INFORME

Informe sobre el estado de la tecnología operativa y la ciberseguridad en 2022

CONTENIDO

Infografía: Hallazgos clave

Personas

33 % de las organizaciones confían la seguridad de TO al vicepresidente/ director de ingeniería/ operaciones de redes

67 % de los líderes de seguridad de TO tienen experiencia en ingeniería de TO

43 % de los encuestados considera que el tiempo de respuesta a incidentes de seguridad es una de las tres principales medidas de éxito

Postura de seguridad

56 % de las organizaciones reportan que se encuentran en el nivel 3 o 4 de madurez de seguridad de TO

50 % dice que la postura de seguridad de TO es un factor significativo en la puntuación de riesgo general

13 % de las organizaciones tiene visibilidad centralizada de todas las actividades de TO

Prácticas de seguridad

48 % informa a la dirección ejecutiva de las vulneraciones de seguridad

32 % implementó un control de acceso a la red basado en funciones

52 % afirma que el SOC monitorea y les da seguimiento a las actividades de TO

Resultados de seguridad

93 % de las organizaciones tuvo más de 1 intrusión el año pasado;
78 % tuvo más de 3

61 % de las intrusiones afectaron a los sistemas de TO

90 % de las intrusiones tardaron horas o más para restablecer el servicio

Mejores prácticas

Es más factible que las organizaciones top-tier:

- Tengan una visibilidad centralizada
- Se midan por el tiempo de respuesta a la vulnerabilidad
- Implementen NAC basado en funciones
- Reporten compromisos a la seguridad
- Tengan un único proveedor de dispositivos TO

Resumen ejecutivo

El Informe sobre el estado de la tecnología operativa y la ciberseguridad en 2022, en su cuarta edición anual, revela que las organizaciones siguen avanzando con demasiada lentitud hacia la plena protección de sus activos de tecnología operativa (TO). Esto llega en un momento en el que los sistemas de TO son cada vez más importantes para el bienestar de muchas organizaciones, los acontecimientos geopolíticos hacen que los ataques sean más probables, se conectan más sistemas de TO a Internet y las amenazas basadas en IP son cada vez más avanzadas y causan más daño. Esta combinación de factores hace que la seguridad de TO aumente en la cartera de riesgos de muchas organizaciones.

Basado en una encuesta mundial realizada a más de 500 profesionales de seguridad de TO, el informe de este año concluye que, aunque la seguridad TO cuenta con la atención de los líderes de las organizaciones, sigue siendo propiedad de profesionales de rango relativamente bajo. Durante años se especuló con la posibilidad de que la seguridad de TO pasara a depender del director de Seguridad Informática, pero no hay indicios de que las cosas estén avanzando en esa dirección. Y aunque la seguridad forma parte de las mediciones de rendimiento, para la mayoría de los encuestados, muchos se miden más en función de factores de eficiencia que podrían provocar la tentación de recortar gastos en seguridad.

Basado en una encuesta mundial realizada a más de 500 profesionales de seguridad de TO, el informe de este año concluye que, aunque la seguridad de TO cuenta con la atención de los líderes de las organizaciones, sigue siendo propiedad de profesionales de rango relativamente bajo.

Las organizaciones vuelven a registrar modestos avances en la madurez general de su postura de seguridad de TO, con un número ligeramente mayor que avanzó hasta el nivel 3. Sin embargo, el examen de las mejores prácticas específicas aporta matices al asunto. Solo el 13 % de los encuestados logró una visibilidad centralizada de todas las actividades de TO y solo el 52 % puede darle seguimiento a todas las actividades de TO desde el Centro de operaciones de seguridad (SOC). Solo alrededor de la mitad de los encuestados afirma hacer un seguimiento e informar varias métricas de seguridad básicas, y menos de la mitad de los encuestados utiliza alguna de una docena de tecnologías y prácticas de seguridad específicas. Esto último indica una diversidad en la forma en que las organizaciones abordan la seguridad de TO y refleja un mercado que todavía está evolucionando.

Algo que mejoró muy poco en el último año son los resultados de seguridad de las organizaciones. Un asombroso 93 % de las organizaciones experimentó una intrusión en los últimos 12 meses y el 78 % experimentó más de tres. Los impactos incluyeron el tiempo de inactividad, la pérdida financiera o de datos, la degradación de la marca e incluso la reducción de la seguridad física. Está claro que la mayoría de las organizaciones tiene trabajo que hacer. Afortunadamente, un pequeño porcentaje de los encuestados consiguió evitar las intrusiones durante el año pasado y este informe identifica varias de las mejores prácticas que es más probable que utilicen.

Introducción

Aunque la TO es menos visible que la TI en la mayoría de las organizaciones y ciertamente en la conciencia pública, no es menos importante para la economía y la vida cotidiana de las personas. Al fin y al cabo, los sistemas de TO controlan las infraestructuras críticas de las que todo el mundo depende: la red eléctrica, los sistemas de agua y alcantarillado, las tuberías de combustible, las plantas de energía y las redes de transporte. Y es esencial para la fabricación de todo tipo de bienes.

La TO es un componente importante de la transformación digital en las organizaciones industriales. La rápida evolución de las condiciones del mercado hizo que la adopción de metodologías y tecnologías de la "Industria 4.0" fuera prácticamente esencial incluso antes del COVID-19. La pandemia no hizo más que acelerar estas tendencias, dejando a aquellos "sin recursos" tecnológicos luchando por actualizar y agilizar sus operaciones.[1]

Las crecientes amenazas a la seguridad

Esta tendencia no pasó desapercibida para los actores de las amenazas. El año pasado, el Informe global del panorama de amenazas de FortiGuard Labs observó un aumento significativo de las detecciones de sistemas de prevención de intrusiones (IPS) en los sistemas de TO.[2] Esta observación coincidió con varios eventos de seguridad de alto perfil que afectaron a los sistemas de TO, incluidos los ataques de ransomware a Colonial Pipeline y JBS que interrumpieron el suministro de gasolina y carne en Norteamérica en mayo y junio pasados.[3]

Una de las razones por la que los ciberataques aumentaron con los sistemas de TO en la última década es que se volvieron más vulnerables a los ataques desde fuera del sitio. Aunque los sistemas de TO estaban tradicionalmente separados de los sistemas de TI, estas dos infraestructuras están hoy casi universalmente integradas. Esto significa que los sistemas de TO ahora están conectados a Internet y son teóricamente accesibles desde cualquier lugar. Esto en sí mismo representa un aumento significativo de la superficie de ataque para las organizaciones industriales, y la creciente ubicuidad de los dispositivos del Internet de las cosas de la industria (IIoT) amplía aún más esa superficie de ataque. Al mismo tiempo, los sistemas de TO conectados son vulnerables a un panorama de amenazas informáticas cada vez más avanzado.

La invasión rusa a Ucrania y los acontecimientos relacionados han puesto otro foco de atención en la seguridad de TO. En abril de 2022, la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) de EE. UU, junto con sus homólogos de Australia, Canadá, Nueva Zelanda y el Reino Unido, advirtió que los actores rusos patrocinados por el Estado han intensificado sus esfuerzos en respuesta a las perjudiciales sanciones impuestas por Occidente. Las agencias instan a los responsables de las redes de infraestructuras críticas a "prepararse y mitigar las posibles ciberamenazas, incluyendo el malware destructivo, el ransomware, los ataques DDoS y el ciberespionaje, al reforzar sus ciberdefensas y actuando con la debida diligencia en la identificación de indicadores de actividad maliciosa".[4]

De hecho, se materializó un aumento de los ataques atribuidos a Rusia y las organizaciones ucranianas se llevaron la peor parte.[5] Pero las organizaciones del resto del mundo no son inmunes, con siete de cada 10 proveedores de infraestructura nacional crítica (CNI) en el Reino Unido reportando un aumento de ciberataques desde el comienzo de la guerra.[6]

La seguridad de TO, se vuelve cada vez más el centro de atención

El resultado es que las empresas de muchos sectores están luchando por proporcionar seguridad a los sistemas de TO cada vez más vulnerables. Un estudio realizado para Fortinet por Westlands Advisory[7] revela que la inversión en tecnologías de seguridad de TI/TO y específicas de TO ascendió a USD 6.9 millones para todo el año 2022. Y estas inversiones están aumentando más rápido que el gasto en ciberseguridad solo de TI, con una tasa de crecimiento anual compuesta (CAGR) proyectada del 21 % para la seguridad de TO y del 16 % para la ciberseguridad de TO/TI de aquí a 2027.

Aunque este aumento de la inversión es una muy buena señal, este informe concluye que, en general, las organizaciones representadas en la encuesta de este año todavía tienen un camino considerable que recorrer para proteger adecuadamente sus sistemas de TO. Sin embargo, un pequeño subgrupo de encuestados pasó los últimos 12 meses sin sufrir una intrusión y este informe intenta destacar algunas de las cosas que esas organizaciones están haciendo bien.

Metodología de este estudio

El Informe sobre el estado de la Tecnología operativa y la ciberseguridad de este año se basa en una encuesta realizada a más de 500 profesionales de TO entre el 14 y el 18 de marzo de 2022. Las preguntas de la encuesta reflejaron en gran medida encuestas similares realizadas en 2019, 2020 y 2021, representadas en versiones anteriores de este informe. Los encuestados respondieron a 40 preguntas sobre el estado de su infraestructura de TO y de seguridad de TO, las mejores prácticas de seguridad y el proceso de selección de proveedores.

Diversas geografías, puestos de trabajo, industrias y dispositivos

Una de las diferencias entre la cohorte de la encuesta de este año y la de años anteriores es que la encuesta es de carácter mundial y no centrada en Norteamérica (Figura 1). En general, los encuestados proceden de un total de 28 países, con 150 encuestados basados en Norteamérica (NA); 70 en Latinoamérica (LATAM); 130 en Europa, Oriente Medio y África (EMEA) y 170 en Asia Pacífico (APAC).

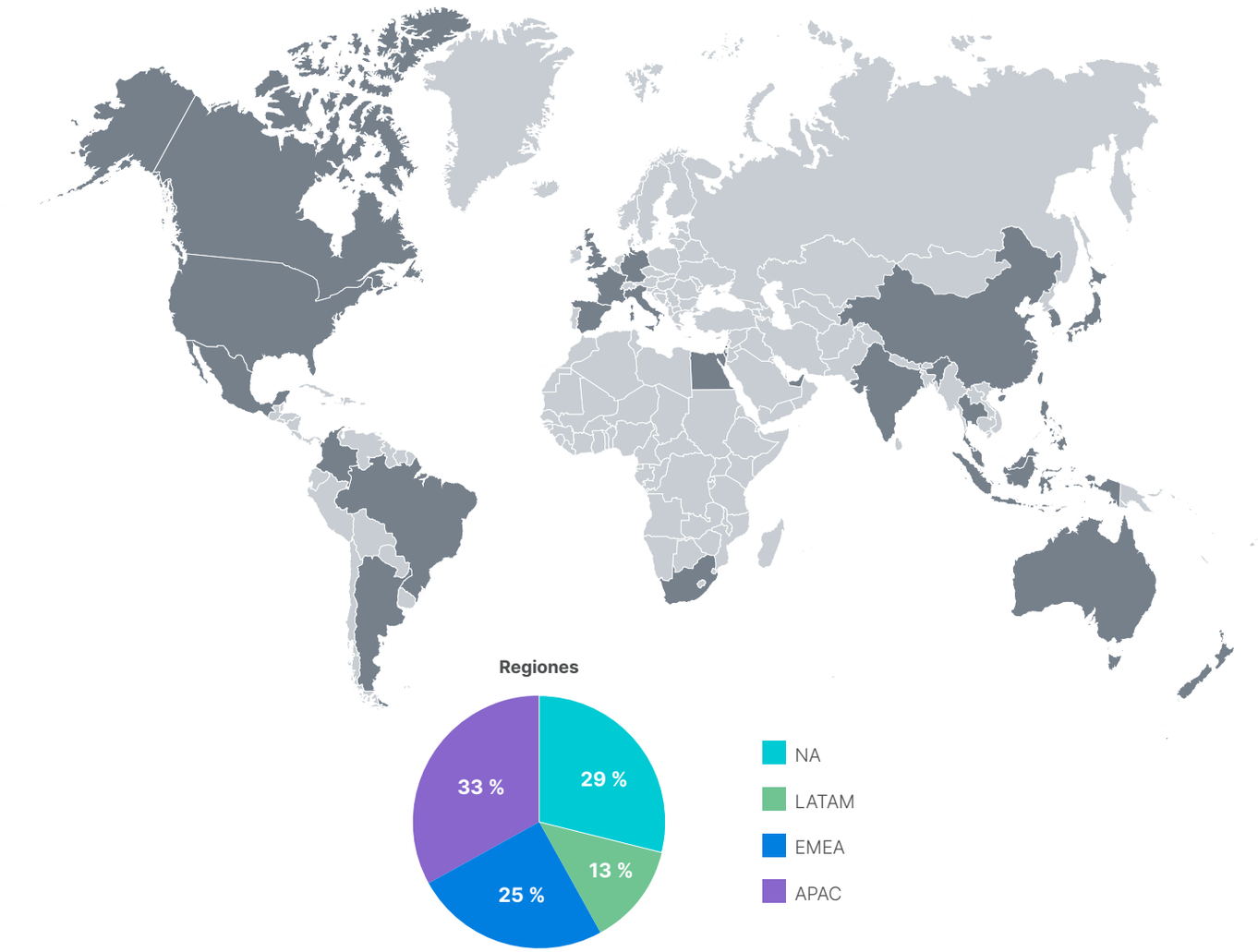


Figura 1: Países y regiones representados en la encuesta.

