XIX Encuesta Nacional de Seguridad Informática

DOI: 10.29236/sistemas.n151a3

Evolución del perfil del profesional de seguridad digital.

Resumen
La encuesta nacional 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 febrero y abril de 2019, contó con la participación de 299 encuestados, quienes con sus respuestas revelan tendencias particulares para Colombia en los temas de seguridad y control. Este ejercicio fue motivado a través de diferentes redes sociales, comunidades y grupos, y contó con la cooperación de otras asociaciones como ISACA, Capítulo Bogotá, TacticalEdge, y CISOS.CLUB. Los resultados de este estudio muestran un panorama de las organizaciones colombianas, en sus distintos sectores productivos, frente a la seguridad de la información y/o ciberseguridad y su evolución en las diferentes dimensiones incluidas en 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 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.

Con esto en mente y considerando otros estudios internacionales como el realizado por PwC, IBM, Ponemon, Deloitte, EY, CISCO, Verizon, Foro Económico Mundial, Champlain College Online (CCO), Fortinet, IDC y Kaspersky se procederá a analizar los resultados de la Encuesta Nacional de Seguridad Informática ACIS 2019.

Dentro de los estudios referentes consultados y analizados, se encuentran el Global State of Information Security realizado por la firma Pricewaterhousecoopers (PwC, 2018), el Global Information Security Survey 2018-19 consolidado por la empresa Ernst &Young (EY, 2018), el Informe Anual de Seguridad de la compañía Cisco (CISCO, 2019), los resultados del documento State of Cybersecurity Implications elaborado por ISACA (ISACA, 2019), el reporte Measuring & Managing the Cyber Risks to Business Operations (Tenable-Ponemon, 2019), el informe anual denominado Data Breach Investigation Report (Verizon, 2019), el reporte llamado The Cyber Resilient Organization, generado por la empresa Ponemon en asocio con IBM (Ponemon, IBM, 2019), el informe de Deloitte The Future of Cyber Sphere (Deloitte, 2019), The Global Risk Report (WEF, 2019), el reporte Anticipating the Unknowns (CISCOb, 2019), el reporte The State of the Cybersecurity Workforce and Higher Education (CCO, 2018), el reporte Out of the Shadow: CISO is in the spotlight! (PwC Luxemburgo, 2018), el reporte The Ciso Ascends From Technologist To Strategic Business Enabler (Fortinet, 2019), The Modern Connected CISO

(IDC, 2019), el reporte What It Takes to Be a CISO: Success and Leadership in Corporate IT Security (Kaspersky, 2019) y el reporte 22nd Annual Global CEO Survey (PwCb, 2019).

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 permite a las organizaciones definir una postura clara en materia de protección.

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

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

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

Hallazgos principales

De la información recogida en este estudio se muestran en la gráfica 1 los aspectos clasificados como importantes por todos los encuestados y reunidos en un grupo denominado top de Hallazgos de las dimensiones de la encuesta.

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%

Gráfica 1: Top de Hallazgos

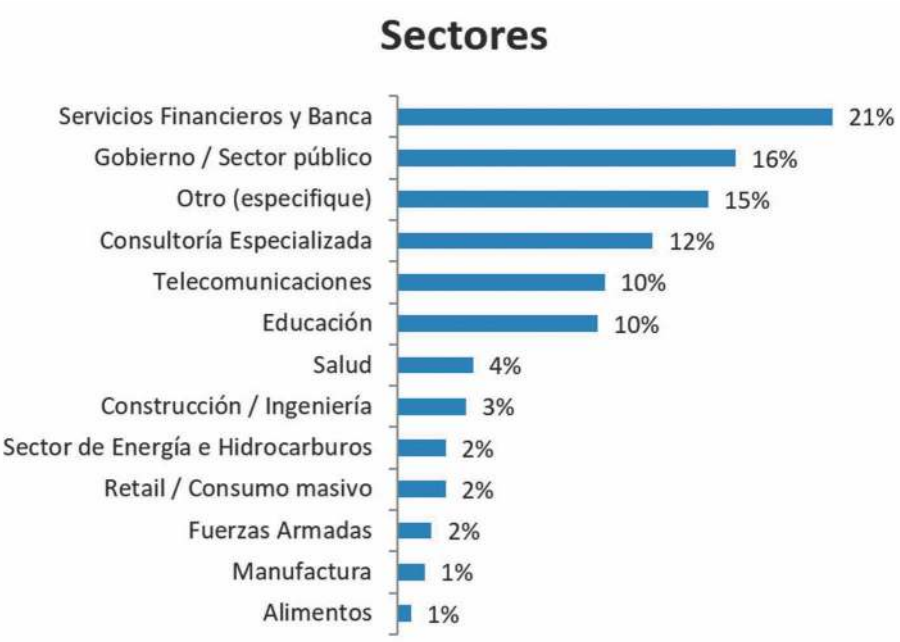
cuenta con un presupuesto para la seguridad de la información en las empresas de la realidad de Colombia. Un 70% indica que la tarea fundamental del responsable de seguridad en Colombia es definir los controles de TI en materia de seguridad de la información. El 70% de los encuestados respondió que en sus empresas se realizan los ejercicios de evaluaciones de riesgos en los que se incluye 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 injerencia están compuestos por el sector financiero, servicios de consultoría especializada y el Gobierno.

La Gráfica 3 muestra el tamaño de las empresas en Colombia, de acuerdo con el número de empleados. El 25% de las empresas está entre los 1001 a 5000 empleados,

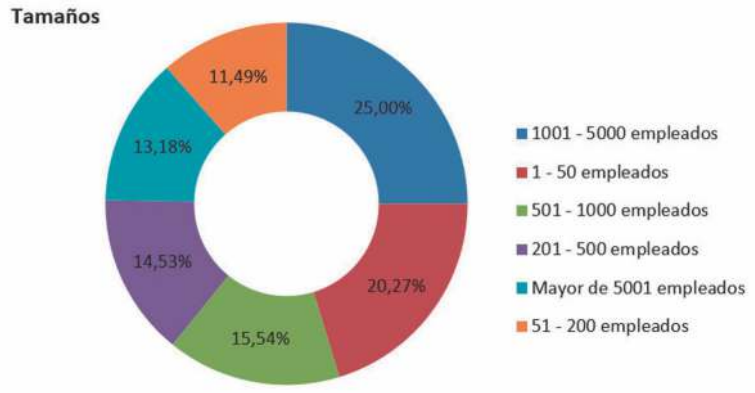


Gráfica 2: Sectores participantes

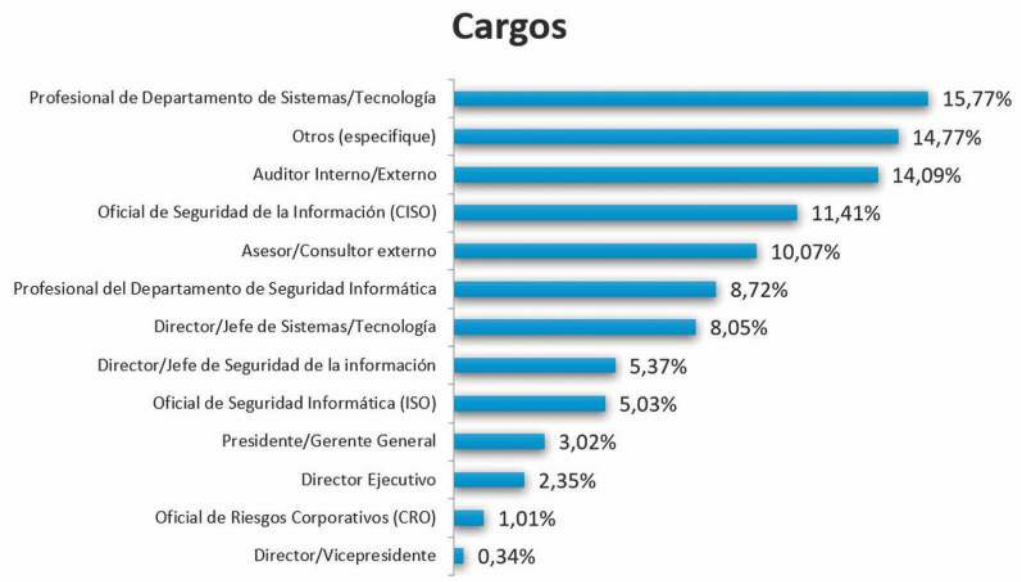
el segundo lugar son las empresas pequeñas (20,27%) que cuentan con 1 a 5 empleados.

