XVIII Encuesta Nacional de Seguridad Informática

Evolución del perfil del profesional de seguridad digital

DOI: 10.29236/sistemas.n147a4

Resumen

La encuesta nacional 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 2018, contó con la participación de 234 encuestados, quienes con sus respuestas permiten conocer la realidad del país. 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, OWASP Capítulo Colombia, y CISOS.CLUB, entidades que colaboraron en dicho proceso para difundir entre sus diferentes grupos de interés el instrumento.

Este estudio cumple con varios propósitos. En primer lugar, muestra el panorama de las organizaciones colombianas frente a la seguridad de la

información y/o ciberseguridad, y su respuesta a las demandas del entorno actual. En segunda instancia, es un instrumento referente para Colombia y Latinoamérica, en la medida en que llama la atención de todos los sectores interesados en los temas relacionados con la seguridad.

La investigación refleja las opiniones de quienes contestan y el análisis está basado en la realidad representada en los datos obtenidos. En ese orden, lo primero que se hace para la obtención de los resultados es preparar y revisar las preguntas de la encuesta; acto seguido preparar los componentes tecnológicos necesarios, publicación e invitación al proceso, distribución a los grupos de interés y cooperantes, recepción de datos, cierre de la encuesta, validación de los datos, normalización y análisis, preparación del informe, preparación de la presentación y publicación de los mismos, en los diferentes medios dispuestos para ello.

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

Andrés R. Almanza J.

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, EY, CISCO, Verizon, ESET, se procederá a analizar los resultados de la Encuesta Nacional de Seguridad Informática ACIS 2018.

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.

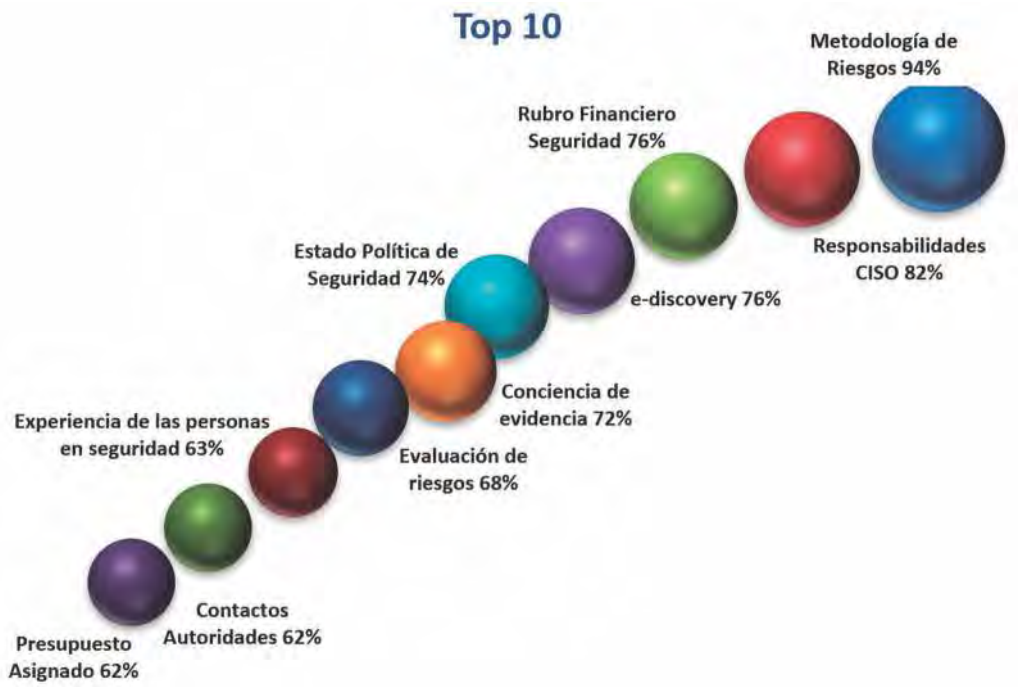
Capital intelectual: Busca definir cómo son las áreas de seguridad y las características básicas en materia de experiencia, formación y capacitación de los profesionales de seguridad. Muestra también la relación de las instituciones de educación superior frente a una realidad tan cambiante.

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 10.

En la gráfica 1 se encuentran los datos más relevantes de la encuesta. El 94% de los encuestados reconoce usar una metodología de gestión de riesgos como herramienta para admi-nistrar los riesgos en materia de segu-ridad digital. Con base en los resulta-dos, un 82% considera que la respon-sabilidad del profesional de seguridad en las organizaciones está centrada en velar por la protección de la información empresarial. Un 76% indica que existe un rubro definido para la seguridad de la información, mientras que un 76% no tienen estrategias de ediscovery, como instrumento para la administración de la evidencia digital ni soporte de las pruebas ante litigios judiciales. Tales porcentajes muestran que no es una práctica aún bien entendida. Un 74% reconoce la importancia de la evidencia digital y tiene conciencia de los procesos relacionados con la identificación, preservación y análisis de la evidencia digital. La evolución de la seguridad dentro de las empresas colombianas aumenta y se ve reflejada en que el 74% de los participantes manifestaron poseer un modelo de políticas de seguridad aprobado y conocido por todos los miembros de la organización. Aunque existe una conciencia clara para usar la gestión de