La encuesta estaba dirigida a personas que ocupan puestos de liderazgo responsables de TO y la seguridad de TO, desde gerentes hasta ejecutivos de nivel C (Figura 2). Representan a una serie de sectores que utilizan mucho la TO, como manufactura, transporte y logística y la atención médica. Seis de cada 10 encuestados son los responsables de la toma de decisiones de compra de TO y el 85 % afirma que se les consulta regularmente sobre las compras de ciberseguridad (Figura 3).

Los encuestados son usuarios de dispositivos de sistemas de control industrial (ICS) y de Supervisory Control and Data Acquisition (SCADA) (control de supervisión y adquisición de datos) fabricados por 15 proveedores diferentes (Figura 4). Como en años anteriores, Honeywell y Siemens siguen siendo las marcas más utilizadas por los encuestados, con más usuarios de Honeywell y Schneider que en años anteriores. El uso de Siemens y Yokogawa disminuyó considerablemente en el mismo periodo. Algunos de estos cambios reflejan la mayor representación geográfica en la encuesta de este año.

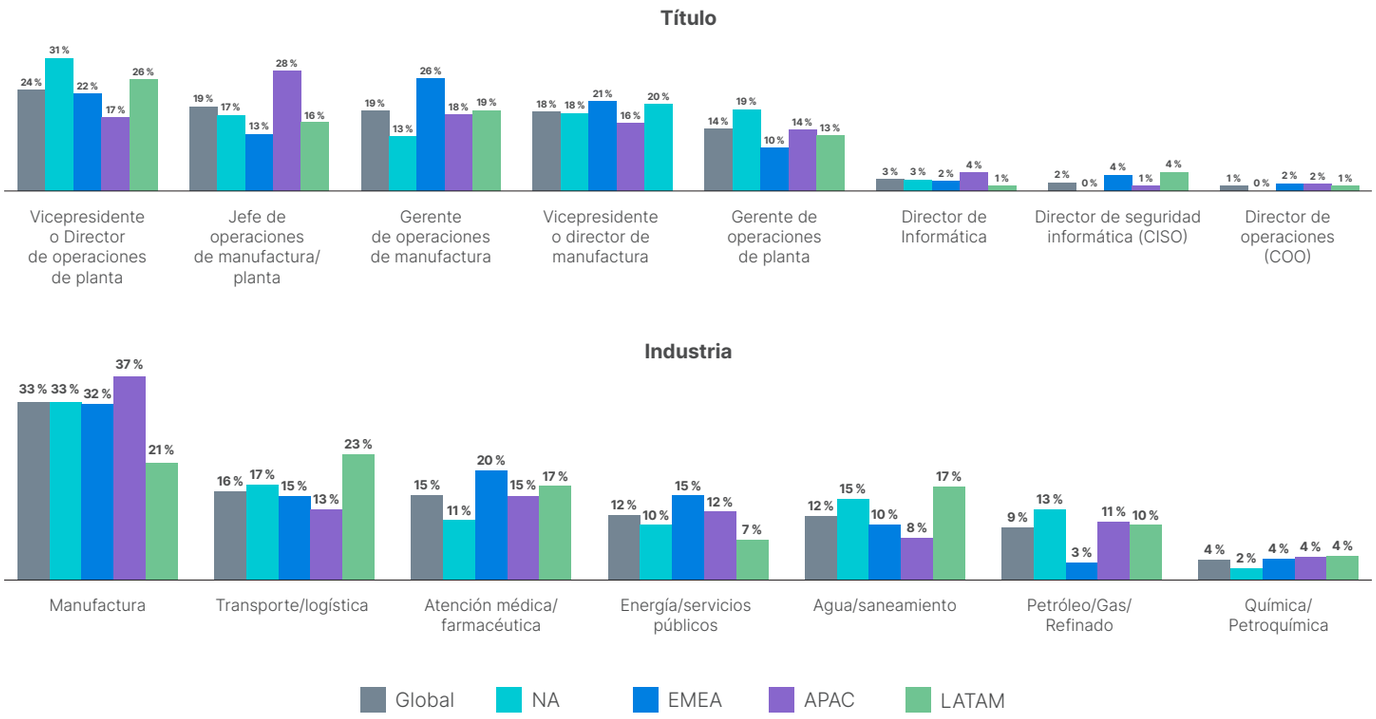


Figura 2: Nombres de puestos de trabajo y sectores por región.

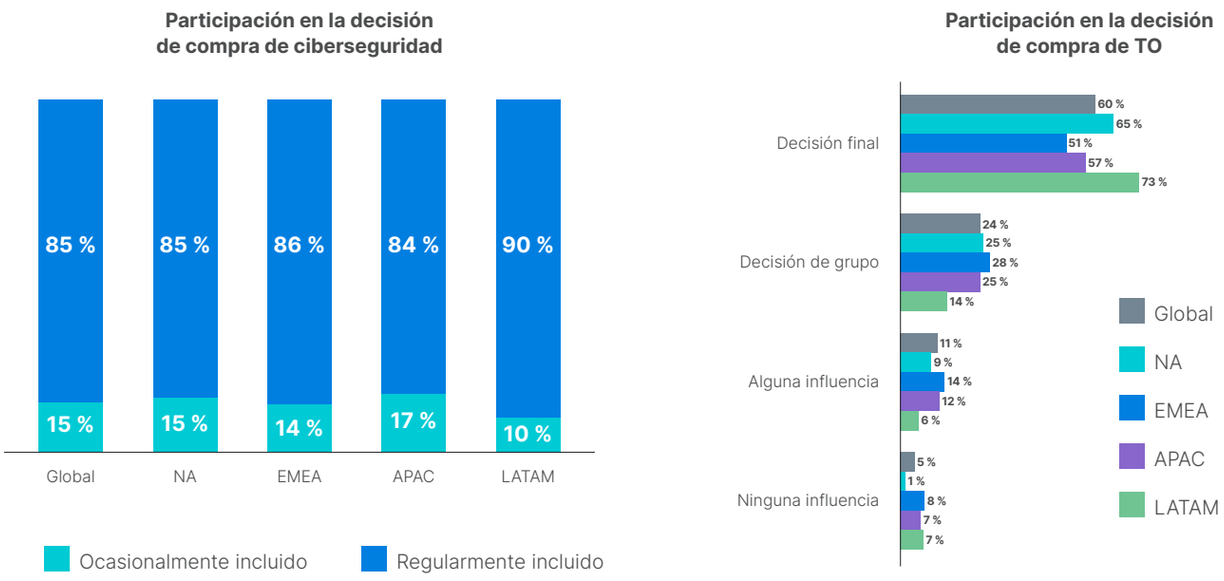


Figura 3: Papel de los encuestados en las compras de ciberseguridad y TO.

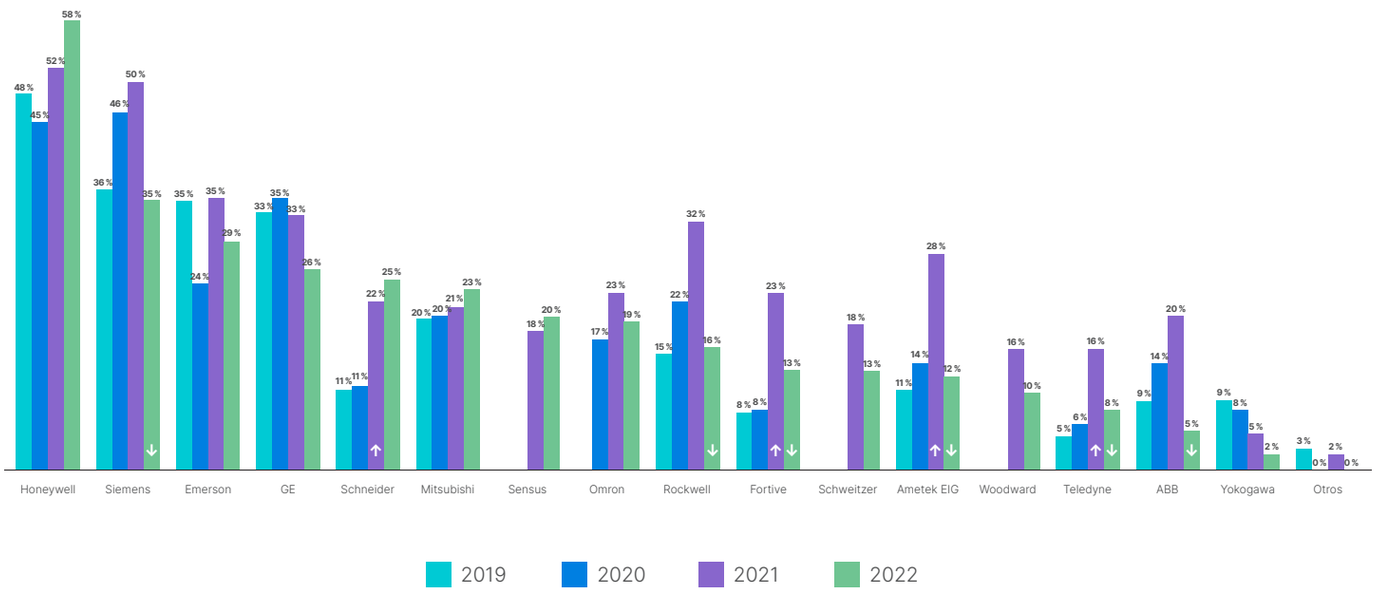


Figura 4: Proveedores de dispositivos de TO en uso.

Identificación de ideas y mejores prácticas

Este informe examina los datos de toda la cohorte y según la región y el sector. También comparamos los resultados norteamericanos de la encuesta de este año con encuestas similares realizadas dentro de Norteamérica en 2019, 2020 y 2021. A partir de este análisis, identificamos cinco perspectivas clave sobre el estado de la ciberseguridad de TO en la actualidad.

En la última sección del informe, analizamos las respuestas de la encuesta según los resultados reales de seguridad de los encuestados y comparamos las organizaciones que no sufrieron ninguna intrusión en el último año con las que sufrieron más de 10 intrusiones. Esta comparación da como resultado varias mejores prácticas a las que las organizaciones "top-tier" tienen más probabilidades de adherirse.

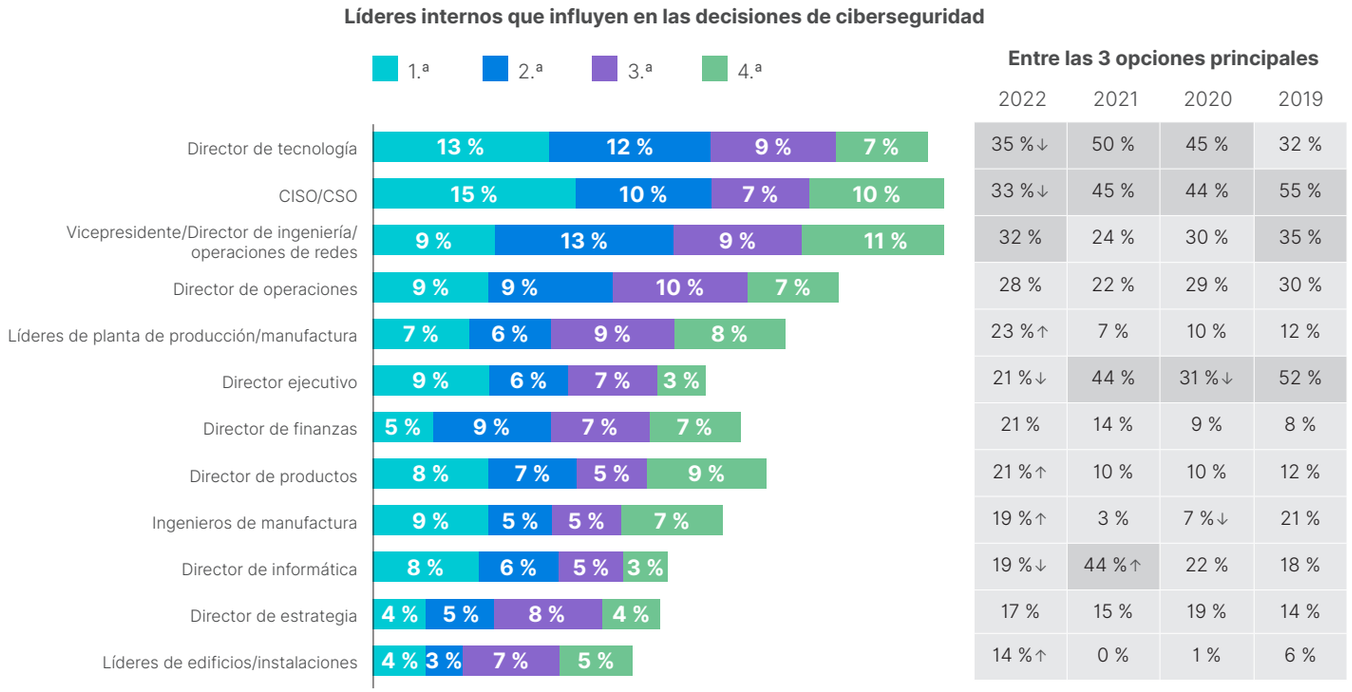
"Las recientes operaciones cibernéticas patrocinadas por el Estado ruso incluyeron ataques de denegación de servicio distribuido (DDoS) y las operaciones más antiguas incluyen el despliegue de malware destructivo contra el gobierno ucraniano y organizaciones de infraestructura crítica".[8]

Conclusiones sobre la seguridad de TO

Los resultados de la encuesta revelan que las organizaciones están cada vez más preocupadas por la seguridad de su infraestructura de TO, pero que su preparación para estas amenazas sigue siendo poco sistemática e incompleta. Identificamos cinco perspectivas clave de la investigación de este año:

Perspectiva 1: La seguridad de TO es una preocupación a nivel corporativo y diferentes grupos asumen la responsabilidad

No es de extrañarse que la seguridad de los sistemas de TO sea objeto de atención de los ejecutivos de muchas organizaciones, y que el Director de tecnología (CTO) y el Director de seguridad/seguridad informática (CISO/CSO) sean los más citados entre los tres principales líderes que influyen en las decisiones de ciberseguridad. Sin embargo, las respuestas a la encuesta indican que estos líderes perdieron una influencia significativa en el último año (Figura 5). El año pasado, el 50 % de las organizaciones situaban al CTO entre los tres principales responsables de la seguridad y el 45 % lo hacían con el CISO/CSO. Estas cifras se redujeron al 35 % y al 33 %, respectivamente, en 2022. La naturaleza global de la encuesta no fue un factor de cambio, ya que las cifras fueron idénticas para los encuestados norteamericanos que para la cohorte general.



