XXII Encuesta Nacional de Seguridad Informática

Aprendiendo del futuro de la ciberseguridad.

DOI: 10.29236/sistemas.n163a4

Andrés R. Almanza J.

Resumen

La encuesta de seguridad informática, capítulo Colombia, soportada por la Asociación Colombiana de Ingenieros de Sistemas (ACIS) y realizada a través de Internet, entre los meses de marzo y mayo de 2022, contó con la participación de 206 encuestados, quienes con sus respuestas permiten conocer la realidad del país en esta temática. La distribución se hizo a través de las diferentes redes sociales, comunidades y grupos. Sus resultados muestran la transformación de las prácticas de seguridad y control en el país, los cuales se contrastan con los referentes internacionales seleccionados para esta versión de la encuesta.

Palabras clave

Seguridad de la información, encuesta, líder, perfil profesional, riesgos de información.

Introducción

Entender la realidad nacional en materia de seguridad de la información y ciberseguridad, permite visualizar los retos a corto, mediano y largo plazo, además de construir mejores posturas de seguridad y control en las organizaciones.

Ese entendimiento, sumado a conocer el contexto internacional, proporciona una proyección al entorno nacional para enfrentar los retos y desafíos en ambientes cada vez más permeados por la realidad digitalmente modificada.

De la misma manera que en otras versiones, la Encuesta Nacional pretende medir las dinámicas y lógicas de las empresas del país, ver otros referentes mundiales en la búsqueda y construcción de los propios.

Año tras año, este estudio ha reflejado cómo ha venido desarrollándose en Colombia la protección de la información en los entornos digitales y cómo en los diferentes sectores (empresarial y académico), la seguridad y la resiliencia digital se convierten en valores estratégicos dentro de las organizaciones.

Como parte de los esfuerzos académicos para estudiar y entender la realidad de la Colombia, se resalta el análisis longitudinal de 10 años titulado “Reflexiones y retos para la academia en la formación de profesionales de seguridad/ciberseguridad en Colombia: 2010 – 2020” (Cano & Almanza, 2021), que fue publicado en el 2021, como un registro analítico y documentado del pasado y una prospectiva sobre el futuro de la seguridad en Colombia, como un soporte más de los análisis realizados y situados de los resultados de esta nueva encuesta.

Como todos los años, se revisan para la realización de este informe, algunos de los reportes más representativos de la industria, para identificar convergencias, divergencias, contradicciones o complementos a los resultados propios de esta investigación.

Estructura de la encuesta

El estudio contempla 39 preguntas repartidas en varias secciones sobre diferentes asuntos.

Demografía: Describe la información del encuestado, cuáles son las tareas que realiza, la visión de la seguridad, además de los roles que en tal sentido puedan existir dentro de su organización. Datos que permiten ubicar el sector al que pertenece, el tamaño y tipo de empresa.

Presupuestos: Relaciona todos los aspectos asociados con los recursos financieros destinados en materia de seguridad y, sobre todo, en qué se concentra la inversión de dichos recursos.

Incidentes de seguridad: Muestra los detalles y tipos de incidentes presentados, un barrido por las prácticas más importantes en el

manejo y diligencia de la evidencia digital, como herramienta en la persecución de los ciberdelincuentes.

Herramientas y prácticas de seguridad: Se refiere a las prácticas comunes en materia de seguridad, ese conjunto de acciones que permite a las organizaciones definir una postura clara en materia de protección.

Políticas de seguridad: Busca conocer el estado de las políticas de seguridad, la práctica de la gestión de riesgos y su integración en el contexto organizacional.

Capital intelectual: Busca definir cómo son las áreas de seguridad y las características básicas en materia de experiencia, formación y capacitación de los profesionales de seguridad. Muestra también la relación de las instituciones de educación superior frente a una realidad tan cambiante.

Temas emergentes: En esta sección se analizan varios aspectos, entre ellos: la percepción del futuro en materia de ciberseguridad; la vinculación de los directivos de la organización en la ciberseguridad empresarial, además de la responsabilidad y el papel del líder de seguridad en el desarrollo de la dinámica de protección de la empresa.

Cambios: Cada año luego de revisados los resultados de la encuesta, las opciones y los análisis correspondientes de pertinencia y relevancia, se cambian, adicionan, o modifican opciones. Este año no fue la excepción y se hace una pequeña variación en cuanto a la cantidad, pasando de 40 en el 2021 a 39 en el 2021. Así mismo, se agrupan preguntas en relación con los temas para motivar un análisis de datos más nutrido y la adición de nuevas opciones de respuesta de acuerdo con las tendencias existentes.

Hallazgos principales

Demografía

Sectores participantes

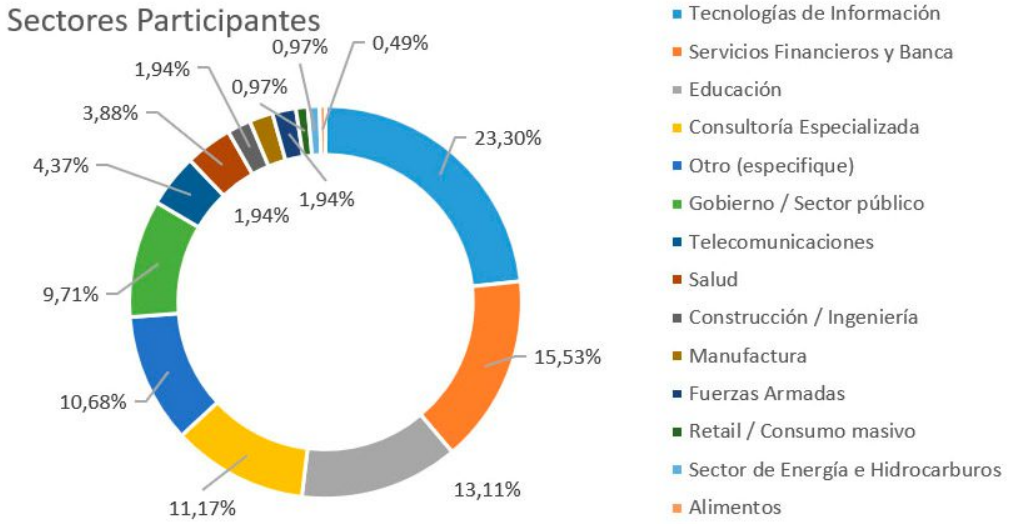
La Figura 1, refleja la participación de 13 sectores de la economía colombiana. Los tres segmentos con mayor participación de la encuesta para este año fueron Sector de Tecnología, Financieros, Educación y Consultoría especializada los más representativos en participación.

La figura 2, muestra el tamaño de las empresas en Colombia, de acuerdo con el número de empleados y se puede observar la participación de empresas de todos los tamaños y cómo la ciberseguridad ha impactado sus operaciones.

La Figura 3, muestra los cargos de los encuestados, entre los que se cuentan oficiales de Seguridad de la información, profesionales del de partamento de seguridad, asesor y consultor externo auditores internos.

Figura 1

Sectores participantes



En la categoría de otros se encuentran a un variado universo de profesionales, entre otras están docentes universitarios, ingenieros del sector de la industria de TI, y algunos otros profesionales de ciberseguridad que no se identifican con las categorías de cargos que contiene la encuesta. Es importante considerar que existe una gran gama de roles que responden la encuesta y dan sus distintas visiones

Figura 2

Tamaño de las empresas participantes.

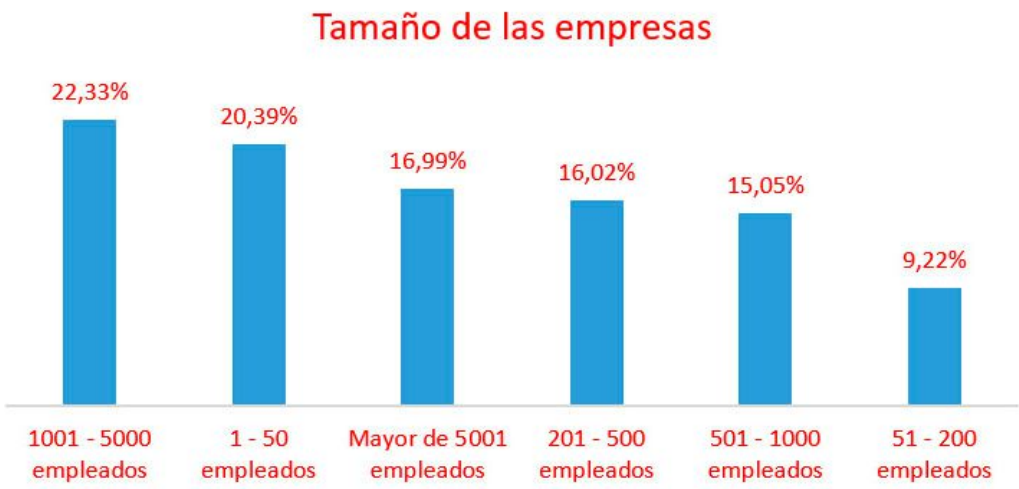
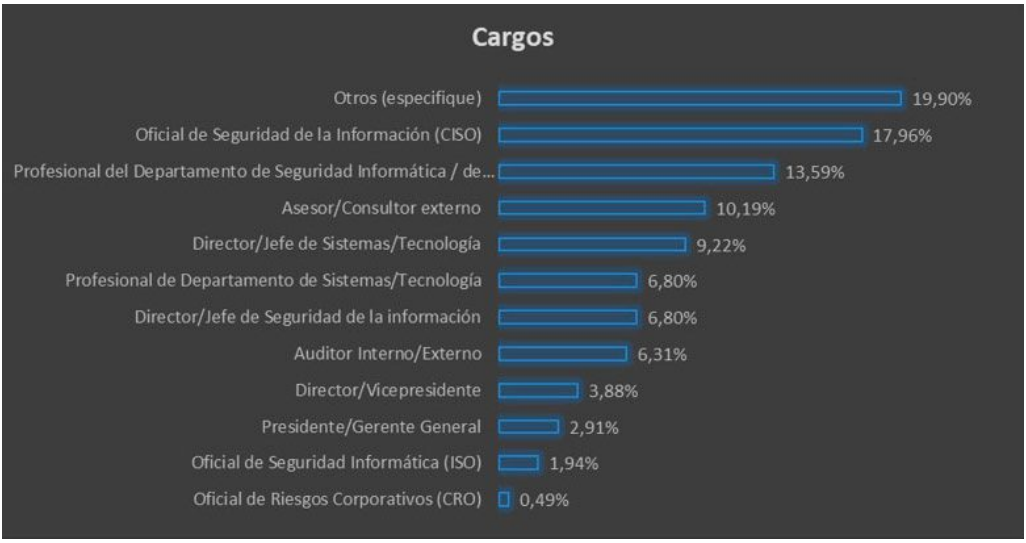


Figura 3

Cargos de los encuestados



acerca de lo que representa la ciberseguridad en sus organizaciones.

La Figura 4, se observan las tareas realizadas por los profesionales de seguridad dentro de las organizaciones. Para este año, el porcentaje más alto está representado por definir controles de TI en materia de seguridad 67%, seguido de establecer e implementar un modelo de políticas 61% y en tercer lugar la creación de programas de entrenamiento en materia de seguridad 57%.

La Figura 5, muestra de quién depende el área de seguridad. Los datos indican que el área de seguridad depende de una dirección propia, Director/Jefe de Seguridad de la Información 31%, seguido por la Vicepresidencia/Director Departamento de Tecnologías de la Información 18% y en tercer lugar del Director/Jefe de Seguridad Informática 12%.

La Figura 6, observan los roles dentro de una organización en materia de seguridad digital. El rol de analista de seguridad de la información es el rol más común que año tras año se manifiesta con un 58%, seguido de la posición CISO u Oficial de Seguridad de la Información 50% y analista de seguridad informática con un 41%.

Consideraciones de los datos

Según las reuniones sostenidas en la agenda global del Foro Económico Mundial en Davos del 2022, en la reunión dentro del foro “Global CyberSecurity Outlook” (WEF, 2022), en el panel se ha expresado

Figura 4

Funciones del responsable de seguridad

Figura 5

Dependencia del área de Seguridad

Figura 6

Roles de Seguridad

que no importa el tamaño de las empresas, todas están expuestas más allá de todos los esfuerzos que se hagan, el adversario digital está al acecho, y se debe adoptar como principio que el ataque va a suceder, desarrollar capacidades, desarrollar cooperación, y entender a la ciberseguridad como un desafío de alta complejidad puede ayudar a abordarlo.

Los roles, la responsabilidad y la visibilidad del profesional de ciberseguridad sigue evolucionando, cada vez se nota su presencia de alguna manera en los distintos niveles de la organización (DarkReading, 2022). En este año al revisar los datos, se puede notar como los distintos sectores de la industria en Colombia tiene la presencia del profesional de seguridad y sus áreas definidas.

Al revisar la distribución de los cargos de los encuestados distribuidos en los sectores de la industria más representativos tenemos que el 22% de los profesionales en todos los sectores son llamados CISOs, siendo el sector financiero 4,24% y el sector de tecnologías de la información 3,64% los que mantienen esa figura. En la misma línea de cargos el 16,97% su cargo es ser profesional del área de seguridad informática o información siendo el sector de las tecnologías de información con un 5,45% el primer lugar y de segundo el sector público con un 3,64%. Al revisar el informe

anual de la Asociación de Control y Auditoría (ISACA) llamado "*State of Cybersecurity 2022*" (ISACA, 2022) se ratifica la tendencia de participación, las industrias o sectores más representativos son la industria de las tecnologías de información 25% y el sector financiero con un 21%. Sectores como el de salud, telecomunicaciones y otros, son sectores que la participación fue realizada por profesionales de las áreas de TI.

En cuanto a los roles y responsabilidades hay una gran variación de lo que hacen los profesionales de seguridad en los distintos sectores de la industria, de tal manera que al revisar el top 3 de funciones o responsabilidades de los principales sectores de la industria se pueden evidenciar en la Tabla 1, en la cual se tiene.

El sector de las tecnologías de la información sus tareas principales están centradas en Definir el programa de privacidad de la información (32%) y la implementación del programa de protección de datos (31%) con el mismo valor revisar la arquitectura de seguridad de la información (31%). El sector finan-

Tabla

Distribución de responsabilidades por sectores

Valores	Tecnologías de Información	Servicios Financieros y Banca	Otro (especifique)	Gobierno / Sector público	Educación	Consultoría Especializada
Aseguramiento de procesos de la organización	29%	19%	16%	11%	12%	13%
Velar por la protección de la información personal	26%	21%	16%	14%	12%	11%
Supervisar y gestionar los procesos de investigaciones forenses digitales	22%	24%	18%	14%	6%	16%
Seguimiento de prácticas en materia de protección de la privacidad de la información personal	29%	14%	20%	14%	10%	14%
Interacción con las diferentes áreas de negocio	28%	23%	17%	10%	12%	10%
Supervisar procesos de cumplimiento regulatorio en tecnología de información	26%	21%	18%	13%	9%	13%
Informar a la alta gerencia sobre el avance del programa de seguridad de la información	28%	27%	13%	14%	9%	11%
Implementación de controles de TI en materia de seguridad de la información	29%	17%	13%	12%	19%	9%
Gestionar el programa de gestión de incidentes de seguridad de la información	23%	19%	13%	17%	16%	12%
Evaluar la eficiencia y efectividad del modelo de seguridad de la información	27%	21%	14%	14%	10%	15%
Seguimiento de prácticas en materia de seguridad de la información	29%	18%	18%	14%	11%	10%
Establecer y revisar la arquitectura de seguridad de la información	31%	16%	15%	14%	11%	13%
Establecer e implementar un modelo de políticas en materia de seguridad de la información	28%	20%	15%	13%	11%	13%
Dirigir y supervisar los programas de riesgos de seguridad de la información de la organización	29%	21%	16%	12%	9%	12%
Definir o diseñar escenarios/simulaciones/Playbooks en relación con ciberriesgos	30%	28%	11%	15%	8%	8%
Definir, implementar y asegurar la estrategia de ciberseguridad de la empresa	27%	21%	15%	13%	11%	14%
Definir programas de resililencia digital	23%	19%	21%	19%	9%	9%
Definir, implementar y asegurar el programa de protección de datos personales de la empresa	31%	20%	13%	13%	11%	11%
Definir, diseñar y velar por el programa de privacidad de la información de la organización	32%	18%	11%	15%	13%	12%
Definición de controles de TI en materia de seguridad de la información	26%	21%	15%	11%	14%	12%
Creación de programas de entrenamiento en materia de seguridad de la información	27%	21%	16%	12%	12%	13%
Creación de programas de gobierno y gestión en materia de seguridad de la información	27%	19%	16%	11%	11%	16%