La Gráfica 4 muestra los cargos de los encuestados, entre los que se cuentan profesionales de las áreas de TI, auditores internos, oficiales de seguridad, consultores, entre otros. 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.

En la Gráfica 5 se observan las tareas realizadas por los profesionales de seguridad dentro de las orga-



Gráfica 3: Tamaño de las empresas



Gráfica 4: Cargos de los Encuestados

Gráfica 5: Funciones del responsable de seguridad

Gráfica 6: Dependencia del área de Seguridad

nizaciones. El porcentaje más alto está representado en definición de controles de TI en materia de seguridad de la información, velar por la protección de la información empresarial 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

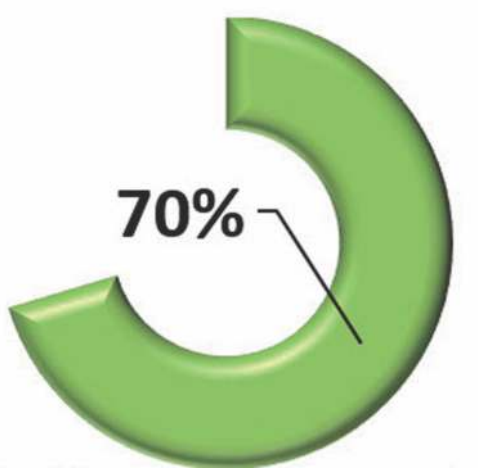
Según el Data Breach Report (2019) de la Firma Verizon, la mayor cantidad de brechas identificadas involucra a negocios pequeños o medianos (43%). Basado en la participación de las empresas que participaron, más del 60% corresponde al rango de pequeñas, medianas empresas y se infiere que, existen altas probabilidades de que las empresas colombianas puedan ser víctimas de un ataque informático. De acuerdo con (CISCOb, 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, poner límites a

Gráfica 7: Roles de Seguridad

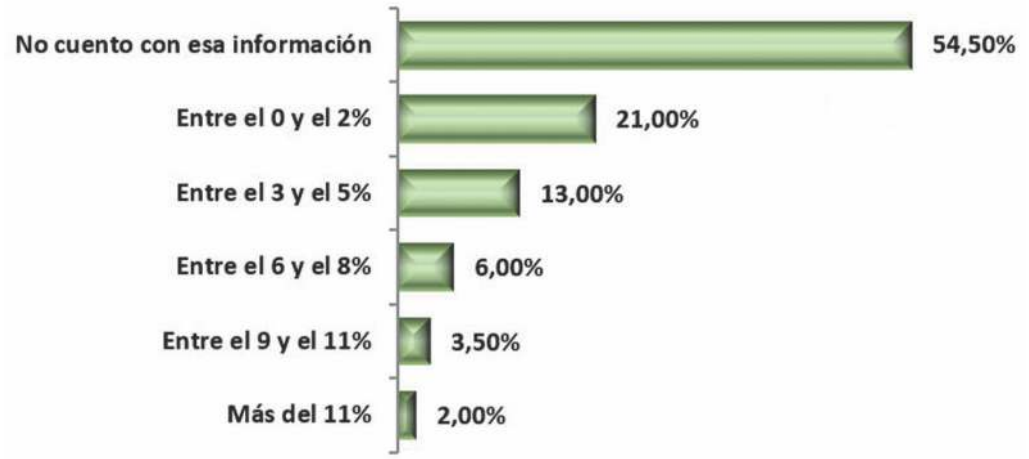
los temas de presupuestos, colaboración con las áreas de la organización, educar y crear cultura, saber cómo se presentan los beneficios de las inversiones en seguridad y ser estratégico en la venta de la implementación de soluciones técnicas de seguridad. En otro informe (Kaspersky, 2019), se resalta que la identificación de riesgos y amenazas son tareas claves de los profesionales de seguridad. Al revisar la tendencia nacional dista completamente. La función principal está relacionada con la implementación de soluciones de TI, basado en 2019.

Presupuestos

En materia de presupuestos, la realidad colombiana es muy interesante en el mundo de la seguridad digital. El 70% de los participantes manifiesta que sí tiene presupuesto asignado a la seguridad digital de sus organizaciones, lo cual se refleja en la Gráfica 8. La Gráfica 9 muestra el monto del presupuesto en relación con el presupuesto global; cerca del 46% 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. Cerca del 47% tiene un

