Informe
LATAM CISO
2023

Perspectivas de CIBERSEGURIDAD de los Líderes de la Industria

LATAM CISO

Duke UNIVERSITY

Para más información, se puede comunicar con **info@latamciso.com**

LATAM CISO

Duke UNIVERSITY

Créditos

Center for Cybersecurity Policy and Law

Centro de Política y Derecho de Ciberseguridad

- Ari Schwartz
- Belisario Contreras
- Alex Botting

Duke University

- David Hoffman
- Daniel Rodríguez Maffioli
- Andy Kotz
- Sofia Bliss-Carrascosa
- Spencer Reeves

Digi Americas Alliance Members

aws CISCO CLOUDFLARE CROWDSTRIKE fluid attacks we hack your software Google LUMU

netskope paloalto NETWORKS tenable Trellix TREND MICRO

Índice

Prefacio

David Hoffman, Profesor de Steed Family, Duke University
Andy Kotz, Investigador, Duke University
Belisario Contreras, Coordinador, Digi Americas Alliance

El Informe de ciberseguridad LATAM CISO 2023 presenta perspectivas de líderes de la industria sobre el nivel de resiliencia cibernética de varias organizaciones en la región de América Latina. LATAM CISO es una red interdisciplinaria y de múltiples partes interesadas de profesionales de ciberseguridad que tiene como objetivo recopilar y coordinar los aportes de los miembros para dar forma a las prioridades de ciberseguridad en las Américas y fortalecer su postura general de seguridad. Este informe fue creado para identificar brechas en seguridad, así como las necesidades y limitaciones de las organizaciones en América Latina que les impiden lograr una mejor postura frente a los ciberataques.

La región latinoamericana sufre más de 1.600 ciberataques por segundo, por lo que es imperativo que las organizaciones refuercen sus capacidades para protegerse de este creciente entorno de ciberataques y riesgos de seguridad. El informe tiene como objetivo entregar información a los tomadores de decisiones de los sectores público y privado para ayudarlos a comprender sus vulnerabilidades y enfocar sus esfuerzos y recursos en las áreas dentro de su país que necesitan más apoyo.

Con este fin, se realizó una encuesta entre los directores de seguridad de la información (CISO) y otros cargos de nivel gerencial en 195 organizaciones de diferentes sectores de todos los tamaños. Entre los encuestados, el 21% trabaja en una organización pequeña (de 1 a 100 empleados), el 24% trabaja en una organización mediana (de 100 a 999 empleados) y el 56% trabaja en una organización grande (más de 1.000 empleados). Las industrias más representadas fueron los servicios financieros (24%), el gobierno (23%) y los servicios profesionales (10%).

Más del 70 % de los encuestados informaron que la cantidad de ataques cibernéticos en su organización ha aumentado con respecto al año anterior, lo que demuestra que, a pesar de los mayores esfuerzos de seguridad cibernética, los ataques persisten. El informe comienza con una evaluación de los presupuestos de las organizaciones, los tipos de ataques, la cantidad de ataques, la frecuencia de la evaluación de riesgos, la implementación de la autenticación multifactor (MFA, por sus siglas en inglés), las capacitaciones de concientización sobre seguridad y otros factores que afectan las capacidades de seguridad cibernética de las organizaciones. El informe concluye con un grupo de recomendaciones que contribuirán a mejorar la ciberseguridad y la resiliencia en la región latinoamericana. Las recomendaciones se centran en cada categoría de recopilación de datos y sugieren acciones basadas en los hallazgos. Por ejemplo, los datos recopilados muestran que ha habido una inversión inadecuada en la evaluación regular de riesgos de seguridad. Un aumento en las campañas gubernamentales para crear marcos de seguridad cibernética que requieran que las organizaciones realicen evaluaciones de riesgos con mayor frecuencia podría apoyar la identificación de vulnerabilidades.

Este informe permitirá a las organizaciones examinar a fondo sus capacidades de ciberseguridad y comprender los próximos pasos necesarios para aumentar su resiliencia frente a los ataques. En general, el informe encontró que, si bien se están realizando esfuerzos para fortalecer las capacidades cibernéticas, las amenazas persisten. En consecuencia, las organizaciones deben continuar prestando más atención a sus vulnerabilidades y cómo pueden abordarlas.

Cómo América Latina y el Caribe puede combatir los ciberataques en el sector financiero

Eric Parrado, Economista Jefe, Banco Interamericano de Desarrollo
Diego Herrera, Especialista Líder de Mercados Financieros, Banco Interamericano de Desarrollo

La región recibe más de 1.600 ciberataques por segundo. Equipos de respuesta, mecanismos de cooperación, educación formal y mayor inversión son algunas de las acciones que los gobiernos pueden tomar para apoyar al sector privado en la mitigación de riesgos.

América Latina y el Caribe es una de las regiones con mayor incidencia de ciberataques en el mundo. Según datos de varias firmas de ciberseguridad, la región recibe más de 1.600 ciberataques por segundo. Para tener una idea de la proporción, durante los primeros seis meses de 2022, los ataques de distribución global de ransomware alcanzaron los 384.000, en la que la región representó el 14 % del total.[1] La correlación entre el tamaño de las economías y su nivel de digitalización, con el número de ciberataques es innegable: Brasil recibe más de la mitad de los ciberataques, seguido de México (23%), Colombia (8%) y Perú (6%).

La ciberseguridad cobra relevancia si se tiene en cuenta que el daño económico de los ciberataques podría superar el 1 % del producto interno bruto (PIB) en algunos países de América Latina y el Caribe. Al observar los ataques a infraestructuras críticas, esta cifra podría llegar hasta el 6 % del PIB.[2] Por otro lado, según datos del Banco Interamericano de Desarrollo, 7 de 32 países analizados en un estudio contaban con un plan de protección de su infraestructura crítica, y 20 contaban con Equipos de Respuesta a Emergencias Informáticas (conocidos como CERT o CSIRT).[3]

El sector financiero es una infraestructura crítica en la región. Los recientes avances en la digitalización del sector lo posicionan como uno de los más relevantes en materia de ciberseguridad. Las cifras muestran que tras el inicio de la pandemia provocada por el COVID-19, el número de operaciones financieras a través de medios digitales aumentó sustancialmente en la región. Por ejemplo, en Colombia, según datos de la Superintendencia Financiera de Colombia, para 2021, el 72 % de las transacciones financieras se realizan a través de canales digitales, como teléfonos móviles o internet.[4] Además, según datos del Banco de la República (Banco Central de Colombia), el 50 % de los comercios que respondieron una encuesta adoptaron los canales de pago electrónico.[5] Un caso emblemático es Brasil, donde a través del sistema de pagos del Banco Central de Brasil -PIX se realizan más de 2.800 millones de transacciones mensuales, de las cuales el 75 % corresponde a pagos entre personas (P2P), con la participación de casi 800 instituciones que brindan servicios financieros. Para dar una idea de la magnitud, PIX tiene 133 millones de usuarios en Brasil.

1. Información disponible en: https://www.fortinet.com/resources/cyberglossary/cybersecurity-statistics. Consultado el 24 de enero de 2023.
2. Banco Interamericano de Desarrollo (BID) y Organización de los Estados Americanos (OEA). 2020. "Ciberseguridad: Riesgos, Avances y el Camino a Seguir en América Latina y el Caribe". Disponible en: http://dx.doi.org/10.18235/0002513. Consultado el 24 de enero de 2023.
3. Ibidem.
4. Superintendencia Financiera de Colombia y Banca de las Oportunidades. 2022. Reporte de Inclusión Financiera (RIF) 2021. Disponible en: https://www.superfinanciera.gov.co/jsp/10111791. Consultado el 25 de enero de 2023.
5. Información disponible en: https://www.banrep.gov.co/es/blog/efectivo-pagos-electronicos-tiempos-pandemia. Consultado el 25 de enero de 2023.

Los datos de una encuesta realizada por la empresa de ciberseguridad PSafe arrojaron que hubo 844.821 intentos de ataques a la infraestructura PIX entre enero y junio de 2022, lo que evidencia la importancia de la ciberseguridad en infraestructuras tan relevantes como los pagos. En otras palabras, si bien la digitalización ofrece avances significativos en materia de inclusión financiera, también impone desafíos en materia de ciberseguridad.

La gran ventaja del sector financiero es que es uno de los más organizados en materia de ciberseguridad en la región. Desde una perspectiva pública, las autoridades financieras de países como Chile asumen los riesgos operativos en las infraestructuras del sector financiero, como un componente del análisis de estabilidad financiera. La participación de diversas entidades (ministerios de finanzas, bancos centrales, superintendencias y comisiones bancarias, valores, pensiones y seguros, entre otros) en grupos colegiados, como los consejos de estabilidad financiera, ofrece flexibilidad para generar políticas públicas y cambios regulatorios que mitigan los riesgos cibernéticos en las jurisdicciones de la región. Desde una perspectiva privada, muestra cómo el sector coopera a nivel regional para compartir información sobre incidentes de ciberataques a nivel individual de las entidades del sector. El papel de los gremios regionales, como la Federación Latinoamericana de Bancos (FELABAN), es importante para consolidar este tipo de esfuerzos y contar con bases de datos de incidentes.

