XXIII Encuesta Nacional de Seguridad Informática

Valor y beneficio de la ciberseguridad.

DOI: 10.29236/sistemas.n169a4

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 2023, contó con la participación de 195 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 que colaboraron también con el diligenciamiento del instrumento. 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 en el corto, mediano y largo plazo, así como ayudar a formular mejoras en la postura de seguridad control y resiliencia 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 el desarrollo de la seguridad y ciberseguridad de las organizaciones y como los diferentes sectores de la industria empiezan a comprender a la seguridad digital y ciberseguridad como herramientas que ayudan a incrementar el valor de estas.

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.

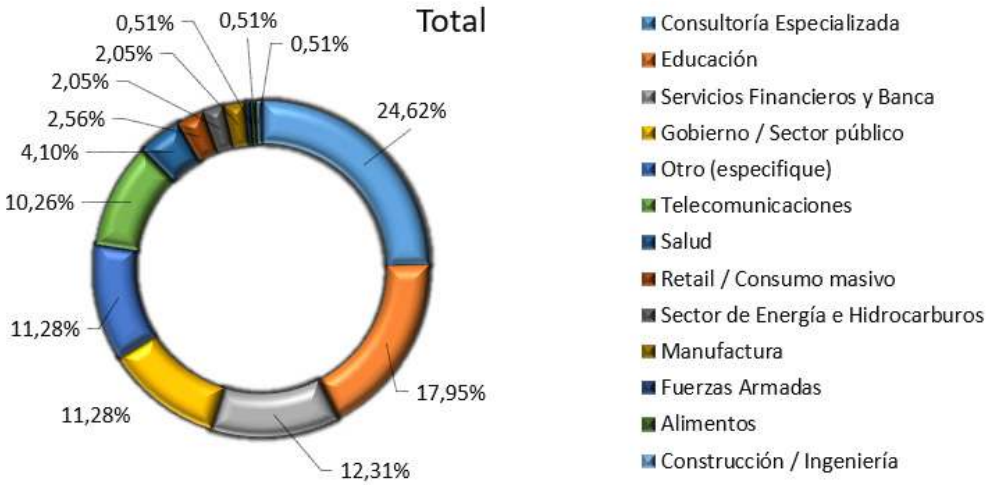
Temas emergentes: En esta sección se analizan varios aspectos, entre ellos: la percepción del futuro en materia de ciberseguridad; la vinculación de los directivos de la organización en la ciberseguridad empresarial, además de la responsabilidad y el papel del líder de seguridad en el desarrollo de la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

Hallazgos principales

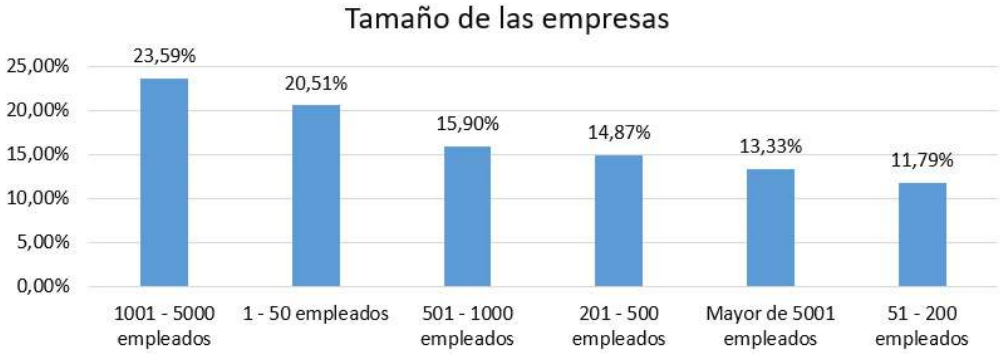
Demografía

Sectores participantes

La gráfica 1 refleja la participación de 13 sectores de la economía colombiana. Los tres segmentos con



Gráfica 1. Sectores participantes

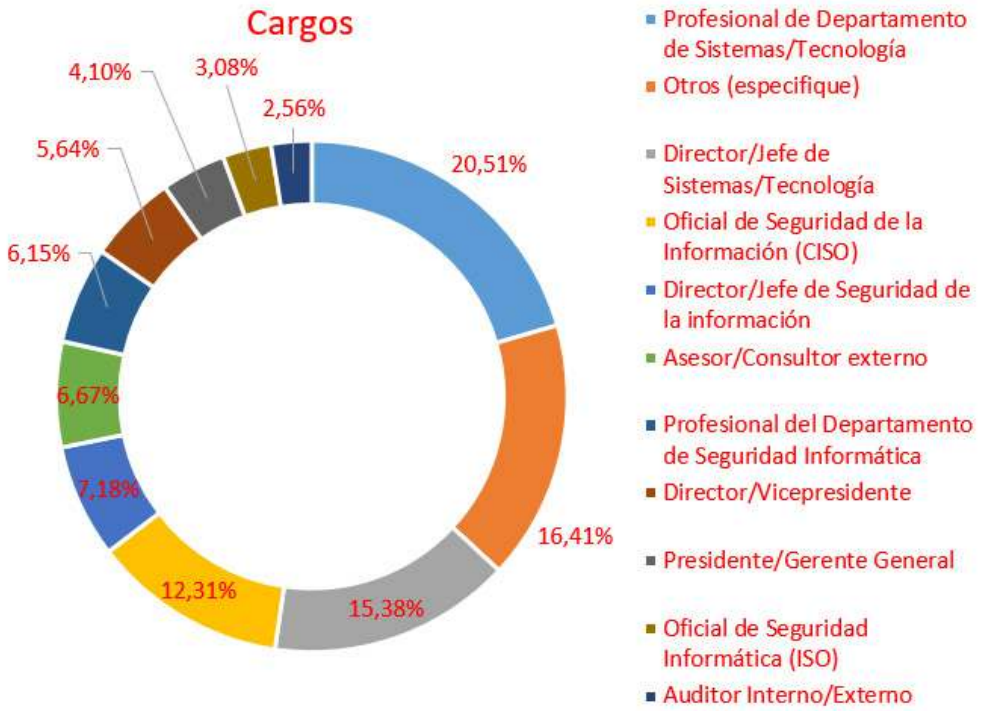


Gráfica 2. Tamaño de las empresas participantes

mayor participación de la encuesta para este año fueron Sector de Tecnología, Financieros, Educación y Consultoría especializada los más representativos en participación.

La gráfica 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 gráfica 3 muestra los cargos de los encuestados, entre los que se

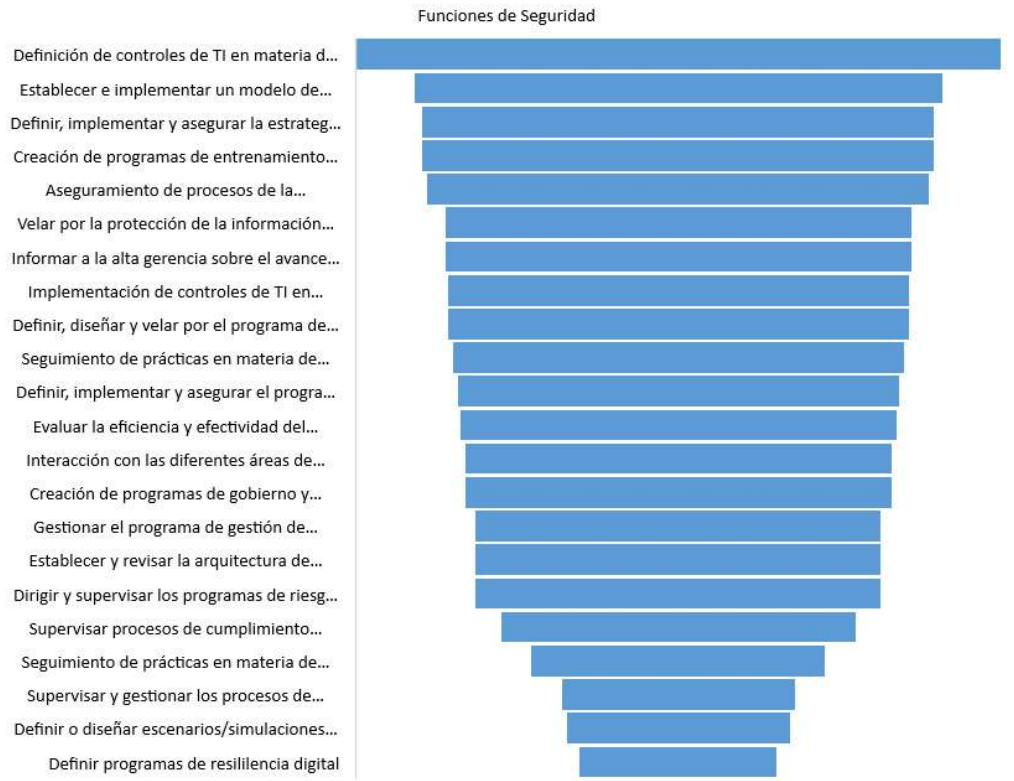


Gráfica 3. Cargos de los encuestados

cuentan oficiales de Seguridad de la información, profesionales del departamento de seguridad, asesor y consultor externo auditores internos.

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 acerca de lo que representa la ciberseguridad en sus organizaciones.

En la gráfica 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, seguido de establecer e implementar un modelo de políticas y en tercer lugar definir, implementar y asegurar la estrategia de ciberseguridad de la empresa.



Gráfica 4. Funciones del responsable de seguridad

Gráfica 5. Dependencia del área de Seguridad

La gráfica 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 35%, seguido por la Vicepresidencia/Director Departamento de Tecnologías de la Información 17% y en tercer lugar del Director/Jefe de Seguridad Informática 15%.

En la gráfica 6 se observan los roles dentro de una organización en materia de seguridad digital. El rol de analista de seguridad de la infor-

Gráfica 6. Roles de Seguridad

mación es el número 1, seguido de la posición CISO u Oficial de Seguridad de la Información y analista de seguridad informática.

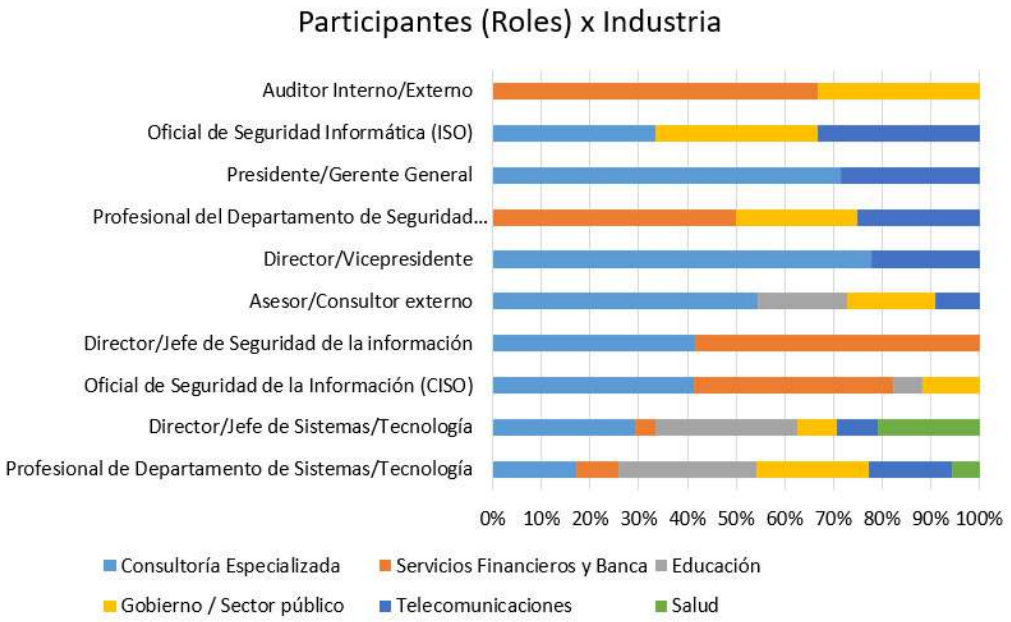
Consideraciones de los datos

Participación de la industria

Este año 2023, ha mantenido comparado con el 2022 una participación interesante de los profesionales de seguridad. Se sigue consolidando la encuesta de seguridad como un instrumento para entender la realidad nacional y en esa medida la participación de estos encuestados se mantiene.

Según las reuniones sostenidas en la agenda global del Foro Económico Mundial en Davos del 2023, se ha vuelto a manifestar que no importa el tamaño de las empresas, o el sector de industria, los riesgos cibernéticos afectan a las empresas y todas sin excepción están expuestas a lo inevitable, un ciberataque. Por tanto, la cooperación, colaboración y entendimiento de la realidad cibernética ya no es un lujo sino una necesidad que necesita de un ejercicios riguroso, constante y consistente, donde se estudie desde múltiples aristas como viene evolucionando el ecosistema digital y como el mismo adopta y fortalece sus esquemas de ciberseguridad en aras de desarrollar una mejor resiliencia.

Al revisar en la gráfica 7 la distribución de los cargos de los encuestados distribuidos en los sectores de



Gráfica 7. Roles x Sectores

la industria y los tamaños de las empresas, encontramos las siguientes consideraciones. En los sectores del Gobierno, Telecomunicaciones y Educación el rol que participa del instrumento es el profesional de las tecnologías de la información. En el sector de Salud participan más los directores de las áreas de tecnología, por su parte el sector financiero y el de consultoría es la figura de CISO y o directores de seguridad los que más participan.

Tendencia de participación que se ratifica al revisar reportes de industria como el informe anual de la Asociación de Control y Auditoría (ISACA) llamado "*State of Digital Trust 2023*" (ISACA, 2023) en donde el 26% de los participantes corresponden al sector financiero, 21% al sector de las tecnologías de la información y el 11% al sector del gobierno. Se puede concluir que estos instrumentos generan con el tiempo confianza de los participantes, puesto que ayudan a explorar con cada año de su realización la realidad del país y con ello ver las dinámicas y cambios en materia de seguridad digital en las empresas.

Roles, responsabilidades y funciones

Si bien es cierto que la función las dos funciones principales de los profesionales de seguridad se mantienen con el pasar del tiempo (definir controles de TI en materia de seguridad y establecer un modelo de políticas), existen pequeñas variaciones en las funciones.

Al revisar los datos por los diferentes sectores de la industria, si se pueden ver unas dinámicas interesantes propias de cada sector, entre los cuales se destacan:

1. A excepción del sector financiero, todos los sectores consideran como función principal que el profesional de seguridad se dedica a la "*Definición de controles de TI en materia de seguridad de la información*"; el sector gobierno es un caso especial pues en la primera posición comparte la función con la función "*Establecer e implementar un modelo de políticas en materia de seguridad de la información*"; contrario a todos los demás para el sector financiero la primera de las funciones es el "*Seguimiento de prácticas en materia de seguridad de la información*"; el sector de telecomunicaciones comparte el primer lugar con la función "*Velar por la protección de la información personal*".
2. En el caso de la segunda función más destacada hay variaciones interesantes, el sector de la consultoría considera que la "*Creación de programas de entrenamiento en materia de seguridad de la información*" ocupa la segunda posición, el sector educación considera a las funciones "*Aseguramiento de procesos de la organización y Definir, implementar y asegurar el programa*

de protección de datos personales de la empresa", que es razonable pues gran parte de la cantidad de datos que se manejan en estos sectores y una de sus funciones es preservar la privacidad, en donde el 44% de los profesionales y equipos de ciber/seguridad suministran información sobre la privacidad de los datos cuando esta es requerida (KPMG, 2023); el sector del gobierno la segunda función más importante la reparten entre "*Aseguramiento de procesos de la organización*"; el sector salud las variaciones entre las funciones son mínimas, pero la que resalta es "*Definir, implementar y asegurar la estrategia de ciberseguridad de la empresa";* el sector de telecomunicaciones considera que la función "Velar por la protección de la información personal", por último el sector financiero considera que la "*Definición de controles de TI en materia de seguridad de la información*" es su segunda función más importante.

3. La tercera función de importancia también tiene interesantes puntos de vistas, el sector de la consultoría considera que "*Definir, implementar y asegurar la estrategia de ciberseguridad de la empresa*"; el sector determina que la función en esta posición es "*Definir, implementar y asegurar el programa de protección de datos personales de la empresa*"; el sector del gobierno ve al "*Dirigir y supervisar los programas de riesgos de seguridad de la información de la organización*"; por su parte el sector de salud ve a la "*Implementación de controles de TI en materia de seguridad de la información";* mientras que el sector financiero considera al "*Establecer e implementar un modelo de políticas en materia de seguridad de la información*"; por último el sector de las telecomunicaciones considera que "*Definir, diseñar y velar por el programa de privacidad de la información de la organización*" que al igual que el sector salud, la información de sus clientes maneja información de datos personales que debe ser protegida, al revisar reportes de industria como (Proofpoint-Ponemon, 2023) e (ISACA, 2023) se ratifica que la protección de la privacidad es un fenómeno relevante para mejorar los ecosistemas digitales de las empresas.

Lo anterior muestra que cada sector de la industria está enfocando sus esfuerzos de acuerdo con sus niveles de madurez y la forma en cómo 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 2022 como lo mencionan informes de la industria (Verizon, 2023). La tabla 1, muestra la forma en como todas las funciones se visibilizan en los sectores principales.

Tabla 1. Distribución de responsabilidades por sectores

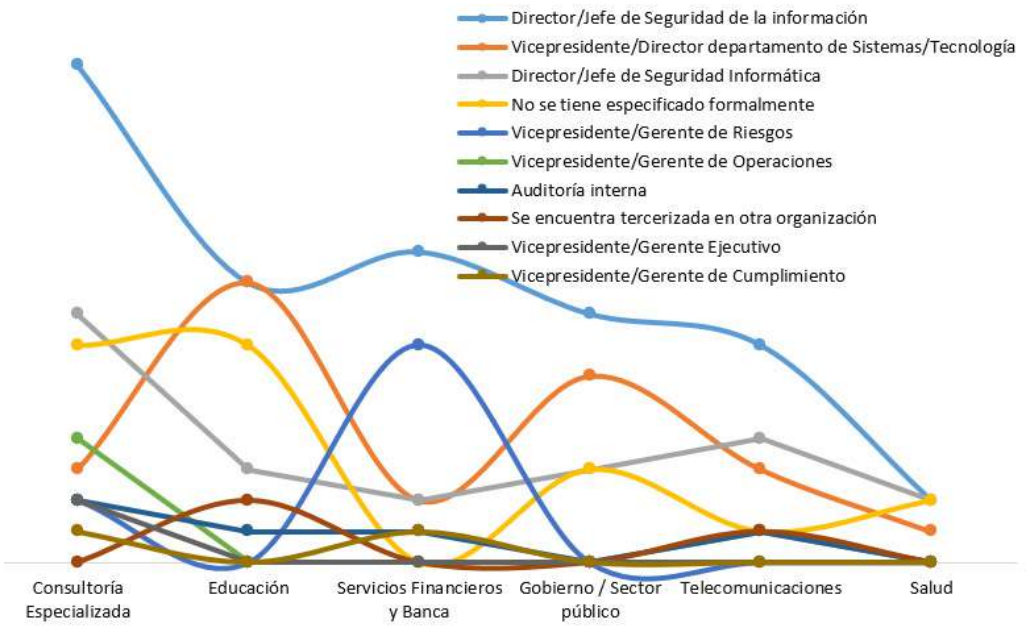
Valores	Consultoría Especializada	Educación	Gobierno / Sector público	Salud	Servicios Financieros y Banca	Telecomunicaciones
Definición de controles de TI en materia de seguridad de la información	17,44%	9,74%	6,15%	3,08%	8,72%	5,13 %
Establecer e implementar un modelo de políticas en materia de seguridad de la información	15,90%	6,67%	6,15%	2,05%	8,21%	3,08 %
Aseguramiento de procesos de la organización	13,85%	8,72%	5,13%	1,54%	8,21%	4,10 %
Definir, implementar y asegurar la estrategia de ciberseguridad de la empresa	16,41%	6,67%	3,59%	3,08%	7,18%	3,08 %
Creación de programas de entrenamiento en materia de seguridad de la información	16,92%	5,64%	3,59%	2,05%	7,69%	3,59 %
Definir, diseñar y velar por el programa de privacidad de la información de la organización	13,33%	7,18%	4,62%	2,56%	5,13%	4,62 %
Implementación de controles de TI en materia de seguridad de la información	12,82%	8,21%	4,62%	3,08%	4,10%	4,10 %
Velar por la protección de la información personal	11,79%	6,15%	4,10%	3,08%	6,15%	5,13 %
Definir, implementar y asegurar el programa de protección de datos personales de la empresa	10,77%	8,72%	4,62%	3,08%	5,13%	4,10 %
Seguimiento de prácticas en materia de seguridad de la información	13,33%	5,64%	3,08%	2,05%	9,23%	2,05 %
Informar a la alta gerencia sobre el avance del programa de seguridad de la información	13,33%	4,62%	3,08%	2,05%	7,69%	3,59 %
Evaluar la eficiencia y efectividad del modelo de seguridad de la información	13,85%	5,13%	4,10%	2,05%	6,15%	2,05 %
Dirigir y supervisar los programas de riesgos de seguridad de la información de la organización	13,33%	4,62%	5,13%	1,54%	7,18%	0,51 %
Creación de programas de gobierno y gestión en materia de seguridad de la información	14,87%	3,59%	2,05%	2,05%	6,67%	2,56 %
Establecer y revisar la arquitectura de seguridad de la información	11,79%	6,15%	2,05%	2,05%	7,18%	2,05 %
Interacción con las diferentes áreas de negocio	11,28%	4,10%	3,08%	2,05%	6,15%	4,10 %
Gestionar el programa de gestión de incidentes de seguridad de la información	11,79%	5,13%	4,10%	2,05%	6,15%	1,03 %
Supervisar procesos de cumplimiento regulatorio en tecnología de información	10,77%	3,59%	3,59%	2,56%	6,15%	2,05 %
Seguimiento de prácticas en materia de protección de la privacidad de la información personal	7,69%	5,64%	1,54%	1,03%	4,10%	3,08 %
Supervisar y gestionar los procesos de investigaciones forenses digitales	6,67%	3,59%	1,54%	1,54%	3,59%	1,03 %
Definir o diseñar escenarios/simulaciones/Playbooks en relación con ciberriesgos	4,62%	3,08%	1,54%	1,54%	3,59%	0,51 %
Definir programas de resiliencia digital	5,13%	3,08%	2,05%	1,03%	2,05%	0,51 %

Seguimos en un proceso de cambios y transformaciones que ha afianzado al trabajo remoto, los ambientes híbridos como realidades que se han plasmado en la vida de las personas y de las organizaciones, que han hecho que el profesional de seguridad tenga que repensar la forma en como desarrolla su función y que reta la práctica, en donde se hace necesario que nuevos aprendizajes y nuevas formas de visualizar el futuro sean posibles. No es posible aprender del futuro, si este no se visualiza en el presente y la realidad existente (Martínez, J., 2021).