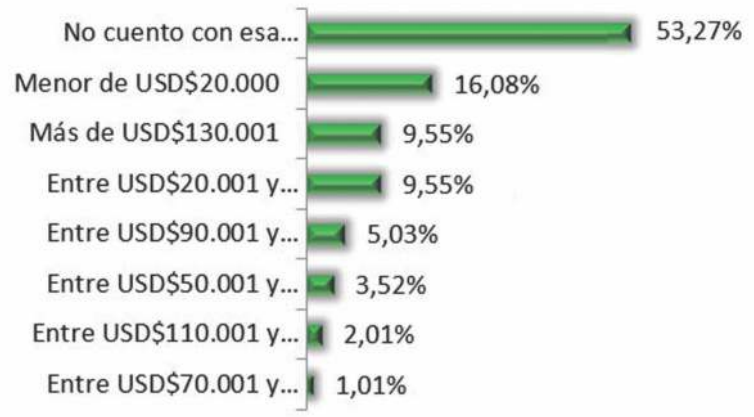


Gráfica 8: Presupuesto de Seguridad

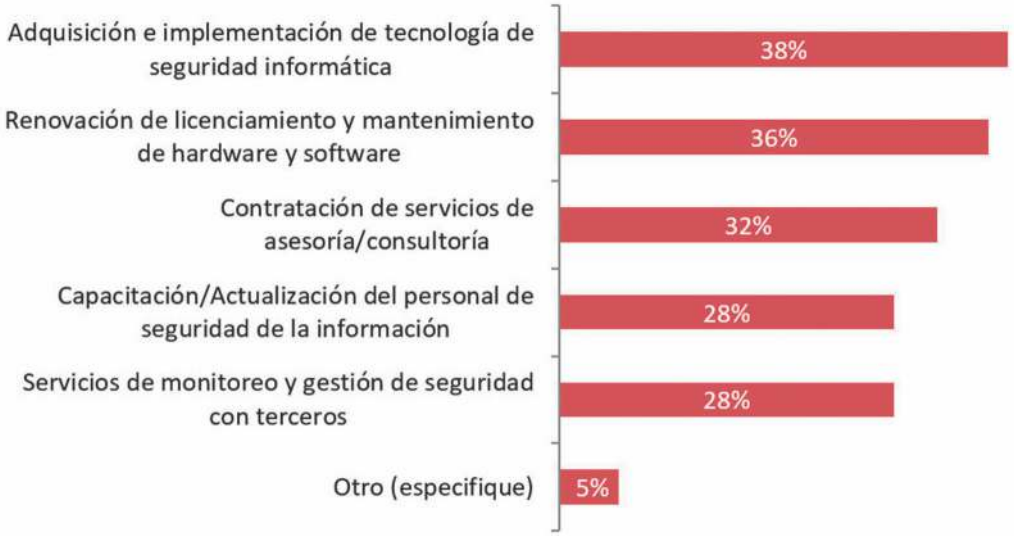


Gráfica 9: Porcentaje del presupuesto Global

monto asignado para la seguridad, el 53% restante manifiesta no conocer dicha información. Esto se puede explicar, toda vez que los cargos de mayor participación están compuestos por auditores y los profesionales de las áreas de tecnologías que pueden no conocer los detalles internos de las áreas de seguridad. La otra gran razón para que se de esta realidad es que muchos de los roles de las organizaciones están asociados con los analistas de seguridad, quienes pueden no conocer estos detalles. La Gráfica 11 muestra cómo se están realizando las inversiones en materia de seguridad. La inversión en tecnologías de seguridad es la parte más importante, seguida de la renovación del licenciamiento de algunas tecnologías en materia de seguridad digital; los servicios de consultoría y asesoría ocupan el tercer lugar; la tercerización de servicios, en materia de seguridad, están en cuarto lugar, y la capacitación y actualización de los profesio-



Gráfica 10: Presupuesto de Seguridad



Gráfica 11: Inversión de Seguridad

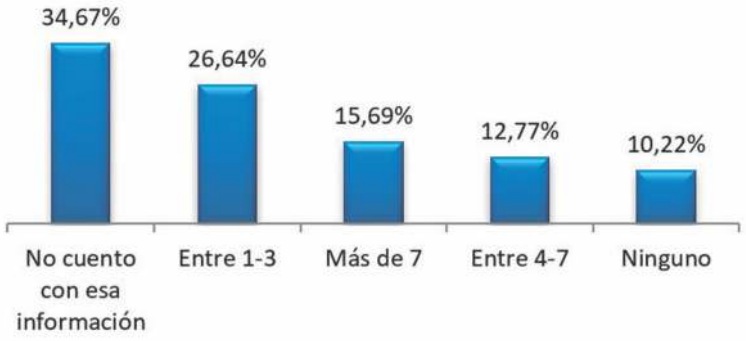
nales de seguridad es el último criterio sobre los presupuestos. La Gráfica 12 representa cuánto dinero se invierte en los criterios identificados. La franja de menos de $US20.000 dólares en Colombia es la que tiene los mayores valores. Sin embargo, la franja de más de $US130.000 dólares es la siguiente, específicamente los servicios gestionados y las relaciones con terceras partes.

Consideraciones de los datos

Los reportes internacionales ratifican la tendencia en Colombia de aumentos pequeños en los presupuestos de seguridad en las organizaciones de todos los tamaños y sectores. No obstante, al revisar el informe (Ponemon, IBM, 2019), se ven grandes diferencias en los valores asignables de presupuestos, según los datos del informe las franjas de los presupuestos están

	Entre US D$110.001 y USD$130.000	Entre US D$20.001 y USD$50.000	Entre US D$50.001 y USD$70.000	Entre US D$70.001 y USD$90.000	Entre US D$90.001 y USD$110.000	Más de USD$130.001	Menor de USD$2
Adquisición e implementación de tecnología de seguridad informática	6%	20%	4%	4%	7%	26%	33%
Capacitación/Actualización del personal de seguridad de la información	4%	22%	9%	2%	7%	22%	33%
Contratación de servicios de asesoría/consultoría	8%	20%	4%	2%	14%	28%	24%
Renovación de licenciamiento y mantenimiento de hardw are y softw are	5%	15%	11%	4%	9%	25%	31%
Servicios de monitoreo y gestión de seguridad con terceros	3%	8%	8%	5%	14%	32%	30%

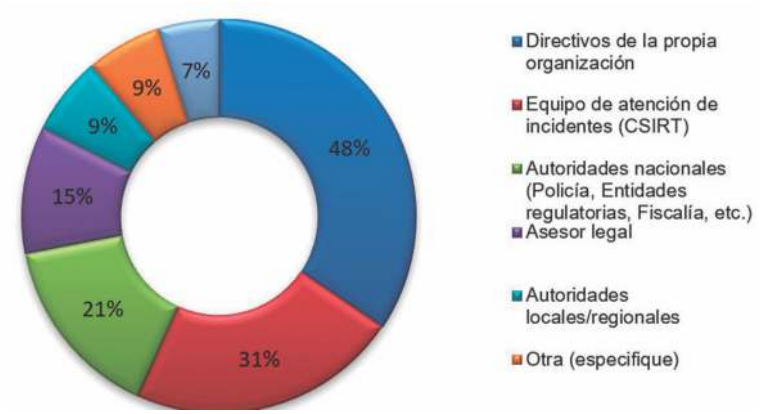
Gráfica 12: Montos en dólares de las inversiones de seguridad. Sectores vs. inversiones



Gráfica 13: Cantidad de Incidentes. Incidentes

entre los $US6 a $US10 millones de dólares como el mejor valor relacionado con el presupuesto sólo asignado a la ciberseguridad. Si bien influyen las realidades económicas y digitales en donde se reali-

Gráfica 14: Tipos de Incidentes de Seguridad



Gráfica 15: A quien se reportan los incidentes

zan los estudios, lo que sí vale resaltar son las tendencias de tener unos presupuestos más dotados para el mundo de la ciberseguridad. En el caso colombiano 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

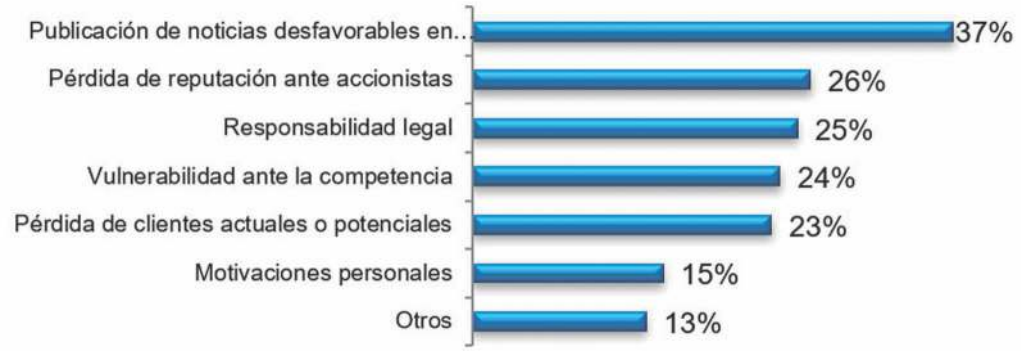
En Colombia se mantiene la tendencia en materia de incidentes de seguridad en concordancia con las tendencias internacionales. Tales desafíos, en términos de preparación y atención, son una exigencia para las organizaciones.

La Gráfica 13 muestra la cantidad de incidentes que se presentan en Colombia, según los participantes. El 56% de ellos manifiesta haber tenido, por lo menos, un incidente de seguridad o ciberseguridad en sus organizaciones. El 35% de los participantes no tiene información al respecto, el 10% de los participantes resalta que no tuvieron un incidente de seguridad.