Entre las 3 opciones principales			
2022	2021	2020	2019
35 %↓	50 %	45 %	32 %
33 %↓	45 %	44 %	55 %
32 %	24 %	30 %	35 %
28 %	22 %	29 %	30 %
23 %↑	7 %	10 %	12 %
21 %↓	44 %	31 %↓	52 %
21 %	14 %	9 %	8 %
21 %↑	10 %	10 %	12 %
19 %↑	3 %	7 %↓	21 %
19 %↓	44 %↑	22 %	18 %
17 %	15 %	19 %	14 %
14 %↑	0 %	1 %	6 %

Figura 5: Líderes internos que influyen en las decisiones de seguridad.

¿Quién lidera y liderará la seguridad de TO?

Sin embargo, cuando se les preguntó quién era el responsable final de la seguridad de TO en sus organizaciones, una tercera parte de los encuestados mencionó al vicepresidente o al director de ingeniería u operaciones de red (Figura 6). Se trata de un gran aumento con respecto al porcentaje del año pasado y el más alto en los cuatro años en que se realizó la encuesta. Refleja que la responsabilidad de la seguridad de TO puede haber ascendido un poco en el organigrama en comparación con años anteriores, en los que una persona con nivel de director o gerente era responsable de la seguridad de TO en la mayoría de las organizaciones.

Los encuestados especulan que este movimiento ascendente en el organigrama continuará. Solo el 15 % de los encuestados afirma que el CISO es el responsable de la seguridad de TO en la actualidad, pero el 79 % dice que espera que la función pase a depender del CISO en los próximos 12 meses (Figura 7). Sin embargo, somos escépticos con respecto a esta afirmación, ya que una gran mayoría de los encuestados hizo esta predicción todos los años en los que se realizó la encuesta y el porcentaje de organizaciones en las que el CISO está actualmente a cargo de la seguridad de TO en realidad disminuyó ligeramente en 2022 en comparación con 2021. La disminución de la influencia del CISO en las decisiones de seguridad, mencionada anteriormente, refuerza este escepticismo.

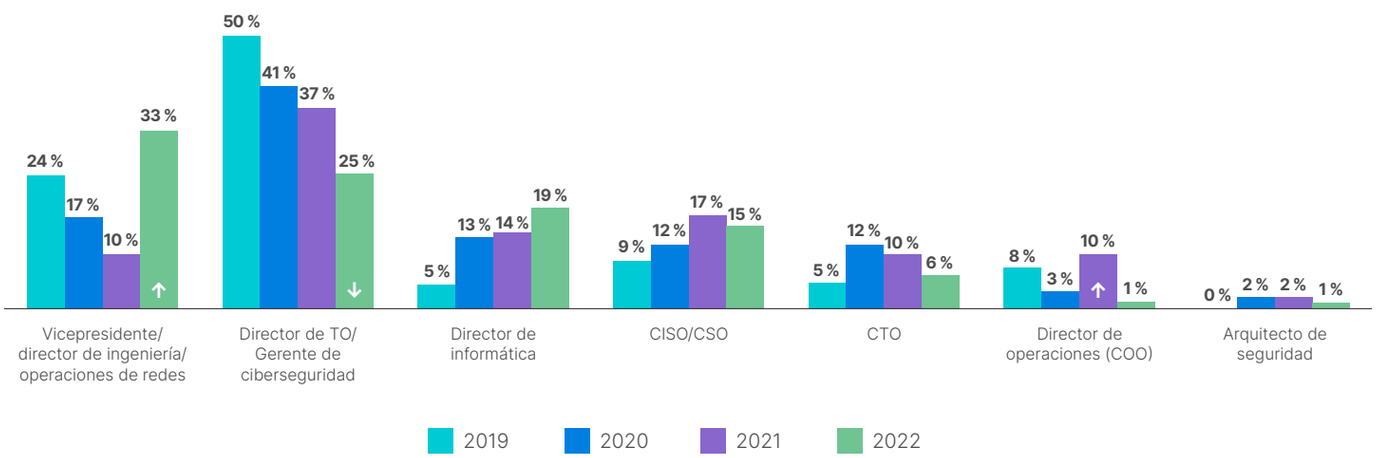


Figura 6: Líder actualmente responsable de la ciberseguridad TO.

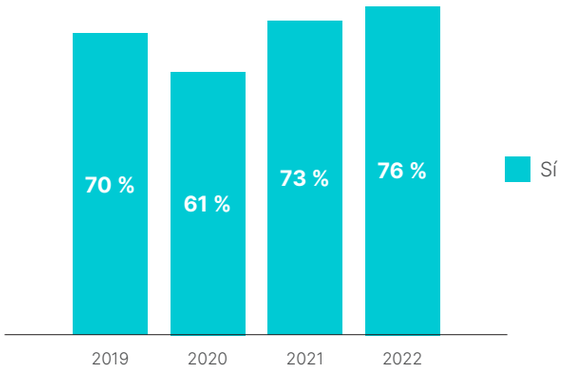


Figura 7: Encuestados que esperan que la seguridad de TO pase a depender del director de Seguridad informática en los próximos 12 meses.

Trayectorias profesionales hacia la seguridad de TO

Para poder participar en la encuesta, los encuestados debían tener una responsabilidad importante en materia de TO. De hecho, el 85 % de ellos dedica más de la mitad de su tiempo a la administración de esa función, y esta consume más de tres cuartas partes de las horas de trabajo del 28 % (Figura 8). Dos tercios de los encuestados en todo el mundo tienen una trayectoria profesional en el ámbito de TO, ya sea en organizaciones industriales o en proveedores de soluciones de TO (figura 9). El tercio restante proviene de un entorno de seguridad de TI, incluyendo más de la mitad de los encuestados de Latinoamérica.

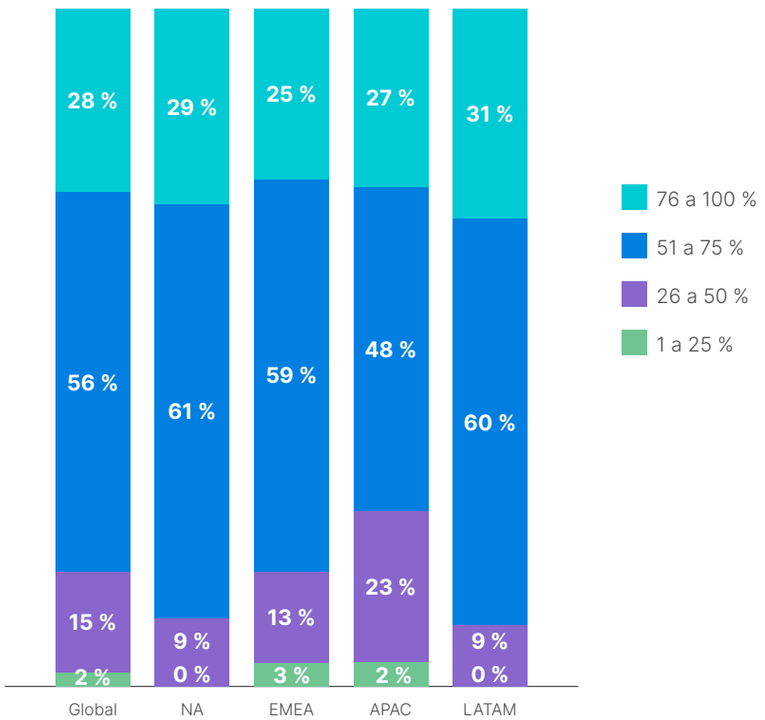


Figura 8: Porcentaje de tiempo dedicado a apoyar/administrar la seguridad de TO.

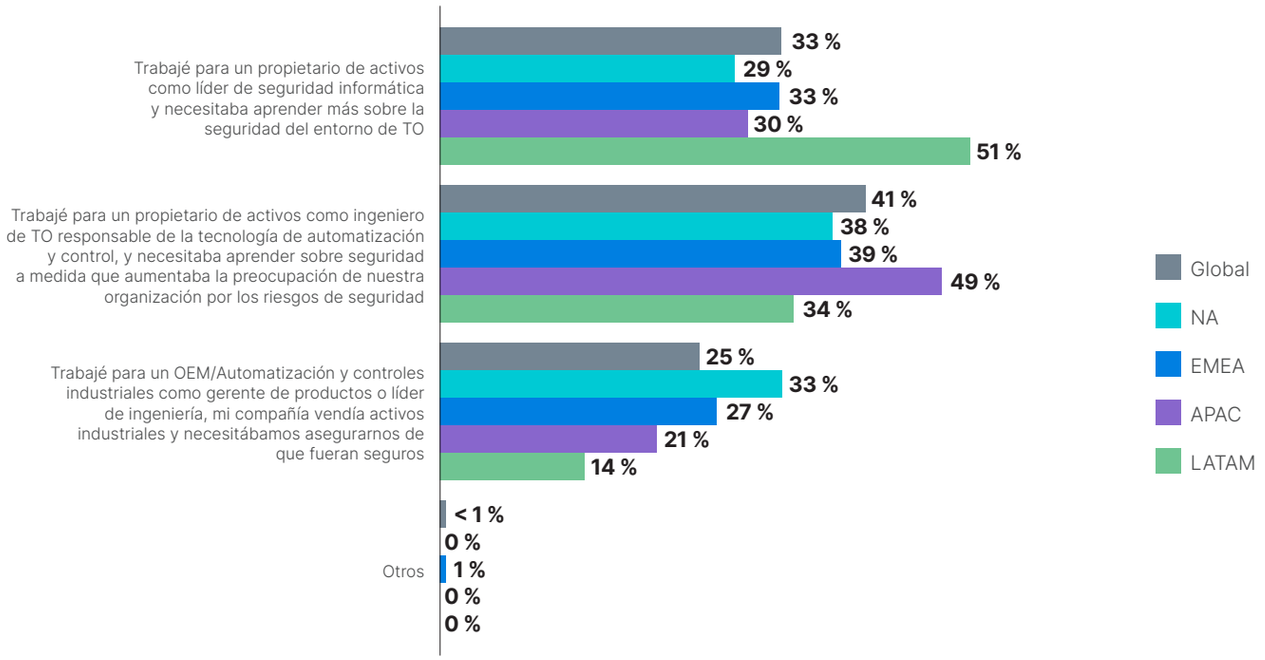
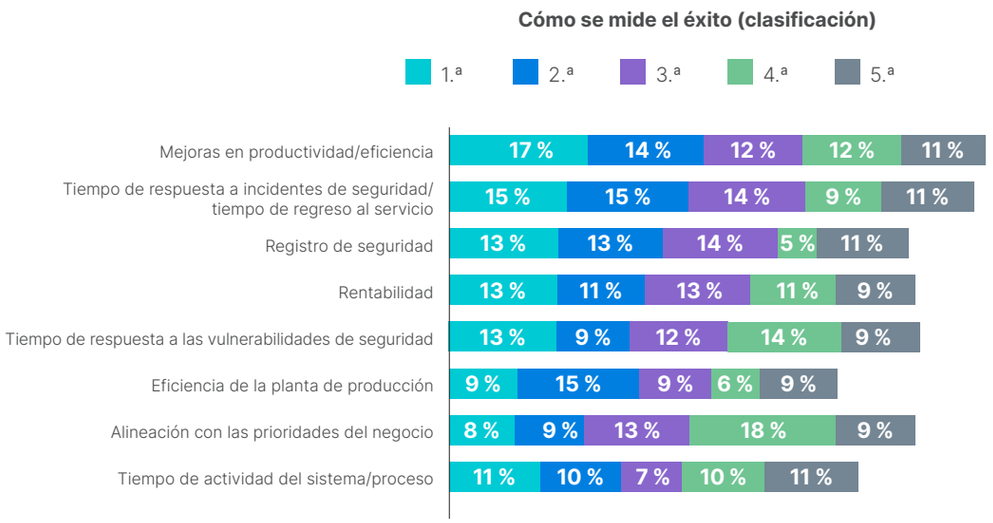


Figura 9: Trayectoria profesional que condujo a la seguridad de TO.