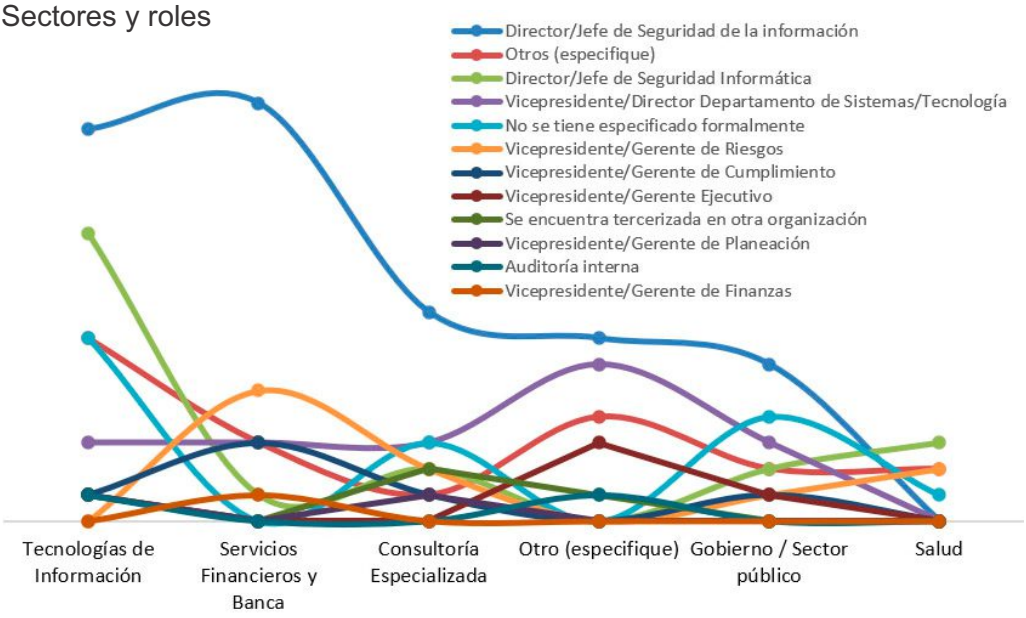
ciero por su parte su principal tarea basado en los resultados es el diseño de los playbooks en relación con los Ciberriesgos (28%), informar a la alta gerencia sobre el avance del programa de seguridad (27%) y supervisar los programas de investigaciones forenses digitales (24%). El sector gobierno está enfocado en definir el programa de resiliencia digital (19%), el programa de gestión de incidentes (17%) y el programa de privacidad de la información (15%). El sector de salud está enfocado en la implementación de controles de TI para seguridad (19%), seguido por la gestión de incidentes (16%) y definir controles de TI para seguridad (14%). El sector de la consultoría está centrado en la creación de los programas de gobierno y gestión en materia de seguridad (16%), supervisión de los procesos de investigaciones forenses (16%) y por último evaluar la efectividad y eficiencia del modelo de seguridad (15%).

Lo anterior muestra que cada sector de la industria está enfocando sus esfuerzos de acuerdo con sus niveles de madurez y la forma en como han evolucionado, ejemplo de esta afirmación es el caso del sector salud, que junto con el sector educación han sido los dos sectores que más han sido afectados durante el 2021 como lo mencionan informes de la industria (IBM, 2022).

Han pasado 2 años desde que el mundo cambió significativamente, el trabajo remoto llegó para quedarse y esa realidad se ha plasmado en la vida de los profesionales

Figura 7

Sectores y roles



de seguridad de la información, ciberseguridad y privacidad, que le ha traído nuevos desafíos frente a la protección, la educación y los aprendizajes de la ciberseguridad.

La dependencia de la ciberseguridad en las organizaciones es otro de los elementos claves, en Colombia existen una variedad de representaciones de acuerdo con los sectores de la industria y su madurez. La Figura 7, muestra la distribución de los cargos en los distintos sectores de mayor representación, en primera instancia a excepción del sector Salud, todos los sectores muestran la figura de un director de seguridad como su principal figura, casos como el sector de tecnologías de la información con un 4.58% de representación que no tienen formalmente definido un rol ni una dependencia, el 3.27% la dependencia de la seguridad está en la figura del gerente de riesgos.

Las organizaciones que tienen la figura o posición de la función de la seguridad dependiendo de un director, muestran grandes avances en el desarrollo de las posturas de seguridad, esto puede ser el piso de apoyo para poder llegar a las instancias directivas y ejecutivas de las organizaciones y por tanto tener mayor visibilidad, en esa misma línea por tanto el rol del profesional líder de seguridad, así como la función debe transformarse (Fortinet, 2022; DarkReading, 2022).

Por tanto, en Colombia los datos para el año 2022 muestran alineación con las tendencias internacionales en relación a cómo la función de seguridad sigue su camino y

Figura 8

Presupuesto de Seguridad

procesos de aprendizaje, cómo avanza su evolución con mayor énfasis en algunos sectores que en otros, donde cada uno de ellos tiene su propio nivel de aprendizaje. El desafío estará en qué tan rápido se avanza para que los retos en materia de protección digital no tomen más ventaja de la que ya existe.

Presupuestos

Continúa la asignación de presupuestos para la ciberseguridad; en esta oportunidad el 83% manifiesta tener asignado un presupuesto de seguridad en la organización que se puede ver en La Figura 8.

La Figura 9, muestra el porcentaje que representa el presupuesto para la ciberseguridad del total del presupuesto de la organización. Cerca del 50% de los encuestados lo conoce, mientras que el otro 50% dice no conocer o no tener la información. De quienes conocen los montos asignados se puede observar que los montos inferiores al 5% del presupuesto global de la compañía representan el 32%, mientras que el 15% están para los montos superiores al 5%. Entre el 0 y 2% representa un 15% mientras que entre 3 y el 5% representa el 16%, 8,6% es más del 11%, 5% está entre el 6 y 8% y entre el 9 y 11% es el 3,7%.

La Figura 10, refleja los montos asignados en las organizaciones para la ciber-seguridad. Para este año cerca del 47% tiene un monto asignado para la seguridad; que aumenta, comparado con el año pasado cerca de un 3%, por su parte el 53% dice no conocer

Figura 9

Porcentaje del presupuesto Global

Figura 10

Presupuesto de Seguridad

cuánto es el presupuesto asignado para la ciber-seguridad. Al revisar los datos, el 17% dice que asigna un presupuesto mayor a $US 130.000 dólares americanos, seguido del aquellos que asignan menos de $US 20.000 y que representa casi el 11%, seguido de aquellos que asignan entre $US 20.000 y $US 50.000 (9%), casi el 4% asigna entre $US 90.000 y $US 110.000.

La Figura 11, muestra la forma cómo se está invirtiendo el dinero en materia de ciberseguridad. Sigue creciendo la inversión en tecnologías de seguridad informática. Renovación de licenciamiento, servicios de monitoreo, capacitación del

Figura 11

Inversión de Seguridad

profesional de seguridad y contratación de consultoría y auditoría.

Consideraciones de los datos

En la Tabla 2, se muestra la distribución de sectores, montos de inversión y tipos de inversiones, de lo que se puede definir lo siguiente. El sector de la consultoría especializada centra las inversiones en la capacitación del personal de seguridad con inversiones menores de los $US20.000 como su valor más alto, sin embargo, también tiene algunas inversiones en el rango de los $US20.000 a los $US50.000. El segundo frente de inversión es la Adquisición de tecnologías de seguridad informática, que no excede

Tabla 2

Distribución de presupuestos

	Menor de USD$20.000	Más de USD$130.001	Entre USD$90.001 y USD$110.000	Entre USD$70.001 y USD$90.000	Entre USD$50.001 y USD$70.000	Entre USD$20.001 y USD$50.000	Entre USD$110.001 y USD$130.000
Consultoría Especializada							
Contratación de servicios de asesoría/consultoría	3,6%	0,0%	0,0%	0,0%	3,6%	3,6%	0,0%
Adquisición e implementación de tecnología de seguridad informática	4,8%	0,0%	0,0%	0,0%	2,4%	4,8%	0,0%
Renovación de licenciamiento y mantenimiento de hardware y software	2,5%	0,0%	0,0%	0,0%	2,5%	2,5%	0,0%
Capacitación/Actualización del personal de seguridad de la información	10,7%	0,0%	0,0%	0,0%	0,0%	3,6%	0,0%
Servicios de monitoreo y gestión de seguridad con terceros	0,0%	0,0%	0,0%	0,0%	2,9%	2,9%	0,0%
Educación							
Contratación de servicios de asesoría/consultoría	0,0%	0,0%	7,1%	0,0%	0,0%	3,6%	3,6%
Adquisición e implementación de tecnología de seguridad informática	2,4%	2,4%	2,4%	0,0%	0,0%	2,4%	2,4%
Renovación de licenciamiento y mantenimiento de hardware y software	5,0%	2,5%	2,5%	0,0%	0,0%	0,0%	2,5%
Capacitación/Actualización del personal de seguridad de la información	0,0%	0,0%	0,0%	0,0%	0,0%	0,0%	0,0%
Servicios de monitoreo y gestión de seguridad con terceros	0,0%	2,9%	2,9%	0,0%	0,0%	2,9%	2,9%
Gobierno / Sector público							
Contratación de servicios de asesoría/consultoría	3,6%	3,6%	3,6%	3,6%	0,0%	3,6%	0,0%
Adquisición e implementación de tecnología de seguridad informática	0,0%	4,8%	2,4%	2,4%	0,0%	4,8%	0,0%
Renovación de licenciamiento y mantenimiento de hardware y software	2,5%	7,5%	2,5%	2,5%	0,0%	5,0%	0,0%
Capacitación/Actualización del personal de seguridad de la información	0,0%	10,7%	3,6%	0,0%	0,0%	3,6%	0,0%
Servicios de monitoreo y gestión de seguridad con terceros	0,0%	5,7%	2,9%	2,9%	0,0%	0,0%	0,0%
Salud							
Contratación de servicios de asesoría/consultoría	0,0%	0,0%	0,0%	0,0%	0,0%	0,0%	0,0%
Adquisición e implementación de tecnología de seguridad informática	2,4%	0,0%	0,0%	2,4%	0,0%	0,0%	0,0%
Renovación de licenciamiento y mantenimiento de hardware y software	2,5%	0,0%	0,0%	2,5%	0,0%	0,0%	0,0%
Capacitación/Actualización del personal de seguridad de la información	0,0%	0,0%	0,0%	0,0%	0,0%	0,0%	0,0%
Servicios de monitoreo y gestión de seguridad con terceros	2,9%	0,0%	0,0%	0,0%	0,0%	0,0%	0,0%
Servicios Financieros y Banca							
Contratación de servicios de asesoría/consultoría	3,6%	28,6%	0,0%	3,6%	0,0%	3,6%	3,6%
Adquisición e implementación de tecnología de seguridad informática	0,0%	21,4%	0,0%	0,0%	2,4%	2,4%	2,4%
Renovación de licenciamiento y mantenimiento de hardware y software	0,0%	17,5%	0,0%	2,5%	2,5%	2,5%	2,5%
Capacitación/Actualización del personal de seguridad de la información	0,0%	21,4%	0,0%	0,0%	3,6%	0,0%	3,6%
Servicios de monitoreo y gestión de seguridad con terceros	0,0%	28,6%	0,0%	2,9%	2,9%	0,0%	2,9%
Tecnologías de Información							
Contratación de servicios de asesoría/consultoría	0,0%	7,1%	0,0%	0,0%	0,0%	3,6%	3,6%
Adquisición e implementación de tecnología de seguridad informática	11,9%	9,5%	0,0%	0,0%	2,4%	2,4%	2,4%
Renovación de licenciamiento y mantenimiento de hardware y software	10,0%	10,0%	2,5%	0,0%	2,5%	2,5%	0,0%
Capacitación/Actualización del personal de seguridad de la información	14,3%	14,3%	3,6%	0,0%	3,6%	0,0%	3,6%
Servicios de monitoreo y gestión de seguridad con terceros	11,4%	11,4%	2,9%	0,0%	2,9%	0,0%	2,9%

en todo caso los $US50.000 dólares americanos.

El sector de la educación tiene un comportamiento distinto, la consultoría es donde hay más concentración de la inversión y sobre todo entre los $US90.000 y los $110.000 dólares, otras franjas tienen valores importantes. El segundo frente de inversiones es el de renovación de licenciamiento que su valor mayor de inversión está por debajo de los $US20.000 dólares americanos, aunque también tiene inversiones por encima de los $US 130.000.

El sector del gobierno por su parte tiene elementos interesantes para revisar, se concentra en capacitar a las personas de las áreas de seguridad con inversiones por encima de los $US130.000 dólares, sigue la renovación del licenciamiento y los servicios de monitoreo y gestión de seguridad por terceros en la misma franja de montos asignados.

El sector salud de otro lado asigna menos de $US20.000 dólares en primera instancia para el monitoreo, y como segundo lugar la renovación de licenciamiento que está en la misma franja, así como también se asignan recursos económicos para este rubro en la franja de los $US70.000 al $US90.000 dólares americanos.

El sector financiero, ratifica la tendencia global, se invierte y es el que más invierte todos los elementos analizados su rango de inversión están por encima de los $US 130.000, que además se confirma a través de los distintos reportes de industria (Verizon, 2022).

En el sector de las tecnologías de la información se muestra que se está capacitando a las personas dedicadas a la seguridad en dos de los rangos, por un lado, se invierte en la franja menor de $US20.000, así como en la franja de $US130.000 dólares americanos, la adquisición de tecnologías es el segundo rubro en importancia donde se hace inversiones, sin embargo, estas están en la franja por debajo de los $US 20.000 dólares.

Invertir en la ciberseguridad es importante, sin embargo, los datos de Colombia empiezan a mostrar que no solo es necesario, también es bueno empezar a hacer inversiones de manera razonable y que estén acordes con la realidad de las organizaciones (CyberEdge, 2022).

Hoy por hoy en Colombia se confirma que las organizaciones están asignando presupuesto, aun así, sigue siendo algo para observar porqué los profesionales de seguridad manifiestan no conocer cuánto es el presupuesto asignado, montos, y sobre todo los valores, esto puede obedecer a que sean presupuestos compartidos con las áreas de tecnologías de la información o el rol del profesional de seguridad que diligencia la encues-

ta no tenga acceso a dicha información.

En Colombia en todos los tamaños de las empresas se invierte en ciberseguridad, está claro que las empresas grandes en el rango de 1000 a 5000 empleados invierten más (22%), sin embargo, las empresas pequeñas de 1 a 50 empleados ocupan el segundo lugar (21%), las empresas de más de 5000 empleados ocupan el tercer lugar (17%), seguido de las empresas de 201 a 500 empleados (16%), luego de 501 a 1000 (15%) y por último las de 51 a 200 empleados (9%). Tendencia que se ratifica a través de informes de industria (CyberEge, 2022).

El porcentaje de asignación de presupuesto con respecto al presupuesto global de la organización sigue siendo bajo al revisar las franjas dominantes, que se ratifican como tendencia que se ven en reportes de industria que sugiere que 8 de cada 10 empresas tienen un presupuesto menos del 10% del presupuesto de la organización (DarkReading, 2022).

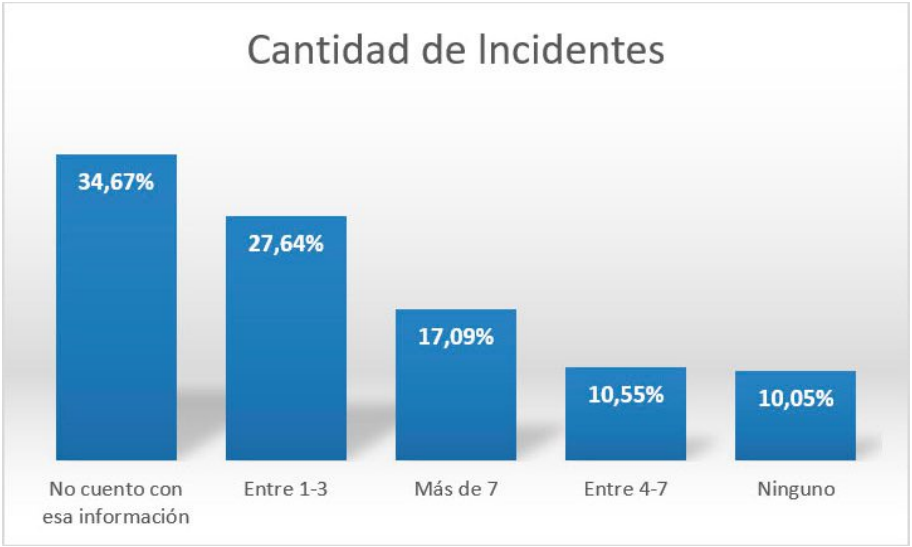
Si bien hoy por hoy es indispensable el presupuesto de seguridad, no es el único factor y en términos generales se ve de manera optimista la asignación del presupuesto para la ciberseguridad (ISACA, 2022). En reportes de industria se reitera esta tendencia, que en Colombia sigue evolucionando y sigue mejorando año tras año.