Dependencia de la seguridad

Con el pasar de los años se ve a un área de seguridad mucho más empoderada y posicionada, los datos ratifican que hay mejoras en la dependencia de seguridad, que soportan la idea de un área que sigue su proceso de consolidación en las empresas.

Este año se ven cambios importantes frente al año inmediatamente anterior, por ejemplo, el sector salud a diferencia del año anterior muestra avances en la creación de áreas de seguridad y tener un director de esta para guiar todas las iniciativas de seguridad. La gráfica 8 muestra la distribución de los cargos en los distintos sectores de mayor representación, casos como el del sector educación que también hace mención que el área de seguridad depende directamente de las áreas de TI, y el sector salud que si



Gráfica 8. Sectores y roles

bien tiene director su segunda posición es ratificada la no existencia de un área para atender estos retos empresariales, muestra un poco la dinámica de madurez en los diferentes sectores. Los demás sectores a su ritmo van mostrando un área que tiene un director y que ejerce en propiedad en sus funciones.

Todos estos datos ratifican el crecimiento y aprendizajes que sigue teniendo el área de seguridad en las empresas, para la construcción de ecosistemas digitales confiables y por tanto posturas de seguridad acordes a la realidad y necesidad de las empresas. Este crecimiento es un soporte vital para la organización y para que paso a paso se siga interpretando a la seguridad como un instrumento que ayude al negocio. Directorios y Ejecutivos de la seguridad cada vez más tienen en su agenda y radar las amenazas cibernéticas (PwCb, 2023; NACD, 2023; Diligent Institute, 2023)

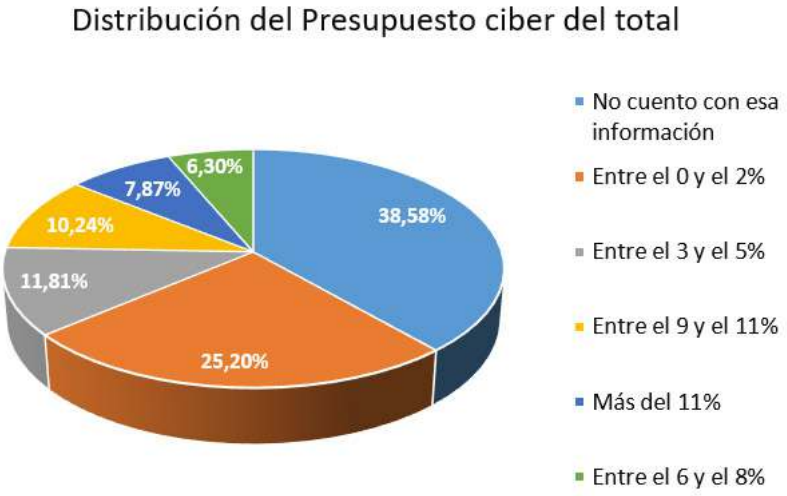
Mientras se siga avanzando en el desarrollo de la función de la seguridad en las organizaciones de Colombia como se viene dando, se seguirá mostrando unos aprendizajes que muy seguramente dejaran lecciones para optimizar y mejorar como igual se manifiesta en la tendencia mundial.

Presupuestos

Continúa la asignación de presupuestos para la ciberseguridad; en esta oportunidad el 73% manifiesta tener asignado un presupuesto de seguridad en la organización. Gráfica 9.

La gráfica 10 muestra el porcentaje que representa el presupuesto para la ciberseguridad del total del

Gráfica 9. Presupuesto de Seguridad

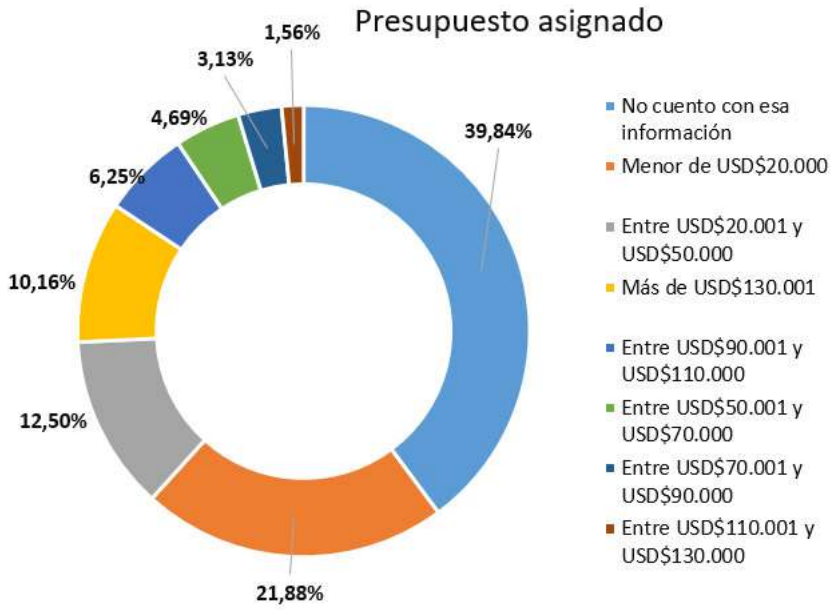


Gráfica 10. Porcentaje del presupuesto Global

presupuesto de la organización. Cerca del 64% de los encuestados lo conoce, mientras que el otro 38% 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 37%, mientras que el 22% están para los montos superiores al 5%. Entre el 0 y 2% representa un 25% mientras que entre 3 y el 5% representa el 12%, 8% es más del 11%, y entre el 9 y 11% es el 10%.

La gráfica 11 refleja los montos asignados en las organizaciones para la ciber-seguridad. Para este año cerca del 60% tiene un monto asignado para la seguridad; que aumenta, comparado con el año pasado cerca de un 13%, por su parte el 40% dice no conocer cuánto es el presupuesto asignado para la ciber-seguridad. Para este año cerca de un 22% dice que asigna menos de $US20.000 dólares americanos en sus presupuestos, seguido 13% que corresponde a la franja entre $US20.000 y $US-50.000; siguiente es el 10% que corresponde a los presupuestos por encima de $US130.000, el 6% asigna entre $US90.000 y $US-110.000, el 5% asigna entre $US-50.000 a $US70.000, 3% asigna entre $US70.000 a $US90.000 y 2% entre $US110.000 a $US-130.000 dólares americanos.

La gráfica 12 muestra la forma cómo se está invirtiendo el dinero en materia de ciberseguridad. El 48% invierte en la adquisición e implementación de tecnología de seguridad, el 39% invierte en renovación de licenciamiento, el 36% invierte en servicios de monitoreo y gestión, el 31% invierte en capacita-



Gráfica 11. Presupuesto de Seguridad

Gráfica 12. Inversión de Seguridad

ción del personal de seguridad y contratación de servicios de consultoría también tiene el 31%.

Consideraciones de los datos

Inversiones en ciberseguridad

Este año tiene consideraciones importantes que vale la pena resaltar, primero la forma en cómo se invierte el presupuesto por sectores de la industria y tamaño de las empresas; tenemos unas variedades de inversiones teniendo los siguientes elementos reflejados en la tabla 2.

Cuando se invierte más del 11% del presupuesto total de la organización sectores como el financiero y telecomunicaciones se resaltan más invirtiendo ambos en los ser-

Tabla 2. Inversiones de seguridad por sectores, presupuestos y montos

Distribución (Presupuesto - Franja) vs Sectores	Telecomunicaciones	Servicios Financieros y Banca	Salud	Gobierno / Sector público	Educación	Consultoría Especializada
Más del 11%						
Entre USD$50.001 y USD$70.000 Adquisición e implementación de tecnología de seguridad informática Renovación de licenciamiento y mantenimiento de hardware y software Servicios de monitoreo y gestión de seguridad con terceros				5,13% 5,88% 6,45%		
Entre USD$70.001 y USD$90.000 Adquisición e implementación de tecnología de seguridad informática Capacitación/Actualización del personal de seguridad de la información Renovación de licenciamiento y mantenimiento de hardware y software Servicios de monitoreo y gestión de seguridad con terceros		2,56% 4,35% 2,94% 3,23%				
Entre USD$90.001 y USD$110.000 Adquisición e implementación de tecnología de seguridad informática Renovación de licenciamiento y mantenimiento de hardware y software Servicios de monitoreo y gestión de seguridad con terceros						2,56% 2,94% 3,23%
Más de USD$130.001 Adquisición e implementación de tecnología de seguridad informática Capacitación/Actualización del personal de seguridad de la información	5,13% 4,35%	2,56% 4,35%				2,56% 4,35%

Contratación de servicios de asesoría/consultoría	4,55%	4,55%				
Renovación de licenciamiento y mantenimiento de hardware y software	5,88%	2,94%				
Servicios de monitoreo y gestión de seguridad con terceros	6,45%	3,23%				
Entre el 9 y el 11%						
Entre USD$110.001 y USD$130.000						
Renovación de licenciamiento y mantenimiento de hardware y software	2,94%					
Entre USD$20.001 y USD$50.000						
Adquisición e implementación de tecnología de seguridad informática						2,56%
Contratación de servicios de asesoría/consultoría						4,55%
Renovación de licenciamiento y mantenimiento de hardware y software						2,94%
Servicios de monitoreo y gestión de seguridad con terceros						3,23%
Entre USD$50.001 y USD$70.000						
Renovación de licenciamiento y mantenimiento de hardware y software						2,94%
Servicios de monitoreo y gestión de seguridad con terceros						3,23%
Entre USD$90.001 y USD$110.000						
Adquisición e implementación de tecnología de seguridad informática				2,56%		
Servicios de monitoreo y gestión de seguridad con terceros				3,23%		
Más de USD$130.001						
Adquisición e implementación de tecnología de seguridad informática					2,56%	
Capacitación/Actualización del personal de seguridad de la información					4,35%	
Contratación de servicios de asesoría/consultoría					4,55%	
Renovación de licenciamiento y mantenimiento de hardware y software					2,94%	
Servicios de monitoreo y gestión de seguridad con terceros					3,23%	
Menor de USD$20.000						
Adquisición e implementación de tecnología de seguridad informática						5,13%
Capacitación/Actualización del personal de seguridad de la información						8,70%
Contratación de servicios de asesoría/consultoría						4,55%
Renovación de licenciamiento y mantenimiento de hardware y software						2,94%
Servicios de monitoreo y gestión de seguridad con terceros						3,23%
Entre el 6 y el 8%						
Entre USD$20.001 y USD$50.000						
Adquisición e implementación de tecnología de seguridad informática	2,56%					5,13%
Capacitación/Actualización del personal de seguridad de la información	4,35%					
Contratación de servicios de asesoría/consultoría	4,55%					9,09%
Servicios de monitoreo y gestión de seguridad con terceros	3,23%					3,23%

Entre USD$70.001 y USD$90.000

Adquisición e implementación de tecnología de seguridad informática

Capacitación/Actualización del personal de seguridad de la información

Renovación de licenciamiento y mantenimiento de hardware y software

Servicios de monitoreo y gestión de seguridad con terceros

Entre USD$90.001 y USD$110.000

Adquisición e implementación de tecnología de seguridad informática

Contratación de servicios de asesoría/consultoría

Renovación de licenciamiento y mantenimiento de hardware y software

Servicios de monitoreo y gestión de seguridad con terceros

Menor de USD$20.000

Adquisición e implementación de tecnología de seguridad informática

Capacitación/Actualización del personal de seguridad de la información

Contratación de servicios de asesoría/consultoría

Renovación de licenciamiento y mantenimiento de hardware y software

Entre el 3 y el 5%

Entre USD$20.001 y USD$50.000

Adquisición e implementación de tecnología de seguridad informática

Capacitación/Actualización del personal de seguridad de la información

Contratación de servicios de asesoría/consultoría

Renovación de licenciamiento y mantenimiento de hardware y software

Servicios de monitoreo y gestión de seguridad con terceros

Entre USD$50.001 y USD$70.000

Renovación de licenciamiento y mantenimiento de hardware y software

Servicios de monitoreo y gestión de seguridad con terceros

Entre USD$70.001 y USD$90.000

Adquisición e implementación de tecnología de seguridad informática

Capacitación/Actualización del personal de seguridad de la información

Menor de USD$20.000

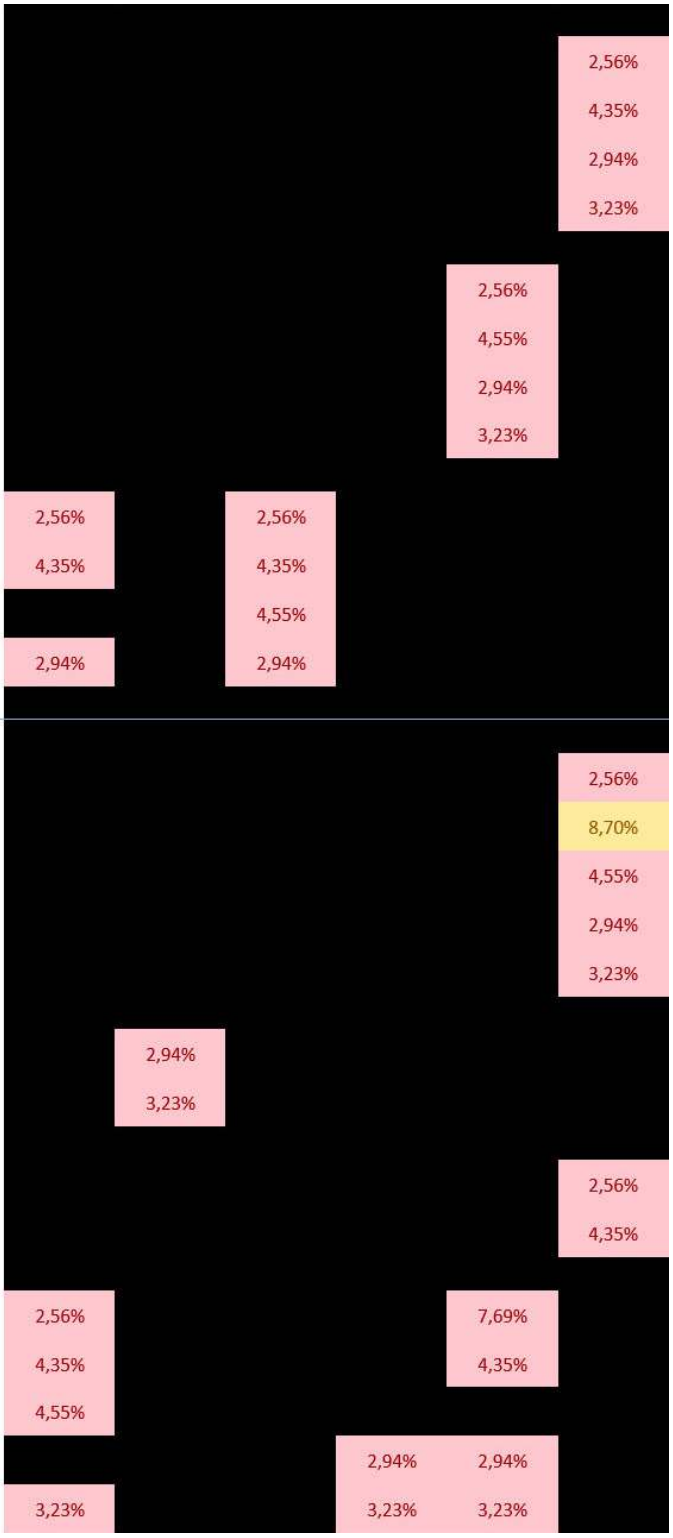
Adquisición e implementación de tecnología de seguridad informática

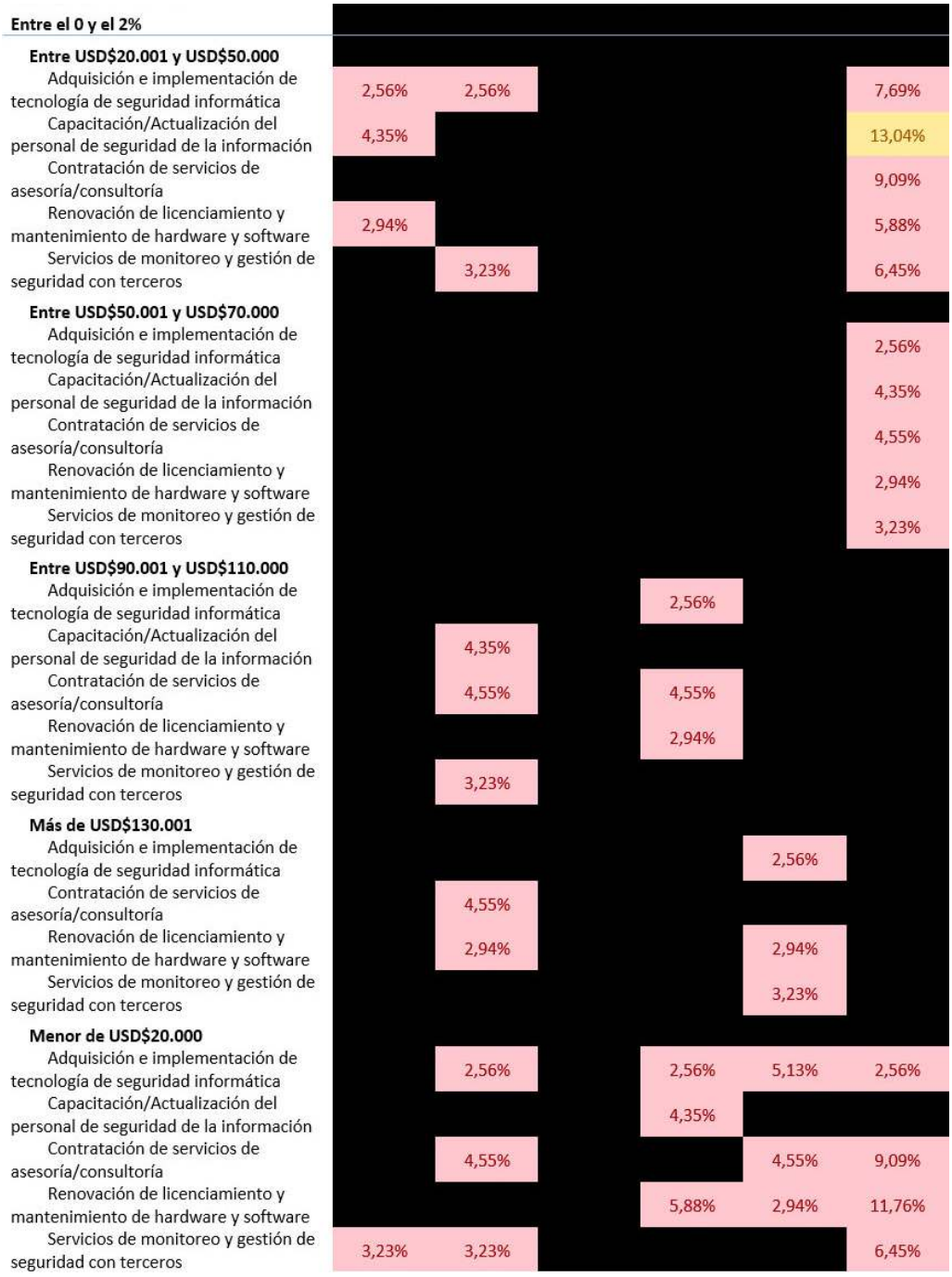
Capacitación/Actualización del personal de seguridad de la información

Contratación de servicios de asesoría/consultoría

Renovación de licenciamiento y mantenimiento de hardware y software

Servicios de monitoreo y gestión de seguridad con terceros





vicios de monitoreo y gestión de seguridad con terceros, sin embargo, el sector financiero solo invierte entre $US50.000 y $US70.000 dólares americanos mientras que el de las telecomunicaciones invierte más de $US 130.000 dólares americanos.

