# XX Encuesta Nacional de Seguridad Informática

DOI: 10.29236/sistemas.n155a4

*Lecciones aprendidas y prospectiva de futuro*

**Resumen**
La encuesta de seguridad informática, capítulo Colombia, soportada por la Asociación Colombiana de Ingeniero de Sistemas (ACIS) y realizada a través de Internet, entre los meses de febrero y abril de 2020, contó con la participación de 214 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, HackLabGirls LATAM, y WOMCY, entidades y comunidades que colaboraron en la distribución y 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 al respecto 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.

Particularmente hay que resaltar que se presentó una investigación con un análisis longitudinal de los primeros 18 años de la encuesta, en un evento internacional denominado, "Estudio de la evolución de la Seguridad de la Información en Colombia: 2000 – 2018" (Cano & Almanza, 2020), donde se presenta un análisis de la historia de la seguridad y ciberseguridad en Colombia, que hace una lectura documentada del pasado, y que, sumado a este documento, permite realizar un poco de prospectiva de cómo podría llegar a ser 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 43 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 permiten 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.

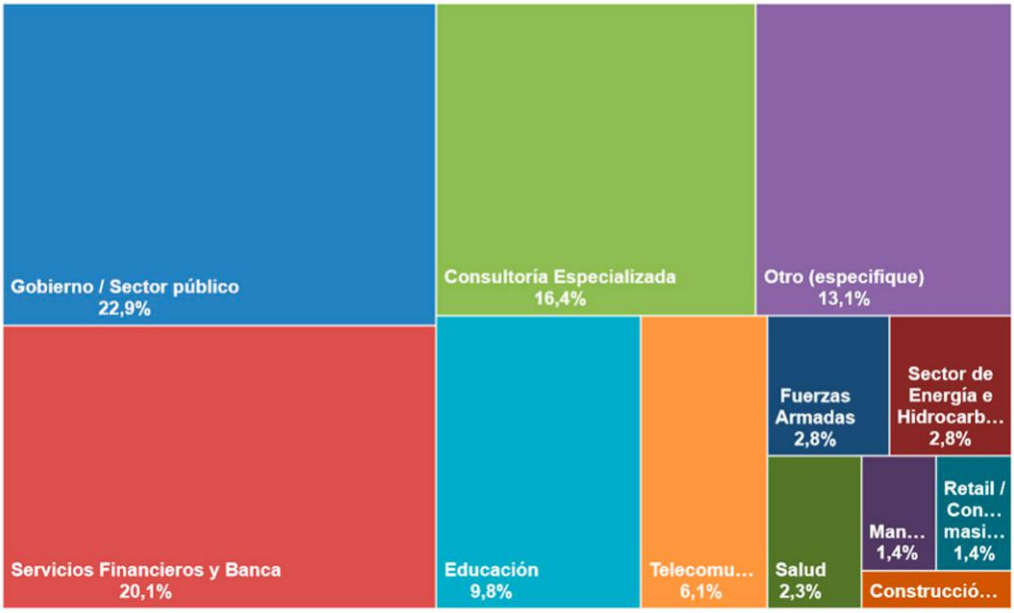
**Capital intelectual**: Busca definir cómo son las áreas de seguridad y las características básicas en materia de experiencia, formación y capacitación de los profesionales de seguridad. Muestra también la relación de las instituciones de educación superior frente a una realidad tan cambiante.

**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

De la información recogida en este estudio se muestran en la siguiente gráfica los aspectos clasificados como importantes por todos los encuestados y reunidos en un grupo denominado top de Hallazgos de las dimensiones de la encuesta.


*Gráfica 1: Top de Hallazgos*



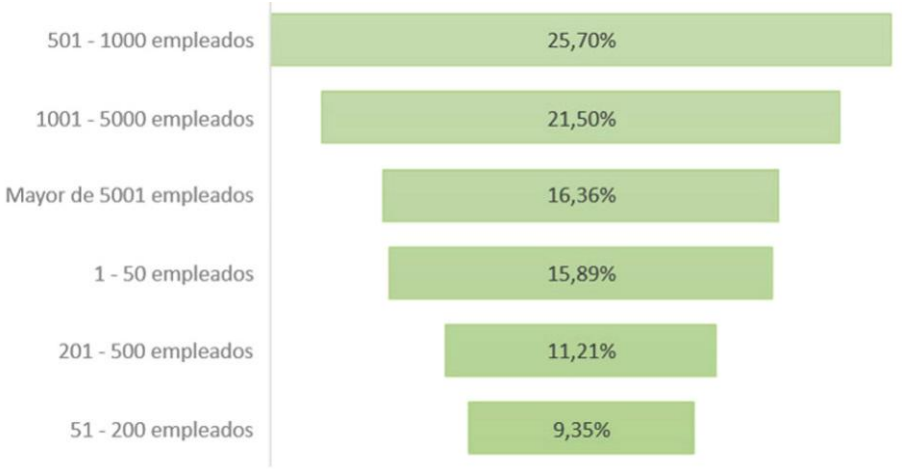

*Gráfica 2: Sectores participantes*

En la gráfica 1 se encuentran los datos más relevantes de la encuesta. El 74% de los encuestados reconoce no usar una estrategia de e-discovery o descubrimiento electrónico para soportar los litigios o reclamaciones legales, un 70% cuenta con un presupuesto para la seguridad de la información en las empresas de la realidad de Colombia. Un 70% indica que la tarea fundamental del responsable de seguridad en Colombia es definir los controles de TI en materia de seguridad de la información. El 70% de los encuestados respondió que en sus empresas se hacen los ejercicios de evaluaciones de riesgos en donde se incluye a la seguridad de la información. Las áreas de seguridad en Colombia están conformadas entre 1 y 5 personas como lo resalta el 64% de los participantes. Las amenazas persistentes avanzadas son la preocupación más importante según el 50% de los encuestados en Colombia. Por último, el 44% manifiesta que la forma como se mantienen actualizados de las fallas de seguridad en Colombia es a través de la lectura de revistas especializadas en materia de seguridad.

## Demografía

### Sectores participantes

La gráfica 2 refleja la participación de 13 sectores de la economía colombiana. Los tres segmentos con mayor participación de la encuesta para este año fueron Gobierno, Sector Financiero y la Consultoría Especializada.

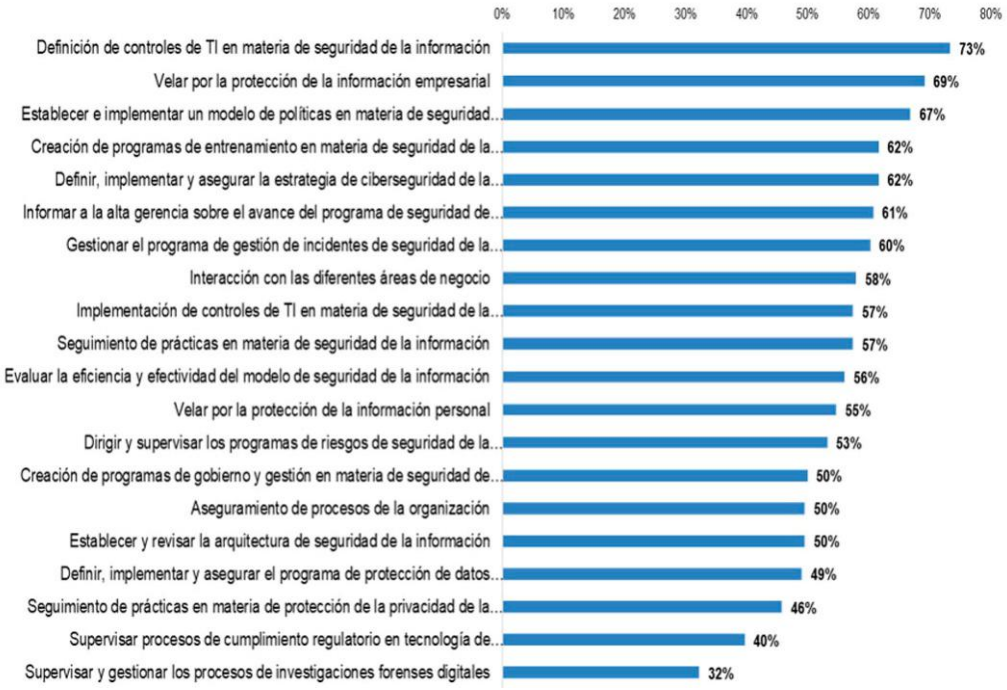



*Gráfica 3: Tamaño de las empresas participantes.*

La Grafica 3 muestra el tamaño de las empresas en Colombia, de acuerdo con el número de empleados. El 25% de las empresas están entre los 501 a 1000 empleados, el segundo lugar son las empresas pequeñas (21,50%) que cuentan con 1001 a 5000 empleados.

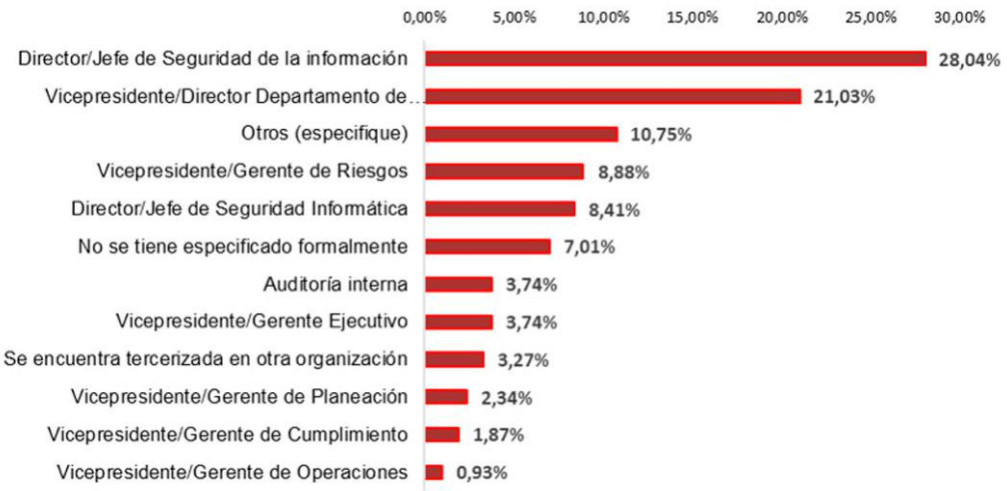
La gráfica 4 muestra los cargos de los encuestados, entre los que se cuentan. Profesionales de las áreas de TI, Oficiales de Seguridad, Auditores Internos, Directores de Seguridad de la Información. Así mismo, figuran otras clasificaciones para los profesionales de seguridad digital en el país, tales como analistas y profesionales de planta de seguridad, docentes de cátedra y planta de las áreas de seguridad como los más relevantes.