Incidentes

La Figura 12, muestra la cantidad de incidentes que se presentan en

Figura 12

Cantidad de Incidentes



Colombia, según los participantes. Para este año cerca del 56% de los encuestados manifiesta que ha estado en contacto con algún incidente de seguridad en su empresa, en comparación con el año inmediatamente anterior, donde el 72% lo ha manifestado. El 33% manifiesta no tener información al respecto de los incidentes en sus organizaciones, el 28% manifiesta haber experimentado entre 1 y 3 incidentes, el 17% comenta que ha experimentado más de 7 incidentes, cerca del 11% informa que ha experimentado entre 4 a 7 incidentes, y solo el 10% señala que no ha experimentado ningún incidente.

La Figura 13, relaciona los tipos de incidentes que se presentaron en las organizaciones, Errores humanos (38%), Phishing (32%) y los ataques de ingeniería social (25%) son las tres primeras posiciones del listado.

La figura 14, representa el costo promedio de los incidentes, el 87% manifiesta que los costos estimados totales luego de sufrir un incidente están por debajo de los

Figura 13

Tipos de Incidentes de Seguridad

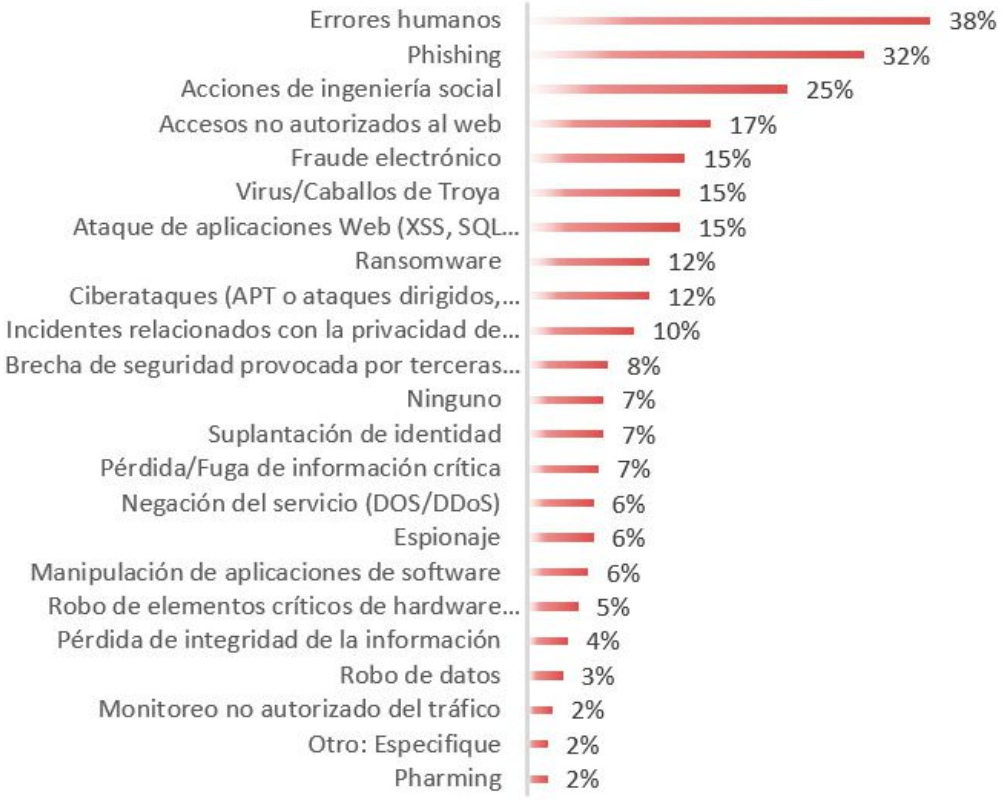
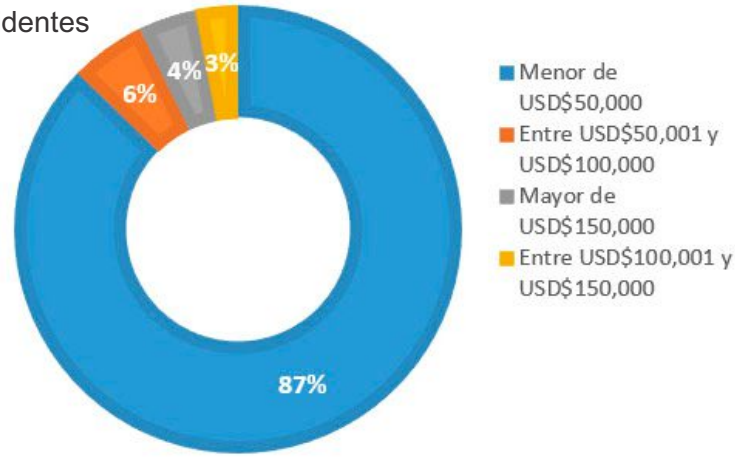


Figura 14

Costos de los Incidentes



$US50.000 dólares americanos, entre $US50.000 y $US100.000 solo el 6%, más de $US150.000 el 4% y entre $US100.000 y $US-150.000 dólares americanos el 3%.

La Figura 15, muestra ante quién se reportan los incidentes de seguridad.

El 61% lo reporta directamente a los directivos de la organización, el 47% lo reporta al equipo de atención de incidentes (CSIRT), el 33% a las autoridades nacionales, el 23% a los asesores legales, el 15% a autoridades locales o regionales y solo el 5% manifiesta que no se denuncian.

Figura 15

A quién se reportan los incidentes

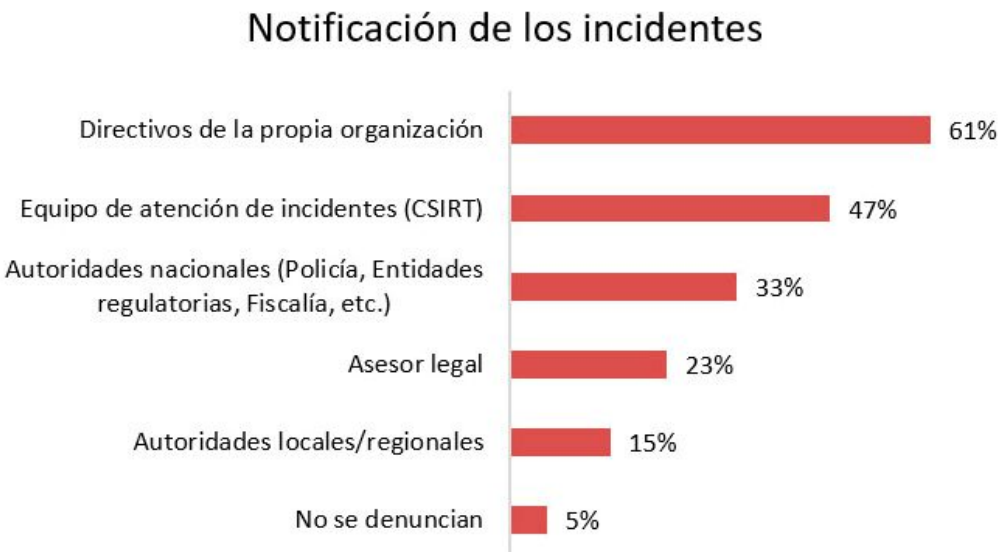


Figura 16

Razones para no denunciar los incidentes

La Figura 16, muestra como los profesionales de ciberseguridad se mantienen informados sobre las vulnerabilidades y fallas de los sistemas. El 55% de los profesionales de seguridad se enteran o están conectados con CSIRTs, el 54% se notifican de su relación con sus proveedores, la lectura de revistas especializadas es la tercera fuente 52%, el 48% se notifica a través de colegas, el 38% lee listas de seguridad, y solo el 7% no tiene ese hábito.

La Tabla 3, se resalta que el 63% de las personas encuestadas si tienen contacto con las autoridades, mientras que el 37% no lo posee.

En cuanto la evidencia digital, los datos muestran que, 81% de los

Tabla 3

Contacto con autoridades

Contacto con autoridades	Porcentaje
No	37,10%
Si	62,90%

Contacto con autoridades	Porcentaje
No	37,10%
Si	62,90%

encuestados si es consciente del manejo de la evidencia digital y que es requerida como parte del proceso de la gestión de incidentes, el 55% no posee un procedimiento formal para la gestión de incidentes, el 44% afirma si tenerlo, solo el 38% ha implementado el procedimiento de gestión de evidencia digital, que dicen tener formalmente definido.

Consideraciones de los datos

Explorando la forma en como en Colombia los distintos sectores de la industria experimentan los distintos incidentes, y en que invierten sus recursos financieros asignados de presupuesto a los desafíos que presenta la ciber-seguridad, la Tabla 4, resalta la cantidad de incidentes que se presentan en los diferentes sectores de industria y adicional los relaciona por el tamaño de la empresa.

Lo que se puede ver en primera instancia es que, en todos los sectores a excepción del sector financiero, las empresas manifiestan que han podido identificar que sufren de 1 a 3 incidentes, resulta de interés que en el global del sector financiero es ningún incidente el mayor valor.

Llama la atención que el sector salud y el sector educación no solo tienen en la franja de 1 a 3 incidentes, su segundo valor más de 7 para el sector educación y entre 4 y 7 para el sector salud, esto confirma la tendencia global que se ha venido experimentando de ser los sectores hoy más apetecidos en la industria por parte del adversario digital como lo menciona IBM en su informe reciente (IBM,2022).

Tabla 4

Distribución de incidentes de seguridad por sectores y tamaños de industria

	Entre 1-3	Más de 7	Ninguno	Entre 4-7
Consultoría Especializada	**4,35%**	**1,74%**	**3,48%**	**0,87%**
1 - 50 empleados	3,48%	0,87%	2,61%	0,00%
201 - 500 empleados	0,00%	0,00%	0,87%	0,87%
Mayor de 5001 empleados	0,00%	0,87%	0,00%	0,00%
51 - 200 empleados	0,87%	0,00%	0,00%	0,00%
Educación	**4,35%**	**2,61%**	**1,74%**	**1,74%**
201 - 500 empleados	1,74%	0,00%	0,87%	0,87%
Mayor de 5001 empleados	1,74%	1,74%	0,00%	0,00%

501 - 1000 empleados	0,87%	0,87%	0,00%	0,87%
51 - 200 empleados	0,00%	0,00%	0,87%	0,00%
Gobierno / Sector público	**6,09%**	**2,61%**	**1,74%**	**2,61%**
1001 - 5000 empleados	2,61%	0,87%	0,00%	1,74%
501 - 1000 empleados	0,87%	0,87%	1,74%	0,00%
Mayor de 5001 empleados	0,87%	0,87%	0,00%	0,87%
201 - 500 empleados	0,87%	0,00%	0,00%	0,00%
51 - 200 empleados	0,87%	0,00%	0,00%	0,00%
Otro (especifique)	**9,57%**	**6,09%**	**0,00%**	**0,87%**
201 - 500 empleados	1,74%	1,74%	0,00%	0,87%
Mayor de 5001 empleados	1,74%	1,74%	0,00%	0,00%
1001 - 5000 empleados	1,74%	0,87%	0,00%	0,00%
1 - 50 empleados	1,74%	0,87%	0,00%	0,00%
501 - 1000 empleados	2,61%	0,00%	0,00%	0,00%
51 - 200 empleados	0,00%	0,87%	0,00%	0,00%
Salud	**1,74%**	**0,00%**	**0,00%**	**1,74%**
501 - 1000 empleados	0,87%	0,00%	0,00%	0,87%
51 - 200 empleados	0,00%	0,00%	0,00%	0,87%
1001 - 5000 empleados	0,87%	0,00%	0,00%	0,00%
Servicios Financieros y Banca	**2,61%**	**4,35%**	**5,22%**	**2,61%**
1001 - 5000 empleados	1,74%	0,87%	1,74%	0,87%
Mayor de 5001 empleados	0,00%	0,87%	1,74%	1,74%
501 - 1000 empleados	0,00%	2,61%	0,00%	0,00%
201 - 500 empleados	0,00%	0,00%	1,74%	0,00%
51 - 200 empleados	0,87%	0,00%	0,00%	0,00%
Tecnologías de Información	**13,91%**	**7,83%**	**4,35%**	**5,22%**
1 - 50 empleados	6,09%	3,48%	2,61%	0,87%
201 - 500 empleados	4,35%	2,61%	0,00%	1,74%
1001 - 5000 empleados	2,61%	0,87%	0,87%	0,00%
51 - 200 empleados	0,87%	0,00%	0,87%	1,74%
Mayor de 5001 empleados	0,00%	0,87%	0,00%	0,87%

Al explorar por tamaños de las empresas y el comportamiento de este podemos encontrar los siguientes datos.

En las empresas de 1 a 50 empleados, los sectores de consultoría especializada y tecnologías de la información son los que predominan en la franja de 1 a 3 incidentes, sin embargo, el sector de tecnología su segundo reglón son la presencia de más de 7 incidentes, tendencia que se ratifica a través del informe de Verizon y CiberEdge (Verizon, 2022; CyberEdge, 2022).

En las empresas de 201 a 500 empleados, son los sectores de la educación y de las tecnologías quienes evidencia la presencia mayor de 1 a 3 incidentes en sus ambientes.

En las empresas de 1000 a 5000 empleados, es el sector de las tecnologías de información, gobierno y el sector salud los que manifiestan los valores más altos de presencia de incidentes en la banda de 1 a 3 incidentes.

Las empresas de más de 5000 empleados, es el sector educación quien está en la primera posición al manifestar la presencia de incidentes de seguridad en sus ambientes operacionales.

Para las empresas de 500 a 1000 empleados, es donde el sector financiero manifiesta que ha experimentado más de 7 incidentes en sus ambientes operacionales.

Por último, en la banda de las 50 a 200 empleados, es el sector de las tecnologías de la información el que ha experimentado incidentes entre 4 a 7 incidentes en sus infraestructuras tecnológicas.

Todos los datos apuntan a sostener la idea que el adversario está atento a todos los sectores, tamaños de la industria. Se observa según los datos que el sector financiero no es el primer sector objetivo por el adversario, explicado por la madurez del sector que entiende el adversario y que prefiere atacar a otros sectores como el de salud, educación, tecnologías inclusive o gobierno como primeras líneas (CyberEdge, 2022; Fireeye, 2022).

En relación con la forma en como los distintos eventos se presentan en las empresas colombianas se puede visualizar en la Tabla 5.

Errores humanos, Phishing y Ataques de Ingeniería Social, son marcados incidentes que suceden en todos los sectores de la industria, sin embargo, en el sector financiero donde los errores humanos no ocupan el primer lugar, lo ocupa el Phishing que es un flagelo que se mantiene como tendencia significativamente importante (Barracuda, 2022; Zscaler, 2022).

