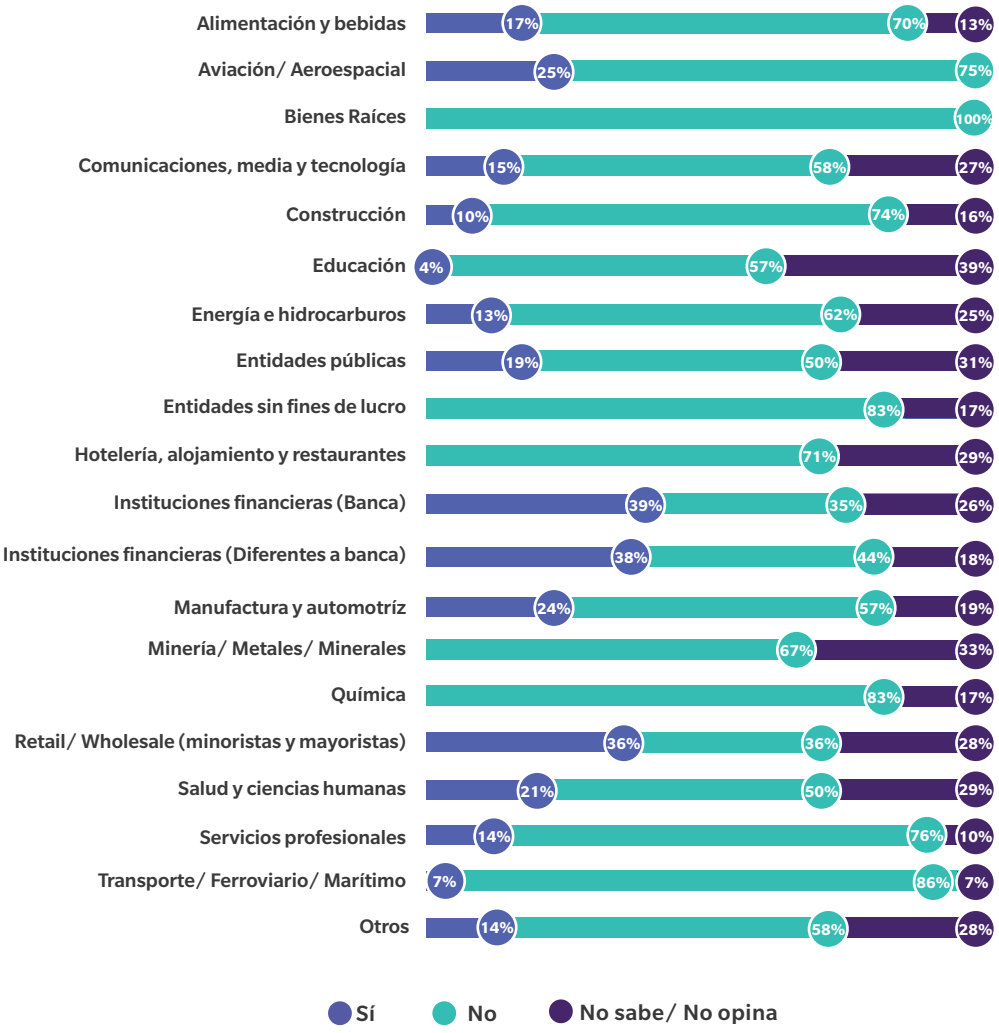
En los últimos meses, esta tendencia se ha incrementado aún más debido a la alta exposición al riesgo que se ha generado como consecuencia del trabajo remoto por el aislamiento social y el alto número de eventos que se han presentado en la región, algunos incluso de carácter público, que han generado a las compañías pérdidas muy cuantiosas, pérdidas que en parte podrían haber sido transferidas al mercado asegurador. En lo corrido de 2020 (enero a 30 de septiembre), Marsh Latinoamérica observó un crecimiento superior al 155% de colocaciones en la región versus el mismo período de 2019.

Históricamente la industria financiera ha sido una de las más afectadas por este tipo de incidentes y, a su vez, una de las más reguladas en torno a la gestión del Riesgo Cibernético, siendo uno de los sectores más maduros en la gestión del mismo. Por esto no es una sorpresa evidenciar que el 39% de las entidades bancarias y el 38% de las demás instituciones financieras diferentes a banca, cuentan con este tipo de coberturas. Muy de cerca sigue el sector retail/wholesale, con un 36% de los encuestados que afirma contar con un seguro de Riesgo Cibernético.

Sorprende que en la industria de hotelería y alojamiento ninguna de las compañías que participaron de este estudio cuenten con un seguro de Riesgo Cibernético. Este sector está altamente expuesto, no solo por tener que almacenar datos de tarjetas de crédito y débito, así como personales de ciudadanos de todas las nacionalidades, incluyendo ciudadanos de la Unión Europea, estadounidenses y, ahora, brasileños, que están protegidos por regulaciones en materia de protección de datos muy estrictas, sino por su dependencia a la tecnología para el desarrollo de su actividad.

