# XXI Encuesta Nacional de Seguridad Informática

Resiliencia un aspecto clave en la ciberseguridad

DOI: 10.29236/sistemas.n159a4

**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 abril y junio de 2021, contó con la participación de 173 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, y contó con la cooperación de otras asociaciones como ISACA Capítulo Bogotá, Tacticaledge, CISOS.CLUB, CISObeat (Perú) entidades y comunidades 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 a corto, mediano y largo plazo, además de construir mejores posiciones en las organizaciones. Ese entendimiento, sumado a conocer el contexto internacional, proporciona una proyección al entorno nacional para enfrentar los retos y desafíos en ambientes cada vez más permeados por la realidad digitalmente modificada.

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

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

Es de resaltar el análisis longitudinal realizado sobre los últimos 10 años de la encuesta, sobre la variable incidentes que fue publicado en 2020 denominado “Evolución de los incidentes de Seguridad de la Información en Colombia: 2010-2020” (Cano & Almanza, 2020), como un registro analítico y documentado del pasado y una prospectiva sobre el futuro de la seguridad en Colombia.

Como todos los años, se revisan para la realización de este informe, algunos de los reportes más representativos de la industria, afines con los datos analizados de este instrumento.

## Estructura de la encuesta

El estudio contempla 40 preguntas repartidas en varias secciones sobre diferentes asuntos.

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

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

**Incidentes de seguridad**: Muestra los detalles y tipos de incidentes presentados, un barrido por las prácticas más importantes en el manejo y diligencia de la evidencia digital, como herramienta en la persecución de los ciberdelincuentes.

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

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

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

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

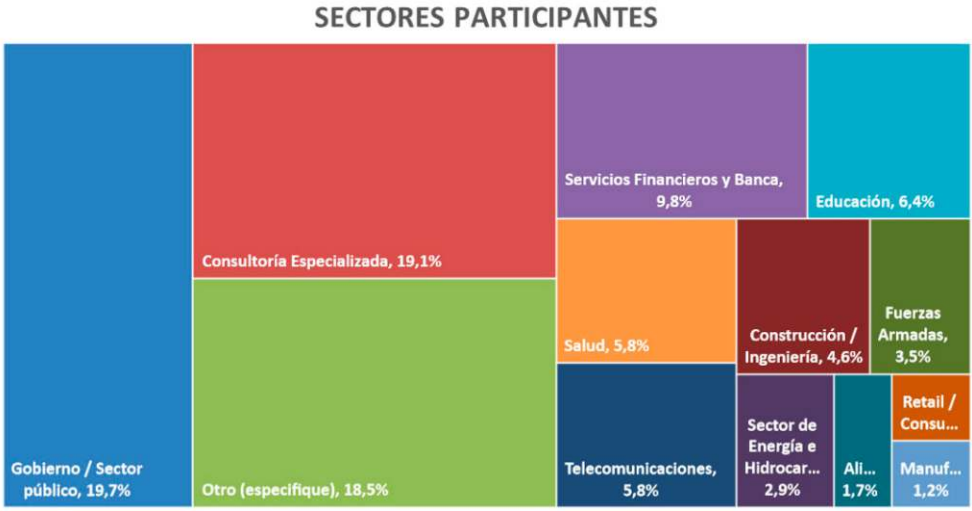
**Cambios:** Cada año luego de revisados los resultados de la encuesta, las opciones y los análisis correspondientes de pertinencia y relevancia, se cambian, adicionan, o modifican opciones. Este año no fue la excepción y tienen unas pequeñas variaciones en cuanto a la cantidad, pasando de 43 en el 2020 a 40 en el 2021.

## Hallazgos principales

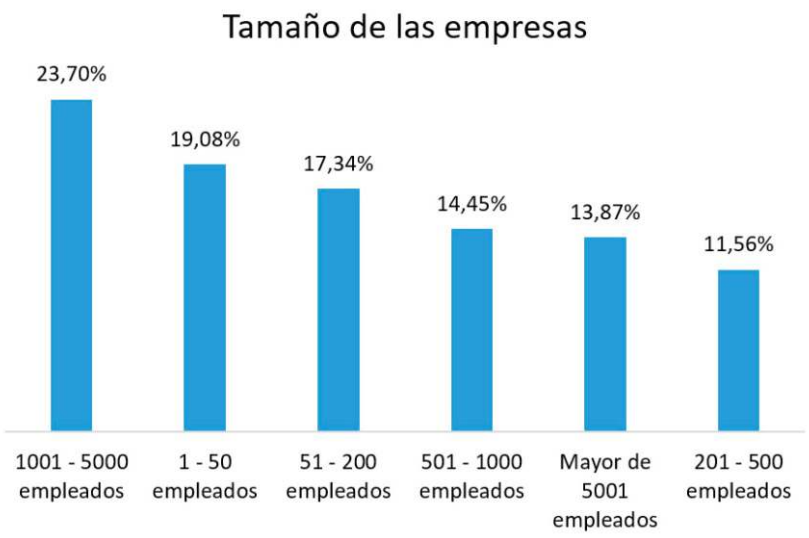
### Demografía

### Sectores participantes

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




*Gráfica 1: Sectores participantes*



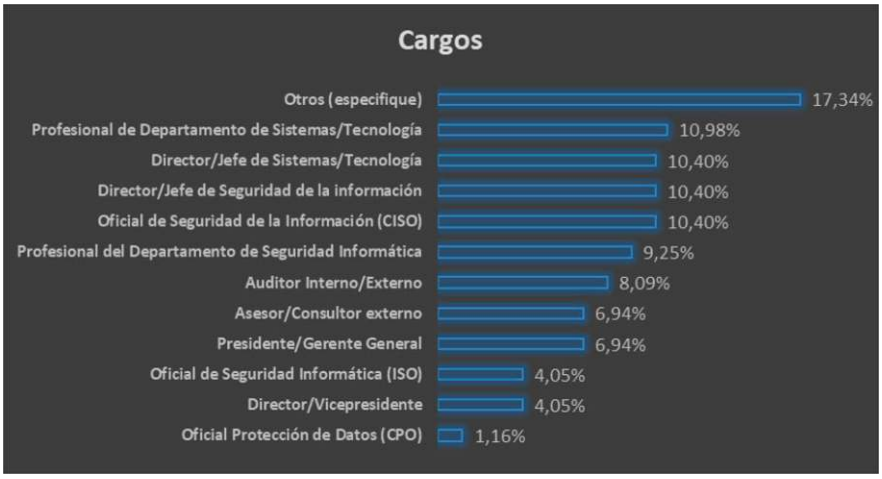

*Gráfica 2: Tamaño de las empresas participantes*

mayor participación de la encuesta para este año fueron Gobierno, Sector Financiero y la Consultoría Especializada.

En este año Gobierno, Consultoría, Otros sectores, Servicios financieros y Educación, son los principales grupos que participan en la encuesta.

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 profesionales de las áreas de TI, oficiales de Seguridad, auditores internos y directores de Seguridad de la Información.

Así mismo, figuran otras clasificaciones para los profesionales de seguridad digital en el país, tales como analistas y profesionales de planta de seguridad, docentes de cátedra y planta de las áreas de seguridad como los más relevantes. 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 la *definición de controles de TI en materia de seguridad de la información*, luego la *creación de programas de entrenamiento* y, en tercer lugar, *establecer e implementar un modelo de políticas*.

La gráfica está expresada con relación a los cambios que sufren las funciones del profesional de seguridad. Para este año se agregaron tres nuevas funciones: Definir, diseñar y velar por el programa de


*Gráfica 4: Funciones del responsable de seguridad*

privacidad de la información; definir o diseñar escenarios/simulaciones/Playbooks en relación con ciberriesgos y definir programas de resiliencia digital.

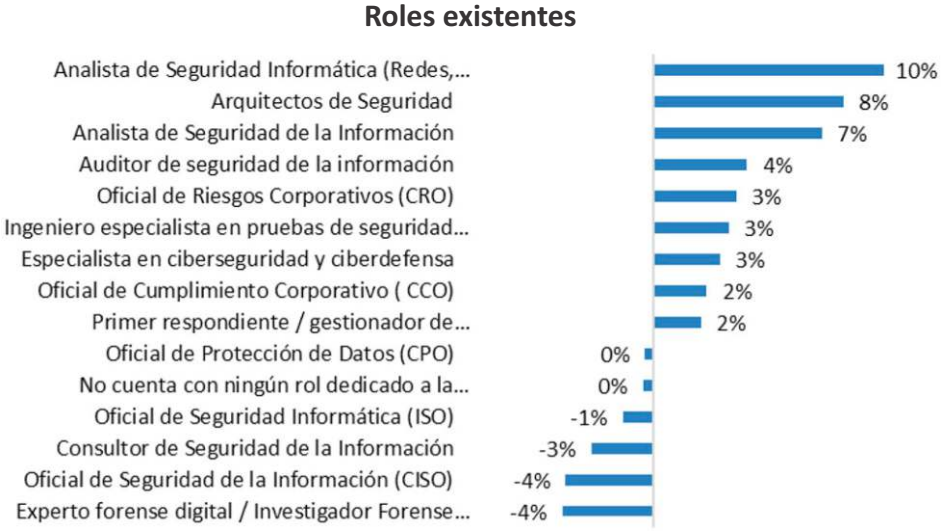
Frente al año anterior, las funciones que reflejan un incremento tienen que ver con la creación del programa de gobierno y gestión, la supervisión de los procesos de cumplimiento, además de velar por la protección de la información personal.

Los que tuvieron decrecimiento en comparación con el año anterior son la supervisión y gestión de los procesos de investigaciones forenses, la interacción con las diferentes áreas del negocio y el más bajo está relacionado con informar a la alta gerencia sobre el avance de los programas de seguridad en la organización.

Esto refleja la dinámica de lo que los profesionales de seguridad en tiempos disruptivos, como los actuales, deben atender y repensar frente a un programa de seguridad de la información: asegurar que se cumpla lo mínimo, para seguir en ese proceso de construir resiliencia digital.

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, seguido por la Vicepresidencia/Director Departa-


*Gráfica 5: Dependencia del área de Seguridad*




*Gráfica 6: Roles de Seguridad*

mento de Tecnologías de la Información y en tercer lugar del Director/Jefe de Seguridad Informática.

En la gráfica 6 se observan los roles dentro de una organización en materia de seguridad digital. En este año los analistas de seguridad de la información, de seguridad informática y el Oficial de Riesgos Corporativos (CRO) son los primeros roles presentes en las organizaciones.

Al comparar con el año anterior encontramos que las posiciones de analistas y arquitectos son las que mayor variación y presencia tienen en las organizaciones. Entre los roles que decrecieron figuran el consultor de seguridad, el CISO y el experto en forensia digital.

## Consideraciones de los datos

Según El *Data Breach Report* (2021) de la Firma Verizon, el tamaño de las empresas sí importa. En su metodología señala que las empresas de menos de 1000 empleados son consideradas (SMB) (*Small, Medium Business*) y por encima de 1000 empleados grandes empresas.

Según este informe, se evidencia que a las empresas grandes y pequeñas las vienen afectando los fenómenos de ciberseguridad a nivel global. Si bien, los grandes titulares de la industria muestran los casos complejos como Solarwinds, Colonial, JBS, Fireeye, entre otros, han ocupado las primeras planas de los medios; no significa que la ciberseguridad en las empresas pequeñas no tenga relevancia.

Los roles y las responsabilidades de los profesionales de seguridad varían, y se mueven de acuerdo con los tiempos que actualmente son turbulentos, inciertos, novedo-

sos y ambigüos (Tessore, 2020). Según F-Secure en su reporte The CISOs' New Dawn (2021), los profesionales de seguridad tanto en Europa (57%) y en los Estados Unidos (59%) ven un claro incremento de responsabilidades en rol. Las temáticas adicionales están relacionadas con la privacidad (tendencia igualmente marcada en Colombia); hecho que confirma al no existir una persona responsable de la protección de los datos personales, lo que termina ubicando esta actividad como parte de las responsabilidades de los profesionales de seguridad.

Así mismo, la pandemia ha cambiado la realidad y ha definido nuevas normas para la protección de los activos digitales de las organizaciones; algunos inclusive empiezan a entender la dinámica del trabajo remoto como una realidad que llegó para quedarse y que significa repensar la forma en cómo las funciones de las áreas de seguridad deben rediseñarse; así lo muestra el informe de la firma Ivanti, titulado How the Pandemic Has Shifted CISO Priorities (2021).

El 93% de los profesionales de seguridad según Ponemon-LogRythm (2021) no reportan directamente al CEO, manifestando que hay al menos tres niveles para que la información llegue a quienes toman decisiones; en consecuencia, es necesario que la dependencia de la seguridad tenga impacto en el proceso de decisiones de la organización; entre más distancia existan entre el Líder de Seguridad Digital, su equipo y los cuerpos directivos, menos agilidad y fluidez en la toma de decisiones claves y mayor será el esfuerzo en el desarrollo de la ciberresiliencia de la organización.