Los errores humanos son un desafío de las empresas, no solo porque se requiere el entrenamiento de las personas de manera permanente y consistente, adicional porque es un

Tabla 5

Distribución de los incidentes de seguridad en los sectores de la industria

Valores	Alimentos	Construcción / Ingeniería	Consultoría Especializada	Educación	Fuerzas Armadas	Gobierno / Sector público	Manufactura	Otro (especifique)	Retail / Consumo masivo	Salud	Sector de Energía e Hidrocarburos	Servicios Financieros y Banca	Tecnologías de Información	Telecomunicaciones
Ninguno	0%	20%	5%	2%	6%	2%	0%	0%	0%	6%	0%	5%	2%	13%
Accesos no autorizados al web	6%	20%	6%	9%	11%	9%	7%	4%	0%	6%	0%	4%	9%	0%
Otro: Especifique	0%	0%	2%	0%	0%	2%	0%	1%	0%	0%	0%	0%	1%	0%
Virus/Caballos de Troya	0%	20%	2%	2%	11%	7%	7%	9%	0%	6%	0%	4%	8%	0%
Robo de elementos críticos de hardware (notebooks, discos, etc.)	0%	0%	3%	4%	6%	0%	4%	1%	20%	0%	17%	0%	1%	0%
Robo de datos	0%	0%	3%	2%	6%	0%	4%	1%	0%	0%	0%	0%	1%	0%
Ransomware	0%	0%	2%	9%	6%	5%	7%	4%	0%	12%	0%	0%	6%	7%
Pharming	6%	0%	3%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	7%
Phishing	6%	0%	14%	19%	6%	10%	11%	13%	20%	6%	33%	15%	10%	20%
Pérdida/Fuga de información crítica	6%	0%	2%	4%	0%	2%	11%	1%	0%	6%	0%	4%	2%	0%
Suplantación de identidad	0%	0%	2%	0%	6%	3%	7%	3%	0%	0%	0%	4%	3%	7%
Manipulación de aplicaciones de software	6%	0%	5%	0%	6%	2%	0%	3%	0%	0%	0%	2%	2%	0%
Negación del servicio (DOS/DDoS)	6%	0%	5%	2%	0%	2%	0%	0%	0%	0%	0%	7%	2%	0%
Espionaje	6%	0%	3%	0%	6%	3%	0%	3%	0%	0%	0%	2%	2%	7%
Incidentes relacionados con la privacidad de los datos personales (publicación de información personal, solicitudes de eliminación de datos personales, etc.)	6%	0%	6%	2%	0%	5%	0%	9%	0%	0%	0%	4%	2%	7%
Fraude electrónico	6%	0%	2%	11%	6%	0%	11%	7%	20%	6%	0%	9%	6%	7%
Errores humanos	6%	40%	6%	13%	11%	19%	15%	24%	20%	24%	17%	7%	15%	20%
Ciberataques (APT o ataques dirigidos, denegación de servicios masiva)	6%	0%	6%	2%	6%	5%	0%	4%	0%	6%	0%	5%	6%	0%
Brecha de seguridad provocada por terceras partes (p.e Cloud Access Security Broker)	6%	0%	5%	0%	0%	2%	0%	1%	0%	0%	17%	5%	5%	0%
Ataque de aplicaciones Web (XSS, SQL Injection, Directory Transversal, etc.)	6%	0%	6%	6%	0%	5%	4%	3%	0%	6%	0%	11%	7%	0%
Acciones de ingeniería social	6%	0%	8%	13%	11%	16%	11%	7%	20%	6%	17%	11%	8%	7%
Monitoreo no autorizado del tráfico	6%	0%	2%	0%	0%	0%	0%	0%	0%	0%	0%	0%	2%	0%
Pérdida de integridad de la información	6%	0%	3%	0%	0%	2%	0%	0%	0%	12%	0%	2%	1%	0%

frente que el adversario ha entendido que puede ser un vector que se expande y permite diseminar otras formas de ataques, ejemplo Ransomware, Phishing, ataques de cadena de suministro, distribución de malware, creación de personas como *insiders*, entre otros (Proofpoint, 2022; FS-ISAC, 2022).

Datos interesantes, el sector de manufactura relaciona la pérdida/fuga de información y el fraude electrónico son su segunda fuente de incidentes de seguridad, el sector de hidrocarburos y energía ve al robo de elementos críticos, y las brechas de terceras partes como fuentes importantes de incidentes en sus ambientes, en el sector de Tecnologías, así como en otros sectores, el acceso no autorizado a aplicaciones es una fuente importante de presencia de incidentes en las empresas de Colombia, la clara tendencia de que el Ransomware está afectando a sectores de la educación y la salud (TrendMicro, 2022; FBI,2022; Keeper, 2022).

Los incidentes de manera general los costos totales estimados están por debajo de los $US50.000, tendencia que se aleja de los informes de industria como el de IBM (IBM, 2022), hay puntos que se resaltan sobre los incidentes y sus costos, por ejemplo el robo de datos, y el Pharming estuvieron en la franja de los $US50.000 a $US100.000, por encima de los $US150.000 robo de datos, Pharming, Denegación de servicio, pérdida o fuga de información crítica, ransomware, robo de elementos críticos y suplantación de identidad, caso que si se adhiere a la tendencia global en relación con el costos del Ransomware y las Denegaciones de servicio, que son los incidentes con costos muy elevados.

La fortaleza de un proceso de gestión de incidentes no solo radica en tener herramientas o personas, es importante la evidencia digital como fundamento, por tanto, manejar, gestionar, e implementar los procesos relacionados con este componente. La tendencia se confirma a través del informa de CyberEdge Group, que manifiesta que el 13% de los encuestados no considera usar alguna solución de esta naturaleza, el resto o ya las tiene en uso, o planea usarlas (CyberEdge, 2022).

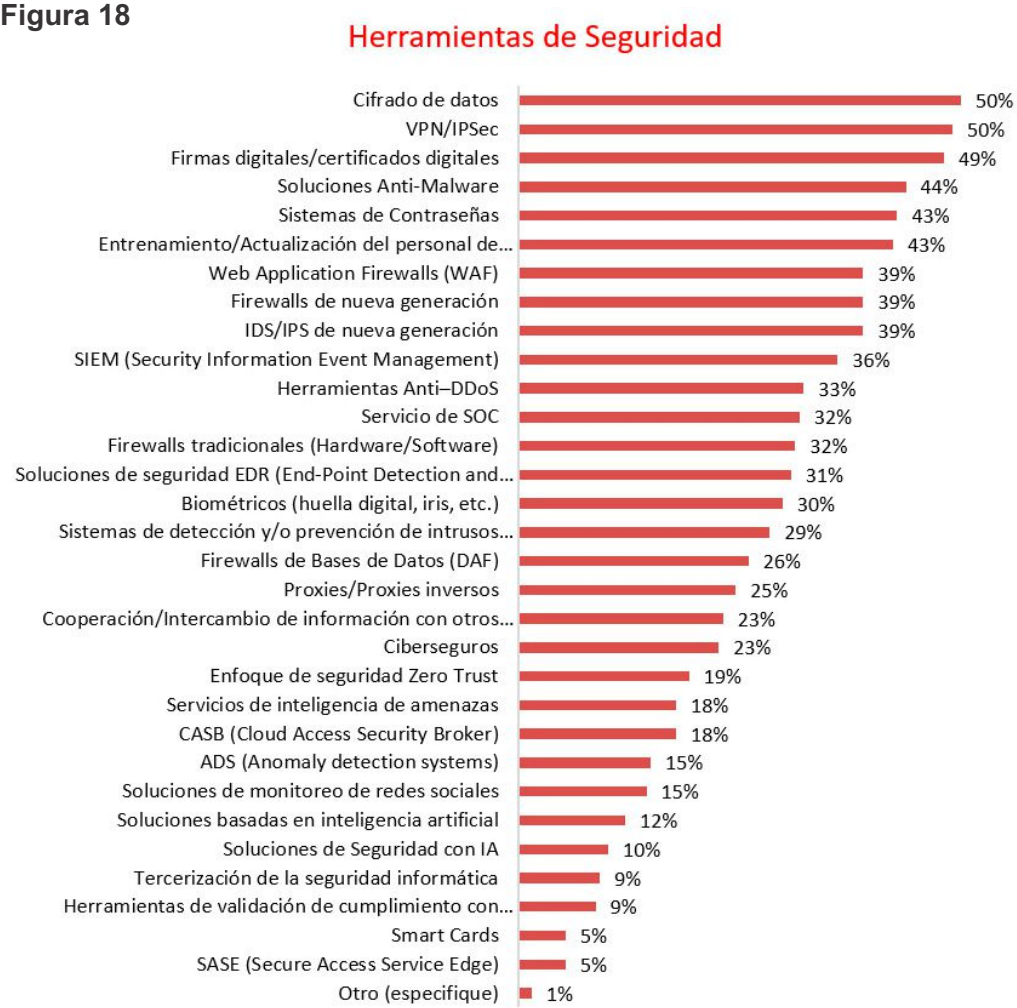
Herramientas

La Figura 17, muestra el comportamiento de la práctica de la frecuencia con que se evalúa la postura de seguridad en la organización. El 36% manifiesta que se hace una vez al año, el 32% afirma que la hace entre 2 y 4 veces al año, más de 4 veces al año lo relaciona el 19% y ninguna evaluación 13%.

La Figura 18, muestra la distribución del uso de las herramientas de seguridad, Cifrado de datos y VPN son las herramientas primariamente usadas con el 50% ambas,

Figura 17

Figura 18



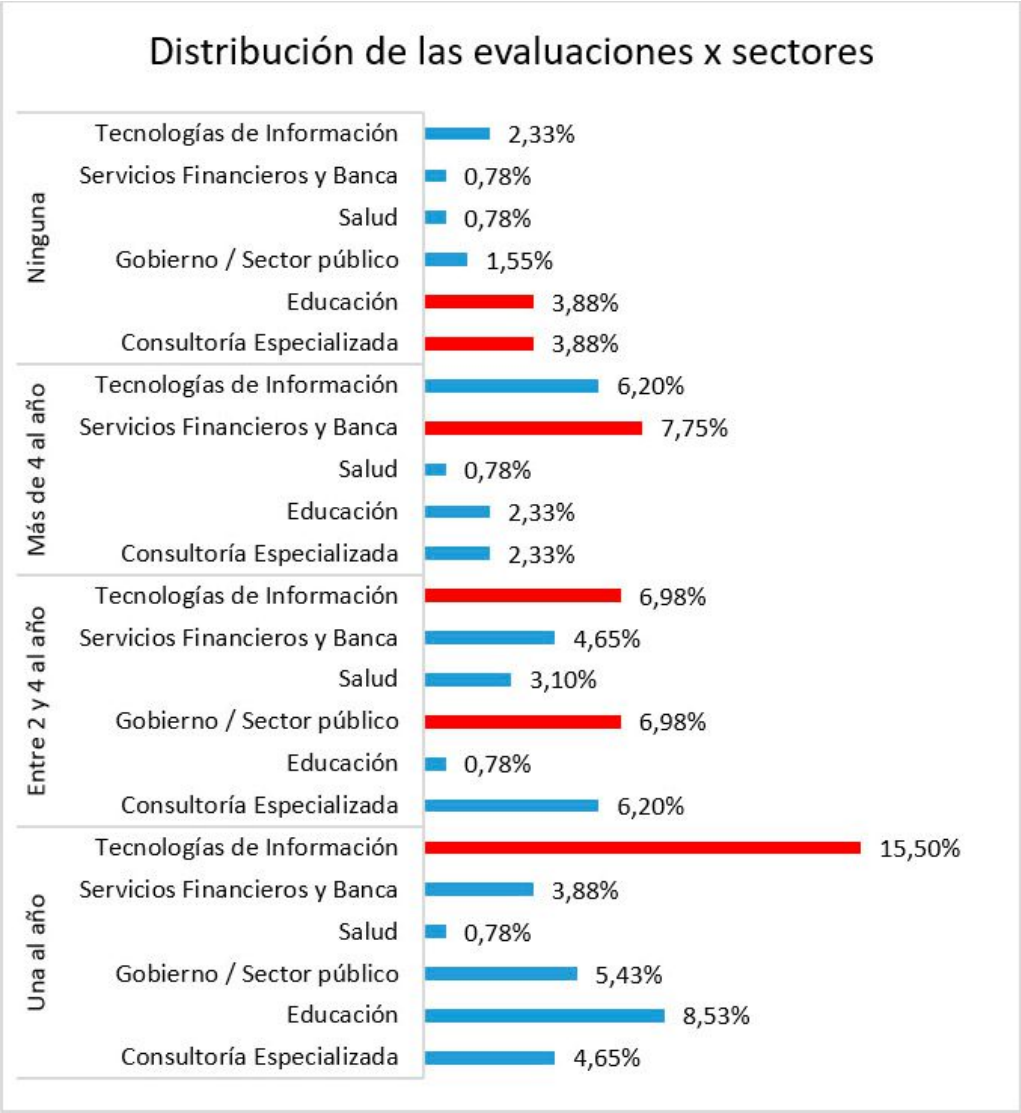
siguen las firmas digitales, soluciones antimalware y los sistemas de contraseña.

Consideraciones de los datos

Al revisar los datos y ver como los distintos sectores de la industria realizan la valoración de la postura de seguridad, está reflejado en la Figura 19, que muestra, los sectores de la educación y la consultoría especializada como valor más importante resalta que no ejecuta ninguna valoración de la postura de seguridad, el sector financiero eje-

Figura 19

Sectores y Evaluaciones de seguridad



cuta más de 4 evaluaciones de seguridad por año, entre 2 y 4 evaluaciones al año el sector de tecnología y gobierno, el sector de tecnología lo hace 1 vez al año.

La industria de manera general resalta la necesidad de realizar los procesos de valoración de la postura de seguridad como mecanismo de dirección y revisión de los trazos y visos definidos a través de las distintas estrategias de seguridad de las empresas.

La medición en términos generales depende mucho de la madurez de las empresas y de sus relaciones con la ciberseguridad, el sector financiero a través de muchos esfuerzos propios y también por las presiones de la regulación, los adversarios y las partes interesados aportan para que estos ejercicios se realicen. Otros sectores como el sector de salud, educación, empiezan a consolidar las valoraciones como ejercicios necesarios e indispensables, que con el paso de los años y de acuerdo con las tendencias internacionales seguirá apuntando a crecer.

Al revisar la forma en como los mecanismos y herramientas de seguridad son usados en los distintos sectores de la industria se visualiza en la Tabla 6. El sector de la consultoría especializada ve a las soluciones de seguridad con IA, las Smart cards y las soluciones basadas en IA, como los principales mecanismos. El sector salud, ve en las Smart cards, los sistemas de detección de anomalías y los proxis los mecanismos más usados. El sector del gobierno ve en las herramientas de validación de cumplimiento con regulaciones internacionales, las firmas digitales y la cooperación e intercambio de información son sus principales mecanismos. El sector de la salud usa la tercerización, las herramientas de validación del cumplimiento y los firewalls de bases de datos como los primeros mecanismos a ser usados. El sector financiero deja claro que el monitoreo de las redes sociales, el cifrado de datos y las soluciones SASE (*Secure Access Service Edge*) ocupan los primeros lugares. El sector de las tecnologías ve en las solucione SASE, las contraseñas y las herramientas sus principales mecanismos de uso.

En el estudio de IBM (IBM, 2022), se resalta que las empresas están tendiendo a usar herramientas de automatización para la seguridad, tales como herramientas de inteligencia artificial y máquinas de aprendizaje, movimiento que también se ve como tendencia de Colombia.

El incremento en soluciones de seguridad orientadas a la red como IDS/IPS, Firewall de nueva generación, soluciones de Data Loss Prevention (DLP), están en los principales rubros de inversión.

En relación con la protección de estaciones de trabajo el mismo infor-

Tabla 6

Distribución de las herramientas de seguridad usadas en los sectores de industria

Valores	Consultoría Especializada	Educación	Gobierno / Sector público	Salud	Servicios Financieros y Banca	Tecnologías de Información
Sistemas de Contraseñas	10,14%	13,04%	13,04%	5,80%	21,74%	36,23%
VPN/IPSec	11,54%	14,10%	17,95%	6,41%	24,36%	25,64%
Web Application Firewalls (WAF)	7,81%	10,94%	21,88%	4,69%	29,69%	25,00%
Tercerización de la seguridad informática	18,18%	18,18%	0,00%	18,18%	36,36%	9,09%
Soluciones de Seguridad con IA	26,67%	6,67%	6,67%	0,00%	26,67%	33,33%
Soluciones de seguridad EDR (End-Point Detection and Response)	15,22%	17,39%	6,52%	2,17%	26,09%	32,61%
Soluciones de monitoreo de redes sociales	4,76%	14,29%	9,52%	4,76%	52,38%	14,29%
Soluciones basadas en inteligencia artificial	23,53%	5,88%	17,65%	0,00%	29,41%	23,53%
Soluciones Anti-Malware	9,86%	12,68%	19,72%	2,82%	21,13%	33,80%
Smart Cards	25,00%	25,00%	12,50%	0,00%	25,00%	12,50%
Sistemas de detección y/o prevención de intrusos IDS/IPS tradicionales	12,77%	12,77%	10,64%	0,00%	31,91%	31,91%
Firewalls de nueva generación	14,06%	12,50%	17,19%	3,13%	23,44%	29,69%
SIEM (Security Information Event Management)	12,07%	8,62%	20,69%	3,45%	25,86%	29,31%
Servicios de inteligencia de amenazas	15,38%	3,85%	19,23%	0,00%	30,77%	30,77%
Servicio de SOC	16,33%	8,16%	20,41%	0,00%	36,73%	18,37%
SASE (Secure Access Service Edge)	12,50%	0,00%	0,00%	0,00%	37,50%	50,00%
Proxies/Proxies inversos	7,69%	20,51%	17,95%	2,56%	23,08%	28,21%
IDS/IPS de nueva generación	15,63%	14,06%	15,63%	3,13%	23,44%	28,13%
Herramientas de validación de cumplimiento con regulaciones internacionales	7,69%	0,00%	23,08%	7,69%	30,77%	30,77%
Herramientas Anti–DDoS	12,73%	12,73%	10,91%	1,82%	27,27%	34,55%
Firmas digitales/certificados digitales	13,92%	8,86%	22,78%	3,80%	24,05%	26,58%
Firewalls tradicionales (Hardware/Software)	8,00%	18,00%	18,00%	6,00%	18,00%	32,00%
Firewalls de Bases de Datos (DAF)	21,43%	4,76%	19,05%	7,14%	16,67%	30,95%
ADS (Anomaly detection systems)	18,18%	22,73%	9,09%	0,00%	27,27%	22,73%
Enfoque de seguridad Zero Trust	23,33%	6,67%	6,67%	3,33%	26,67%	33,33%
Cooperación/Intercambio de información con otros (estado, proveedores, aliados, sectores, pares)	11,11%	13,89%	22,22%	2,78%	27,78%	22,22%
Entrenamiento/Actualización del personal de seguridad/ciberseguridad	21,43%	8,57%	8,57%	4,29%	24,29%	32,86%
Cifrado de datos	17,65%	8,24%	14,12%	2,35%	23,53%	34,12%
Ciberseguros	8,82%	17,65%	5,88%	0,00%	41,18%	26,47%
CASB (Cloud Access Security Broker)	20,00%	10,00%	10,00%	0,00%	26,67%	33,33%
Biométricos (huella digital, iris, etc.)	18,00%	14,00%	16,00%	0,00%	22,00%	30,00%

me resalta que las soluciones *anti-malware*, cifrado de discos, antivirus avanzados basados en inteligencia artificial también están considerados.