Cuando se invierte entre el 9 y el 11% del presupuesto global, el sector que resalta es el de la consultoría especializada que invierte menos de $US20.000 dólares en capacitación y/o actualización del personal de seguridad de la información.

Cuando se invierte entre el 6 y 8% del presupuesto global, el sector de la consultoría especializada nuevamente es el que invierte más en la franja de los $US20.000 a $US 50.000 dólares en servicios de contratación de servicios de asesoría/consultoría.

Entre el 3 y el 5 % del presupuesto global tiene un comportamiento similar, es el sector de consultoría especializada que invierte más en la franja de los $US20.000 a $US 50.000.

Por último, en la franja del 0 al 2% del presupuesto global es la capacitación del personal de seguridad el rubro de inversión más alto, que a su vez lo hace el sector de la consultoría especializada.

Hay consideraciones importantes en la tabla 3 que podría ser un resumen diciendo que cerca del 40% de los encuestados manifiestan no conocer el presupuesto que se asigna para la ciberseguridad, que, al explorar los datos, es indistinto del rol o cargo que desempeñe, esto es interesante porque sugiere que no son los CISOS o responsables de seguridad los que asignan o definen los presupuestos, sino

Tabla 3. Inversiones de seguridad por sectores

Sectores	No cuento con esa información	Menor de USD$20.000	Entre USD$20.001 y USD$50.000	Más de USD$130.001	Entre USD$50.001 y USD$70.000	Entre USD$90.001 y USD$110.000	Entre USD$70.001 y USD$90.000	Entre USD$110.001 y USD$130.000
Consultoría Especializada	8,00%	7,00%	8,00%	1,00%	2,00%	1,00%	3,00%	
Servicios Financieros y Banca	8,00%	1,00%	2,00%	2,00%	1,00%	2,00%	1,00%	
Telecomunicaciones	6,00%	5,00%	2,00%	3,00%				1,00%
Educación	8,00%	5,00%		2,00%		1,00%		
Gobierno / Sector público	7,00%	3,00%			2,00%	2,00%		
Salud	3,00%	1,00%		1,00%	1,00%			
Total, general	**40,00%**	**22,00%**	**12,00%**	**9,00%**	**6,00%**	**6,00%**	**4,00%**	**1,00%**

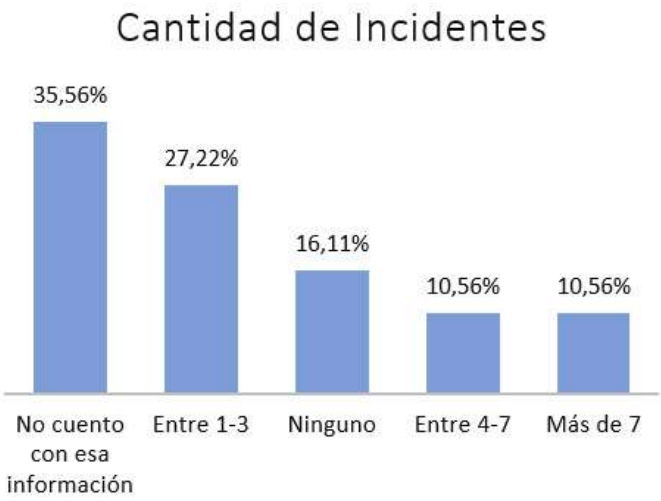
otras áreas en las mismas empresas. De los que indican conocerlo, el 22% advierte que sus presupuestos de seguridad están por debajo o igual a $US20.000 dólares, que puede ser un comportamiento normal frente a los vientos de contracción de mercados y posible recesión con la que comenzó el año 2023 (PwC, 2023; EY, 2023) y en esa misma línea el sector que más invierte en esa franja es el sector de la consultoría especializada. La segunda franja más usada en inversiones está entre $US20.000 y $US 50.000, que al igual que la anterior es el sector de la consultoría especializada, el que más se mueve en esta franja y le sigue la banda de inversión por encima de los $US 130.000 en el que el sector de las telecomunicaciones es el que se resalta.

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, 2023).

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 encuesta no tenga acceso a dicha información.

Incidentes

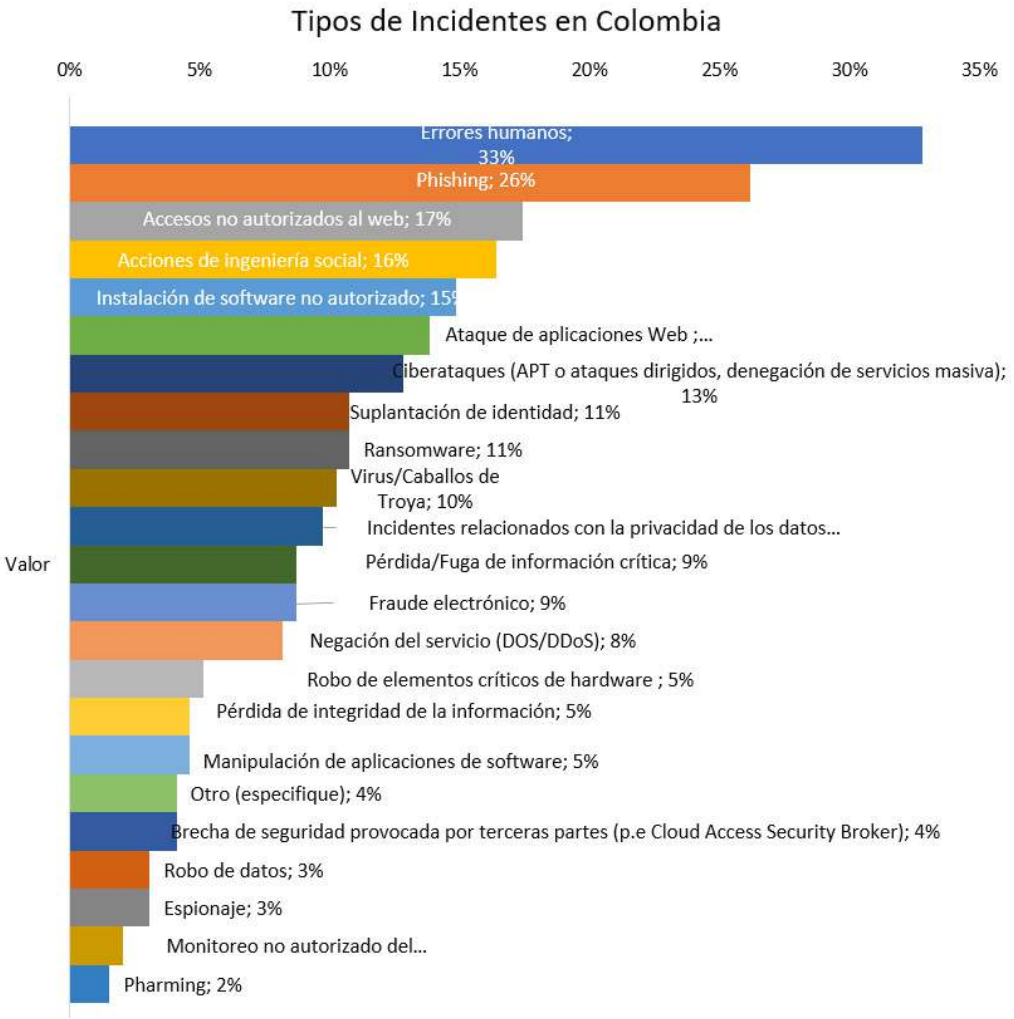
La gráfica 13 representa la cantidad de incidentes que para este



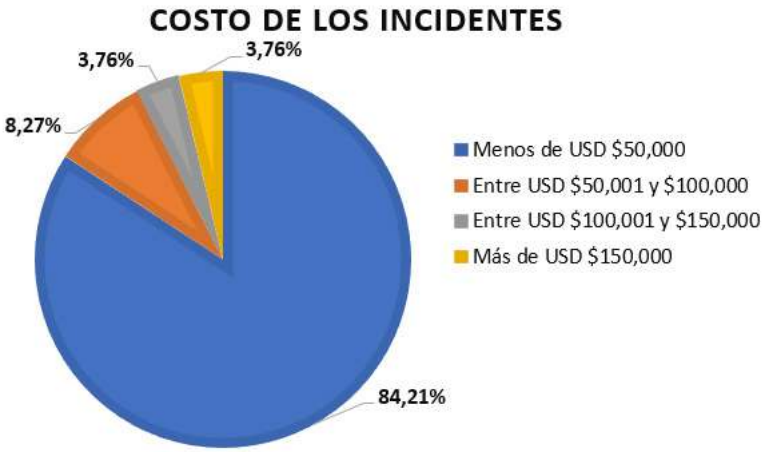
Gráfica 13. Cantidad de Incidentes

año los encuestados manifestaron que se presentaron. Para este año cerca del 48% 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 56% lo ha manifestado. El 36% manifiesta no tener información al respecto de los incidentes en sus organizaciones, al revisar los detalles se encuentra que el 27% manifiesta haber experimentado entre 1 y 3 incidentes, tanto para los que expresan que han experimentado entre 4 y 7 incidentes, como los que han experimentado más de 7 incidentes el valor es cerno al 11%.

La gráfica 14 relaciona los tipos de incidentes que se presentaron en



Gráfica 14. Tipos de Incidentes de Seguridad



Gráfica 15. Costos de los Incidentes

las organizaciones, Errores humanos (33%), Phishing (26%) y accesos no autorizados al web (17%) son los tres primeros que han sido identificados en este año. Si bien comparados con el año pasado disminuyen un poco todos los valores los cambios no son significativos para decir que hay un cambio de tendencia.

La gráfica 15 representa el costo promedio de los incidentes cibernéticos en las empresas colombianas, el 84% manifiesta que los costos estimados totales luego de sufrir un incidente están por debajo de los $US50.000 dólares americanos, entre $US50.000 y $US 100.000 solo el 8%, más de $US 150.000 el 4% y entre $US100.000 y $US150.000 dólares americanos el 4%

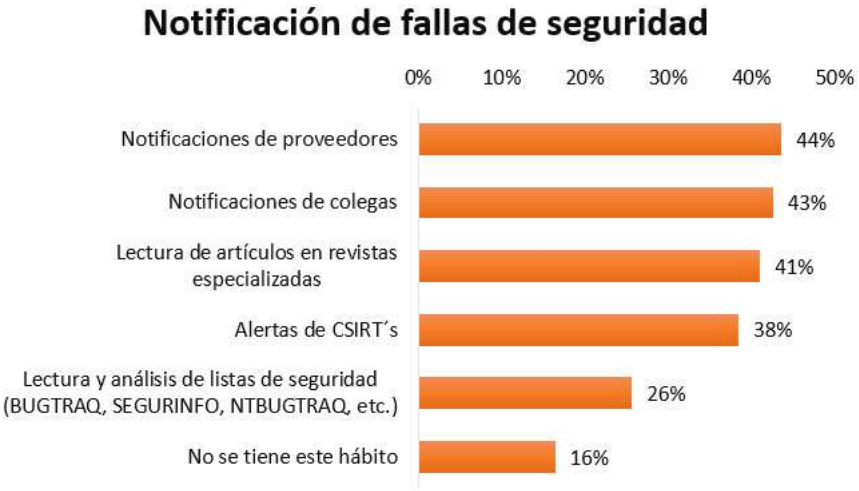
La gráfica 16, muestra ante quién se reportan los incidentes de seguridad. El 64% lo reporta directamente a los directivos de la organización, el 38% lo reporta al equipo de atención de incidentes (CSIRT), el 34% a las autoridades nacionales, el 32% a los asesores legales, el 17% a autoridades locales o regionales y solo el 5% manifiesta que no se denuncian. Para este año hubo más reporte hacia los directivos un aumento del 3% y una disminución del 4% de reportes ante los CSIRT, otro dato interesante es el aumento de más del 10% en incremento en reporte de incidentes a los asesores legales, y se mantiene en el 5% igual aquellos que no dicen nada o no notifican nada de sus incidentes.

La gráfica 17, muestra como los profesionales de ciberseguridad se mantienen informados sobre las vulnerabilidades y fallas de los sistemas. El 44% de los profesionales de seguridad se enteran a través de

Gráfica. 16 A quien se reportan los incidentes

sus proveedores en primera medida, seguido de la notificación de colegas con un 43%, la lectura de artículos especializados o revistas un 41% de las veces es usado para enterarse de las anomalías digitales, las alertas de un CSIRT el 38% de las veces el 26% de los casos es a través de listas de seguridad y solo el 16% no tiene ese hábito.

Comparado con el año pasado hay unos drásticos cambios; es la primera vez que los profesionales estrechan sus relaciones de confianza con sus aliados (proveedores) y son informados por estos sobre las anomalías digitales; el otro cambio drástico es el descenso vertiginoso de los CSIRT en este ejercicio.



Gráfica. 17 Notificación de incidentes

Contacto con autoridades	Porcentaje
No	44,03%
Si	55,97%

La tabla 4 se resalta que el 56% de las personas encuestadas si tienen contacto con las autoridades, mientras que el 44% no lo posee.

En cuanto la evidencia digital, los datos muestran que, 71% de los encuestados si es consciente del manejo de la evidencia digital y que es requerida como parte del proceso de la gestión de incidentes, el 28% está dividido en partes iguales para los que no saben y los que no son conscientes de la evidencia y su manejo como parte del proceso de incidentes.

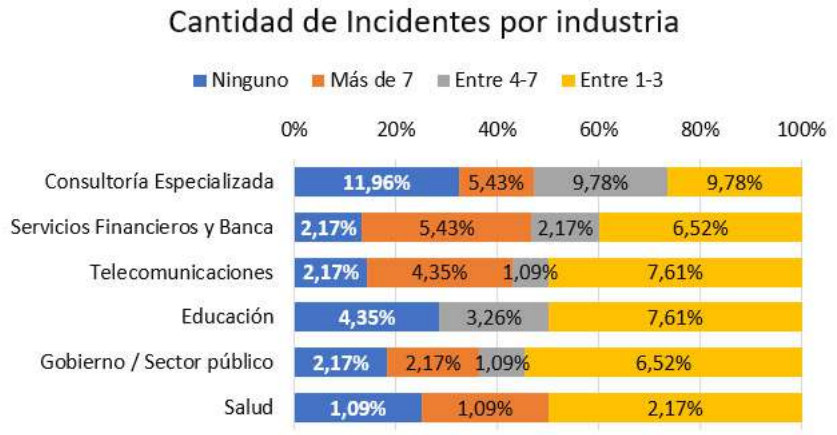
Al revisar qué tanto de esa consciencia se lleva a la práctica encontramos que el 46% manifiesta tener un procedimiento formal y establecido para la gestión de incidentes y un 54% no. Para este año se indago por la implementación de dicho procedimiento encontrando que solo el 65% de lo que lo tienen aprobado lo han implementado formalmente, los informales rondan el 17%, el 10% no lo han hecho y el 8% restante no sabe si eso se ha implementado.

Consideraciones de los datos

Frecuencias de los incidentes

Explorando la forma como experimentan en Colombia los diferentes sectores de la industria los distintos incidentes, la gráfica 18, muestra cómo los distintos sectores sufren las distintas franjas de incidentes.

Lo primero para resaltar es que todos los sectores más representativos y los otros sectores experi-



Gráfica 18. Cantidad de Incidentes por sectores

mentan incidentes cibernéticos, tendencia que se confirma a través de reportes como (Verizon, 2023) (CyberEdge, 2023), (Cano & Almanza, 2021).

Llama la atención en el sector de la consultoría especializada, que su valor más alto esté relacionado con no manifestar incidentes, aspecto que puede tener dos lecturas, una pobre capacidad para gestionar y tratar incidentes (SecureWorks, 2023), o unas escalas inadecuadas en la clasificación y triage de los incidentes (CheckPoint, 2023), (Magnet, 2023).

Al revisar con detalle estos datos, la tabla 5, los muestra por sectores, tamaños de empresas y la cantidad de estos, de los cuales se puede decir.

Y en que invierten sus recursos financieros asignados de presupuesto a los desafíos que presenta la ciber-seguridad, la tabla 5, resalta la cantidad de incidentes que se presentan en los diferentes sectores de industria y adicional los relaciona por el tamaño de la empresa.

Al revisar la tabla, vemos el top 5 (Resaltado en rojo) que contiene lo siguiente son las empresas muy pequeñas del sector de la consultoría especializada las que manifiestan no tener incidentes, llama la atención que las empresas grandes (1001-5000) empleados del mismo sector manifiesten que no tienen incidentes, interesante ver que la proporción mayor de 4 incidentes hacia arriba en las empresas pequeñas sea en suma mucho

Tabla 5. Distribución de incidentes por sectores y tamaños

Sectores/Tamaños	Ninguno	Más de 7	Entre 4-7	Entre 1-3
Consultoría Especializada				
1 - 50 empleados	5,43%	3,26%	4,35%	2,17%
1001 - 5000 empleados	3,26%		1,09%	
201 - 500 empleados		1,09%		3,26%
501 - 1000 empleados			2,17%	2,17%
51 - 200 empleados	2,17%	1,09%	2,17%	1,09%
Mayor de 5001 empleados	1,09%			1,09%
Servicios Financieros y Banca				
1 - 50 empleados		1,09%		
1001 - 5000 empleados		1,09%		1,09%

201 - 500 empleados	1,09%	1,09%	1,09%	3,26%
501 - 1000 empleados	1,09%			
51 - 200 empleados			1,09%	1,09%
Mayor de 5001 empleados		2,17%		1,09%
Educación				
1001 - 5000 empleados			2,17%	2,17%
201 - 500 empleados	1,09%			1,09%
501 - 1000 empleados	1,09%			3,26%
51 - 200 empleados	1,09%			
Mayor de 5001 empleados	1,09%		1,09%	1,09%
Telecomunicaciones				
1 - 50 empleados	2,17%	2,17%		2,17%
1001 - 5000 empleados				2,17%
501 - 1000 empleados		1,09%	1,09%	1,09%
51 - 200 empleados		1,09%		1,09%
Mayor de 5001 empleados				1,09%
Gobierno / Sector público				
1001 - 5000 empleados		2,17%		2,17%
201 - 500 empleados				2,17%
501 - 1000 empleados	1,09%		1,09%	1,09%
51 - 200 empleados	1,09%			1,09%
Salud				
1001 - 5000 empleados		1,09%		1,09%
201 - 500 empleados	1,09%			
51 - 200 empleados				1,09%

mayor a las que dicen no tenerlos cerca del 8% en comparación con el 5%, el patrón de comportamiento en los sectores de la industria se mantiene donde es entre 1 a 3 incidentes es la constante y en las empresas entre 200 a 1000 de todos los sectores se manifiestan incidentes de toda naturaleza.

No todas las verticales empresariales en Colombia tiene los mismos tipos de incidentes; la tabla 6 muestra dos visiones. la primera vi-

sión resalta el top 3 de tipos de incidentes por sector, la segunda parte resalta el top 1 en materia del tipo de incidente del total de veces que se presenta.