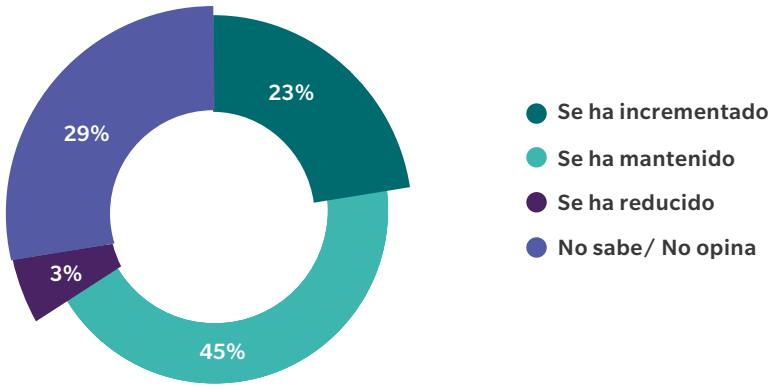
Finalmente, vale la pena resaltar el porcentaje en el sector de manufactura, donde el 24% de los encuestados manifiestan contar con esta cobertura. Este es un de los sectores en los que, precisamente, se ha evidenciado mayor preocupación en la gestión del riesgo, incluyendo la transferencia del mismo. Esto debido a la automatización de sus procesos productivos y el impacto que un evento cibernético les podría ocasionar.

¿Su organización cuenta con un seguro de riesgo cibernético?

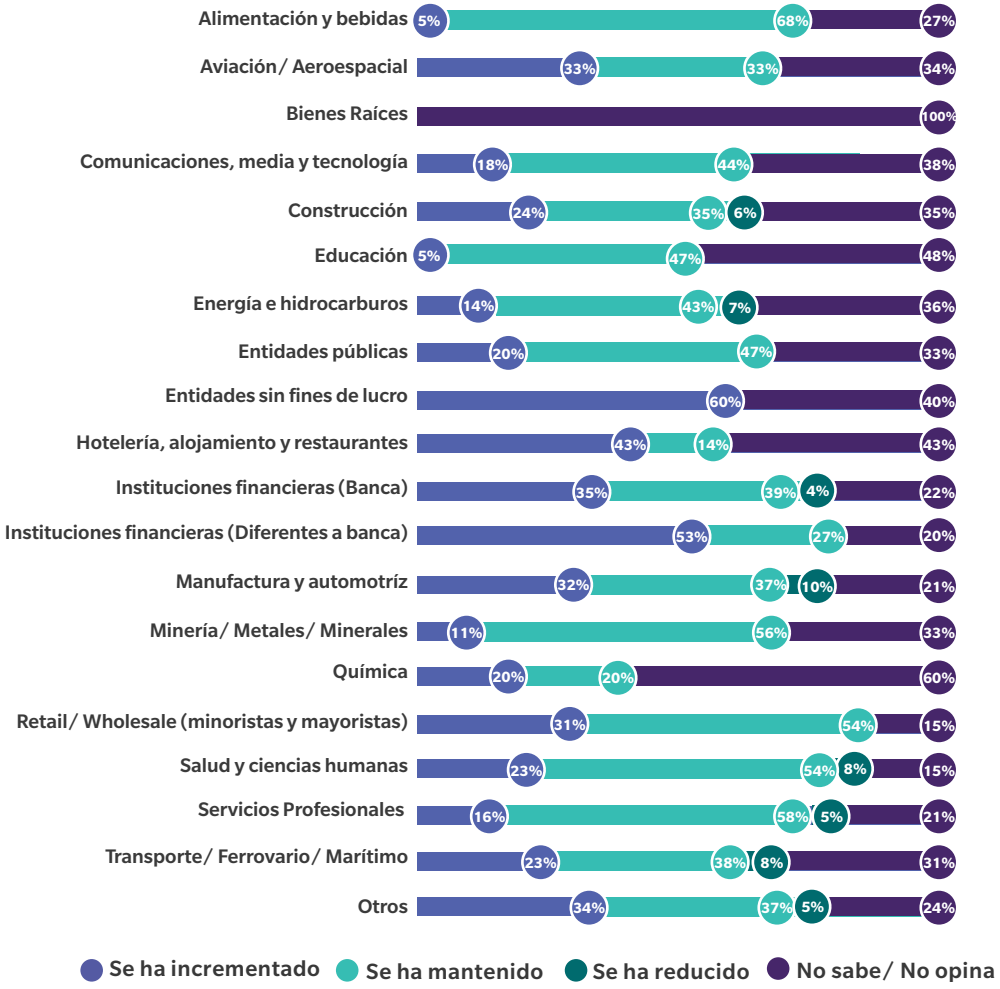


El nuevo modelo de trabajo remoto está cambiando la percepción de las organizaciones sobre la importancia de la contratación de seguros de Riesgo Cibernético. El 23% de los encuestados manifestó que su percepción sobre la relevancia de este mecanismo de transferencia aumentó y se puede evidenciar, por ejemplo, en sectores como el de hotelería, alojamiento y restaurantes, donde el 43% de los encuestados consideran que la importancia en la contratación de este tipo de seguros aumentó.