En cuanto a la protección de la capa de aplicaciones, los *Firewalls Web*, de bases de datos la protección de APIs son los controles que más se están usando y se tiene proyectado utilizar.

Políticas

La Figura 20, refleja el estado de las políticas de seguridad en las organizaciones colombianas, el 72%

Figura 20

Estado de las Políticas

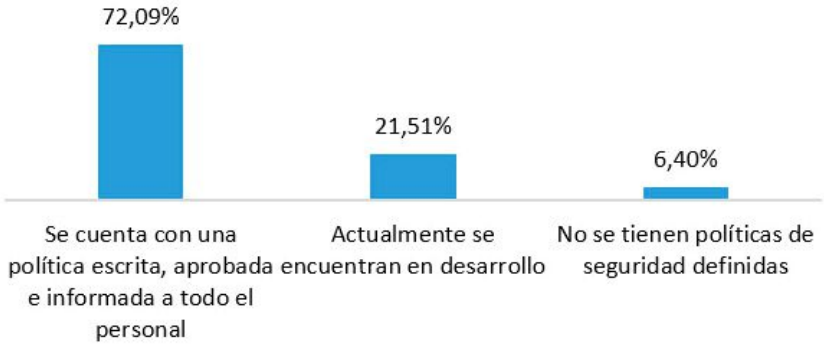


Figura 21

Obstáculos de la seguridad

de los encuestados manifiesta que tienen formalizada sus políticas de seguridad, el 22% actualmente en desarrollo y solo el 7% señala no tener políticas de seguridad de la información.

La Figura 21, resalta cuales son los obstáculos para tener una postura de seguridad en las organizaciones, en primer lugar, la falta de cultura o ausencia de esta con un 44%, la falta de colaboración entre áreas y departamentos 27%, falta de tiempo es el tercer lugar 26%.

La Figura 22, refleja el nivel de consciencia de los directivos en materia de seguridad, encontrando que, la alta dirección entiende participa y toma decisiones relacionadas con la seguridad de la información en 42%, la dirección entiende y atiende las recomendaciones en materia de seguridad de la información 28%, la dirección entiende y atiende recomendaciones en materia de seguridad, el 18% considera que la dirección poco se involucra en el tema, y el 10% manifiesta que la alta dirección solo delega y espera avances e informes.

La gestión de riesgos de seguridad es un elemento esencial, en esa línea el 78% de los encuestados tiene un proceso de gestión de riesgos y solo 22% no lo posee.

En la Figura 23, que resalta cada cuanto son ejecutados dichos ejercicios, el 50% manifiesta que al menos la ejecuta 1 vez al año, el 27% más de dos y solo dos el 23%.

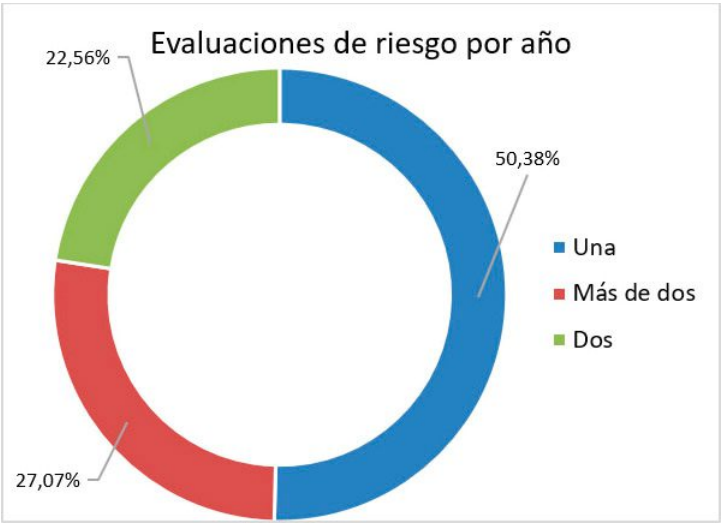
Dentro de las personas que contestaron que no lo hacen, al indagar en las razones de por qué no es realizada la gestión de riesgos. El primer motivo que resaltan los partici-

Figura 22

Consciencia de los directivos

Figura 23

Evaluaciones de Riesgos



pantes está relacionado con no tener un proceso formal de gestión de riesgos (37%), seguido de que ya está incluido en el proceso de gestión de riesgo empresarial 24%, el desconocimiento del tema 11% es el tercer lugar, la falta de presupuesto el 4 lugar con 11% y por último el no tener asociados riesgos con el tratamiento de la información 11%.

La Tabla 7, muestra las metodologías de gestión de riesgos usadas

Tabla 7

Uso de metodologías de gestión de riesgos

Metodología de Gestión de Riesgos	Porcentaje
ISO 27005	43%
ISO 31000	36%
SARO	14%
GRC (Governance, Risk & Compliance)	13%
No se cuenta con metodología	12%
Magerit	7%
ERM(Enterprise Risk Management)	7%
Otra (especifique)2	4%
Octave	1%
AS/NZ 4360	1%
Otra (especifique)	0%

por los participantes del estudio. En primer lugar, está ISO 27005 como la más usada con el 43%, seguido de ISO 31000 36%, SARO 14%, como las tres primeramente usadas, llama la atención que comparado con el año inmediatamente anterior hay un cambio significativo en el uso de ISO 31000 frente a ISO 27005.

La Figura 24, muestra la forma en como las organizaciones hacen las asociaciones entre incidentes de seguridad y el riesgo. El 67% asocia los incidentes de seguridad con riesgos de ciberseguridad, el 58% los asocia con riesgos operacionales, el 43% los asocia con riesgos reputacionales, el 40% con riesgos legales, el 37% con riegos económicos, el 30% los asocia a riesgos transversales y otros solo es usado con el 1% de las veces.

La Tabla 8, muestra la distribución del uso de los distintos marcos de trabajo (*frameworks*) aplicados en las organizaciones colombianas: ISO/IEC 27001, NIST, ITIL y COBIT son los más usados. Disminuye contra el año anterior el no usar ningún marco de buenas prácticas.

En cuanto a las regulaciones que las organizaciones deben cumplir, el caso colombiano menciona que, el 60% de los participantes manifiesta que sí existen regulaciones que son aplicables a sus modelos de negocio, el 25% considera que no está sujeto a cumplir ningún marco regulatorio o normativos, el 12% debe cumplir con marcos regulatorios internacionales y solo el 4% menciona a otros elementos de regulación.

Consideraciones de los datos

Los riesgos de seguridad de la información y ciberseguridad en definitiva son una realidad como lo es ratificado en el informe del Foro Económico Mundial (WEF, 2022), el cual manifiesta que la prioridad

Figura 24

Tipos de Riesgos

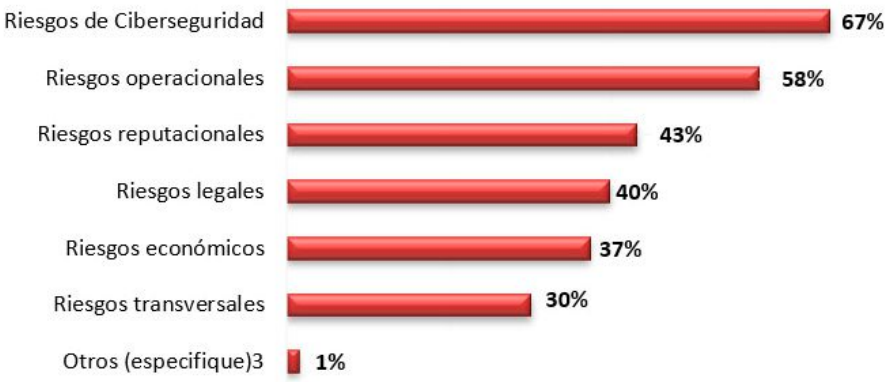


Tabla 8

Uso de marcos de trabajo de ciber-seguridad

Marco de referencia	Porcentaje
ISO 27001	69%
Guías del NIST (National Institute of Standards and Technology) USA	37%
ITIL	26%
COBIT	20%
PCI-DSS	17%
Ninguna	6%
Guías de la ENISA (European Network of Information Security Agency)	6%
ISM3 - Information Security Management Maturity Model	3%

de estos tipos de ataques es alta en las organizaciones del mundo.

Al revisar como las juntas directivas en los distintos sectores de la industria están involucradas con los temas de la ciberseguridad, tenemos elementos interesantes a considerar a través de la Figura 25.

Las juntas directivas que se involucran y toman decisiones en el mundo de la ciberseguridad, primeramente, están en el sector de las tecnologías de la información, y en el sector financiero. Al revisar con aquellos cuerpos directivos que entienden y reciben recomendaciones, pero no toman decisiones, el sector de la educación ocupa el primer lugar, seguido del sector financiero y el de las tecnologías de la información. Al ver aquellos cuerpos ejecutivos que poco o nada se involucran tenemos al sector del gobierno como el primero en la lista y al sector de la educación en segundo lugar. Para aquellos equipos directivos que solo delegan y esperan resultados, se tiene que el sector de la educación y las tecnologías de la información ocupan los primeros lugares.

Esto resalta la idea de que la madurez de las organizaciones se ve reflejada desde la posición que decide asumir la dirección en relación con la ciberseguridad, cuando los líderes de riesgo y de seguridad vuelven a la seguridad un asunto de los negocios, se crea un compromiso en la dirección y cuerpos directivos no solo se involucran en ellos (Accenture, 2020).

Es claro que existen obstáculos para que la postura de seguridad de una organización se de en los ambientes organizacionales, la postu-

ra de ciberseguridad tiene muchos componentes que deben trabajar de manera unida, alineados a una gran estrategia basada en la gestión de los ciberriesgos, de tal manera que alimente el trabajo colaborativo y cooperativo (Marsh, 2022).

En la realidad de Colombia la Tabla 9, expresa cuales son los obstáculos más representativos que los distintos sectores de la industria ha experimentado. En el sector de Educación vemos a la falta de formación técnica, la poca visibilidad a nivel ejecutivo y la escaza formación en gestión segura de la información los primeros tres obstáculos, por su parte en el sector del gobierno la poca visibilidad en el sector en el nivel ejecutivo, el poco entendimiento de los flujos de la información en la organización, y otros factores. En el sector salud está la escaza formación en gestión segura de la información, las limitaciones de las habilidades gerenciales y capacidades de liderazgo de los cisos y la complejidad tecnológica son los primeros obstáculos relacionados. El sector finan-

Figura 25

Juntas directivas por sectores

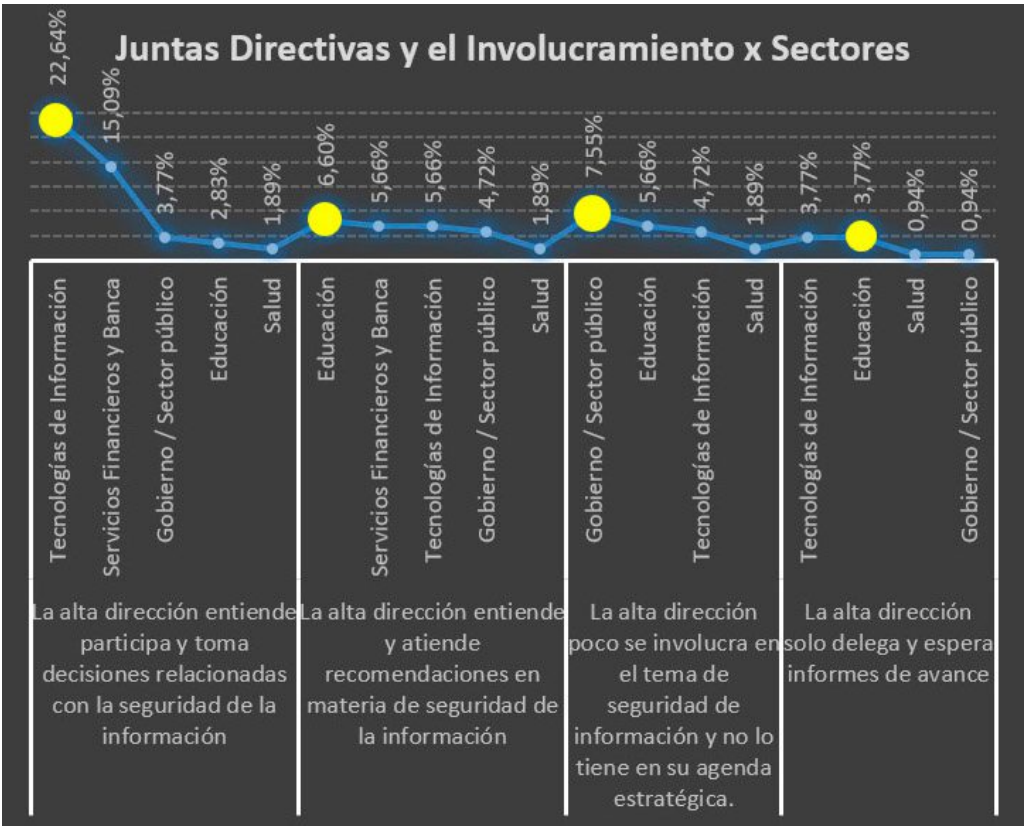


Tabla 9

Obstáculos de la ciberseguridad por sectores

Obstáculos para la ciberssegurídad	Educación	Gobierno / Sector público	Salud	Servicios Financieros y Banca	Tecnologías de Información
Ausencia o falta de una cultura en seguridad de la información	20,31%	20,31%	9,38%	12,50%	37,50%
Otros (especifique)	12,50%	25,00%	0,00%	37,50%	25,00%
No se tienen obstáculos	0,00%	0,00%	0,00%	60,00%	40,00%
Poca visibilidad del tema a nivel ejecutivo	34,62%	26,92%	3,85%	7,69%	26,92%
Poco entendimiento de los flujos de la información en la organización	26,32%	26,32%	10,53%	21,05%	15,79%
Poco entendimiento de la seguridad de la información					
Limitadas habilidades gerenciales y de liderazgo de los CISO's	30,77%	7,69%	15,38%	7,69%	38,46%
Inexistencia de política de seguridad					
Falta de tiempo	27,59%	20,69%	6,90%	17,24%	27,59%
Falta de formación técnica	47,37%	15,79%	5,26%	15,79%	15,79%
Falta de colaboración entre áreas/departamentos	21,88%	25,00%	6,25%	15,63%	31,25%
Escasa formación en gestión segura de la información	34,38%	12,50%	15,63%	6,25%	31,25%
Falta de apoyo directivo	27,59%	24,14%	10,34%	13,79%	24,14%
Complejidad tecnológica	30,43%	13,04%	13,04%	26,09%	17,39%

ciero por su parte señala no tener obstáculos, otros y la complejidad tecnológica como sus primeros desafíos. En el sector de las tecnologías manifiestan no tener obstáculos, seguido de las limitaciones de los cisos en las habilidades de gerencia y las capacidades de liderazgo y en tercer lugar la falta de cultura de ciberseguridad.