De las tablas se pueden resaltar los siguientes aspectos:

1. Todos los sectores de la industria nacional sufren algún tipo de ciber incidente.
2. El top 5 de los incidentes de todas las industrias son Errores humanos, phishing, acceso no autorizado al web, instalación de software no autorizado y los ata-

Tabla 6. Tipos de incidentes x industria

	Visual por Sectores Empresariales (Top 3) lectura vertical						Visual por tipo de Incidentes (Top 1) lectura horizontal					
Tipos de Incidentes	**Telecomunicaciones**	**Servicios Financieros y Banca**	**Salud**	**Gobierno / Sector público**	**Educación**	**Consultoría Especializada**	**Telecomunicaciones**	**Servicios Financieros y Banca**	**Salud**	**Gobierno / Sector público**	**Educación**	**Consultoría Especializada**
Errores humanos	10%	13%	25%	17%	14%	17%	8%	14%	6%	11%	16%	34%
Phishing	8%	15%	13%	12%	10%	9%	8%	22%	4%	10%	14%	24%
Accesos no autorizados al web	13%	4%	6%	7%	13%	6%	18%	9%	3%	9%	26%	21%
Instalación de software no autorizado	6%	3%	13%	7%	7%	8%	10%	7%	7%	10%	17%	34%
Acciones de ingeniería social	6%	7%	13%	5%	6%	6%	9%	16%	6%	6%	13%	25%
Ataque de aplicaciones Web	8%	4%		7%	11%	5%	15%	11%		11%	30%	22%
Ciberataques (APT o ataques dirigidos, denegación de servicios masiva)	10%	3%		5%	3%	6%	20%	8%		8%	8%	32%
Suplantación de identidad	2%	8%	6%	2%	6%	4%	5%	29%	5%	5%	19%	24%
Virus/Caballos de Troya	2%	3%		7%	8%	5%	5%	10%		15%	30%	30%
Ransomware	6%	4%		5%	1%	6%	14%	14%		10%	5%	33%
Incidentes relacionados con la privacidad de los datos personales	2%	4%	6%	2%	7%	3%	5%	16%	5%	5%	26%	21%
Pérdida/Fuga de información crítica	6%	6%	6%	7%		3%	18%	24%	6%	18%		24%
Negación del servicio (DOS/DDoS)	6%	3%		2%	7%	3%	19%	13%		6%	31%	25%
Fraude electrónico	2%	6%		5%	1%	3%	6%	24%		12%	6%	24%
Robo de elementos críticos de hardware	2%	1%	6%	2%		4%	10%	10%	10%	10%		50%
Pérdida de integridad de la información		3%		2%	1%	4%		22%		11%	11%	56%
Manipulación de aplicaciones de software		4%		2%		2%		33%		11%		22%
Brecha de seguridad provocada por terceras partes (p.e Cloud Access Security Broker)	4%	3%			1%	1%	25%	25%			13%	13%
Espionaje	2%	1%	6%		1%	2%	17%	17%	17%		17%	33%
Robo de datos	2%	1%			1%	2%	17%	17%			17%	33%
Monitoreo no autorizado del tráfico		1%				2%		25%				75%
Pharming		3%			1%			67%			33%	

ques de ingeniería social como lo más representativo.

3. Los errores humanos es el incidente que es común a todos los sectores.
4. Phishing es el segundo, sin embargo, no es el más presente en todos los sectores.
5. Al revisar sector por sector encontramos particularidades (Tabla 6 primera parte). Para el caso del sector de telecomunicaciones el incidente top 1, es acceso no autorizado al web, en el sector financiero es el Phishing, en los sectores de salud, gobierno, educación y consultoría especializada es el error humano el incidente número 1.
6. Al revisar la parte 2 de la tabla que está categorizada por la presencia del tipo de incidentes y su distribución en los distintos sectores, se encuentran cosas interesantes. En el sector salud, encontramos como los ataques de denegación de servicios y todas las afectaciones a las aplicaciones web y accesos no autorizados tiene fuerte presencia. El sector de la consultoría especializada menciona que todos los incidentes tienen presencia en su sector. El pharming, suplantación de identidad fraude electrónico y fuga de información incidentes que marcan presencia importante. El sector de telecomunicaciones muestra un interesante comportamiento pues son las brechas de seguridad de terceros particularmente lo que está asociado al cloud computing lo que se resalta como incidente importante.

Las tendencias de Colombia en materia de la presencia de los incidentes cibernéticos no se alejan de las tendencias internacionales, por una parte, los errores humanos se han resaltados en reporte de industria como, donde la variedad de técnicas novedosa que usan los adversarios digitales pone demasiada presión en las personas y los inducen en muchos casos a errores (Proofpoint(a), 2023; FS-ISAC, 2023).

Para el caso del Phishing es uno de los fenómenos más estudiados y analizados por distintos especialistas de la industria, el reporte de Verizon (Verizon, 2023; FBI, 2023) manifiesta que el 74% de las brechas de seguridad donde se involucran datos, también tienen involucradas personas, en ese sentido la firma Knowbe4 resalta de los estudios de pruebas de phishing realizadas que más del 33% de las personas no entrenada no pasaran las pruebas de phishing (Knowbe4, 2023; Proofpoint(c), 2023). La fundación de investigación en seguridad informática revela que de 1466 dominios analizados entre abril y mayo del 2023 el 26% fueron phishing (Finsin, 2023). Barracuda networks en su informe resalta que el 50% de las empresas fueron víctimas de Spear Phishing, de la misma manera manifiesta que una empresa normal recibe 5 emails de Spear phishing muy personalizados por día

(Barracuda, 2023), (Barracuda(b), 2023). Zscaler en su reporte resalta que el incremento de los ataques de phishing desde el 2021 al 2022 creció cerca de un 47% (Zscaler, 2023). En el compendio de análisis de industria se resalta que los ataques de phishing que buscan credenciales crecen un 527% (Cofense, 2023).

La ingeniería social como otra de las técnicas usadas es una tendencia global, donde las víctimas usan la conversación para construir confianza y se valen de cualquier método para poder engañar a sus víctimas y son los temas de la actualidad, relevancia y los que socialmente conectan los que son más usados (Proofpoint(d), 2023).

Para el caso de las fallas de aplicaciones y dada las tendencias globales o megatrends del Web 3.0 como una realidad innegable donde las APIs y las aplicaciones son la norma (HCLTech, 2023), lo cual también está aunado a la presencia del cloud computing como un apalancador de ambientes digitales en donde se expanden o extienden los riesgos de manera natural (ArticWolf, 2023). El 75% de los responsables de seguridad están algo preocupados por la cantidad de vulnerabilidades y amenazas por las aplicaciones en ambientes productivos (Dynatrace, 2022). El 32% de las aplicaciones han tenido ataques de DDos durante el 2022 en su último cuarto (Indusface, 2022). Solo el 2% confía en las estrategias de defensas para proteger sus aplicaciones y sobre todo en la nube (Opswat, 2023).

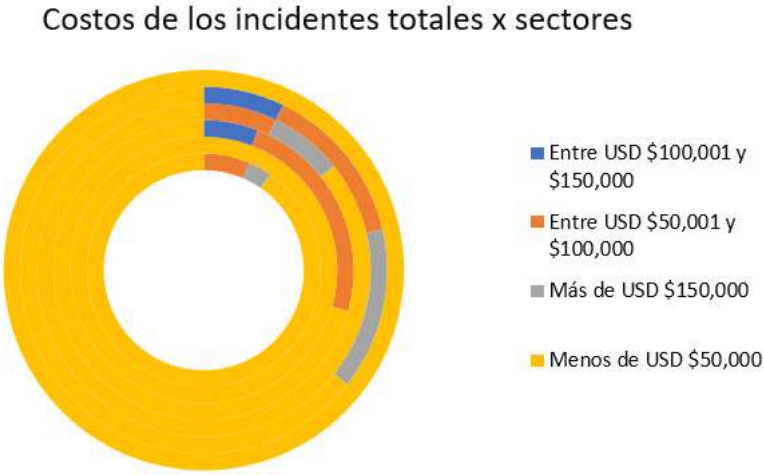
Muchos de los eventos del año 2022 (PwCc, 2022) han sido precedente para que el 2023 sea un año donde se tenga mayor atención a la presencia de los eventos cibernéticos que marcan a las organizaciones no solo a nivel internacional, sino nacional también.

Costos de los incidentes

Los costos de los incidentes tienen un comportamiento y cada vez que hay en los distintos sectores de la industria colombiana nuevos patrones que muestran la dinámica de cómo son estos, y cuáles son sus costos. La gráfica 19, representa los costos de los incidentes por sectores de industria, cada anillo es un sector de industria y en él se muestra la distribución de las franjas de valores económicos de los mismos.

Del cual se puede extraer lo siguiente:

1. Más del 90% de los costos asociados a un incidente cibernético están por debajo de los $US 50.000 dólares, una cifra no menor para el valor del peso colombiano, en una aproximado cercano en pesos de 200.000 millones de pesos colombianos haciendo el cálculo de una tasa representativa de 4.000 pesos.
2. A excepción del sector salud y educación, todos los demás sec-

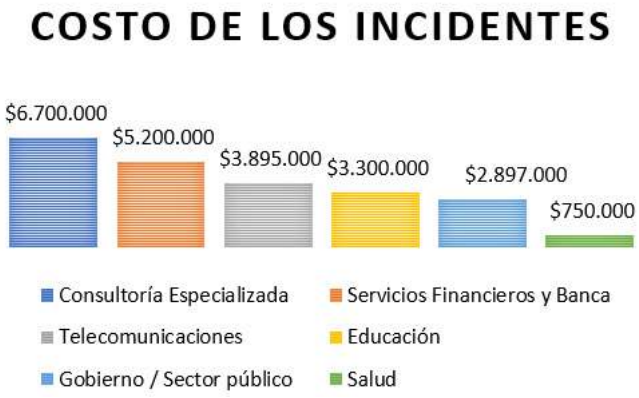


Gráfica 19. Costos de incidentes por industria

tores representativos (telecomunicaciones, financiero, gobierno y consultoría) tienen incidentes con costos en las demás bandas indagadas. Casos como el sector de telecomunicaciones donde tiene incidentes en todas las bandas.

3. Se resalta qué en comparación con los demás sectores, el sector financiero tiene menos incidentes de montos mayores de $US 50.000 dólares, comparado con los demás sectores representativos, mientras que el sector financiero solo tiene dos incidentes por encima de los $50.000 dólares, el sector de telecomunicaciones y gobierno tienen 5, y la consultoría especializada tiene 3.

Para este año analizando los datos recolectados, se ha determinado el



Gráfica 20. Costos de los incidentes x sectores de industria

costo total aproximado de los incidentes por sector de la industria, el cual se refleja en la gráfica 20. En ella se resalta que un promedio aproximado de los 22 tipos de incidentes que mide la encuesta le costó al sector de la consultoría especializada en dólares americanos cerca de $US 6.7 millones, al sector financiero le costó un estimado de 5.2 millones, al sector de las telecomunicaciones 3,9 millones de dólares al sector de educación 3,3 millones, al sector del gobierno sus costos pudieron llegar a cerca de 2,9 millones y por último al sector salud cerca de 750 mil dólares americanos.

La gráfica 21, muestra la distribución de los costos por tipo de incidente, en el cual tenemos que los errores humanos es el incidente que más les cuesta a las empresas colombianas en un total aproximado de $US 3,650.000, phishing seguido con 2.848.000 mil dólares, acceso no autorizado al web $US-1.850 millones.

Al revisar o decepcionar estos costos por sectores de la industria en los tipos de incidentes analizados, también se encuentran variaciones importantes, reflejadas en la tabla 7.

Gráfica 21. Costos totales por tipo de incidente

Tabla 7. Costos x tipo de incidentes en los sectores empresariales

Tipos de Incidentes	Telecomunicaciones	Servicios Financieros y Banca	Salud	Gobierno / Sector público	Educación	Consultoría Especializada
Errores humanos	$ 350.000	$ 600.000	$ 200.000	$ 450.000	$ 450.000	$ 1.100.000
Phishing	$ 349.000	$ 600.000	$ 50.000	$ 300.000	$ 300.000	$ 550.000
Accesos no autorizados al web	$ 350.000	$ 300.000	$ 50.000	$ 150.000	$ 400.000	$ 350.000
Acciones de ingeniería social	$ 150.000	$ 350.000	$ 100.000	$ 150.000	$ 200.000	$ 500.000
Ataque de aplicaciones Web	$ 350.000	$ 150.000	$ -	$ 200.000	$ 350.000	$ 350.000
Instalación de software no autorizado	$ 200.000	$ 150.000	$ 100.000	$ 200.000	$ 250.000	$ 500.000
Ciberataques (APT o ataques dirigidos, denegación de servicios	$ 399.000	$ 250.000	$ -	$ 199.000	$ 100.000	$ 450.000
Ransomware	$ 299.000	$ 300.000	$ -	$ 249.000	$ 50.000	$ 350.000
Suplantación de identidad	$ 150.000	$ 350.000	$ 50.000	$ 100.000	$ 200.000	$ 250.000
Pérdida/Fuga de información crítica	$ 300.000	$ 250.000	$ 50.000	$ 150.000	$ -	$ 300.000
Virus/Caballos de Troya	$ 50.000	$ 150.000	$ -	$ 249.000	$ 250.000	$ 300.000
Negación del servicio (DOS/DDoS)	$ 299.000	$ 100.000	$ -	$ 50.000	$ 250.000	$ 200.000
Incidentes relacionados con la privacidad de los datos personales	$ 50.000	$ 150.000	$ 50.000	$ 100.000	$ 250.000	$ 200.000
Fraude electrónico	$ 50.000	$ 250.000	$ -	$ 200.000	$ 50.000	$ 200.000
Robo de elementos críticos de	$ 149.000	$ 100.000	$ 50.000	$ 50.000	$ -	$ 250.000
Pérdida de integridad de la	$ -	$ 250.000	$ -	$ 50.000	$ -	$ 250.000
Brecha de seguridad provocada por terceras partes (p.e Cloud Access	$ 150.000	$ 150.000	$ -	$ -	$ 50.000	$ 100.000
Espionaje	$ 150.000	$ 100.000	$ 50.000	$ -	$ 50.000	$ 100.000
Robo de datos	$ 100.000	$ 100.000	$ -	$ -	$ 50.000	$ 150.000
Manipulación de aplicaciones de	$ -	$ 200.000	$ -	$ 50.000	$ -	$ 100.000
Pharming	$ -	$ 250.000	$ -	$ -	$ 50.000	$ -
Monitoreo no autorizado del tráfico	$ -	$ 100.000	$ -	$ -	$ -	$ 150.000

De la tabla anterior se pueden determinar los siguientes puntos:

1. Al sector de la consultoría especializada es al que más le cuesta los errores humanos, en relación con los demás sectores.
2. En el sector de las telecomunicaciones los ciberataques avanzados son los que más cuestan.
3. En el sector financiero se puede observar que son los clientes a quienes van mayormente dirigidos los ataques, phishing, ingeniería social y la identidad están dentro de los incidentes con mayores costos.
4. En el sector de gobierno el ransomware y el malware tradicional hace parte de la batería de incidentes que más se presentan.
5. En el sector de la educación el acceso no autorizado a sus aplicaciones web es el segundo incidente con mayores costos.

En el gráfico 23, se tiene la distribución normal de los incidentes cibernéticos de todos los sectores analizados. Hoy se puede afirmar con los datos obtenidos de la encuesta, que los incidentes cibernéticos en promedio le pueden costar a una empresa entre 50.000 dólares americanos y cerca de 3.8 millones de dólares, siendo la franja de $200.000 dólares hasta $US 2.700.000 millones de dólares el costo en el que más oscila los incidentes cibernéticos en la industria nacional. Cabe mencionar que estos valores no son para un solo incidente sino la presencia de varios en las distintas industrias.

En este año al mezclar los datos de costos de incidentes vs inversiones del presupuesto global (Tabla 8), se puede determinar que las empresas que hacen menores inversiones tienen mayor probabilidad sin importar el tamaño, o el sector de evidenciar entre 1 a 3 incidentes, siendo esta la franja más probable, en la medida que se invierta más se puede disminuir la tasa de presencia de incidentes, sin embargo, no es que no se presenten ninguno de ellos.

Aquellos que invierten entre el 0 y 2% del total de su presupuesto para la ciberseguridad tienen un 36% más de probabilidad de que un incidente se presente, y exactamente un 24% que se presente entre 1 y 3 incidentes en las empresas de Colombia, si se revisa las otras franjas, lo que se puede ver es que en la medida que incremente las empresas su inversión en seguridad, disminuye en 2,3 y hasta 4 veces la posibilidad de que un incidente que se va presentar cueste menos de $US 50.000 dólares americanos. Es importante manifestar que invertir en seguridad no evitará que los incidentes no pasen, solo harán

Distribución de los incidentes cibernéticos

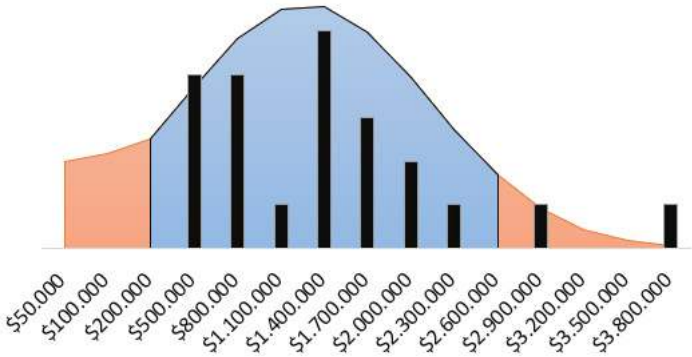


Tabla 8. Costos de los incidentes vs Inversiones vs Cantidad de Incidentes

Etiquetas de fila	Menos de USD $50,000	Entre USD $50,001 y $100,000	Entre USD $100,001 y $150,000	Más de USD $150,000
Entre el 0 y el 2%	**36,00%**	**2,00%**	**0,00%**	**0,00%**
Entre 1-3	24,00%	2,00%		
Entre 4-7	4,00%			
Más de 7	8,00%			
Entre el 3 y el 5%	**14,00%**	**2,00%**	**4,00%**	
Entre 1-3	8,00%	2,00%	4,00%	
Entre 4-7	2,00%			
Más de 7	4,00%			
Más del 11%	**6,00%**	**4,00%**	**4,00%**	**2,00%**
Entre 1-3			2,00%	2,00%
Entre 4-7	4,00%			
Más de 7	2,00%	4,00%	2,00%	
Entre el 9 y el 11%	**10,00%**	**2,00%**		**2,00%**
Entre 1-3	10,00%			
Entre 4-7				2,00%
Más de 7		2,00%		
Entre el 6 y el 8%	**8,00%**	**4,00%**		
Entre 1-3	2,00%			
Entre 4-7	2,00%	4,00%		
Más de 7	4,00%			
Total general	**74,00%**	**14,00%**	**8,00%**	**4,00%**

menos plausible que sus impactos tengan costos más manejables para la realidad de las empresas colombianas.

Al revisar las tendencias y reportes internacionales, se puede encontrar puntos en los cuales la realidad de Colombia se conecta la internacional.

Los ataques de aplicaciones se ven como un vector emergente y particularmente en el mundo de las API (Aplication Program Interfaces) el cual ha incrementado de 2021 a 2022 cerca de un 23% (Vmware, 2022; Imperva, 2022).

Los ataques de phishing, ingeniería social, en especial los de tipo Business Email Compromise es de los que más se usa (Secureworks, 2023), (Kroll, 2022), (Ironscale, 2022).

Los costos de los ciberataques crecen año tras año (Verizon, 2023; Sophos, 2023). En el caso de Ransomware para Colombia se siguen experimentando costos, es una tendencia creciente que ha mostrado que en la realidad nacional también este tipo de incidentes generan efectos en las empresas, y si bien el rigor diario de las noticias de ciberseguridad muestra permanentemente ataques de esta naturaleza, pues se ratifica que frente a otros tipos de ataques aún no están en los primeros lugares en términos de costos (Cybereason, 2022),

Los datos de Colombia muestran una desviación frente a la tendencia global en relación con el sector salud estudios como (Ponemon-Proofpoint, 2022; MinterEllison, 2023) muestran que es uno de los sectores más atacados (frecuencia) y su implicaciones e impactos

(costos) elevados, mientras en Colombia no se ve esa misma tendencia, esto se puede explicar porque el sector de la salud de Colombia, se encuentra en un estado de aprendizaje y madurez de sus prácticas de ciberseguridad y por tanto las capacidades de tener procesos de gestión de incidentes y monitoreo de los mismos sea baja para poder identificar lo que sucede.

Herramientas

La gráfica 22, muestra la distribución del uso de las herramientas de seguridad, en ella se evidencia que

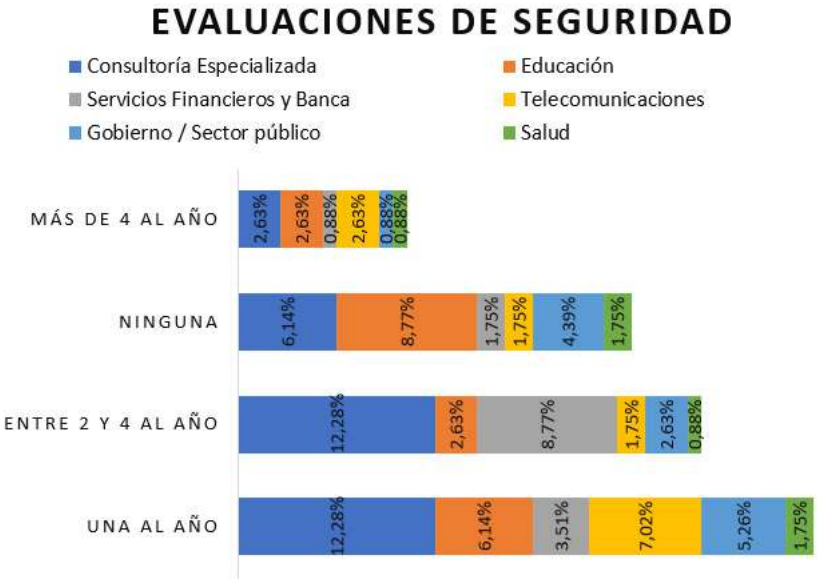
Gráfica 22: Herramientas de seguridad

el cifrado de datos, las VPNs, los sistemas de contraseñas, las soluciones antimalware y las firmas digitales, corresponden al top 5 de herramientas más usadas en las empresas de todos los tamaños y sectores de la industria nacional.