En Colombia, si bien hay un director de seguridad nombrado o CISO como posición, esto no significa que esté reportando directamente a quienes toman decisiones; se ha avanzado en el tema, pero se requieren mayores esfuerzos en la materia.

Por tanto, esta realidad presenta nuevos aprendizajes en las funciones, roles y responsabilidades de los profesionales de seguridad que seguro en la realidad de Colombia no es distinta y que crea nuevas oportunidades para repensar lo que el profesional de seguridad hace, y hará según evolucionan los tiempos.

## Presupuestos

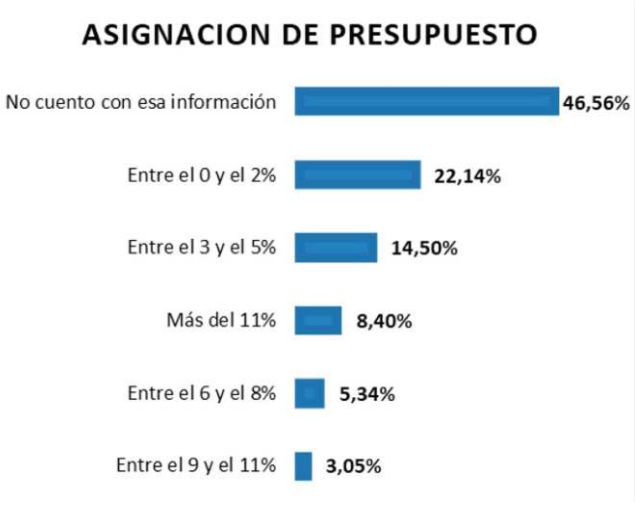
Continúa la asignación de presupuestos para la ciberseguridad; en esta oportunidad el 80% manifiesta tener asignado un presupuesto de seguridad en la organización. Gráfica 7.

La gráfica 8 muestra el monto del presupuesto en relación con el presupuesto global; cerca del 53% de los encuestados lo conoce, mientras que el 47% dice no conocer o no tener la información. Con rela-


*Gráfica 7: Presupuesto de Seguridad*

ción al año anterior, también incrementa el conocimiento del presupuesto asignado del total de la organización. De quienes conocen los montos asignados se puede observar que los montos inferiores al 5% del presupuesto global de la compañía representan el 69%, mientras que el 31% están para los montos superiores al 5%.

La gráfica 9 refleja la distribución de los presupuestos en dólares. Para este año cerca del 52% tiene un monto asignado para la seguridad; que aumenta, comparado con el año pasado cerca de un 7%, mientras el 48% restante manifiesta no conocer dicha información. Algunos movimientos interesantes al revisar y comparar con el año ante-




*Gráfica 8: Porcentaje del presupuesto Global*


*Gráfica 9: Presupuesto de Seguridad*


*Gráfica 10: Inversión de Seguridad*

rior. Aumenta en todos los rangos establecidos con excepción de las franjas de los $US110.000 a $US 130.000 y $US70.000 a $US 90.000 donde disminuye. No obstante, el mayor incremento en términos porcentuales es la franja de mayor de $US130.000, esto es claramente explicable por el hecho que las inversiones en seguridad cada vez son más especializadas y por tanto tienen mayores valores de inversión.

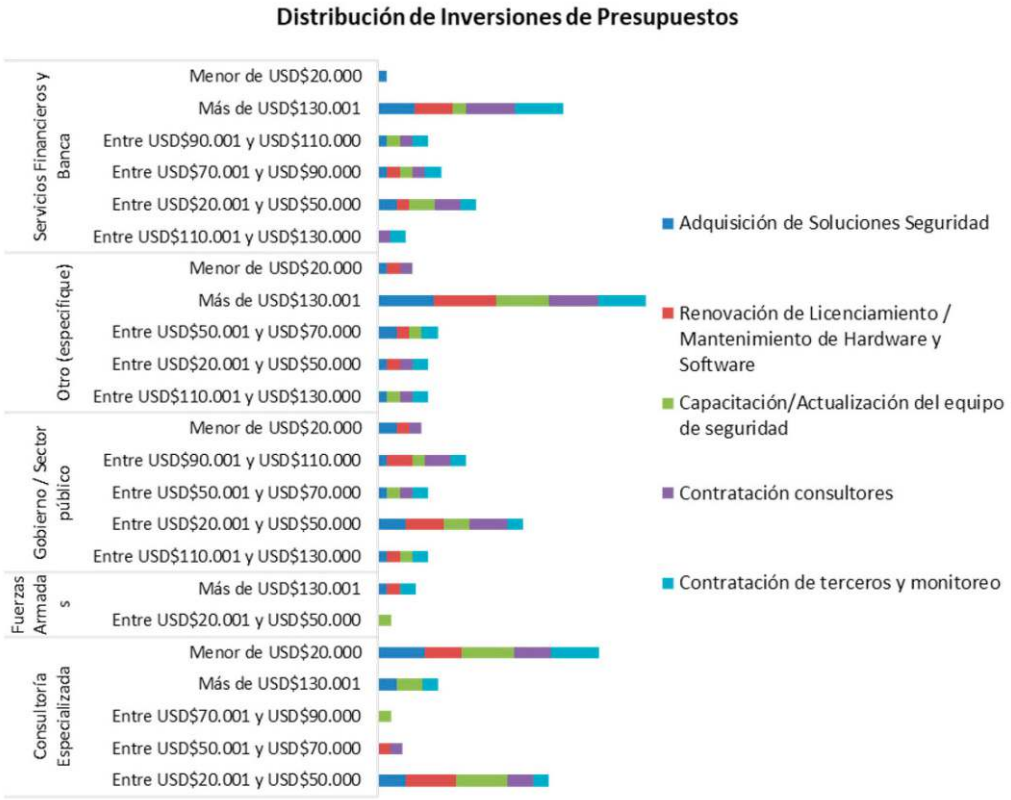
La gráfica 10 muestra la forma cómo se está invirtiendo el dinero en materia de ciberseguridad. Sigue creciendo la inversión en tecnologías de seguridad informática. Renovación de licenciamiento, Sensibilización, Contratación de consultorías y el Monitoreo son en su or-

den la forma en cómo se invierten estos presupuestos asignados.

En la gráfica 11 se puede observar la forma en cómo cada sector de la industria hace sus respectivas distribuciones de las inversiones en seguridad. Hay datos interesantes a observar, el sector financiero invierte en todas las franjas, llama la atención que las inversiones en la franja de más de $US130.000 dólares, es la que involucra a todos los tipos de inversiones, el mismo comportamiento lo mantienen otros sectores, y el sector de Fuerzas Armadas en menor proporción.

El sector de Gobierno mantiene su distribución de inversiones en la franja entre $US20.000 y $US-50.000 y $US90.000 y $US-110.000 dólares, como la distribución más alta; en el sector de la consultoría especializada las franjas más altas son todas las que están por debajo de $US50.000.

Al revisar la destinación de estas franjas se encuentra que la adquisición de soluciones de seguridad no es el primer destino de ninguno de los sectores de la industria principalmente, es solo la destinación de segunda importancia en el Go-




*Gráfica 11: Montos en dólares de las inversiones de seguridad. Sectores vs. inversiones*

bierno, Fuerzas Armadas, y otros sectores.

La renovación de licenciamiento y mantenimiento de *hardware* y *software* es la destinación primaria del sector de Fuerzas Armadas y otros sectores, mientras que es la segunda destinación de inversiones en sectores como la Consultoría especializada.

La Capacitación/Actualización del personal de seguridad de la información solo es la destinación primaria del sector de Consultoría y de ningún otro sector en segundo lugar. La Contratación de servicios de asesoría/consultoría es la destinación primaria de inversiones del sector Financiero, de otros sectores no lo es.

Los Servicios de monitoreo y gestión de seguridad con terceros, es de la destinación en primaria instancia del sector de Gobierno, mientras que la segunda destinación de inversiones del sector Financiero.

## Consideraciones de los datos

Los reportes internacionales ratifican la tendencia de Colombia sobre los aumentos en los presupuestos de seguridad en las organizaciones de todos los tamaños y sectores. Sin embargo, al revisar el informe ISACA (2021) se muestran leves descontentos por la disminución de los presupuestos afectados por la situación disruptiva de la pandemia a nivel global. No obstante, en el mismo estudio se ve un optimismo al ver un incremento de los presupuestos en términos históricos, y en la misma línea se observa un optimismo moderado hacia los próximos 12 meses en relación con el incremento de estos.

En el informe de Ponemon-IBM (2020) el desafío se mantiene con relación a las inversiones de ciberseguridad, mientras que la sofisticación de los ataques incrementa. Son necesarias mayores inversiones en tecnologías, procesos y personas en la búsqueda de organizaciones más resilientes frente a los ciberataques, igual se considera en el informe que si bien los presupuestos mejoran, cerca del 40% considera como gran desafío la consecución de presupuestos acordes con la situación actual.

Todos los informes revisados durante el 2021 (ISACA, 2021; Ponemon-IBM, 2020, Vanti, 202x; Verizon, 2021) y otros son concluyentes en afirmar que el modelo de seguridad ha cambiado por las condiciones disruptivas de la pandemia, y sobre todo por los posibles escenarios del trabajo que vendrán en los próximos tiempos (CISOs. CLUB, 2021), lo que hará que los presupuestos en materia de seguridad cambien y las inversiones en seguridad se ajusten con estos nuevos escenarios.

Sin perjuicio de lo anterior, las inversiones en seguridad se consideran insuficientes para invertir en las

tecnologías más avanzadas requeridas para atender escenarios disruptivos, como lo manifiesta el 63% de los encuestados del informe de Ponemon-LogRhytmn (2021).

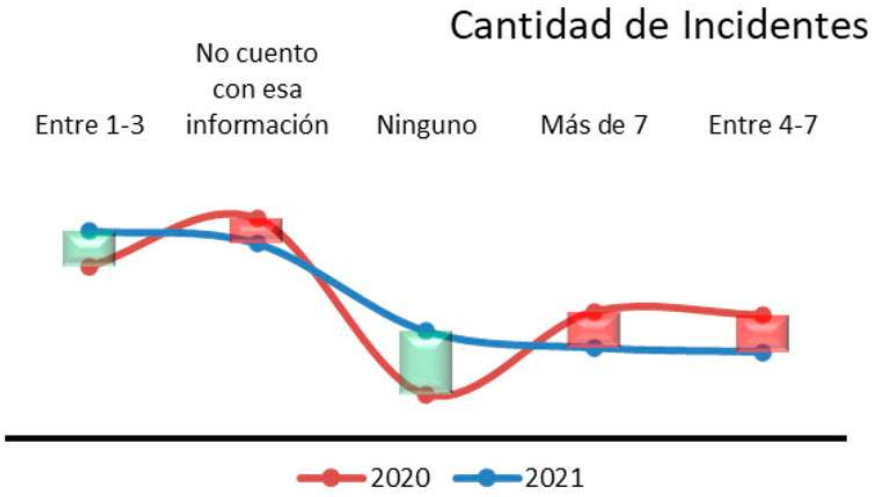
## Incidentes

En Colombia se mantiene la tendencia en materia de incidentes de seguridad en concordancia con las tendencias internacionales. Tales desafíos, en términos de preparación y atención son una exigencia para las organizaciones.