Perspectiva 2: Algunas organizaciones todavía tienden a priorizar la eficiencia sobre la seguridad de TO.

Aunque es probable que todas las organizaciones afirmen estar preocupadas por la seguridad de TO, una forma de discernir la importancia de la seguridad es observar cómo se mide a los líderes de TO. En la encuesta de este año, la mejora de la eficiencia y la productividad sigue siendo la medida de éxito más citada y se encuentra entre las tres primeras métricas en el 43 % de las organizaciones (Figura 10). Esta medida es la más citada como una de las tres principales medidas de éxito todos los años en que se realizó la encuesta, pero su prevalencia disminuyó un 14 % de 2021 a 2022.

El Director de seguridad informática es el principal influenciador de las decisiones de seguridad de TO en solo el 33 % de las organizaciones, por debajo del 45 % en 2021.



Entre las 3 opciones principales

	2022	2021	2020	2019
Mejoras en productividad/eficiencia	43↓	57 %	46 %	55 %
Tiempo de respuesta a incidentes de seguridad/ tiempo de regreso al servicio	43 %	N/A	N/A	N/A
Registro de seguridad	40 %	34 %	44 %	41 %
Rentabilidad	37 %	41 %	40 %	53 %
Tiempo de respuesta a las vulnerabilidades de seguridad	34 %↓	47 %↑	32 %	44 %
Eficiencia de la planta de producción	32 %	42 %	41 %↓	42 %
Alineación con las prioridades del negocio	29 %	33 %	24 %	29 %
Tiempo de actividad del sistema/proceso	29 %↓	41 %	40 %	35 %

Figura 10: Clasificación de las métricas de éxito.

Al mismo tiempo, una métrica de seguridad, el tiempo de respuesta a incidentes o regreso al servicio, también fue citada por el 43 % de los encuestados como una de las tres principales mediciones, lo que sin duda es una buena señal. También se produjeron descensos significativos en la importancia del tiempo de respuesta a las vulnerabilidades de seguridad y el tiempo de actividad del sistema/proceso, pero el hecho de que la métrica de respuesta a incidentes fuera nueva para la encuesta de 2022 puede ser una de las razones por las que las otras opciones relacionadas con la seguridad descendieron.

Preocupación en particular por el ransomware

El ransomware domina los titulares de los medios de comunicación en el ámbito de la ciberseguridad desde hace varios años y las organizaciones manifiestan una gran preocupación por esta táctica, a pesar de que es menos común que otros tipos de ataques. Más de dos tercios de los encuestados en todo el mundo, y tres cuartas partes en Norteamérica, dicen estar más preocupados por el ransomware que por otras intrusiones (Figura 11). El ransomware causó daños importantes y costos económicos a lo largo de los años, y un buen resultado de su gran visibilidad es que las organizaciones están debidamente preocupadas. Sin embargo, otros tipos de ataques perjudiciales pueden no recibir la atención que merecen debido a su menor visibilidad.

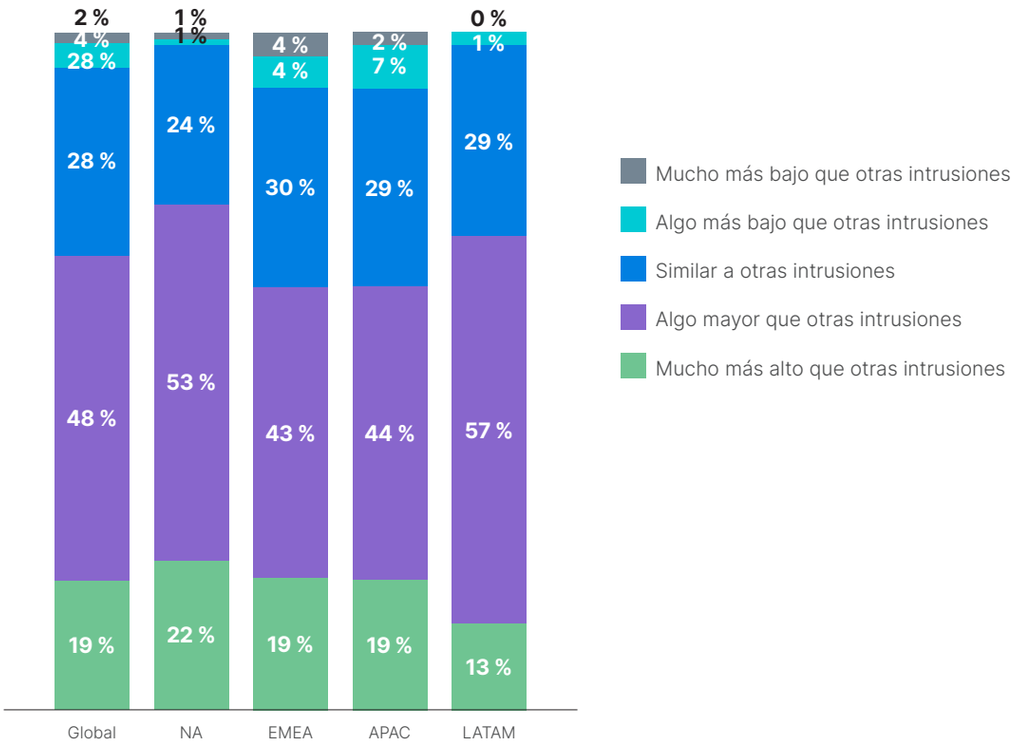


Figura 11: Nivel de preocupación por el ransomware.

Clasificación de la importancia de las herramientas de ciberseguridad

Los encuestados no saben qué características de las soluciones de ciberseguridad son las más importantes para sus organizaciones. Las herramientas de análisis, supervisión y evaluación de la seguridad fueron citadas como las más importantes, pero solo por una pluralidad del 17 % (Figura 12). En general, las soluciones de administración y supervisión del cumplimiento fueron las más citadas entre las tres primeras y las características de protección de protocolos específicos de TO ocuparon el segundo lugar.

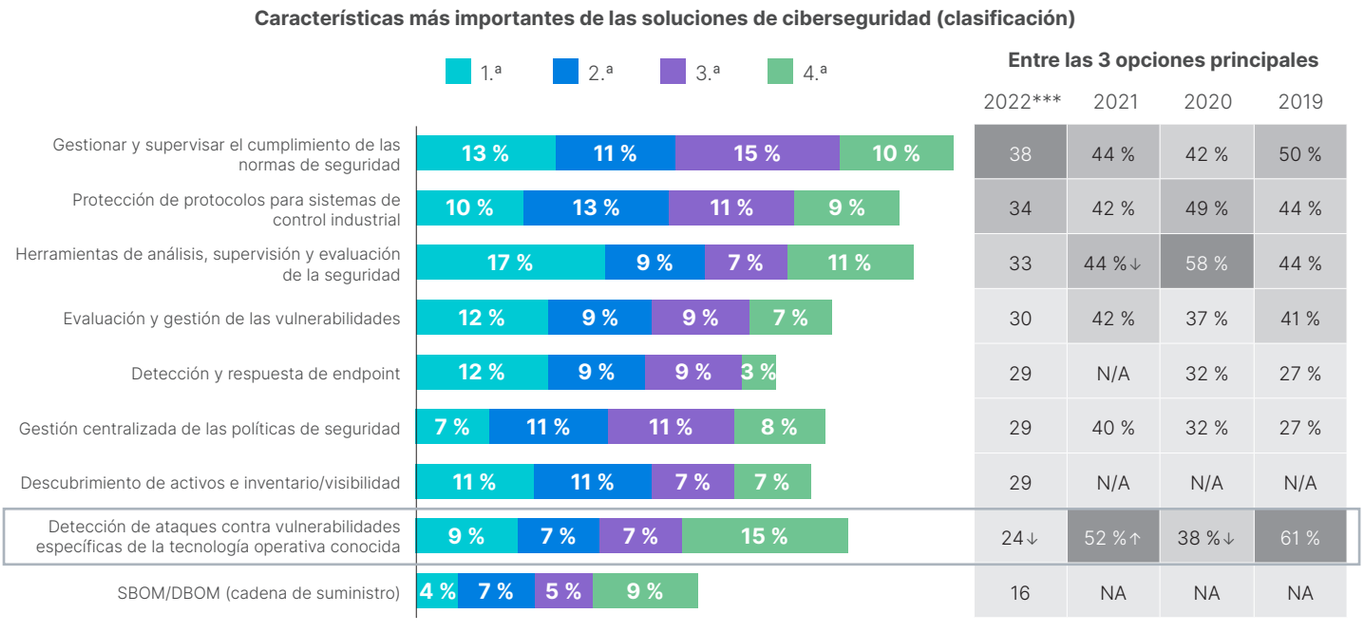


Figura 12: Clasificación de las características más importantes de las soluciones de ciberseguridad.

Perspectiva 3: Las organizaciones informan de una mejora gradual de la postura de seguridad de TO, pero se necesitan más mejoras

Al igual que en años anteriores, nuestra encuesta pedía a los encuestados que informaran del nivel de madurez de la seguridad de TO que alcanzaron sus organizaciones, con una breve descripción de cada uno de los cinco niveles de madurez. Entre todos los encuestados, el 84 % alcanzó al menos el nivel 2, habiendo establecido accesos y perfiles (Figura 13). La mitad de los encuestados alcanzó al menos el nivel 3 estableciendo un comportamiento predictivo y el 21 % alcanzó el nivel 4 con la orquestación y la automatización.

Esto representa una mejora marginal con respecto a 2021, sobre todo gracias a que las organizaciones pasaron del nivel 2 al 3. El porcentaje de organizaciones que alcanzaron al menos el nivel 3 aumentó del 44 % al 50 % año tras año.

El tiempo de respuesta a incidentes de seguridad y de regreso al servicio es una de las tres principales métricas de éxito de las TO en el 43 % de las organizaciones.

Al analizar los resultados por geografía, una mayor proporción de encuestados de Latinoamérica y APAC tienen el nivel 4. Mientras tanto, en Norteamérica, un mayor número de organizaciones están en el nivel 1, pero menos en el 4, lo que deja a más del 70 % de las organizaciones en los niveles intermedios.

Lamentablemente, solo la mitad de los encuestados afirma que la postura de seguridad de TO de su organización es un factor importante en su puntuación de riesgo general (Figura 14), aunque casi todas las demás organizaciones lo incluyen como un factor moderado.

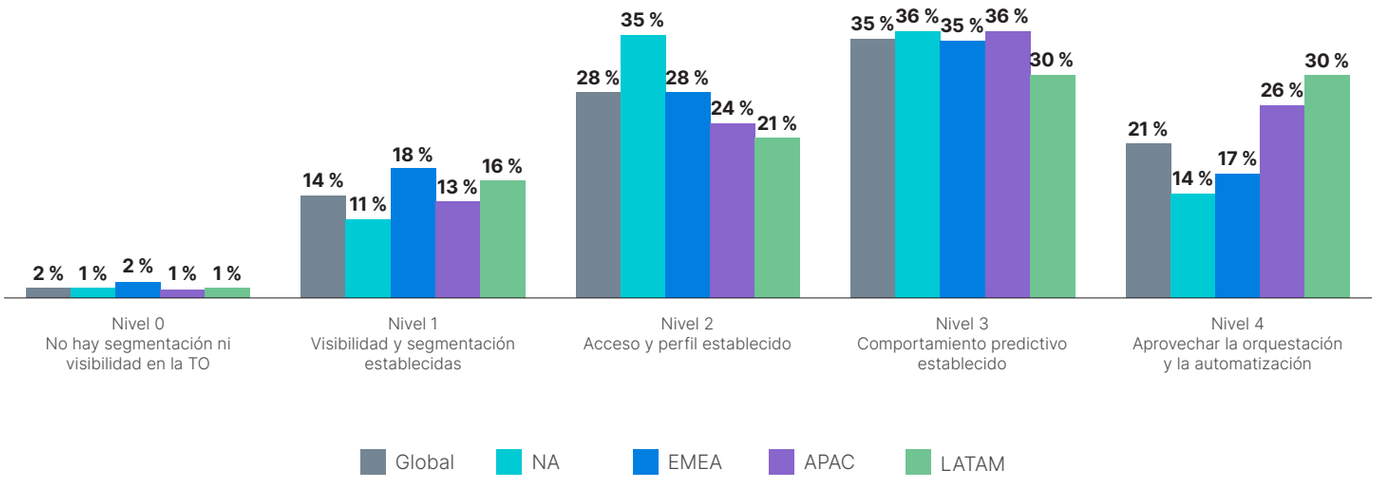


Figura 13: Nivel de madurez de la postura de ciberseguridad de TO.