La Gráfica 14 relaciona los tipos de incidentes que se presentaron en las organizaciones. En ella se relacionan los errores humanos, el *phishing*, la instalación de *software* malicioso y la ingeniería social como los de mayor incidencia.

La Gráfica 15 muestra a quién se reportan los incidentes de seguridad. Los datos reflejan que, ante un incidente y su identificación, el 48% de los participantes lo notifica a la propia organización en cabeza de sus directivos; 31% a los equipos de atención de incidentes CSIRT y 21% a las autoridades de orden nacional como los datos más relevantes.

La Gráfica 16 las razones por las que no se denuncian los incidentes. Se destacan fundamentalmente la imagen 37%, la reputación 26%, y la responsabilidad legal 25%, como las razones que aducen los en-



Gráfica 16: Razones para no denunciar los incidentes

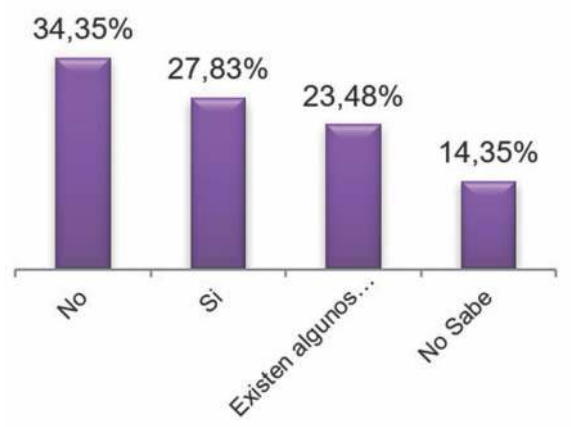
Gráfica 17 Mecanismos para denunciar/compartir

cuestados sobre el porqué no se denuncian los incidentes. La Gráfica 17 muestra la forma los mecanismos que se podrían utilizar para compartir información o denunciar información. En primer lugar, usar canales privados y cifrados como el mecanismo más idóneo, 56%.

La evidencia digital y su uso dentro del proceso de gestión de incidentes es pieza fundamental para un adecuado mejoramiento. La Gráfica 18, resalta la importancia y consciencia en relación con el adecuado manejo de la evidencia digital. El 74% resalta que es consciente de

Gráfica 18: Consciencia de la Evidencia Digital

ello. Sin embargo, la Gráfica 19 muestra que el 34% no posee un



Gráfica 19: Procedimiento de Gestión de Evidencia Digital

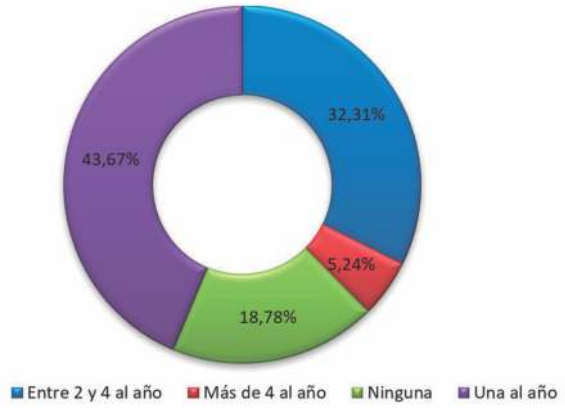
Gráfica 20: Contactos con autoridades locales/regionales

procedimiento para hacer la gestión de la evidencia digital. La Gráfica 20 resalta que el 62% mantiene algún tipo de contacto con autoridades del orden local o regional. La Gráfica 21 señala que el 74% de los participantes no posee una estrategia para el descubrimiento electrónico, que les permita soportar litigios o reclamaciones legales.

Consideraciones de los datos

Los reportes internacionales como (Tenable-Ponemon, 2019) y (CISCO, 2019), indican que los incidentes que interrumpen los procesos (54%) son la preocupación más grande para las empresas. Esto ratifica lo encontrado para la realidad de Colombia, sobre los incidentes en Colombia como *Malware, Phishing* y Acceso no autorizado, los cuales son incidentes que van en la misma línea de interrumpir las operaciones de las empresas. De igual manera, la presencia de los incidentes en Colombia se puede ratificar con el informe (Ponemon, IBM,

Gráfica 21: e-discovery



Gráfica 22: Evaluaciones de Seguridad

2019) según el cual cerca del 79% de las compañías tienen más de un incidente de seguridad. El mismo informe resalta la importancia de intercambiar y compartir la información, 58%; dicho estudio resalta que se han visto beneficiados con compartir información, toda vez que sus procesos de aprendizaje y contención frente a los incidentes de seguridad han mejorado. En Colombia aún no se piensa del todo en ello y por tanto se evidencia lejanía de esta práctica. La práctica de la gestión de incidentes que en Colombia según los datos se resalta como una práctica no desarrollada, se ratifica a través del informe (EY, 2018) el cual describe que las inversiones en seguridad están orientadas a fortalecer la gestión de incidentes, toda vez que se considera una práctica con muy poca madurez en las organizaciones, cerca del 10% de los participantes hace esta consideración. El informe (Deloitte, 2019), resalta que los impactos mayores a la hora de un incidente se expresan en términos de pérdidas 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 al no denunciar los incidentes, toda vez que la pérdida de la reputación, confianza, sanciones y/o multas son las razones que se aducen para no hacerlos.

Herramientas

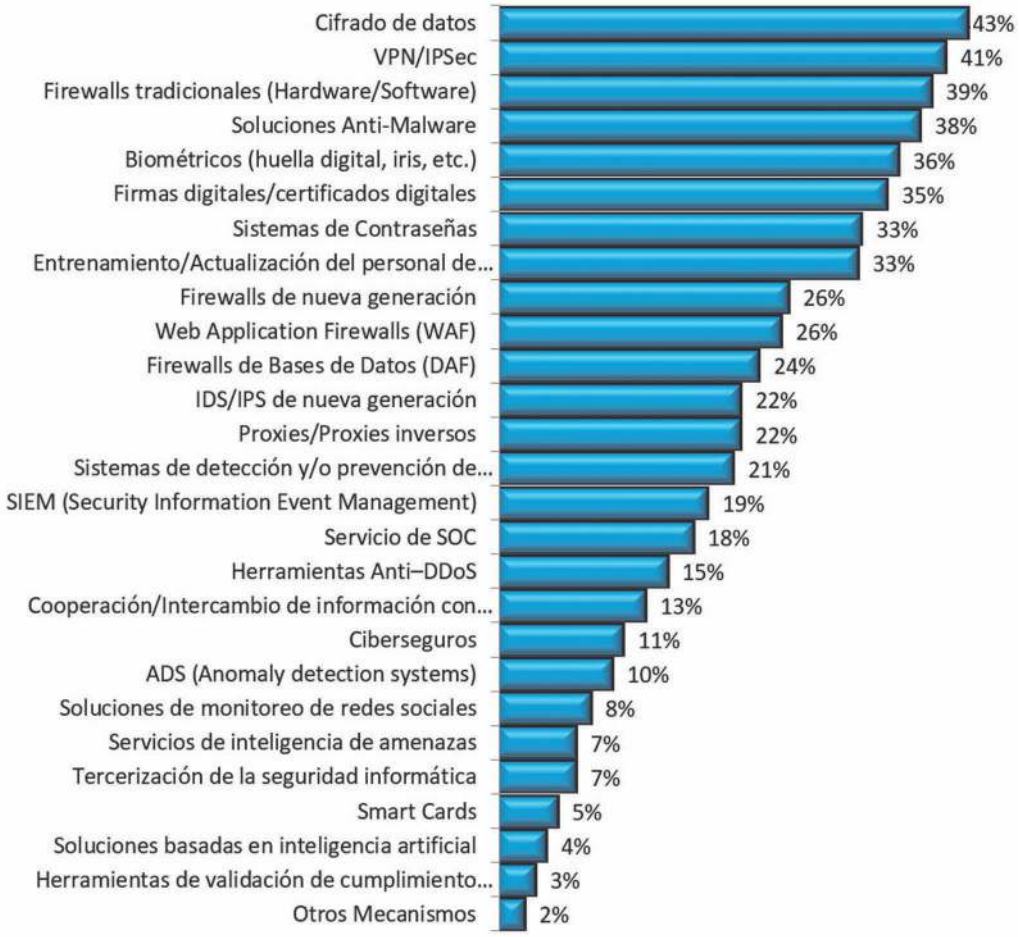
La Gráfica 22 muestra el uso de las evaluaciones de seguridad como una de las prácticas más usadas. Un 82% de los participantes manifiesta hacer uso de esta práctica como instrumento clave para validar el estado de la seguridad digital de la organización. El 44% de los participantes usa esta práctica una vez al mes; el 32% entre dos y 4 veces al año; el 19% usa más de 4 veces al año y el 5% dice no usarla.