Gráfica 1: Top 10 de Resultados

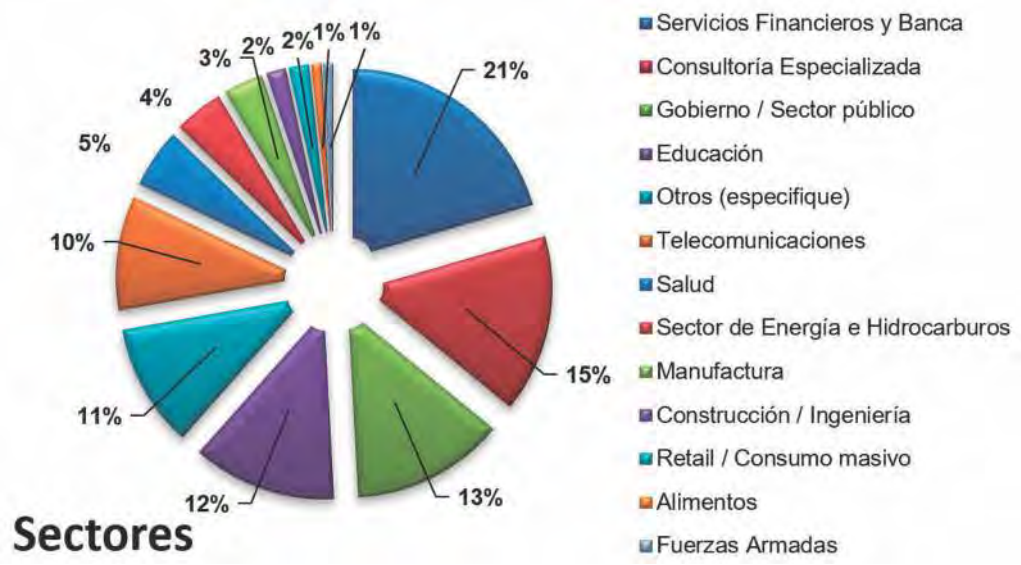
riesgos, sólo el 68% identifica en sus modelos los riesgos relacionados con la seguridad digital, lo que significa la existencia de retos interesantes en el uso de la gestión de riesgos como instrumento para la toma de decisiones en torno a la seguridad digital. La experiencia de los profesionales de seguridad es otro de los datos relevantes de esta encuesta, el 63% de los participantes manifiesta que el profesional de seguridad debe contar, por lo menos, con dos años de experiencia para ocupar la posición en las distintas organizaciones de Colombia. Por otra parte, la cooperación se ha convertido en un factor fundamental en nuestro país; de ahí que el 62% de los encuestados manifiesta mantener contacto con las autoridades nacionales e internacionales, frente a los incidentes de seguridad o ciberseguridad. El último dato relevante del top 10 está centrado en los presupuestos de seguridad; un 62% de los participantes desconoce el monto asignado para el año 2018.

Demografía

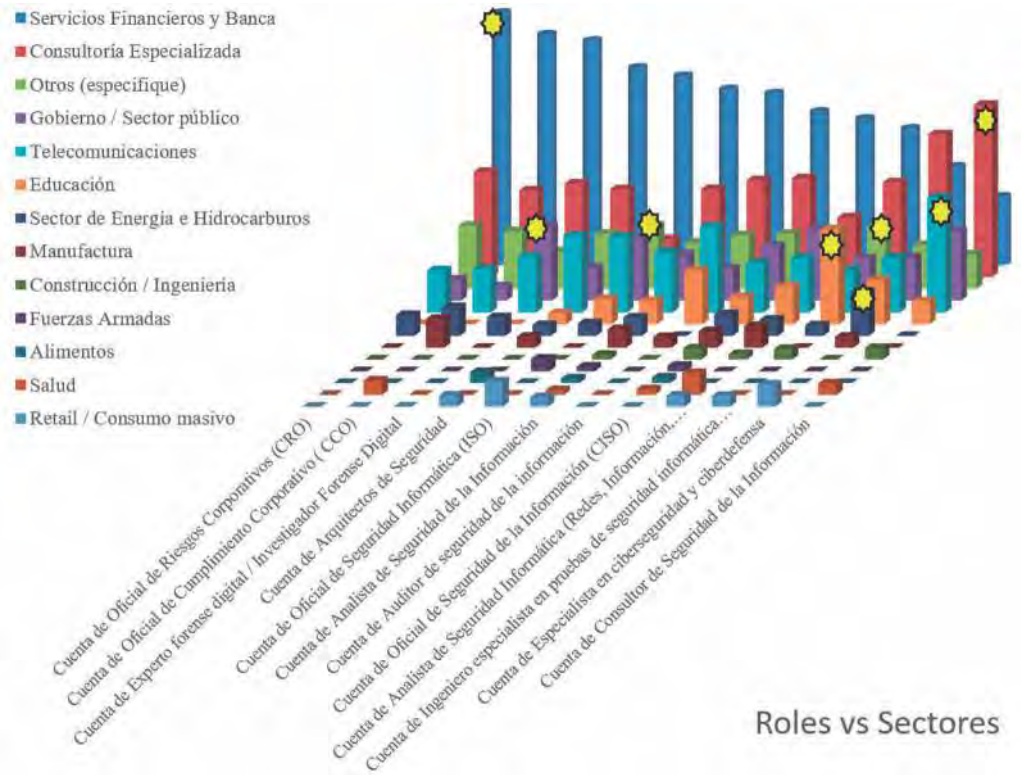
Sectores participantes

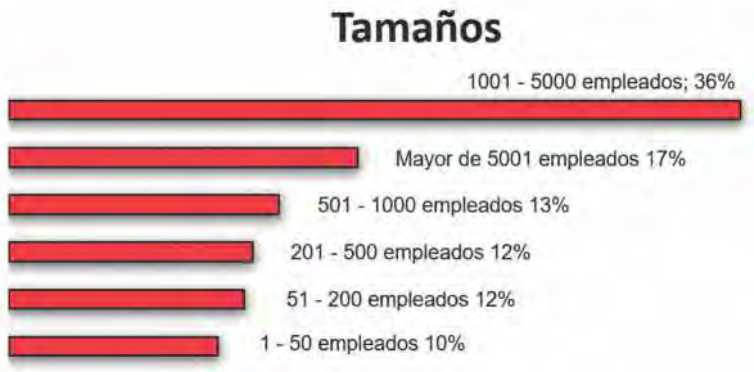
La gráfica 2 refleja la participación de 13 sectores de la economía colombiana. Los tres segmentos con mayor injerencia están compuestos por el sector financiero, servicios de consultoría especializada y el Gobierno.