Como consecuencia de la pandemia ¿Cómo ha cambiado la percepción de su organización acerca de la importancia de la contratación de un seguro de riesgo cibernético?



Como consecuencia de la pandemia ¿Cómo ha cambiado la percepción de su organización acerca de la importancia de la contratación de un seguro de riesgo cibernético?



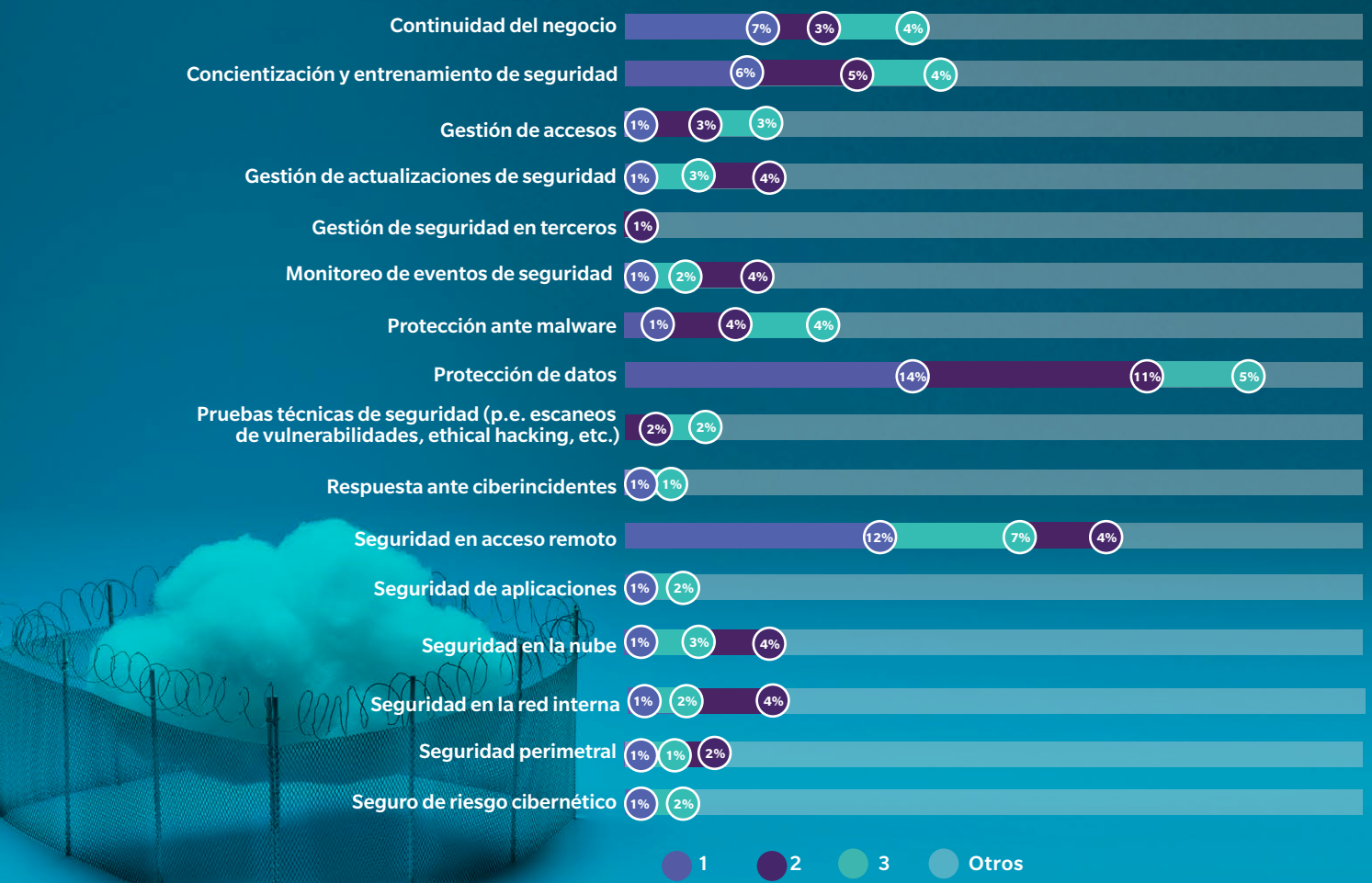
06 Prioridades de ciberseguridad en Latinoamérica

Con la llegada de la pandemia, las prioridades en ciberseguridad se han reevaluado en el trascurso del año. La protección de datos, la seguridad del acceso remoto y la continuidad del negocio, ocupan los primeros lugares entre la lista de prioridades de las compañías.

Entre las prioridades en materia de ciberseguridad, la protección de datos ocupa el primer lugar para los encuestados. El segundo lugar está dado por la seguridad en acceso remoto, lo cual está estrechamente relacionado al modelo de trabajo que se ha desarrollado como consecuencia de la pandemia, y que seguirá extendiéndose por un período considerable de tiempo en varias industrias.

Por último, pero no menos importante para las empresas, se encuentra la continuidad del negocio, seguido por los procesos de concientización y entrenamiento en seguridad para los empleados.

¿Cuáles de los siguientes aspectos son sus tres principales prioridades?