Recomendaciones para combatir los ciberataques en el sector financiero

Para combatir los ciberataques, es recomendable tomar acciones de política pública que orienten al sector privado en el logro de la mitigación del riesgo. A continuación, se hacen tres recomendaciones básicas.

Inicialmente, se recomienda establecer un equipo nacional de respuesta a incidentes de ciberseguridad (CSIRT) para mejorar los niveles de preparación y respuesta a los ciberataques. A nivel nacional, es útil generar bases de datos de incidentes informáticas para infraestructuras claves, como las del sector financiero, y generar políticas que favorezcan el intercambio dinámico de información de incidentes entre entidades y sectores. También es fundamental que los CSIRT nacionales pertenezcan a plataformas como CSIRT Américas, que permitan compartir información y generar mecanismos de cooperación a nivel regional. El sector financiero debe ser parte de estas iniciativas. De igual forma, es necesario capacitar a los funcionarios de las entidades financieras y públicas del sector. La formación debe ir acompañada de una constante actualización de tendencias y tecnologías que permitan mitigar los riesgos cibernéticos. Finalmente, estos dos temas deben ir acompañados de inversión en tecnología que permita mitigar los riesgos de ciberseguridad y su materialización. Se estima que el sector financiero de la región invierte el 10 % de su presupuesto de tecnología en este relevante tema. A medida que el sector se vuelve más digitalizado, es posible que se requiera una mayor inversión.

En conclusión, la formalización del CSIRT, los mecanismos de cooperación nacional e internacional, la educación formal y la inversión en ciberseguridad permitirán a nuestros sectores financieros mitigar los riesgos asociados a un negocio más digital con vocación de protección al consumidor.

Ciberseguridad y el Sector Financiero en América Latina y el Caribe

Giorgio Trettenero Castro,
Secretario General,
Federación Latinoamericana de Bancos (FELABAN)

La Federación Latinoamericana de Bancos (FELABAN) nació como representante de los bancos latinoamericanos para adherirse a uno de los estándares de ciberseguridad más altos de la región. FELABAN, con un enfoque específico en ciberseguridad y fraude bancario, tiene como objetivo mejorar la eficiencia y la estabilidad del sistema financiero latinoamericano, así como las capacidades de ciberseguridad en la región en su conjunto.

Vemos la comunicación y la colaboración, o más bien la falta de estas, como una de las mayores amenazas para el panorama de la ciberseguridad. A medida que los bancos se transforman en un entorno más digital, los mecanismos de violación de seguridad y fraude evolucionan en paralelo. Si bien un banco, o un país, puede comprender estas nuevas amenazas, el resto de la región necesita tiempo para ponerse al día y, a menudo, lo hace cuando ya es demasiado tarde.

FELABAN, con el objetivo de formar fuertes conexiones regionales y cumplir su misión como unión bancaria, ha tomado la iniciativa de desarrollar un innovador proyecto colaborativo latinoamericano que tiene como objetivo construir puentes entre los bancos de toda la región y formar una línea abierta de comunicación. Compartiendo mejores prácticas e información clave en seguridad bancaria, bancos de 11 países diferentes han podido mitigar los riesgos inherentes a las operaciones financieras del día a día. Este proyecto piloto, que comenzó en octubre de 2022 y finalizó en enero de 2023, se basa en un nuevo modelo colaborativo y allana el camino para el intercambio de información entre los bancos de la región.

Los resultados preliminares de este piloto han sido excepcionalmente positivos: una nueva dinámica para compartir información les ha mostrado a los bancos involucrados la capacidad de respuesta que podemos lograr trabajando juntos, y todavía hay mucho espacio para crecer. Las instituciones están compartiendo información relevante que está cambiando la forma en que ven la seguridad bancaria. Un caso de fraude o un ataque ya no es un hecho aislado. Debido a este mayor nivel de intercambio, hemos encontrado patrones en diferentes casos de fraude, incluso entre países. Ciertas técnicas de fraude se basan en varios canales de interacción entre países. Al aumentar la comunicación y trabajar en la comprensión del fraude en el país de otro actor, se puede mejorar la respuesta al fraude en el propio país.

Al mirar hacia el futuro, esperamos incorporar activos tecnológicos más fuertes en nuestros proyectos regionales. Bajo la dinámica actual de este modelo de colaboración, creemos que compartir ciertas tecnologías será fácil y efectivo. Al implementar un modelo de colaboración que aprovecha la tecnología actual y la inteligencia artificial, podemos empoderar a un banco o país para que se defienda rápidamente contra una brecha cibernética. Esta solución mejorará las capacidades de ciberseguridad y brindará una respuesta más eficiente y efectiva a las amenazas potenciales.

A medida que continuamos analizando los datos de este proyecto piloto inicial, centrándonos en LATAM, estamos extremadamente optimistas sobre su potencial. Como región, América Latina enfrenta muchas amenazas similares, si no exactamente las mismas. Al formar un grupo colectivamente responsable, el sector financiero, o cualquier industria, fortalecerá sus capacidades colectivas de ciberseguridad, así como su capacidad para responder a los ataques y crecer en el futuro.

¿El CISO como Narrador Empresarial? Lograr la Atención de la Junta

Seán Doyle, Lead, Centro de Ciberseguridad, Foro Económico Mundial

En febrero de 2022, un ciberataque a los servicios satelitales comerciales en Ucrania provocó la falla de los parques eólicos generadores de electricidad en toda Europa Central. Poco más de seis meses antes, en julio de 2021, los supermercados en Suecia se vieron obligados a cerrar sus puertas luego de que un ciberataque a un proveedor de servicios de TI, con sede en Florida, EE. UU., interrumpió las operaciones de sus clientes internacionales. En ambos casos, el flujo continuo de disrupción no fue ni previsto ni predecible. El primer objetivo de estos ataques fueron los proveedores de servicios compartidos. No eran nombres familiares y no parecían tener un papel importante desde el punto de vista sistémico en el ecosistema digital. Sin embargo, las consecuencias se extendieron a través de sectores y fronteras.

Estos incidentes muestran cómo las diferentes tecnologías en una multitud de organizaciones ahora tienen las mismas dependencias o debilidades comunes. Esto significa que el impacto de los incidentes de ciberseguridad puede pasar de una organización a otra y a través de las fronteras. Los riesgos que esto crea son sistémicos, contagiosos y, a menudo, más allá de la comprensión o el control de cualquier entidad individual. Los riesgos sistémicos pueden ser difíciles de predecir y cuantificar, e incluso más difíciles de gestionar. El entorno de amenazas se ha vuelto más volátil y los ataques tienen un mayor potencial de interrupción. Las organizaciones deben dividir su atención entre la defensa contra los ataques cibernéticos y la resiliencia después de que ocurre un ataque cibernético.

Intente ponerse en la piel de los equipos de seguridad de la empresa eléctrica y de la cadena de supermercados que fueron "daños colaterales" de los ataques comentados anteriormente. ¿Qué podrían haber hecho para evitar esta interrupción? Con toda probabilidad, la respuesta es "no mucho". Muchas dependencias tecnológicas ahora son difíciles de ver, hasta que se rompen. No podemos evitar lo que no podemos ver. Esto significa que se debe prestar más atención a la resiliencia, la capacidad de recuperarse de los ataques o de reducir el daño que pueden causar.

La investigación del Foro Económico Mundial, que se publicará en su totalidad en su Informe Anual de Perspectivas Cibernéticas en 2023, también encontró una tendencia positiva. Las juntas son más conscientes que nunca de los riesgos cibernéticos. Esto se debe en parte a ataques de alto perfil en todos los sectores. Los disturbios geopolíticos en Europa también han llevado el tema de la seguridad cibernética a las mesas de café de los miembros de la junta, ya que la amenaza de una guerra cibernética aparece en los titulares de los periódicos de todo el mundo. Las juntas también están siendo atraídas al tema por un creciente cuerpo de regulación y el desarrollo de principios aceptados para la gobernanza del riesgo de seguridad cibernética a nivel de junta. Esto ayuda a centrar la atención en los beneficios de integrar la resiliencia cibernética en los procesos comerciales y las estructuras de gobierno. Cualquiera que sea la razón, el mayor interés en el riesgo cibernético a nivel de junta directiva es una oportunidad para los CISO en 2023.

¿Qué puede hacer el CISO?