La Gráfica 23 indica cuáles son los mecanismos de seguridad comúnmente usados en las organizaciones. El cifrado de datos 43%, VPNs 41% y Firewalls tradicionales 39% son los tres mecanismos más usados basados en las respuestas de los participantes.

La gráfica 24, enfatiza en las herramientas que más se usan para notificarse de las fallas de seguridad los profesionales. El 44% usa la lectura de sitios especializados, como la práctica más común.

Consideraciones de los datos

La tendencia en Colombia se mantiene comparada con los años anteriores. Así mismo lo ratifican los datos internacionales, el informe de (Deloitte, 2019) muestra que las organizaciones interactúan con sus unidades de negocios a través de las evaluaciones de seguridad o auditorías, en un 29% El informe de (Tenable-Ponemon, 2019) señala que la frecuencia de realizar las evaluaciones de seguridad muestra la madurez y la madurez tiende a mostrar priorización para realizar



Gráfica 23: Mecanismos de Seguridad

estos ejercicios. Así las cosas, en Colombia los datos muestran una evolución significativa de esta práctica y basado en ello es posible afirmar que hay una tendencia a la madurez de la misma.

Políticas

La Gráfica 25 refleja el estado de las políticas de seguridad en las organizaciones colombianas; el 61% de los encuestados manifiesta tener formalizada sus políticas de se-

Gráfica 24: Mecanismos de notificación

Gráfica 25: Estado de las Políticas

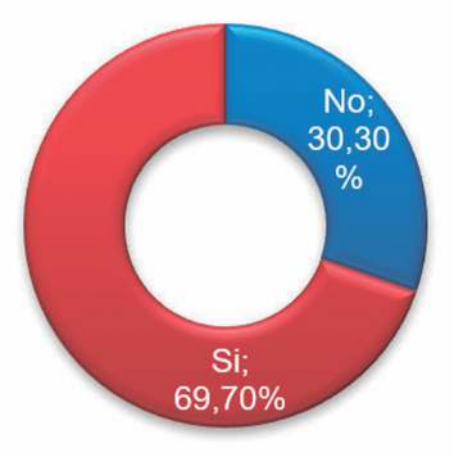
guridad, el 28% actualmente en desarrollo y, sólo el 11%, dice no tener políticas de seguridad de la información.

La Gráfica 26, muestra lo que manifiestan los participantes al indagar por los obstáculos por los cuales no hay una postura adecuada de seguridad en sus empresas.

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 clave. En la Gráfica 27, el 69% de los participantes hace una evaluación de riesgos de seguridad digital y la incluyen en sus ejercicios globales de gestión de riesgos. En la Gráfica 28, el 69% realiza ejercicios de evaluación de riesgos una vez al año, el 22% dos al año y el 9% más de dos al año.

La gráfica 29, muestra las razones de por qué no es realizada la ges-

Gráfica 26: Obstáculos de la Seguridad



Gráfica 27: Gestión de Riesgos de Seguridad

tión de riesgos. El primer motivo que señalan los participantes está relacionado con no disponer de un proceso formal de gestión de riesgos (35%).

La Gráfica 30 muestra el tipo de metodologías usadas al realizar los ejercicios de gestión de riesgos de seguridad; la ISO 31000, con un 27%, es la metodología más usada. La Gráfica 31, indica que los incidentes de seguridad son asociados a algún tipo de riesgos. El 55% de los incidentes se asocia como cate-

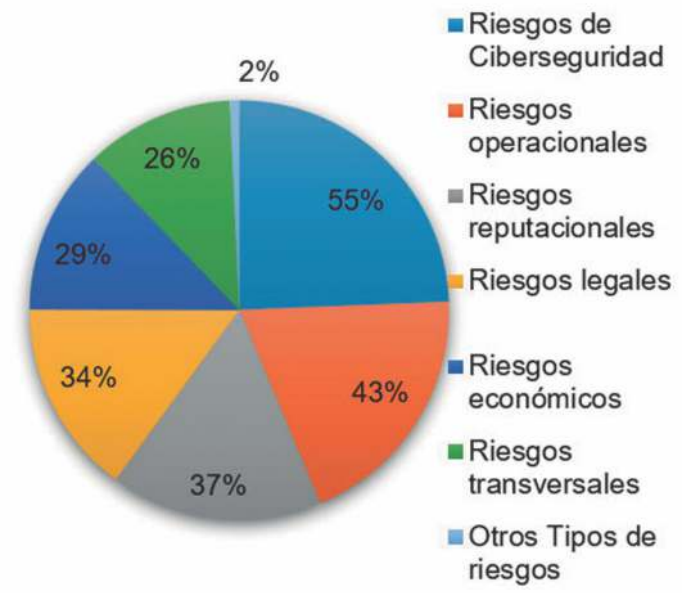
Gráfica 28: Cantidad de Gestión de Riesgos en Seguridad

Gráfica 29: Razones para no realizar la gestión de riesgos

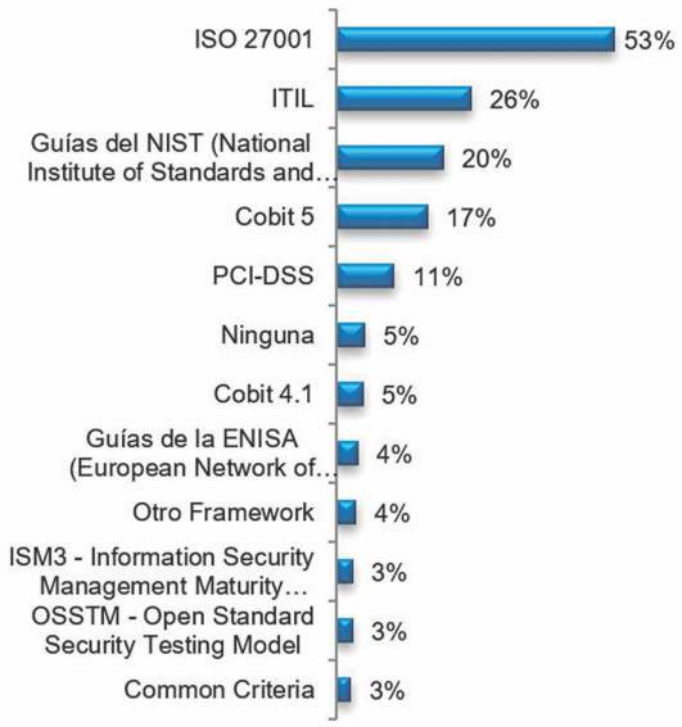
Gráfica 30: Tipos de Metodología

goría en los procesos de identificación de riesgos, a los riesgos de ciberseguridad; el 43% lo asocia a riesgos de operación, el 37% los relaciona con riesgos reputacionales.