La gráfica 23 muestra el comportamiento de como las organizaciones en Colombia por industria realizan una evaluación de la postura de seguridad general. Se mantiene la tendencia con respecto al año inmediatamente anterior 36% dice que lo hace al menos una vez, entre 2 y 4 el 29% una disminución moderada con relación al año anterior un aumento importante en 6 puntos porcentuales que no se hizo siendo este año del 25% y un 11% lo hace más de 4 veces al año. Al revisar por sectores se observa como el sector de la consultoría especializada ocupa el primer lugar con excepción de ninguna donde es el sector de la educación el que tiene el primer puesto en no realizar este tipo de prácticas. El sector financiero definitivamente se consolida en manifestar que es de 2 a 4 evaluaciones de seguridad la que hace en un periodo de un año, llama la atención que el sector gobierno la segunda posición es el de ninguna que no es mucha la diferencia entre las dos posiciones.

Consideraciones de los datos

Al hacer una inspección de como los mecanismos de seguridad son usados en las empresas colombianas y cuáles son las tendencias por sectores de la industria encontramos la tabla 9, la cual contiene la



Gráfica 23: Evaluaciones de Seguridad

Tabla 9 Herramientas usadas por sectores de la industria.

Mecanismos de seguridad	Consultoría Especializada	Educación	Gobierno / Sector público	Salud	Servicios Financieros y Banca	Telecomunicaciones
Cifrado de datos	39%	14%	7%	6%	19%	10%
VPN/IPSec	29%	14%	7%	6%	24%	7%
Sistemas de Contraseñas	30%	16%	11%	5%	12%	12%
Firmas digitales/certificados digi	32%	11%	11%	6%	20%	5%
Soluciones Anti-Malware	39%	9%	7%	3%	17%	9%
Web Application Firewalls (WAF	30%	11%	10%	3%	17%	7%
Firewalls tradicionales (Hardwar	33%	17%	9%	7%	12%	7%
Biométricos (huella digital, iris, e	27%	14%	9%	4%	20%	7%
Firewalls de nueva generación	26%	9%	9%	8%	22%	4%
Entrenamiento/Actualización de	41%	7%	1%	4%	18%	8%
Firewalls de Bases de Datos (DAF	24%	16%	3%	7%	22%	11%
IDS/IPS de nueva generación	33%	3%	9%	5%	24%	7%
Servicio de SOC	28%	7%	4%	0%	28%	8%
Soluciones de seguridad EDR (En	36%	4%	6%	5%	21%	5%
SIEM (Security Information Even	27%	3%	9%	0%	32%	5%
Herramientas Anti–DDoS	31%	7%	7%	3%	26%	6%
Sistemas de detección y/o preve	27%	6%	6%	6%	24%	6%
Proxies/Proxies inversos	39%	7%	3%	3%	16%	3%
Enfoque de seguridad Zero Trust	29%	4%	3%	3%	26%	6%
Ciberseguros	28%	3%	1%	7%	24%	14%
Cooperación/Intercambio de inf	30%	6%	0%	7%	22%	7%
Servicios de inteligencia de ame	29%	4%	1%	0%	25%	4%
ADS (Anomaly detection system	38%	4%	3%	5%	19%	5%
Soluciones de Seguridad con IA	41%	3%	1%	6%	12%	6%
Soluciones basadas en inteligen	35%	3%	3%	0%	18%	0%
Tercerización de la seguridad inf	38%	7%	1%	13%	13%	0%
Herramientas de validación de c	38%	1%	0%	8%	23%	0%
Soluciones de monitoreo de red	25%	1%	0%	0%	42%	8%
Otro (especifique)	38%	3%	4%	0%	0%	0%
Smart Cards	33%	1%	0%	0%	33%	0%

distribución por sectores de industria de los mecanismos de seguridad.

Algunas particularidades al revisar los datos los cuales se pueden describir así.

1. La sumatoria global muestra al cifrado de datos como el mecanismo número 1 de todos.
2. En el sector de la consultoría se ve al entrenamiento de los profesionales de seguridad, el uso de la IA y las soluciones Antimalware como los mecanismos tendencia en dicho sector.
3. En el sector de la educación y gobierno usan los mecanismos tradicionales como firewalls de redes y de bases de datos, así como los sistemas de contraseñas y firmas digitales como las herramientas más usadas.
4. En el sector salud la tercerización, herramientas de validación de requisitos regulatorios internacionales y los firewalls de nueva generación son observados como mecanismos a ser usados.
5. El sector financiero usa con frecuencia monitoreo de redes sociales, Smart cards y los Siem como herramientas útiles para manejar su seguridad
6. El sector de telecomunicaciones es un sector que usa los Ciberseguros, los sistemas de contraseñas y los firewalls de bases de datos.

En el estudio de IBM (IBM, 2023), 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 informe resalta que las soluciones *antimalware*, cifrado de discos, antivirus avanzados basados en inteligencia artificial también están considerados.

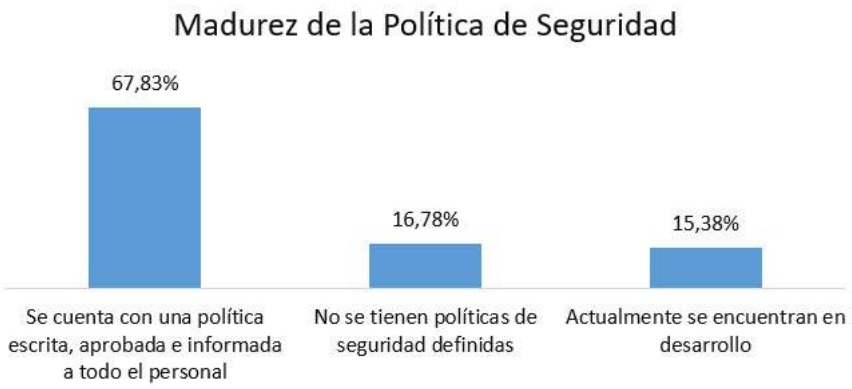
En cuanto a la protección de la capa de aplicaciones, los *Firewalls Web*, de bases de datos la protección de APIs son los controles que más se están usando y se tiene proyectado utilizar.

Los controles de seguridad siempre serán una herramienta indispensable para tener una higiene digital adecuada, en Colombia se ratifica la tendencia de uso de controles para combatir y contrarrestar a un adversario digital que cada vez acecha más, hace uso de capacidades adicionales y las empresas en su camino de desarrollar y sostener la resiliencia operacional cada vez más necesitan de estas soluciones (Marsh, 2022).

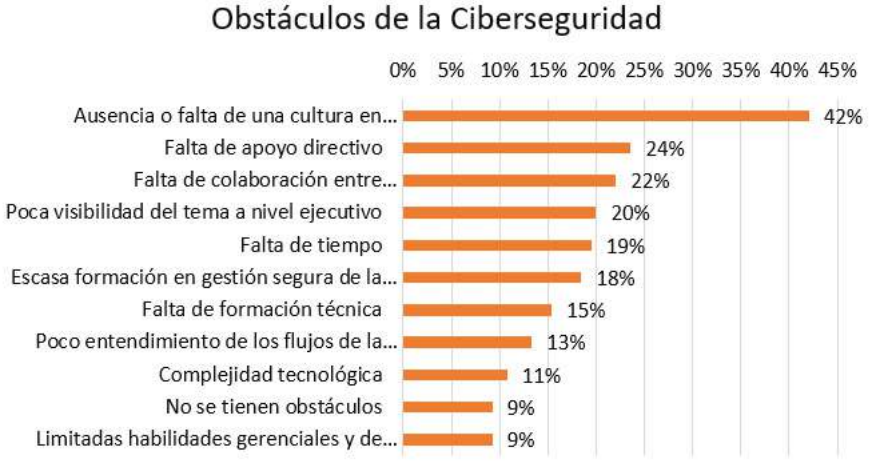
Políticas

La gráfica 24, refleja el estado de las políticas de seguridad en las organizaciones colombianas, el 68% de los encuestados manifiesta que tienen formalizada sus políticas de seguridad disminución de 4 puntos porcentuales frente al año 2022, el 15% actualmente en desarrollo y con un aumento del 9% frente al año anterior, el 16% señala no tener políticas de seguridad de la información.

La gráfica 25, 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 42%, la falta de apoyo directivo 24% y la falta de colaboración entre áreas 22% son los tres primeros lugares, cambios importantes para este año en los puestos 2 y 3 con relación al año anterior.



Gráfica: 24 Estado de las Políticas

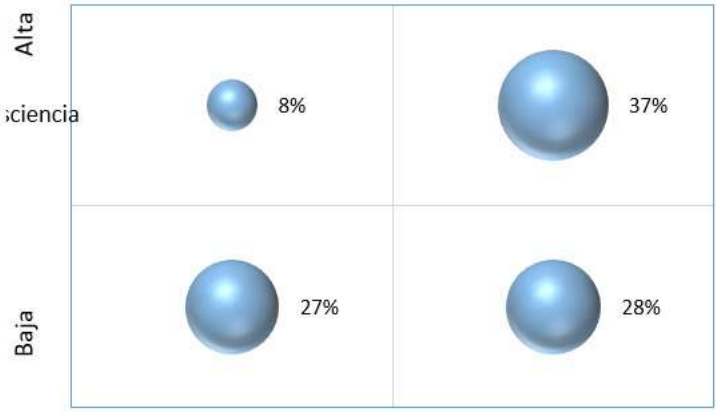


Gráfica 25 Obstáculos de la seguridad

La gráfica 26 refleja el nivel de consciencia y competencia de los directivos en materia de seguridad, encontrando que, la alta dirección con un 37% toma decisiones en materia de ciberseguridad, 28% atiende las recomendaciones de sus profesionales, 27% no participa en la toma de decisiones y no se involucra, y el 8% delega y espera informa de avances.

La gestión de riesgos de seguridad es un elemento esencial, en esa línea el 75% de los encuestados tiene un proceso de gestión de riesgos y solo 25% no lo posee.

En la gráfica 27, se resalta cada cuanto son ejecutados dichos ejercicios, el 56% manifiesta que al menos la ejecuta 1 vez al año, el 20% más de dos y solo dos el 24%. Es-



Gráfica 26: Consciencia de los directivos

Gráfica 27 Ejecución de Evaluaciones de riesgo

tos valores corresponden a aquellos que dijeron que si realizan la evaluación de riesgo en sus empresas

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 principal motivo que resaltan los participantes está relacionado con no tener un proceso formal de gestión de riesgos (31%), disminución con relación al año anterior en 6 puntos porcentuales, seguido por un lado del desconocimiento del tema 23% y que ya está incluido en el proceso de gestión de riesgo empresarial 23%, la falta de presupuesto 11% y por último el no tener asociados riesgos con el tratamiento de la información 11%.

La tabla 10 muestra las metodologías de gestión de riesgos usadas por los participantes del estudio. En primer lugar, está ISO 27005 como la más usada con el 27%, seguido de ISO 31000 25%, 14% menciona no tener una metodología.

La Gráfica 28 muestra la forma en como las organizaciones hacen las asociaciones entre incidentes de seguridad y el riesgo. El 57% asocia los incidentes de seguridad con riesgos de ciberseguridad, el 48% los asocia con riesgos operacionales, el 36% los asocia con riesgos reputacionales, el 35% con riesgos legales, el 32% con riegos económicos, el 26% los asocia a riesgos transversales.

La tabla 11 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.

Tabla 10. Metodologías para la gestión de riesgos

Metodologías	%
ISO 27005	27%
ISO 31000	25%
No se cuenta con metodología	14%
Magerit	9%
SARO	9%
GRC (Governance, Risk & Compliance)	8%
ERM(Enterprise Risk Management)	5%
Octave	4%
AS/NZ 4360	1%

Gráfica 28: Tipos de Riesgos

Tabla 11

ISO 27001	52%
Guías del NIST	22%
ITIL	18%
COBIT	13%
Ninguna	9%
PCI-DSS	9%
Guías de la ENISA	5%
ISM3 - Information Security Management Maturity Model	2%

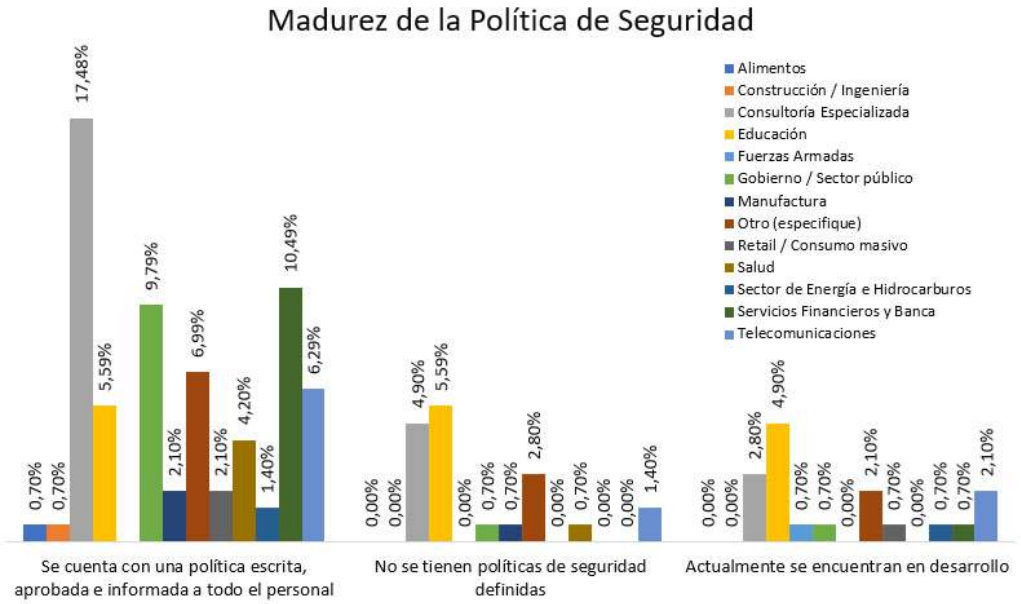
En cuanto a las regulaciones que las organizaciones deben cumplir, el caso colombiano menciona que, el 48% de los participantes manifiesta que sí existen regulaciones que son aplicables a sus modelos de negocio, el 38% considera que no está sujeto a cumplir ningún marco regulatorio o normativos, el 7% debe cumplir con marcos regulatorios internacionales y solo el 7% menciona a otros elementos de regulación.

Consideraciones de los datos

Gobierno y Gestión de la Seguridad

La gestión y el gobierno de la seguridad son instrumentos de alto valor para hacer que las estrategias de seguridad tanto en el corto plazo como en el largo plazo funcionen y nutran a los negocios de condiciones que apalanquen la confianza digital en todas las partes interesadas, aumenten la resiliencia operacional del negocio y en últimas generen beneficios (Accenture, 2023).

En ese sentido la política de seguridad en Colombia en todos los sectores de la industria ha encontrado una consolidación importante al estar definida y formalizada en la realidad de las empresas colombianas. La gráfica 29, muestra esa distribución por sectores en donde se puede ver reflejada la madurez de la política como instrumento del programa para la gestión y el gobierno de la seguridad. El sector de la consultoría especializada manifiesta con un 17,5% tener aprobada una política, el sector de educación es el sector con mayor valor 5,59% comparado con los otros sectores en no tener una política, el sector de la educación en términos de comparaciones con los demás sectores es el que tiene el valor más alto 4,90% en manifestar que está en desarrollo su política de seguridad, dicho de otra manera, el sector de la educación reconoce que tiene una deficiencia al no tener una política de seguridad formalizada, sin

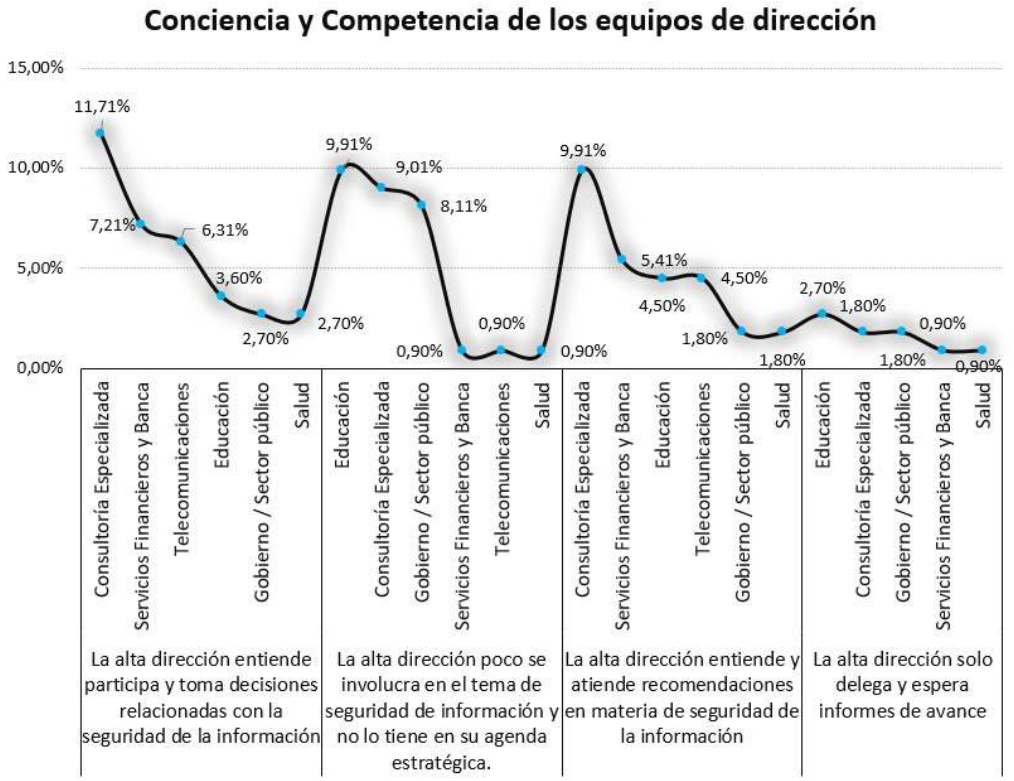


Gráfica 29. Madurez de la política de seguridad por sectores de industria

embargo, está hoy haciendo esfuerzos por desarrollarla y disminuir la brecha de gestión, dato no menor, dado que junto con el sector salud, son los sectores más apetecidos por los adversarios digitales como lo manifiestan reportes de industria (Verizon, 2023), (IBMb, 2023). Otro dato importante e interesante de análisis es que el sector financiero manifiesta no tiene en esta muestra de datos empresas que no tengan política de seguridad, o la tiene muy formalizada, o la está desarrollando.

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, 2023), el cual manifiesta que la prioridad de estos tipos de ataques es alta en las organizaciones del mundo.

Las responsabilidades de un gobierno de seguridad de la información están centradas en que sus directivos tengan un contacto directo con la ciberseguridad (NACD, 2023), participen de ella y tomen decisiones basados en los datos, tendencias recientes como las directrices propuestas por la Security Exchange Commission (SEC), que ha propuesto una responsabilidad



Gráfica 30. Juntas directivas x sectores

más avanza en materia de responsabilidad de los cuerpos directivos y que planea para finalizar el año 2023 (Toscano, 2023).

En este sentido, al revisar la forma en como los cuerpos directivos se involucran en la toma de decisiones de la seguridad por sectores de la industria se tiene la gráfica 30.

Las juntas directivas que se involucran y toman decisiones en el mundo de la ciberseguridad, primeramente, están en el sector de la consultoría especializada y el sector financiero, mismo comportamiento que tiene estos cuerpos directivos que con menos madurez al menos atienden las recomendaciones de seguridad, la variación radica en la tercera posición donde el sector salud atiende más que el sector de telecomunicaciones.

Los cuerpos directivos del sector educación, consultoría especializada caso especial de empresas pequeñas y el sector de gobierno muestran un comportamiento de poco interés en participar o atender recomendaciones de seguridad

Los equipos directivos que solo delegan y esperan algún tipo de informe de avance de estos temas, el sector de educación, consultoría empresas pequeñas de menos de 50 empleados tienen este comportamiento y el sector del gobierno.