Todos los sectores de la industria colombiana no ven o asocian sus incidentes de seguridad de la misma manera, hay una variedad interesante que se ve reflejada en la Figura 25, que resalta cosas interesantes. El sector de las tecnologías de la información relacionan sus incidentes con riesgos de tipo económico como primera alternativa,

mientras que el sector financiero los tiene enmarcados como riesgos de ciberseguridad igual que lo hace el sector educación, interesante pues la madurez del sector de educación comparado con el sector financiero no son iguales pero si manejan la misma forma de hacer visible el desafío de la ciberseguridad. El sector salud asocia sus incidentes de seguridad con riesgos operacionales, mientras que el sector gobierno como primera opción los asocia a riesgos transversales, también interesante pues si bien muestra un avance importante en la relevancia que tiene el riesgo en las entidades del gobierno, la madurez de sus prácticas basado en los datos no es la más avanzada. La consultoría especializada enmarca los incidentes de seguridad y ciberseguridad en los riesgos reputacionales.

Lo cierto de todos los datos es que todos los sectores a su manera resaltan la necesidad de hacer un buen gobierno de seguridad a través del modelamiento de los riesgos y tenerlos presentes como herramientas claves para orientar los esfuerzos de la ciberseguridad es un factor esencial para poder estar cerrando la brecha frente a un adversario digital que cada vez más tiene presencia, posición, intención, intensidad e impacto (WEF, 2022).

Capital intelectual

La Tabla 10, relaciona la cantidad de personas que conforman las áreas de seguridad, la primera posición la ocupa las áreas con un tamaño de 1 a 5 personas, seguido de aquellas que son mayores de 15 personas, seguido de las que tienen entre 6 a 10 personas, ninguna persona dedicada en el 4 lugar y por último las que tienen entre 11 a 15 personas.

La Figura 26, representa la comparación de las certificaciones que los profesionales de seguridad han alcanzado en la actualidad y que desean alcanzar en el tiempo. CISM, CISSP, CRISC, CEH y CISA, son las certificaciones que muestran mayor deseo de ser alcanzada al revisar la diferencia frente a quienes las han alcanzado.

La Figura 27, representa que tipo de información entrega el profesional de seguridad en la organiza-

Tabla 10

Tamaño de las áreas de seguridad

Tamaño	Porcentaje
1 a 5	61,01%
Más de 15	18,24%
6 a 10	10,69%
Ninguna	5,66%
11 a 15	4,40%

Figura 26

Certificaciones alcanzadas vs deseadas

ción. La entrega de información para la toma de acciones, seguido de la entrega de información para la toma de decisiones son las dos principales.

El CISO, es la figura más representativa como cabeza visible para guiar y orientar la ciberseguridad en las organizaciones. La Figura 28, muestra la forma en que las organizaciones ven o identifican el tipo de CISO que existe en ellas.

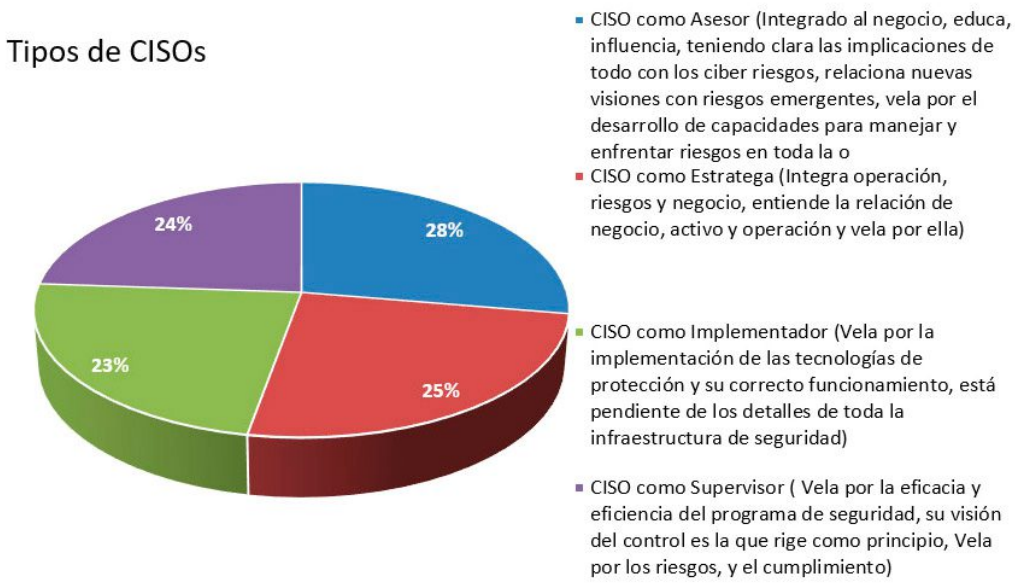
Los profesionales de seguridad, especialmente los CISOs tienen

Figura 27

Entrega de información

Figura 28

Tipo de CISO



preferencias para su crecimiento y formación, la Figura 29 representa la forma en como escogen formarse, en primer lugar, están las certificaciones, segundo lugar la educación formal, seguido de las charlas especializadas, los cursos cortos, diplomados y en el último lugar la formación ejecutiva.

De igual manera todo profesional de seguridad tiene oportunidades en las que puede crecer y mejorar, es por esa razón que se revisa cuales pueden ser los puntos de mejora en términos de capacidades, en primer lugar, están las capacidades de liderazgo, seguido de las capacidades de gestión, luego de las capacidades intelectuales, seguido por las humanas, y por último la experiencia profesional, como lo muestra la Figura 30.

Consideraciones de los datos

El talento humano en seguridad tiene cada vez más tensiones y presiones que lo han puesto en el centro de muchos análisis y observaciones, muchos profesionales sienten la tensión de los movimientos de la ciberseguridad y dicha tensión hace que el fenómeno llamado gran renuncia producido como efecto colateral de la pandemia los haga considerar salir de sus empresas, pensando más en la tranquilidad y bienestar (Deepinstinct, 2022).

Hay una gran controversia sobre la escasez de talento, mientras unos defienden que no existe talento, otros están defendiendo la tesis que es la escasez de habilidad y conocimiento del profesional de segu-

Figura 29

Preferencias de formación

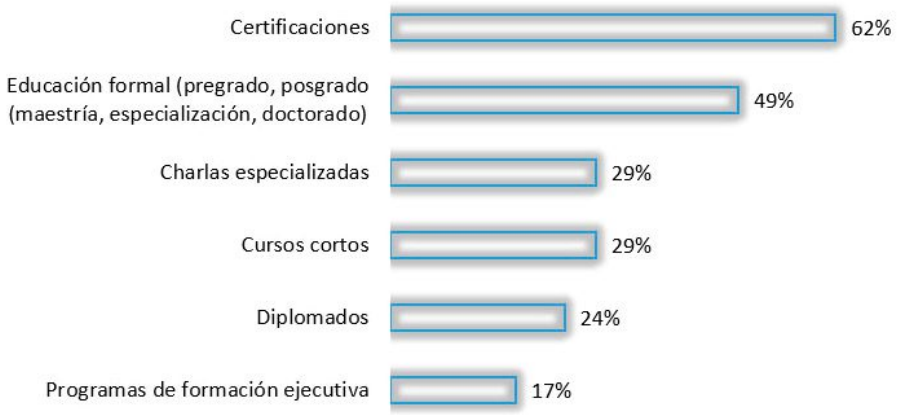


Figura 30

Capacidades por mejorar

ridad lo que se debe trabajar, diciendo que talento humano si existe, pero no preparado para enfrentar los nuevos desafíos de la ciberseguridad (ISACA, 2022).

Al revisar los datos para Colombia y ver como se desenvuelven las áreas de seguridad en los sectores de la industria y los tamaños de esta, hay datos muy interesantes, como los expuestos en la Tabla 11. Los datos revelan que en primer lugar la madurez de las empresas del sector financiero que, en ninguna de sus franjas de tamaño de empresa, no tiene reportado que no exista área de seguridad. De hecho, los valores altos y representativos están en las áreas de más de

15 personas, para empresas de más de 1000 empleados. Consultoría especializada, sector salud, sector de las tecnologías y sector educación manifiestan que no tienen ninguna persona para atender los desafíos de seguridad, el sector del gobierno es variado, llama la atención que las empresas de 1000 a 5000, su área de seguridad es de 1 a 5 como su mayor valor, y entre 11 y 15 en una mucho menor proporción. Así mismo el sector manifiesta que sin importar el tamaño de la empresa, no existe organizaciones que no tengan talento de seguridad asignado. Otro dato llamativo es el tema del sector salud su área predominante es la de 1 a 5 personas sin importar el tamaño de la empresa.

El reporte de MarlinHawk (2020) muestra que el promedio de los profesionales estudiados del mundo de la seguridad tiene 4 años en una posición en esta área. Desde el mismo informe resalta que el 94% de los profesionales de seguridad tienen un grado obtenido en la universidad, que el 84% está relacionado con ciencias de la computación, que cerca del 44% surgen de las áreas de TI.

Los distintos roles que contestan la encuesta tienen distintas preferencias en relación con las certificaciones, lo que si es cierto es que el profesional de seguridad más allá del rol tiene intención de seguir creciendo y formándose en materia de ciberseguridad, precisamente para estar disponible frente a la demanda de trabajo que existe en la actualidad (ISACA, 2022).

Al revisar los datos de Colombia y ver las preferencias más y menos apetecidas en materia de certificaciones por los roles definidos, se encuentran reflejadas en la Figura 31.

En la figura 31 los asesores y consultores muestran no estar intere-

Tabla 11

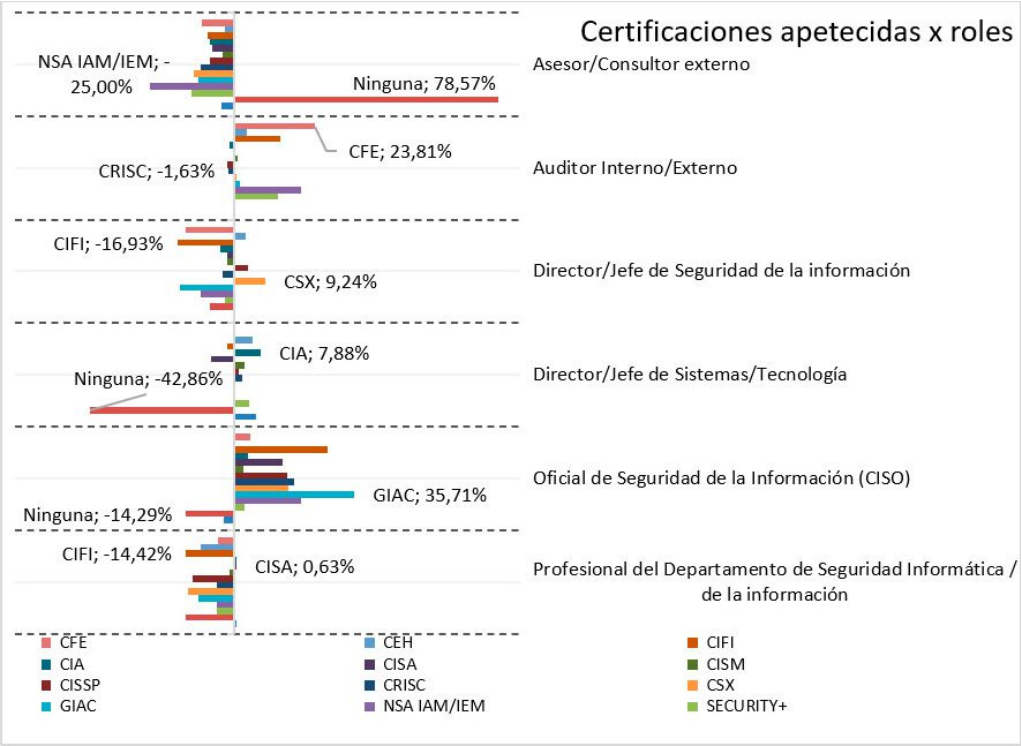
Distribución del tamaño de las áreas de seguridad por sectores y tamaño de empresa

Tamaño del Area/Sector - Tamaño empresa	1 a 5	Más de 15	6 a 10	Ninguna	11 a 15
Tecnologías de Información					
1 - 50 empleados	10,17%	0,00%	0,00%	1,69%	0,00%
201 - 500 empleados	4,24%	0,85%	2,54%	0,00%	0,00%
1001 - 5000 empleados	1,69%	3,39%	0,00%	0,00%	0,00%

51 - 200 empleados	3,39%	0,85%	0,00%	0,00%	0,00%
Mayor de 5001 empleados	0,00%	2,54%	0,00%	0,00%	0,00%
501 - 1000 empleados	0,85%	0,00%	0,00%	0,00%	0,00%
Servicios Financieros y Banca					
1001 - 5000 empleados	0,85%	3,39%	0,85%	0,00%	0,85%
Mayor de 5001 empleados	0,00%	3,39%	0,85%	0,00%	0,00%
201 - 500 empleados	3,39%	0,00%	0,00%	0,00%	0,00%
501 - 1000 empleados	0,85%	0,85%	0,00%	0,00%	0,00%
1 - 50 empleados	0,00%	0,00%	0,85%	0,00%	0,00%
51 - 200 empleados	0,85%	0,00%	0,00%	0,00%	0,00%
Consultoría Especializada					
1 - 50 empleados	7,63%	0,00%	0,85%	0,85%	0,00%
Mayor de 5001 empleados	0,00%	1,69%	0,00%	0,00%	0,00%
1001 - 5000 empleados	0,85%	0,85%	0,00%	0,00%	0,00%
201 - 500 empleados	0,00%	0,00%	0,85%	0,85%	0,00%
501 - 1000 empleados	0,00%	0,85%	0,00%	0,00%	0,00%
51 - 200 empleados	0,85%	0,00%	0,00%	0,00%	0,00%
Educación					
501 - 1000 empleados	1,69%	0,00%	0,85%	1,69%	0,00%
Mayor de 5001 empleados	1,69%	0,85%	0,85%	0,00%	0,00%
1001 - 5000 empleados	2,54%	0,00%	0,85%	0,00%	0,00%
201 - 500 empleados	3,39%	0,00%	0,00%	0,00%	0,00%
1 - 50 empleados	0,85%	0,00%	0,00%	0,00%	0,00%
Gobierno / Sector público					
1001 - 5000 empleados	5,08%	0,00%	0,00%	0,00%	1,69%
501 - 1000 empleados	3,39%	0,00%	0,85%	0,00%	0,00%
Mayor de 5001 empleados	0,00%	0,85%	0,00%	0,00%	0,85%
201 - 500 empleados	0,85%	0,00%	0,00%	0,00%	0,00%
51 - 200 empleados	0,85%	0,00%	0,00%	0,00%	0,00%
Salud					
501 - 1000 empleados	0,85%	0,00%	0,00%	0,00%	0,00%
Mayor de 5001 empleados	0,85%	0,00%	0,00%	0,00%	0,00%
51 - 200 empleados	0,85%	0,00%	0,00%	0,00%	0,00%
1001 - 5000 empleados	0,85%	0,00%	0,00%	0,00%	0,00%
1 - 50 empleados	0,85%	0,00%	0,00%	0,00%	0,00%
201 - 500 empleados	0,85%	0,00%	0,00%	0,00%	0,00%

Figura 31

Preferencias de certificaciones por roles



sados en tener este compendio de certificaciones, bien sea porque ya las tienen, o porque están interesadas en otros motivos, así mismo en ese grupo lo menos apetecido es la certificación NSA/ISA. El rol auditor prefiere la certificación CFE con el 23,81% y la que menos apetece es el CRISC, los directores jefes de seguridad lo que más apetecen es la certificación CSX (ISACA's Cybersecurity Nexus), mientras que es CIFI (Certified Information Forensics Investigator) es la menos apetecida. El director jefe de Tecnología aprecia la CIA (Certified Internal Auditor), mientras que no tener ninguna no es una opción viable. Para los oficiales de seguridad CISO todas están en rangos positivos, destacándose las certificaciones GIAC del Sans Institute, y no es una opción viable el no tener alguna certificación. Para el profesional de seguridad del compendio de certificaciones está en su radar CISA (Certified Information System Auditor) y la que menos le llama la atención es CIFI.