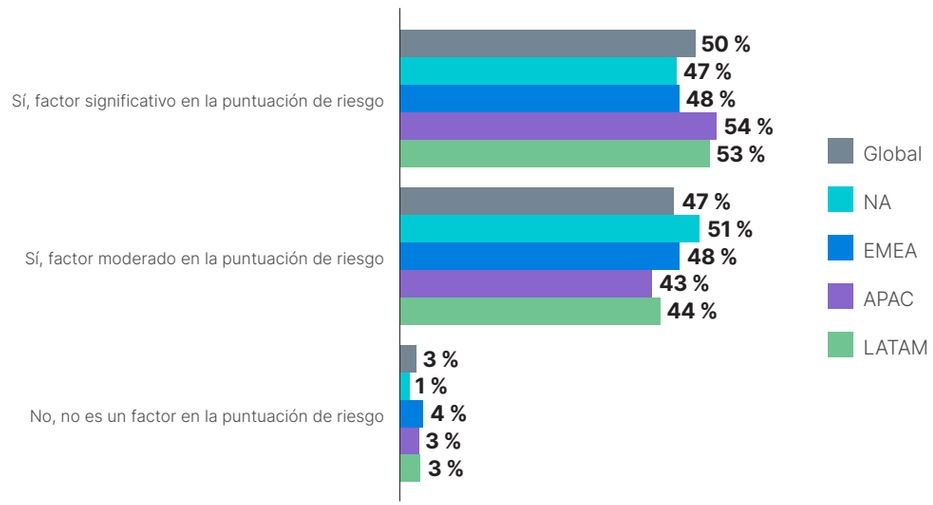


Figura 14: Importancia de la postura de seguridad de TO en la puntuación de riesgo global.

Madurez de la ciberseguridad en general

También se les pidió a los encuestados que calificaran la madurez de su programa general de ciberseguridad, incluyendo TI y TO. En este caso, es más probable que los encuestados hayan alcanzado el nivel 3 (59 %), pero es menos probable que alcanzaran el nivel 4 (16 %, Figura 15). Una vez más, las empresas de Latinoamérica y APAC muestran una mayor madurez, mientras que las de Norteamérica son más bajas en general. Las organizaciones más grandes y las del sector manufacturero tienen más probabilidades de tener niveles de madurez más altos, al igual que las organizaciones en las que los principales líderes de tecnología y seguridad tienen influencia sobre las decisiones de ciberseguridad (Figura 16).

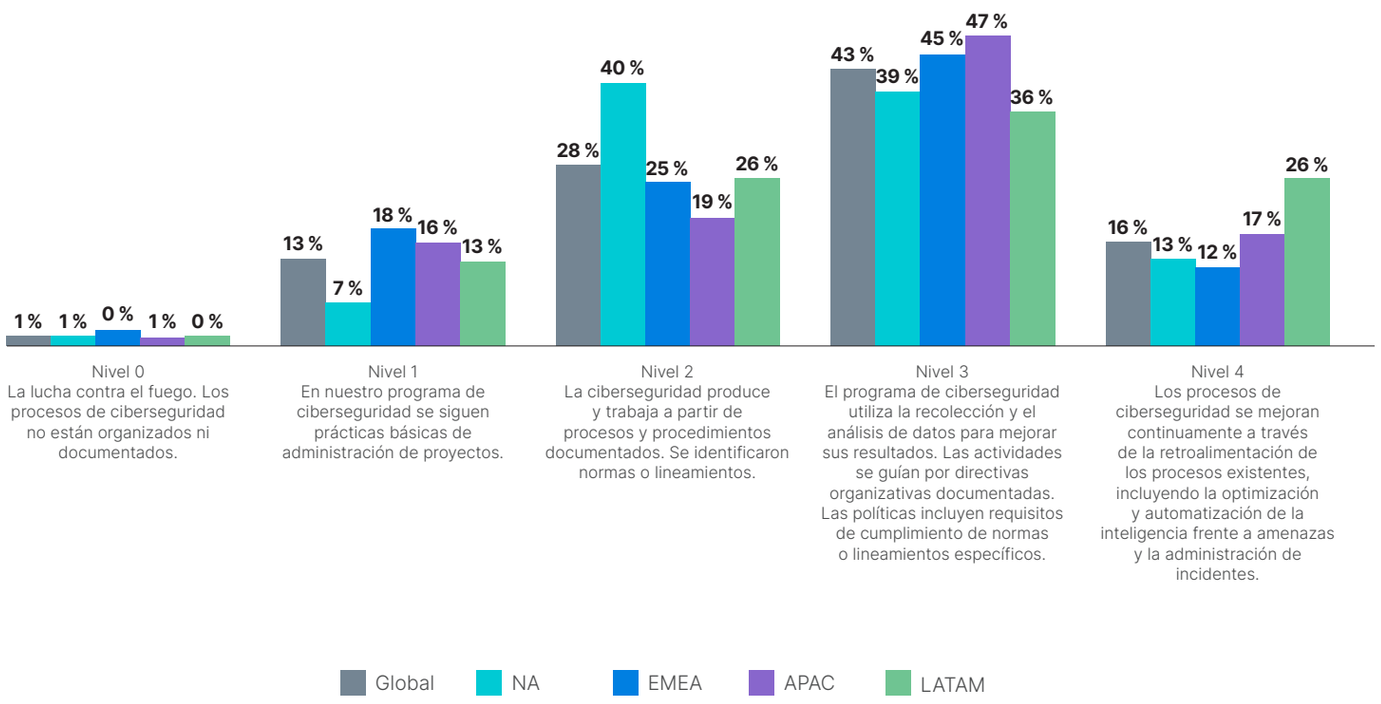
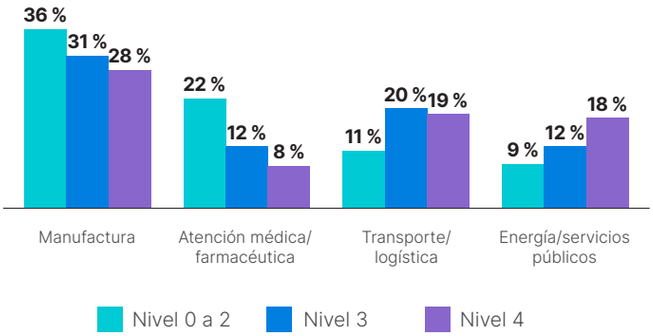
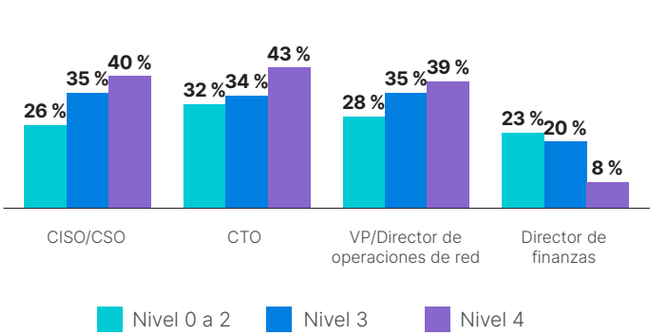


Figura 15: Nivel de madurez del programa general de ciberseguridad.





% Más de 5000 empleados		
21 %	28 %	41 %

% de ciberseguridad que ayuda/impulsa mi éxito		
65 %/4 %	82 %/6 %	83 %/11 %
% ayuda que facilita las normas de seguridad		
40 %	46 %	58 %

Figura 16: Datos demográficos seleccionados de los encuestados por nivel de madurez del programa de ciberseguridad.

Visibilidad centralizada

El establecimiento de la visibilidad de los procesos de TO se incluye en el nivel 1 de nuestra matriz de madurez de seguridad de TO, pero la granularidad de esa visibilidad puede marcar la diferencia. Aunque el 98 % de los encuestados afirma tener al menos el nivel 1 de madurez de seguridad de TO, solo el 74 % dice que más de tres cuartas partes de sus actividades de TO son visibles para el equipo de operaciones de seguridad (Figura 17). Esta cifra es del 77 % en Norteamérica, lo que supone una mejora con respecto a los resultados de la encuesta norteamericana de años anteriores (Figura 18). Sin embargo, el porcentaje de encuestados norteamericanos que tienen una visibilidad del 100 % parece estar en declive: del 23 % en 2020 al 13 % en 2022.

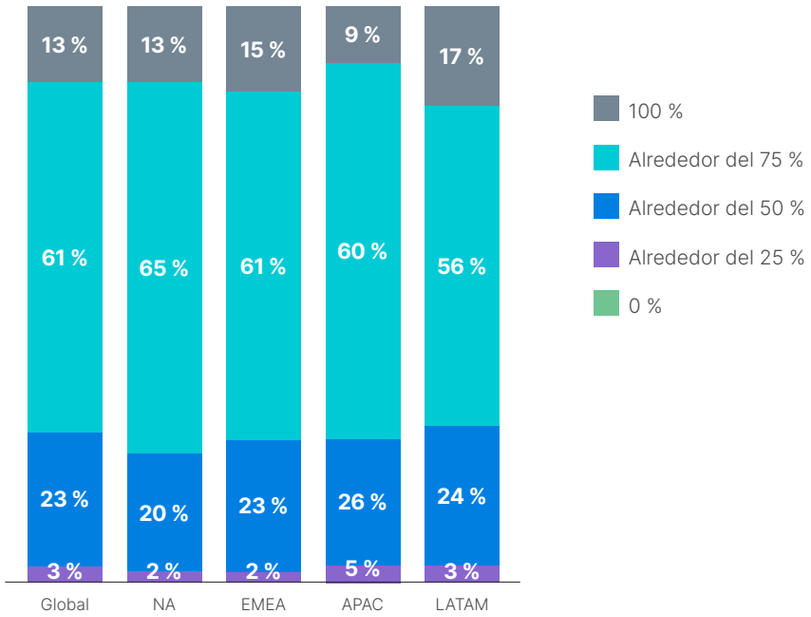


Figura 17: Visibilidad de las actividades de TO por parte de las operaciones de seguridad.

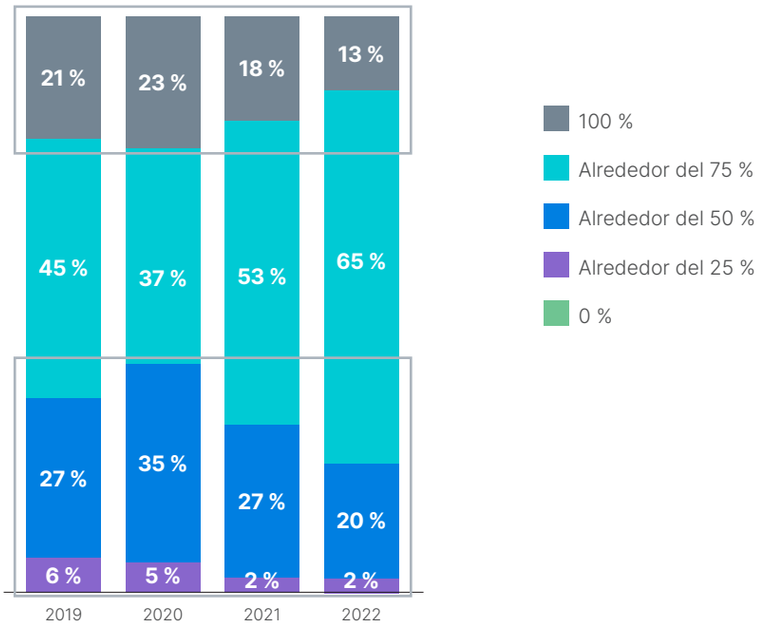


Figura 18: Visibilidad de las actividades de TO por operaciones de seguridad, Norteamérica.

Perspectiva 4: Las organizaciones tienen diversas formas de abordar la seguridad de TO y muchas de ellas tienen brechas de seguridad

Debido a que los sistemas de TO solían estar aislados de Internet en años pasados, la necesidad de proteger los sistemas de TO contra las amenazas informáticas es relativamente nueva y nuestra encuesta reveló que las prácticas de seguridad aún no se estandarizan.

Como hemos comentado, un enfoque es confiar la administración de seguridad de TO al SOC, que desempeña esa función para los sistemas de TI desde hace años. Casi todos los encuestados adoptaron este enfoque para al menos algunas actividades de TO, pero solo el 52 % de las organizaciones lograron habilitar el monitoreo y el seguimiento de *todas* las actividades de TO por parte del equipo del SOC (Figura 19). Esta cifra no varía en los cuatro años que hemos realizado esta encuesta. Las empresas de APAC lo están haciendo mejor en este sentido, ya que el 59 % supervisa todas las actividades del SOC.

El 50 % de las organizaciones alcanzó el nivel 3 de madurez de seguridad de TO, frente al 44 % en 2021.

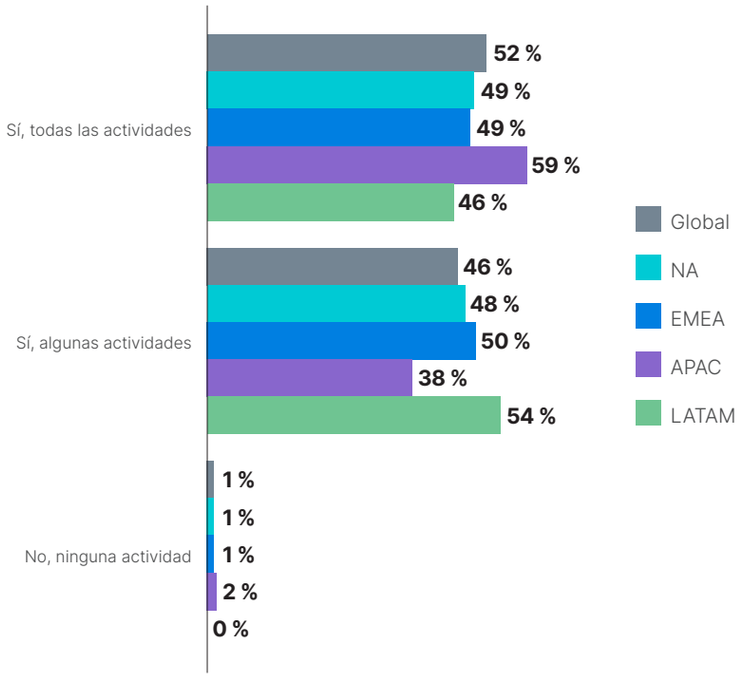


Figura 19: Actividades de TO monitoreadas y con seguimiento por el SOC.