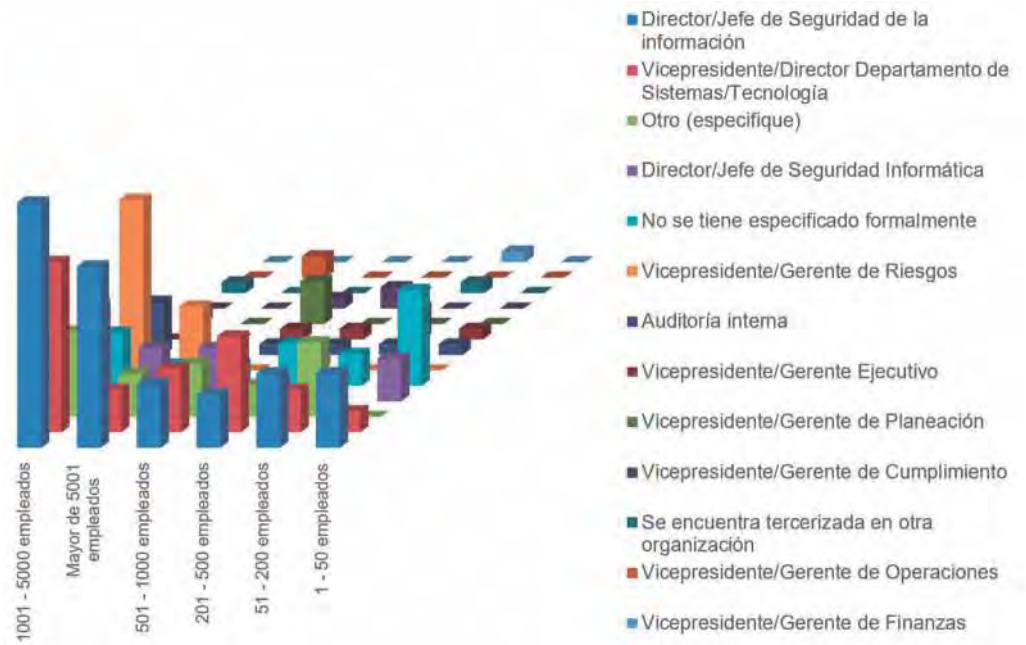
La Gráfica 3 muestra el tamaño de las empresas en Colombia, de acuerdo con el número de empleados. Como se puede observar, el 53% de la mues-



Gráfica 2: Sectores participantes







Gráfica 3: Tamaño de las empresas. Dependencia vs. tamaño

tra incluye a empresas de gran tamaño más de 1000 en Colombia.

La Gráfica 4 muestra los cargos de los encuestados, entre los que se cuentan auditores, profesionales de TI, profesionales de seguridad, CISOs. Así mismo, figuran otras clasificaciones para los profesionales de seguridad digital en el país, tales como analistas y profesionales de planta de seguridad, entre otros.

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

Gráfica 4: Cargos de los encuestados

dad digital y establecer un modelo de políticas en materia de seguridad digital.

La Gráfica 6 muestra de quién depende el área de seguridad. Los datos indican que el área de seguridad depende de una dirección propia. Por otro lado, están las áreas de tecnología con la responsabilidad de dirigir la seguridad digital en las empresas.

En la Gráfica 7 se observan los roles dentro de una organización, en materia de seguridad digital. En Colombia figuran los analistas de seguridad (in-

Gráfica 5: Funciones del responsable de seguridad

Gráfica 6: Dependencia del área de Seguridad

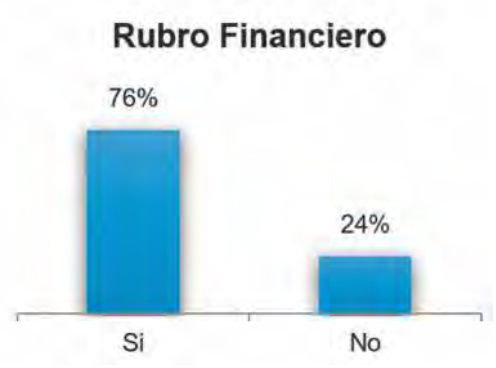
formación e informática); le sigue el cargo denominado CISO, al que se suman los ingenieros de pruebas, entre los principales roles

Presupuestos

La realidad colombiana es muy interesante, en materia de presupuestos en

Gráfica 7: Roles de Seguridad

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; el 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. El 39% de los participantes tiene conocimiento de los valores asignados para el 2018, mientras el 62% manifiesta no conocer los valores asignados. 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

Gráfica 9: Porcentaje del presupuesto Global

Gráfica 10: Presupuesto de Seguridad

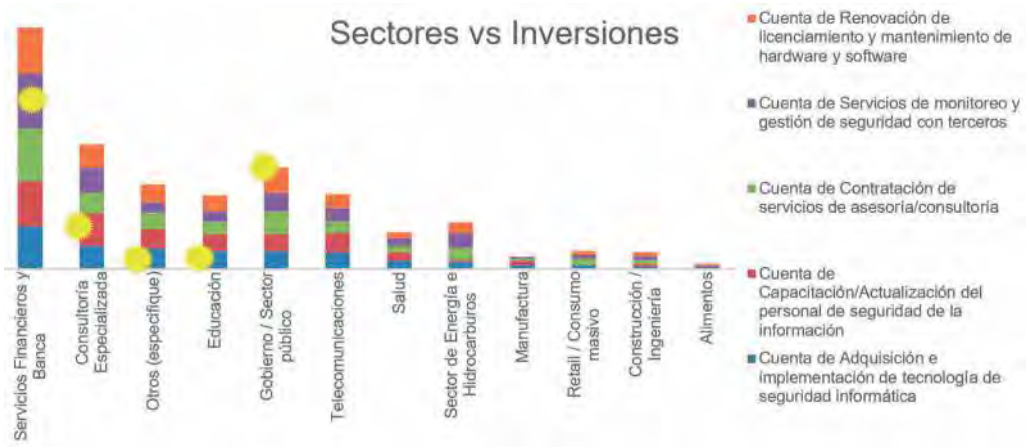
Gráfica 11: Inversión de Seguridad

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 profesionales de seguridad es el último criterio sobre los presupuestos. La Gráfica 12 muestra en dólares, los montos de la inversión en diferentes tópicos. La franja de recursos financieros menos usada corresponde al rango entre $US70.000 a $US90.000 dólares.

Incidentes

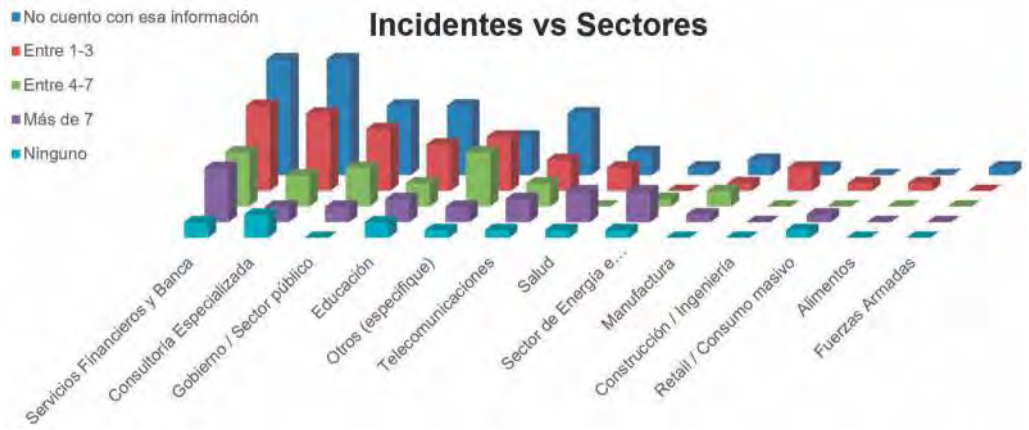
En Colombia se mantiene la tendencia en materia de incidentes de seguridad en concordancia con las tendencias internacionales. Tales desafíos, en términos de preparación y atención, son una exigencia para las organizaciones.