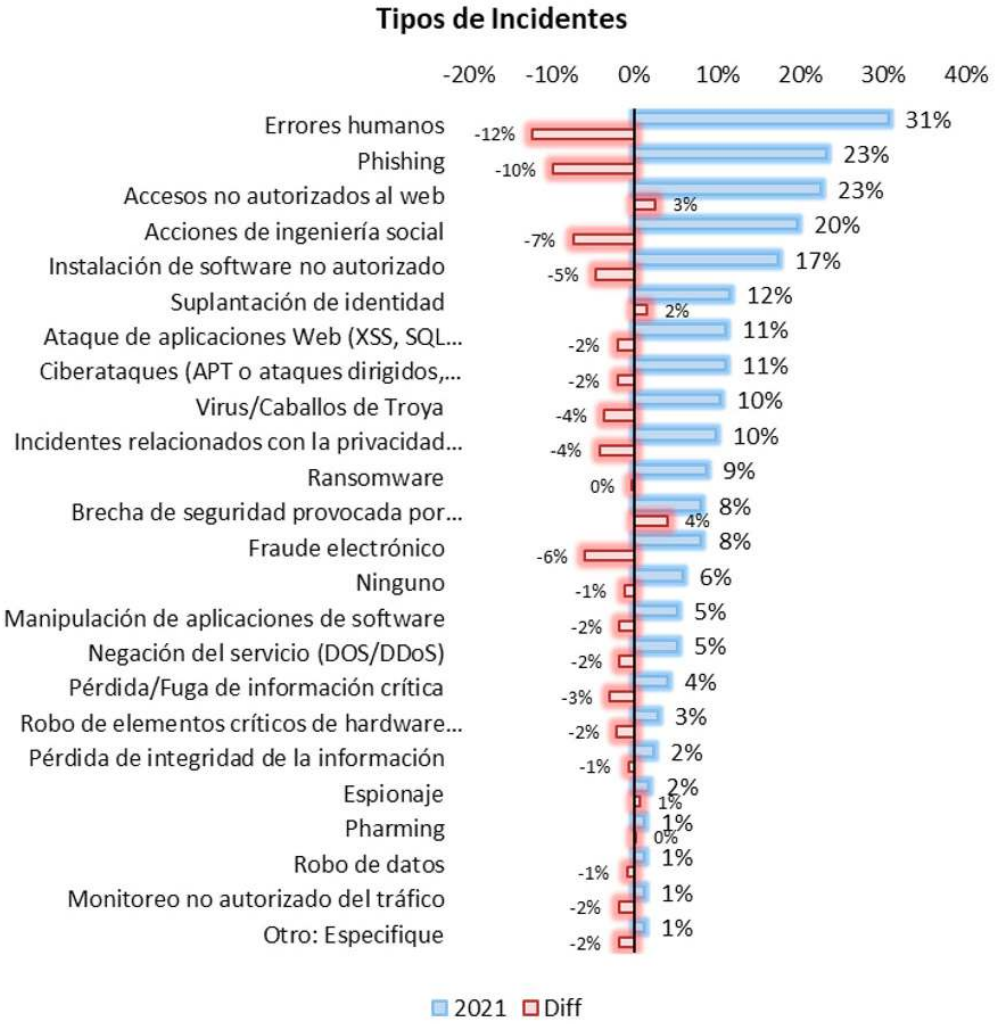
La gráfica 12 muestra la cantidad de incidentes que se presentan en Colombia, según los participantes. Para este año el 72% de los encuestados manifiesta que ha estado en contacto con algún incidente de seguridad en su empresa, en comparación con el año inmediatamente anterior, donde el 68% lo ha manifestado.

En este año, en comparación con el anterior, hay una disminución de las personas que manifiestan no tener conocimiento sobre los incidentes de seguridad, pasando del 32% en el 2020, al 28,31% en el 2021. Llama la atención que hubo un incremento del 9% de aquellos que manifiestan no tener incidentes de seguridad, y la disminución de un 5% en las franjas de incidentes entre 4 y 7 y más de 7 respectivamente. Por el otro lado, se incrementa un 5% de quienes manifiestan tener entre 1 y 3 incidentes en sus organizaciones.

La gráfica 13 relaciona los tipos de incidentes que se presentaron en las organizaciones, así como su variación con relación al año anterior. Para este año hay datos interesantes, se mantienen los errores humanos como el tipo de incidente más reportado; sin embargo, de-



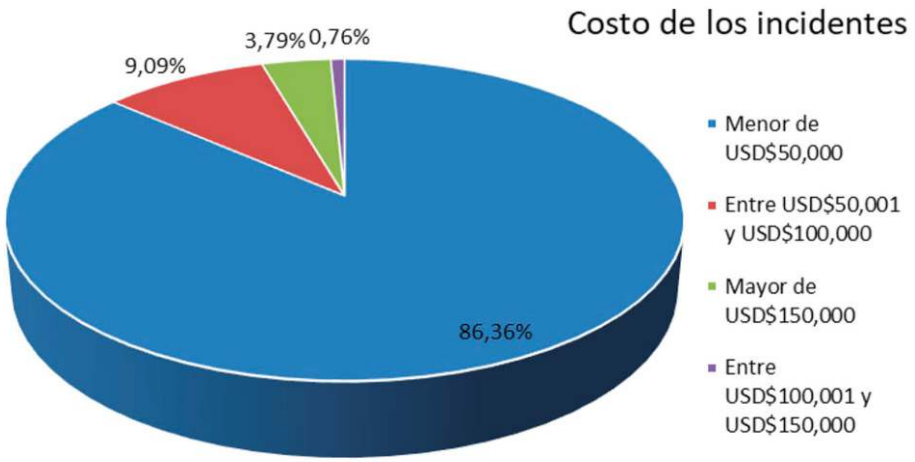

*Gráfica 12: Cantidad de Incidentes. Incidentes*




*Gráfica 13: Tipos de Incidentes de Seguridad*

crece un 12% frente al año anterior. Las brechas de seguridad provocadas por terceros es el tipo de incidente que mayor crecimiento con un 4%, seguido de acceso no autorizados en la web (3%) y suplantación de identidad (2%).

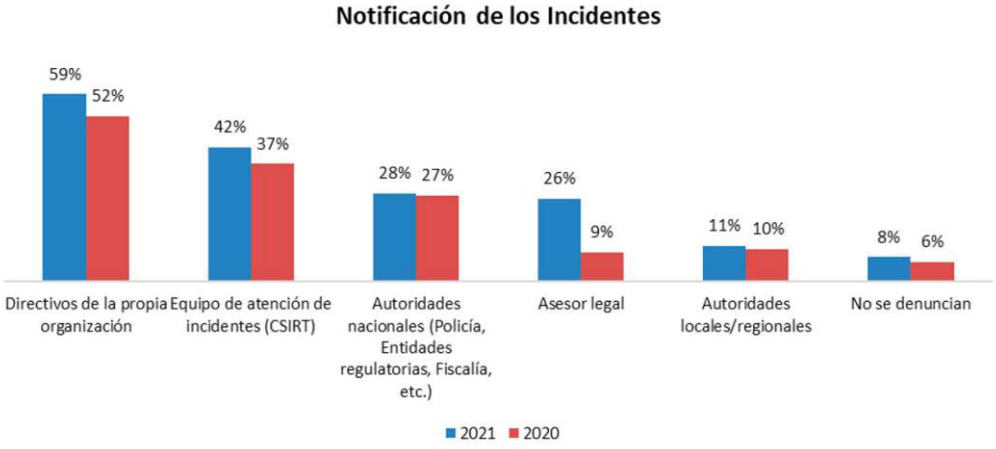
La gráfica 14 representa el costo promedio de los incidentes. Al igual que el año anterior los datos reflejan que hay costos involucrados en relación con los incidentes de seguridad; cerca del 86% manifiesta que sus incidentes cuestan menos de $US50.000, cerca del 9% entre $US50.000 y $US100.000, el 4% manifiesta que le cuesta más de $US150.000 y solo el 1% manifiesta que está en la franja de los $US100.001 hasta los $US150.000 dólares.



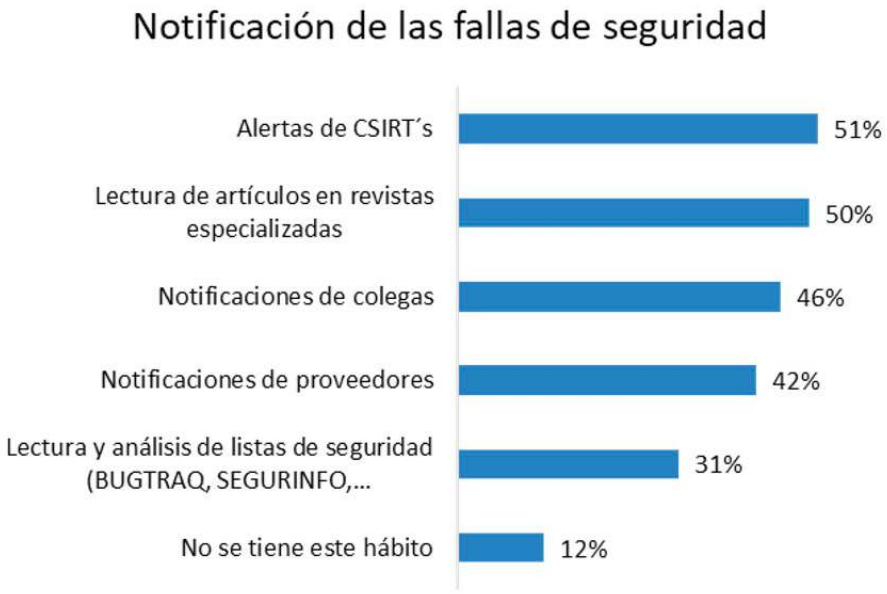

*Gráfica 14: Costos de los Incidentes*

La gráfica 15, muestra ante quién se reportan los incidentes de seguridad. El 59% lo reporta directamente a los directivos de la organización, el 42% lo reporta al equipo de atención de incidentes (CSIRT), el 28% a las autoridades nacionales, el 26% a los asesores legales, el 11% a autoridades locales o regionales y solo el 8% manifiesta que no se denuncian.

La gráfica 16, muestra las razones, como se mantienen los profesionales de seguridad informados acerca de las vulnerabilidades y fallas de los sistemas. Se encuentra que el 51% de los profesionales de




*Gráfica 15: A quien se reportan los incidentes*




*Gráfica 16: Razones para no denunciar los incidentes*

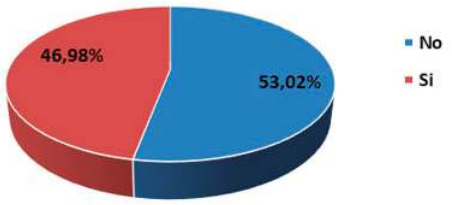
seguridad se enteran o están conectados con CSIRTs, las revistas especializadas son el segundo recurso usado con un 50%, seguido por la notificación con los colegas 46%, luego el contacto con los proveedores (42%), listas de seguridad el 31% y solo el 12% manifiesta no tener ese hábito.

La gráfica 17 resalta que el 61% mantiene algún tipo de contacto con autoridades del orden local o regional, mientras que el 39% no lo hace

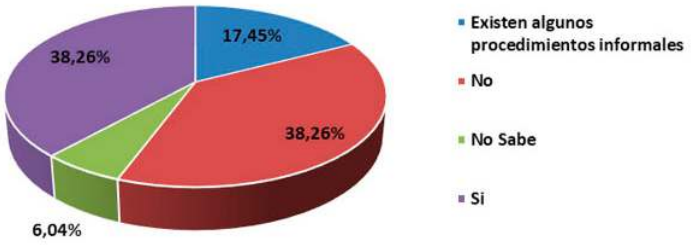
La evidencia digital y su uso dentro del proceso de gestión de incidentes es pieza fundamental para un


*Gráfica 17: Mecanismos para denunciar/compartir*


*Gráfica 18: Consciencia de la Evidencia Digital*




*Gráfica19: Procedimiento de Gestión de Evidencia Digital*




*Gráfica 20: Implementación de procedimientos de evidencia digital*

adecuado mejoramiento. La gráfica 18, resalta la importancia y consciencia en relación con el adecuado manejo de la evidencia digital. El 73% resalta que es consciente de ello, el 14% no lo es y el 13% restante no sabe del tema. La gráfica 19 muestra que el 53% manifiesta tener un procedimiento aprobado para manejo de la evidencia digital y el 47% no lo tiene. La gráfica 20 para este año quiso revisar qué tan

implementados están dichos procedimientos, el 38% manifiesta que existe un procedimiento formal al respecto y el 17% manifiesta que existe informalidad en dichos procedimientos. El 38% indica no tenerlos y solo el 6% no sabe si existe algún procedimiento implementado.

## Consideraciones de los datos

Los reportes internacionales como Verizon (2021) señala que al menos ellos han podido analizar cerca de 29.207 incidentes y que de ellos 5.258 se confirmaron como brechas de seguridad. Algunos datos interesantes indican que el 85% de las brechas involucran a las personas, el 61% a las credenciales y el robo de estas, confirmando la tendencia en Colombia.

El mismo informe advierte que la media del costo de un incidente está en $US21.659; sin embargo, el rango total de los incidentes está entre $US865 y $US653,587. Si bien en Colombia estamos en el rango de la media, hay que resaltar que puede haber mediciones inexactas frente a los costos, toda vez que los incidentes como el *Ransomware* generan un costo adicional, que a lo mejor no se ha considerado.

*Ransomware* definitivamente ha sido el incidente del año 2020; si bien en Colombia es un incidente que se mantiene con niveles bajos en su ejecución, puede no estar en el radar de los profesionales de seguridad, toda vez que desde el año 2020 y hasta la fecha en el 2021, se han visto muchos casos de este tipo, en donde el promedio de pago es de $US170.404 según Sophos (2021). Lo mismo se puede evidenciar en el informe del FBI (2021) que resalta la importancia que ha cobrado el *ransomware* como el incidente que hoy se está considerando a nivel de los estados como un ataque terrorista, con el fin de darle toda la atención de acuerdo con las exigencias de esa clasificación.

Los incidentes cada vez son más serios y complejos de investigar afirma el reporte de CyberEdge Group (2021). En este sentido, se aumentan las iniciativas, cerca del 70%, que permitan mejorar la capacidad de las organizaciones para responder a incidentes, según lo manifiestan IDG (2021). Estos datos confirman los resultados de Colombia, donde el proceso de atención de incidentes es esencial, y por lo tanto debe mejorarse continuamente pese a las presiones propias de dicho proceso: dar respuesta al incidente, investigar el incidente y hacer un manejo adecuado de la evidencia digital.