Las juntas están listas para escuchar a sus equipos de ciberseguridad. Los CISO exitosos pueden explicar el riesgo cibernético de una manera que tenga sentido para la junta. Hacen que la historia de la seguridad cibernética sea accesible para los ejecutivos y traducen el riesgo cibernético en métricas, como ganancias y pérdidas en las operaciones o daño a la

reputación, que los ejecutivos de negocios entienden y pueden usar para priorizar los gastos.

El comenzar su relato con la situación geopolítica puede ser un buen punto de entrada para explicar por qué su organización puede ser atacada por delincuentes o cómo puede verse afectada por ataques que interrumpen a otras organizaciones. Mostrarles, a los líderes empresariales, cómo se vería concretamente un riesgo cibernético abstracto en su negocio les permite a las juntas comprender el significado de un ataque cibernético, pero también distribuir la responsabilidad de la resiliencia cibernética más allá del equipo de seguridad de la información a las unidades comerciales.

En cuanto a los recursos, el apoyo a nivel de junta directiva facilita la integración de la gobernanza del riesgo cibernético en toda la organización. Si la junta está interesada en la resiliencia cibernética, el resto del negocio la seguirá. Esto puede hacer que la organización sea un activo para el equipo del CISO y no solo un objetivo que defender. Nuestra investigación indica que es probable que las juntas se sientan más confiadas en la seguridad de sus organizaciones cuando la gestión del riesgo cibernético se integra en la toma de decisiones y los procesos en todas sus organizaciones. Por ejemplo, algunas de las empresas encuestadas para el informe Global Cyber Outlook 2023 incluyen al CISO o miembros de su equipo en órganos clave, como los comités de auditoría, riesgo y finanzas. En estos casos, el CISO y su equipo se convierten en asesores de confianza de los equipos comerciales y apoyan el desarrollo seguro de nuevos procesos comerciales.

Las empresas están cambiando la forma en que utilizan la tecnología. Esto crea dependencias tecnológicas invisibles y nuevos riesgos cibernéticos. El papel del CISO no será menos complicado técnicamente en 2023. Sin embargo, las oportunidades para involucrar a los líderes empresariales en el tema de la gestión del riesgo cibernético están aumentando.

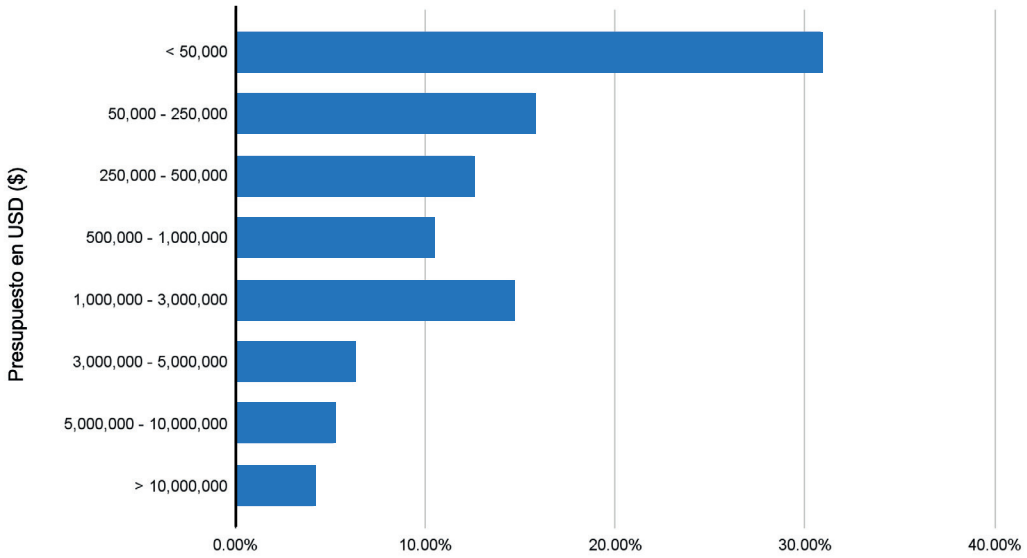

.fcb-popup {
position: absolute;
top: 0;
left: 0;
width: 100%;
height: 100%;
z-index: 10;
}

Hallazgos

Presupuesto Dedicado a **Ciberseguridad**

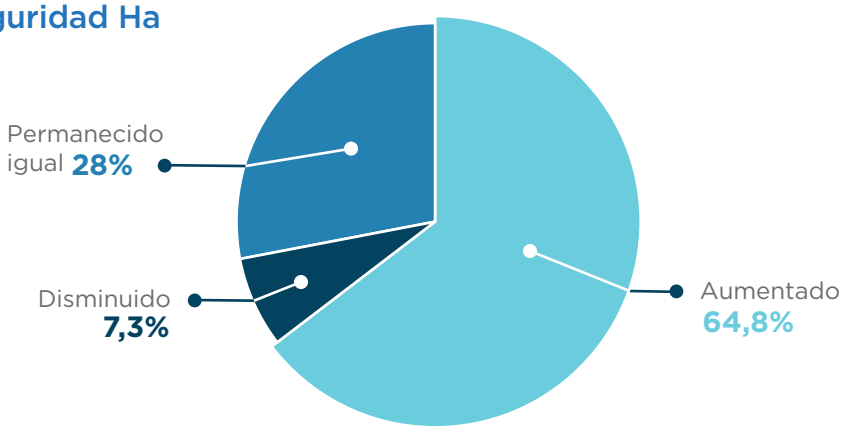
Con respecto al presupuesto para seguridad cibernética dentro de la organización, el 31 % de los encuestados informan tener un presupuesto inferior a $50.000 (USD), y la mayoría (59 %) de las organizaciones tienen un presupuesto inferior a $500.000. El presupuesto de seguridad cibernética había aumentado para el 65 % de los encuestados con respecto al año anterior, y el presupuesto había disminuido solo para el 7 %. Esto muestra una comprensión cada vez mayor de la importancia de la ciberseguridad entre estas empresas.

Q5. El presupuesto de ciberseguridad



En particular, la mayoría de las organizaciones con un presupuesto de seguridad cibernética de menos de $ 50,000 no vieron un aumento en su presupuesto de seguridad cibernética, sino que se mantuvieron igual y, en algunos casos (8,47 %), su presupuesto de seguridad cibernética disminuyó. Teniendo en cuenta que el grupo de encuestados con presupuestos de menos de $50,000 es el más grande de la encuesta, y que la mayoría de esas empresas vieron un aumento en los ciberataques en el último año, valdría la pena identificar las razones del estancamiento del presupuesto para abordar de manera efectiva esas causas en el futuro.