La Gráfica 32 ilustra el uso de los distintos marcos de trabajo (*frameworks*) usados en las organizaciones colombianas: ISO/IEC 2700, ITIL, NIST y Cobit 5 son los más usados. La Gráfica 33 refleja las regulaciones a las que las organizaciones están sometidas; en el caso colombiano, el 66% de los participantes manifiesta que sí existen re-



Gráfica 31: Tipos de Riesgos



Gráfica 32: Marcos de trabajo usados

gulaciones a las que sus organizaciones se ven sometidas. La tendencia internacional se orienta a que, cada vez más, existirán regulaciones más globales. La regulación GDPR (General Data Protection Regulation) nace como una necesidad de la Comunidad Europea

Gráfica 33: Regulaciones o normativas

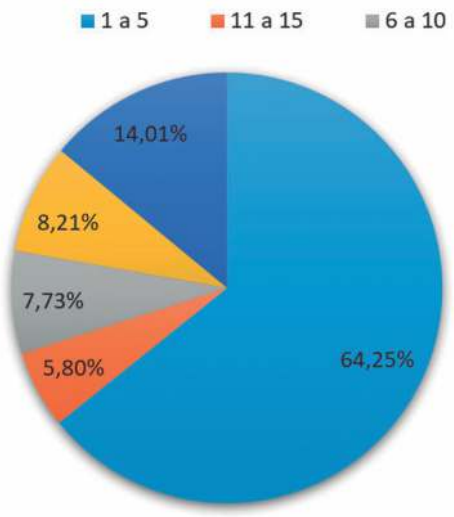
(EU), de gran impacto a nivel global.

Consideraciones de los datos

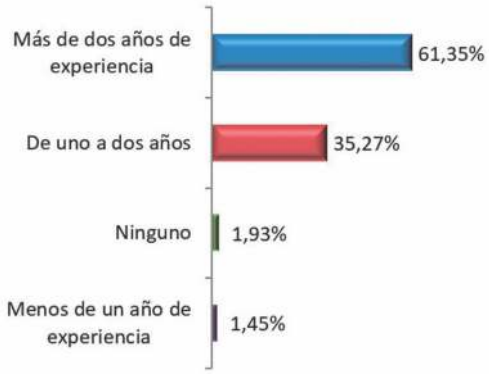
En definitiva, los riesgos de seguridad de la información y ciberseguridad son una realidad como lo ratifica el informe del Foro Económico Mundial (WEF, 2019), el cual manifiesta que la prioridad de estos tipos de ataques es alta en las organizaciones del mundo. Esto ratifica la tendencia de los resultados 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, así se ve ratificado en el informe de (PwC, 2018), en el que el 39% está muy confiado en sus capacidades de gestionar ciberataques basados en la práctica de gestionar los riesgos. Así mismo, el informe de (Deloitte, 2019) indica que el 50% de los participantes usan metodologías de riesgos y la cuantificación de los mismos 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 de Colombia apunta a tener un modelo fortalecido en relación con las políticas, ratificado con el informe de (CISCO, 2019), el cual señala que más del 85% conoce muy bien las políticas y su efecto dentro de las organizaciones.

Capital intelectual

La Gráfica 34 muestra el grupo de organizaciones que cuenta con un recurso dedicado a la seguridad; en ellas, cerca del (86%) manifiesta tener recursos dedicados a la seguridad. La Gráfica 35 muestra que el tiempo de experiencia promedio para que los profesionales de seguridad sean contratados en Colombia es superior a dos (2) años (62%).

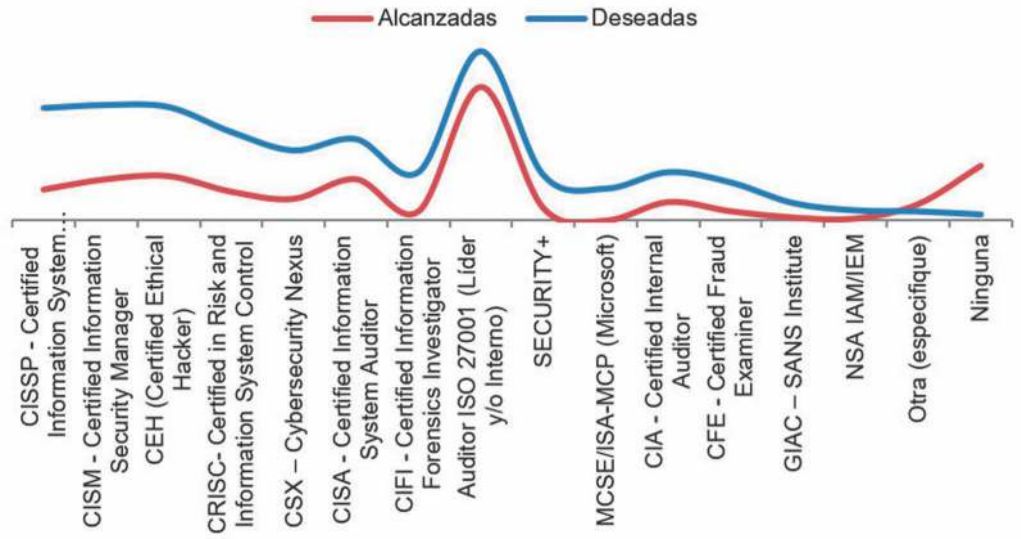


Gráfica 34: Recursos dedicados a la Seguridad



Gráfica 35: Experiencia del profesional

La Gráfica 36, representa la comparación de las certificaciones que



Gráfica 36: Certificaciones alcanzadas vs deseadas

los profesionales de seguridad poseen en la actualidad y que desean alcanzar en el tiempo. CISSP, CISM, CEH, CRISC son las certificaciones que mayor variación tienen de lo poseído actualmente y lo deseado en el futuro no muy lejano.

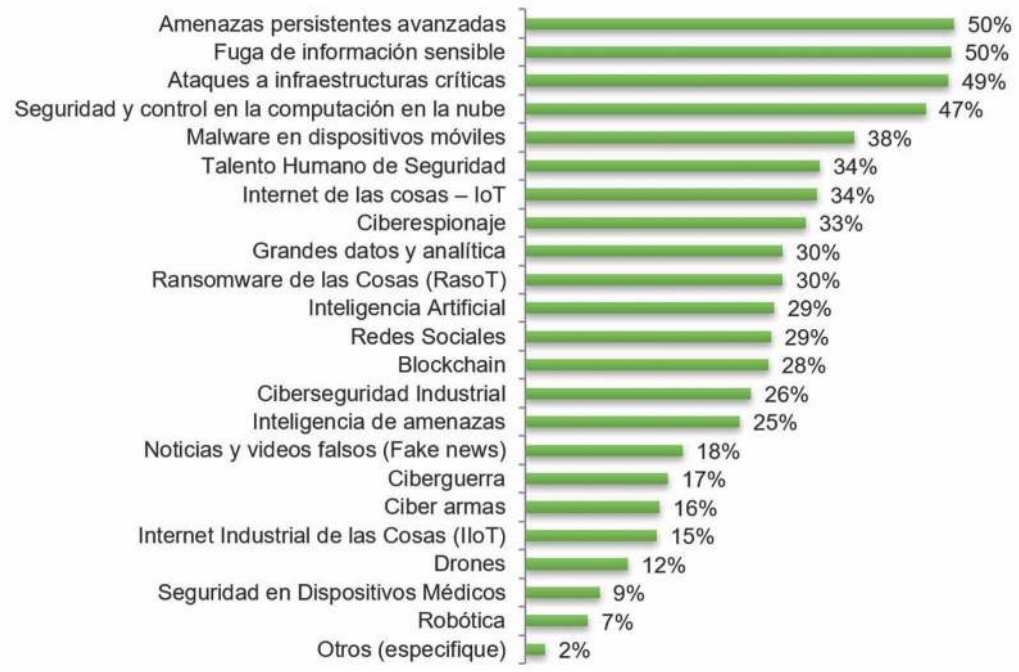
La Gráfica 37, indaga sobre la forma en que la educación ha participado en la formación de los profesionales de seguridad. El 31% manifiesta que los niveles de investigación son escasos; el 28% manifiesta que existen limitados labora-