Definitivamente manejar evidencia, poseer un proceso y tenerlo implementado es indispensable si se quiere tener un proceso de gestión de incidentes robusto y que apalanque la resiliencia digital de las empresas. En el informe de CyberEdge Group (2021), el 13% de los

encuestados no considera usar alguna solución de esta naturaleza, el resto o ya las tiene en uso, o planea usarlas. Por tanto, ratifica lo que está sucediendo en Colombia en este aspecto, es importante y hay que trabajar más en dirección a fortalecer la implementación de este tipo de procedimientos.

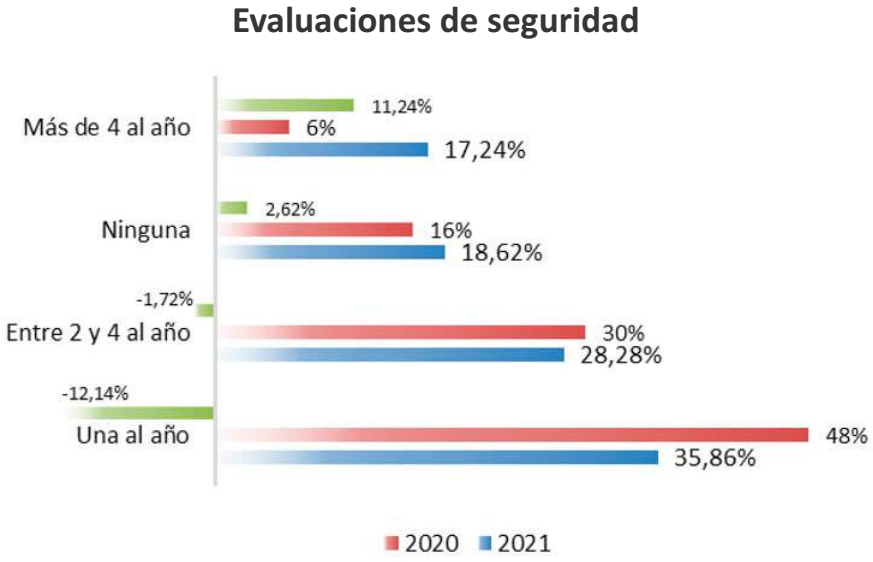
Accenture (2020), indica que la respuesta de incidentes como proceso de la organización se ha incrementado en términos de las inversiones de seguridad, al menos un 25%. Estos datos soportan y ratifican lo que sucede en Colombia, los incidentes tienen presencia, tienen costos y tienen impacto. Accenture (2020) igualmente muestra que el 79% de las empresas bajo estudio están de acuerdo con la colaboración y cooperación entre empresas, como mecanismos para estar mejor preparados para enfrentar los ciberataques, ratificando la tendencia de Colombia en ese sentido.

Los profesionales de seguridad se mantienen informados y usan la práctica de leer artículos y publicaciones especializadas, tendencia que se ratifica a través del informe de Verizon (2021), el cual señala que las investigaciones de seguridad son las formas más utilizadas para descubrir brechas de seguridad.

En Colombia, la práctica de la gestión de incidentes se identifica como una práctica no desarrollada, pero con avances importantes, resultado que ratifica los hallazgos del informe de IDC (2021), según el cual las inversiones en seguridad están orientadas a fortalecer la gestión de incidentes, toda vez que se considera una práctica que necesita mejorar su madurez en las organizaciones para así fortalecer la resiliencia digital.

Todos los grandes informes de la industria concuerdan en confirmar la tendencia de Colombia, en el sentido de que la gran mayoría de organizaciones sufrieron, sufren y sufrirán de un ciberataque; por tanto, la premisa del cuándo, cómo, el porqué, son innecesarias de responder, hoy estamos más ante la necesidad de saber que hacer en el momento de la crisis.

La ciberresiliencia es una capacidad de las organizaciones, que debe ser desarrollada de manera integral en las organizaciones, aquellos tiempos en donde los incidentes de seguridad son atendidos solo por el área de seguridad y de tecnologías de la información están desapareciendo, tal vez pueda darse para incidentes básicos (EY & IIA, 2021); sin embargo, en incidentes complejos en los que la recuperación y la respuesta demandan mayores esfuerzos e involucran a muchas partes, la gestión de incidentes demanda un proceso multidisciplinario; tener planes claros, con ejercicios probados puede ser la clave para que este proceso sea de utilidad en los momentos de crisis.




*Gráfica 21: Evaluaciones de Seguridad*

## Herramientas

La gráfica 21 muestra el uso de las evaluaciones de seguridad como una de las prácticas más usadas. Un 81% de los participantes manifiesta hacer uso de esta práctica como instrumento clave para validar el estado de la seguridad digital de la organización. El 36% de los participantes usa esta práctica una vez al año; el 28% entre dos y 4 veces al año; el 17% manifiesta usa más de 4 veces al año y el 19% dice no usarla.

La gráfica 22 indica cómo los sectores están usando las evaluaciones de seguridad para evaluar y valorar su postura de seguridad; en tal sentido se observa que en pro de mejorar su ciberresiliencia, quien más usa una evaluación de seguridad al año es el sector gobierno con un 10,34%, seguido del sector de la consultoría especializada con un 9,66%. Entre dos y cuatro valoraciones al año se ubican la consultoría especializada con un 6,90%, seguido los servicios financieros con un 6,21%. Ninguna evaluación de seguridad al año está dentro de otros sectores; el segundo lugar es para el sector salud con un 2,76%. Más de cuatro evaluaciones de seguridad al año están dentro de otros sectores, seguido de la consultoría especializada con un 4,14%.

Cabe resaltar que los servicios Financieros y el sector de *Retail* no dejan de hacer pruebas de seguridad durante un período de un año. Por lo demás, los restantes sectores no ejecutan pruebas de seguridad.

La gráfica 23, muestra cuáles son los mecanismos de seguridad co-


*Gráfica 22: Evaluaciones de Seguridad por Sectores*

múnmente usados en las organizaciones. VPNs 53%, el cifrado de datos con un 49% seguido de las soluciones *antimalware*; sin embargo, comparado con el año inmediatamente anterior, son los servicios de inteligencia de amenazas el 7% las soluciones de seguridad con Inteligencia Artificial (IA) 5% y el cifrado de datos con 4% los que tienen un incremento en su uso frente al año 2020.

La gráfica 24 muestra la forma como los sectores principales de la industria usan los diferentes tipos de tecnologías con relación a la ciberseguridad. El sector financiero se concentra en la tercerización de la seguridad, seguido de las soluciones de monitoreo de redes sociales y luego herramientas que le permitan dar cumplimiento a los marcos normativos. El sector Gobierno por su parte se concentra en herramientas de denegación de servicio, seguido de las tecnologías tradicionales de firewall y las vpns. La consultoría especializada tiene como herramientas primarias, las soluciones de seguridad con IA, seguido de los sistemas de contraseña y las soluciones con enfoque de zero trust.

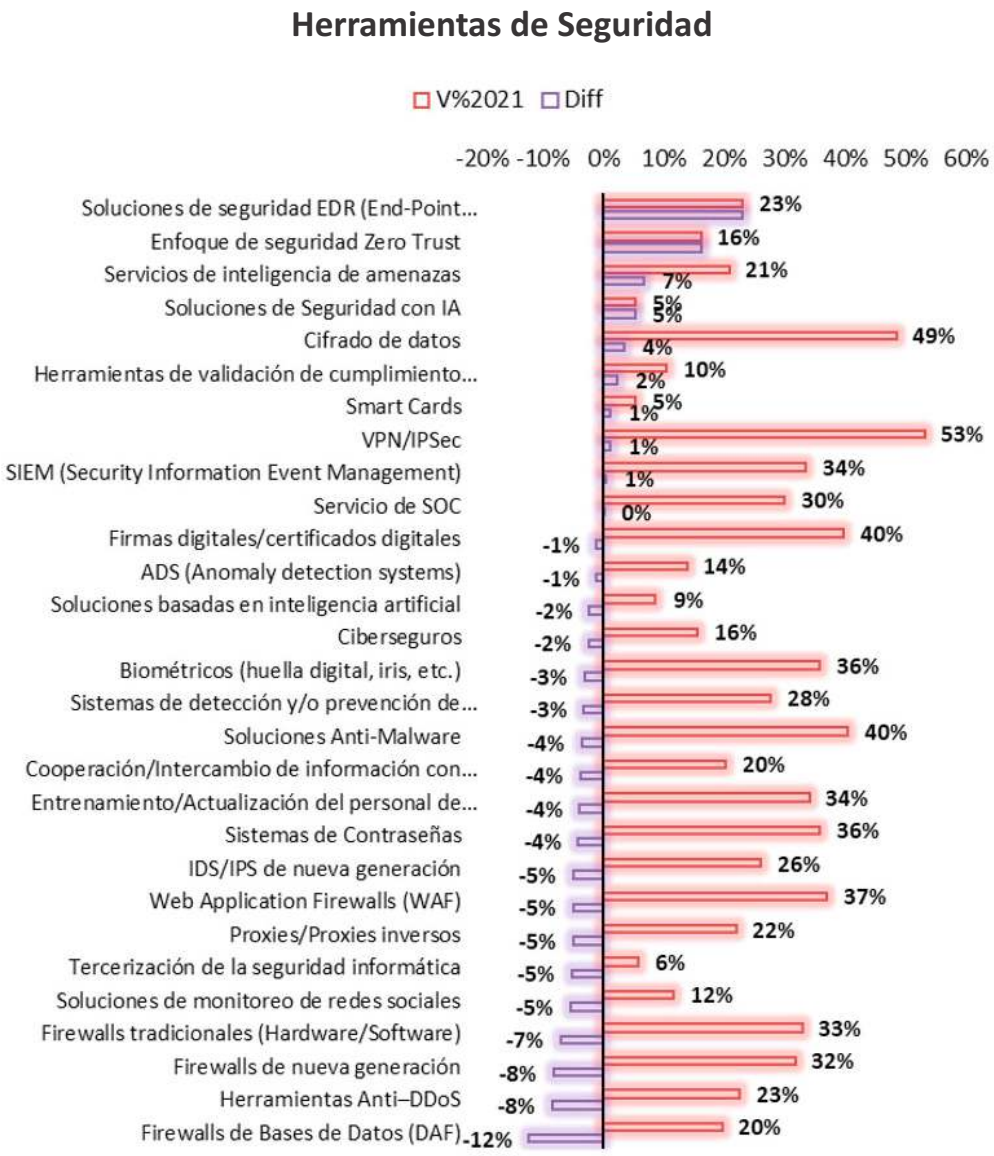
Llama la atención que el sector salud y otros sectores, también han estimado que las primeras soluciones de seguridad sean aquellas que usan la IA.

## Consideraciones de los datos

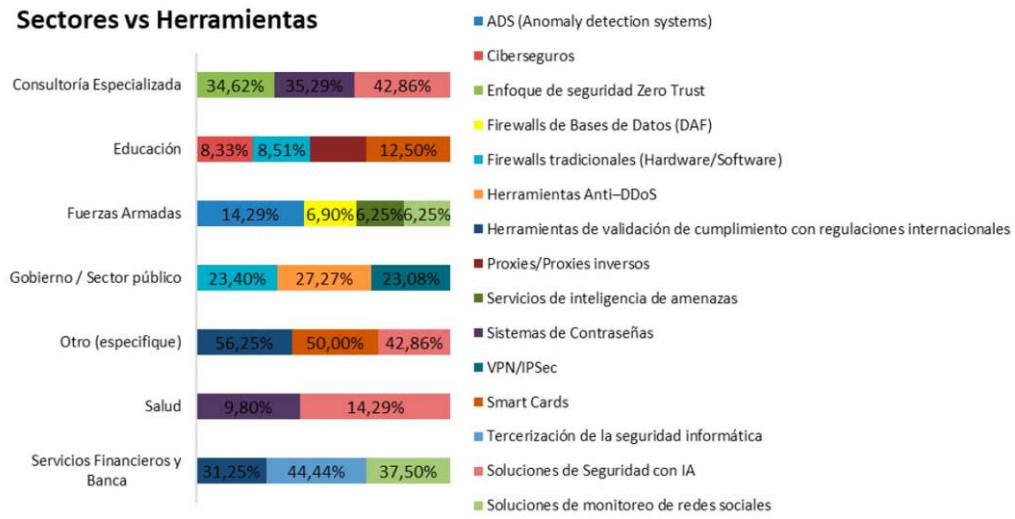
La tendencia en el uso de mecanismos de seguridad se mantiene al compararse con los años anteriores, sin perjuicio de algunas pequeñas variaciones en los mecanismos tradicionales. Para este

año se agregaron nuevas soluciones, como el enfoque de Zero Trust, las soluciones de EDR, las cuales ya se reporta su uso en el sector de la Consultoría especializada, otros sectores, el sector de Gobierno, y los servicios Financieros.