*Gráfica 4: Cargos de los encuestados*




*Gráfica 5: Funciones del responsable de seguridad*

En la gráfica 5 se observan las tareas realizadas por los profesionales de seguridad dentro de las organizaciones. El porcentaje más alto está representado por la definición de controles de TI en materia de seguridad de la información, velar por la protección de la información em-




*Gráfica 6: Dependencia del área de seguridad*

presarial y establecer e implementar un modelo de políticas en materia de seguridad de la información como las principales.

La gráfica 6 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 del Director/Jefe de Seguridad Informática y como tercer lugar la Vicepresidencia/Director Departamento de Tecnologías de la Información.

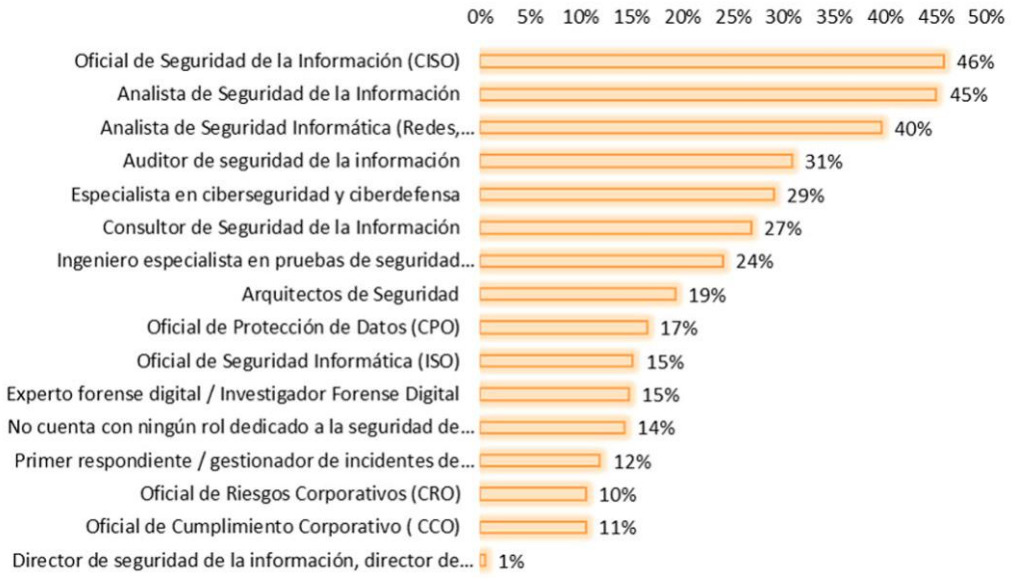
En la gráfica 7 se observan los roles dentro de una organización, en materia de seguridad digital. En Colombia figuran los analistas de seguridad (información e informática); le sigue el cargo denominado CISO, al que se suman los ingenieros de pruebas, entre los principales roles.

## Consideraciones de los datos

Según El *Data Breach Report* (2020) de la Firma Verizon, manifiesta que el tamaño de las empresas sí importa. En su metodología define que las empresas de menos de 1000 empleados son consideradas (SMB) (*Small, Medium Business*) y por encima de 1000 empleados son consideradas grandes empresas.

En ambos casos el informe indica que es muy probable que las pequeñas empresas no estén generando los esfuerzos suficientes para identificar a sus adversarios.

Al contrastar con los resultados de este año, encontramos que en Co-




*Gráfica 7: Roles de Seguridad*

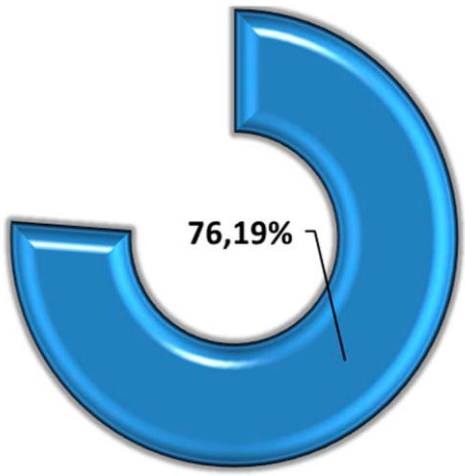
lombia hay una distribución de empresas interesante: participan empresas grandes de más de 1000 empleados con un 38% y 62% son de menos de mil. Por tanto se puede advertir que existe una alta probabilidad de que las empresas colombianas puedan ser víctimas de un ataque informático.

De acuerdo con CISCO (CISCOc, 2019), una de las funciones primarias de los responsables de seguridad de las empresas está relacionada en primer lugar con la atención a los riesgos, colocar límites a los temas de presupuestos, colaboración con las áreas de la organización, educar y crear cultura, saber cómo se presentan los beneficios de las inversiones en seguridad y ser estratégico en la venta de la implementación de soluciones técnicas de seguridad.

En otro informe Kaspersky (2019), se resalta que la identificación de riesgos y amenazas son tareas claves de los profesionales de seguridad. En otro reporte (Marlin Hack, 2020), se afirma que solo el 50% del tiempo del profesional de seguridad se dedica a su función principal que es la de proteger y defender el negocio, así mismo, el 40% manifiesta que su función principal es la de buscar soluciones tecnológicas de protección. Al revisar la tendencia nacional para 2020 ésta dista completamente. La función principal está relacionada con la implementación de soluciones de TI.

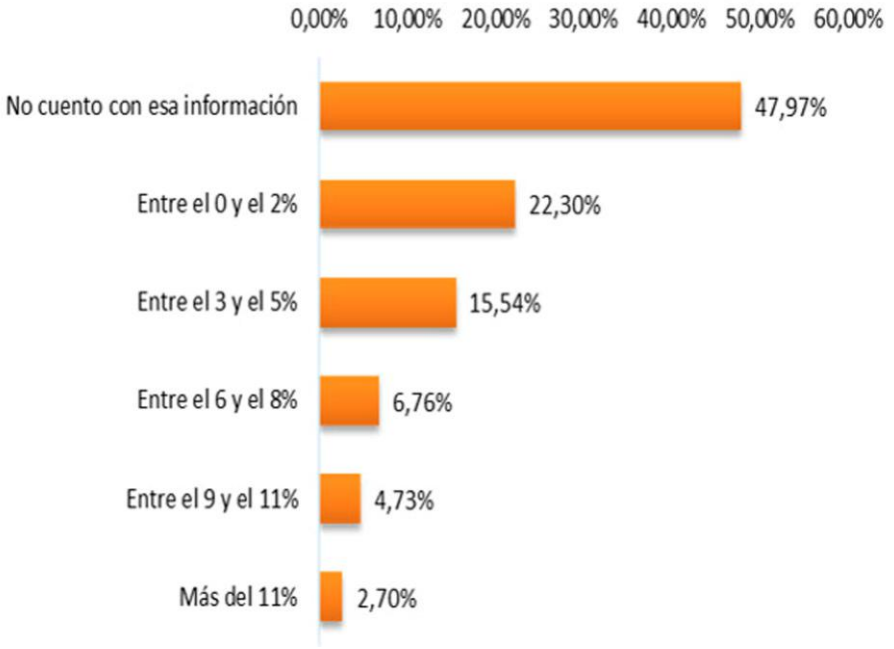
## Presupuestos

La realidad colombiana es muy interesante, en materia de presupuestos en el mundo de la seguridad digital. El 76% de los participantes manifiesta que sí tiene presupuesto asignado a la seguridad digital de sus organizaciones, lo cual se refleja en la gráfica 8.

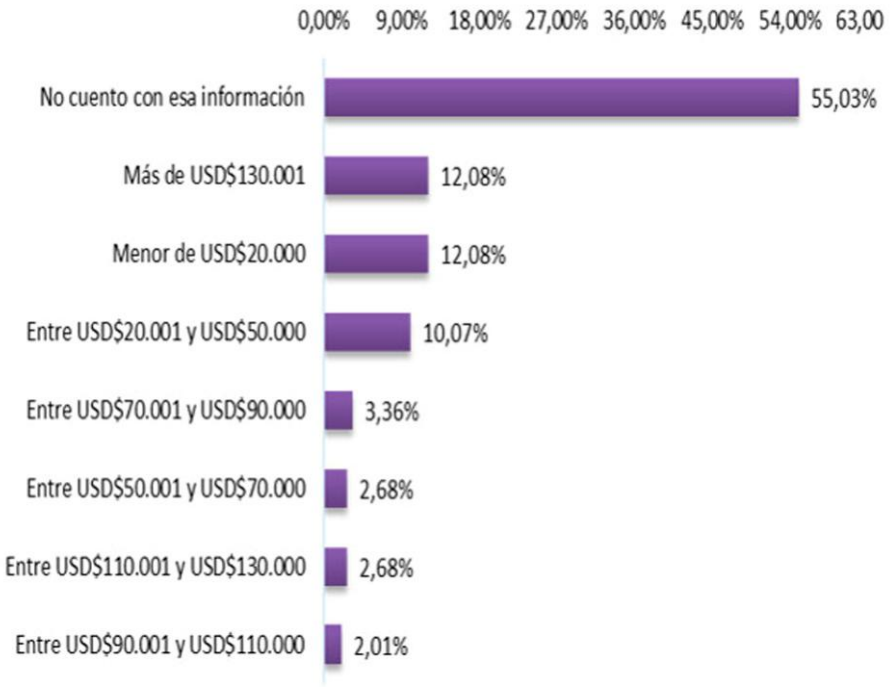



*Gráfica 8: Presupuesto de Seguridad*

La gráfica 9 muestra el monto del presupuesto en relación con el presupuesto global; cerca del 47% de los encuestados lo conoce, mientras que el 54% dice no conocer o no tener la información. La gráfica 10 refleja la distribución de los presupuestos en dólares. Para este año cerca del 45% tiene un monto asignado para la seguridad, el 55% restante manifiesta no conocer dicha información. Esto se puede explicar, toda vez que los cargos de mayor participación están com-




*Gráfica 9: Porcentaje del presupuesto Global*




*Gráfica 10: Presupuesto de Seguridad*


*Gráfica 11: Inversión de Seguridad*

puestos por auditores y los profesionales de las áreas de tecnologías que pueden no conocer los detalles internos de las áreas de seguridad. La otra razón para que se dé esta realidad es que muchos de los roles de las organizaciones están asociados con los analistas de seguridad, quienes suelen no conocer estos detalles. La gráfica 11 muestra cómo se están realizando las inversiones en materia de seguridad, siendo la inversión en tecnologías de seguridad la de mayor interés. Las otras temáticas que se resaltan son la contratación de servicios de consultoría, la renovación del licenciamiento de algunas tecnologías en materia de seguridad digital, la capacitación del área de seguridad, monitoreo y gestión con terceros. La gráfica 12 representa la distribución de los sectores principales y sus franjas de inversión, por los rubros estudiados donde se hacen las inversiones. En ella se pueden ver las tendencias de cada uno de los sectores, ejemplo el sector de fuerzas armadas que sus inversiones están por encima de los US$130.000 en la renovación de licencias y/o hardware, como su valor más representativo, en las otras consideraciones mueven sus presupuestos sobre la misma franja de los US$130.000.