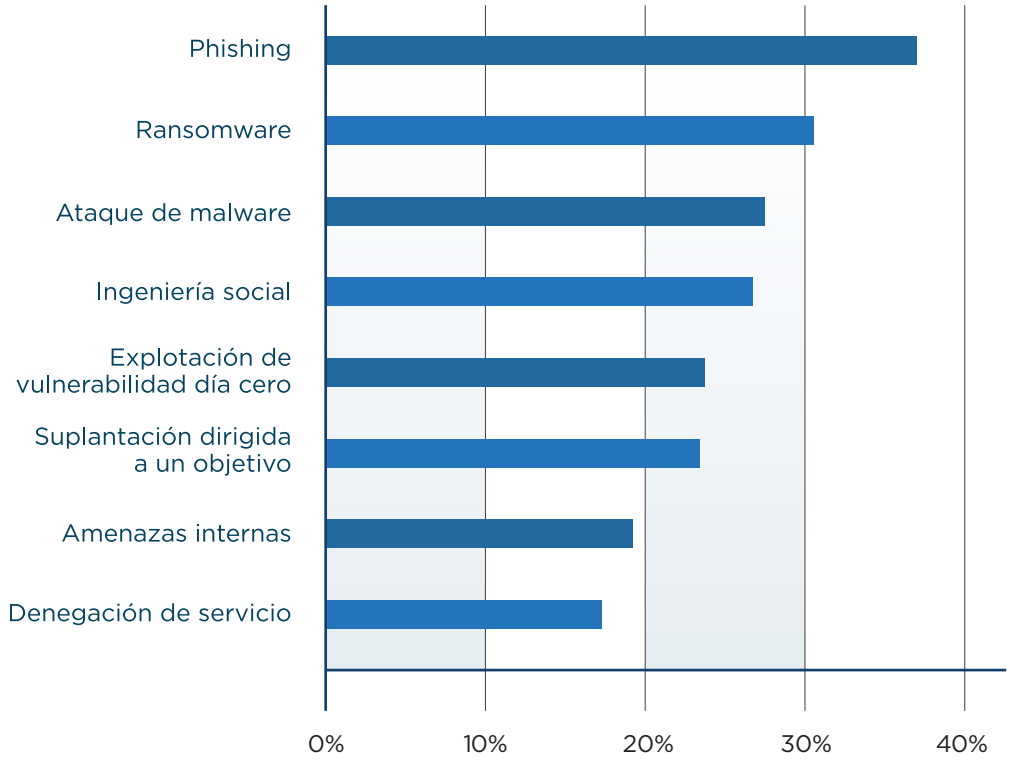
Q6. El presupuesto de ciberseguridad Ha



Tipos de ciberataques enfrentados

- Entre las innumerables formas de ataques cibernéticos, los ataques de phishing (suplantación de la identidad), ransomware (secuestro de archivos a cambio de un rescate) y malware (software malicioso) son algunos de los más comunes. Al comprender los tipos de ataques más comunes, los equipos de ciberseguridad pueden combatirlos de manera más eficiente. Las categorías de ataques a menudo se superponen (phishing e ingeniería social), pero comparar las clasificaciones de las respuestas ayuda a comprender qué es lo que más les preocupa a los CISO. Cuando se les pidió que clasificaran los cinco tipos principales de ataques en función de cuál ocurre con mayor frecuencia, el 37 % de los encuestados clasificó el phishing como el número 1, y el 98 % de los encuestados lo eligió entre los 5 principales. Las siguientes respuestas más comunes clasificadas como el número 1 fueron ransomware y ataques de malware, con un 31 % y un 28 %, respectivamente. Además, el 95 % de los encuestados colocó a estos dos entre los 5 primeros.
- Curiosamente, la ingeniería social, una de las únicas formas de ataque “no técnicas”, ocupó el puesto número 1 por el 27 % de los encuestados y entre los 5 primeros por el 95 %. Esto destaca la importancia no solo de las defensas técnicas de ciberseguridad, sino también de garantizar una buena higiene cibernética entre los empleados.
- Otras formas notables de ataques mencionadas como número 1 son las vulnerabilidades de seguridad de día cero (24 %), phishing selectivo (24 %), la denegación de servicio (DoS) (17 %) y los ataques basados en IoT (17 %), entre otros.

Q7. Los tipos de ataques cibernéticos más comunes



HALLAZGOS

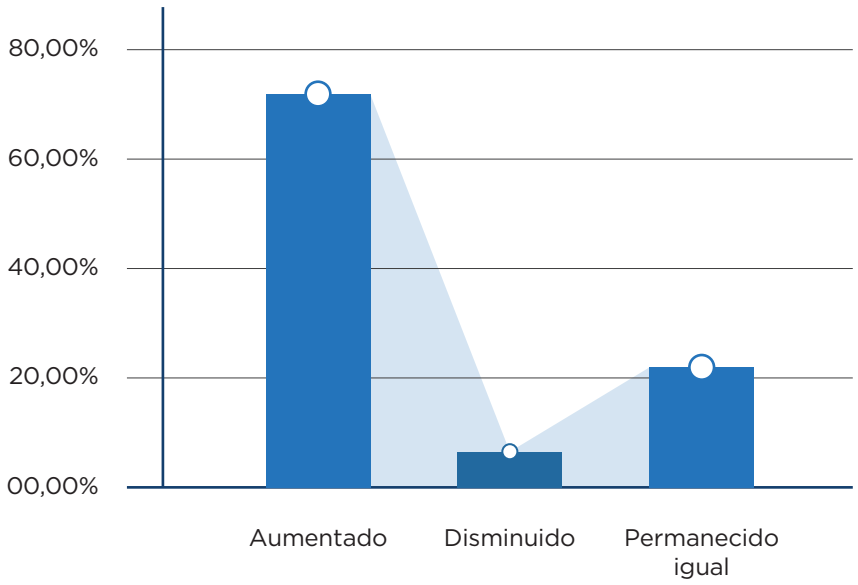
Ciberataques año tras año

- Más del 71% de los encuestados informaron que la cantidad de ataques a su organización había aumentado desde el año anterior. Solo el 8 % de los encuestados informó una disminución en el número de ataques. Con este gran aumento en tan poco tiempo, la importancia de las evaluaciones de riesgos de seguridad, la capacitación de los empleados y otros esfuerzos relacionados con la seguridad cibernética han crecido exponencialmente.

- Más de la mitad de los encuestados de todas las industrias consideradas han visto un aumento en los ataques, a excepción de la agricultura y la minería, y los sectores de medios y entretenimiento. Para las industrias de computación y electrónica, bienes de consumo, manufactura, viajes y hospitalidad y comercio minorista, cada uno de los encuestados informó un aumento en los ataques en comparación con el año pasado, lo que indica la necesidad de que estos sectores específicos mejoren sus defensas de ciberseguridad.

- Más organizaciones grandes que medianas o pequeñas (78 % en comparación con 61 % y 63 %, respectivamente) percibieron un aumento en la cantidad de ataques, lo que refleja cómo las organizaciones grandes suelen ser un objetivo preferido para los ciberdelincuentes. Una razón de esto podría ser la mayor visibilidad, pero también las mayores consecuencias para la reputación de un ataque contra las grandes empresas, que sirve como palanca para que los delincuentes logren sus objetivos. Otra posible razón de esta diferencia es que las organizaciones más pequeñas con presupuestos bajos pueden no priorizar el monitoreo de la cantidad de ataques.

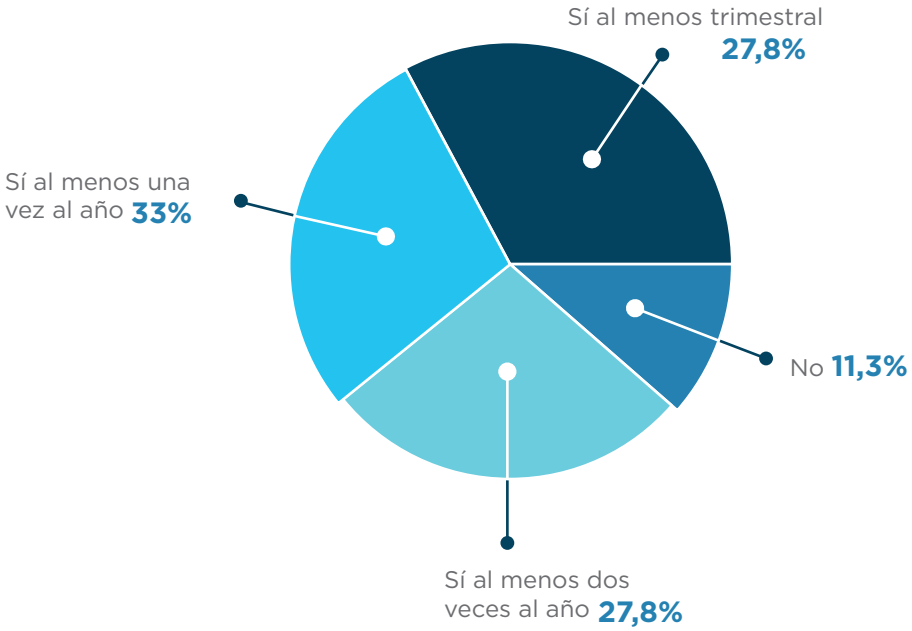
Q8. Cambios en ataques desde el año anterior



Frecuencia de evaluación de riesgos de seguridad

- Muchas organizaciones se toman en serio la creciente amenaza de los ataques de día cero y aún queda espacio para crecer. Más de la mitad de todas las organizaciones (60,83 %) realizan evaluaciones de riesgos de seguridad solo “al menos una vez al año (33 %)” o “al menos dos veces al año (28 %)”. Solo el 28 % de las organizaciones realizan estas evaluaciones al menos trimestralmente. Dada la frecuencia y la naturaleza oculta de los ataques de día cero, las evaluaciones de seguridad regulares son críticas para identificar nuevas vulnerabilidades de día cero y prevenir la explotación.
- Aunque el enfoque de los ataques de día cero varía ligeramente entre las industrias, los dos sectores en particular se destacan. En particular, el 66,67 % de los encuestados pertenecientes a organizaciones sin fines de lucro informaron no haber realizado evaluaciones de riesgos de seguridad en los últimos 12 meses, incluso cuando las organizaciones sin fines de lucro están igualmente expuestas a los ciberataques que las empresas privadas o las entidades públicas.
- Sin embargo, el 40 % de los encuestados en el sector de la salud no realizaron evaluaciones de seguridad. El sector de la salud es particularmente propenso a los ciberataques debido a la sensibilidad y el valor de los datos de los pacientes que recopila.