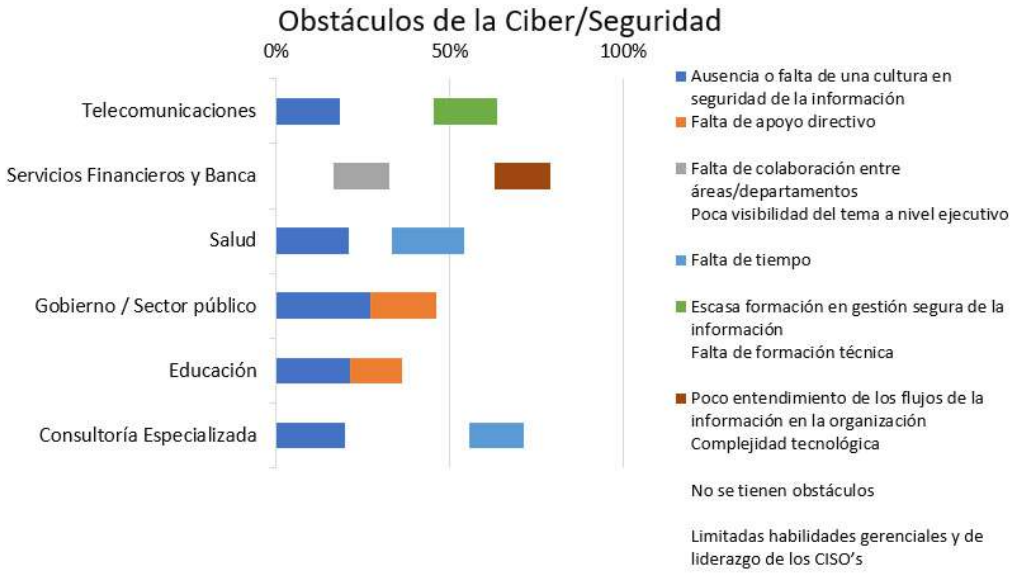
Esto resalta la idea de que la madurez de las organizaciones se ve reflejada desde la posición que decide asumir la dirección en relación con la ciberseguridad, cuando los líderes de riesgo y de seguridad vuelven a la seguridad un asunto de los negocios, se crea un compromiso en la dirección y cuerpos directivos no solo se involucran en ellos (Accenture, 2023).

Es claro que existen obstáculos para que la postura de seguridad de una organización fluya en los ambientes organizacionales, la postura 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, así mismo maximizar el valor de las inversiones, y el beneficio que los programas produzcan (Nuspire, 2023), son parte de los que pueden existir para el Líder de Seguridad Digital de las empresas colombianas.

En la gráfica 31, se expresa cuáles son los obstáculos más representativos que los distintos sectores de la industria ha experimentado.

De la gráfica y los datos recolectados se pueden afirmar lo siguiente:

1. La cultura de seguridad es un factor diferencia en todos los sectores y es un gran obstáculo para que la postura de seguridad permee la organización.
2. Cada sector tiene un sentir con particularidades de como los



Gráfica 31. Obstáculos de la Seguridad por sectores

obstáculos hacen que los programas de seguridad no fluyan de la manera más adecuada posible.

3. Por ejemplo, el sector de telecomunicaciones resalta que uno de sus factores claves tiene que ver con las capacidades humanas y habilidades gerenciales de sus CISOs.
4. El sector financiero resalta los pocos entendimientos de los flujos de información es un factor que definitivamente hace fuerte presencia.
5. La falta de tiempo es el factor relevante en el sector salud y consultoría especializada, el cual inquieta pues muestra que no es la seguridad vista como un asunto de negocio, sino como un reto del momento en el que se requiera.
6. El sector gobierno ha considerado que el poco interés que este tema tiene tanto en el nivel ejecutivo como el apoyo que a este tema se le debe dar, como el obstáculo importante a considerar.
7. El apoyo de la dirección es otro de los impedimentos para que la ciber-seguridad fluya en las organizaciones.

Lo cierto de todos los datos y la gráfica 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 orien-

tar 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, 2023).

Gestión del Riesgo

Gestionar el riesgo es una de las formas eficientes para no solo dar soporte y resiliencia operacional a los negocios, adicional es una forma de tomar decisiones que soporten el desarrollo de los negocios en el corto, mediano y largo plazo (Thompson, C., & Hopkin, P., 2021).

En la realidad colombiana los diferentes sectores de la industria ven a riesgo como un instrumento de conexión con la seguridad y ciberseguridad, sin embargo, la madurez en la práctica aún sigue un camino de aprendizajes propio de las dinámicas organizacionales, tendencia que no se aleja de la realidad global (ECIIA, 2024).

La radiografía de la gestión de riesgo en Colombia puede ser descrita de la siguiente manera:

1. Las empresas colombianas realizan al menos un ejercicio al año de valoración de riesgos. Siendo el sector de la consultoría especializada el que hace uso de todas las frecuencias de realización de la evaluación de riesgos
2. El sector de Consultoría especializada y gobierno realiza dos evaluaciones de riesgo al año con mayor porcentaje
3. El sector de educación usa una al año como su forma de explorar los riesgos.
4. En el sector salud se mantiene el desconocimiento del tema como la principal causa por la que estos ejercicios no se hacen en las empresas, entidades y/o organizaciones
5. En el sector de la Educación si bien se dice que se hace una vez, al indagar en dichos sectores por que no se hace, la manifestación está relacionada a que no existe un proceso formal de gestión de riesgos.
6. En cuanto a metodología del marco ISO tanto 27005 y 31000 son las metodologías más usadas en todos los sectores, sin embargo, el sector de la educación llama la atención porque en este sector no tener una metodología formal para gestionar los riesgos es el valor más alto de todos los sectores de la industria analizados.
7. Sin excepción de los sectores de la industria analizados, todos catalogan sus incidentes como un ejercicio asociado al riesgo cibernético, tema no menor porque muestra que en Colombia se empieza a entender que el riesgo cibernético merece un tratamiento diferencial a otros riesgos, esto mismo podría dar luz para que la resiliencia operacional tenga cabida en las empresas y de la misma manera se

comprenda que el riesgo cibernético deja de ser un asunto de tecnologías y es más un asunto de negocio (AON,2023).

Capital intelectual

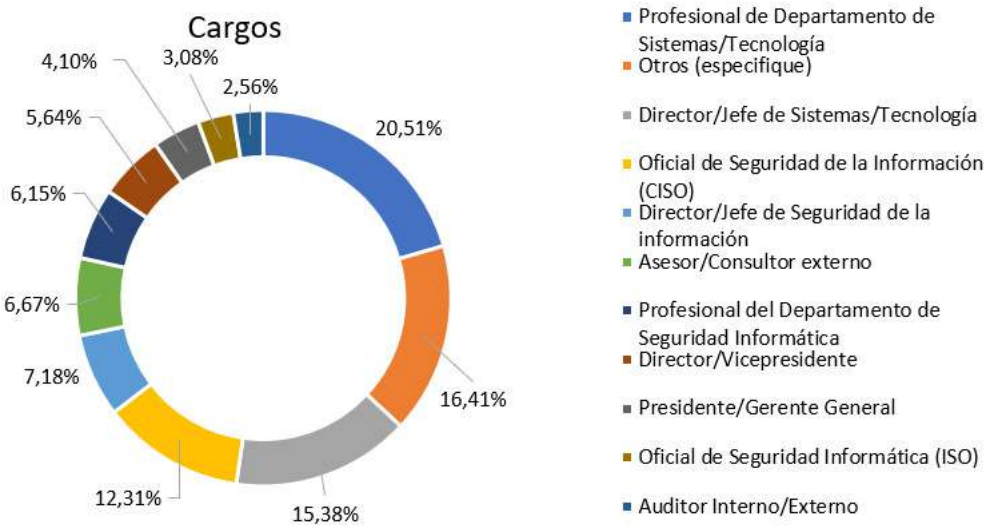
La gráfica 32 muestra los participantes de la encuesta de seguridad, en las cuales se puede ver que los profesionales de tecnología, de seguridad son los que más participan, el caso de otros está representado entre otros a docentes de las áreas de seguridad, especialistas de ciberseguridad que no se identifican con los roles propuestos.

Son múltiples y variadas las funciones del profesional de seguridad en las empresas de Colombia, la gráfica 33 muestra las múltiples funciones que hoy desempeña el profesional.

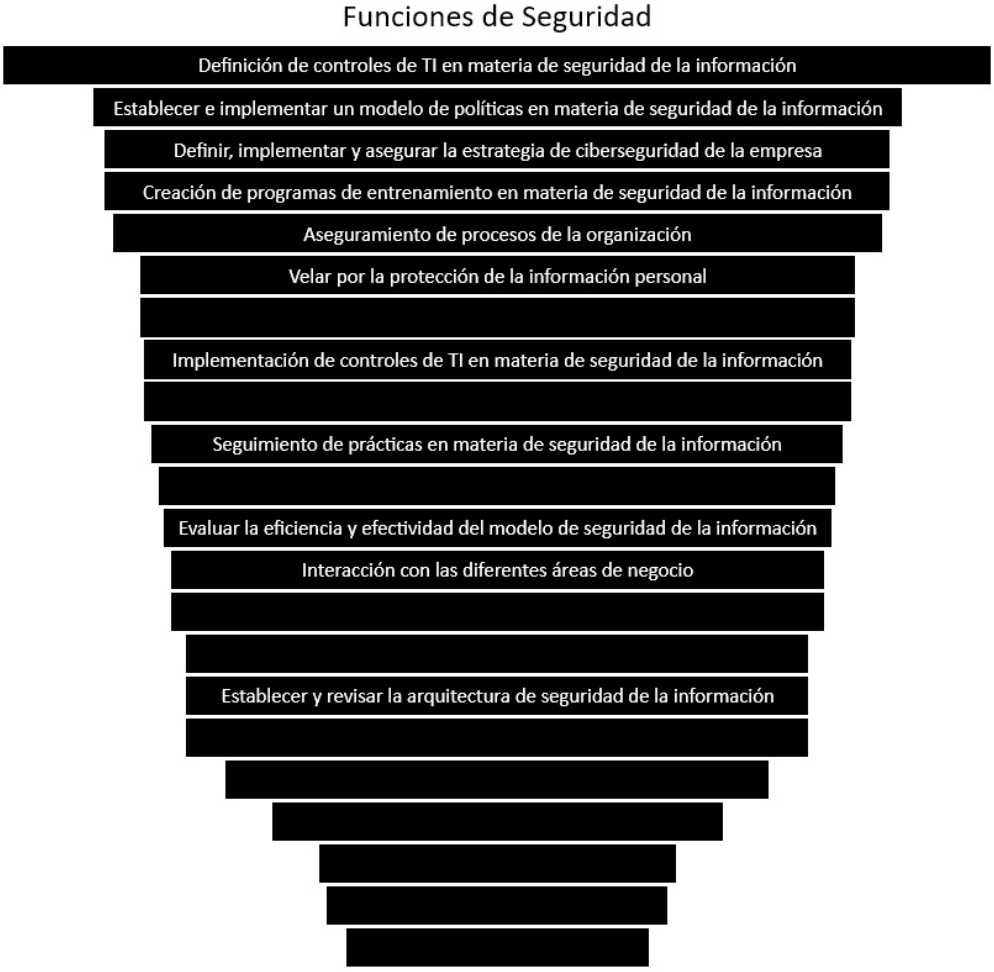
Las tres primeras funciones tienen que ver con, Definición de controles de TI en materia de seguridad de la información 65%, Establecer e implementar un modelo de políticas en materia de seguridad de la información 53%, Definir, implementar y asegurar la estrategia de ciberseguridad de la empresa 52%.

La gráfica 34 muestra la dependencia del área de seguridad en las empresas.

La gráfica 35 muestra los distintos roles que son usados en las empresas de la realidad colombiana.



Gráfica 32. Cargo de los participantes de la encuesta



Gráfica 33. Funciones del profesional de seguridad

Los tres roles más comunes, el analista de seguridad de la información 43%, el Oficial de Seguridad de la Información 37% y el analista de seguridad informática 33%.

La gráfica 36, muestra el tamaño de las áreas de seguridad, llama que el segundo valor de mayor importancia es ninguno con el 16,15%, el tamaño definitivamente consolidado es de 1 a 5 profesionales conformando un área de seguridad con el 58,46%.

Consideraciones de los datos

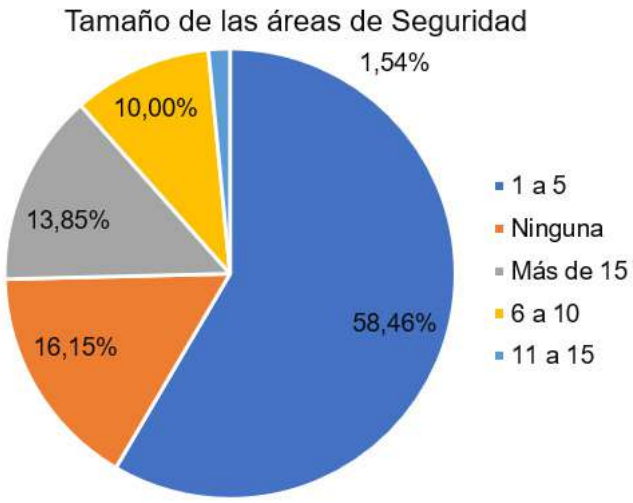
Quien es el profesional de seguridad

En Colombia el profesional de seguridad es un perfil, diverso y con muchas capacidades. La encuesta nacional de seguridad tiene parti-

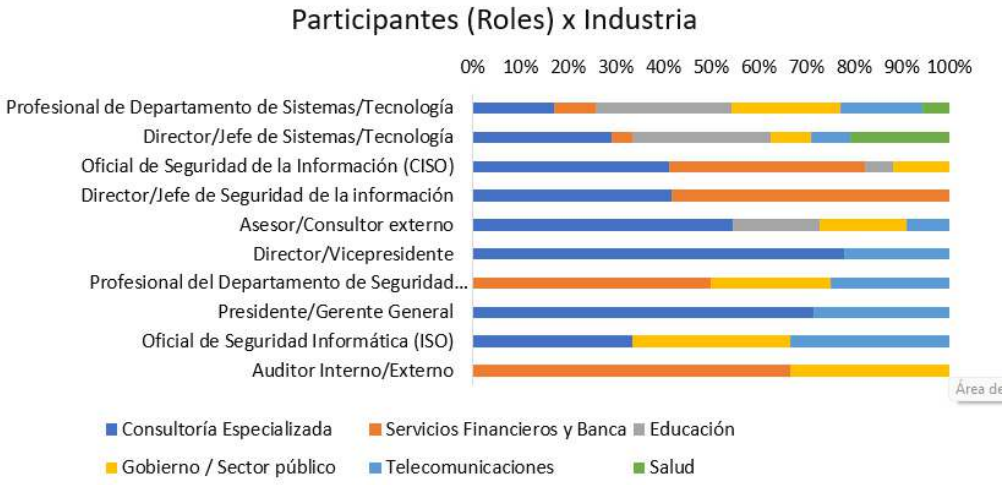
Gráfica 34. Dependencia de la Seguridad

Gráfica 35. Roles de Seguridad

cipación de múltiples sectores de industria y profesionales de las áreas afines. En la gráfica 36, vemos la distribución de profesionales por sector de industria, encontrando que el sector educación, telecomunicaciones y gobierno tiene una alta participación los profesionales de TI en el diligenciamiento de la encuesta, en el sector de la consultoría especializada y el sector salud, son los directores de tec-



Gráfica 36. Tamaño del área de Seguridad

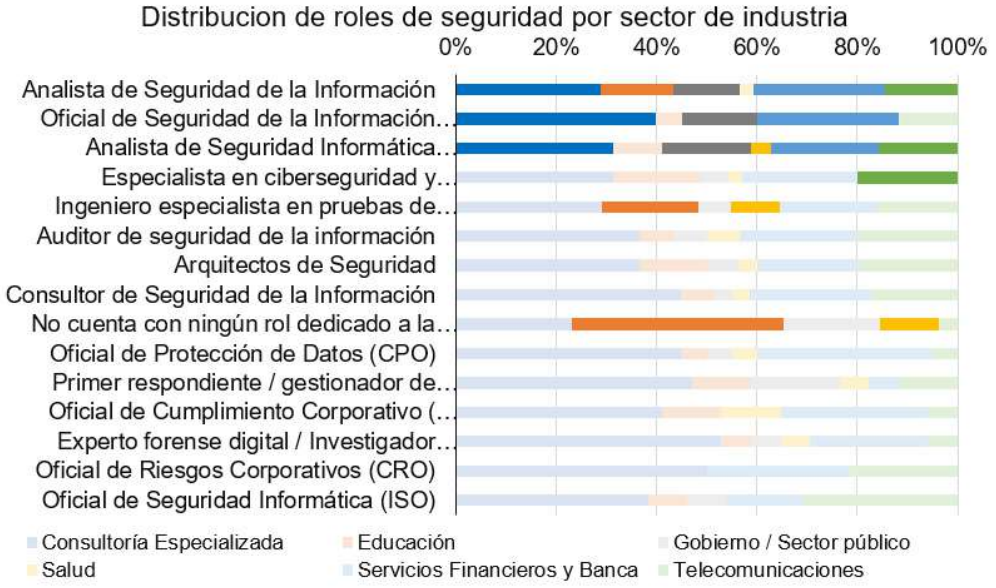


Gráfica 36. Participantes de la encuesta (Roles)

nologías los que más diligencian el instrumento, los Cisos y directores de seguridad del sector financiero y la consultoría especializada son seguidamente los que más participan.

Las diferentes industrias tienen tipos de roles y es lo que hace que se deban revisar roles, funciones e industrias.

La gráfica 37, muestra como las diferentes industrias determinan los roles que conforman sus áreas de seguridad, y esto claramente influye en la cantidad de funciones y responsabilidades del área de se-



Gráfica 37. Distribución de roles de seguridad por sector de industria

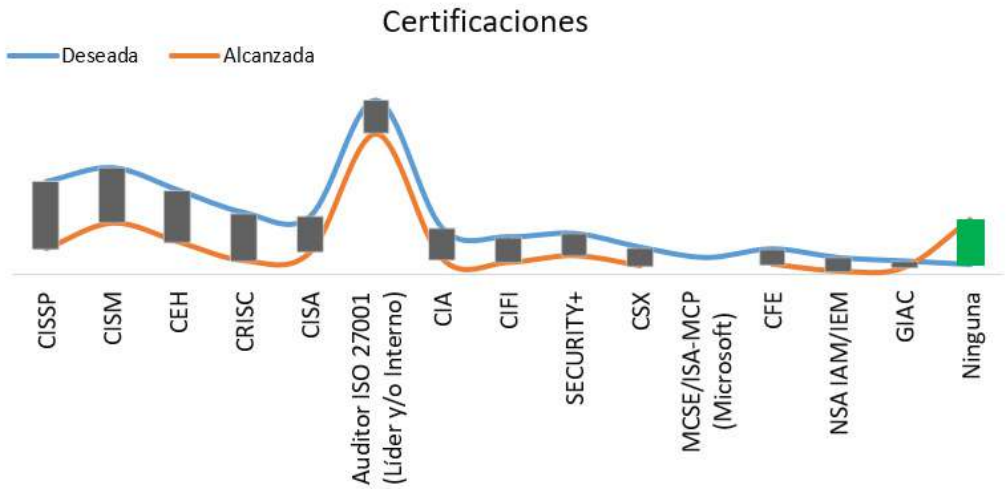
guridad, así como su nivel de entrega de información.

Este gráfico, determina cuáles son los tres roles más usados en los sectores más representativos de la industria en Colombia, diciendo el analista de seguridad de la información, el CISO Oficial de Seguridad de la Información, y el analista de seguridad informática son los roles primarios que existen, muy formalmente definido el rol del CISO está en el sector de la consultoría especializada, el financiero y el gobierno en ese orden de importancia.

El analista de seguridad informática está mayormente formalizado o es el rol principal en la consultoría especializada, que en los servicios financieros que en el sector financiero.

En el sector de las telecomunicaciones lo más común es encontrar analista de seguridad de la información como primer rol identificado.

Sectores que preocupan son el sector salud y educación, los cuales manifiestan como su valor más representativo, el hecho de que la función de seguridad no está y no ha dedicado ningún talento humano a esta función, lo que indicará o que no se desarrollan todas las funciones de seguridad o en su defecto las comparten específicamente con el área de tecnología.



Gráfica 38 Certificaciones de los profesionales de seguridad

Las certificaciones son parte esencial de la vida del profesional de seguridad y alcanzarlas hace parte del desarrollo de su carrera (ISSA-ISG, 2023; ISACA, 2023; Fortinet, 2023). La gráfica 38, precisamente refleja y se conecta con las tendencias internacionales.

Esta gráfica representa dos momentos, el primer momento está relacionado con las certificaciones que hoy el profesional de seguridad posee, en ese orden de ideas, lo que más hoy se ha alcanzado en el horizonte es la certificación de Auditor ISO 27001 en Colombia, seguido de CISM y CISSP respectivamente, sin embargo, al revisar lo que el profesional de seguridad desea lograr, se invierten los papeles y encontramos que la certificación de CISSP es la que más se busca en el contexto nacional seguido de CISM, y CEH respectivamente.

Los profesionales de seguridad en busca del desarrollo de su carrera profesional ven en las certificaciones una forma de mejorar no solo sus conocimientos, sino su valor de mercado. (ISSA-ESG, 2023).

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 tran-

quilidad y bienestar (Deepinstinct, 2023).

¿Qué hace comúnmente?

Son diversas las actividades que hacen los profesionales de seguridad, y que dependen en gran medida de la madurez, formación del área de seguridad en las empresas, así como el sector (ArticWolf, 2023).

Para los sectores más importantes de la industria colombiana, definitivamente el área de seguridad y sus profesionales están centrados en la Definición de controles de TI en materia de seguridad de la información, sin embargo, al revisar las siguientes funciones si hay cambios interesantes por sector de la industria.