Gráfica 37: Papel de la educación

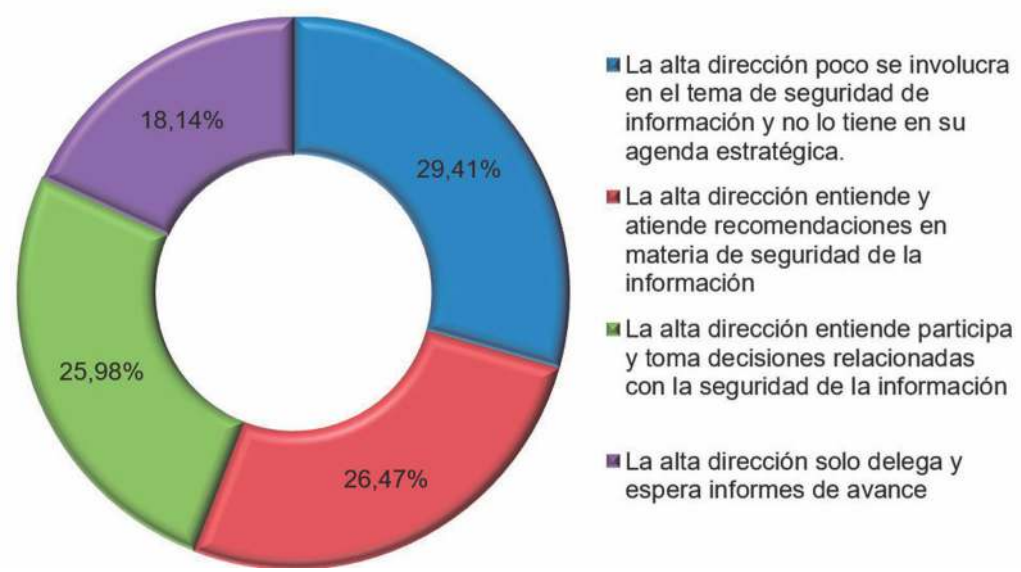
torios e infraestructuras para soportar los cursos especializadas 28%.

Consideraciones de los datos

La experiencia del profesional de seguridad de las organizaciones en Colombia es clave, así como su formación. Las tendencias internacionales ratifican los resultados de Colombia. En su informe (Kaspersky, 2019), lo resalta diciendo que muchos de los perfiles de seguridad (CISO), fundamentalmente, tienen más de 5 años de experiencia en el cargo (52) %; sólo un 12% tiene entre uno y dos años de experiencia en el cargo. Desde el punto de vista académico, el mismo informe señala que el (68%) de los CISOs tienen una maestría. En cuanto a las certificaciones se observa que sólo el 46% de la población estudiada posee una certificación. No obstante, el informe (Kaspersky, 2019) ratifica la tendencia de Colombia en términos de certificaciones, con ISO 27001, CISSP, CISM como las certificaciones más apetecidas por los profesionales de seguridad a nivel global; hecho confirmado en el informe (PwC Luxemburgo, 2018). Por el lado de la educación superior, el informe (CCO, 2019) resalta que 72% de las personas en este estudio seguiría una carrera en ciberseguridad, si ésta fuera financiada por su empleador. El mismo 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



Gráfica 38: Desafíos del 2019

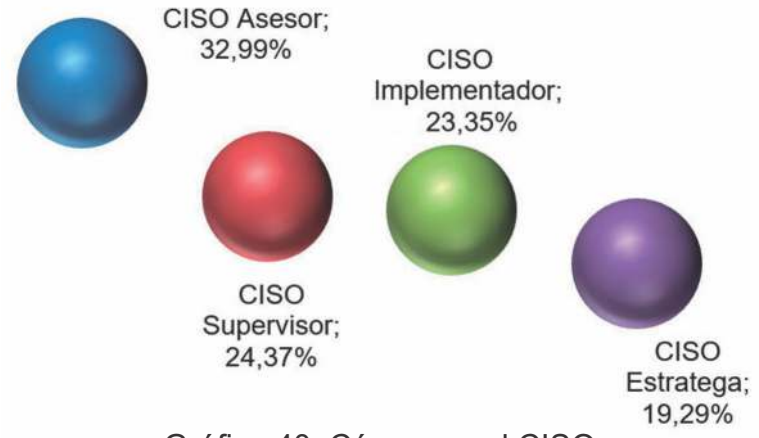


Gráfica 39: Involucramiento de los Directivos

concluye que el sector de la educación juega un papel fundamental en ambos sentidos; el 91% considera que se pueden crear más programas de formación, así como ayudar a desarrollar mejores capacidades para desempeñar los diferentes cargos de la ciberseguridad (90%). Al revisar los datos nacionales se ratifica el potencial de la universidad en la formación de capacidades acordes con los roles; sin embargo, no se observa que en Colombia exista esta potencial formación de los profesionales de seguridad.

Temas emergentes

La Gráfica 38 muestra los temas relevantes y emergentes que tienen en la mira los profesionales de seguridad. El más relevante, las amenazas persistentes avanzadas, fuga de información sensible, los ata-



Gráfica 40: Cómo ven al CISO

Gráfica 41: Entrega de información del profesional de seguridad

ques de infraestructuras críticas y la seguridad de la computación en la nube son los de más alto valor.

La gráfica 39, relaciona la forma en cómo las juntas directivas, o comités ejecutivos se relacionan con la seguridad. El 57% están atendiendo y participando activamente, mientras que el 47% restante delega o poco se involucra en los temas de seguridad en Colombia.

Las Gráficas 40, 41 y 42 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 este año, el 33% resalta que en Colombia es visto como un asesor, luego como supervisor, implementador y en último lugar como estratega.

La Gráfica 41 muestra la forma como el líder de seguridad se comunica con la organización y se observa que la información comunicada hoy por parte del líder de seguridad está relacionada con la gestión de la seguridad para la toma de decisiones (31%), seguido de la información relacionada con las brechas de seguridad (29%) y, en tercer lugar, la información relacionada con los riesgos (29%).

La Gráfica 42 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 habilidades técnicas y/o experiencia en lo que puede enfocarse el líder de seguridad por mejorar (41%), seguido de las habilidades gerenciales (37%) y, en tercer lugar, la formación académica y técnica (32%).