En el estudio de Ponemon-IBM (2020), se resalta que las empresas están tendiendo a usar herra-




*Gráfica 23: Mecanismos de Seguridad usados*




*Gráfica 24: Mecanismos de seguridad en Sectores*

mientas de automatización para la seguridad, tales como herramientas de inteligencia artificial y máquinas de aprendizaje, movimiento que también se ve como tendencia de Colombia.

La tendencia de seguir invirtiendo en tecnologías y servicios de seguridad se confirma, no solo son las soluciones actuales, sino en todo aquello que tiene enfoque de nube también muestra un profundo interés. Según CyberEdge Group (2021), 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.

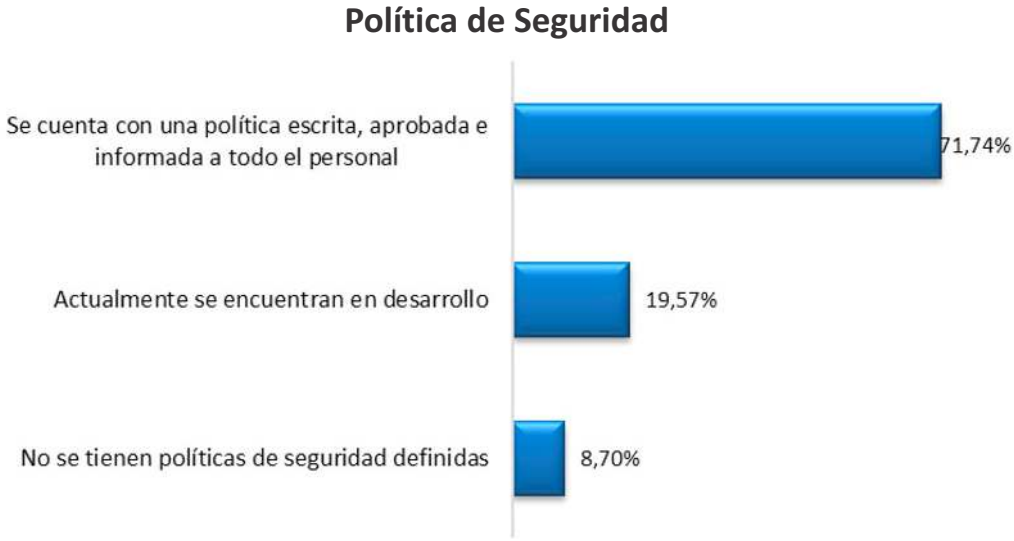
En relación con la protección de estaciones de trabajo el mismo informe resalta que las soluciones *antimalware*, cifrado de discos, antivirus avanzados basados en inteligencia artificial también están considerados.

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.

## Políticas

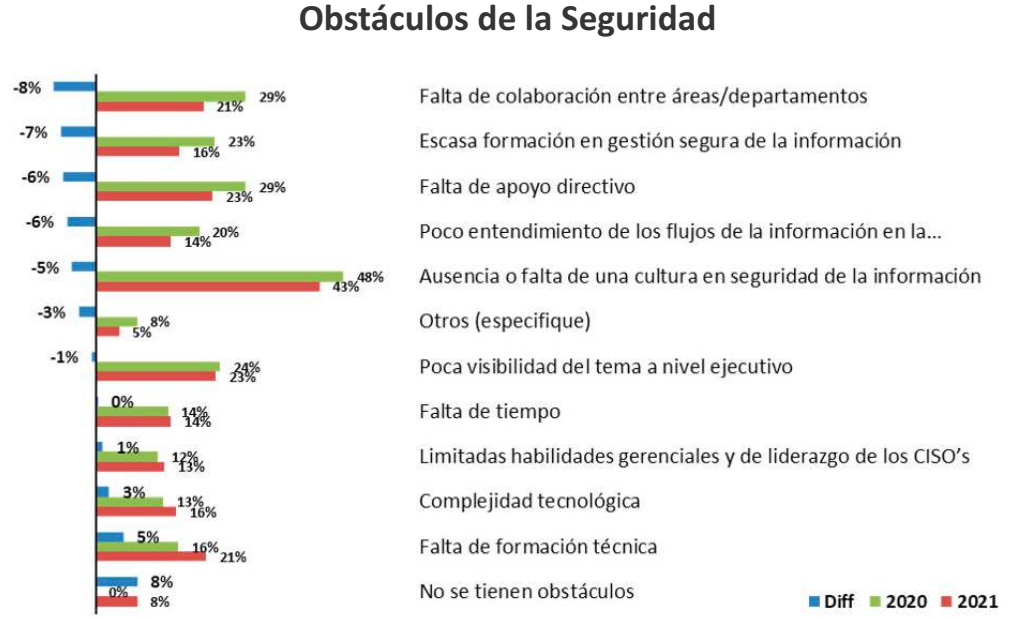
La gráfica 25 refleja el estado de las políticas de seguridad en las organizaciones colombianas; el 72% de los encuestados manifiesta que tienen formalizada sus políticas de seguridad, el 20% actualmente en desarrollo y solo el 8,7% señala no tener políticas de seguridad de la información.

La gráfica 26, muestra lo que manifiestan los participantes al indagar por los obstáculos por los cuales no

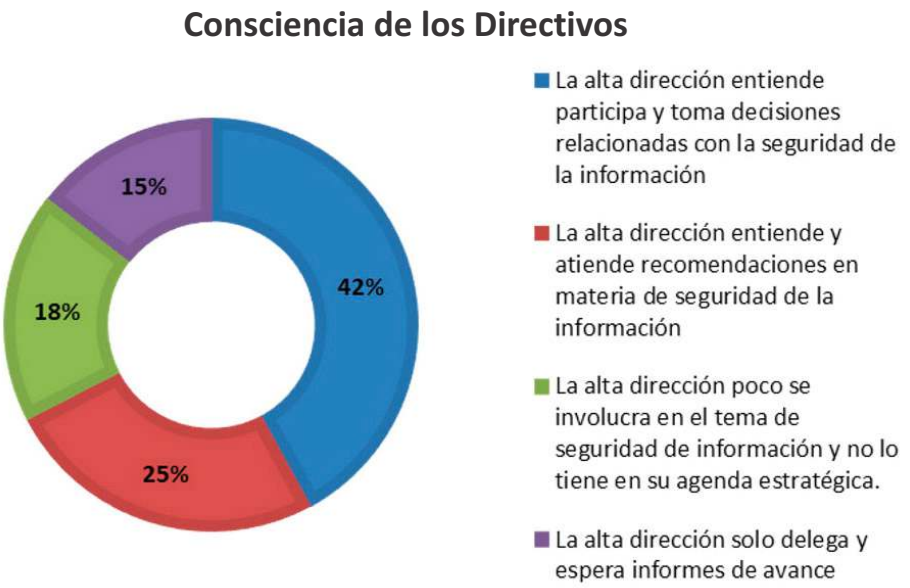



*Gráfica: 25 Estado de las Políticas*

hay una postura adecuada de seguridad en sus empresas. Ausencia o falta de cultura de seguridad 43%, la poca visibilidad a nivel ejecutivo 23% y la falta de apoyo directivo 23% son los tres principales motivos del año 2021. Sin embargo, al comparar con el año inmediatamente anterior estos tres elementos principales decrecen de




*Gráfica 26: Obstáculos de la Seguridad*




*Gráfica 27: Consciencia de los directivos*

manera interesante. Lo que más crece frente al año anterior es la falta de formación técnica 5%, la complejidad tecnológica 3% y las limitadas habilidades gerenciales de los CISOs con un 1% en total, todos los demás criterios descienden en comparación con el año inmediatamente anterior.

La gráfica 27 refleja el nivel de consciencia de los directivos en materia de seguridad, encontrando que la alta dirección entiende participa y toma decisiones relacionadas con la seguridad de la información en 42%, la dirección entiende y atiende las recomendaciones en materia de seguridad de la información 25%, la dirección poco se involucra en el tema 18% y la alta dirección solo delega y espera avances de informes un 15%; al revisar con el año inmediatamente anterior, se tiene una mejora significativa en este aspecto, crece cerca de un 10% el involucramiento de las altas direcciones y su activa participación en la toma de decisiones, y decrecen los demás criterios.

La gestión de riesgos como parte estructural de las funciones y tareas de los responsables de seguridad y sus organizaciones es otro de los componentes claves.

En la gráfica 28, el 79% de los participantes hace una evaluación de riesgos de seguridad digital y la incluyen en sus ejercicios globales de gestión de riesgos, mientras que solo el 21% no lo hace. La gráfica 29 muestra la frecuencia de ejecución de las evaluaciones de riegos, el 50% manifiesta que al menos la ejecuta 1 vez al año, el 26% más de dos y solo dos el 24%.


*Gráfica 28: Evaluaciones de Riesgos*

La gráfica 30, muestra las razones de por qué no es realizada la gestión de riesgos. El primer motivo que resaltan los participantes está relacionado con no tener un proceso formal de gestión de riesgos (28%), seguido del desconocimiento del tema 28%, así como informar que ya está incluido en el proceso de gestión de riesgo empresarial 28%, la falta de presupuestos 14% y la última consideración se relaciona con no tener asociados riesgos al tratamiento de la información con un 3%

La Gráfica 31 muestra el tipo de metodologías usadas al realizar los ejercicios de gestión de riesgos de seguridad; la ISO 31000, con un 39%, es la metodología más usada; comparado con el año anterior es la que mejor crecimiento tiene. ERM (*Enterprise Risk Management*) como metodología sigue en segundo lugar y para Colombia SARO (Sistema de Administración de Riesgo Operativo) es el tercer escaño.

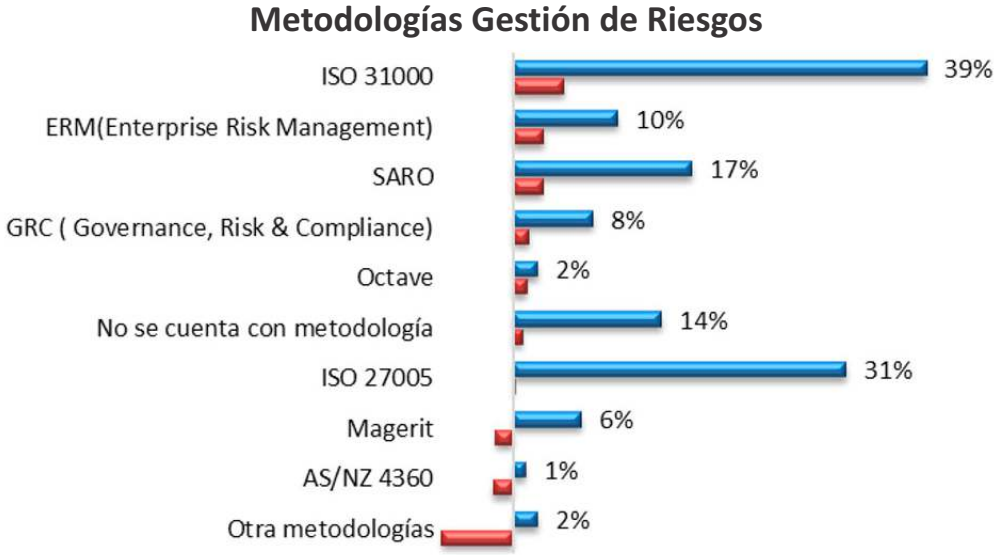
La Gráfica 32 muestra el tipo de riesgo usado para representar los


*Gráfica 29: Evaluaciones de Riesgos*

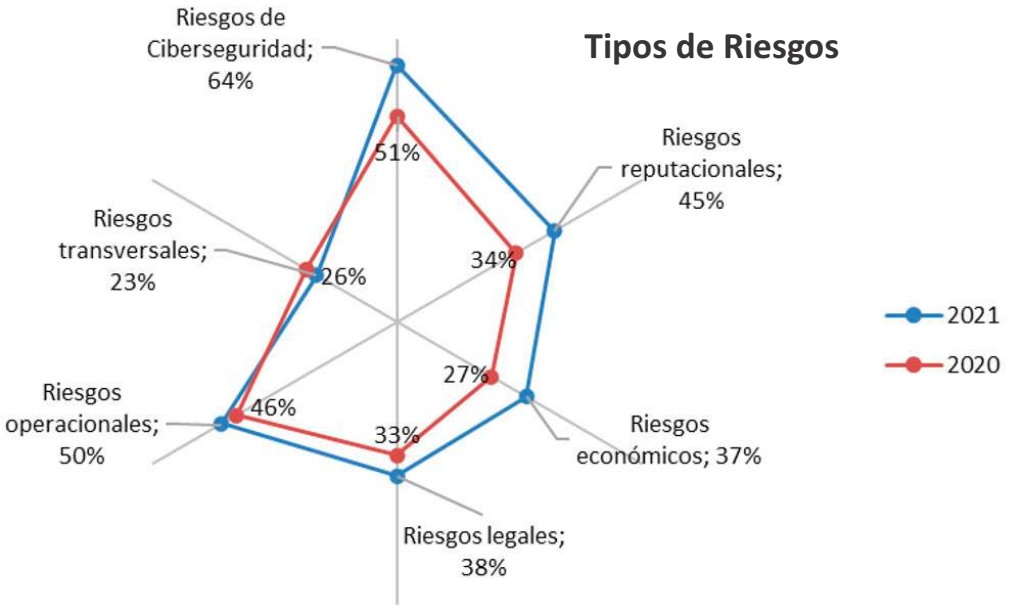

*Gráfica 30 Razones para no realizar la gestión de riesgos*

incidentes de seguridad en las organizaciones. Todas las categorías tienen incrementos importantes; al revisar los detalles vemos que los riesgos de tipo económico tienen un crecimiento del 37%, los riesgos reputacionales 33%, los riesgos de ciberseguridad 25%, riesgos legales 16%, riesgos operacionales 9%, los riesgos transversales decrecen el 11%