Seguimiento e informe de las métricas

Cuando se trata de dar seguimiento a las métricas de seguridad y de informar sobre ellas, los resultados son contradictorios. Cuando se les presentó una lista de mediciones básicas de ciberseguridad que posiblemente deberían ser objeto de seguimiento en todas las organizaciones, no más del 52 % de los encuestados afirmó que dan seguimiento a alguna de ellas (Figura 20).

Si se comparan los resultados de Norteamérica con los de años anteriores, el porcentaje que da seguimiento e informa varias de las métricas disminuyó significativamente a partir de 2021 (Figura 21), incluidas las vulnerabilidades detectadas y bloqueadas y las intrusiones detectadas y solucionadas.

Porcentajes similares de encuestados reportan información básica de seguridad de TO a la dirección ejecutiva de manera regular. Cuando se les presentó una lista que incluía información crítica, como informes de cumplimiento, evaluaciones de seguridad y compromisos de seguridad, no más del 53 % informó a la dirección ejecutiva sobre un solo elemento (Figura 22).

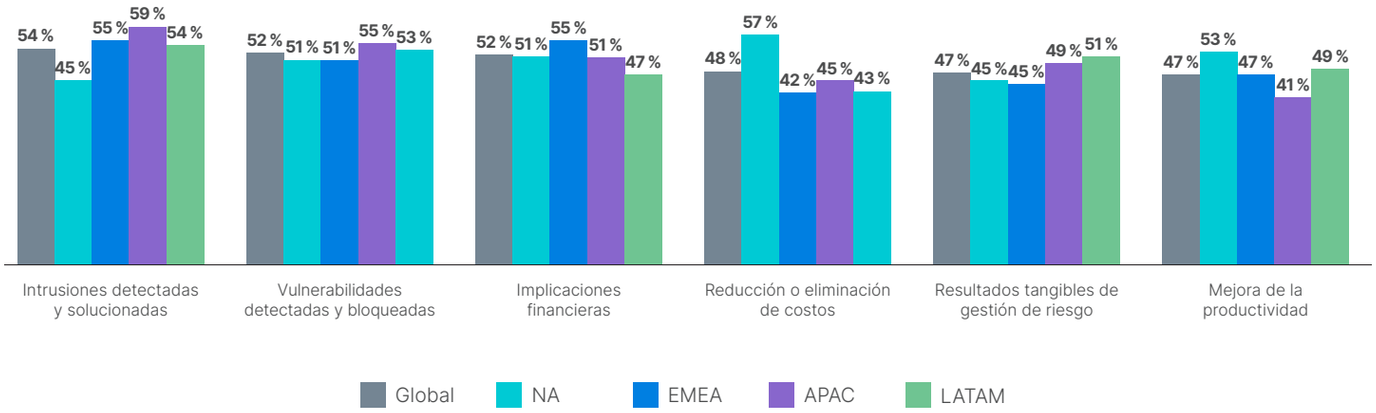


Figura 20: Medidas de ciberseguridad con seguimiento e informe.

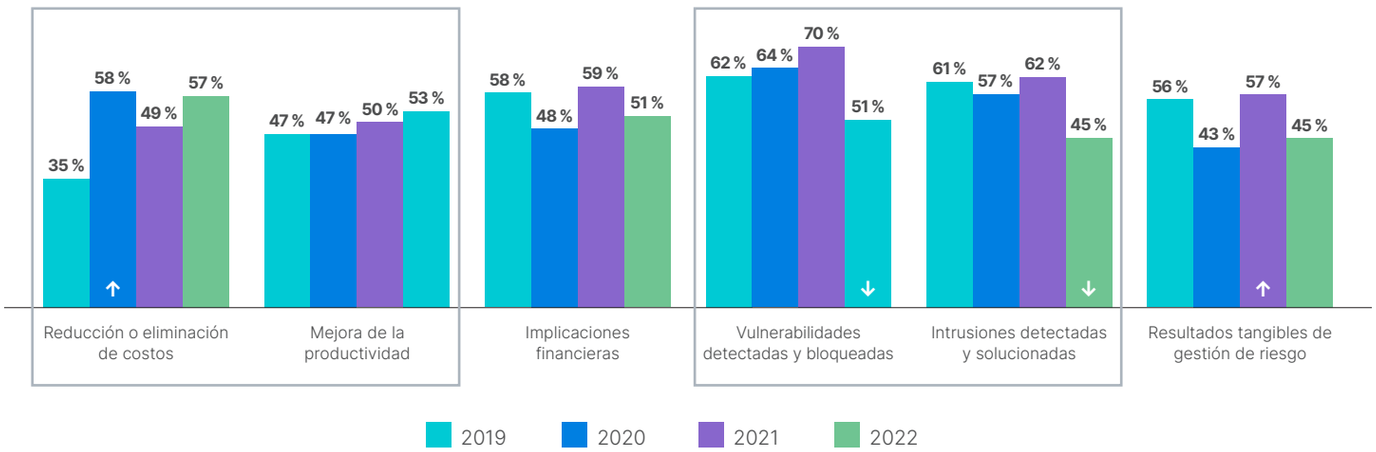


Figura 21: Mediciones de ciberseguridad a las que se hace seguimiento y se informa, Norteamérica.

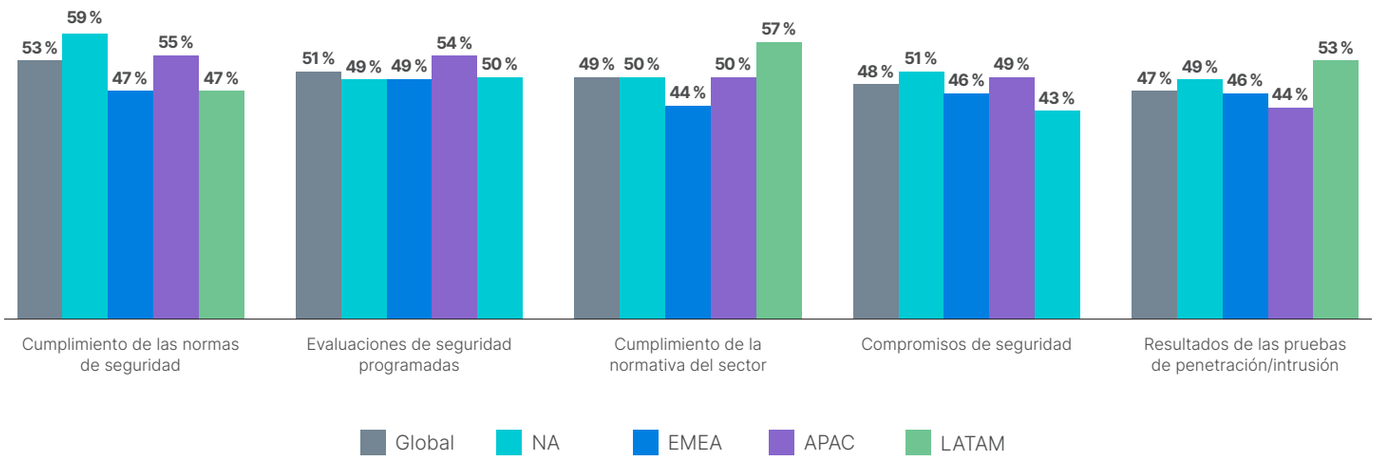


Figura 22: Problemas de ciberseguridad en TO comunicados a la dirección ejecutiva.

Características de seguridad que se usan

Las respuestas de los encuestados son diversas en cuanto a las herramientas y características de seguridad que utilizan para proteger sus sistemas de TO. Ante una lista bastante completa de herramientas y procesos, ninguna característica es utilizada por más del 47 % de los encuestados (Figura 23). Entre las soluciones incluidas por primera vez este año se encuentran el acceso remoto seguro (41 %); la seguridad, la orquestación, la automatización y la respuesta de seguridad (SOAR; 37 %) y el uso de inteligencia frente a amenazas (36 %).

Este enfoque de "algo de lo anterior" refleja un aspecto de la seguridad que, en muchos sentidos, todavía está en su fase inicial, con diferentes organizaciones probando diferentes enfoques. Una práctica cuya popularidad está disminuyendo claramente es el uso del centro de operaciones de red (NOC) para la gestión de la seguridad de TO (Figura 24). Curiosamente, los encuestados norteamericanos tienden a utilizar menos funciones y prácticas de la lista en general.

No más del 47 % de las organizaciones utiliza una sola herramienta o enfoque de seguridad de TO.

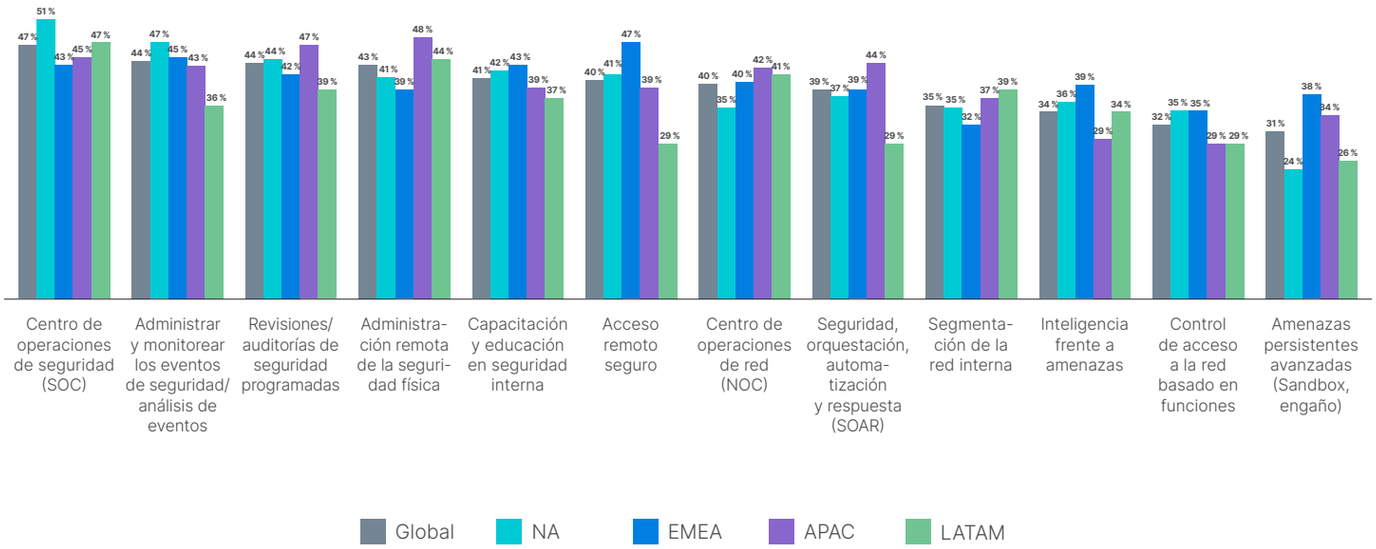


Figura 23: Características de ciberseguridad y seguridad existentes.

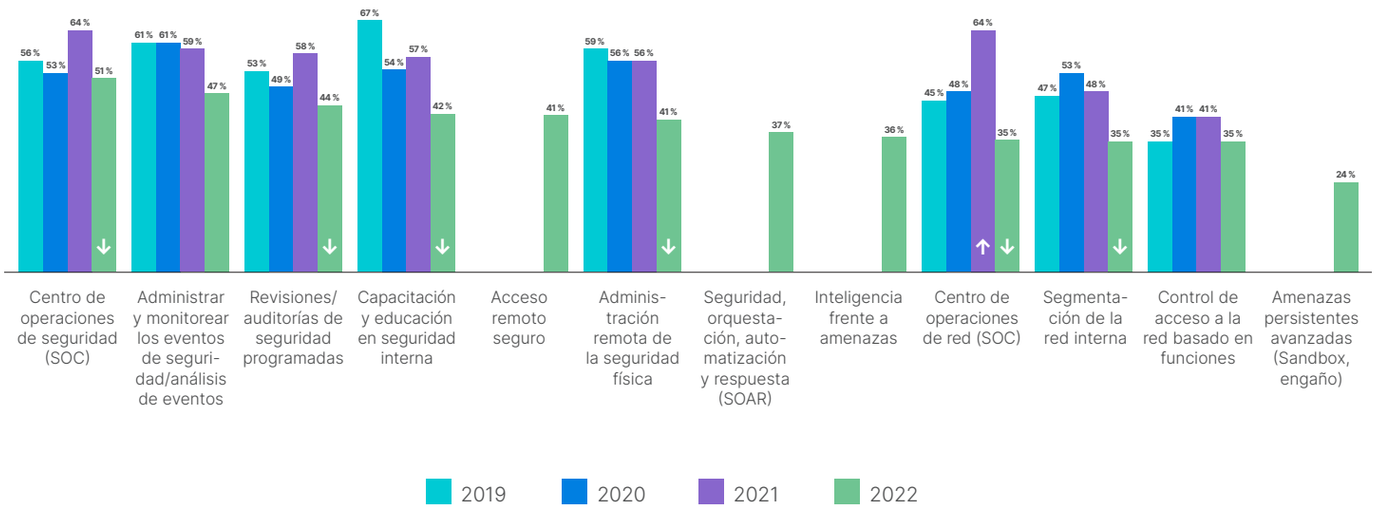


Figura 24: Características de ciberseguridad y seguridad existentes, Norteamérica.