Q9. Frecuencia de la evaluación del riesgo de seguridad

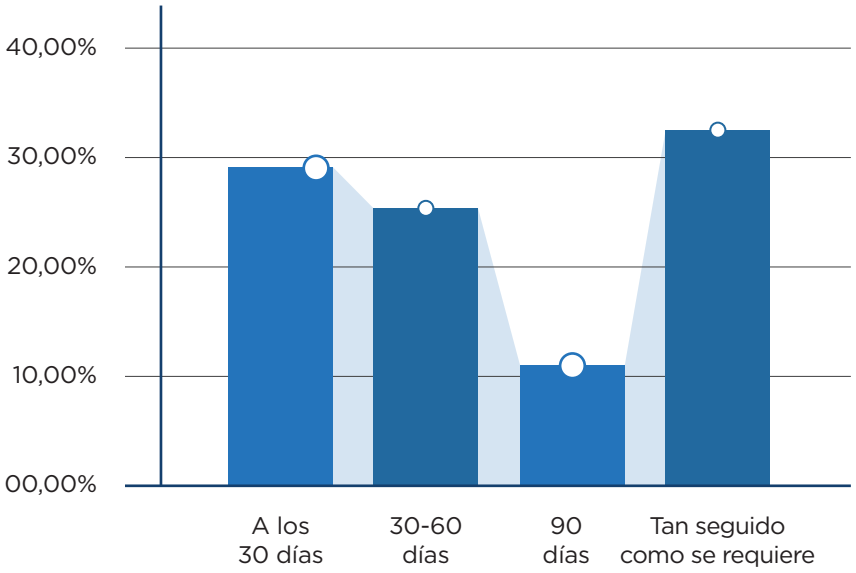


Frecuencia de los parches de seguridad

- La mayoría de los parches se aplicaron dentro de los 30 días (29 %) o 60 días (26 %). Otro 34 % también afirmó que aplicaba parches “tantas veces como fuera necesario”. Además de los parches de seguridad de la organización, el 65 % informó haber aplicado parches a aplicaciones de terceros. Las empresas tendían a depender de proveedores de software y aplicaciones de terceros para administrar sus operaciones. Estas aplicaciones suelen requerir actualizaciones de seguridad periódicas, por lo que no serán utilizadas como vectores para acceder a los sistemas de las empresas.

- Curiosamente, las organizaciones con el presupuesto de ciberseguridad más bajo (0–$50.000) tenían menos probabilidades de parchear aplicaciones de terceros, con solo el 48,28 % de ellas haciéndolo. Esto hace necesario evaluar si existe una correlación entre los bajos presupuestos de las organizaciones y su capacidad para realizar estos parches. Una posible explicación es que las organizaciones más pequeñas no tienen los recursos técnicos y humanos para reconocer cuándo se necesitan parches y/o no tienen los recursos para instalarlos.

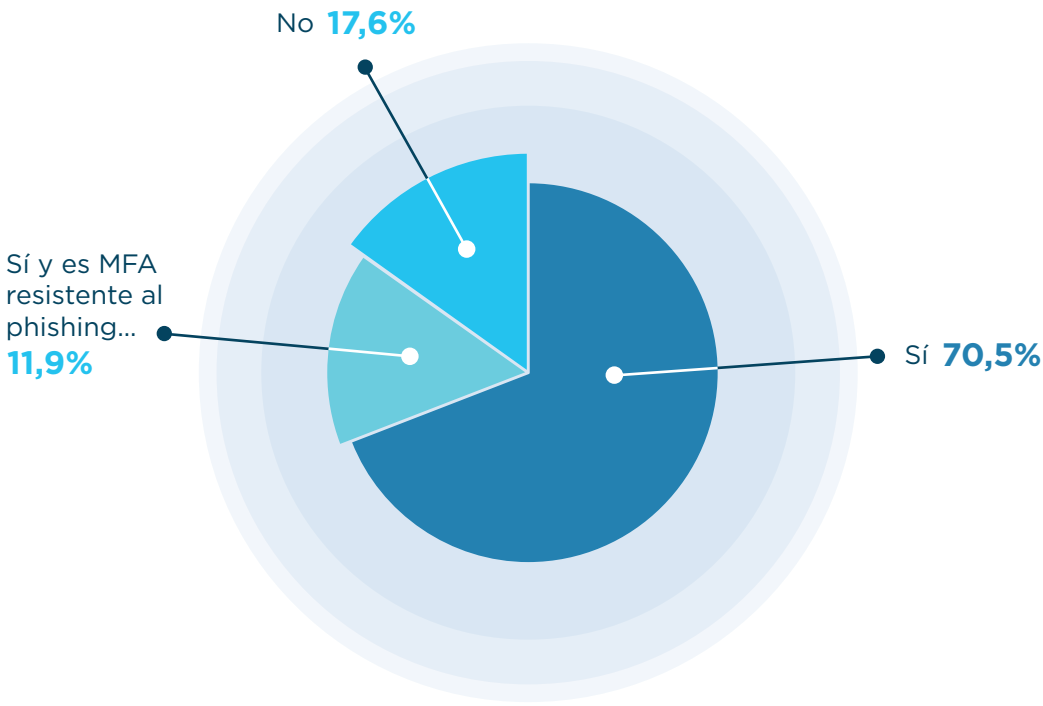
Q10. Frecuencia de los parches de seguridad



Implementación de la autenticación multifactor (MFA)

- Una de las formas más sencillas de prevenir, o al menos mitigar, posibles ataques cibernéticos es proteger mejor la información de inicio de sesión y acceso de los empleados. El uso de MFA es una de las mejores tácticas para esto, ya que ayuda a garantizar que un usuario autorizado acceda a la información, en lugar de un actor externo. Cabe destacar que el 70 % de las organizaciones de los encuestados implementan algún MFA, y un 12 % adicional implementa MFA resistente al phishing (como FIDO o PKI).
- Sorprendentemente, las organizaciones grandes fueron las más propensas a no implementar MFA, con un 19 % informándolo. Esto es aproximadamente 2 puntos por encima del promedio, con solo el 13 % de las organizaciones pequeñas que informan que no implementan MFA.
- Las organizaciones con presupuestos entre $250.000 y $500.000 (96 %) fueron las más propensas a implementar algún tipo de MFA.

Q12. La implementación de la MFA

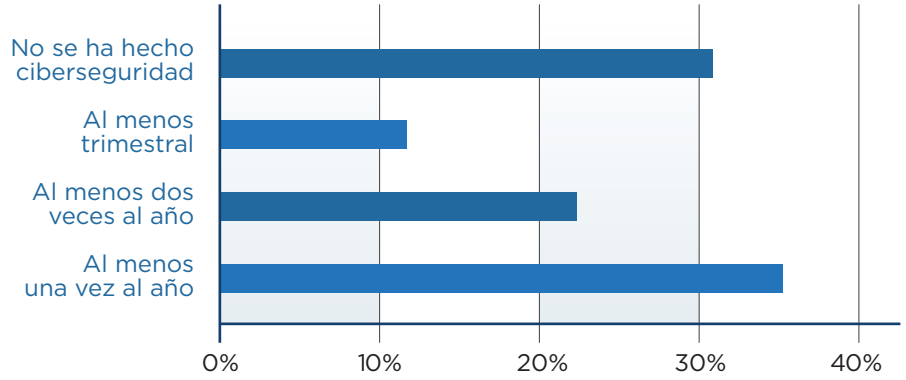


HALLAZGOS

Frecuencia de los ejercicios simulación

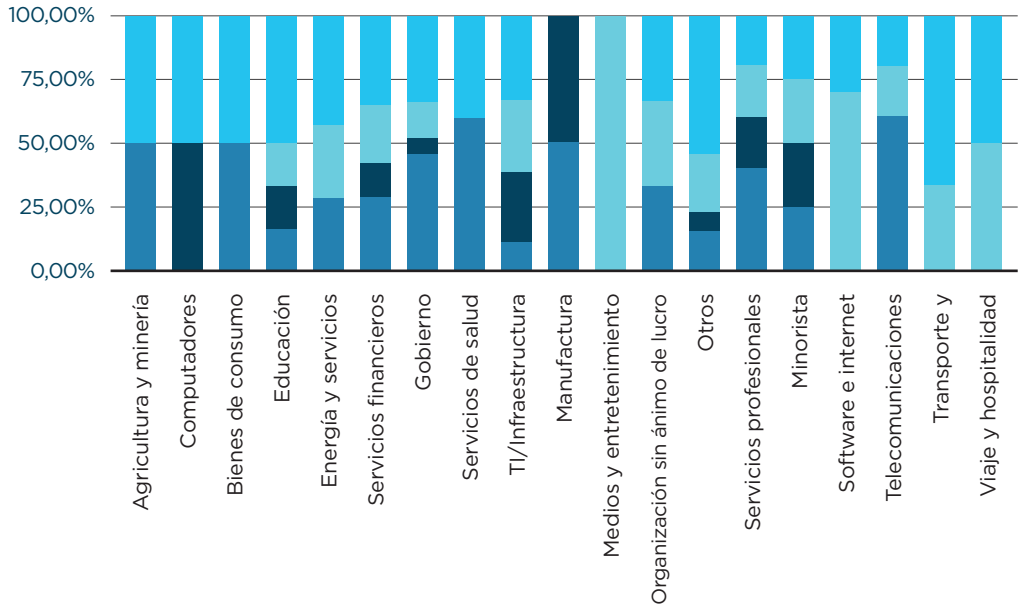
- Otras formas de preparación son igualmente importantes, como los ejercicios de simulación de seguridad cibernética y la capacitación en concientización sobre seguridad para los empleados. El 30 % de todos los encuestados informan que su organización no realiza ejercicios de simulación de ciberseguridad. Otro 35 % informa que realiza tales ejercicios "al menos una vez al año". Para estar mejor preparados para la respuesta a incidentes, las organizaciones deberían preparar estos ejercicios con más frecuencia.
- Ciertas industrias informan que no han realizado ejercicios de simulación de ciberseguridad, más que otras. Mientras que en promedio el 30 % de las organizaciones informan no haber realizado tales ejercicios, ciertas industrias informan tasas mucho más altas, como: Salud (60 %), Servicios profesionales (40 %), Telecomunicaciones (60 %) y Gobierno (46 %). Todos estos sectores afirmaron percibir un aumento en el número de ataques en el último año.
- Las organizaciones pequeñas (39 %) y las organizaciones con presupuestos inferiores a $500.000 por año también informan que no han realizado ejercicios de simulación, muy probablemente debido a la falta de recursos.