La Gráfica 13 muestra la cantidad de incidentes que se presentan en Colombia, según los participantes. El

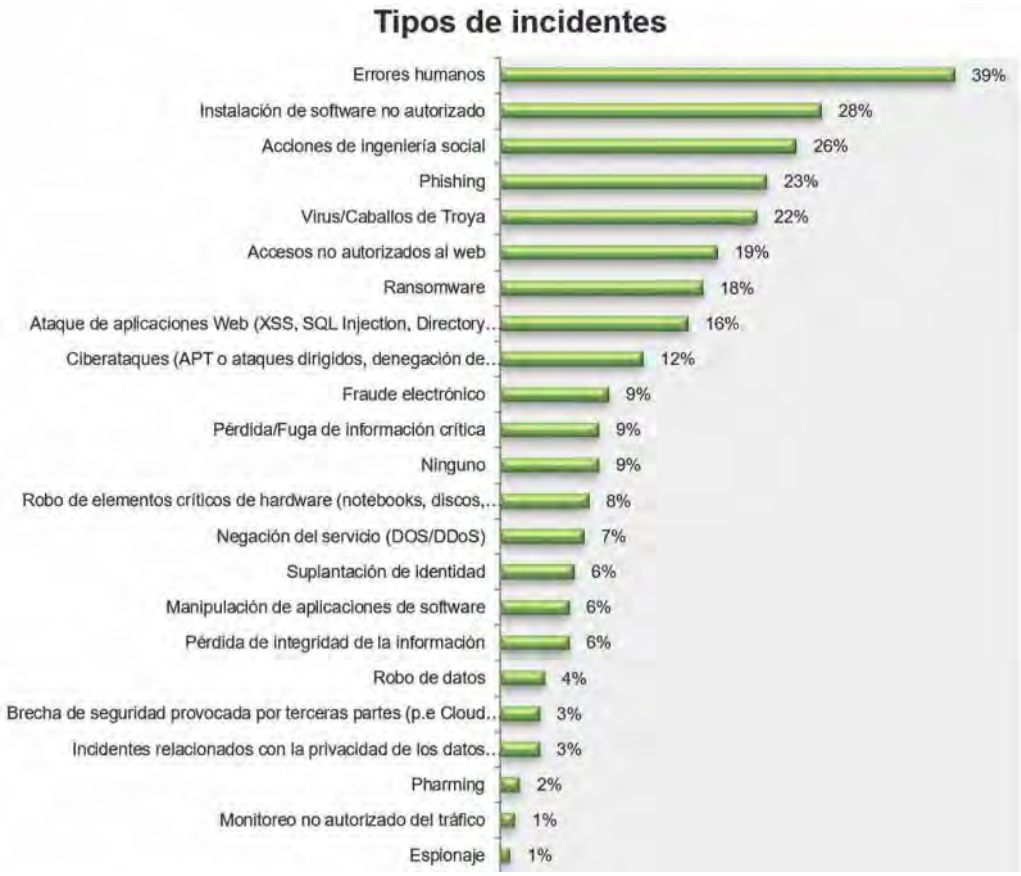


Gráfica 12: Montos en dólares de las inversiones de seguridad. Sectores vs. inversiones

65% 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.



Gráfica 13: Cantidad de Incidentes. Incidentes vs sectores



Gráfica 14: Tipos de Incidentes de Seguridad

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

La Gráfica 15 muestra la acción de los encuestados frente a un incidente, en términos de las notificaciones respectivas. Los datos reflejan que, ante un incidente y su identificación, el 52% de los participantes lo notifican a la propia organización, y el 31% al equipo de respuesta a incidentes. La Gráfica 16 refleja la forma como mejor se comunican los incidentes, máxime cuando éstos deben ser notificados a entes externos a la organización. El 62% de los encuestados manifiesta que con canales seguros se debe realizar este tipo de procedimientos.

En la Tabla 1 se relacionan los ítems asociados a la evidencia digital, como parte fundamental del proceso de gestión de incidentes. El 72% de los encuestados tiene conciencia para identificar, preservar, y analizar la evidencia como parte de dicho proceso. No obstante, sólo el 22% realiza procedimientos formales y un 30% no formales. En esa misma medida, el 70% dice no tener procedimientos de e-discovery o descubrimiento electrónico, como herramienta para soportar los posi-

Gráfica 15: Notificaciones de un Incidente

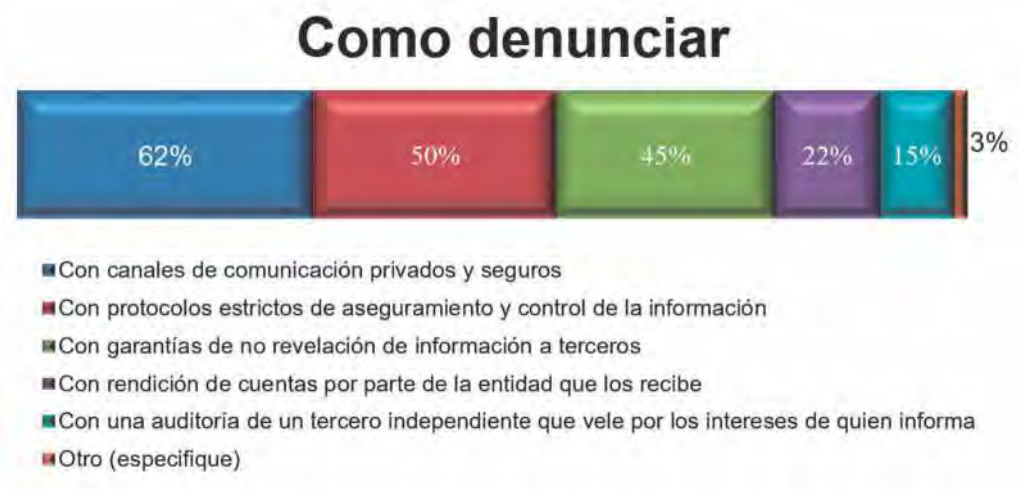
bles litigios o reclamaciones legales. Es importante señalar que, cerca del 62% de los participantes, tiene contacto con autoridades de orden nacional e internacional, como parte de las prácticas claves en los procesos de gestión de incidentes.