Sector financiero, en este sector las tres funciones principales son, Seguimiento de prácticas en materia de seguridad de la información, Definición de controles de TI en materia de seguridad de la información, Establecer e implementar un modelo de políticas en materia de seguridad de la información, Aseguramiento de procesos de la organización.

Consultoría especializada, sus principales actividades están centradas en, Definición de controles de TI en materia de seguridad de la información, Creación de programas de entrenamiento en materia de seguridad de la información, Definir, implementar y asegurar la estrategia de ciberseguridad de la empresa.

Gobierno / Sector público, sus actividades principales son: Definición de controles de TI en materia de seguridad de la información, Creación de programas de entrenamiento en materia de seguridad de la información, Definir, implementar y asegurar la estrategia de ciberseguridad de la empresa y Dirigir y supervisar los programas de riesgos de seguridad de la información de la organización. Existen dos funciones que comparten los mismos valores.

Telecomunicaciones, las áreas de seguridad se centran en Definición de controles de TI en materia de seguridad de la información, Velar por la protección de la información personal, Definir, diseñar y velar por el programa de privacidad de la información de la organización.

Educación, sus áreas de seguridad se centran en, Definición de controles de TI en materia de seguridad de la información, Aseguramiento de procesos de la organización, Definir, implementar y asegurar el programa de protección de datos personales de la empresa.

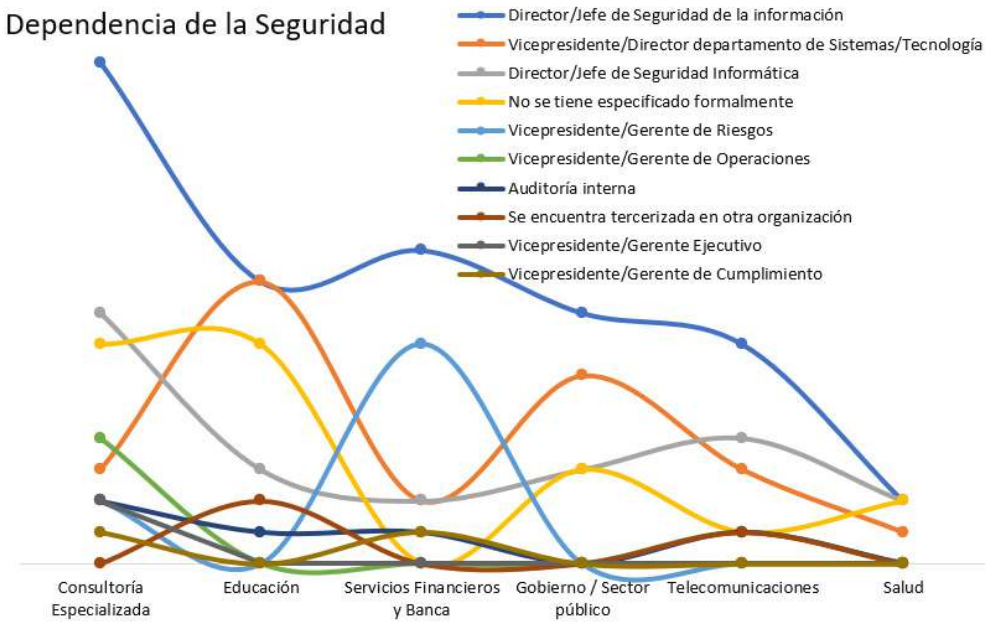
Salud, las actividades de seguridad en las que se centran sus equipos son, Definición de controles de TI en materia de seguridad de la información, Definir, implementar y asegurar la estrategia de ciberseguri-

dad de la empresa, Velar por la protección de la información personal, Definir, implementar y asegurar el programa de protección de datos personales de la empresa.

La tabla 12, es el detalle de todas las actividades y funciones del área de seguridad.

En cuanto a la dependencia de la seguridad, los diferentes sectores de la industria tienen posiciones interesantes, la gráfica 39, se puede observar que, el sector de la consultoría especializada tienen junto al sector financiero un área de seguridad posicionada y claramente definida de quien depende toda la función de seguridad, llama la atención que en estos mismos sectores la dirección de TI no tiene ninguna relación con la dependencia de seguridad, lo cual muestra y refleja una madurez en la función, el sector financiero adicional a lo anterior también muestra que la seguridad de la información puede estar dependiendo de una vicepresidencia de riesgo, comportamiento único en los sectores de la industria de Colombia.

Situaciones inquietantes, el sector salud es el único sector que muestra que no se tiene formalmente definida la función y la dependencia de la seguridad, deja al descubierto



Gráfica 39. Dependencia de la Seguridad por sectores

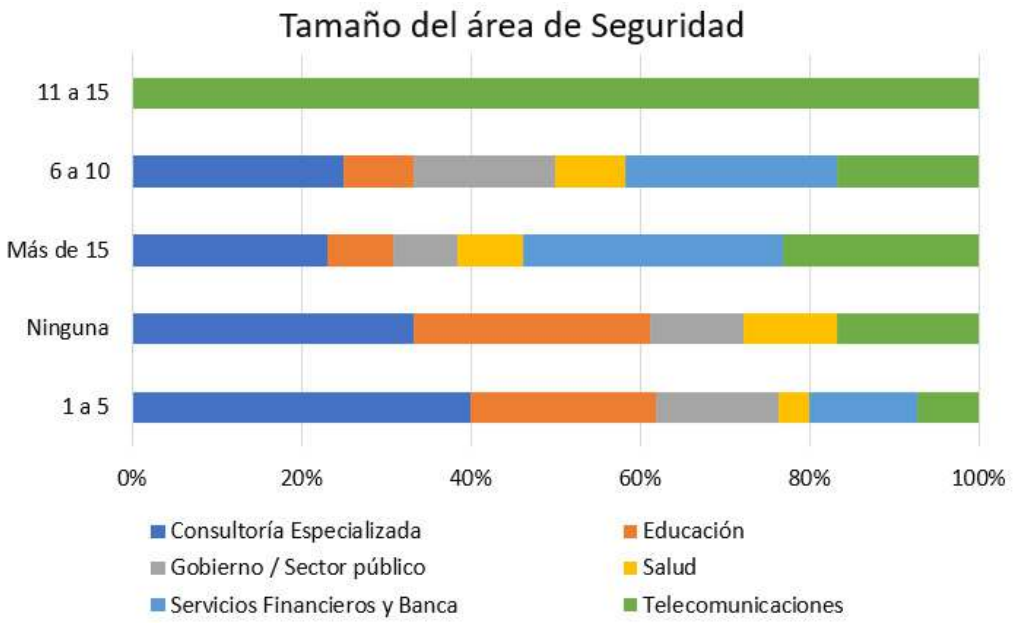
Tabla 12. Distribución de funciones del profesional de seguridad por sectores

Criterios	Consultoría Especializada	Educación	Gobierno / Sector público	Salud	Servicios Financieros y Banca	Telecomunicaciones
Definición de controles de TI en materia de seguridad de la información	17,44%	9,74%	6,15%	3,08%	8,72%	5,13%
Establecer e implementar un modelo de políticas en materia de seguridad de la información	15,90%	6,67%	6,15%	2,05%	8,21%	3,08%
Aseguramiento de procesos de la organización	13,85%	8,72%	5,13%	1,54%	8,21%	4,10%
Definir, implementar y asegurar la estrategia de ciberseguridad de la empresa	16,41%	6,67%	3,59%	3,08%	7,18%	3,08%
Creación de programas de entrenamiento en materia de seguridad de la información	16,92%	5,64%	3,59%	2,05%	7,69%	3,59%
Definir, diseñar y velar por el programa de privacidad de la información de la organización	13,33%	7,18%	4,62%	2,56%	5,13%	4,62%
Implementación de controles de TI en materia de seguridad de la información	12,82%	8,21%	4,62%	3,08%	4,10%	4,10%
Velar por la protección de la información personal	11,79%	6,15%	4,10%	3,08%	6,15%	5,13%
Definir, implementar y asegurar el programa de protección de datos personales de la empresa	10,77%	8,72%	4,62%	3,08%	5,13%	4,10%
Seguimiento de prácticas en materia de seguridad de la información	13,33%	5,64%	3,08%	2,05%	9,23%	2,05%
Informar a la alta gerencia sobre el avance del programa de seguridad de la información	13,33%	4,62%	3,08%	2,05%	7,69%	3,59%
Evaluar la eficiencia y efectividad del modelo de seguridad de la información	13,85%	5,13%	4,10%	2,05%	6,15%	2,05%

Dirigir y supervisar los programas de riesgos de seguridad de la información de la organización	13,33%	4,62%	5,13%	1,54%	7,18%	0,51%
Creación de programas de gobierno y gestión en materia de seguridad de la información	14,87%	3,59%	2,05%	2,05%	6,67%	2,56%
Establecer y revisar la arquitectura de seguridad de la información	11,79%	6,15%	2,05%	2,05%	7,18%	2,05%
Interacción con las diferentes áreas de negocio	11,28%	4,10%	3,08%	2,05%	6,15%	4,10%
Gestionar el programa de gestión de incidentes de seguridad de la información	11,79%	5,13%	4,10%	2,05%	6,15%	1,03%
Supervisar procesos de cumplimiento regulatorio en tecnología de información	10,77%	3,59%	3,59%	2,56%	6,15%	2,05%
Seguimiento de prácticas en materia de protección de la privacidad de la información personal	7,69%	5,64%	1,54%	1,03%	4,10%	3,08%
Supervisar y gestionar los procesos de investigaciones forenses digitales	6,67%	3,59%	1,54%	1,54%	3,59%	1,03%
Definir o diseñar escenarios/simulaciones/Playbooks en relación con ciberriesgos	4,62%	3,08%	1,54%	1,54%	3,59%	0,51%
Definir programas de resiliencia digital	5,13%	3,08%	2,05%	1,03%	2,05%	0,51%

las grandes falencias y claramente se conecta con las tendencias internacionales de ser uno de los sectores que más requiere de atención por el interés del adversario, así como la necesidad de fortalecer la función de seguridad (Proofpoint-Ponemon, 2023). De la misma manera inquietante que sectores como la educación, y el sector gobierno tengan este mismo comportamiento de no tener definida una línea de dependencia y que claramente hace que gobernar la seguridad y definir roles y responsabilidades sea mucho más complejo de realizar (Accenture, 2023)

Las áreas de seguridad en los distintos sectores de la industria en sus tamaños determinan el hacer y actuar del profesional de seguridad y sobre todo quien, sectores como las telecomunicaciones es el único sector que manifestó tener un área de seguridad entre 11 y 15 personas, mientras que los demás sectores de la industria tienen variedad



Gráfica 40. Tamaño del área de seguridad x sector de industria

en los tamaños de las áreas de seguridad. La gráfica 40, es una representación del tamaño de las áreas de seguridad distinguidas por los sectores de la industria.

Definitivamente se consolidad que un área de seguridad en Colombia tiene un tamaño hasta máximo 5 personas, sin decir que los demás tamaños no sean representativos, áreas de seguridad grandes, más de 15 personas las lidera el sector financiero, áreas entre 6 y 10 personas las lideran el sector de la consultoría especializada y el sector financiero, el sector de la consultoría especializada lidera en las áreas de 1 a 5 personas, y sorprende que el mismo sector sea el líder de las empresas que manifiestan no tener áreas de seguridad, seguido del sector educación.

En esa misma medida los tamaños de las áreas determinan los quehaceres de estas, mientras que las áreas pequeñas (1-5) profesionales de seguridad que en su mayoría son analista de seguridad de la información, de seguridad informática y coordinador de seguridad (CISO), se dedican a asegurar procesos, verificar eficacia y gestionar los incidentes. Las áreas medianas (6 a 15), que tienen un líder de seguridad con funciones ejecutivas al que se le llama CISO en algunos casos, tienen como funciones primarias hacer un seguimiento de las prácticas de seguridad, guiar a la empresa en aprender de sus incidentes a través de los procesos forenses y mejorar las capacidades cibernéticas de las empresas a través del diseño de playbooks en relación con el ciberriesgo. Por otro

lado, las áreas grandes (Más de 15), las cuales están conformadas por uno o varios líderes de seguridad con funciones específicas, arquitectos de seguridad y los roles de analistas muy bien definidos, se dedican principalmente a simular al adversario en relación con riesgo cibernético, mejorar las capacidades de la empresa en relación con la resiliencia empresarial y aprender de los incidentes a través de los procesos forense, que pueden ser evidenciados en la tabla 13. Sorprende que las áreas que manifiestan no tener una estructura definida para atender las funciones de seguridad, si realiza algunas actividades y las principales están todas centradas proteger de alguna manera la información y dedicarse cumplir con los requerimientos de cumplimiento de protección de datos bajo el contexto de la regulación colombiana.

El CISO un ejecutivo en aprendizajes

Un rol profesional que ha tenido una relevancia importante en los tiempos de transformación de las empresas en el contexto digital (Proofpointb, 2023), con los cambios drásticos que la tecnología y los negocios vienen experimentando, los incrementos de la actividad hostil del adversario digital y la necesidad de las empresas de hacerse sostenibles en un ecosistema digital toma relevancia el rol y sobre todo la información que entrega.

La gráfica 41, muestra precisamente que tipo de información entrega en el CISO en la empresa. Cabe destacar que cada sector de la industria tiene unos matices importantes en la forma como es percibido el rol y cómo evalúan su valor.

Gráfica 41. Información que entrega el CISO por sector de la industria

Tabla 13. Funciones de seguridad por tamaño del área de seguridad

Funciones	Ninguna	Más de 15	6 a 10	11 a 15	1 a 5
Velar por la protección de la información personal	17,39%	17,39%	15,22%		50,00%
Aseguramiento de procesos de la organización	8,89%	15,56%	8,89%	2,22%	64,44%
Supervisar y gestionar los procesos de investigaciones forenses digitales		25,00%	20,83%		54,17%
Supervisar procesos de cumplimiento regulatorio en tecnología de información	10,26%	17,95%	12,82%		58,97%
Seguimiento de prácticas en materia de seguridad de la información	9,43%	18,87%	16,98%		54,72%
Seguimiento de prácticas en materia de protección de la privacidad de la información personal	6,45%	19,35%	12,90%		61,29%
Interacción con las diferentes áreas de negocio	12,50%	22,50%	15,00%		50,00%
Informar a la alta gerencia sobre el avance del programa de seguridad de la información	7,84%	17,65%	13,73%		60,78%
Implementación de controles de TI en materia de seguridad de la información	15,09%	18,87%	9,43%		56,60%
Gestionar el programa de gestión de incidentes de seguridad de la información	4,55%	18,18%	13,64%		63,64%
Evaluar la eficiencia y efectividad del modelo de seguridad de la información	9,09%	15,91%	11,36%		63,64%
Establecer y revisar la arquitectura de seguridad de la información	12,82%	23,08%	7,69%		56,41%
Establecer e implementar un modelo de políticas en materia de seguridad de la información	12,28%	14,04%	12,28%		61,40%
Dirigir y supervisar los programas de riesgos de seguridad de la información de la organización	9,76%	17,07%	9,76%		63,41%
Definir programas de resiliencia digital	15,00%	25,00%	15,00%		45,00%
Definir, implementar y asegurar la estrategia de ciberseguridad de la empresa	10,71%	16,07%	16,07%		57,14%
Definir, diseñar y velar por el programa de privacidad de la información de la organización	16,00%	12,00%	12,00%		60,00%
Definición de controles de TI en materia de seguridad de la información	15,15%	15,15%	10,61%	1,52%	57,58%
Creación de programas de entrenamiento en materia de seguridad de la información	12,73%	20,00%	12,73%		54,55%
Definir o diseñar escenarios/simulaciones/Playbooks en relación con ciberriesgos	9,09%	31,82%	18,18%		40,91%
Creación de programas de gobierno y gestión en materia de seguridad de la información	4,17%	20,83%	12,50%		62,50%
Definir, implementar y asegurar el programa de protección de datos personales de la empresa	16,00%	14,00%	14,00%		56,00%

En el sector de la consultoría especializada, el gobierno y el sector financiero, lo que más se valora es que el CISO, entrega información relacionada con la gestión de la seguridad para la toma de acción, por encima de los demás criterios. Una particularidad en el sector de la consultoría especializada es que el CISO también entrega información relacionada con los riesgos de seguridad y ciberseguridad para la toma de decisiones.

En el sector de la educación se reconoce que no existe esta figura, si bien es cierto que desarrollan algunas funciones con relación a la seguridad no existe un rol líder que se encargue de orientar a la empresa en ese sentido, lo cual claramente refleja un bajo nivel de gobierno de la seguridad.

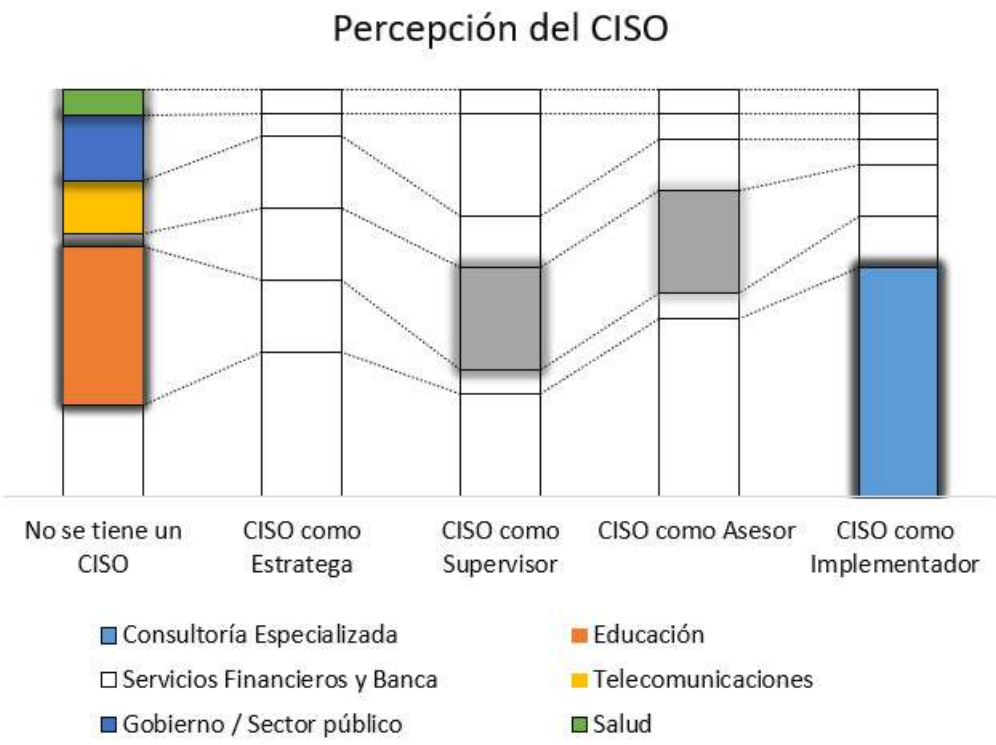
En el sector de la salud y de telecomunicaciones, lo que entrega el CISO como información en el caso de las empresas que tienen este cargo definido, entrega solo información de las posibles brechas de seguridad, esto se puede leer como una actividad reactiva que denota la emergencia manifiesta de desarrollar esta posición, frente a un constante asedio del adversario en el sector (Proofpoint-Ponemon, 2023).

Todas las organizaciones de una u otra manera perciben al CISO (Proofpoint, 2023), para el caso de la realidad nacional existen posiciones interesantes y encontradas que pueden ser explicadas por la realidad y madurez de las empresas y el sector en el que ellas se desempeñan. La gráfica 42, pretende explicar este comportamiento.

La figura de un CISO ejecutivo, un rol que va más allá de una visión netamente técnica y que esté más orientada al negocio parece ser por los datos que no es la lectura que están haciendo los distintos sectores de la industria, a excepción del sector financiero todos los demás sectores señalan que esa figura no existe, en especial el sector de la educación que es el que más lo resalta.

El sector de la consultoría especializada ve al CISO como un implementador del programa de seguridad y los controles, al revisar con las funciones del área, entonces claramente se puede determinar que la lectura es de un CISO táctico en el mejor de los casos que ayuda en la implementación y eso aunado a la información que entrega información de gestión se ratifica este nivel de lectura.

El sector financiero tiene una vista encontrada, por un lado lo ven como un supervisor una lectura viable toda vez que es un sector de la industria con una regulación amplia que debe velar por el cumplimiento de muchas medidas de control frente a los marcos regulatorios nacionales e internacionales, y en segundo lugar como un asesor que está soportado en la idea que en-



Gráfica 42. Percepción del CISO por industria

trega información de la gestión de riesgos y cuyas áreas de seguridad ya están desarrollando y viendo a la seguridad como una función que apoya a la resiliencia operacional del negocio.

Esto muestra que las empresas colombianas tienen unas grandes oportunidades para fortalecer el rol, darle un nivel de relevancia como ejecutivo y hacer que esta relación prospere, madure y contribuya al desarrollo de los modelos de negocio (Chelly, M. et all, 2023).

En cuanto a la forma como el CISO prefiere incrementar su valor y conocimientos es variado, la principal fuente para ello son las certificaciones con un 51%, la educación formal 41%, seguido de los cursos cortos con un 26%, la gráfica 43 muestra esta tendencia.