Definitivamente las certificaciones tienen un impacto significativo en los profesionales de seguridad, aumentando su nivel de consciencia de la ciberseguridad, su nivel de conocimiento, y mejora de las tareas

(Fortinet, 2022), sin embargo, no significa siempre que estar certificado represente ser el mejor rol para una determinada posición, aprender y tener capacidad para seguir aprendiendo se convierte definitivamente en un factor fundamental (Martínez, 2022), para crecer en el mundo de la ciberseguridad.

Ser CISO definitivamente representa un desafío en todas las organizaciones, sin importar la naturaleza de esta, o sus condiciones principales es un rol que demanda esfuerzos, resistencia, preparación y consistencia (Proofpoint, 2022). La siguiente Tabla 12, detalla que tipo de información el profesional de seguridad entrega a las distintas instancias de la organización por sectores. Tanto el sector de consultoría especializada, educación y salud hablan de un CISO que no está entregando información de ningún tipo, y por tanto puede estar equivocándose la organización a la hora de tomar decisiones, bien sea por que no haya definido que se necesite, o porque el CISO no tenga su voz definida. La importancia de la comunicación de los aspectos de seguridad en todas las esferas de la organización es clave, ganarse un espacio es un desafío que debe hacerse y son de las apuestas importantes que los cisos deben realizar (Accenture, 2020). Por otro lado tenemos en el sector de gobierno que el CISO se dedica a entregar información de las vulnerabilidades, como el primer tipo de información que entrega, en el sector financiero se manifiesta que lo que más entrega el ciso es información para la toma de decisiones, que adicional muestra y ratifica el nivel de madurez del sector en la materia, por su parte en el sector de las tecnologías de la información vemos que el ciso entrega informa-

Tabla 12

Entrega de información del CISO por sector de la industria

Entrega de Información del CISO en los sectores principales	Consultoría Especializada	Educación	Gobierno / Sector público	Salud	Servicios Financieros y Banca	Tecnologías de Información
Información relacionada con la gestión de la seguridad para la toma de acciones	12,82%	14,10%	16,67%	2,56%	17,95%	35,90%
No está entregando información	16,67%	16,67%	8,33%	25,00%	0,00%	33,33%
Información técnica relacionada con vulnerabilidades, amenazas, e incidentes	12,90%	11,29%	19,35%	3,23%	24,19%	29,03%
Información relacionada con los riesgos en Seguridad de la Información y Ciberseguridad para la toma de decisiones	12,68%	15,49%	14,08%	1,41%	25,35%	30,99%
Información relacionada con las brechas de seguridad existentes en la organización	15,25%	8,47%	13,56%	3,39%	23,73%	35,59%

ción para la acción, es decir una posición táctica para la implementación de acciones o posibles controles que estos requieran.

Al revisar la forma en como se espera que se comporte el CISO en las empresas de los distintos de la industria, hay datos interesantes relacionados en la Tabla 13. siguiente.

En el sector de la consultoría, educación y financiero se ve como un asesor, que está integrado al negocio y se espera que lo esté, sin embargo, al revisar la información que entrega, solo se ve que en el sector financiero cumple su rol acorde a lo que se espera del mismo. Por el otro lado, en el sector de las tecnologías y el sector salud, es visto como un estratega y su lenguaje se espera que sea de riesgos, sin embargo, en el sector de tecnologías lo que predomina es la entrega de información para la acción, y en el sector salud no está entregando información, lo cual hace ver que hay desfases en lo que sucede con el rol. Por último, el sector del gobierno lo ve como un supervisor, una persona que sigue un programa y por su cumplimiento, y al revisar el tipo de información que entrega se puede evidenciar que es el más consistente, puesto que lo ven como un supervisor y responde en la misma medida entregando información técnica que puede ayudar a cumplir con un programa de ciberseguridad.

Los profesionales de seguridad saben que hay que fortalecer tanto sus habilidades y sus capacidades, las habilidades a través de las certificaciones como lo resaltan los da-

Tabla 13

Visibilidad del CISO por sector de la industria

Visibilidad del CISO	Consultoría Especializada	Educación	Gobierno / Sector público	Salud	Servicios Financieros y Banca	Tecnologías de Información
CISO como Asesor (Integrado al negocio, educa, influencia, teniendo clara las implicaciones de todo con los ciber riesgos, relaciona nuevas visiones con riesgos emergentes, vela por el desarrollo de capacidades para manejar y enfrentar riesgos en toda la organización)	5,93%	5,93%	4,24%	0,85%	5,93%	6,78%
CISO como Estratega (Integra operación, riesgos y negocio, entiende la relación de negocio, activo y operación y vela por ella)	3,39%	1,69%	0,85%	1,69%	4,24%	11,86%
CISO como Implementador (Vela por la implementación de las tecnologías de protección y su correcto funcionamiento, está pendiente de los detalles de toda la infraestructura de seguridad)	3,39%	3,39%	4,24%	1,69%	4,24%	5,93%
CISO como Supervisor (Vela por la eficacia y eficiencia del programa de seguridad, su visión del control es la que rige como principio, Vela por los riesgos, y el cumplimiento)	3,39%	4,24%	5,08%	0,85%	2,54%	7,63%

tos de este año. Las siguientes Tablas (14,15) relacionan como los tipos de cisos prefieren formarse y en que prefieren hacerlo.

Es interesante, mientras que los CISOs tipo Asesor y Estratega prefieren la formación ejecutiva, el ciso implementador prefiere los diplomados y el supervisor las charlas especializadas.

Ahora al revisar las razones por la que toman estos programas, buscando las oportunidades de mejora en su carrera profesional, se puede visualizar en la Tabla 15. El CISO tipo asesor, toma programas para gestionar las capacidades humanas, entendido como la necesidad de poder integrarse mejor con las organizaciones en las que trabaja y darle un nuevo sentido a la función que desempeña, el ciso estratega toma en primera instancia los programas para mejorar su capacidad de gestión, requiere de comunicación y entendimiento de negocios

Tabla 14

Tipo de CISO y sus preferencias de formación

Tipo de CISO	Educación formal (pregrado, posgrado (maestría, especialización, doctorado)	Charlas especializadas	Diplomados	Certificaciones	Cursos cortos	Programas de formación ejecutiva
CISO como Asesor	30,00%	27,12%	22,00%	25,00%	27,12%	33,33%
CISO como Estratega	25,00%	23,73%	20,00%	25,00%	20,34%	27,78%
CISO como Implementador	23,00%	22,03%	32,00%	25,00%	28,81%	25,00%
CISO como Supervisor	22,00%	27,12%	26,00%	25,00%	23,73%	13,89%

Tabla 15

Tipo de CISO y las capacidades que puede mejorar

Tipo de CISO	Capacidades estratégicas (liderazgo, comunicación, rendición de cuentas, proyecciones financieras, pensamiento estratégico, pensamiento sistémico, visión (prospectiva y pronóstico))	Capacidades intelectuales (formación académica, conocimientos técnicos, análisis, síntesis)	Experiencia profesional	Capacidades Humanas (Empatía, Inteligencia Emocional, Creatividad, Curiosidad, Imaginación, Proactividad)	Capacidades de gestión (Habilidades para comunicar e interconectar negocios y necesidades en materia de seguridad de la información, entender el negocio, entender a las partes interesadas)
CISO como Asesor	25,93%	28,57%	23,33%	29,73%	28,57%
CISO como Estratega	26,85%	26,19%	25,00%	31,08%	32,97%
CISO como Implementador	23,15%	21,43%	28,33%	18,92%	18,68%
CISO como Supervisor	24,07%	23,81%	23,33%	20,27%	19,78%

como algo necesario para el desarrollo de la función. El CISO tipo implementador quiere mejorar su saber hacer, por eso mejorar la experiencia profesional es lo más adecuado, y el CISO tipo supervisor, está buscando poder llegar a los otros tipos de CISO, por eso buscar mejorar sus capacidades estratégicas para poder conectar todo lo aprendido de la gestión y llevarlo a un siguiente nivel.

Todos estos datos ratifican la situación de Colombia en relación con el desarrollo del profesional de seguridad, sus capacidades, competencias y habilidades que deben ser desarrolladas continuamente y más ahora que los entornos cambiantes requieren de una acelerada capacidad para ser abordados.

Temas emergentes

La Figura 32, muestra los temas relevantes y emergentes que tienen en la mira los profesionales de seguridad. Para este año el tema más relevante tiene que ver con la seguridad y control en la nube, seguido de las amenazas persistentes a-

Figura 32

Temas emergentes

vanzadas, la fuga de información sensible, los ataques a infraestructuras críticas, y el talento humano de seguridad como el quinto lugar.

Consideraciones de los datos

Al revisar los temas emergentes y disgregarlos por sectores, podemos encontrar como cada sector ve y visualiza los desafíos, acorde con la realidad del sector, la madurez de este, y en esa línea sus capacidades y oportunidades.

En la Tabla 16, se evidencian como los sectores más relevantes de la industria ven sus temas y ponen atención y seguro esfuerzos por entenderlos y manejarlos.

Tabla 16

Distribución de temas emergentes por sectores de industria

Temas emergentes por sectores	Tecnologías de Información	Servicios Financieros y Banca	Salud	Gobierno / Sector público	Educación	Consultoría Especializada
Fuga de información sensible	28,17%	16,90%	7,04%	18,31%	15,49%	14,08%
Seguridad en Dispositivos Médicos	35,00%	5,00%	15,00%	10,00%	20,00%	15,00%
Robótica	27,27%	27,27%	9,09%	18,18%	9,09%	9,09%
Talento Humano de Seguridad	34,43%	16,39%	4,92%	19,67%	16,39%	8,20%
Ransomware de las Cosas (RasoT)	33,33%	10,53%	7,02%	21,05%	17,54%	10,53%
Redes Sociales	40,00%	12,50%	5,00%	17,50%	12,50%	12,50%
Noticias y videos falsos (Fake news)	35,29%	11,76%	5,88%	14,71%	23,53%	8,82%
Malware en dispositivos móviles	37,50%	12,50%	7,14%	16,07%	16,07%	10,71%
Internet de las cosas – IoT	34,09%	6,82%	9,09%	13,64%	20,45%	15,91%
Inteligencia de amenazas	35,85%	18,87%	1,89%	16,98%	13,21%	13,21%
Seguridad y control en la computación en la nube	32,50%	18,75%	6,25%	16,25%	11,25%	15,00%
Inteligencia Artificial	44,44%	17,78%	4,44%	11,11%	13,33%	8,89%
Grandes datos y analítica	35,29%	20,59%	11,76%	11,76%	14,71%	5,88%
Geopolítica global	52,63%	10,53%	0,00%	10,53%	10,53%	15,79%
Internet Industrial de las Cosas (IIoT)	50,00%	14,29%	0,00%	7,14%	21,43%	7,14%
Ciberseguridad Industrial	38,89%	13,89%	5,56%	8,33%	13,89%	19,44%
Desinformación	37,21%	11,63%	9,30%	11,63%	16,28%	13,95%
Drones	66,67%	16,67%	16,67%	0,00%	0,00%	0,00%
Ciberguerra	39,02%	19,51%	0,00%	14,63%	12,20%	14,63%
Amenazas persistentes avanzadas	35,44%	17,72%	5,06%	15,19%	12,66%	13,92%
Ciberespionaje	41,51%	11,32%	0,00%	15,09%	13,21%	18,87%
Ciber armas	44,00%	4,00%	0,00%	12,00%	12,00%	28,00%
Blockchain	35,71%	14,29%	7,14%	19,05%	14,29%	9,52%
Ataques a infraestructuras críticas	31,25%	12,50%	6,25%	20,31%	12,50%	17,19%

El sector de las tecnologías de la información ve a la geopolítica global, así como al internet industrial de las cosas y los drones como sus primeros lugares para prestar atención. El sector financiero ve en la robótica, los grandes datos y la analítica y la ciberguerra factores de alerta que deben ser considerados. Por su parte el sector salud, ve en los drones, la seguridad de los dispositivos médicos y los grandes datos y analítica sus principales retos. El sector gobierno ve en el ransomware de las cosas, los ataques a infraestructuras críticas y el talento humano de seguridad, como las principales fuentes de desafío. El sector de la educación por su parte considera las fake news, al internet industrial de las cosas, y al internet de las cosas, sus principales retos. Por último, el sector de consultoría especializada ve en las ciberarmas, la ciberseguridad industrial y el ciberespionaje, las fuentes principales para atender el presente y el futuro, al menos el cercano.

Reflexiones finales

Año tras año, el estudio muestra un afianzamiento de la seguridad digital como un instrumento corporativo en las empresas colombianas. En este contexto, cada vez más incierto, son necesarias perspectivas más incluyentes que involucren a los actores y los lleven a repensar o pensar de manera distinta la protección de la información, sin perder de vista lo ya alcanzado, y así enfrentar y superar la realidad del mundo en que se desenvuelven.

Este último período evaluado ha venido cargado del afianzamiento producido por el fenómeno denominado pandemia que ha revolucionado y cambiado la forma en cómo la seguridad se tiene que plantear en las organizaciones, si bien es cierto que se habla de volver a los niveles prepandemia, lo claro es que la vida y la ciberseguridad nunca volverán a dichos estadios, pues las organizaciones no tienen muchos planes para perder el terreno ganado en materia de transformación digital.

En un primer momento vimos a las empresas volcadas al contexto digital y aprendiendo de muchas maneras lo que significaba entrar por completo en una realidad virtual. Luego un período de afianzamiento en el mundo digital que ha empezado a mostrar un poco de lo que vendrá en ambiente postpandemia, donde los entornos de trabajo, las fuerzas laborales y los procesos organizacionales serán diferentes (Davis, 2021).

La confianza en los entornos digitales y la construcción de la capacidad de ciberresiliencia se fundamenta en una estructura de gobierno de la seguridad, en la que las políticas, la gestión de riesgos y el conjunto de buenas prácticas se convierten en elementos centrales para dirigir los programas de ciberseguridad. La conexión entre una

estrategia de seguridad y los objetivos de seguridad que sean claros ayudaran a construir y fomentar la ciberresiliencia (World Goverment Summint – EY, 2020).

Confianza digital, va más allá de las tecnologías que puedan ser de utilidad para protegerse del adversario digital, implica componentes como la gestión de riesgos, como la ética en el manejo de los datos, el uso de buenas prácticas, y la participación de todos los actores de un ecosistema digital que cada vez es más complejo (Deloitte,2021).

Situaciones como la evolución de los adversarios, la pandemia y la realidad digital de las organizaciones han cambiado la forma de ver la ciberseguridad, y así mismo la necesidad de repensar las prácticas de gestión de riesgos. Entender que es necesario evolucionar de la protección de una infraestructura, a la defensa y anticipación de un adversario digital, para ello se requiere que las prácticas estándares se consoliden en las organizaciones y así poder dar pasos más importantes que permitan evolucionar en las capacidades de la ciberseguridad, que desarrolle mejores posturas de seguridad y que repercutan en una adecuada ciberresiliencia.

Crear valor en un contexto digital, implica crear nuevos y novedosos esfuerzos por desarrollar programas de ciberseguridad que atiendan a las necesidades de las organizaciones, por un lado mejorar la práctica y el proceso al interior de las organizaciones para fortalecer lo que se debe hacer, en ello la seguridad de la información es un elemento clave, así como la seguridad informática. La primera desarrolla los procesos y refuerza la práctica, y la segunda apoya desde la vista tecnológica el diseño de esa arquitectura que busca proteger y asegurar. Por el otro lado, la ciber-seguridad juega un papel indispensable para defender una organización en un ecosistema digital extremadamente denso, y anticiparse a un adversario cada vez más complejo.

Las discusiones alrededor de como se ve la ciberseguridad hacia adelante y cuáles son los temas emergentes que tienen en la mente no solo los profesionales de la seguridad, sino aquellos que tratan de visualizar el futuro, está centrado en ver a la ciberseguridad como un "*wicked problem*"[1] (WEFb, 2022).

Otro de los temas que trae gran preocupación a la mesa es el tema del talento de ciberseguridad (Stottandmay, 2022). Los ciberriesgos en general están en la agenda de todos los CEO de las organizacio-

[1] *Wicked Problem*: Un problema complejo es un problema social o cultural que es difícil o imposible de resolver por cuatro razones: conocimientos incompletos o contradictorios, el número de personas y opiniones implicadas, la gran carga económica y la naturaleza interconectada de estos problemas con otros. Fuente: https://www.wickedproblems.com/1_wicked_problems.php

nes de todo el mundo y eso no es una sorpresa, realmente es una constante de los últimos años (PwC, 2022). Las tensiones geopolíticas, la reciente guerra en Ucrania, y los conflictos posteriores que se divisaran en el espacio digital son parte de lo que se visualiza no solo para el largo, también en el corto plazo (Infosecurity, 2022).