## Consideraciones de los datos

Los reportes internacionales ratifican la tendencia de Colombia de ver aumentos pequeños en los presupuestos de seguridad en las organizaciones, de todos los tama-

ños y sectores. Sin embargo, al revisar el informe Ponemon-IBM (2020) y de ISACA (2020), muestran que los presupuestos año a año se incrementan, confirmando la tendencia de Colombia.

En el informe de Ponemon-IBM (2020) solo el 33% considera que se tienen los presupuestos adecuados en materia de ciberseguridad para garantizar la ciberresiliencia, se pasó en promedio de $US3,4 millones a $US3,6 millones. Si bien influyen las realidades económicas y digitales en donde se realizan los estudios lo que sí vale resaltar son las tendencias de tener unos pre-

| | 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 |
|---|---|---|---|---|---|
| Consultoría Especializada | | | | | |
| Entre USD$20.001 y USD$50.000 | 2,13% | 5,41% | 0,00% | 4,88% | 0,00% |
| Entre USD$90.001 y USD$110.000 | 0,00% | 0,00% | 2,70% | 0,00% | 3,23% |
| Menor de USD$20.000 | 6,38% | 13,51% | 8,11% | 4,88% | 6,45% |
| Educación | | | | | |
| Entre USD$20.001 y USD$50.000 | 2,13% | 0,00% | 0,00% | 2,44% | 0,00% |
| Entre USD$50.001 y USD$70.000 | 2,13% | 0,00% | 2,70% | 2,44% | 0,00% |
| Menor de USD$20.000 | 2,13% | 2,70% | 0,00% | 2,44% | 0,00% |
| Fuerzas Armadas | | | | | |
| Más de USD$130.001 | 4,26% | 2,70% | 0,00% | 4,88% | 0,00% |
| Gobierno / Sector público | | | | | |
| Entre USD$110.001 y USD$130.000 | 4,26% | 2,70% | 2,70% | 4,88% | 9,68% |
| Entre USD$20.001 y USD$50.000 | 6,38% | 2,70% | 8,11% | 4,88% | 3,23% |
| Entre USD$50.001 y USD$70.000 | 6,38% | 2,70% | 5,41% | 7,32% | 0,00% |
| Entre USD$70.001 y USD$90.000 | 2,13% | 2,70% | 2,70% | 0,00% | 3,23% |
| Entre USD$90.001 y USD$110.000 | 2,13% | 2,70% | 2,70% | 2,44% | 3,23% |
| Más de USD$130.001 | 6,38% | 2,70% | 5,41% | 4,88% | 6,45% |
| Menor de USD$20.000 | 2,13% | 2,70% | 0,00% | 2,44% | 3,23% |
| Otro (especifique) | | | | | |
| Entre USD$20.001 y USD$50.000 | 0,00% | 8,11% | 5,41% | 2,44% | 3,23% |
| Entre USD$70.001 y USD$90.000 | 0,00% | 0,00% | 2,70% | 0,00% | 0,00% |
| Más de USD$130.001 | 6,38% | 8,11% | 8,11% | 9,76% | 6,45% |
| Menor de USD$20.000 | 2,13% | 8,11% | 2,70% | 4,88% | 3,23% |
| Sector de Energía e Hidrocarburos | | | | | |
| Más de USD$130.001 | 8,51% | 5,41% | 5,41% | 4,88% | 9,68% |
| Servicios Financieros y Banca | | | | | |
| Entre USD$20.001 y USD$50.000 | 4,26% | 5,41% | 5,41% | 2,44% | 6,45% |
| Entre USD$70.001 y USD$90.000 | 4,26% | 2,70% | 2,70% | 4,88% | 6,45% |
| Entre USD$90.001 y USD$110.000 | 2,13% | 2,70% | 2,70% | 2,44% | 3,23% |
| Más de USD$130.001 | 10,64% | 8,11% | 8,11% | 7,32% | 9,68% |
| Menor de USD$20.000 | 10,64% | 2,70% | 10,81% | 9,76% | 12,90% |
| Telecomunicaciones | | | | | |
| Entre USD$110.001 y USD$130.000 | 0,00% | 2,70% | 2,70% | 0,00% | 0,00% |
| Entre USD$20.001 y USD$50.000 | 2,13% | 2,70% | 2,70% | 2,44% | 0,00% |

*Gráfica 12: Montos en dólares de las inversiones de seguridad. Sectores vs. inversiones*

supuestos más dotados para el mundo de la ciberseguridad. En el caso Colombia lo que sí se puede ver es que la franja mayor a los $US130.000 dólares también tiene un porcentaje importante y con tendencia a seguir creciendo en los próximos años.

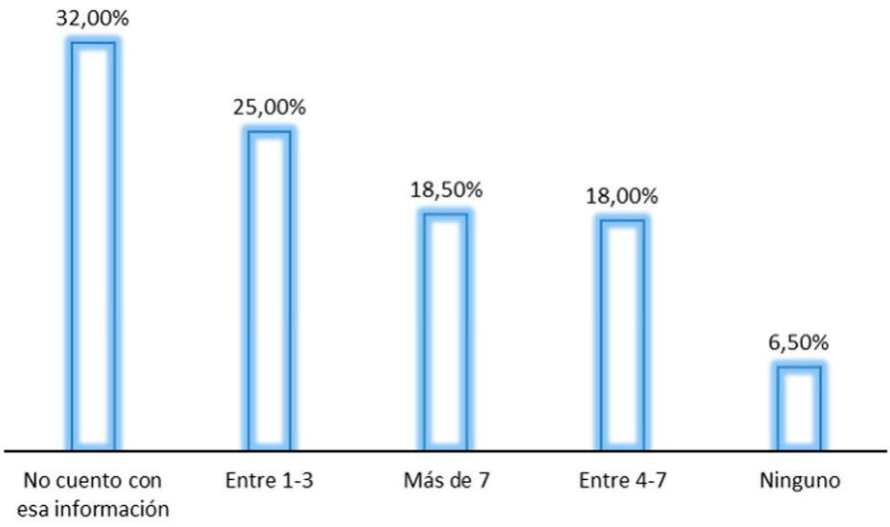
## Incidentes

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.

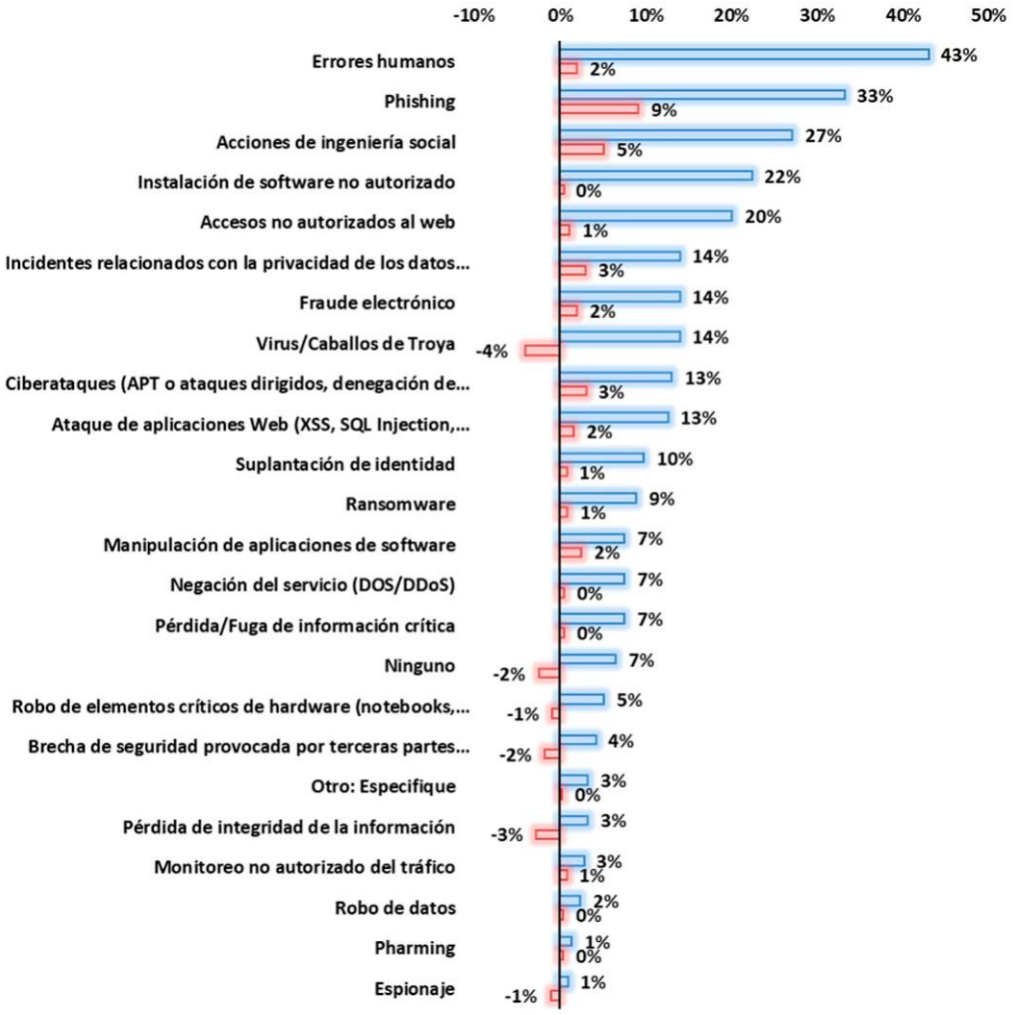
La gráfica 13 muestra la cantidad de incidentes que se presentan en Colombia, según los participantes. El 68% de ellos manifiesta haber tenido, por lo menos, un incidente de seguridad o ciberseguridad en sus organizaciones. El 32% de los participantes no tiene información al respecto, el 6,5% de los participantes resaltan que no tuvieron un incidente de seguridad.