Sin embargo, el CISO en cada sector de la industria si muestra unos interesantes patrones de formación.

Los Cisos en el sector de la consultoría prefieren los cursos de formación ejecutiva con un 55% de las veces por encima de todos los demás, los pocos Cisos que existen en el sector salud prefieren con un 22% los diplomados, los Cisos del sector gobierno prefieren la educa-

Gráfica 43. Preferencia de formación del CISO

ción formal, claramente aprovechando los convenios y oportunidades que ofrece el estado en la formación en el mundo de las Tics, los profesionales de seguridad que se identifican como Cisos pese a que no estén definidos como tal, prefieren el mundo de las certificaciones. En el sector financiero la situación es diferente los Cisos en este sector por la importancia y relevancia prefieren las charlas especializadas y claramente los eventos de gran tamaño en ciberseguridad son de sus preferidos, por último y no menos importante los Cisos del sector de las telecomunicaciones prefieren los cursos cortos. La tabla 13 describe este comportamiento.

Siendo el CISO nuevo dentro de la esfera de los ejecutivos de las empresas, es claro que tiene que empezar a pulir sus capacidades. Al revisar lo que consideran los encuestados que debe mejorar, sus capacidades estratégicas se colocan en primer lugar con un 41%; un 36% las capacidades intelectuales; un 26% las capacidades humanas; y, por último, la experiencia profesional con un 25%.

Es de anotar que las dinámicas de las empresas y los sectores de la industria colombiana hacen que se tengan algunos matices interesantes de estos datos, representados en la gráfica 44.

El sector de la consultoría en términos generales ve que las capacidades estratégicas son aquellas que deben ser mejoradas por los Cisos, razonable si analizamos que son áreas de seguridad más maduras que necesitan ya de un ejecutivo que pueda liderar y comunicar de una mejor manera la seguri-

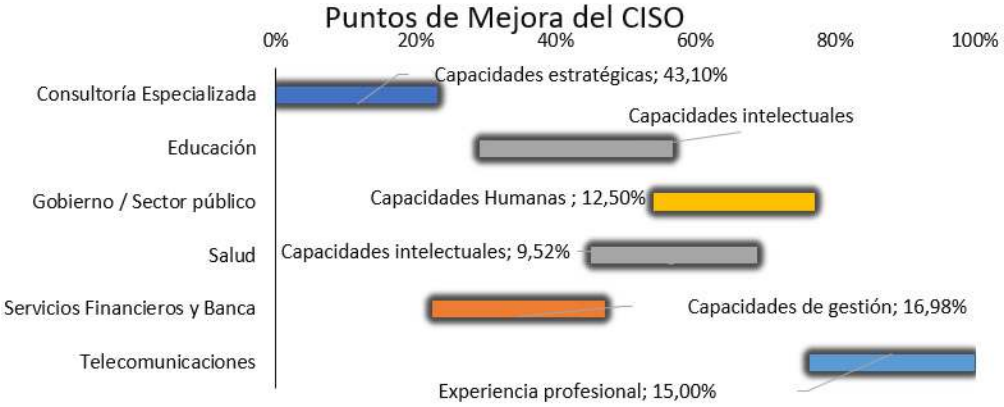
Tabla 14. Preferencia de formación de los Cisos por sectores de industria

Tipo de Formación	Consultoría Especializada	Educación	Gobierno / Sector público	Salud	Servicios Financieros y Banca	Telecomunicaciones
Educación formal universitaria	37,10%	17,74%	14,52%	3,23%	14,52%	12,90%
Charlas especializadas	42,86%	11,43%	11,43%	2,86%	20,00%	11,43%
Programas de formación ejecutiva	54,84%	9,68%	6,45%	3,23%	16,13%	9,68%
Cursos cortos	44,12%	8,82%	11,76%	5,88%	11,76%	17,65%
Certificaciones	38,46%	15,38%	12,82%	7,69%	15,38%	10,26%
Diplomados	42,42%	21,21%	9,09%	6,06%	15,15%	6,06%

dad como lo demanda la organización.

En el sector de la educación y salud, se necesita que el CISO mejore sus capacidades intelectuales que están asociadas a la actualización de sus conocimientos, toda vez que en este sector es probable que los profesionales de TI estén haciendo las transiciones al mundo de la seguridad y por tanto la actualización es importante.

El sector público, considera que las capacidades humanas de los Cisos son algo muy importante y que debe mejorar, es entendible puesto que en este sector el CISO es visto como un supervisor que puede ser interpretado como una persona rígida y poco flexible que puede



Gráfica 44. Puntos de mejora del CISO

estar necesitando mejorar su nivel de relacionamiento para que sus iniciativas pasen de un deber hacer como mensaje a uno de poder hacer para generar valor.

El sector financiero, considera que las capacidades de gestión son importantes y sobre todo que en este sector se debe enriquecer mucho el lenguaje del profesional al hablar de los riesgos bien sea porque requiera para tener diálogos abiertos con los líderes financieros y gerentes de las empresas (Balbix, 2023).

En el sector de las telecomunicaciones la experiencia de los Cisos es lo que se debe mejorar de tal manera que le ayude a sobre llevar los distintos retos que el sector posee, esto es un ejercicio que puede tener sus riesgos porque al buscar personas con mucha experiencia se puede incurrir en el riesgo de acrecentar la brecha de talento de la que hoy se habla en el mercado de la ciberseguridad (ISACA, 2023).

Temas emergentes

La gráfica 45 muestra los temas relevantes y emergentes que tienen en la mira los profesionales de seguridad. Para este año amenazas persistentes avanzadas, fuga de información sensible, ataques a infraestructuras críticas, seguridad y control en la computación en la nube y la inteligencia artificial, son los temas que más están en el radar de

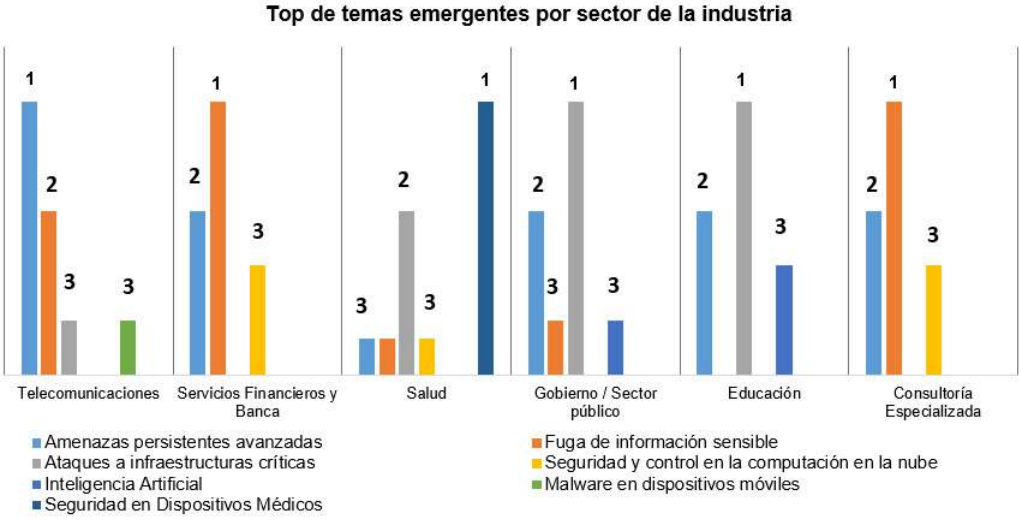
Gráfica 45. Temas emergentes

los profesionales de seguridad. Parámetros que coinciden con algunos de los asuntos que despiertan la atención de la agenda de los ejecutivos de seguridad en este 2023 y los que se verán en el 2024 (IBMc, 2023; Gartner, 2023; Forrester, 2022).

Consideraciones de los datos

Para todos los sectores de la industria se encuentran matices interesantes que direccionan claramente los esfuerzos y orientaciones del profesional y las áreas de seguridad, lo cual obviamente lleva a ver sectores con niveles de esfuerzo, madurez y realidades algo distantes. La gráfica 46 muestra los patrones de interés de los distintos sectores de la industria en relación con los temas emergentes.

De ella se puede decir, el sector de las telecomunicaciones ve a las amenazas persistentes, la fuga de información, el malware de dispositivos móviles y los ataques a infraestructuras críticas como sus mayores temas emergentes. El sector financiero por otro lado, ve a la fuga de información, las amenazas persistentes avanzadas y seguridad y control en la computación en la nube como sus temas a ser monitoreados y considerarlos emergentes. El sector de la salud ve la seguridad en los dispositivos médicos como su tema más relevante en segundo lugar los ataques de infraestructuras críticas y en tercer lugar se comparten el puesto la seguridad y control en la computación en la nube y las amenazas persistentes avanzadas. El sector del gobierno ve a los ataques de infraes-



Gráfica 46. Distribución de temas emergentes por sectores de la industria

tructuras críticas, las amenazas persistentes, fuga de información e inteligencia artificial como elementos claves que deben ser observados. El sector de la educación los ataques de infraestructuras críticas, amenazas persistentes y la inteligencia artificial como sus elementos relevantes. Por último la consultoría especializada ve a al fuga de información sensible, las amenazas persistentes y a la seguridad y control en la nube como un elemento emergente y de interés.

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 postpandemia que ha revolucionado y cambiado la forma en cómo la seguridad se tiene que plantear en las organizaciones.

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).

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 ciberseguridad 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 encontrar equilibrio entre el valor de las nuevas tecnologías y los ciberriesgos que esto conlleva (WEFb, 2023). Otro de los temas que trae gran atención a la mesa es el tema de los equipos de ciberseguridad (Stottandmay, 2023). Los ciberriesgos y la ciberresiliencia en general están en la agenda de todos los CEO de las organizaciones de todo el mundo y eso no es una sorpresa, realmente es una constante de los últimos años (Istari, 2023). 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 (WEFb, 2023). 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 (Mandiant, 2023).

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 (Mandiantb, 2023). 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 (Giarrusso, M., Nyholm, N., & Seth, K., 2023).

Claramente la pandemia dio una nueva visión al 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, 2023).

En esta nueva era los ejecutivos de seguridad 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 (Heidrick, 2023; Proofprintb, 2023; Coalfire, 2023), que deben poder actualizar el conjunto de herramientas como la comunicación para que puedan interactuar con mayor determinación en los equipos de trabajo.

Los datos de la realidad colombiana 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:

Afianzamiento

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, han empezado a ver a la resiliencia como una capacidad necesaria para operar.
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 voz del CISO continúa su proceso de afianzamiento den-

tro de las organizaciones, cada vez se ven más plazas creadas de profesionales de seguridad como CISOs, directores/gerentes 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 entorno tan cambiante como el actual.

5. 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.
6. 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 organizaciones 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.

Exploración:

7. 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.
8. 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 a repensar sus saberes previos, salir de su zona de confort de manera permanente, entrenarse y continuamente estar en proceso de aprendizaje (Martínez, 2022).
9. 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.

10. 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.
11. 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.
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.

El Futuro:

14. 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.

Referencias

Accenture. (2023). How cybersecurity boosts enterprise reinvention to drive business resilience. https://www.accenture.com/content/dam/accenture/final/accenture-com/document/Accenture-State-Cybersecurity.pdf

AON, (2023). How cyber risk touches nearly all aspects of business risk. https://www.aon.com/2023-cyber-resilience-report/risk/how-cyber-risk-touches-nearly-all-aspects-of-business-risk/

ArcticWolf. (2023). The state of cybersecurity: 2023 trends report. https://arcticwolf.com/resource/aw/the-state-of-cybersecurity-2023-trends-report

Balbix. (2023). Anuj Magazine. Cyber risk in CFO lingo: CISOs need a financial vocabulary. https://www.balbix.com/blog/cyber-risk-in-cfo-lingo-cisos-need-a-financial-vocabulary/

Barracuda. (2023). 2023 spear-phising trends. https://www.barracuda.com/reports/spear-phishing-trends-2023

Barracuda(b). (2023). 2023 email security trends. https://www.barracuda.com/reports/email-security-trends-report-2023

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

CheckPoint. (2023) Global analysis. https://go.checkpoint.com/2023-cyber-security-report/chapter-04.php

Chelly, M. L., Tan, S., & Tran, H. (2023). Building a Cyber Resilient Business: A cyber handbook for executives and boards. Packt Publishing.

Coalfire. (2023). The state of CISO influence 2023. https://www.coalfire.com/insights/resources/reports/the-state-of-ciso-influence-2023

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

Cofense (2023). from https://cofense.com/lp/q1-cofense-phishing-intelligence-report/

CyberEdge Group. (2023). Cyberthreat Defense Report. https://cyber-edge.com/cdr/

Cybereason. (2022). Ransomware the true cost to business 2022. https://www.cybereason.com/ransomware-the-true-cost-to-business-2022

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

Diligent Institute. 2023. What Directors Think 2023. Diligent Institute. https://www.diligentinstitute.com/research/what-directors-think-2023/

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

Deepinstinct. (2023). Voice of SecOps V4. https://info.deepinstinct.com/voice-of-secops-v4-2023

Dynatrace. (2022). Observability and security are key to closing vulnerability gaps. https://www.dynatrace.com/news/press-release/global-ciso-research-2022/

ECIIA. (2023). Risk in Focus 2024: Hot topics for internal auditors. https://www.eciia.eu/2023/09/risk-in-focus-2024-hot-topic-for-internal-auditors/

EY. (2023). If AI holds the answers, are CEOs asking the right strategic questions? https://www.ey.com/en_gl/ceo/ceo-outlook-global-report

Forrester. (2022). Forrester's 2023 predictions indicate a bumpy road ahead for CISOs. VentureBeat. https://venturebeat.com/security/forrester-2023-predictions-indicate-a-bumpy-road-ahead-for-cisos/

Gartner. (2023). Top 10 Strategic Predictions for 2023 and beyond. (n.d.). Gartner. https://www.gartner.com/en/articles/gartner-top-10-strategic-predictions-for-2023-and-beyond

FBI. (2023). Internet crime report 2022. https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

FINSIN. (2023). Reporte (bi)mensual de Phishing Abril y Mayo 2023. FINSIN. https://finsin.cl/2023/06/13/reporte-bimensual-de-phishing-abril-y-mayo-2023/

Fortinet. (2023). Cybersecurity Skills Gap. https://www.fortinet.com/content/dam/fortinet/assets/reports/2023-cybersecurity-skills-gap-report.pdf

FS-ISAC. (2023). Navigating Cyber2023. https://www.fsisac.com/navigatingcyber2023

Giarrusso, M., Nyholm, N., & Seth, K. (2023). 2023 EY Global Third-Party Risk Management Survey. https://www.ey.com/en_gl/risk/2023-ey-global-third-party-risk-management-survey

Heidrick. 2023 global chief information security officer (CISO) survey. https://www.heidrick.com/en/insights/cybersecurity/2023-global-chief-information-security-officer-survey

HCLTech. (2023). Tech Trends 2023 – Business and Industry Edition. https://www.hcltech.com/sites/default/files/document/open/TechTrends2023_Business-and-Industry-edition-FV.pdf

IBM. (2023). Chief Executive Officer Study: Decision-making in the age of AI. https://www.ibm.com/thought-leadership/institute-business-value/c-suite-study/ceo

IBM(b). (2023). Cost of a Data Breach Report 2023. https://www.ibm.com/downloads/cas/E3G5JMBP

IBM(c). (2023). IBM institute for business value | research brief. Ibm.com. Retrieved October 17, 2023, from https://www.ibm.com/downloads/cas/JLKJK1ZP

Indusface. (2022). The state of application security 2022. https://www.indusface.com/resources/research-reports/the-state-of-application-security-q4-2022/

Imperva. (2022). Quantifying the cost of API insecurity. https://www.imperva.com/resources/resource-library/reports/quantifying-the-cost-of-api-insecurity/

Ironscale. (2022). How much does phishing cost businesses? https://secure.ironscales.com/the-business-cost-of-phishing/report-download

ISACA. (2023). State of Cybersecurity 2023, Global Update on Workforce Efforts, Resources and Cyberoperations. https://www.isaca.org/state-of-cybersecurity-2023

ISSA-ESG. (2023) Life and times 2023 download landing page. https://issai.informz.net/issai/pages/life_and_times_2023

ISTARI (2023). The CEO report on cyber resilience. https://istari-global.com/insights/articles/ceo-report/

KPMG. (2023). Cybersecurity considerations 2023. https://kpmg.com/xx/en/home/insights/2023/02/cybersecurity-considerations-2023.html

KnowBe4. (2023). TYP phishing by industry benchmarking. https://www.knowbe4.com/typ-phishing-by-industry-benchmarking

Kroll. (2023). Cyber Risk and CFOs. https://www.kroll.com/-/media/kroll-images/pdfs/cyber-risk-cfos-report.pdf

Magnet. (2023). 2023 State of Enterprise Digital Forensics and Incident Response. https://www.magnetforensics.com/resources/2023-state-of-enterprise-digital-forensics-and-incident-response/

Mandiant (2023). M-Trends 2023. https://www.mandiant.com/m-trends

Mandiant(b). (2023). | Mandiant Cyber Security Forecast 2023. https://www.mandiant.com/resources/reports/mandiant-cyber-security-forecast-2023

Marsh. (2022). Cyber resilience: 12 key controls to strengthen your security. https://www.marsh.com/us/services/cyber-risk/insights/cyber-resilience-twelve-key-controls-to-strengthen-your-security.html

Martinez, J. (2021). N°179 Aprender del futuro. http://www.javiermartinezaldanondo.com/n179-aprender-del-futuro/

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

Minterellison. (2023). Perspectives on Cyber Risk 2023: the real cost of a data breach – Insight. https://www.minterellison.com/articles/

perspectives-on-cyber-risk-2023-the-real-cost-of-a-data-breach

NACD. (2022). 2022 GOVERNANCE OUTLOOK. https://boardleadership.nacdonline.org/rs/815-YTL-682/images/2022_Governance_Outlook.pdf

Nuspire. (2023). Second annual CISO research report on challenges and buying trends: A focus on optimization. https://5182296.fs1.hubspotusercontentna1.net/hubfs/5182296/Analyst%20research/Nuspire_Annual%20CISO%20Report_25May23.pdf

OPSWAT. (2023). 2023 state of web application security. https://www.opswat.com/resources/reports/2023-state-of-web-application-security

PwC. (2023). Cyber threats 2022: A year in retrospect. https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect.html

PwC(b). 2023. Winning today's race while running tomorrow's. PwC. https://www.pwc.com/gx/en/issues/c-suite-insights/ceo-survey-2023.html

PwC(c) (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-Ponemon. (2023). 2023 Ponemon healthcare cybersecurity report. https://www.proofpoint.com/us/resources/threat-reports/ponemon-healthcare-cybersecurity-report

Proofpoint(a). (2023). 2023 Human Factor. https://www.proofpoint.com/uk/resources/threat-reports/human-factor

Proofpoint(b). (2023). 2023 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

Proofpoint(c). (2023). 2023 State of the Phish. https://www.proofpoint.com/us/resources/threat-reports/state-of-phish

Proofpoint(d). (2023). WHAT WE KNOW overview. https://www.proofpoint.com/sites/default/files/threat-reports/Proofpoint_Threat_Research_Social_Engineering_Report_2022.pdf

Secureworks. (2023). Learning from incident response: 2022 year in review. https://www.secureworks.com/resources/rp-irs-learning-from-incident-response-team-2022-year-in-review

Sophos. (2023). El estado del ransomware 2023. https://assets.sophos.com/X24WTUEQ/at/jr9ftt3m4qmzbw86m8wgq5f/sophos-state-of-ransomware-2023-wpes.pdf

Stottandmay. (2023). Cyber Security in Focus 2023. https://resources.stottandmay.com/hubfs/Research/2023_Cyber%20Security%20in%20Focus_Web.pdf

TrendMicro. (2023). Future/tense: Trend micro security predictions 2023. https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2023

Thompson, C., & Hopkin, P. (2021). Fundamentals of risk management: Understanding, evaluating and implementing effective enterprise risk management (6th ed.). Kogan Page.

Toscano, J. Final decision on SEC's cyber-security disclosure rules pushed to. https://www.forbes.com/sites/joetoscano1/2023/07/02/final-decision-on-secs-cybersecurity-disclosure-rules-pushed-to-october-2023/

Verizon (2023). Data Breach Investigation Report. https://www.verizon.com/business/resources/T5b/reports/2023-data-breach-investigations-report-dbir.pdf

Vmware. (2022). Global Incident Response Threat Report. https://www.vmware.com/content/dam/learn/en/amer/fy23/pdf/1553238_Global_Incident_Response_Threat_Report_Weathering_The_Storm.pdf

WEF - World Economic Forum (2023) Global Risk Report 2023. https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf

WEF(b) - World Economic Forum (2023) Global Cybersecurity Outlook. Meeting of experts. https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf

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

Zscaler. (2023). Informe sobre el estado del phishing de Zscaler ThreatLabz https://info.zscaler.com/resources-industry-reports-threatlabz-phishing-report-es

***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.*