Consideraciones de los datos

Los diferentes informes como (EY, 2018), (CISCO, 2019), (CISCOb,

2019), (Deloitte, 2019), e (IDC, 2019), ratifican las observaciones de los datos de Colombia en relación con los temas más relevantes del presente y futuro cercano, observados por los responsables de seguridad digital del país. La nube es la tendencia en todos los informes y confirma lo que sucede en Colombia; la movilidad y sus ataques, aunque no está en el top de preocupaciones, sí está en la agenda; los ataques complejos como APT (Amenazas Persistentes Avanzadas) y los ataques a infraestructuras críticas son otros de los elementos que dichos informes muestran como temas claves para ser observados por los profesionales de seguridad. En cuanto a los mismos se ratifica que las habilidades gerenciales, el liderazgo y la comunicación son piezas fundamentales de los nuevos líderes de seguridad, así lo manifiesta el reporte (Fortinet, 2019). En consecuencia, se ratifica lo observado para la realidad colombiana. En Colombia se ve al CISO como un asesor y supervisor de la seguridad; al contrastar los informes internacionales como (IDC, 2019), (Kaspersky, 2019), (PwC Luxemburgo, 2018), los cuatro informes confirman que el CISO es visto como un elemento que cada vez más tiene una visión de negocios; sin embargo (PwC Luxemburgo, 2018) y (IDC, 2019), resalta que el líder de seguridad debe trabajar bastante en su imagen conocida como el "doctor No". En Colombia, la posición del CISO ha evolucionado y se confirma su ascenso en la organización, pasando de labores técnicas a labores de nivel ejecutivo; di-

Gráfica 42: Camino de crecimiento de un profesional de seguridad

cha tendencia se confirma con el informe (PwC Luxemburgo, 2018) en el que se observa que el 34% de los participantes ven al líder de seguridad en un nivel 2 dentro de las estructuras organizacionales. No obstante, como indica el mismo informe y confirmando la tendencia de Colombia, es necesario que se trabaje en fortalecer muchas de sus capacidades. Las altas direcciones tienen en sus mentes las amenazas digitales, así lo muestran los datos en Colombia y de la misma manera lo resaltan las tendencias internacionales (PwCb, 2019), las cuales indican que el 40% de los CEO de las compañías observadas, tienen en el top de sus agendas estos temas y le dan la importancia necesaria.

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. Esta realidad crea nuevos y desafiantes escenarios que se transforman en riesgos para las organizaciones; sin embargo, invitan a desarrollar nuevos, continuos y creativos esfuerzos en procura de proteger y crear valor como la confianza y confiabilidad, permitiendo lograr posturas digitales más confiables en un mercado 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 necesarios los pensamientos amplios que involucren a los actores y los lleven a pensar en un replanteamiento de la protección de la información, sin perder de vista lo ya alcanzado, para enfrentar 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; pero, sobre todo, se trata de espacios que exigen anticiparse a observar los entornos cambiantes y superpuestos, en procura de la protección de la información.

En la realidad colombiana, los datos muestran que los esfuerzos se vienen haciendo, que año tras año las demandas de la realidad digitalmente modificada transforman la visión de la seguridad. El contexto internacional indica la misma tendencia.

En la realidad nacional se pueden concluir los siguientes aspectos:

1. La realidad digital hace que a todos los sectores e industrias les importe el tema de ciberseguridad. A 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. Sin embargo, sectores como el de la salud y retail vienen observando y dando pasos pequeños en procura de atender la realidad en materia de confianza digital.

2. 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.

3. La posición del profesional de seguridad continúa su proceso de afianzamiento dentro de las organizaciones, en una realidad digitalmente modificada. Hoy vemos que el responsable de seguridad ha evolucionado un poco más de su *back* técnico que aún debe ser fortalecido como lo ratifican los datos; ha ido creando capacidades en otras dimensiones que se convierten en claves para el desempeño 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 haceres. 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.

4. A nivel nacional, se mantiene la sólida tendencia de usar mecanismos tecnológicos como las principales herramientas de protección; si bien las tendencias internacionales ya dan esto por sentado, sí se debe hacer un llamado tanto a los responsables de seguridad como a las organizaciones, para que vean la seguridad como un tema un poco más amplio. Las tendencias internacionales precisamente ratifican que es necesario extender la visión de la seguridad como una fuente de aporte al valor de la organización y de los objetivos de su negocio.

5. 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 unos programas de seguridad que permeen todos los niveles organizacionales, sobre prácticas centradas en los diferentes grupos de interés, dirigidas a construir posturas de seguridad diferentes, basadas en los desafíos que debe asumir el talento humano.

6. 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. En ambientes internacionales es limitado el uso de la nube, producto del desconocimiento y los riesgos que ésta implica.

7. 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.

En resumen, el panorama general de la seguridad en Colombia muestra cambios importantes y se mueve en la misma línea de las tendencias internacionales en los aspectos revisados. Se registran nuevos desafíos y una gran oportunidad para potenciar a las organizaciones, en procura de construir posturas de seguridad digital más confiables y resilientes, encaminadas a mejorar e impulsar su competitividad actual y futura.

Referencias

PwC, 2018. Global Information Security Survey. Recuperado de: https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey.html

EY, 2018. Global Information Security Survey 2018-19. Recuperado de: https://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2018-19/$FILE/ey-global-information-security-survey-2018-19.pdf

CISCO, 2019. Informe Anual de Seguridad. Recuperado de: https://www.cisco.com/c/dam/global/es_mx/solutions/pdf/cybersecurity-series-threat.pdf

ISACA, 2019. State of Cybersecurity Implications. Recuperado de: https://cybersecurity.isaca.org/state-of-cybersecurity

Verizon 2019. Data Breach Investigation Report. Recuperado de: https://enterprise.verizon.com/resources/reports/2019/2019-data-breach-investigations-report.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

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

WEF, 2019 (World Economic Forum). The Global Risk Report 2019. Recuperado de: https://www.weforum.org/reports/the-global-risks-report-2019

CISCOb, 2019. Anticipating the Unknowns. Recuperado de: http://ebooks.cisco.com/story/anticipating-unknowns

CCO, 2018 (Champlain College Online). The State of the Cybersecurity Workforce and Higher Education. Recuperado de: https://www.champlain.edu/champlain-college-online/about-us/in-the-news/cybersecurity-survey-2018

PwC Luxemburgo, 2018. Out of the Shadow: CISO is in the spotlight!. Recuperado de: https://www.pwc.lu/en/digital-services/cyber-security/docs/pwc-ciso-survey-2018.pdf

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

IDC, 2019. The Modern Connected CISO. Recuperado de: https://www.capgemini.com/wp-content/uploads/2019/01/The-Modern-Connected-CISO.pdf

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

PwCb, 2019. 22nd Annual Global CEO Survey. Recuperado de: https://www.pwc.com/gx/en/ceo-survey/2019/report/pwc-22nd-annual-global-ceo-survey.pdf

Tenable-Ponemon, 2019. Measuring & Managing the Cyber Risks to Business Operations. Recuperado de: https://www.tenable.com/cyber-exposure/ponemon-cyber-risk-report

Andrés R. Almanza J., Ms.C, CISM. *Coach Ejecutivo y Chief Growth Officer en CISOS.CLUB. Ingeniero de Sistemas y Computación de la Universidad Católica de Colombia. Especialista en Seguridad en Redes de la Universidad Católica de Colombia. Máster en Seguridad Informática, Ms.C, de la Universidad Oberta de Cataluña, España. Profesional certificado como Coach Ejecutivo y de Vida, por la International Coaching Leadership and Future Achivement. Profesional certificado como Information Security Manager (CISM), por ISACA. Docente de Cátedra de la Universidad Externado de Colombia. Miembro del Comité Editorial de la Revista "Sistemas" de la Asociación Colombiana de Ingenieros de Sistemas (ACIS).*