La gráfica 33 ilustra el uso de los distintos marcos de trabajo (*frame-*




*Gráfica 31: Tipos de Metodología*

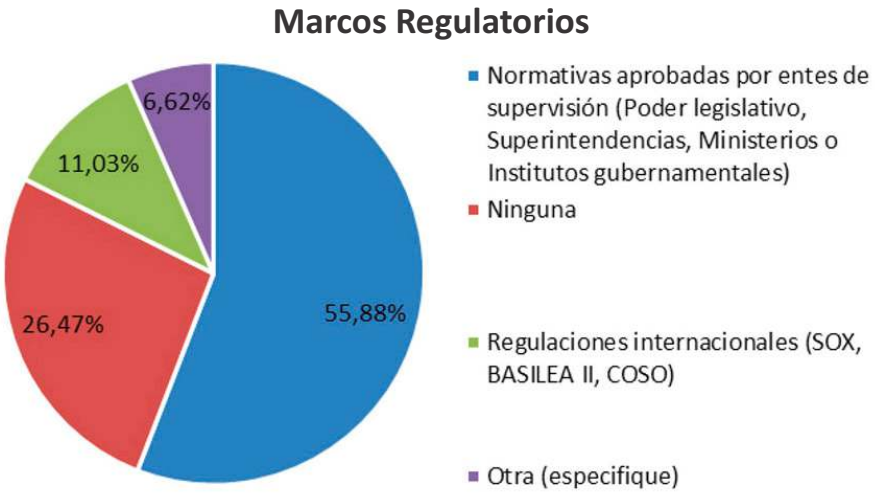



*Gráfica 32: Tipos de Riesgos*

*works*) usados en las organizaciones colombianas: ISO/IEC 27001, NIST, ITIL y COBIT son los más usados. Disminuye contra el año anterior el no usar ningún marco de buenas prácticas.

La gráfica 34 refleja las regulaciones que las organizaciones deben asegurar. En el caso colombiano, el 74% de los participantes manifiesta que sí existen regulaciones que se deben cumplir, bien sea en un mar-


*Gráfica 33: Marcos de trabajo usados*




*Gráfica 34: Regulaciones o normativas*

co nacional o internacional al que estén sometidos, mientras que el 26% considera que no está sujeto a cumplir ningún marco regulatorio o normativos.

## Consideraciones de los datos

Los riesgos de seguridad de la información y ciberseguridad en definitiva son una realidad como lo es ratificado en el informe del Foro Económico Mundial (WEF, 2021), el cual manifiesta que la prioridad de estos tipos de ataques es alta en las organizaciones del mundo.

La confianza en los entornos digitales y la construcción de la capacidad de ciberresiliencia se fundamenta en una estructura de gobierno de la seguridad, en la que las políticas, la gestión de riesgos y el conjunto de buenas prácticas se convierten en elementos centrales para dirigir los programas de ciberseguridad. La conexión entre una estrategia de seguridad y los objetivos de seguridad que sean claros ayudaran a construir y fomentar la ciberresiliencia (World Goverment Summint – EY, 2020).

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

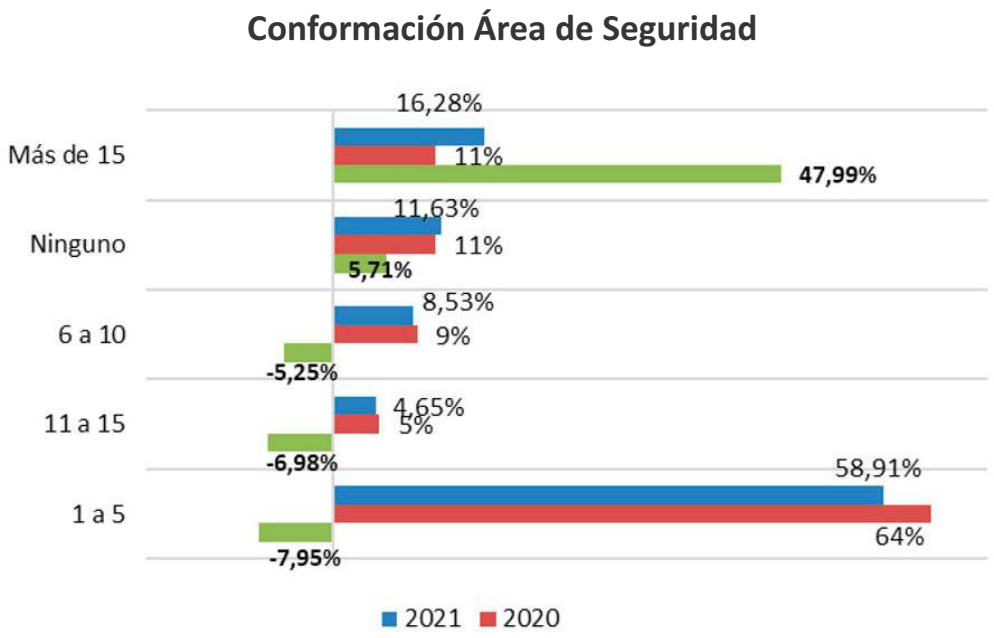
Así mismo, el informe de Deloitte (2019) resalta que el 50% de los participantes usan metodologías de riesgos y la cuantificación de estos como instrumentos y prácticas sólidas para la atención de los ciberataques de seguridad en las empresas.

Con relación a las políticas y su adopción, la tendencia en Colombia

para contar con un modelo fortalecido de políticas de seguridad y control es ratificado con el informe de CISCO (CISCO, 2020), el cual muestra que las compañías que se adhieren a sus prácticas, políticas de seguridad tienen costos menores por brechas relacionadas con los datos en comparación con quienes no lo hacen, lo cual puede apoyar el comportamiento de Colombia en este sentido.

Cada vez más toda la organización como un organismo vivo, desde sus niveles directivos deben entender desde lo más profundo lo que significa gobernar los riesgos en el contexto digital, es imperativo para desarrollar mejores modelos sostenibles en los ambientes digitales disruptivos en los que se desenvuelven las organizaciones de hoy y del futuro. (EY & IIA, 2021)

Situaciones como la evolución de los adversarios, la pandemia y la realidad digital de las organizaciones han cambiado la forma de ver la ciberseguridad, y así mismo la necesidad de repensar las prácticas de gestión de riesgos, de solo entender que es necesario proteger una infraestructura a defender y anticiparse de un adversario digital, para ello se requiere que lo fundamental se consolide en las organizaciones y así poder dar pasos más importantes que permitan evolucionar en la práctica de la ciberseguridad, que desarrolle mejores posturas de seguridad y que repercutan en una adecuada ciberresiliencia.




*Gráfica 35: Tamaño del área de seguridad.*

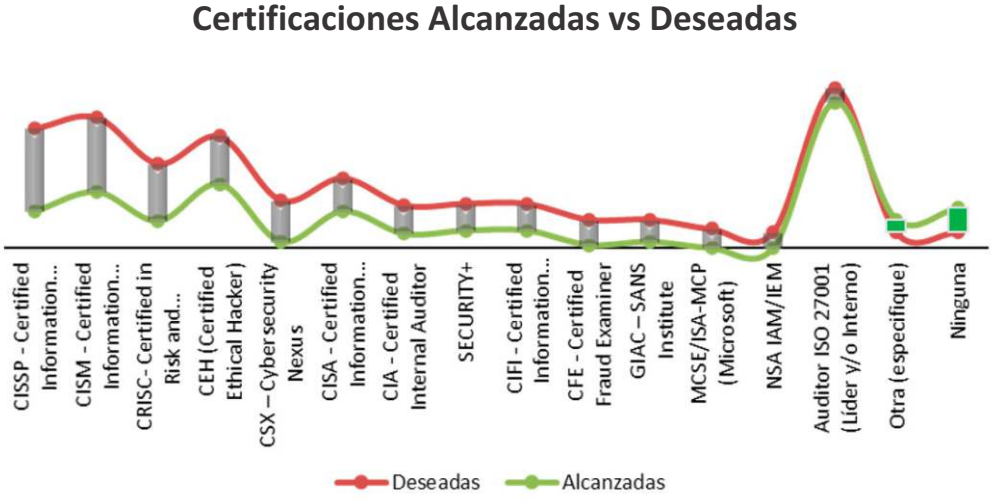
## Capital intelectual

La gráfica 35 relaciona los recursos dedicados a la seguridad en las empresas, cerca del 88%, manifiesta tener recursos dedicados a la seguridad, la predominancia es de 1 a 5 con un 59%. Sin embargo, al revisar los datos contra el año 2020, encontramos que hay una variación importante, crecen las áreas de seguridad en un 48% en el rango de más de 15 personas, crece un 5% no tener recursos asignados a la seguridad, y decrecen las demás franjas.

La gráfica 36, representa la comparación de las certificaciones que los profesionales de seguridad han alcanzado en la actualidad y que desean alcanzar en el tiempo. CISSP, CISM, CRISC y CEH y CSX, son las certificaciones que mayor variación tienen entre lo que se tiene actualmente y lo deseado en el futuro. Resaltar que cada vez más son menos personas las que no están en el grupo de no poseer alguna certificación

Para este año se ha decidido incluir una nueva variable en relación con la preferencia que tienen los profesionales de seguridad sobre su formación. La gráfica 37, indica que las certificaciones son la primera opción con un 60% y el 49% la educación formal como segunda opción, entendida como todos los programas ofrecidos por la universidad como (pregrado, postgrado).

Al revisar los datos en profundidad se encuentra que los CISOs prefieren en primera instancia las charlas especializadas con un 42% y los programas de formación ejecutiva con el 38%, mientras que los directores de seguridad prefieren la educación formal en primer lugar 30,30% seguido de los cursos cortos con el 30%. El profesional de




Gráfica 36: Certificaciones alcanzadas vs deseadas


*Gráfica 37: Preferencias de formación*

seguridad prefiere para su formación los diplomados (33%) seguido de las charlas especializadas (32%). El Oficial de Seguridad Informática para desarrollar sus competencias y habilidades, prefiere los cursos cortos 20% y los diplomados (17%). Los profesionales con el cargo de privacidad prefieren los programas de formación ejecutiva (8%) seguido de las certificaciones con un 2%.

La Gráfica 38, muestra las brechas que se identifican para los profesionales de seguridad en la actuali-

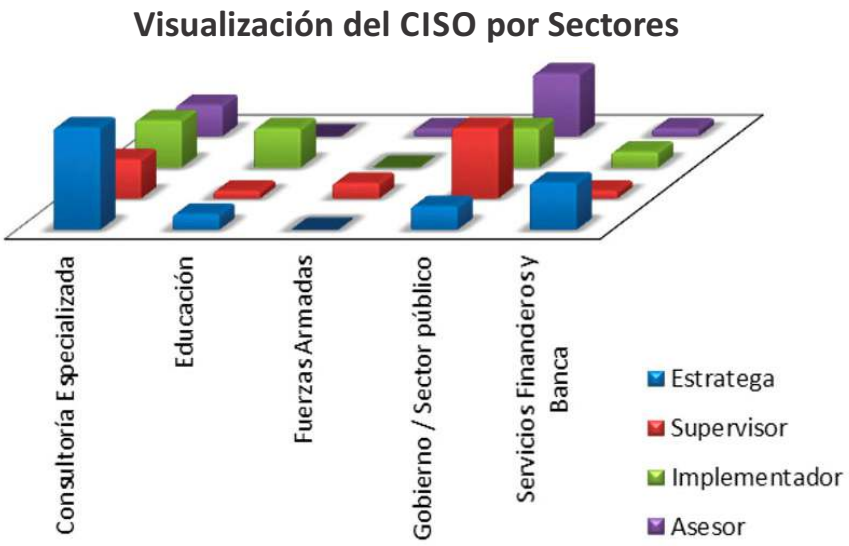

*Gráfica 38: Brechas del profesional de seguridad*


*Gráfica 39: Tipo de CISO*

dad y en dónde pueden mejorar. De acuerdo con los resultados se observa que las capacidades estratégicas son el primer lugar 47%, seguido de las capacidades intelectuales (37%), las capacidades de gestión (36%), las capacidades humanas (36%), la experiencia profesional el 25% y otras consideraciones el 1%. Comparado con el año anterior hay variaciones importantes, las capacidades intelectuales tienen un incremento del 12%, capacidades estratégicas tiene un incremento del 3%, es decir que es necesario cerrar las brechas en esos aspectos, mientras que las capacidades de gestión decrecen un 30% y la experiencia profesional decrece un 42%, lo que significa que en dichos aspectos se ha mejorado.