Teniendo en cuenta las principales prioridades de las compañías en temas de ciberseguridad, a continuación revisamos los aspectos que deben tenerse en cuenta para mejorar su gestión a nivel de protección de datos y seguridad en acceso remoto:

Protección de datos

Debido al aumento de ataques cibernéticos y los métodos innovadores de los ciberdelincuentes, las empresas deben desarrollar e implementar estrategias que les permitan proteger sus datos confidenciales y reducir el impacto de estos ataques. Estas estrategias deberían considerar:

- Identificar dónde la empresa se encuentra en mayor riesgo y cuánto podría costarle un ciberataque. Esto le ayudará a definir dónde debe concentrar su tiempo y recursos.
- Desarrollar una Política de Protección de Datos para definir y administrar las formas en que la empresa puede mitigar el riesgo cibernético. La política puede abarcar: cómo se almacenan los datos, quién tiene acceso a los sistemas, cómo se deben usar el correo electrónico y el acceso a Internet, y cómo informar un incidente cibernético.
- Realizar y mantener un inventario de activos de información.
- Implementar mecanismos para el monitoreo, detección y bloqueo oportuno de intentos de fuga de información.
- Determinar cómo responderá la empresa y se recuperará de una brecha de datos, incluida la notificación a los terceros afectados, la gestión de los medios y la recuperación de datos perdidos.

Seguridad en acceso remoto

Ya se ha mencionado cómo ha venido evolucionando el trabajo remoto durante la pandemia y las consecuencias que se han dado debido a las formas en que se tuvo que dar acceso remoto a los trabajadores. Es por esto que, sobre este aspecto, es importante mencionar algunos consejos de seguridad para el trabajo remoto:

- **Seguridad corporativa:**
  - Proporcione a los empleados mensajes de comunicación y concienciación periódicos, incluidos conocimientos básicos de seguridad.
  - Cree una dirección de correo electrónico para reenviar correos electrónicos sospechosos (phishing).
  - Actualice la Política de Uso Aceptable de su empresa para abordar el trabajo desde casa y el uso de activos informáticos domésticos.
  - Identifique funciones que solo se pueden realizar en un entorno seguro en la oficina (es decir, no de forma remota).
  - Desarrolle manuales específicos de COVID-19 y adapte los planes de respuesta ante ciberincidentes y recuperación ante desastres al contexto actual.
  - Asegúrese de implementar las actualizaciones de software de manera oportuna.
  - Utilice un sistema de gestión de usuarios privilegiados.
  - Fomente el uso de herramientas de gestión de contraseñas y ejecute auditorías de contraseñas.
  - Habilite la autenticación multifactor en todas partes, especialmente en cuentas de correo electrónico, servicios de VPN y conexiones remotas, y otros servicios expuestos a Internet.
  - Proporcione controles de seguridad en el hogar para los empleados y brinde canales de soporte.
- **Seguridad del hogar (para empleados)**
  - Restablezca las contraseñas predeterminadas del enrutador Wi-Fi doméstico y habilite el cifrado WPA2.
  - Nunca deje su computador y otros dispositivos móviles desatendidos en espacio público o desbloqueado en su casa.
  - No use el computador portátil del trabajo para fines personales, no comparta su equipo con los miembros de su familia, ni use un computador personal para el trabajo si tiene un equipo corporativo.
  - Evite el uso de memorias USB y otros dispositivos de almacenamiento extraíbles. En su lugar, utilice el almacenamiento en la nube o el mecanismo de almacenamiento autorizado por la empresa.
  - Mientras trabaja desde casa, silencie o apague cualquier asistente digital (por ejemplo, Alexa, Google Home, etc.) ya que estos puden grabar conversaciones cercanas.
  - Mantenga un área de trabajo limpia y habilite un bloqueo de pantalla de 5 minutos.
  - Guarde todos los documentos en papel de forma segura y destrúyalos antes de desecharlos.

07

Conclusiones

El trabajo remoto ha permitido que las organizaciones sean más conscientes sobre la exposición que tienen al Riesgo Cibernético y la necesidad de gestionarlo adecuadamente.

Sin embargo, este riesgo ha estado latente hace varias décadas y ha evolucionado a pasos agigantados. Para una adecuada gestión se deben seguir una serie de buenas prácticas, que les permitirán a las compañías reducir la probabilidad de materialización del riesgo o las equiparán con herramientas para responder y recuperarse de una manera más rápida y eficiente. A continuación, se detallan algunas de estas prácticas:

- Teniendo en cuenta que la pandemia forzó a las empresas a adoptar esquemas de trabajo remoto, éstas se deben asegurar de tener implementados los controles más críticos para trabajar bajo esta modalidad. Lo más recomendable es realizar una evaluación de ciberseguridad en trabajo remoto e implementar los controles necesarios para mitigar sus riesgos principales.
- Realizar periódicamente sesiones de concientización y entrenamiento a sus empleados en seguridad de la información y ciberseguridad. Dentro de las sesiones, se debe buscar aumentar la conciencia de los empleados sobre los riesgos de manejar información confidencial o sensible, identificar correos electrónicos sospechosos y mostrarles la relevancia de una adecuada gestión del riesgo por su parte y los posibles efectos de un uso inseguro de los recursos tecnológicos de la organización. Para esto, es importante que previamente se evalúe la cultura de ciberseguridad con el objetivo de implementar planes de concientización a la medida de las necesidades de la organización.
- Revisar y actualizar los procedimientos de ciberseguridad existentes, garantizando que los mismos se adapten a la nueva realidad y sean útiles para la detección, respuesta y recuperación ante un entorno tan cambiante.
- Con el fin de detectar oportunamente incidentes de seguridad, evaluar la viabilidad de:

  - Implementar mecanismos que permitan detectar oportunamente los ciberataques.