La gráfica 14 relaciona los tipos de incidentes que se presentaron en las organizaciones, así como su variación con relación al año anterior. Tenemos en este sentido, errores humanos, phishing y ataques generales de ingeniería social como los principales de este año, y comparado con el año inmediatamente anterior es el phishing el que más varía con un 9%. Llama la atención que para 2020 decrece en un 2% aquellos que dicen no haber recibido ningún ataque durante el año.

La grafica 15 que es un valor nuevo medido este año, se evalúa cuanto en promedio le puede estar costando un incidente de seguridad a las



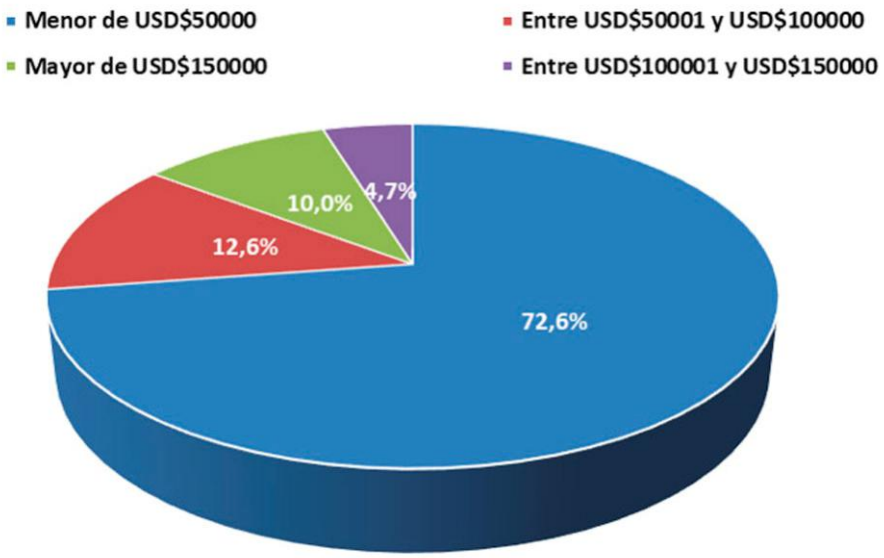

*Gráfica 13: Cantidad de Incidentes. Incidentes*




*Gráfica 14: Tipos de Incidentes de Seguridad*

empresas. Los datos muestran que cerca del 73% manifiestan que sus incidentes cuestan menos de $US 50.000, cerca del 13% entre $US 50.000 y $US 100.000, el 10% manifiesta que le cuesta más de $US 150.000 y el resto manifiesta que está en la franja de los $US 100.001 hasta los $US 150.000 dólares.

La gráfica 16, muestra ante quien se reportan los incidentes de seguridad. Los datos reflejan que, ante un incidente y su identificación, el 52% de los participantes lo notifican a los directivos de la organización, 37% a los equipos de atención de incidentes CSIRT (*Computer Security Incident Response Team*), 27% a las autoridades de orden




*Gráfica 15: Costos de los Incidentes*

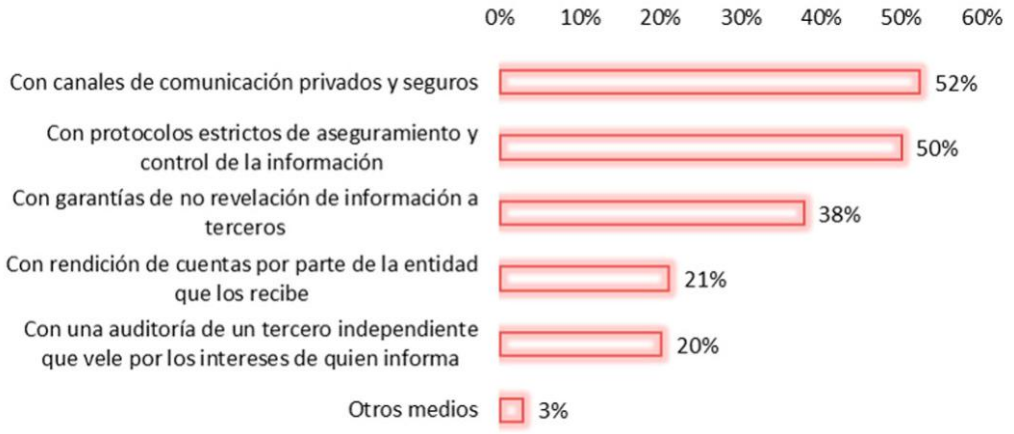

*Gráfica 16: A quien se reportan los incidentes*


*Gráfica 17: Razones para no denunciar los incidentes*

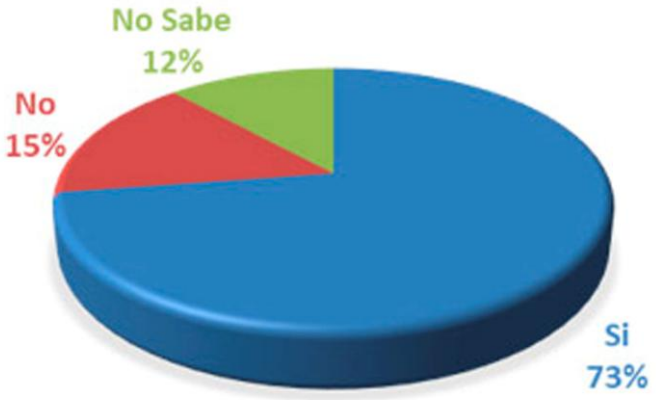
nacional como los datos más relevantes.

La gráfica 17, muestra las razones por las que no se denuncian los incidentes. En esta fundamentalmente la imagen 34%, la reputación 28%, y la responsabilidad legal 24% son las razones que aducen los encuestados de por qué no se denuncian los incidentes. La gráfica 18 muestra la forma los mecanismos que se podrían utilizar para compartir información o denunciar información. En primer lugar, está usar canales privados y cifrados como el mecanismo más idóneo 52% y protocolos de aseguramiento de la información bien definidos (50%), sería la forma en como estos intercambios de información se realizarían.

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




*Gráfica 18: Mecanismos para denunciar/compartir*

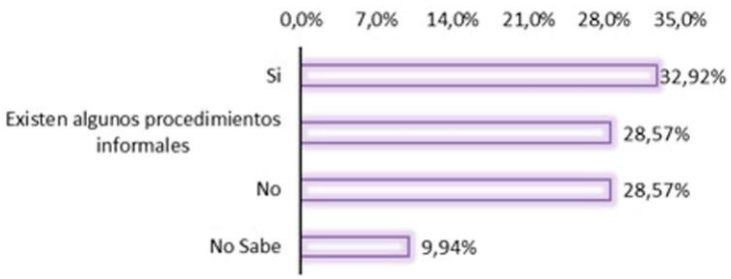



*Gráfica 19: Consciencia de la Evidencia Digital*

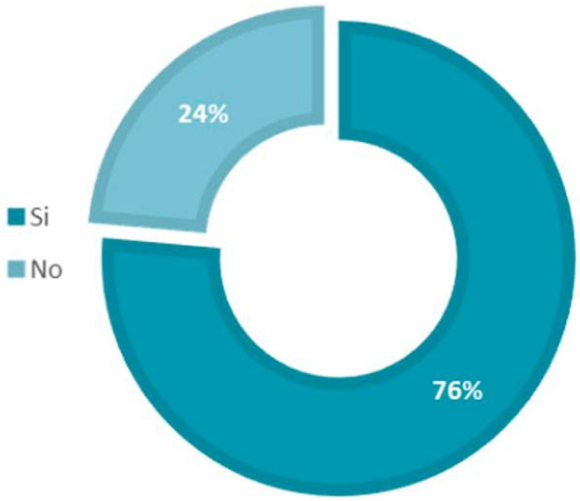
adecuado mejoramiento. La gráfica 19, resalta la importancia y consciencia en relación con el adecuado manejo de la evidencia digital. El 73% resalta que es consciente de ello. Sin embargo, la gráfica 20 muestra que solo el 33% posee un procedimiento para hacer la gestión de la evidencia digital y el 29% manifiesta informalidad en la práctica de los procedimientos adecuados. La gráfica 21 resalta que el 76% mantiene algún tipo de contacto con autoridades del orden local o regional.

## Consideraciones de los datos

Los reportes internacionales como Ponemon-IBM (2020) y EY (2020), resalta que al menos el 57% de las organizaciones estudiadas han tenido un incidente de seguridad, que desemboca en una disrupción de la organización y/o algún proceso de TI, así mismo resalta que al menos 55% ha sufrido de brechas de seguridad donde se han comprometido al menos 1000 registros de datos, donde existe información sensible de clientes y confidencial.




*Gráfica 20: Procedimiento de Gestión de Evidencia Digital*




*Gráfica 21: Contactos con autoridades locales/regionales*

Accenture (2020), manifiesta que la respuesta de incidentes como proceso de la organización que 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 manifiesta 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.

No obstante, en el mismo estudio consideran que se deben hacer más esfuerzos para aquellos que todavía tienen dudas, como son los casos en nuestro país. En Colombia aún no se piensa del todo en ello y por tanto se evidencia que no se está cerca de esta práctica. El costo de los incidentes es otro de los factores claves, el estudio de Accenture (2020) muestra en sus datos que el promedio de costos totales de un ciberataque es de $US380.000 dólares por incidente.