Los adversarios cada vez más orientados, especializados y distribuidos, con mayor intensidad, intención y recursos para hacer su trabajo, estarán a la orden del día, en el mismo sentido, la línea delgada entre adversarios y Estados apoyándolos hará de la zona gris un lugar más denso para estar alerta (Fireeye, 2022). Las ciberoperaciones están a la orden del día, y con el conflicto en el cual se encuentra el mundo aún más. Es por ello, que se verán mayores movimientos por parte de gobiernos y naciones en el manejo de sus operaciones cibernéticas, de tal manera que debe haber un especial cuidado del ecosistema en el que se desenvuelven no solo las naciones, sino las organizaciones (Maniant, 2022).

Definitivamente los riesgos que se presentan e incrementan por las cadenas de suministro serán otro de los juegos a atender en un espacio de trabajo cada vez más complejo, no solo para las organizaciones financieras, en todos los sectores de la industria la tensión y presión es importante pues no trabajar con los terceros y no hacerlos parte de un modelo integrado de protección puede traer consecuencias desafortunadas (FS-ISAC, 2022). Claramente la pandemia y estos dos años de vivir en ella ha mostrado el valor del mundo digital, sin embargo, también ha mostrado por un lado el aumento sostenido de los riesgos, ha visibilizado aún más la capacidad del adversario por hacer daño, así mismo ha acelerado el desarrollo de las capacidades organizacionales tanto para asegurar y proteger, como para anticipar y defenderse de un adversario cada vez más dotado (Trendmicro, 2022).

El mundo OT (Tecnología de Operación), ha tenido grandes impactos por diferentes anomalías, no por nada está en las preocupaciones de sectores como el de las fuerzas armadas, tendencia que también se puede ver advertir en el informe de IBM (2022) y que muestra que este es un escenario complejo que debe ser protegido por las implicaciones que tiene en las múltiples industrias.

Los ejecutivos de seguridad de esta nueva era se enfrentan de una manera más directa a otros escenarios dinámicos que demandan reacciones rápidas y prospectivas arriesgadas. Estos implican desarrollar espacios para anticiparse y observar los entornos cambiantes y superpuestos, en procura de la protección de la información y los nuevos activos digitales.

Por tanto, esta nueva realidad hace que los líderes de seguridad necesiten evolucionar, no solo por desarrollar nuevas habilidades, a su vez capacidades y competencias que los posibiliten para enfrentar los desafíos actuales. Los Líderes de seguridad seguirán siendo líderes de niveles medios (Fireeye, 2022; Proofprint, 2022; Navisite, 2021), que deben poder actualizar el conjunto de herramientas como la comunicación para que puedan interactuar con mayor determinación en los equipos de trabajo.

En la realidad colombiana, los datos muestran que los esfuerzos se vienen haciendo y las demandas de la realidad digitalmente modificada aceleran la transformación de la visión de la seguridad de la información. El contexto internacional ratifica algunas de las tendencias de Colombia

En la realidad nacional se pueden concluir los siguientes aspectos:

1. Sectores como el sector financiero han mostrado una evolución y madurez que se ve reflejada en sus capacidades para atender los desafíos de la ciberseguridad, no significando por supuesto que son invulnerables al adversario, sino que pueden estar mejor preparados para enfrentarlo.

2. Las áreas de seguridad siguen ganando terreno, espacio, posición, poder e influencia, todos los sectores de la industria a su ritmo lo ven y siguen aprendiendo, a lo mejor no con la velocidad que debería ser, pero al menos los marcadores e indicadores muestran progreso en todos ellos.

3. Las compañías de gran tamaño, con más de 1000 empleados, son las que tienen mayor claridad en torno a un área independiente y a un director de seguridad. En tales empresas grandes, el área de seguridad depende de las direcciones como la de gestión de riesgos. Es interesante observar entre las organizaciones de todos los tamaños, el bajo porcentaje que no tiene un cargo o responsabilidades definidas.

4. La posición del profesional de seguridad continúa su proceso de afianzamiento dentro de las organizaciones, cada vez se ven más plazas creadas de profesionales de seguridad como CISOs y directores de seguridad en las organizaciones, estos movimientos demandan la creación de nuevas y actualizadas conjunto de competencias, capacidades y habilidades que le permitan desarrollar mejor sus nuevas funciones. La formación, crecimiento y aprendizaje del CISO, sigue estando presente, no se puede sustraer su esfuerzo por seguir asimilando lo que significa la función, el rol y sobre todo la adaptabilidad en un en-

torno tan cambiante como el actual.

5. Entre más disruptivos son los entornos de trabajo, las nuevas capacidades como las estratégicas, las humanas y las técnicas necesitan ser desarrolladas de manera integral para atender la demanda de nuevas responsabilidades.

6. La confianza digital que los negocios actuales necesitan muestra cada vez más que es necesario un profesional de seguridad más empoderado, más desarrollado y preparado; por tanto, eso invita al profesional de ciberseguridad salir de su zona de confort de manera permanente, entrenarse y adicional aprender es la clave para enfrentar el desafío (Martínez, 2022).

7. La práctica básica, como la gestión de riesgos, el uso de marcos de referencia, son una realidad en Colombia, su afianzamiento es requerido, para que el fundamento de la ciberseguridad esté acorde con las necesidades de las empresas, y así poder avanzar en el desarrollo de capacidades que lleven a las organizaciones a un estado de ciberresiliencia que soporte las operaciones del negocio.

8. La realidad digital hace que todos los sectores e industrias lleven su mirada al tema de ciberseguridad. A los sectores como el financiero, la consultoría especializada y el gobierno les interesa participar y conocer la realidad de la seguridad, tendencia observada en diferentes informes publicados sobre seguridad y ciberseguridad.

9. Los riesgos es el lenguaje común de los negocios y a su vez es un instrumento catalizador de un programa de seguridad. Los Líderes de seguridad digital están considerando este instrumento como una valiosa oportunidad para elevar su interlocución con los niveles directivos y ejecutivos, para poder tomar caminos acordes a la realidad digital de la empresa.

10. La confianza digital y la ciberresiliencia se convierten en un generador de nuevos negocios; tendencias internacionales también sostienen que dicha confianza es una fuente que motiva a cultivar las relaciones entre consumidores y quienes ofrecen los servicios, para configurar un activo valioso a la hora de manejar y maniobrar en los ecosistemas digitales actuales.

11. A nivel nacional, se mantiene la sólida tendencia de usar mecanismos tecnológicos como las principales herramientas de protección. Si bien las tendencias internacionales dan esto por sentado, se debe hacer un llamado tanto a los responsables de seguridad como a las organi-

zaciones para que vean a la seguridad como un tema inherente a la dinámica empresarial. Las tendencias internacionales ratifican que es necesario extender la visión de la seguridad como una fuente generación de valor para la organización y los objetivos de su negocio.

12. El poder de las anomalías digitales, de los adversarios y de la realidad digital se entiende cada vez más en el marco de las organizaciones colombianas. Más allá de lo técnico, se registran los errores humanos y, en tal sentido, es necesario pasar de procesos de sensibilización al cambio de comportamientos, liderado por los responsables de la seguridad, con el ánimo de crear una nueva cultura alrededor de entornos digitalmente modificados. Así mismo, es necesario gestionar un programa de seguridad que permee todos los niveles organizacionales basados en prácticas dirigidas a los diferentes grupos de interés, y orientadas a construir posturas de seguridad diferenciadas y articuladas desde los desafíos que debe asumir el talento humano.

13. Las nuevas tecnologías como Cloud, IoT, IA, *machine learning, Zero Trust* y otras, están cambiando la concepción del mundo, la forma de interactuar y los retos a los que se enfrentan las organizaciones a nivel nacional e internacional. De ahí que los profesionales de seguridad deban tener claridad para profundizar en estas nuevas tendencias y su uso.

14. Es claro que el cisne negro (o ¿sorpresa predecible?) denominado Covid-19, ha cambiado por completo no solo la forma de ver la vida, sino ha resaltado la importancia de la ciberseguridad y la gestión de las tecnologías de la información. Hoy más que nunca se observa a la ciberseguridad como una capacidad empresarial, que ofrece y aporta en el desarrollo de negocios digitales, y que se enfrenta y enfrentará las tensiones geopolíticas y de cumplimiento con mucha más profundidad. Esta capacidad deberá apalancar la confianza digital necesaria para ofrecer servicios y desarrollar modelos de negocio en el ecosistema digital de hoy como fundamento del nuevo normal que empezamos a construir.

15. No es viable predecir el futuro, pero si es necesario crear escenarios, desarrollar libros de jugadas (*Playbooks*), hacer ejercicios de simulaciones, revisiones y auditorías a las cadenas de suministro, entre muchas otras acciones que le ayuden a la organización a estar preparada y a sus líderes de seguridad a ser tomadores de inciertos, y en la misma línea poder ayudar a la organización a gestionar y disminuir los posibles riesgos que

la incertidumbre trae (Cocron & Aronhime, 2022).

En resumen, el panorama general de la seguridad en Colombia muestra el sostenido proceso de cambios apalancados en la realidad actual empujada por una presencia de una pandemia que dos años después no termina y que sigue empujando a los negocios a un contexto digital cada vez más complejo.

El año 2021 fue un año que afianzó un nuevo modelo de vida y sociedad, el año 2022 es el momento para desarrollar nuevas formas de aprender y de seguro nuevos aprendizaje para los posibles futuros que tendremos que construir y donde la ciberseguridad tendrá parte esencial, como lo han mencionado en muchas reuniones e instancias internacionales.

Sea esta la oportunidad para decir que este es un ejercicio para repensar lo que creemos que sabemos y explorar aquello que no sabemos, para así, deconstruir muchas cosas en procura de nuevos aprendizajes que nos lleven por caminos distintos y conocimiento renovados.

Agradecimientos

Se hace un reconocimiento y mención especial a la cooperación recibida por parte de otras asociaciones tales como, Tacticaledge, CISOS.CLUB, Asociación Colombiana de Profesionales de Seguridad y CiberSeguridad (APSIC), CISObeat (Perú), Consejo de Seguridad de la Información y Ciberseguridad (México), Sociedad Chilena de Seguridad de la Información (SOCHISI), así como a todas las personas que atendieron el llamado a través de los distintos medios digitales.

Referencias

Accenture. (2020). The Cyber-Committed CEO and Board. https://www.accenture.com/_acnmedia/PDF-132/Accenture-Cyber-Committed-CEO-And-Board.pdf

Barracuda. (2022). Spear Phishing: Top Threats and Trends. https://assets.barracuda.com/assets/docs/dms/Spear-phishing-vol7.pdf

Cano, J. & Almanza, A. (2021) "Reflexiones y retos para la academia en la formación de profesionales de seguridad/ciberseguridad en Colombia: 2010 - 2020" (2021). ISLA 2021 Proceedings. 7 https://aisel.aisnet.org/isla2021/7

Cocron, A. & Aronhime, L. (2022). Risk, Uncertainty, and Innovation. Nato Review. https://www.nato.int/docu/review/articles/2022/04/14/risk-uncertainty-and-innovation/index.html

CyberEdge Group (2022). Cyberthreat Defense Report. https://cyber-edge.com/wp-content/uploads/2022/04/CyberEdge-2022-CDR-Report.pdf

DarkReading. (2022). The state of CISO influence 2021. The maturing CISO role. https://www.coalfire.com/documents/reports/the-state-of-ciso-influence

Davis. D. (2021). 5 Models for the Post-Pandemic Workplace. HBR. https://hbr.org/2021/06/5-models-for-the-post-pandemic-workplace

Deloitte (2021). Building The Resilient Organization. https://www2.deloitte.com/content/dam/insights/articles/US114083_Global-resilience-and-disruption/2021-Resilience-Report.pdf

Deepinstinct. (2022). Voice of SecOps 2022. https://info.deepinstinct.com/voice-of-secops-v3-2022

FBI. (2022). Internet Crime Report 2021. https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

Fireeye (2022). M-Trends 2021. https://www.arrow.com/ecs-media/16352/fireeye-rpt-mtrends-2021.pdf

Fortinet. (2022). 2022 Cybersecurity Skills Gap. https://www.fortinet.com/content/dam/fortinet/assets/reports/report-2022-skills-gap-survey.pdf

FS-ISAC. (2022). Navigating Cyber2022. https://www.fsisac.com/hubfs/NavigatingCyber-2022/NavigatingCyber2022-TLPWHITE-FIN.pdf

IBM (2022). Cost of a Data Breach Report 2021. https://www.ibm.com/downloads/cas/OJDVQGRY

INFOSECURITY (2022). State of cybersecurity report 2022. https://www.infosecurity-magazine.com/white-papers/state-of-cybersecurity-report-2022/

ISACA (2022). State of Cybersecurity 2022. Global Update on Workforce Efforts, Resources and Cyberoperations. https://www.isaca.org/go/state-of-cybersecurity-2022

Keeper. (2022). Ransomware impact report. https://www.keeper.io/hubfs/PDF/2021-ransomware-impact-report.pdf

Mandiant. (2022). | MANDIANT M-TRENDS 2022. https://www.mandiant.com/media/15671

Marsh. (2022). The state of cyber resilience. https://www.marsh.com/us/services/cyber-risk/insights/the-state-of-cyber-resilience.html

Marlin Hawk (2020). Global Snapshot: The CISO in 2020. Recuperado de: https://www.marlinhawk.com/docs/Marlin-Hawk-Global-CISO-Research-Report.pdf

Martinez, J. (2022). La información es inútil sin conocimiento. https://www.linkedin.com/pulse/la-informaci%25C3%25B3n-es-in%25C3%25BAtil-sin-conocimiento-javier-mart%25C3%25ADnez-aldanondo/?trackingId=%2F8Kotk%2BATGGJnh%2FuRNG70Q%3D%3D

Navisite. (2021). The State of Cybersecurity Leadership and Readiness. https://www.navisite.com/resources/reports-1/state-of-cybersecurity-leadership-and-readiness-report

PwC (2022). 2022 Global Risk Survey Embracing risk in the face of disruption. https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/assets/pwc-global-risk-survey-report-2022-main.pdf

Proofpoint. (2022). 2022 Voice of the CISO REPORT. Global Insights Into CISO Challenges, Expectations and Priorities. https://www.proofpoint.com/sites/default/files/white-papers/pfpt-us-wp-voice-of-the-CISO-report.pdf

Stottandmay. (2022). Cyber Security in Focus 2022.

https://fs.hubspotusercontent00.net/hubfs/2529404/Research/Cyber_Security_in_Focus_22.pdf?_hsmi=201423978

TrendMicro. (2022). Navigating New Frontiers Trend Micro 2021 Annual Cybersecurity Report. https://documents.trendmicro.com/assets/rpt/rpt-navigating-new-frontiers-trend-micro-2021-annual-cybersecurity-report.pdf

Verizon (2022). Data Breach Investigation Report. https://www.verizon.com/business/resources/reports/2022/dbir/2022-dbir-data-breach-investigations-report.pdf

WEF - World Economic Forum (2022) Global Cybersecurity Outlook 2022. https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf

WEFb - World Economic Forum (2022) Global Cybersecurity Outlook. Meeting of experts. https://www.weforum.org/events/world-economic-forum-annual-meeting-2022/sessions/global-cybersecurity-outlook-1a06c9fd7d

World Government – EY. (2020) Cyber Resilience in the Digital Age. https://www.worldgovernmentsummit.org/api/publications/document?id=24717dc4-e97c-6578-b2f8-ff0000a7ddb6

Zscaler. (2022). 2022 ThreatLabz Phishing Report. https://www.zscaler.com/resources/industry-reports/2022-threatlabz-phishing-report.pdf

***Andres R. Almanza J., Ms.C, CISM**. Chief Growth Officer en CISOS.CLUB, Investigador en Ciberseguridad SegInfo y Liderazgo. | Executive Certificate in Cybersecurity Leadership & Strategy by FIU University | Certificado como ISO 27001 Lead Implementer and 27005 Lead Manager from PECB | CISM, ITILv3, LPI| Certificado como Coach Profesional Internacional, Master in Leadership and Organizational Development with Coaching, Executive Master's in Leadership Skills Developed in Harvard, & Coach Profesional avalado por International Coach Federation| Profesional en Ingeniería de Sistemas | especialista en seguridad en redes y máster en seguridad de la información. Docente del programa de maestría de la Universidad Externado de Colombia y de la Universidad de las Américas en Ecuador. Creador de la Comunnidad CISOS.CLUB, CISOS-COL y CISOS-LATAM (Linkedin) y Miembro del comité editorial de la revista sistemas de ACIS.*