Herramientas

La Gráfica 17 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 39% de los participantes usa esta práctica una vez al mes; el 34% entre dos y 4 veces al año; el 18% dice no usarla y el 9% usa más de 4 veces al año los procesos de evaluaciones de seguridad en sus organizaciones.

Conciencia de la evidencia digital	**72%**
Procedimientos de evidencia digital	53%
Estrategia de E-Discovery	24%
Contacto con autoridades	62%

Tabla 1: Evidencia Digital



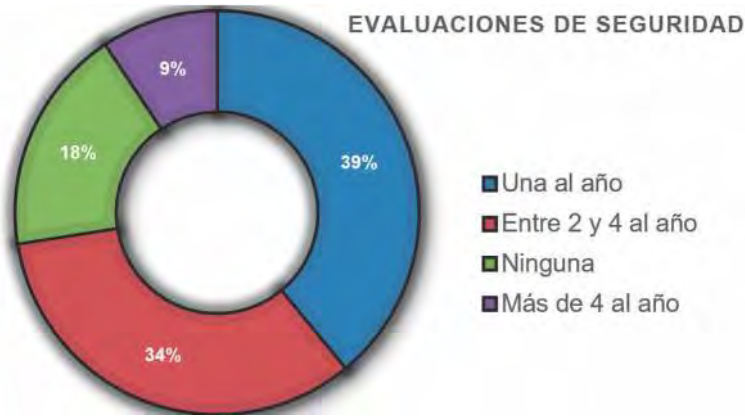
Gráfica 16: Mecanismos para denunciar

La Gráfica 18 indica cuáles son los mecanismos de seguridad comúnmente usados en las organizaciones. La Virtual Private Network (VPN), los *Firewalls*, y las soluciones *Antimalware* son los mecanismos más usados en las organizaciones colombianas.

Como parte de las prácticas en materia de seguridad los participantes se mantienen notificados de las fallas de seguridad, a través de múltiples mecanismos, entre los que se destacan la lectura de artículos y revistas especializadas (48%); la cooperación con colegas (47%); la notificación de los proveedores (42%); alertas de Computer Security Incident Respond Team (CSIRT), (35%) y la lectura de listas de seguridad (31%). Cabe señalar que sólo un 8% no usa este tipo de prácticas, a la hora de estar informado sobre las fallas de seguridad.

Políticas

La Gráfica 19 refleja el estado de las políticas de seguridad en las organizaciones colombianas; el 90% de los participantes manifiesta tener una o algu-

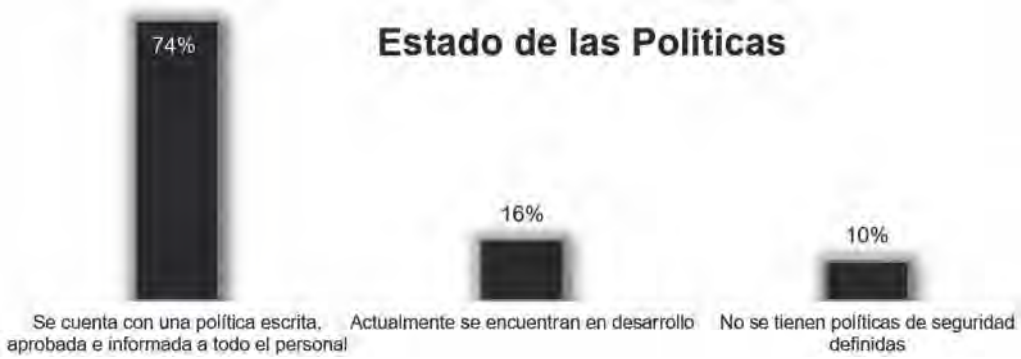


Gráfica 17: Evaluaciones de Seguridad

Gráfica 18: Mecanismos de Seguridad

nas en sus diferentes estadios. En comparación con años anteriores, se observa un claro crecimiento notorio.

Las organizaciones y sus responsables de seguridad entienden que las políticas no son el único ni el ultimo instrumento para construir posturas de seguridad. Al indagar sobre los obstáculos por los cuales no hay posturas adecuadas en materia de seguridad en las empresas, un 49% de los partici-



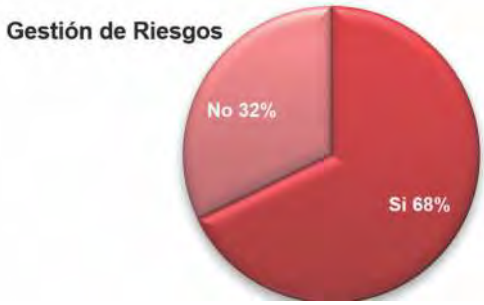
Gráfica: 19 Estado de las Políticas

Gráfica 20: Obstáculos de la Seguridad

pantes señala como factor más importante, la ausencia de una cultura de seguridad, como lo muestra la Gráfica 20.

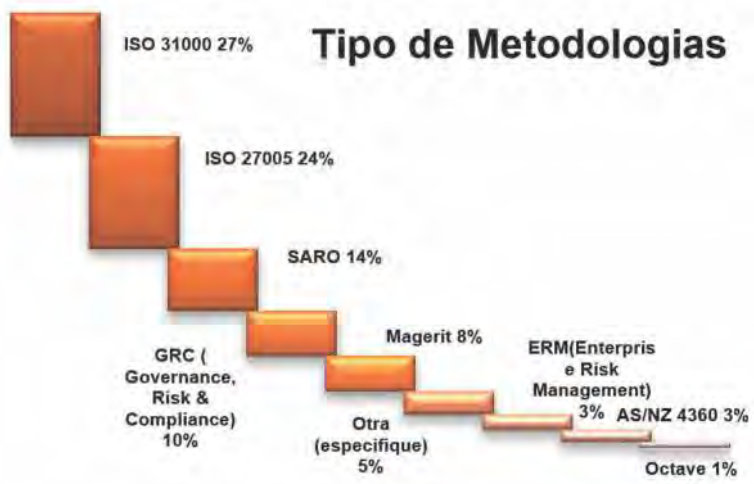
La gestión de riesgos como parte estructural de las funciones y tareas de los responsables de seguridad y sus organizaciones es otro de los componentes claves. En la Gráfica 21, el 68% de los participantes hace una evaluación de riesgos de seguridad digital y la incluyen en sus ejercicios globales de gestión de riesgos. En la Gráfica 22, el 97% realiza el ejercicio en un rango entre una y más de dos veces en el año, lo que ratifica la importancia de realizar estos ejercicios como herramientas para la toma de decisiones en las organizaciones. El Foro Económico Mundial en su informe del año 2018, señala los riesgos cibernéticos como una de las amenazas más probables de este tiempo, de ahí la importancia en el uso de estas prácticas y como herramientas para la construcción de posturas digitales consistentes y coherentes en la realidad colombiana.