  - Monitorear periódicamente los sistemas de información y los activos para identificar comportamientos inusuales que puedan evidenciar ciberataques contra la entidad.

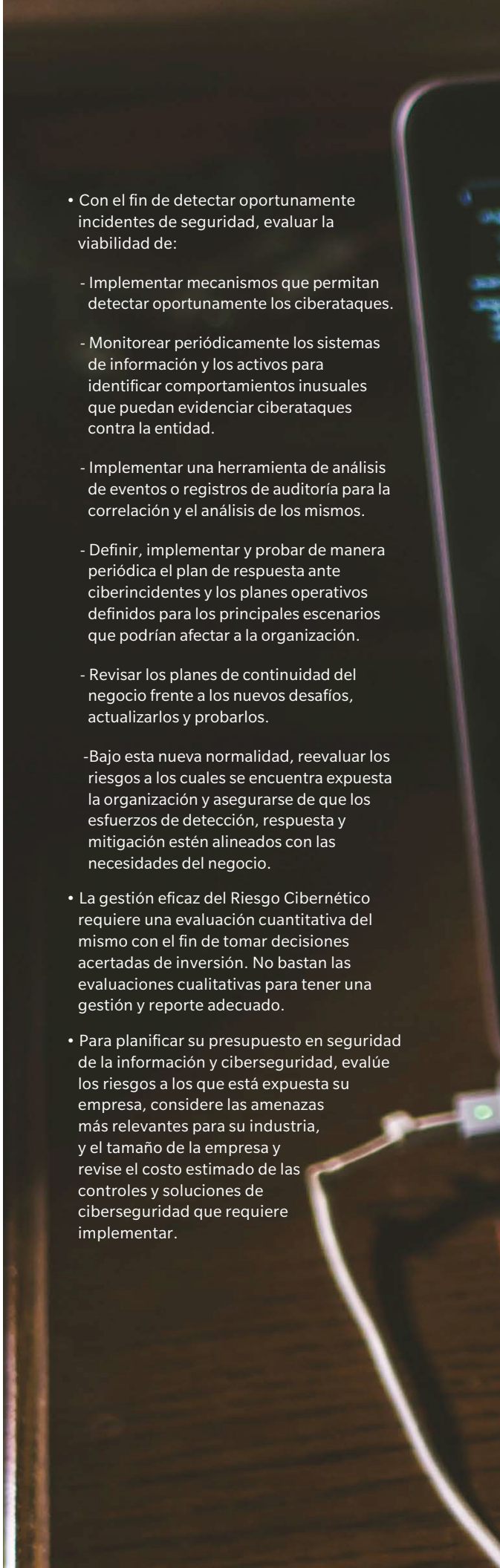
  - Implementar una herramienta de análisis de eventos o registros de auditoría para la correlación y el análisis de los mismos.

  - Definir, implementar y probar de manera periódica el plan de respuesta ante ciberincidentes y los planes operativos definidos para los principales escenarios que podrían afectar a la organización.

  - Revisar los planes de continuidad del negocio frente a los nuevos desafíos, actualizarlos y probarlos.

  -Bajo esta nueva normalidad, reevaluar los riesgos a los cuales se encuentra expuesta la organización y asegurarse de que los esfuerzos de detección, respuesta y mitigación estén alineados con las necesidades del negocio.

- La gestión eficaz del Riesgo Cibernético requiere una evaluación cuantitativa del mismo con el fin de tomar decisiones acertadas de inversión. No bastan las evaluaciones cualitativas para tener una gestión y reporte adecuado.
- Para planificar su presupuesto en seguridad de la información y ciberseguridad, evalúe los riesgos a los que está expuesta su empresa, considere las amenazas más relevantes para su industria, y el tamaño de la empresa y revise el costo estimado de las controles y soluciones de ciberseguridad que requiere implementar.



- No existen tecnologías o procesos que eliminen el Riesgo Cibernético y, en muchas ocasiones, las pérdidas generadas por la materialización de dichos riesgos pueden impactar de forma crítica las finanzas y operaciones de las compañías. Por esto, la transferencia del riesgo se convierte en un complemento indispensable para la gestión integral del mismo.

- El Riesgo Cibernético impacta a todas las áreas del negocio, por lo que se hace indispensable evaluar los mecanismos de gestión, incluida la transferencia en seguros tradicionales para entender si los impactos que se puedan generar a través de la materialización de este riesgo están siendo tratados de manera adecuada. Un análisis de brechas de cobertura en los programas de seguro tradicionales es fundamental para tener un entendimiento claro de la situación de la compañía.