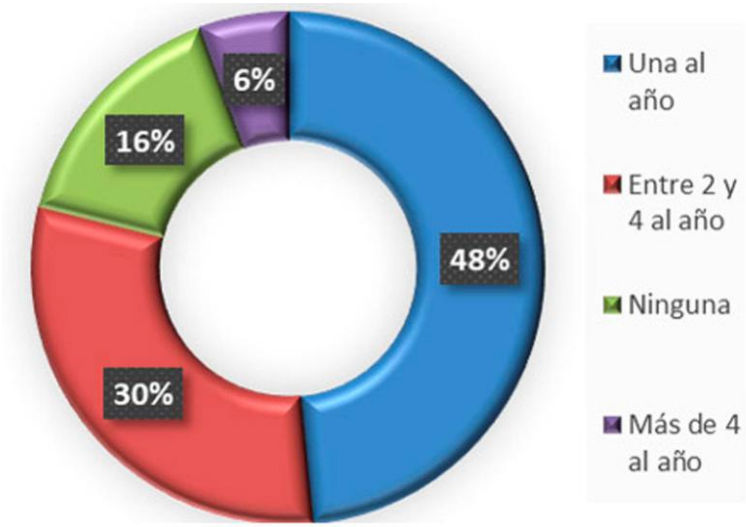
En Colombia y por primera vez este estudio analiza los costos estimados de un incidente de seguridad, cuyos resultados no confirman las lecturas internacionales. La mayoría de los encuestados (73%) relaciona que los costos de los incidentes están por debajo de los $US 50.000 dólares, y solo el 27% considera los costos por encima de ese valor. En este punto, pueden considerarse dos lecturas, una que no es están considerando todos los costos implicados a la hora de analizar un incidente siguiendo una metodología concreta, y otra, que

el plan de gestión de incidentes no es evaluado regularmente como lo sugiere el estudio de CISCO (2020), el cual manifiesta que en las empresas medianas y pequeñas está práctica no es desarrollada.

La práctica de la gestión de incidentes que en Colombia según los datos recabados se identifica como una práctica no desarrollada, resultado que ratifica los hallazgos del informe de EY (2018) que describe que las inversiones en seguridad están orientadas a fortalecer la gestión de incidentes toda vez que se considera una práctica que tiene muy poca madurez en las organizaciones cerca del 10% de los participantes hace esta consideración. El informe de Deloitte (2019), resalta que los mayores impactos de un incidente se expresan en términos perdidas de utilidades (21%), pérdida de confianza (21%), pérdida de reputación (16%), multas y sanciones (14%). Estos datos ratifican las preocupaciones de los responsables de seguridad en Colombia al no denunciar los incidentes, comoquiera que la pérdida de la reputación, de confianza, las sanciones y/o multas son las razones que se aducen para no hacerlos.

## Herramientas

La gráfica 22 muestra el uso de las evaluaciones de seguridad como una de las prácticas más usadas. Un 84% de los participantes manifiesta hacer uso de esta práctica como instrumento clave para validar el estado de la seguridad digital de la organización. El 48% de los participantes usa esta práctica una vez al mes; el 30% entre dos y 4 veces al año; el 6% manifiesta usa más de 4 veces al año y el 16% dice no usarla.




*Gráfica 22: Evaluaciones de Seguridad*

| Etiquetas de fila | Una al año | Entre 2 y 4 al año | Ninguna | Más de 4 al año |
|---|---|---|---|---|
| Gobierno / Sector público | 20,50% | 3,73% | 1,86% | 0,62% |
| Servicios Financieros y Banca | 8,07% | 9,94% | 2,48% | 2,48% |
| Consultoría Especializada | 6,83% | 6,21% | 4,35% | 0,00% |
| Otro (especifique) | 5,59% | 2,48% | 0,62% | 1,24% |
| Educación | 4,35% | 3,73% | 0,62% | 0,00% |
| Telecomunicaciones | 0,62% | 1,24% | 3,11% | 0,62% |
| Fuerzas Armadas | 0,00% | 1,24% | 0,00% | 0,62% |
| Sector de Energía e Hidrocarburos | 1,24% | 0,62% | 0,00% | 0,00% |
| Salud | 0,62% | 0,62% | 0,62% | 0,00% |
| Construcción / Ingeniería | 0,62% | 0,00% | 0,62% | 0,00% |
| Manufactura | 0,00% | 0,00% | 1,24% | 0,00% |
| Retail / Consumo masivo | 0,00% | 0,62% | 0,00% | 0,00% |

*Gráfica 23: Evaluaciones de Seguridad por Sectores.*

La gráfica 23 indica como los sectores de están usando las evaluaciones de seguridad. El sector Gobierno, con un 21% usa al menos una prueba de seguridad al año, el sector Financiero cerca del 10% lo hace entre 2 y 4 veces al año, y la consultoría especializada con un 7% lo hace también una vez al año.

La gráfica 24, muestra cuáles son los mecanismos de seguridad comúnmente usados en las organizaciones. VPNs 52%, soluciones Antimalware 44% y WAF (*Web Application Firewalls*) 42% son los de mayor uso, sin embargo, comparado con el año inmediatamente anterior, las herramientas anti DDOS (16%), los WAF (16%), los firewall de nueva generación (14%), los SIEM (14%) (*Security Information Event Management*), los servicios de SOC (13%) y las VPNs (12%) son los que mayor crecimiento respecto del año anterior.

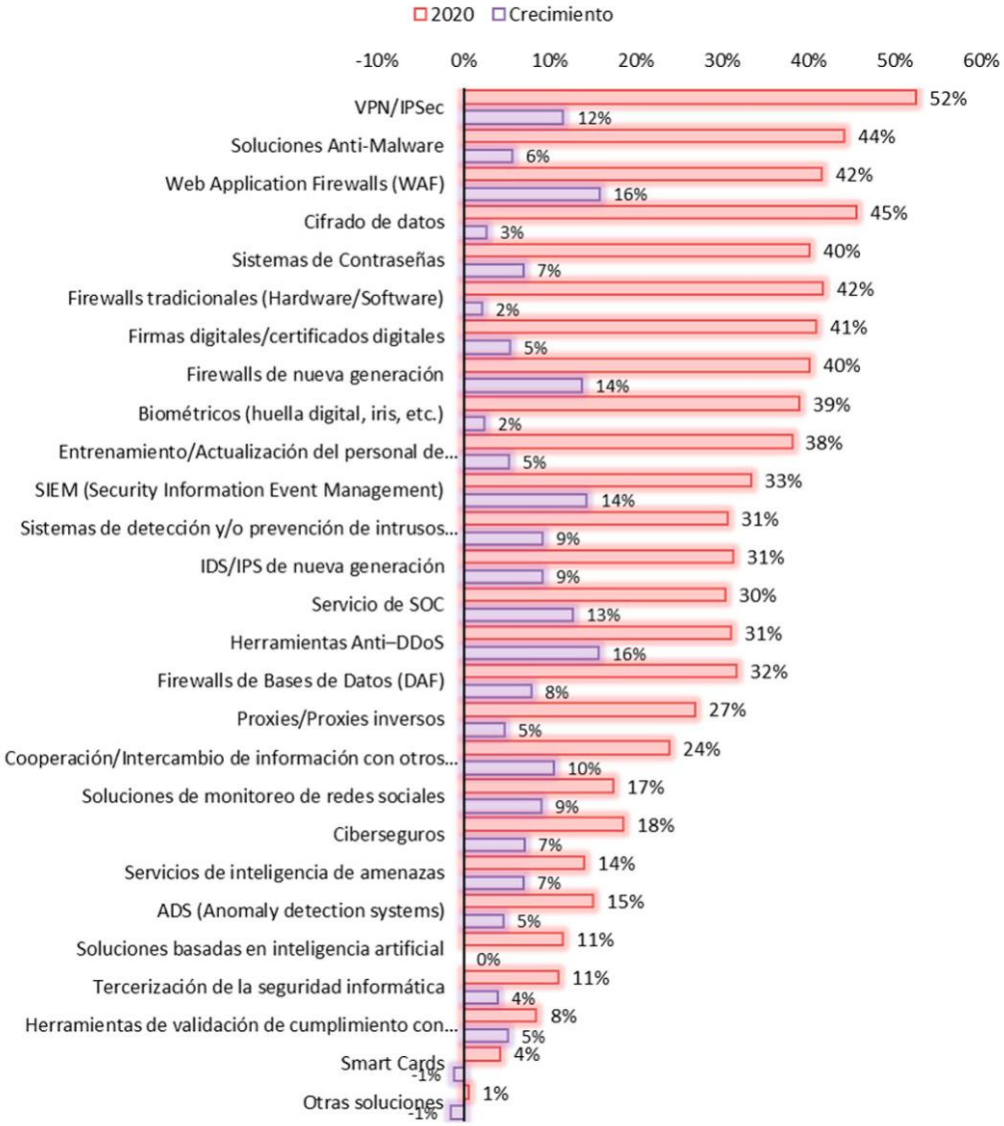
La gráfica 25 resalta las herramientas que más se usan para notificarse de las fallas de seguridad los profesionales. El 55% usa la lectura de sitios especializados como la práctica más común.

## Consideraciones de los datos

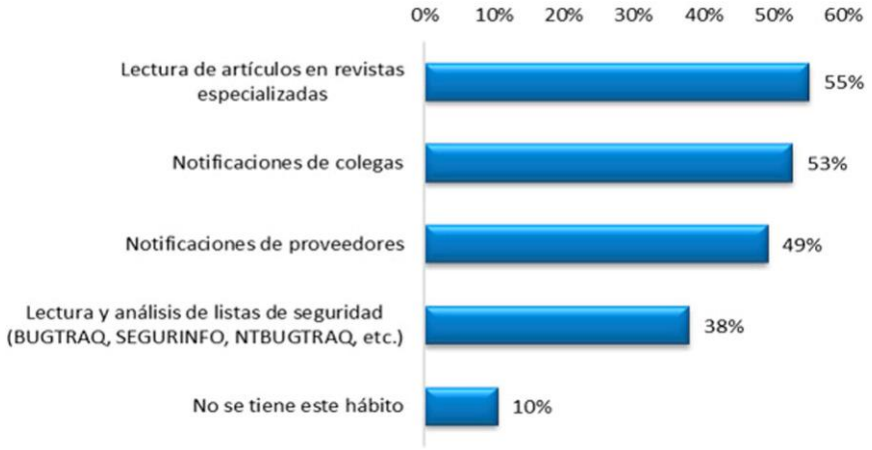
La tendencia en Colombia se mantiene al compararse con los años anteriores. Así mismo lo ratifican los datos internacionales, el informe de CISCO (2020) que sostiene que el 86% de las empresas pequeñas y medianas valoran la efectividad de sus programas de seguridad, comparado con el 90% de las empresas de gran tamaño. En el mismo informe sostiene que las empresas mejoran sus infraestructuras de seguridad, aun así, no son suficientes para atender los desafíos de protección y continuidad de la operación como les gustaría.

En el estudio de Ponemon-IBM (2020), 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. Así las cosas, en Colombia los datos muestran una evolución significativa de esta práctica y basado en ello se puede visualizar que despunta una tendencia en este 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 (2020), quien señala que las investigaciones de seguridad son las formas más utilizadas para descubrir brechas de seguridad.