Al indagar por qué no se realiza la gestión de riesgos de seguridad, se encuentra que el 38% lo hace dentro del proceso corporativo de gestión de riesgos. Este dato es muy interesante porque indica que la seguridad digital es transversal a los procesos, las perso-



Gráfica 21: Gestión de Riesgos de Seguridad

Gráfica 22: Cantidad de Gestión de Riesgos en Seguridad



Gráfica 23: Tipos de Metodología

nas, además de proporcionar una visión integral para el negocio. La Gráfica 23 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 24 representa el tipo de riesgos asociados a los

Gráfica 24: Tipos de Riesgos

Gráfica 25: Marcos de trabajo usados

incidentes de seguridad. La categoría de riesgos operativos es la más usada para esta situación.

La Gráfica 25 ilustra el uso de los distintos marcos de trabajo (*frameworks*) usados en las organizaciones colombianas: ISO/IEC 2700, ITIL y Cobit 5 son los más usados. La Gráfica 26 refleja las regulaciones a las que las organizaciones están sometidas; en el caso colombiano, el 63% de los participantes manifiesta que sí existen regulaciones 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 (EU), de gran impacto a nivel global.

Gráfica 26: Regulaciones o normativas

Capital intelectual

Las áreas de seguridad de la información en Colombia están formadas por grupos de una a cinco personas, de acuerdo con los participantes. La Gráfica 27 muestra el grupo de organizaciones que cuentan con un recurso dedicado a la seguridad (81%). La Gráfica 28 resalta que el tiempo de experiencia promedio para que los profesionales de seguridad sean contratados en Colombia es superior a dos (2) años y su experiencia es importante (91%) y necesaria para desempeñar un cargo en materia de seguridad. La Gráfica 29 indica que la certificación que poseen en la actualidad los profesionales de seguridad, corresponde a la de Auditor ISO/IEC 27001. Por otro lado, también se observa que estos profesionales buscan en el futuro cercano certificaciones como la Certified Information Security Mana-

Gráfica 27: Recursos dedicados a la Seguridad

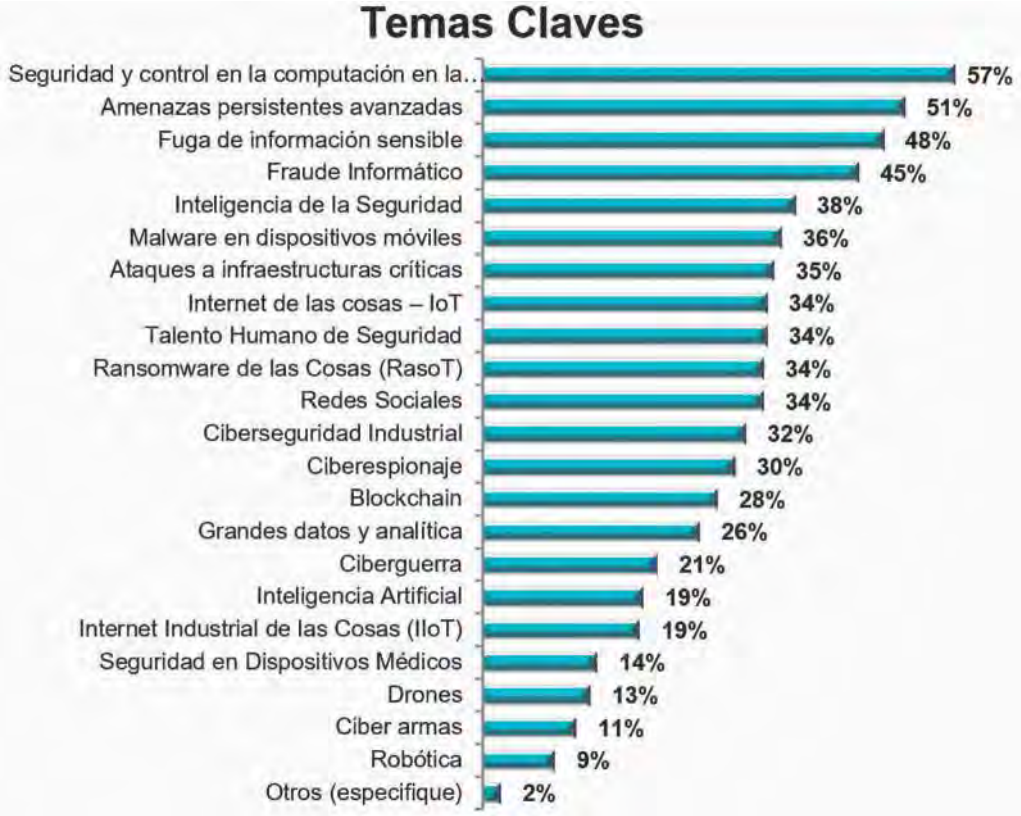
Gráfica 28: Experiencia del profesional

Gráfica 29: Certificaciones poseídas vs deseadas

Gráfica 30: Papel de la educación

ger (CISM), como oportunidades para mejorar sus perfiles. La tendencia internacional lo ratifica, en el sentido de que los perfiles de los profesionales de seguridad se pueden mejorar con las ofertas de certificaciones y educación formal.