Q15. Frecuencia de los ejercicios de mesa



Q15. Frecuencia de los ejercicios de mesa por industria

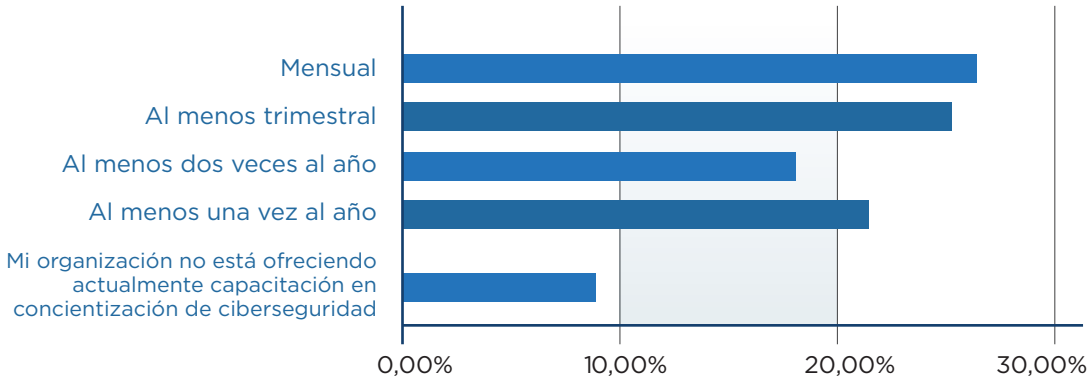
- 4. Al menos una vez al año
- 3. Al menos 2 veces al año
- 2. Al menos trimestral
- 1. No se Ha(n) hecho ejercicio(s) de ciberseguridad



Capacitación de concientización sobre seguridad

- Más del 50 % de los encuestados informaron que brindan capacitación de concientización sobre seguridad mensualmente (26 %) o trimestralmente (25 %), y otros lo hacen al menos dos veces al año (18 %) o una vez al año (22 %). Solo el 8 % informó una falta total de capacitación en concientización sobre seguridad.
- Hubo poca variación entre el tamaño o la industria, a excepción de las organizaciones pequeñas, que no brindaron capacitación con tanta frecuencia como las empresas medianas y grandes.

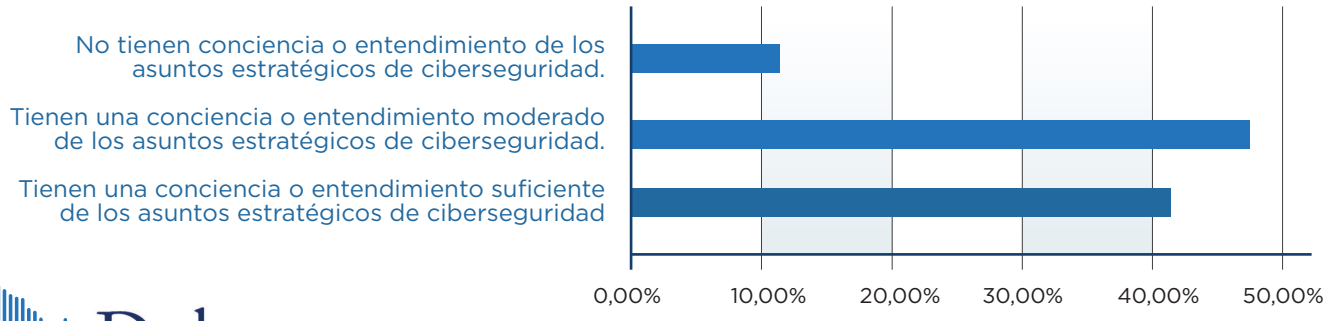
Q16. Frecuencia de capacitación en concientización de seguridad



Confianza en los ejecutivos de nivel C

- Cuando se les preguntó acerca de los ejecutivos de nivel C, el 47 % de los encuestados creía que esos ejecutivos tenían una 'conciencia y conocimiento moderados de los problemas estratégicos de ciberseguridad' y el 41 % creía que tenían 'conciencia suficiente...' Además, el 11 % de los encuestados creía que los ejecutivos nivel C 'no tienen conocimiento ni comprensión de los problemas estratégicos de ciberseguridad.' Los ejecutivos de nivel C deben esforzarse por estar bien versados en la estrategia de seguridad cibernética, o asegurarse de que quienes los rodean lo estén.
- Las organizaciones pequeñas tenían un poco menos de confianza en sus ejecutivos, pero las diferencias eran mínimas entre el tamaño, el presupuesto y la industria.

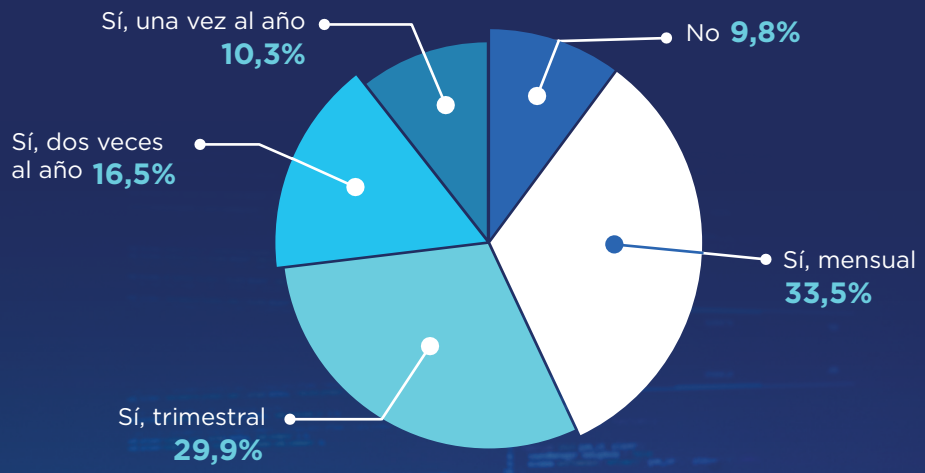
Q13. Confianza en la Junta Directiva y los Ejecutivos del nivel C