*Gráfica 24: Mecanismos de Seguridad usados*




*Gráfica 25: Mecanismos de notificación*

## Políticas

La gráfica 26 refleja el estado de las políticas de seguridad en las organizaciones colombianas; el 69,6% de los encuestados manifiestan que tienen formalizada sus políticas de seguridad, el 21,7% actualmente en desarrollo y solo el 8,7% dicen no tener políticas de seguridad de la información.

La gráfica 27, muestra lo que manifiestan los participantes al indagar por los obstáculos por los cuales no hay una postura adecuada de seguridad en sus empresas. La ausencia de una cultura, la falta de apoyo directivo y la falta de colaboración entre área son las tres razones principales que se mantiene como obstáculos de la seguridad.

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

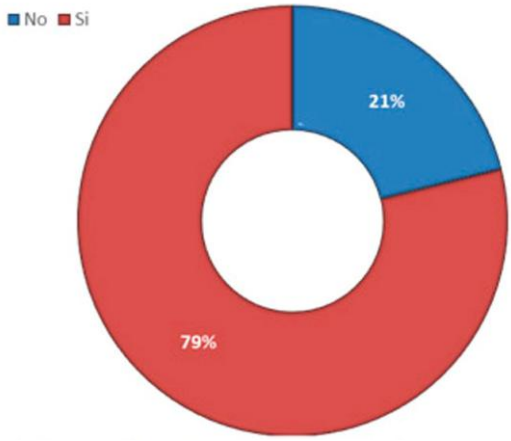

*Gráfica: 26 Estado de las Políticas*


*Gráfica 27: Obstáculos de la Seguridad*

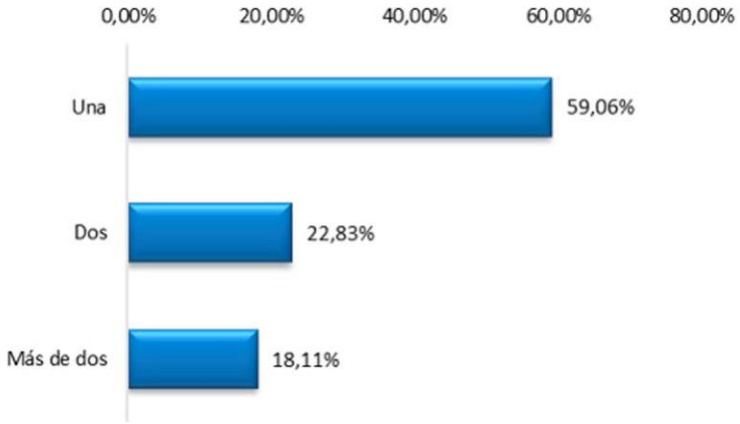
riesgos de seguridad digital y la incluyen en sus ejercicios globales de gestión de riesgos. En la gráfica 29, cerca del 60% realiza el ejercicio de evaluación de riesgos una vez al año, el 22,8% dos al año y el 18% más de dos al año.

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 no tener un proceso formal de gestión de riesgos (44%).

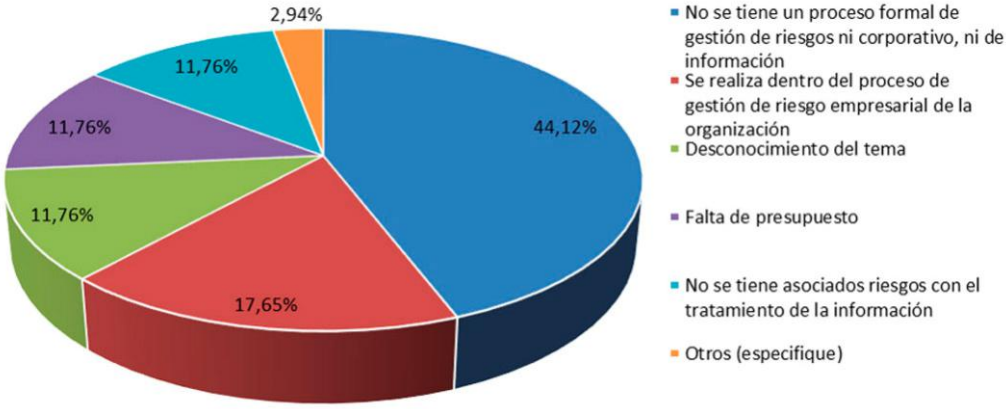
La Gráfica 31 muestra el tipo de metodologías usadas al realizar los ejercicios de gestión de riesgos de seguridad; la ISO 31000, con un 34%, es la metodología más usada. La Gráfica 32, muestra que los incidentes de seguridad son asociados a algún tipo de riesgos. El 51% de los incidentes de seguridad se aso-




*Gráfica 28: Gestión de Riesgos de Seguridad*

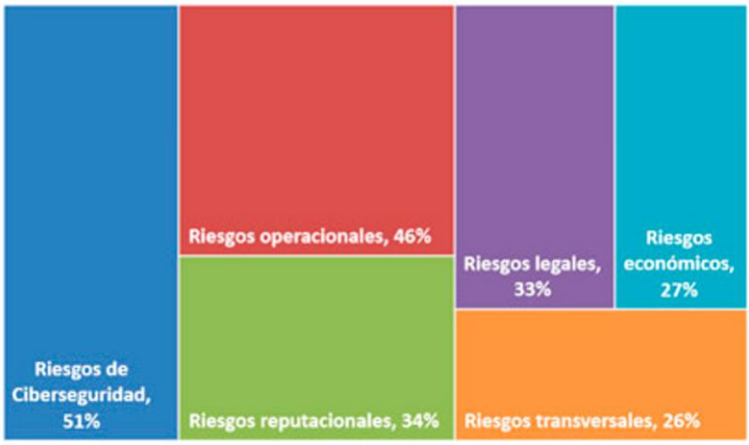



*Gráfica 29: Cantidad de Gestión de Riesgos en Seguridad*




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


*Gráfica 31: Tipos de Metodología*



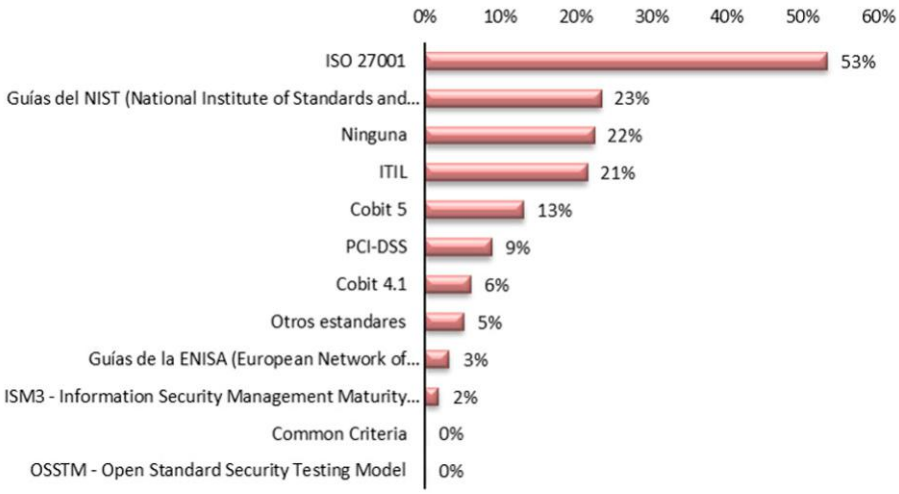

*Gráfica 32: Tipos de Riesgos*

cian a los riesgos de ciberseguridad; el 46% lo asocian a riesgos de operación, el 34% los relacionan con riesgos reputacionales.

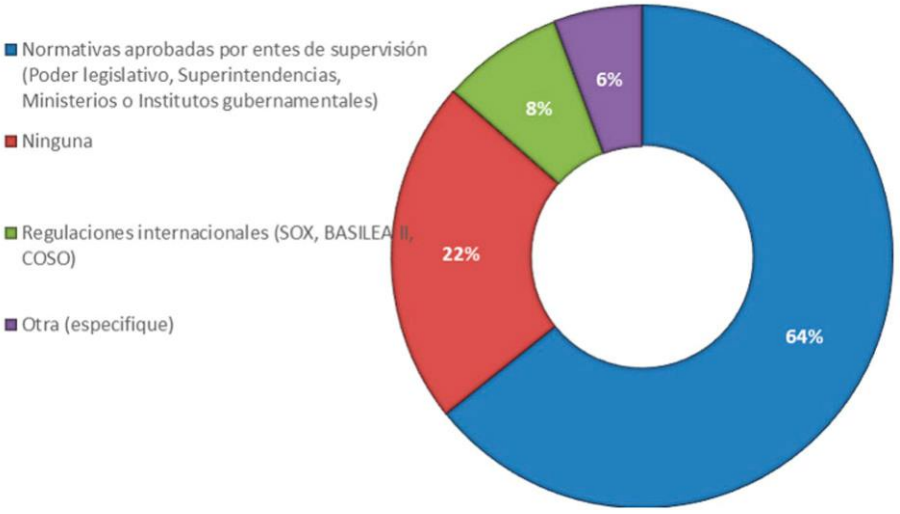
La gráfica 33 ilustra el uso de los distintos marcos de trabajo (*frameworks*) usados en las organizaciones colombianas: ISO/IEC 27001, NIST, Ninguna, ITIL y Cobit 5 son los más usados. La gráfica 34 refleja las regulaciones que las organizaciones deben asegurar. En el caso colombiano, el 64% de los participantes manifiesta que sí existen regulaciones que las organizaciones debe cumplir.

## Consideraciones de los datos

Los riesgos de seguridad de la información y ciberseguridad en defi-




*Gráfica 33: Marcos de trabajo usados*

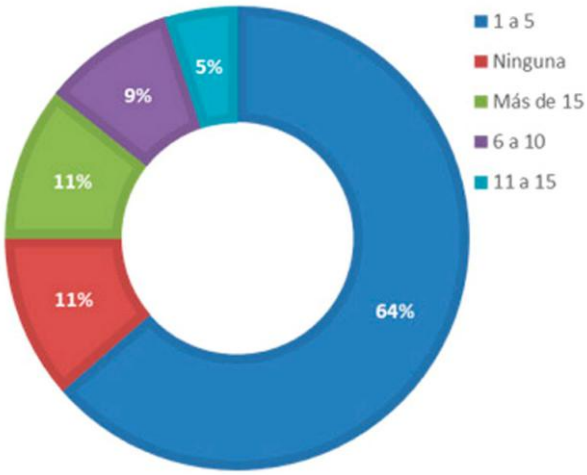



*Gráfica 34: Regulaciones o normativas*

nitiva son una realidad como lo es ratificado en el informe del Foro Económico Mundial (WEF, 2020), el cual manifiesta que la prioridad de estos tipos de ataques es alta en las organizaciones del mundo. Esto ratifica la tendencia de los resultados de Colombia que ven en la práctica de gestión de riesgos una herramienta vital para la construcción de capacidades frente a la atención de los ciberataques, por su parte el estudio de Pricewaterhouse Coopers (PwCb, 2020) resalta que una mayor digitalización en el contexto actual, habilita a la función de gestión de riesgos corporativos a tener relevancia, a responder y pronosticar mejor, y comprometer a las partes interesadas para actuar en un ecosistema digital, como el actual.