La Gráfica 30 indaga sobre la forma en que la educación ha participado en la



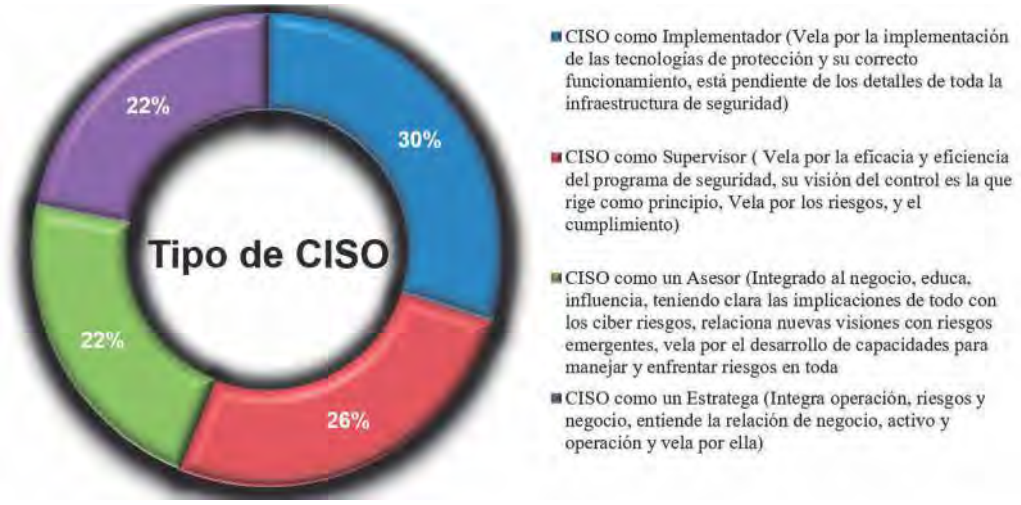
Gráfica 31: Desafíos del 2018

Gráfica 32: Involucramiento de los Directivos

formación de los profesionales de seguridad. En este sentido, el punto a resaltar por parte de los participantes es que no existe la suficiente investigación, que es escasa o insuficiente en materia de seguridad digital, con un 41%. De igual forma se advierte una ligera mejora en la formación académica de los profesores, en temas de seguridad y control respecto del año anterior.

Temas emergentes

La Gráfica 31 muestra los temas inherentes a los profesionales de seguridad durante el año 2018, los cuales pueden producir importantes desafíos



Gráfica 33: Cómo ven al CISO

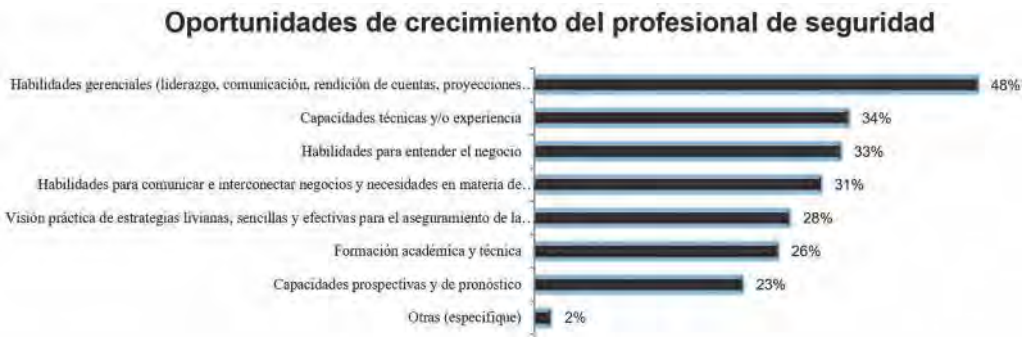
en el desarrollo de los distintos negocios. El más relevante, la computación en la nube como uno de los grandes desafíos de las organizaciones colombianas. Las amenazas avanzadas continúan en la lista, de la misma manera que la fuga de información sensible, como temas claves para tener presentes.

Una de las grandes preocupaciones de muchos profesionales de seguridad está centrada en sus juntas directivas y cómo se deben vincular a todas las iniciativas en materia de ciberseguridad; así mismo lo manifiestan los distintos referentes internacionales. En este sentido, la Gráfica 32, muestra según los participantes el nivel de involucramiento de los directivos de las organizaciones en Colombia. En este sentido, se ratifica la tendencia internacional orientada a que cada vez más los niveles ejecutivos (C-Levels) y los niveles directivos (Board Level) están involucrados en la realidad de la ciberseguridad y la seguridad digital de sus empresas. En el contexto colombiano, el 71% de los encuestados manifiesta que de alguna manera están estos niveles involucrados; sólo el 29% de los participantes no ve que estos cuerpos directivos se involucren.

Líder de Seguridad de la Información

Las Gráficas 33, 34 y 35 reflejan la forma como el CISO se ve, se desenvuelve y cómo puede evolucionar en el contexto de las organizaciones nacionales. La Gráfica 33 muestra la forma como es visto el profesional de seguridad. Vale anotar que continúa la visión del CISO como un implementador de las tecnologías de protección; así lo ratifican los datos obtenidos, considerando que las inversiones de seguridad precisamente se centran en ello; y, en torno a los top en términos de controles usados, las herramientas tecnológicas están en los primeros lugares. Una segunda mirada al profesional de seguridad está relacionada con el *compliance*; en otras palabras, un profesional que vela por el cumplimiento regulatorio, el control y su implementación, un asesor que se encarga de educar, influenciar en alguna medida a toda la organización; y, por último, un profesional estratega o líder que se integra dentro de la empresa y ve el

Gráfica 34: Entrega de información del profesional de seguridad



Gráfica 35: Camino de crecimiento de un profesional de seguridad

mundo de una manera distinta, en términos de la seguridad.

La Gráfica 34 muestra la forma como el líder de seguridad se comunica con la organización, en todos sus niveles. La comunicación es una de las nuevas herramientas claves que deben ser usadas por los profesionales de seguridad, como lo manifiestan algunos estudios internacionales. En primer lugar, en Colombia ellos suministran información técnica, seguida por la información relacionada con los riesgos de seguridad de la información y luego sobre la gestión y las brechas e incidentes de seguridad. En la totalidad de los datos se puede ver que, efectivamente, el profesional de seguridad entrega algún tipo de información.

La Gráfica 35 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 gerenciales son uno de los elementos identificados como aspecto a mejorar; las capacidades técnicas y la experiencia figuran en el siguiente nivel, seguidas por la necesidad de involucrar el entendimiento del negocio como parte de las capacidades de los profesionales de seguridad.

Reflexiones finales

Año tras año, el estudio muestra un afianzamiento de la seguridad digital como un instrumento corporativo en las empresas colombianas. En este contexto, cada vez más incierto, son 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.