El CISO, es la figura más representativa como cabeza visible para guiar y orientar la ciberseguridad en las organizaciones. La Gráfica 39 muestra la forma en que las organizaciones ven o identifican el tipo de CISO que existe en ellas, el 28% ven al CISO como un supervisor, el 28% lo ven como un estratega, el 22% lo ven como un asesor, y el 22% restante como un implementador. Frente al año anterior hay un incremento significativo del 63% en el tipo estratega, 18% de incremento en la vista supervisor, mientras que decrece un 22% el implementador y un 28% como asesor.

En la Gráfica 40, se explora la forma en cómo los sectores principales de la industria ven la posición del CISO, el sector de la consulto-




*Gráfica 40: Tipo de CISO x Sectores*

ría especializada y los servicios financieros ven al ciso como una posición estratégica, el sector del gobierno y las fuerzas armadas ven al rol del ciso como un supervisor, mientras que el sector de la educación lo visualiza como un implementador.

La Gráfica 41, muestra el tipo de información que el CISO entrega en la organización, el 44% entrega


*Gráfica 41 Tipo de información que entrega el CISO*

información relacionada con la gestión para la toma de decisiones, el 40% entrega información relacionada con los riesgos en seguridad de la información, el 34% información relacionada con vulnerabilidades, el 32% entrega información relacionada con las brechas de seguridad existentes, el 17% no entrega información, y el 1% relaciona otros puntos.

En relación con el año inmediatamente anterior tenemos variaciones importantes, crece en un 24% que el CISO no está entregando información, seguido de la entrega de información con la gestión de la seguridad para la toma de decisiones 10%, mientras que todos los demás valores tienen disminuciones importantes. Decrece en primer lugar la entrega de información de las brechas de seguridad un 19%, seguido de la información técnica de vulnerabilidades 22% y 23% decrece la entrega de información relacionada con los riesgos en seguridad de la información y ciberseguridad.

## Consideraciones de los datos

En Colombia se ratifica que las organizaciones piensan en tener áreas de seguridad de un tamaño pequeño, sin embargo, los fenómenos disruptivos como la pandemia, hicieron que para el año 2020 las áreas de seguridad tuvieran que incrementar su tamaño y capacidades. Esto reflejado en el incremento del 50% en tener precisamente este tipo de áreas de seguridad.

Existe una tendencia macada a hablar de una brecha de talento de ciberseguridad, todos los informes coinciden en que cada vez más es necesario tener una fuerza de trabajo en las áreas de seguridad entrenada de diferentes formas, lo que implica, una fuerza entrenada que tiene mayores posibilidades para enfrentar los desafíos actuales (ISACA, 2021).

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

El estudio de ISACA (2021) muestra que los perfiles de seguridad buscados apuntan a algún grado de formación formal en ciberseguridad; sin embargo, el mismo estudio muestra que tener el grado no necesariamente significa un grado alto de preparación para enfrentar los roles en materia de seguridad.

Para (ISC2, 2021) un profesional de seguridad es una amalgama de muchas variables en cuanto a su formación, indicando que estos profesionales en su mayoría, cerca del 76%, poseen algún tipo de grado entre el pregrado y un estudio formal de postgrado.

En relación con las certificaciones, CISSP, CISM, CRISK y CEH, muestran ser las certificaciones con mayor relevancia en el mundo de los profesionales de seguridad digital, son inclusive las que más desean los profesionales, en comparación con lo que más tienen en la actualidad. Estos datos son igualmente ratificados por el informe de Kaspersky (2019), con relación a las certificaciones.

El valor de la educación en seguridad y control es muy alto, y no dista de la función que cumplen los entes de certificación, consideraciones efectuadas por el informe de ENISA (2020). Definitivamente formarse en ciberseguridad es importante, y los datos muestran que las preferencias son variadas en esta materia, todos los informes consultados muestran las fortalezas de todas las formas de educación, y relacionan que ninguna es enemiga de la otra, por el contrario, se debe trabajar por inclusive incentivar el usar marcos de trabajo generales como el modelo del NIST (INFOSEC, 2021).

Este estudio indica que todos los actores como el gobierno, la academia y la industria deben trabajar de la mano para ir cerrando las brechas estimadas de profesionales de seguridad que existen en la actualidad. De igual manera el informe indaga sobre cómo las universidades pueden trabajar y ayudar en la creación tanto de formación como de soluciones para enfrentar los desafíos en materia de ciberseguridad y concluye que el sector de la educación juega un papel fundamental en ambos sentidos.

Las nuevas capacidades son elementos esenciales en la vida de los profesionales de ciberseguridad. (ISACA, 2021; ISC2, 2021). Capacidades de liderazgo, comunicación y capacidades humanas son necesarias para desarrollar cualquier función en materia de ciberseguridad (F-Secure, 2021). Marlin Hawk (2020) resalta que una de las actividades fundamentales de los Líderes de Seguridad (25%) está asociada con el desarrollo de talentos de ciberseguridad, y por tanto de las capacidades de gestión y liderazgo que son indispensables en el desarrollo de la función de seguridad.

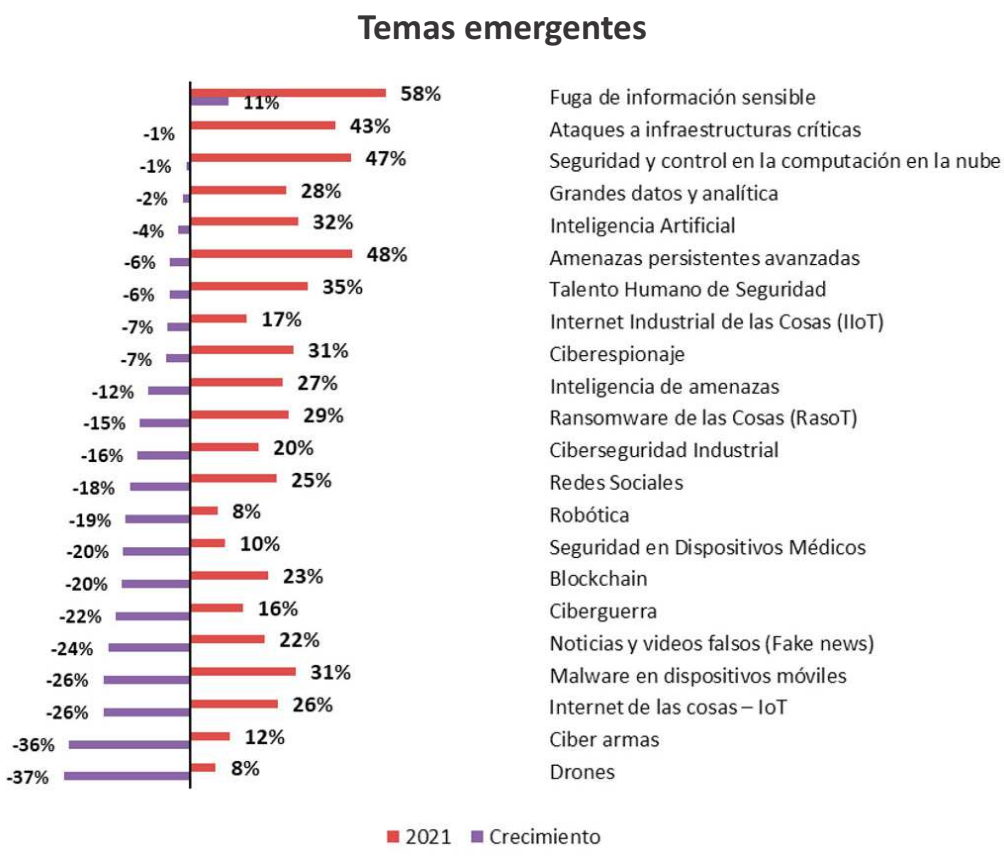
La forma en cómo puede avanzar un profesional de seguridad en otros cargos y generar mayor visibilidad, es a través del desarrollo de nuevas capacidades y habilidades: capacidades de liderazgo, capacidades para entender el negocio y de comunicación son claves para ello (ESG-ISSA, 2020).

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

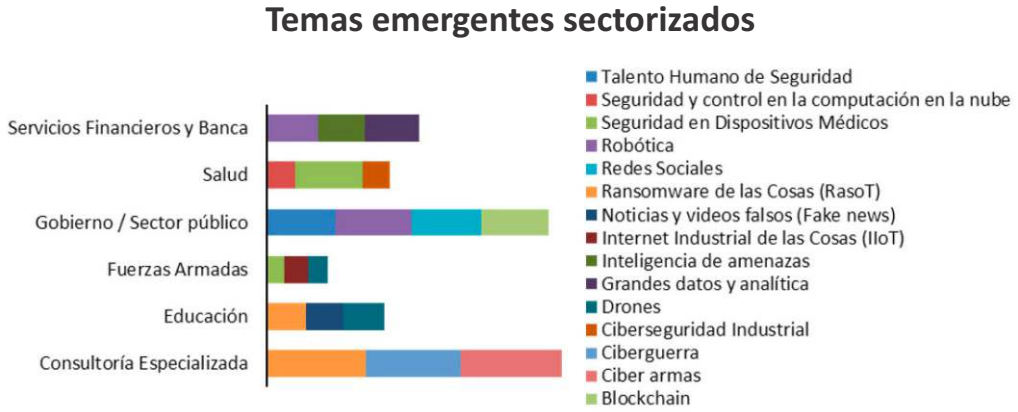
## Temas emergentes

La gráfica 42 muestra los temas relevantes y emergentes que tienen en la mira los profesionales de seguridad. El más relevante, la fuga de información sensible, las amenazas persistentes avanzadas y la seguridad de la computación en la nube son los de más alto valor. Sin embargo, con relación al año anterior el único que tiene un incremento, es decir sigue siendo un tema que está en el radar y las inquietudes de los profesionales de seguridad es la fuga de información sensible que incrementa un 11%, todos los demás valores tienen una disminución en algún grado.

Al revisar directamente lo que inquieta a los sectores de la industria, se observan aspectos interesantes en la Grafica 43; primero se seleccionan los temas más importantes por sectores, encontrando que para el sector financiero los tres temas principales son grandes datos y analítica, la robótica y automatización, la inteligencia de amenazas. Para el sector de gobierno, la robótica aparece en primer lugar, seguido las redes sociales y por úl-




*Gráfica 42: Temas emergentes*




*Gráfica 43: Temas emergentes por sectores*

timo el talento de seguridad y *blockchain*. En el sector de salud, los temas son seguridad en los dispositivos médicos, la seguridad en la nube y ciberseguridad industrial. En las fuerzas armadas, el internet industrial de las cosas, los drones, y la seguridad en dispositivos médicos, así mismo el sector educativo tiene en su radar tienen los drones, el *ransomware* de las cosas y *las fake news*, por último, para la consultoría especializada están las ciberarmas, el *ransomware* de las cosas y la ciberguerra.

## Consideraciones de los datos

Los profesionales de seguridad de Colombia ven el panorama de los desafíos de la ciberseguridad y sus consideraciones ponen de manifiesto la inquietud latente de lo que vendrá. Informes como el de Fireeye (2021) soportan las consideraciones locales, en el sentido de observar al *ransomware* y su evolución que se ha venido desarrollando alrededor del globo.

Booz Allen Hamilton (2020) en su informe de tendencias de la ciberseguridad, resalta que el *malware* evoluciona y en sus consideraciones ve a los drones como una fuente para que ello se desarrolle movilizando el mundo de las ciberoperaciones y las tensiones militares que esto ocasiona.

El mundo OT (Tecnología de Operación), ha tenido grandes impactos por diferentes anomalías, no por nada está en las preocupaciones de sectores como el de las fuerzas armadas, tendencia que también se puede ver advertir en el informe de IBM (2021) y que muestra que este es un escenario complejo que debe ser protegido por las implicaciones que tiene en las múltiples industrias.

## 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 de un fenómeno denominado pandemia que definitivamente ha revolucionado y cambiado la forma en cómo la seguridad se tiene que plantear en las organizaciones.

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

Cada vez más, las organizaciones se enfrentan a una realidad digitalmente modificada, en la que las nuevas tecnologías permean cada uno de los ambientes organizacionales y personales. Este contexto crea nuevos y desafiantes escenarios que se transforman en riesgos para las organizaciones, así como en una invitación para desarrollar nuevos, continuos y creativos esfuerzos en procura de proteger y crear valor como la confianza, la confiabilidad y la resiliencia en un mercado cada vez más competitivo y exigente.