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 (CISCOb, 2020) que manifiesta que aquellas compañías que se adhieren a sus prácticas y políticas de seguridad tienen costos menores por brechas relacionadas con los datos en comparación con quienes no se adhieren, lo cual puede apoyar el comportamiento de Colombia en este sentido.

La tendencia internacional se orienta a que, cada vez más, existirán regulaciones más globales. La regulación GDPR (*General Data*



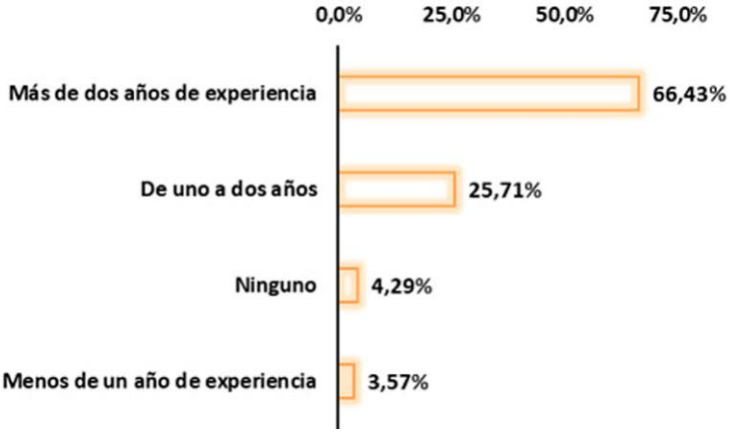

*Gráfica 35: Recursos dedicados a la Seguridad*

*Protection Regulation*) nace como una necesidad de la Comunidad Europea (EU), de gran impacto a nivel global.

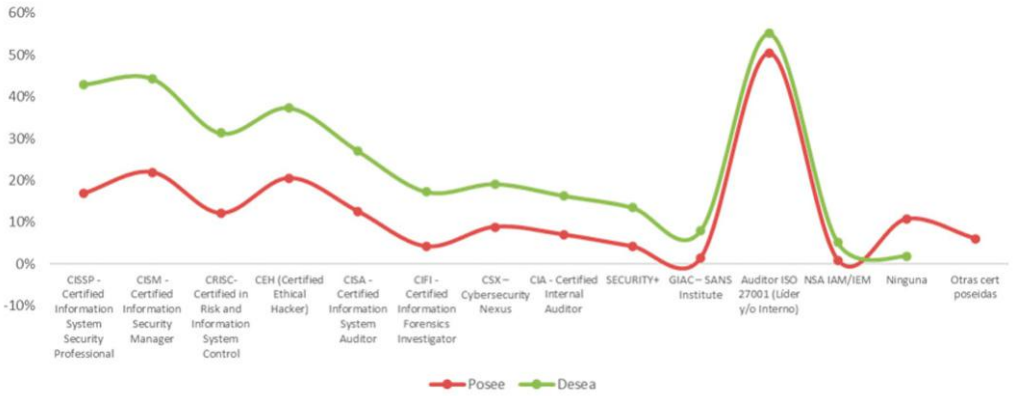
## Capital intelectual

La gráfica 35 relaciona los recursos que son dedicados a la seguridad en las empresas, cerca del 89%, manifiesta tener recursos dedicados a la seguridad, la predominancia es de 1 a 5 con un 64%. La gráfica 36 resalta que el tiempo de experiencia promedio para que los profesionales de seguridad sean contratados en Colombia es superior a dos (2) años (66%).

La gráfica 37, representa la comparación de las certificaciones que los profesionales de seguridad poseen en la actualidad y que desean alcanzar en el tiempo. CISSP, CISM,




*Gráfica 36: Experiencia del profesional*




*Gráfica 37: Certificaciones alcanzadas vs deseadas*

CRISC y CEH, son las certificaciones que mayor variación tienen entre lo que se tiene actualmente y lo deseado en el futuro.

La gráfica 38, indaga sobre la forma en que la educación ha participado en la formación de los profesionales de seguridad. El 31% manifiesta y reconoce que se están ofreciendo programas académicos de grados y posgrado en temas de seguridad, el 29% que los niveles de investigación son escasos en Colombia.

## Consideraciones de los datos

La experiencia del profesional de seguridad de las organizaciones en Colombia es clave, así como su formación. Las tendencias internacionales igual ratifican los resultados


*Gráfica 38: Papel de la educación*

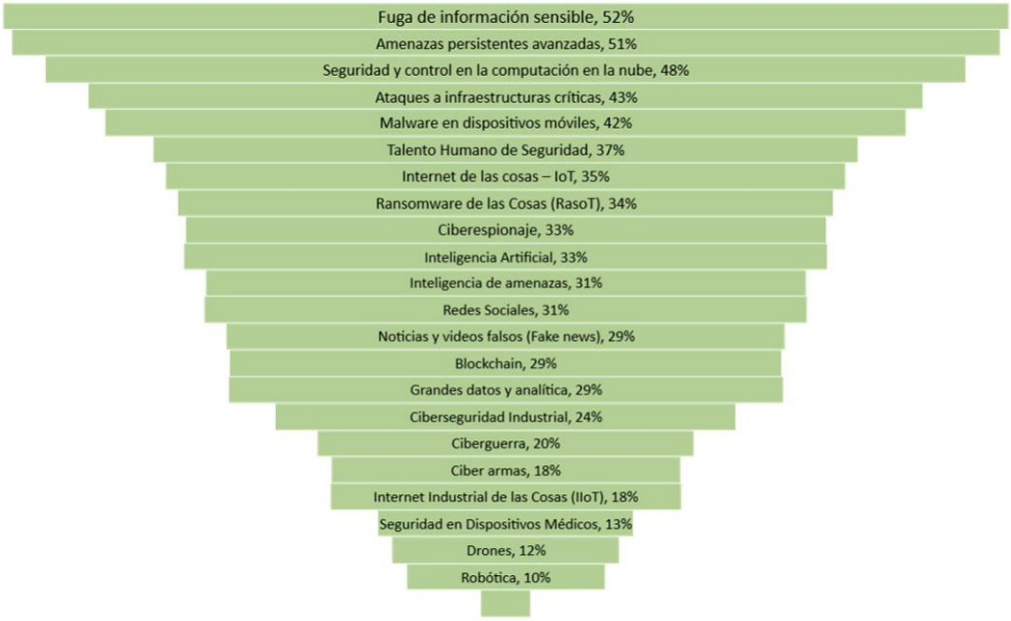
de Colombia. En su informe ISACA (2020), resalta que es clave la experiencia de los profesionales de seguridad. De igual forma, el reporte de MarlinHawk (2020), muestra que el promedio de los profesionales estudiados del mundo de la seguridad tiene 4 años en una posición en esta área. Desde el mismo 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 (2020) muestra en sus datos que solo el 47% considera algo importante un grado universitario para los profesionales de seguridad y le dan más importancia a la experiencia (73%). El informe también resalta que ni los grados universitarios, ni los cursos complementarios de formación, dan una garantía que demuestre conocimientos avanzados, o habilidades suficientes.

En relación con las certificaciones, CISSP, CISM, CRISK y CEH, muestran ser las certificaciones, que tienen más 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. Por otra parte, el estudio de ISC$^2$ (2019) ratifica que son los profesionales de seguridad quienes en su mayoría pagan por las certificaciones que obtienen.

Con relación a la educación y su importancia en la vida del profesional de la seguridad, los datos muestran en Colombia, que se reconocen los esfuerzos que hacen los programas por formar a los profesionales de seguridad. Datos que se pueden ver refrendados en el documento de ISC$^2$ (2019), donde se manifiesta que cerca del 87% de la población analizada tienen algún tipo de estudio formal y estudio avanzado académico con relación al mundo de la seguridad, reforzando así la tendencia de Colombia a tener programas formales de educación superior en ciberseguridad.

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 (2019). 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 como 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.



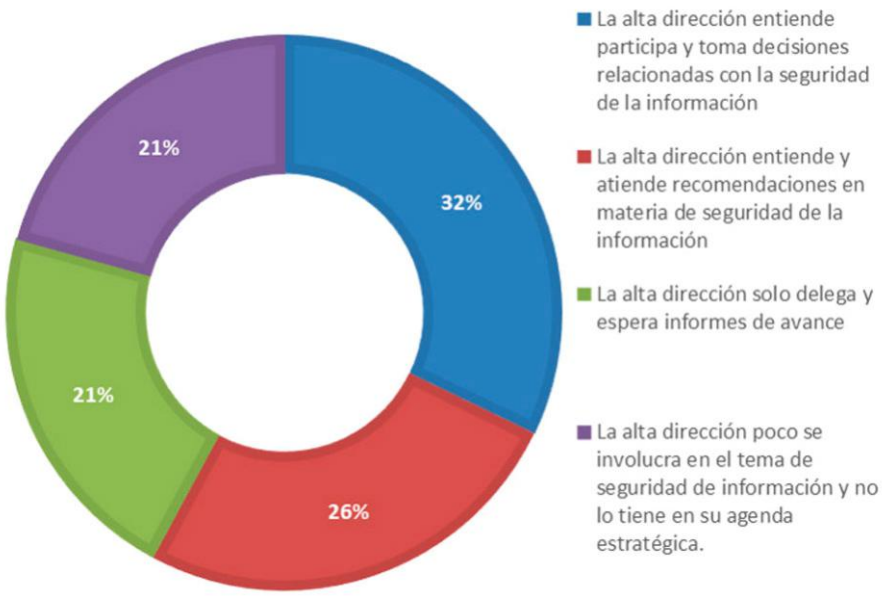

*Gráfica 39: Temas emergentes*

## Temas emergentes

La gráfica 39 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.

La gráfica 40, relaciona la forma en como las juntas directivas, o comités ejecutivos se relacionan con la seguridad. El 51% están atendiendo y participando activamente, mientras que el 42% restante delega o poco se involucra en los temas de seguridad en Colombia.