08

Microsoft Defense Report - 2020

Introducción:

En septiembre de 2020, Microsoft publicó un estudio sobre la situación. de la seguridad, destacando los acontecimientos globales de los últimos 12 meses y las observaciones de las actividades de ciberdelincuencia (1). Hemos podido observar que en tiempos de crisis, los ciberdelincuentes continúan e incluso incrementan su actividad y se busca reducir el impacto de los ataques, lo cual es un desafío complejo, en constante evolución y sin fin.

Los datos del informe se generaron con base en la base de los miles de millones de clientes a los que Microsoft presta servicio en todo el mundo, lo que le permite agregar datos de seguridad de un amplio y diverso espectro de empresas, organizaciones y consumidores. Esto nos permitió generar una imagen clara del estado actual de la ciberseguridad, incluyendo indicadores que nos ayuden a predecir lo que los atacantes harán a continuación. Esta foto del estudio es generada por más de 8 billones de señales por día (2), incluyendo la nube, los endpoints y la inteligencia perimetral. También compartimos lecciones aprendidas de los clientes que tuvieron que pasar a un esquema de trabajo totalmente remoto y a historias de primera línea de nuestros profesionales de respuesta a incidentes que ayudan a los clientes de todo el mundo a responder a los ataques más diversos.

Estas señales son evaluadas por miles de expertos en seguridad en 77 países, que interpretan y contribuyen con nuestra ingeniería avanzada y telemetría para obtener la información necesaria. Nuestros expertos en seguridad incluyen analistas, investigadores, ingenieros y científicos de datos.

Los siguientes son algunos temas presentados en el informe de Microsoft que refuerzan los puntos señalados en el informe regional para LATAM publicado conjuntamente entre Marsh y Microsoft.

El estado de la ciberdelincuencia

La ciberdelincuencia es un negocio y, como cualquier otro negocio, necesita innovar para ser rentable y exitoso. Los ciberdelincuentes se pueden encontrar a nivel mundial y tienen diferentes conjuntos de habilidades y motivaciones. Ellos son oportunistas y la falta de higiene básica de la seguridad en cualquier ecosistema sigue permitiéndoles utilizar vulnerabilidades conocidas o variantes de ellas, para explotar sus entornos.

También aprovechan con gran éxito el miedo y la incertidumbre asociados con COVID-19. Si bien los ataques con temas relacionados a COVID-19 representan un pequeño porcentaje del malware total que observamos, nuestro seguimiento de estos ataques muestran la rapidez con la que los ciberdelincuentes se mueven para adaptar sus actividades a los temas del día.

Por supuesto, COVID-19 fue sólo uno de los temas explorados por los ciberdelincuentes. La Unidad de Delitos Digitales (DCU) de Microsoft trabaja con socios y autoridades en más de 50 países para tomar medidas legales y técnicas coordinadas para eliminar dominios y direcciones URL malintencionados y, cuando sea posible, procesar a las personas responsables.

El gran objetivo de los ciberdelincuentes, ahora más que nunca, es la identidad. Quieren obtener credenciales de acceso a cualquier costo, a menudo, no sólo para atacar a la empresa que tiene una credencial comprometida, sino también para utilizar ese acceso con el objetivo de afectar a otros entornos, ejecutando ataques conocidos como BEC (Business Email Compromise).

El compromiso de correo electrónico empresarial es un tipo de phishing que se dirige específicamente a las empresas. Se caracteriza por las técnicas utilizadas para hacerse pasar por alguien a quien las víctimas probablemente tomen gran importancia, como el CEO de la compañía, CFO, o un empleado de Contabilidad. BEC también puede implicar una transacción de negocio a negocio. Por ejemplo, el ciberdelincuente puede acceder al sistema de una empresa y luego hacerse pasar por esa empresa para solicitar fraudulentamente un pago.

Históricamente, los ciberataques eran vistos como un sofisticado conjunto de acciones dirigidas a ciertas industrias, lo que dejó a las industrias restantes creyendo que estaban fuera del ámbito de la ciberdelincuencia y sin contexto sobre las amenazas a las que debían hacer frente.

El ransomware representa un cambio importante en este panorama de amenazas, y ha hecho de los ataques cibernéticos un peligro muy real y omnipresente para todos. Los archivos cifrados y perdidos, y las notas de rescate amenazantes se han convertido en el mayor temor para la mayoría de los equipos ejecutivos.

El modelo económico de ransomware capitaliza la percepción errónea de que un ataque ransomware es sólo un incidente de malware, mientras que en realidad ransomware es una violación que involucra a adversarios humanos atacando una red.

Basándose en el trabajo realizado por el equipo de respuesta a incidentes de Microsoft durante los últimos 12 meses, el Equipo de Microsoft Detection and Response Team – de Detección y Respuesta de Microsoft –DART, ha identificado que más del 70% de los ataques de ransomware operados por el hombre en el último año se originaron a partir de un simple ataque de fuerza bruta de RDP (4).