Definitivamente los directivos de las organizaciones colombianas están interesados en los temas de ciberseguridad, en un informe reciente de Nominet (2020) se resalta que más del 84% de los niveles directivos y ejecutivos incluyen los temas de seguridad en sus reuniones.

Lo mismo menciona el documento de PwC (2021) donde resalta que el 47% de los CEO de su estudio global están preocupados por los temas relacionados con las ciberamenazas. Lo anterior, ratifica para Colombia que los directivos, y ejecutivos de la seguridad están interesados en estas temáticas, y esperan que los Líderes de Seguridad Digital, los orienten sobre estos riesgos.

Mejorar la resiliencia digital, pasa por gobernar y establecer cultura de ciberseguridad en las organizaciones, pasa porque toda la organización y sus miembros se adhieran a la buena práctica. Esto demanda que sus máximos líderes asuman las responsabilidades y entiendan con claridad lo que significa el ciberriesgo, de tal manera que le permita manejarlo en la realidad actualmente modificada y en los nuevos normales que se exigen (Dobrygowski & Vadala, 2020).

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

Esta nueva realidad por tanto 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 (Elliot, 2021), que deben poder actualizar el conjunto de herramientas como la comunicación para que puedan interactuar con más determinación con sus equipos de trabajo.

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

En la realidad nacional se pueden concluir los siguientes aspectos:

1. En las organizaciones colombianas, las áreas de seguridad y ciberseguridad tienen dos posiciones marcadas. Algunas cuentan con una dirección propia y definida, mientras otras dependen formalmente de las áreas de tecnología. Pero eso no significa en ninguno de los dos casos que esté llegando su mensaje a los tomadores de decisiones.
2. 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.
3. La posición del profesional de seguridad continúa su proceso de afianzamiento dentro de las organizaciones, cada vez se ven más plazas creadas de profesionales de seguridad como CISOs y directores de seguridad en las organizaciones, estos movimientos demandan la creación de nuevas y actualizadas conjunto de competencias, capacidades y habilidades que le permitan desarrollar mejor sus nuevas funciones
4. Entre más disruptivos son los entornos de trabajo, las nuevas capacidades como las capacidades estratégicas, humanas y técnicas necesitan ser desarrolladas de manera integral para

atender la demanda de nuevas responsabilidades.

5. Los datos de Colombia muestran la importancia del profesional de seguridad, su relevancia para mantener un negocio con los niveles de confianza digital adecuados pensando en las dinámicas digitales. Así mismo, se invita al profesional a seguir expandiendo y ampliando tanto sus saberes como sus prácticas. Hay muchos desafíos y se requiere del crecimiento del profesional de una manera rápida, oportuna y con altos niveles de adaptabilidad para afrontar los desafíos actuales y futuros como Líder de Seguridad.
6. La formación del profesional de seguridad es variada y puede darse de múltiples maneras, ninguna de ellas resta a las demás, por tanto, es importante que en el radar del profesional de seguridad existan todas las opciones que le permitan desarrollar su plan de crecimiento y carrera profesional.
7. La experiencia, los conocimientos y sus adicionales (como las certificaciones) en la vida del profesional de seguridad en la realidad de Colombia son importantes, se complementan y no se oponen, por el contrario, alimentan el camino para tener un mayor potencial en el mercado laboral colombiano.
8. La realidad digital hace que todos los sectores e industrias lleven su mirada al tema de ciberseguridad. A los sectores como el financiero, la consultoría especializada y el gobierno les interesa participar y conocer la realidad de la seguridad, tendencia observada en diferentes informes publicados sobre seguridad y ciberseguridad.
9. Los riesgos es el lenguaje común de los negocios y a su vez es un instrumento catalizador de un programa de seguridad. Los Líderes de seguridad digital están considerando este instrumento como una valiosa oportunidad para elevar su interlocución con los niveles directivos y ejecutivos, para poder tomar caminos acordes a la realidad digital de la empresa.
10. La confianza digital y la ciberresiliencia se convierten en un generador de nuevos negocios; tendencias internacionales también sostienen que dicha confianza es una fuente que motiva a cultivar las relaciones entre consumidores y quienes ofrecen los servicios, para configurar un activo valioso a la hora de manejar y maniobrar en los ecosistemas digitales actuales.
11. A nivel nacional, se mantiene la sólida tendencia de usar mecanismos tecnológicos como las principales herramientas de protección. Si bien las tendencias internacionales dan esto por sentado, se debe hacer un llamado tanto a los responsables de seguridad como a las 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.

12. El poder de las anomalías digitales, de los adversarios y de la realidad digital se entiende cada vez más en el marco de las organizaciones colombianas. Más allá de lo técnico, se registran los errores humanos y, en tal sentido, es necesario pasar de procesos de sensibilización al cambio de comportamientos, liderado por los responsables de la seguridad, con el ánimo de crear una nueva cultura alrededor de entornos digitalmente modificados. Así mismo, es necesario gestionar un programa de seguridad que permee todos los niveles organizacionales basados en prácticas dirigidas a los diferentes grupos de interés, y orientadas a construir posturas de seguridad diferenciadas y articuladas desde los desafíos que debe asumir el talento humano.
13. Las nuevas tecnologías como Cloud, IoT, IA, *machine learning* Zero Trust y otras, están cambiando la concepción del mundo, la forma de interactuar y los retos a los que se enfrentan las organizaciones a nivel nacional e internacional. De ahí que los profesionales de seguridad deban tener claridad para profundizar en estas nuevas tendencias y su uso.
14. Los resultados de la encuesta reflejan que, a la hora de implementar modelos de seguridad, las organizaciones usan algún estándar, hecho motivado más por las regulaciones que por una intención de proteger, lo que genera el debate nacional e internacional alrededor de tales asuntos. La meta de la protección organizacional no debe estar sujeta al cumplimiento.
15. Es claro que el cisne negro (o ¿sorpresa predecible?) denominado Covid-19, ha cambiado por completo no solo la forma de ver la vida, sino ha resaltado la importancia de la ciberseguridad y la gestión de las tecnologías de la información. Hoy más que nunca se observa a la ciberseguridad como una capacidad empresarial, que ofrece y aporta en el desarrollo de negocios digitales, y que se enfrenta y enfrentará las tensiones geopolíticas y de cumplimiento con mucha más profundidad. Esta capacidad deberá apalancar la confianza digital necesaria para ofrecer servicios y desarrollar modelos de negocio en el ecosistema digital de hoy como fundamento del nuevo normal que empezamos a construir.

En resumen, el panorama general de la seguridad en Colombia muestra cambios importantes, grandes movimientos y desafíos emergentes. La realidad llamada Covid-19 ha creado una ventana de oportu-

nidad para que la ciberseguridad se afiance como herramienta indispensable para apalancar los negocios.

El año 2021 está marcado por el desarrollo del "nuevo normal", que, si bien no hay consensos a la fecha, sí ha empezado a dar lineamientos de posibles futuros, en los que no existe una sola opción, sino múltiples escenarios que permitan diseñar posibles alternativas, cosas que se han venido aprendiendo sobre la marcha, donde la ciberseguridad no es la excepción.

En este ejercicio, es necesario repensar lo ya conocido y concebido como verdades definidas para reescribir nuevas prácticas tendientes a apoyar a las empresas para que caminen por la constante de la incertidumbre, que no es otra cosa que entender la dinámica de los ecosistemas digital en los cuales las organizaciones se mueven hoy.

## Referencias


Booz Allen Hamilton (2020). 2020 CYBERSECURITY THREAT TRENDS OUTLOOK. https://content.fireeye.com/m-trends/rpt-m-trends-2020

Cano, J. & Almanza, A. (2020) Estudio de la evolución de la Seguridad de la Información en Colombia: 2000 - 2018. *Revista Iberoamericana de Sistemas y Tecnologías de Información*. E27. Marzo. 470-483. https://www.researchgate.net/publication/339629757_Estudio_de_la_evolucion_de_la_Seguridad_de_la_Informacion_en_Colombia_2000_-_2018

CISCO (2020). Securing What's Now and What's Next. Recuperado de: https://www.cisco.com/c/dam/en/us/products/collateral/security/2020-ciso-benchmark-cybersecurity-series-feb-2020.pdf

CISOS.CLUB (2021). Modelos Post Pandemia de Entornos de Trabajo (Infografía). https://www.linkedin.com/feed/update/urn:li:activity:6809142558334214145/

CyberEdge Group (2021). Cyberthreat Defense Report. https://www.herjavecgroup.com/wp-content/uploads/2021/04/CyberEdge-2021-CDR-Report-v1.1.pdf

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

Deloitte (2019). The Future of Cyber Sphere 2019. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/finance/us-the-future-of-cyber-sphere.pdf

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

Dobrygowski, D. & Vadala, D. (2021). Does Your Board Really Understand Your Cyber Risks?. HBR. https://hbr.org/2020/09/ does-your-

board-really-understand-your-cyber-risks

Eliot, B. (2021). It's Time to Free the Middle Manager. HBR. https://hbr.org/2021/05/its-time-to-free-the-middle-manager

ENISA (2020). Cybersecurity skills development in the eu. https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union/at_download/fullReport

ESG-ISSA (2020). The Life and Times of Cybersecurity Professionals 2020. https://www.esg-global.com/esg-issa-research-report-2020

EY (2020). How does security evolve from bolted on to built-in? https://www.ey.com/Publication/vwLUAssets/2020_GISS_pdf/$FILE/ey-global-information-security-survey-2020-report.pdf

EY & IIA. (2021). The risky six. https://global.theiia.org/knowledge/Public%20Documents/EY-The-Risky-Six-Board-Disconnections.pdf

FBI. (2021). Internet Crime Report 2020. https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

F-Secure (2021). The CISOs' New Dawn. https://www.f-secure.com/content/dam/f-secure/en/business/cisos-new-dawn/collaterals/mdr-the-cisos-new-dawn.pdf

Fireeye (2021). M-Trends 2021. https://www.fireeye.com/content/dam/collateral/en/rpt-mtrends-2021.pdf

IBM (2021). X-Force Threat Intelligence Index 2021. https://www.ibm.com/downloads/cas/M1X3B7QG

IDG (2021). Cybersecurity at a Crossroads. https://www.insightcdct.com/getattachment/40ff5ebd-03f2-4d4d-8f4e-b7871c00fd5f/Complete-2021-IDG-survey-results.aspx

INFOSEC (2021). 2021 Cybersecurity Role & Career Path Clarity Study. https://www.infosecinstitute.com/form/2021-role-clarity-study/

ISACA (2021). State of Cybersecurity 2021, Part 1: Global Update on Workforce Efforts, Resources and Budgets. https://www.isaca.org/bookstore/bookstore-wht_papers-digital/whpsc211

$(ISC)^2$. (2021). Cybersecurity Professionals Stand Up to a Pandemic. https://www.isc2.org/-/media/ISC2/Research/2020/Workforce-Study/ISC2ResearchDrivenWhitepaperFINAL.ashx?la=en&hash=2879EE167ACBA7100C330429C7EBC623BAF4E07B

Ivanti (2021). How the Pandemic Has Shifted CISO Priorities. https://www.ivanti.com/resources/v/doc/pr-survey-report/ivi-2459-emea-ciso-survey-en

Kaspersky (2019). What It Takes to Be a CISO: Success and Leadership in Corporate IT Security. https://kas.pr/4sw6

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

Nominet (2020). THE CISO STRESS REPORT. Recuperado de: https://media.nominetcyber.com/wpcontent/uploads/2020/02/Nominet_The-CISO-Stress-Report_2020_V10.pdf

Ponemon-IBM (2020). The Cyber Resilient Organization. https://www.ibm.com/downloads/cas/VR9E8AKM

Ponemon-LogRhytmn (2021). Security and the C-Suite: Making Security Priorities Business Priorities. https://gallery.logrhythm.com/analyst-reviews-and-reports/na-report-ponemon-security-and-csuite.pdf

PwC (2021). 24nd Annual Global CEO Survey. A leadership agenda to take on tomorrow. https://www.pwc.com/gx/en/ceo-agenda/ceosurvey/2021/report.html

Sophos. (2021). The State of Ransomware 2021. https://news.sophos.com/en-us/2021/04/27/the-state-of-ransomware-2021/

Tessore, C. (2020). Vuca y tuna abordaje conceptual cambios de paradigma en contextos vuca y tuna. Changes of paradigm in vuca and tuna a conceptual approach. https://www.academia.edu/41717050/VUCA_Y_TUNA_ABORDAJE_CONCEPTUAL_CAMBIOS_DE_PARADIGMA_EN_CONTEXTOS_VUCA_Y_TUNA

Verizon (2021). Data Breach Investigation Report. https://enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pdf

WEF - World Economic Forum (2021) The Global Risk Report 2020. Recuperado de: https://www.weforum.org/reports/the-global-risks-report-2021

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

***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.*