Complejidad de los sistemas de seguridad y percepción de la eficacia

La complejidad es uno de los problemas que pueden obstaculizar la seguridad de TO. La gran mayoría de las organizaciones utiliza entre dos y ocho proveedores diferentes para sus dispositivos de TO y tiene entre 100 y 10 000 dispositivos en funcionamiento (Figura 25). Solo el 7 % de las organizaciones consiguió reducir el número de proveedores a uno.

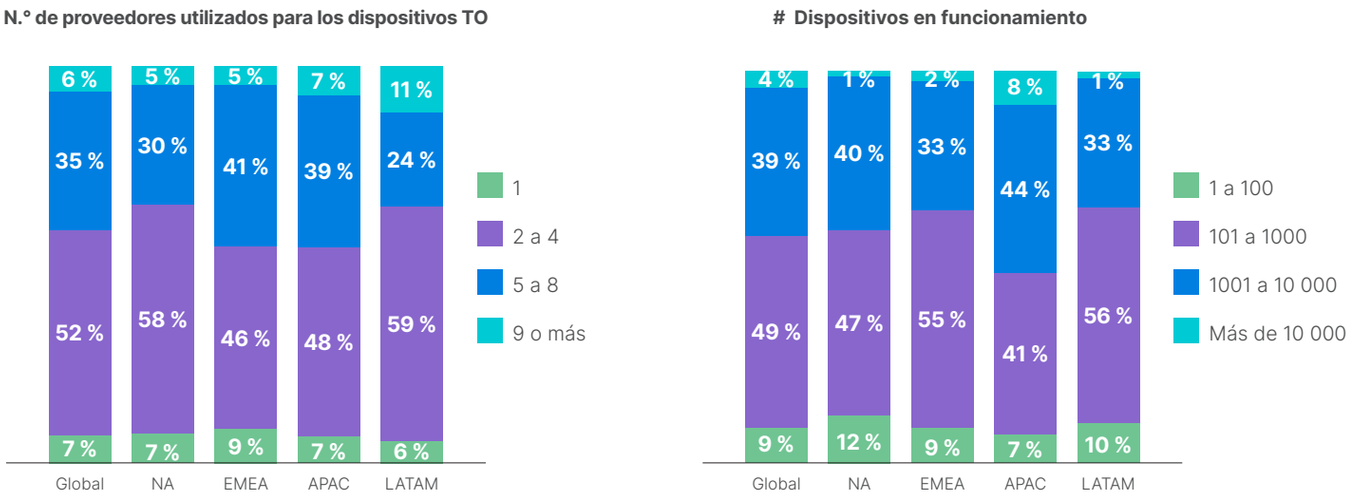


Figura 25: Proveedores de TO y dispositivos de TO en uso.

Perspectiva 5: la mayoría de las organizaciones sigue sufriendo múltiples intrusiones al año

Cada año, hacemos una pregunta sencilla a los encuestados sobre sus resultados de seguridad: ¿Cuántas intrusiones sufrieron en los últimos 12 meses? En 2022, tres cuartas partes de los encuestados admitieron que sufrieron al menos tres intrusiones, el 19 % tuvo más de seis y el 7 % tuvo más de 10 (Figura 26). Solo el 6 % de los encuestados declaró que no sufrió ninguna intrusión en 12 meses.

Si se observan los resultados norteamericanos de esta pregunta a lo largo de cuatro años, las cosas no mejoran en general, con aproximadamente el mismo porcentaje de los que sufrieron tres o más intrusiones desde 2020 (Figura 27). Un pequeño consuelo es que el porcentaje de encuestados norteamericanos que tuvo 10 o más intrusiones disminuyó del 12 % al 5 % año tras año.

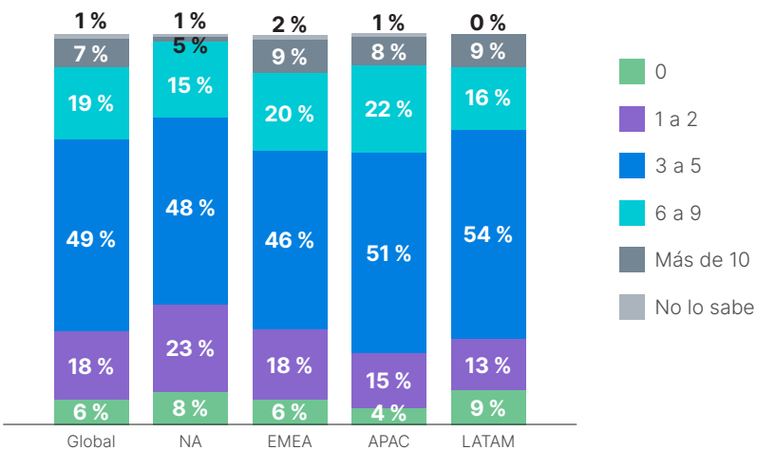


Figura 26: Cantidad de intrusiones durante el último año.

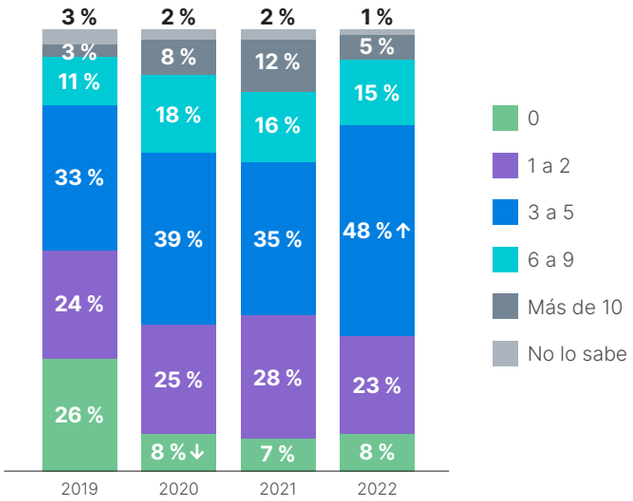


Figura 27: Número de intrusiones en el último año, Norteamérica.

Tipos de ataques

Los encuestados experimentaron una gran variedad de tipos de ataques, lo que no es sorprendente dado el número de intrusiones. Un total de ocho tipos de ataques afectaron al menos a una cuarta parte de los encuestados cada uno, con el malware y la suplantación de identidad encabezando la lista al afectar a más del 40 % de las organizaciones (Figura 28). El ransomware afectó a menos de un tercio de las organizaciones en general, pero al 44 % de las empresas latinoamericanas. Los encuestados latinoamericanos experimentaron menos suplantación de identidad que en las otras regiones. En cuanto a los resultados de Norteamérica durante cuatro años, el malware y las infracciones internas maliciosas mostraron disminuciones este año (Figura 29).

Aunque el número general de intrusiones es notablemente similar, independientemente del nivel de madurez de seguridad declarado, probablemente porque las organizaciones más maduras son capaces de detectar un mayor porcentaje de las intrusiones que se producen. Pero si se observa por tipo de ataque, queda claro que las organizaciones más maduras tienen menos problemas con las amenazas internas, mientras que detectan más ataques desde el exterior (Figura 30).

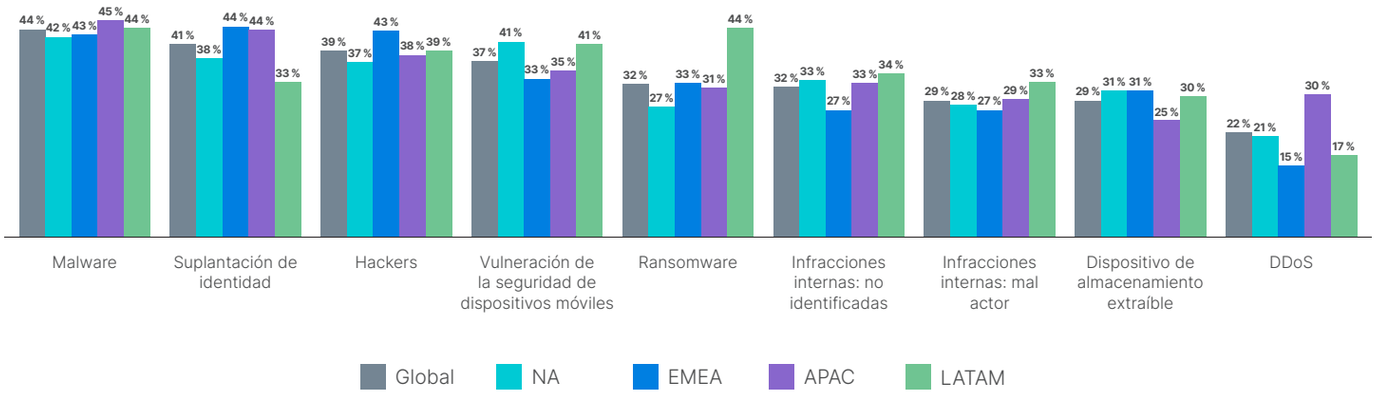


Figura 28: Tipos de intrusiones experimentadas.

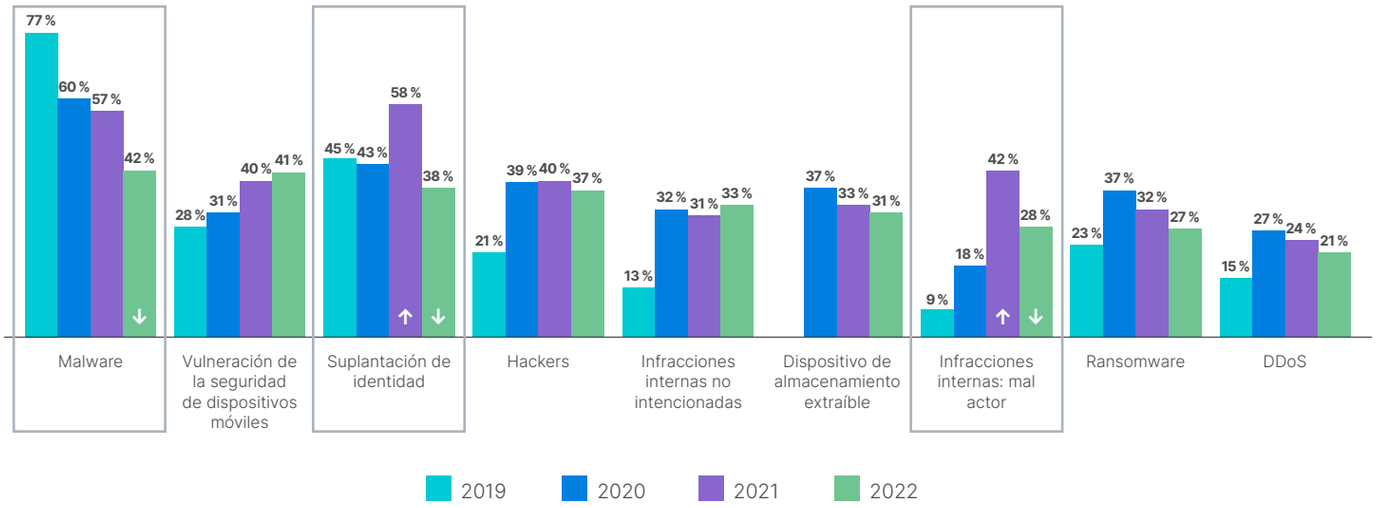


Figura 29: Tipos de intrusiones experimentadas, Norteamérica.

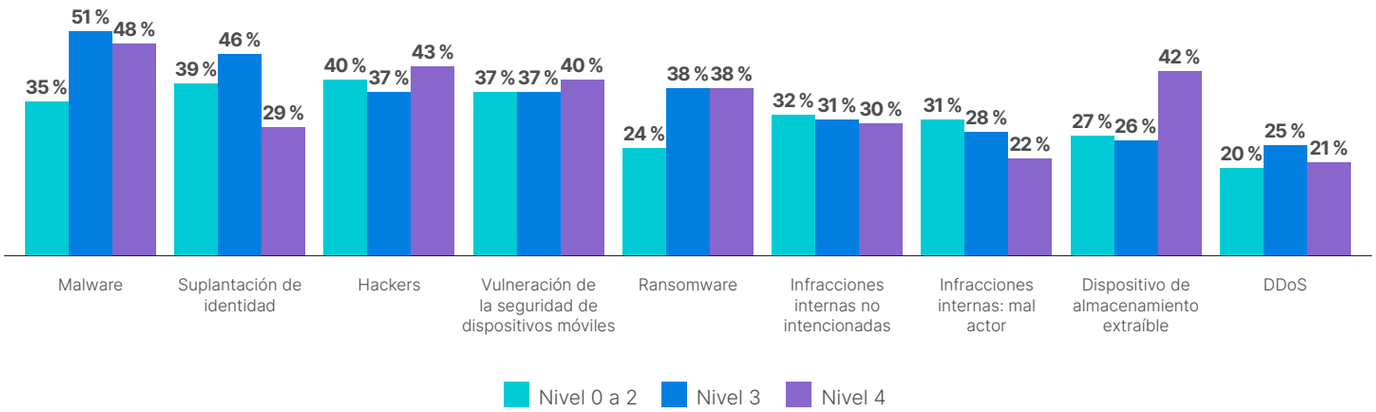


Figura 30: Tipos de intrusiones experimentadas por el nivel de madurez de seguridad informada.