En este escenario de ataque, Azure AD vio también un aumento de los ataques basados en identidad mediante la fuerza bruta en las cuentas corporativas durante el primer semestre de 2020. Los ciberdelincuentes parecían aprovechar la interrupción causada por la respuesta de las organizaciones COVID-19.

El aprendizaje automático en este contexto desempeña un papel cada vez más central en las operaciones y productos de las organizaciones de todo el mundo, y también se ha convertido en una herramienta invaluable en la lucha contra la ciberdelincuencia; sin embargo, los algoritmos de Machine Learning también son blancos de ataque, por lo que es importante defenderse de los ataques a los sistemas de Machine Learning.

El Internet de las Cosas (IoT) también debería ser un punto de atención, después de todo, habían 26.66 mil millones de dispositivos activos de Internet de las cosas (IoT) en 2019, y se estima que para 2022 habrá 50 mil millones de dispositivos de consumo de IoT en todo el mundo (5). Si bien los fabricantes de dispositivos IoT tienen la responsabilidad de diseñar productos seguros, su rápida proliferación ha hecho que estos productos sean atractivos para un creciente volumen de ciberataques.

Y cuando se trata de amenazas internas, una gran cantidad de CISOs de todo el mundo se preguntan ahora: "¿Está mi organización efectivamente preparada para identificar y remediar los mayores riesgos internos?". Una de las razones de este problema es COVID-19 y la rápida transformación digital que ha obligado a las organizaciones a emprender. Según investigaciones recientes, más de 300 millones de empleados de oficinas están trabajando desde casa, con recursos limitados y un mayor estrés. (7) Estos empleados no solo están entrando en entornos empresariales y aplicaciones de negocio, sino también accediendo, editando y compartiendo datos confidenciales.

Recomendaciones basadas en el Informe de Defensa Digital de Microsoft.

Sobre la base de los billones de señales evaluadas por Microsoft, a continuación, presentamos algunas recomendaciones de seguridad importantes, que deben priorizarse en vista del escenario actual de transformación digital y ciberataques.

1. La adopción de la autenticación multifactor (MFA) puede evitar ataques basados en credenciales. MFA debe ser necesario para todas las cuentas administrativas y se recomienda encarecidamente para todos los usuarios. El método preferido debe ser la aplicación de autenticación en lugar de SMS o voz siempre que sea posible.

2. Capacitar a los empleados. En Microsoft, nuestra estrategia ha pasado de ser una mentalidad compatible a un modelo de desarrollo de aprendizaje y desarrollo de habilidades para adultos. Este modelo asegura la construcción de habilidades progresivamente para ayudarnos a lograr los resultados de comportamiento deseados y reducir el riesgo. Utilizamos una serie de micropresentaciones, o entrenamientos en línea más cortos, lanzados durante todo el año. Esta cadencia permite a los empleados absorber información en partes manejables, mantiene el compromiso de nuestros empleados y ayuda a solidificar sus habilidades para mejorar el conocimiento.

3. Para las organizaciones que usan tecnologías modernas como Windows 10, recomendamos la autenticación facial, Biometría de las manos o un código PIN.

4. Para las organizaciones con aplicaciones o procesos que necesitan autenticarse, se recomienda adoptar una solución de administración segura de contraseñas, como una bóveda de contraseñas, que requiere que los empleados usen contraseñas únicas y aleatorias para acceder a toda la información confidencial, y en todos los servidores y dispositivos, incluidos los controladores de IoT y la infraestructura de red, como routers y firewalls.

5. Para limitar el riesgo de ataque, las organizaciones también deben evaluar a sus proveedores de servicios para asegurarse de que siguen las prácticas recomendadas para el acceso con privilegios mínimos a cuentas y servicios. El acceso a la red para el soporte debe supervisarse y protegerse mediante la autenticación multifactor (MFA) y el acceso Just-In-Time.

6. La implementación de estrategias de Zero Trust para IoT/OT está justificada. Utilice una red independiente o dirigida para dispositivos IoT y OT. Considere políticas de segmentación más granulares dentro de la propia red de OT, en varias capas. Audite, y revalide identidades y credenciales con acceso autorizado a dispositivos, usuarios y procesos de IoT.

7. 21.000 horas es el tiempo que pasan anualmente los analistas de seguridad realizando pruebas de evaluación de falsos positivos (6). La explosión de datos y señales es un problema para muchos SOC y analistas. Busque SIEMs modernos que utilicen tecnologías como el aprendizaje automático para reducir los falsos positivos y aumentar las alertas que realmente importan. Machine Learning puede ayudar a identificar a los atacantes que utilizan técnicas basadas en el comportamiento, que pueden no ser detectadas por los sistemas basados en reglas tradicionales.

8. La aplicación de parches de seguridad para sistemas orientados a Internet es crítico para prevenir ataques. Al administrar la infraestructura VPN, es fundamental que las organizaciones conozcan el estado actual de los parches de seguridad relacionados.