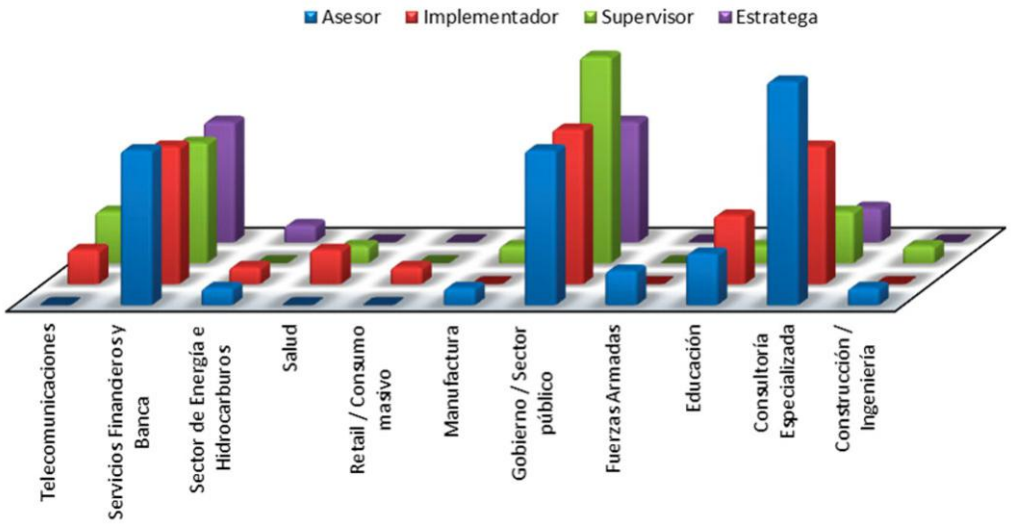
Las gráficas 41, 42 y 43 reflejan la forma como el CISO se ve, se desenvuelve y cómo puede evolucionar en el contexto de las organizaciones nacionales. La gráfica 40 muestra la forma como es visto el profesional de seguridad, en los diferentes sectores de la industria. En este año el 31% resalta que en Colombia es visto como un Asesor, luego como Implementador, Supervisor y en último lugar como Estratega. Interesante ver como en cada industria tienen una vista de su posición. Mientras el sector Financiero y la consultoría especializada esa es la vista que predomina (Asesor), con mucho más fuerza en el sector de consultoría, en el sector de Gobierno, lo ven con fuerza como un Supervisor, esto es, una persona que vela por la eficacia y eficiencia del programa de seguridad, su visión del control es la que rige




*Gráfica 40: Involucramiento de los Directivos*

como principio, vela por los riesgos, y el cumplimiento.

La gráfica 41 muestra la forma como el líder de seguridad entrega información a los grupos de interés, el 51% manifiesta que entrega información con relación a los riesgos en seguridad y ciberseguridad, el 43% manifiesta que entrega in-




*Gráfica 41: Cómo ven al CISO*


*Gráfica 42: Entrega de información del profesional de seguridad*

formación relacionada con los aspectos técnicos, el 40% indica que entrega información relacionada con la gestión, y así mismo, con las brechas de seguridad, y el 14% no entrega información a ningún grupo de interés.

La Gráfica 43 muestra las oportunidades de crecimiento y mejora en las que los profesionales de seguridad pueden trabajar, como parte del cierre de brechas existentes. En primer lugar, las capacidades de gestión son el primer espacio que reconocen como oportunidad para mejorar (52%), las capacidades de liderazgo en segundo lugar (46%), las capacidades técnicas y de experiencia en tercer lugar (44%), las


*Gráfica 43: Camino de crecimiento de un profesional de seguridad*

capacidades de pronóstico con un 36%, la formación académica y técnica un 33% como los aspectos de mejoras y oportunidades.

## 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 (2020), soportan las consideraciones locales, en el sentido de observar a las amenazas avanzadas y los desafíos de la nube como factores claves a tener en cuenta. 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. Por su parte ESET (2019), considera a la inteligencia artificial y las máquinas de aprendizaje un componente clave en su informe de tendencias, que también tiene cabida en los datos de la encuesta de Colombia.

En cuanto a los profesionales de seguridad se ratifica que las habilidades gerenciales, el liderazgo y la comunicación son piezas fundamentales de los nuevos líderes de seguridad, así lo manifiesta se ratifica en el reporte Fortinet (2019). 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. ISACA (2020) por su parte, resalta que las brechas más amplias que deben cerrar los profesionales son las “habilidades blandas”, con un 32%, seguido de sus habilidades técnicas con un 30%, que coincide con la realidad en Colombia. 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 (2020) donde resalta que el 50% de los CEO de su estudio global están preocupados por los temas relacionados con las ciberamenazas y el 33% de éstos lo ubica en top 5 de preocupaciones en la ejecución de la estrategia de seguridad. 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 éstos riesgos.

## Reflexiones finales

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 una invitación para desarrollar nuevos, continuos y creativos esfuerzos en procura de proteger y crear valor como la confianza, confiabilidad y resiliencia en un mercado cada vez más competitivo y exigente.

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.

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.

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 indica 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. 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.

2. La posición del profesional de seguridad continúa su proceso de afianzamiento dentro de las organizaciones. Hoy vemos que el responsable de seguridad ha evolucionado un poco más en su formación técnica, aunque aún debe ser fortalecida como lo ratifican los datos. No obstante, ha ido creando capacidades en otras dimensiones que se convierten en claves para el desem-

peño de su función. 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.

3. 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. La educación definitivamente juega un papel vital, y de igual manera junto con los entes de certificación se deben trabajar de manera conjunta para ir cerrando las brechas que no solo en Colombia, sino en el mundo se tienen con respecto a los talentos de seguridad que se requieren en los ambientes organizacionales.

4. La realidad digital hace que todos a todos los sectores e industrias lleven su mirada al tema de ciberseguridad. Sectores como el sector 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.

5. Los riesgos como instrumento catalizador de un programa de seguridad se convierten en Colombia en una buena herramienta, para desarrollar el programa de ciberseguridad. Los Líderes de seguridad digital están considerando este instrumento como una valiosa oportunidad para elevar su interlocución con los niveles directivos y ejecutivos, y juntos poder tomar caminos acordes a la realidad digital de la empresa.

6. La confianza digital, se convierte 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.

7. 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 lla-

mado tanto a 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.

8. 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 permeen 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.

9. Las nuevas tecnologías como Cloud, IoT, IA, *machine learning* entre 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.

10. 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.

11. 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. El 2020 está marcado por la construcción de nuevos normales, basado en los eventos globales que vive el mundo, y por tanto no la ciberseguridad, no será la excepción. En este ejercicio, será necesario repensar lo ya conocido y concebido como verdades definidas para reescribir nuevas prácticas, y así, apoyar a las empresas para caminar por la constante de la incertidumbre, que define las pautas de los movimientos del ecosistema digital en el que se desenvuelven las organizaciones hoy.

## Referencias


(ISC)2, (2019). (ISC)2 Cybersecurity Workforce Study, 2019. Recuperado de: https://cybersecurity.isaca.org/state-of-cybersecurity

Booz Allen Hamilton (2020). 2020 Cybersecurity Threat Trends Outlook. Recuperado de: https://content.fireeye.com/m-trends/rpt-m-trends-2020

CISCO (2020). Big Security in a Small Business World. Recuperado de: https://www.cisco.com/c/dam/en/us/products/collateral/security/2020-smb-cybersecurity-series-may-2020.pdf

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. Recuperado de: https://www.researchgate.net/publication/339629757_Estudio_de_la_evolucion_de_la_Seguridad_de_la_Informacion_en_Colombia_2000_-_2018

CISCOb (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

CISCOc (2019). Anticipating the Unknowns. Recuperado de: http://ebooks.cisco.com/story/anticipating-unknowns

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

ENISA (2020). Cybersecurity Skills Development In The EU. Recuperado de: https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union/at_download/fullReport

ESET (2019). Cybersecurity Trends 2020- Thechnology is getting smarter – Are We? . Recuperado de: https://www.welivesecurity.com/wp-content/uploads/2019/12/ESET_Cybersecurity_Trends_2020.pdf

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

Fireeye (2020). M-Trends 2020. Recuperado de: https://content.fireeye.com/m-trends/rpt-m-trends-2020

Fortinet (2019). The Ciso Ascends From Technologist To Strategic Business Enabler. Recuperado de:

https://hub.fortinet.com/hiring-guides/the-ciso-ascends-from-technologist-to-strategic-business-enabler

ISACA (2020). Global Update on Workforce Efforts and Resources. Recuperado de: https://cybersecurity.isaca.org/state-of-cybersecurity

Kaspersky (2019). What It Takes to Be a CISO: Success and Leadership in Corporate IT Security. Recuperado de: 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/wp-content/uploads/2020/02/Nominet_The-CISO-Stress-Report_2020_V10.pdf

Ponemon-IBM (2019). The Cyber Resilient Organization. Recuperado de: https://newsroom.ibm.com/2019-04-11-IBM-Study-More-Than-Half-of-Organizations-with-Cybersecurity-Incident-Response-Plans-Fail-to-Test-Them

PwC (2020). 23nd Annual Global CEO Survey. Recuperado de: https://www.pwc.com/gx/en/ceo-survey/2020/reports/pwc-23rd-global-ceo-survey.pdf

PwCb (2020). Being a Smarter risk taker through digital transformation. Recuperado de: https://www.pwc.com/us/en/services/risk-assurance/library/assets/pwc-2019-risk-study.pdf

Verizon (2020). Data Breach Investigation Report. Recuperado de: https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf

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

***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 Ingenieria de Sistemas | especialista en seguridad en redes y master 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.*

***Jeimy J. Cano M., Ph.D, CFE, CICA**. Ingeniero y Magíster en Ingeniería de Sistemas y Computación por la Universidad de los Andes. Especialista en Derecho Disciplinario por la Universidad Externado de Colombia. Ph.D en Business Administration por Newport University, CA. USA. y Ph.D en Educación por la Universidad Santo Tomás. Profesional certificado como Certified Fraud Examiner (CFE), por la Association of Certified Fraud Examiners y Certified Internal Control Auditor (CICA) por The Institute of Internal Controls. Profesor Distinguido de la Facultad de Derecho, Universidad de los Andes. Es director de la Revista Sistemas de la Asociación Colombiana de Ingenieros de Sistemas –ACIS–.*