Impacto de los ataques

Curiosamente, un porcentaje ligeramente mayor de ataques afectó a los sistemas de TO que a los de TI (Figura 31), ya que el 61 % de las intrusiones afectaron a los sistemas de TO y el 60 % a los de TI. Los impactos comerciales de las intrusiones no fueron en absoluto triviales. Cerca de la mitad de los encuestados sufrieron una interrupción operativa que afectó la productividad, mientras que más de un tercio tuvo un impacto en los ingresos, en la pérdida de datos, en el cumplimiento y en el valor de la marca, además de amenazas a la seguridad física (Figura 32). Y el 90 % de los encuestados admite que el regreso al servicio fue un proceso que duró horas o más (Figura 33).

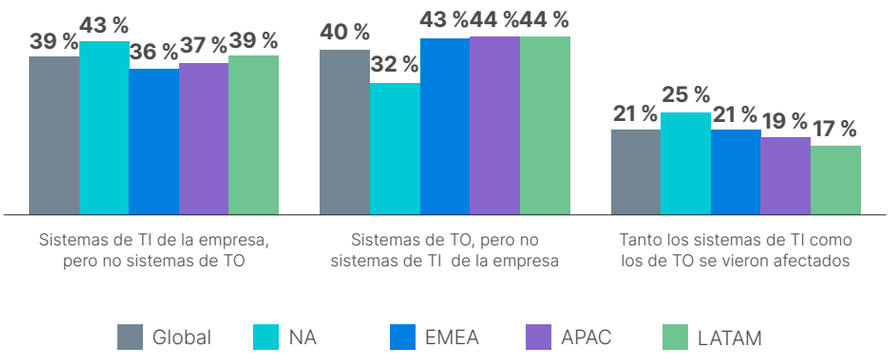


Figura 31: Entornos afectados por las intrusiones.

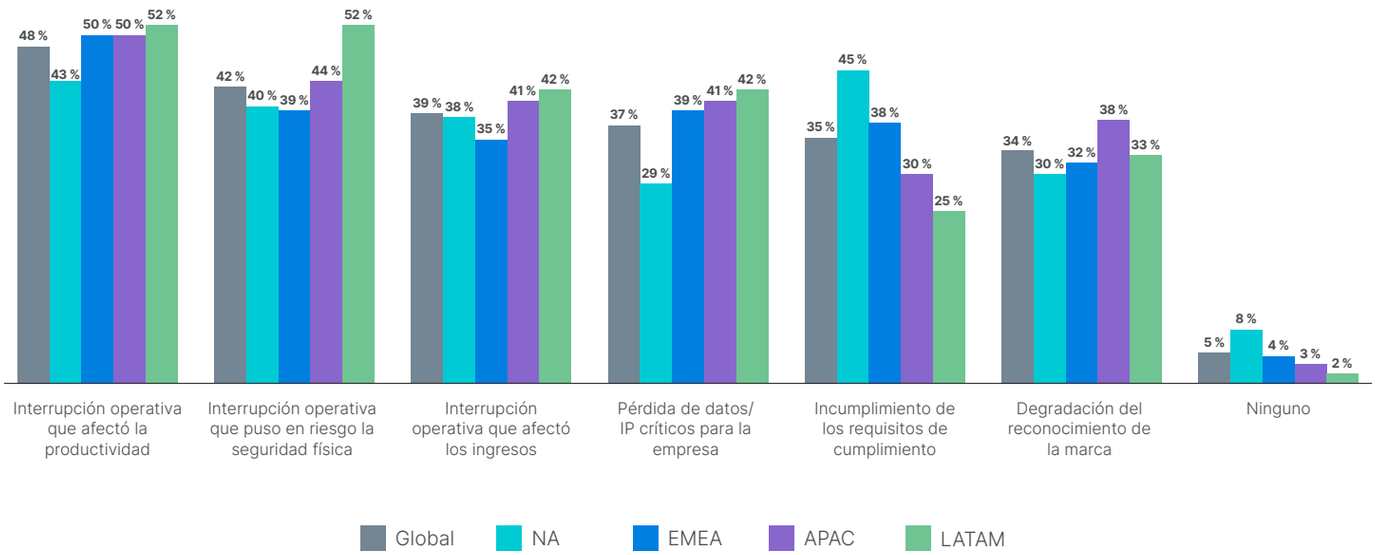


Figura 32: Impactos organizacionales de las intrusiones.

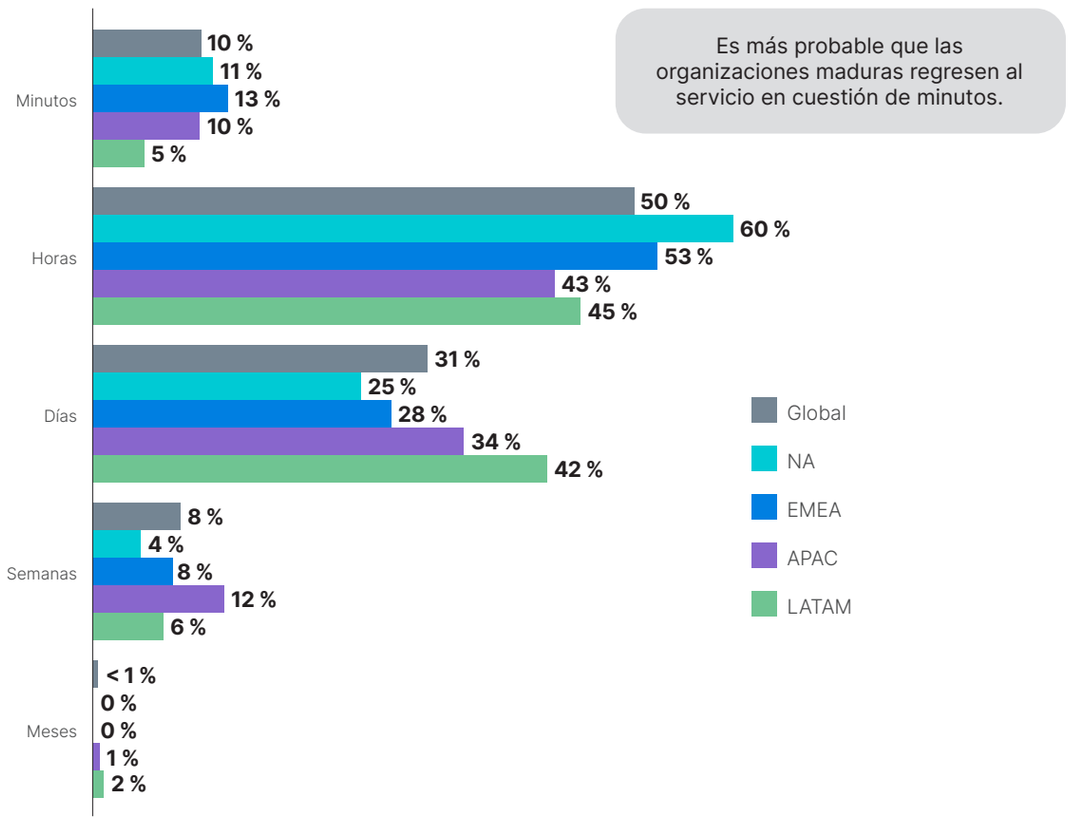


Figura 33: El tiempo de regreso al servicio más largo después de una intrusión.

Las mejores prácticas de las organizaciones top-tier.

Solo el 6 % de las organizaciones representadas en la encuesta de este año afirman que no tuvieron ninguna intrusión en los últimos 12 meses, mientras que el 5 % informó *más de 10 intrusiones*. Comparamos las prácticas.

Solo el 6 %
de los encuestados
puede afirmar que no hubo
intrusiones en el último año.

1. Las organizaciones top-tier (de primer nivel) tienen un 17 % más de probabilidad de que todas sus actividades de TO sean visibles de forma centralizada para las operaciones de ciberseguridad.

La visibilidad centralizada de extremo a extremo de todas las actividades de TO es clave para garantizar su seguridad y esto es definitivamente un trabajo en progreso en la mayoría de las organizaciones. Las organizaciones top-tier tienen más del triple de probabilidades de haber logrado dicha visibilidad que sus homólogas de nivel inferior.

2. Las organizaciones top-tier tienen un 177 % más de probabilidad de tener el tiempo de respuesta a las vulnerabilidades de seguridad como una de sus tres principales métricas de éxito.

Como dice el viejo adagio, "lo que se mide, se mejora", y responder rápidamente a las vulnerabilidades de la seguridad de TO es clave para proteger estos sistemas. Las organizaciones con mejores resultados tienen casi tres veces más probabilidades de que esta medición sea una parte destacada de su revisión del rendimiento.

3. Las organizaciones top-tier tienen un 37 % más de probabilidad de contar con tecnología de control de acceso a la red basada en funciones.

Garantizar que solo las personas autorizadas puedan acceder a sistemas específicos es fundamental para asegurar cualquier activo tecnológico. Cuando se trata de TO, las personas que necesitan acceder a dichos sistemas tienen un rango relativamente estrecho de nombres de puestos. Las organizaciones que evitaron las intrusiones el año pasado son mucho más propensas a tener estos controles.

4. Las organizaciones top-tier tienen un 48 % más de probabilidad de informar compromisos de seguridad a la dirección ejecutiva.

Los temas que se incluyen en los informes periódicos a la dirección ejecutiva tienden a permanecer en primera línea durante todo el año. Las organizaciones que mantienen a los altos cargos informados de las vulneraciones de seguridad tienden a tener menos. Las organizaciones top-tier tienden a ser más transparentes con la dirección ejecutiva.

5. Las organizaciones top-tier tienen un 32 % más de probabilidades de que su SOC supervise y haga un seguimiento de la seguridad de TO.

Los centros de operaciones de seguridad (SOC) existen desde hace décadas y desarrollaron las mejores prácticas granulares para administrar la seguridad de TI. Es más probable que los líderes de TO que lograron evitar las intrusiones confiaron la seguridad de TO al mismo grupo.

6. Las organizaciones top-tier tienen un 44 % más de probabilidades de hacer un seguimiento e informar de las intrusiones detectadas y solucionadas.

Entender los ataques pasados agudiza las habilidades de una organización para frustrar los futuros, y esto comienza con el mantenimiento de registros. Las organizaciones que evitaron las intrusiones son más propensas a denunciarlas de forma rutinaria cuando se producen.

7. Las organizaciones top-tier son infinitamente más propensas a utilizar un solo proveedor para sus dispositivos TO habilitados para IP.

Evitar la complejidad de las redes y los sistemas es una buena manera de reducir la superficie de ataque y mejorar la postura de seguridad. Ninguna de las organizaciones que sufrió 10 o más intrusiones utilizaba un solo proveedor para sus dispositivos TO con IP, mientras que casi un tercio de las organizaciones top-tier sí lo logró.

Conclusión

El Informe sobre el estado de la tecnología operativa y la ciberseguridad en 2022 concluye que los esfuerzos de seguridad de TO de las organizaciones de todo el mundo no avanzan lo suficiente hacia la plena protección de los sistemas ICS y SCADA en el mundo relativamente nuevo de la tecnología operativa conectada. El progreso incremental que se hizo en la madurez de la seguridad desde el año pasado hizo poco para mover la aguja en los resultados reales de seguridad. El resultado es que la gran mayoría de las organizaciones sigue sufriendo intrusiones, varias veces al año en la mayoría de los casos.

Debido al clima geopolítico, los gobiernos de todo el mundo advierten que es probable que aumenten los ciberataques contra las infraestructuras críticas y los activos económicos clave. Las organizaciones industriales de un amplio espectro de sectores harán bien en avanzar rápidamente en la madurez de sus esfuerzos de seguridad de TO, aprovechando el comportamiento predictivo, la orquestación y las tecnologías de automatización para establecer un verdadero acceso de confianza cero y defenderse de las amenazas procedentes de personas internas malintencionadas y bienintencionadas, ciberdelincuentes externos y atacantes patrocinados por el Estado.

Referencias

[1] Mayank Agrawal, et. al, "Industry 4.0: Reimagining Manufacturing Operations After COVID-19", McKinsey, 29 de julio de 2020.

[2] "Global Threat Landscape Report, 1H 2021", Fortinet, agosto de 2021.

[3] Clare Duffy, "Colonial Pipeline Attack: A 'Wake Up Call' about the Threat of Ransomware", CNN, 16 de mayo de 2021; Liam Tung, "Ransomware: Meat Firm JBS Says It Paid Out $11m After Attack," ZDnet, 10 de junio de 2021.

[4] "Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure", CISA, 20 de abril de 2022.

[5] Catherine Stupp, "Russian Cyberattacks Increase on Ukraine's Critical Infrastructure: Report", Wall Street Journal, 5 de abril de 2022.

[6] Phil Muncaster, "Critical Infrastructure Firms See Cyber-Attacks Surge", InfoSecurity, 10 de mayo de 2022.

[7] Steven Webb, "IT/OT & OT Total Available Market Analysis", Westlands Advisory Research for Fortinet, marzo 2022.

[8] "Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure", CISA, 20 de abril de 2022.

julio 6, 2022 10:46 a. m.

1578659-0-0-ES