9. Como dijo Satya Nadela: "Hemos visto dos años de transformación digital en dos meses". Con usuarios trabajando de forma remota, es obligatorio tratar cada acceso como si se originara de una red poco fiable, la estrategia de Zero Trust ayuda a solidificar la seguridad de las VPN para trabajar desde casa. Este es precisamente el enfoque necesario con los trabajadores remotos de hoy en día porque provienen de redes domésticas que no son de confianza y las arquitecturas VPN utilizadas para ampliar las redes corporativas a veces están fallando.

10. Los programas internos de gestión de riesgos exitosos deben integrarse con procesos que permitan la colaboración entre las partes interesadas clave de toda la organización, para tomar las medidas necesarias. No es sólo un problema de seguridad, sino que requiere la colaboración entre los equipos de seguridad, recursos humanos y legales para garantizar que los riesgos internos se identifiquen y se manejen de manera coherente con los requisitos conformidad.

11. Debido a que el 90% de los ataques comienzan con un correo electrónico, evitar el phishing (y sus variantes basadas en texto y correo de voz, vishing y SMiShing) puede limitar la oportunidad para que los atacantes tengan éxito. Las plataformas de higiene del correo electrónico que incorporan filtrado de enlaces y comprobación, como Safelinks, proporcionan la protección más completa.

12. La configuración incorrecta es otro vector de ataque prominente y un ejemplo de cómo los pequeños cambios pueden resultar en problemas importantes. La implementación de un sólido programa de gestión de cambios automatizado permite a las empresas revisar los cambios antes de que se realicen y confirmar que el cambio no abrirá una nueva ruta de ataque, ni pondrá a la organización en riesgo.

13. Toda organización está involucrada en el desarrollo de software, ya sea escribiendo por sí misma o comprándolo a un proveedor. Incluso si los controles robustos están en el lugar más bajo de la pila, la organización está en riesgo si la capa de aplicación no es segura. Recomendamos un ciclo de vida de desarrollo de software sólido que incluya modelado de amenazas, revisiones de diseño y pruebas de aplicaciones estáticas y dinámicas, y pruebas de penetración de producción.

Conclusiones

Las circunstancias de la pandemia COVID-19, y la respuesta corporativa a la misma, presentan una oportunidad para forjar la resiliencia en la empresa. Debemos utilizar las lecciones del pasado y las diversas estrategias que hemos puesto en marcha para sobrevivir a la pandemia en nuestra visión empresarial más amplia.

En cierta medida, la respuesta empresarial a COVID-19 ha cambiado nuestros procedimientos operativos, así como el vocabulario que utilizamos para describir las medidas reactivas y las lecciones aprendidas. Términos como "límite de seguridad ampliado", "resiliencia pandémica" e "infraestructura humana" son ahora objeto de análisis ejecutivos e informes de la junta en todo el mundo. Este nuevo vocabulario destaca el surgimiento de áreas críticas de resiliencia que las empresas tradicionalmente no examinan.

Sobre la base de las medidas que se han puesto en marcha para mejorar nuestra postura de seguridad e incorporar las lecciones aprendidas desde el comienzo de COVID-19, han surgido tres áreas críticas para guiar el impulso de la resiliencia empresarial.

1. Zona crítica 1 - Ampliar el límite de seguridad de la empresa más allá del perímetro tradicional.
2. Zona crítica 2- Priorizar la resiliencia operativa
3. Zona crítica 3- Validación de la resiliencia de la infraestructura humana

Referencias.

(1) https://www.microsoft.com/en-us/security/business/security-intelligence-report

(2) Estas señales se recopilan teniendo en cuenta la privacidad del cliente. Los datos que recopilamos dependen del contexto de sus interacciones con Microsoft y de las elecciones que realice, incluida su configuración de privacidad y los productos y características que utilice.

(3) Microsoft Defender para Office 365, Microsoft Defender para Endpoint, Microsoft 365 Defender y Microsoft Defender for Identity pueden proteger contra el phishing de credenciales y BEC.

(4) 5 https://www.bleepingcomputer.com/news/security/fbi-says-140-million-paid-to-ransomware-offers-defense-tips/

(5) https://cybertechaccord.org/iot-security/

(6) Instituto Ponemon; 30 Uso de la importancia del rol de Azure Active Directory (AAD)

(7) https://www.bcg.com/publications/2020/covid-remote-work-cyber-security.asp

CONTACTOS

Para más información puede ponerse en contacto con nosotros.

GERARDO HERRERA
Líder de Consultoría en Riesgos para Marsh Latinoamérica
Gerardo.herrera@marsh.com

EDSON VILLAR
Líder de Consultoría en Riesgo Cibernético para Marsh Latinoamérica
Edson.villar@marsh.com

ÁNGELA CUBILLOS
Consultora Senior en Riesgo Cibernético para Marsh Latinoamérica
Angela.cubillos@marsh.com

MARCELLO ZILLO NETO
Jefe de Asesoría en Seguridad para Latinoamérica Microsoft
Marcello.Neto@microsoft.com

PAULINA VÉLEZ
Líder de Seguro de Riesgo Cibernético para Marsh Latinoamérica
Paulina.velez@marsh.com

PAULA ORDOÑEZ
Líder de Productos Financieros (FINPRO) para Marsh Latinoamérica
Paula.ordonez@marsh.com

MARSH | Microsoft