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 creciente expansión digital hace de la realidad un mejor lugar; se enfrentan nuevos y desafiantes riesgos, que invitan a la reflexión en procura de proteger el valioso activo de la información, encaminada a lograr posiciones más confiables en un mercado competitivo y exigente.

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 a 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. De acuerdo con los resultados obtenidos, 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.

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. De asesor técnico, se espera que el CISO se convierta en asesor, suministrando información estratégica para la toma de decisiones, de tal manera que las vías de comunicación con los miembros de la empresa sean más expeditas, en busca de proteger la información.

4. A nivel nacional, se mantiene la sólida tendencia de usar mecanismos tecnológicos como las principales herramientas de protección. De igual manera, se abre camino la seguridad más allá de unas implementaciones tecnológicas y en la protección, una oportunidad para construir nuevos estándares alrededor de la cultura organizacional.

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 inter-

nacional. 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

Clinton Larry. (2017) Cyber-Risk Oversight. Director´s Handbook Series. NACD (National Association of Corporate Directors). Recuperado de: https://www.nacdonline.org/files/FileDownloads/NACD%20Cyber-Risk%20Oversight%20Handbook%202017.pdf

Choudhary, U. (2015) This Might Be The Next Coveted Leadership Position Of 2015. *F@stcompany Magazine.* Recuperado de: https://www.fastcompany.com/3043376/how-to-earn-respect-from-the-hottest-seat-in-leadership-today

World Economic Forum. (2018). The Global Risks Report 2018 13th Edition. Mayo. Recuperado de: http://www3.weforum.org/docs/WEF_GRR18_Report.pdf

World Economic Forum. (2018). Cyber Resilience Playbook for Public-Private Collaboration. Mayo. Recuperado de: http://www3.weforum.org/docs/WEF_Cyber_Resilience_Playbook.pdf

ISACA. (2018). State of Cybersecurity 2018. Recuperado de: https://cybersecurity.isaca.org/state-of-cybersecurity

Deloitte. (2017). Cybersecurity and the role of internal audit An urgent call to action. Recuperado de: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-cyber-ia-urgent-call-to-action.pdf

Deloitte. (2017). The value of visibility Cybersecurity risk management examination. Recuperado de: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-the-value-of-visibility-cybersecurity-risk-management-examination.pdf

Deloitte. (2017). Assessing cyber risk Critical questions for the board and the C-suite. Recuperado de: https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-ers-assessing-cyber-risk.pdf

IBM. (2018). IBM X-Force Threat Intelligence Index 2018. Recuperado de: https://microstrat.com/sites/default/files/security-ibm-security-solutions-wg-

research-report-77014377usen-20180329.pdf

Raj Samani, McAfee Chief Scientist. (2018) Navigating a Cloudy Sky. Recuperado de: http://www.redseguridad.com/content/download/73021/580227/file/rp-navigating-cloudy-sky.pdf

CISCO. (2018). Reporte Anual de Seguridad 2018. Recuperado de: https://www.cisco.com/c/es_co/products/security/security-reports.html

PwC. (2017). Revitalizing privacy and trust in a data-driven world. Recuperado de: https://iapp.org/media/pdf/resource_center/revitalizing-privacy-trust-in-data-driven-world.pdf

PwC. (2018). The Anxious Optimist in the Corner Office. Recuperado de: https://www.pwc.com/gx/en/ceo-survey/2018/pwc-ceo-survey-report-2018.pdf

PwC. (2017). Strengthening digital society against cyber shocks. Recuperado de: https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey/strengthening-digital-society-against-cyber-shocks. html

PwC. (2017). Moving forward with cybersecurity and privacy. Recuperado de: https://www.pwc.com/kr/ko/industries/automotive/201512_moving-forward-with-cybersecurity-and-privacy_en. pdf

PwC. (2017). Toward new possibilities in threat management. Recuperado de: https://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/assets/gsiss-report-cybersecurity-privacy-possibilities.pdf

Verizon. (2018). 2018 Data Breach Investigations Report. Recuperado de: https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf

Ponemon Institute. (2018). 2018 Cost of Insider Threats: Global. Recuperado de: https://www.observeit.com/ponemon-report-cost-of-insider-threats/

Ponemon Institute & IBM. (2018). The Third Annual Study on the Cyber Resilient Organization. Recuperado de: https://info.resilientsystems.com/hubfs/IBM_Resilient_Branded_Content/White_Papers/2018_Cyber_Resilient_Organization_Study.pdf

Ponemon Institute & F5 Networks. (2017). The Evolving Role of CISOs. Recuperado de: https://f5.com/Portals/1/PDF/labs/Evolving_Role_of_CISOs_Aug2017.pdf?ver=2017-09-18-100218-007

EY. (2017). Cyber resiliency: evidencing a well-thought-out strategy. Mayo. Recuperado de: http://www.ey.com/Publication/vwLUAssets/EY-cyber-resiliency-evidencing-a-well-thought-out-strategy/$FILE/EY-cyber-resiliency-evidencing-a-well-thought-out-strategy.pdf

EY. (2017). An integrated vision to manage cyber risk. Recuperado de: http://www.ey.com/Publication/vwLUAssets/ey-an-integrated-vision-to-manage-cyber-risk/$File/ey-an-integrated-vision-to-manage-cyber-risk.pdf

EY. (2017). Cybersecurity regained: preparing to face cyber attacks. Recu-

perado de: http://www.ey.com/Publication/vwLUAssets/ey-cybersecurity-regained-preparing-to-face-cyber-attacks/$FILE/ey-cybersecurity-regained-preparing-to-face-cyber-attacks.pdf

Accenture. (2018). Gaining Ground On The Cyber Attacker. Recuperado de: https://www.accenture.com/t20180416T134038Z__w__/us-en/_acnmedia/PDF-76/Accenture-2018-state-of-cyber-resilience.pdf

Gemalto. (2018). 2017 The Year of Internal Threats and Accidental Data Breaches. Recuperado de: https://breachlevelindex.com/assets/Breach-Level-Index-Report-2017-Gemalto.pdf

Rachel Linthwaite, Market Impact Consultant. (2017) Drop A Pin At The Intersection Of Digital Experience And Security. Forrester Consulting. Mayo. Recuperado de: https://www.akamai.com/us/en/multimedia/documents/white-paper/forrester-digital-maturity-thought-leadership-white-paper.pdf

***Andres 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).*