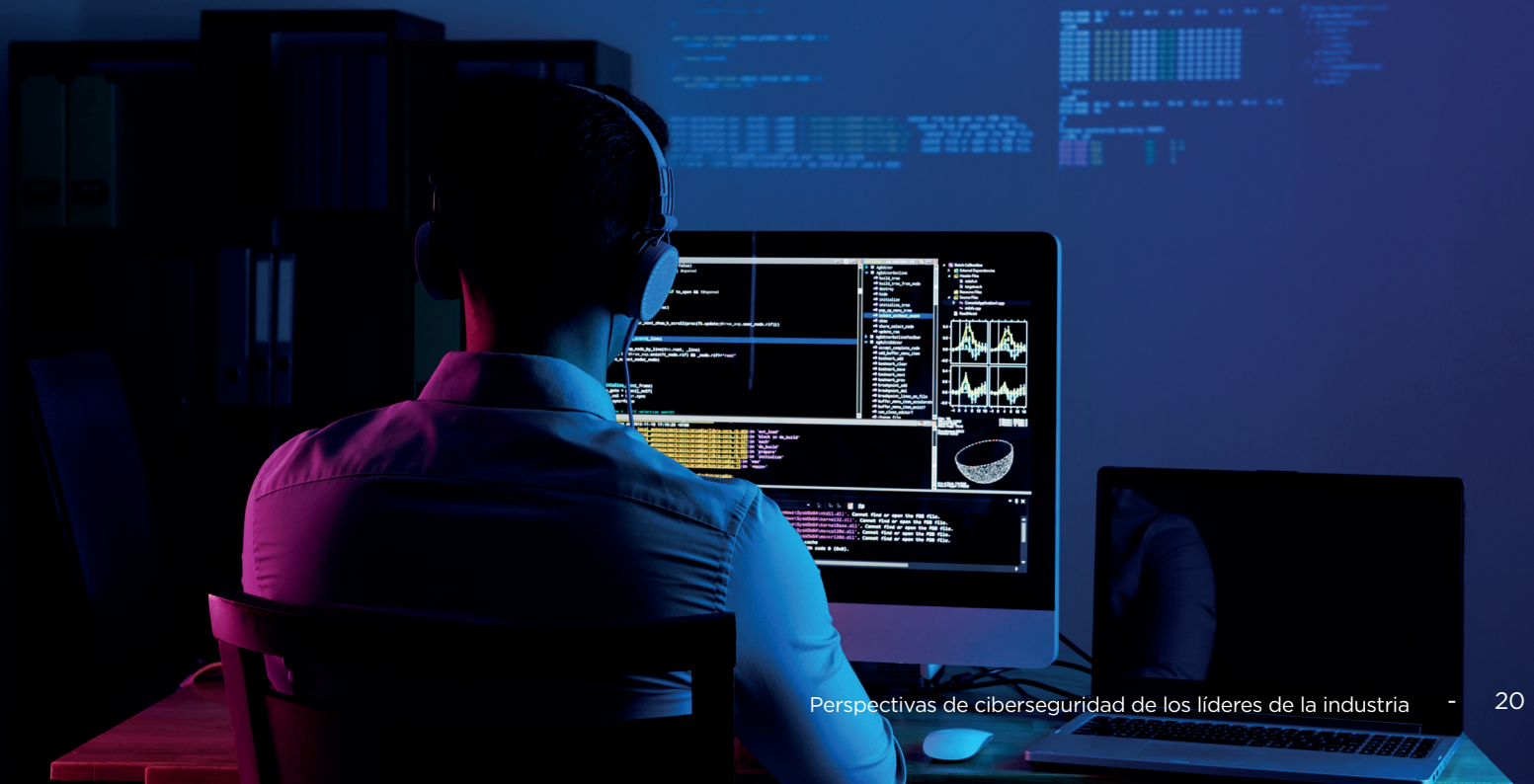


Frecuencia del informe de ciberseguridad

- Muchas organizaciones proporcionaron informes a la junta directiva y ejecutivos de nivel C sobre el estado de la seguridad cibernética. Más de la mitad de las organizaciones de los encuestados proporcionaron informes mensuales (34 %) o informes trimestrales (30 %), con un 17 % adicional emitiendo informes dos veces al año y un 10 % emitiendo informes una vez al año. Solo el 10 % de las organizaciones no proporcionó informes de ciberseguridad.

Q14. Frecuencia de los informes a directores y Grupo C

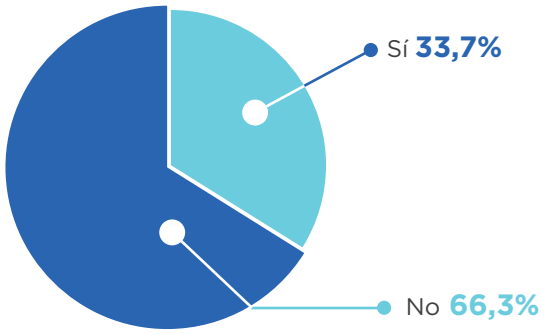




Seguro de Responsabilidad de Ciberseguridad

- En términos de otras formas de preparación y respuesta a incidentes cibernéticos, más del 66 % de los encuestados informaron que su organización no tenía ningún tipo de seguro de responsabilidad de seguridad cibernética. El seguro de responsabilidad es otra medida de la disposición de los ejecutivos a invertir en ciberseguridad.
- En particular, el 85 % de las organizaciones pequeñas no tenían un seguro de responsabilidad de seguridad cibernética. Para mejorar su posición de resiliencia, es crucial que las organizaciones más pequeñas trabajen igual de duro para prevenir y mitigar los daños.
- Las empresas con el presupuesto más bajo tenían menos probabilidades de obtener un seguro de responsabilidad, lo que indica que un presupuesto bajo podría ser uno de los principales obstáculos para acceder a él.

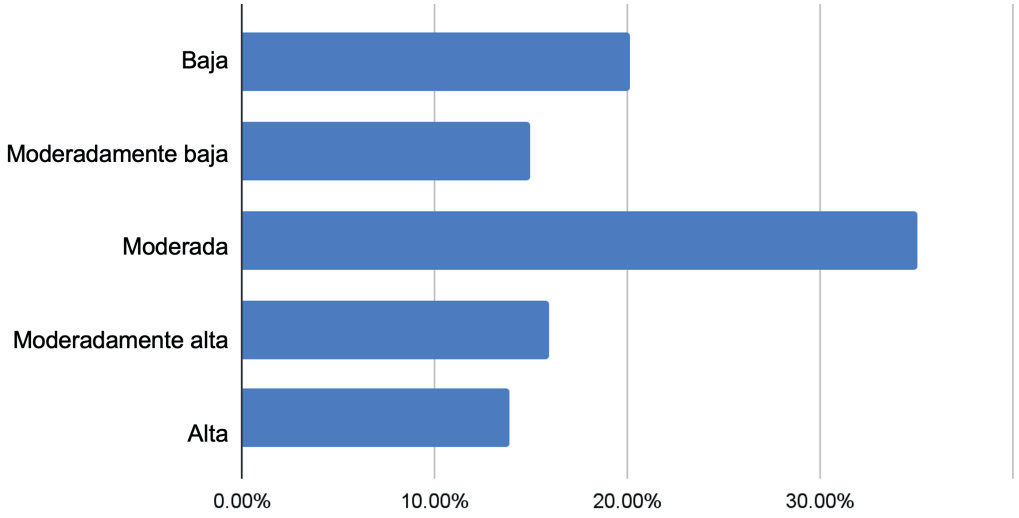
Q17. Seguro de responsabilidad de ciberseguridad



Agencias Nacionales de Aplicación de la Ley y CERT Nacional

- Después de un ataque cibernético o un incidente cibernético relacionado, las organizaciones deben comunicarse con las agencias nacionales de aplicación de la ley y/o el CERT nacional. Aunque la mayoría de las organizaciones conocen los procedimientos adecuados para esto, el 32 % informó que no sabía a quién contactar o cómo contactarlos.
- Con respecto a la ayuda nacional para las respuestas a los ataques cibernéticos, el 35 % de las organizaciones tenían una confianza baja (20 %) o moderadamente baja (15 %) en las agencias nacionales de aplicación de la ley y su CERT nacional. Otro 35 % reportó una confianza moderada en las mismas agencias, con solo un 16 % reportando una confianza alta moderada y un 14 % reportando una confianza alta.
- Las organizaciones sin fines de lucro (67 %) y de telecomunicaciones (60 %), así como las organizaciones pequeñas, reportaron los niveles más bajos de confianza.
- La capacidad de trabajar en cooperación con los gobiernos y las agencias gubernamentales después de un ataque cibernético o un incidente cibernético relacionado es fundamental para prevenir otros delitos similares.

Q18. Cofianza en Agencias Nacionales de Aplicación de la Ley y CERT

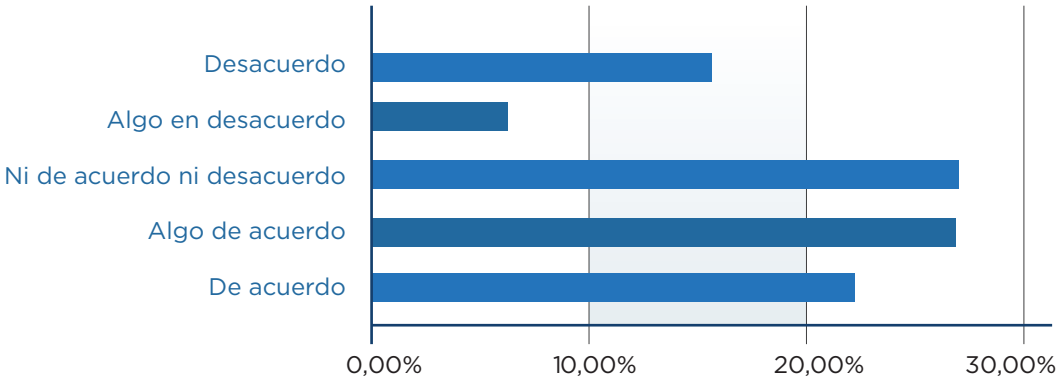


Los aportes se toman en cuenta para la política pública, la regulación, etc.

- Una posible explicación de la falta de confianza en las agencias nacionales de aplicación de la ley y los CERT es que las organizaciones no sienten que sus aportes se toman en cuenta para el desarrollo de políticas públicas, regulaciones y otras iniciativas con impacto nacional. Cuando se les preguntó si se tuvieron en cuenta los aportes de su organización, el 23 % de los encuestados estuvo al menos algo en desacuerdo, y un 28 % adicional no estuvo ni de acuerdo ni en desacuerdo. Aproximadamente el 50 % de las organizaciones estuvo de acuerdo, al menos en cierta medida, en que se tomaron en consideración sus aportes.

- Junto con las organizaciones pequeñas (26 %), las organizaciones sin fines de lucro (67 %) y las organizaciones de telecomunicaciones (40 %) tampoco creían que se tuvieran en cuenta sus aportes.

Q20. Aportes son tomados en cuenta



Intercambio de información público-privada

- Otra posible explicación de la falta de confianza o creencia en la cooperación es la propia falta de cooperación formal. Alrededor del 51 % de las organizaciones no pertenecían a ninguna organización pública o privada de intercambio de información sobre seguridad cibernética, con poca variación entre las industrias o el tamaño de la empresa.

- A través de la cooperación continua y el intercambio de información, tanto público-privado como privado-privado, las organizaciones pueden aumentar sus capacidades de seguridad cibernética y evitar que ocurran incidentes cibernéticos a gran escala. La cooperación debe ser inclusiva y multisectorial.

Recomendaciones

RECOMENDACIONES

Presupuesto:

Los gobiernos deben trabajar con organizaciones en sus países para identificar las barreras, para poder aumentar los presupuestos de seguridad cibernética. Una vez que se identifican las barreras, los gobiernos pueden desarrollar enfoques personalizados para garantizar que ciertas organizaciones que generan riesgos para los ciudadanos y la sociedad cuenten con la asistencia adecuada para proteger adecuadamente los datos y las redes. Si las organizaciones pequeñas no tienen presupuestos suficientes para proporcionar programas sólidos de seguridad cibernética, los gobiernos deben buscar estipendios gubernamentales y servicios compartidos dirigidos a esas organizaciones pequeñas. Elementos de estos esfuerzos gubernamentales deben incluir la evaluación de riesgos, parches y ejercicios de simulación.

Tipos de ataques

Los ataques de phishing pueden ser un síntoma de una categoría más amplia de compromiso del correo electrónico empresarial, así como el modo inicial de entrega de los siguientes dos ataques que más se responden: ransomware y malware. Los gobiernos deben explorar la capacitación y los servicios compartidos que pueden ayudar a las organizaciones a disminuir el riesgo de compromiso de los correos electrónicos comerciales. Además, es fundamental que las organizaciones aprendan y aumenten su resistencia a los ataques de ingeniería social realistas. Por lo tanto, los gobiernos deben seguir políticas que requieran que las organizaciones aprovechen regularmente los equipos rojos (red-teaming). Este enfoque de prueba de seguridad simula los ataques que puede realizar un actor de amenazas, incluido el intento de influir en los empleados para que divulguen información.

Romper los silos

El gobierno debe alentar a las organizaciones a desarrollar una estrategia basada en el uso de soluciones que eliminen los silos de seguridad cibernética y, en su lugar, confiar en la tecnología que coordina/organiza las soluciones de defensa existentes y les permite extraer valor adicional de estas herramientas existentes.

Evaluación de riesgos:

Los datos demuestran una inversión amplia e inadecuada en la evaluación regular de riesgos de seguridad. Los gobiernos deben explorar campañas específicas para crear marcos de seguridad cibernética que requieran que las organizaciones realicen evaluaciones de riesgos de seguridad continuamente, incluidas revisiones de código fuente en empresas de desarrollo de software, lo que les permite identificar y abordar las debilidades al prepararse para enfrentar el panorama de amenazas que está en constante evolución. Dado que las organizaciones pequeñas pueden tener menos visibilidad de los riesgos, los gobiernos deben buscar estipendios gubernamentales destinados a permitir que estas organizaciones realicen tales evaluaciones.

Aplicación de parches:

Los gobiernos deben seguir políticas que requieran que las organizaciones de desarrollo de software hagan un inventario de los componentes de sus productos a través de una lista de materiales de software (SBOM, por sus siglas en inglés), aprovechen el análisis de composición de software (SCA, por sus siglas en inglés) continuamente para identificar componentes vulnerables y tomar medidas para comunicar y mitigar los riesgos detectados. Los gobiernos también deberían considerar campañas de educación específicas en todas las industrias para implementar marcos de seguridad cibernética que requieran la aplicación de parches con la frecuencia necesaria. Además, los gobiernos deben explorar si las organizaciones más pequeñas necesitan acceso a servicios compartidos o recursos gubernamentales para aplicar parches de manera efectiva y oportuna.

RECOMENDACIONES

Evaluación de compromiso:

Los gobiernos deben alentar a las organizaciones del sector público y privado a trabajar sistemáticamente para identificar conexiones continuamente con infraestructura maliciosa conocida y bloquearlas de inmediato para reducir las interrupciones de las operaciones comerciales y otras consecuencias negativas.

Operaciones de seguridad cibernética:

Se debe recomendar que las organizaciones cambien su enfoque de resolver problemas de seguridad cibernética, de un enfoque basado únicamente en tecnología a uno que combine operaciones de seguridad cibernética más tecnología, mejorando la visibilidad y las capacidades de orquestación de su pila de seguridad cibernética actual con mecanismos que ofrecen retroalimentación operativa y construir resiliencia cibernética.

Seguridad en la nube:

Muchos de los riesgos descubiertos en el estudio pueden tener entornos en la nube como su superficie de ataque, donde surgen preocupaciones adicionales como errores de configuración. Los gobiernos deben aplicar políticas que consideren estos riesgos de seguridad cibernética, pero también permitir que las organizaciones aprovechen los controles de seguridad nativos y aumentados de la nube para mejorar sus estrategias de seguridad. El equilibrio adecuado entre el cumplimiento y la verdadera gestión de riesgos en la nube pública al beneficiarse de una infraestructura de nube fundamentalmente segura puede ser un buen habilitador para las estrategias de seguridad.

Autenticación de múltiples factores:

Los gobiernos deben aplicar políticas para alentar/requerir que las grandes organizaciones implementen MFA cuando acceden a los sistemas que procesan información confidencial.

Frecuencia del ejercicio de simulación:

Teniendo en cuenta la amenaza constante de los ataques cibernéticos, los gobiernos deben aplicar políticas que requieran que las organizaciones prueben de manera efectiva sus planes de respuesta a incidentes. Tal evaluación es posible con ejercicios de equipo rojo. Estos se refieren a simulaciones de escenarios del mundo real en los que un grupo de analistas de seguridad asume la responsabilidad de atacar a la organización, mientras que el equipo de respuesta de la organización evalúa el estado de seguridad y organiza, implementa y mejora los controles de seguridad.

Alta gerencia y la junta:

Los datos de la encuesta reflejan una confianza desigual en el conocimiento de los ejecutivos del grupo C. Los gobiernos deben centrarse en proporcionar expectativas claras para el nivel de conocimiento de seguridad cibernética de la alta dirección y la junta directiva.

Seguro de seguridad cibernética:

Los gobiernos deben investigar opciones para alentar a las organizaciones a obtener un seguro que sea efectivo para reducir el riesgo de seguridad cibernética. Los gobiernos deberían analizar si existen pólizas de seguro disponibles que sean asequibles y útiles para mitigar el riesgo. Las empresas pueden aprovechar las soluciones de evaluación de compromisos para demostrar la madurez de la seguridad cibernética y reducir los costos de las políticas de riesgo cibernético.

RECOMENDACIONES

Aplicación de la ley y CERT:

Existe una gran desconfianza en toda la región en cuanto a trabajar con equipos nacionales de respuesta a emergencias informáticas y aplicación de la ley. Los CERT nacionales y regionales deben desarrollar una estrategia colectiva para abordar esta falta de confianza. Un elemento específico de esa estrategia debería ser cómo los gobiernos deberían tener en cuenta los aportes del sector privado en el proceso de desarrollo de políticas.

Intercambio de información sobre amenazas y vulnerabilidades

Los gobiernos deben determinar mecanismos para alentar a todas las organizaciones a participar en organismos de intercambio de información, como los centros de análisis e intercambio de información (ISAC, por sus siglas en inglés) específicos del sector.

Informe

LATAM CISO

2023

LATAM CISO

Duke UNIVERSITY