Tendencias 2016
Encuesta nacional de seguridad informática*

Retos de la ciberseguridad.

Andrés Ricardo Almanza Junco, M.Sc.

La encuesta nacional de seguridad informática, capítulo Colombia, realizada por ACIS a través de Internet, contó con la participación de 121 encuestados, quienes con sus respuestas permiten conocer la realidad del país.

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.

Agradecemos de manera muy especial a la Organización de Estados Americanos (OEA), por su apoyo en la difusión y distribución de la encuesta en todos sus Estados miembros. Así mismo, a la organización.CO, por su colaboración en el mismo sentido, entre las diferentes comunidades.

Metodología

El análisis presentado a continuación se desarrolló con base en una muestra aleatoria y de manera interactiva, a través de una página *web* dispuesta por Acis, para tal fin. Considerando las limitaciones, en términos de tiempo y recursos disponibles, se han tenido en cuenta los aspectos más sobresalientes de los resultados obtenidos, en procura de mostrar a los lectores las tendencias identificadas.

Lo nuevo

En este 2016 el formato oficial de la encuesta cuenta con algunas modificaciones. Contempla una nueva pregunta y adición de opciones en las actuales, así como una revisión sobre lo evaluado año tras año, en la búsqueda de conocer mejor el ambiente que viven las organizaciones colombianas y latinoamericanas, en el marco de la seguridad de la información y/o ciberseguridad.

En primer lugar, fue complementada con la cantidad de sectores, incluyendo al de Retail/Consumo masivo, toda vez que una de las tendencias internacionales vigentes y cada vez más desarrolladas es el ataque a los POS o puntos de ventas, de ahí el interés en conocer la realidad en dicho sector.

De igual manera, contempla la ampliación en el conjunto de roles y responsabilidades del Chief Information Security Officer –CISO- o Director de Seguridad de la Información, frente a un escenario digital cada vez más complejo, dinámico, volátil e incierto. Así mismo, dentro de las ampliaciones de la encuesta está conocer qué tipos de cargos se han venido creando en las organizaciones relacionadas con la seguridad de la información y/o ciberseguridad, como tendencia no sólo global, sino nacional.

Por otra parte, se busca saber cómo las organizaciones han venido enfrentando la anomalía del momento, el *Ransomware*, el cual ha tenido gran injerencia a nivel global; además de indagar si han incluido en sus consideraciones frente a la cadena de servicios en materia de la seguridad de la información y ciberseguridad, estas nuevas tendencias de monitoreo inteligente de amenazas.

Con relación a los estándares la encuesta busca saber cómo las industrias han optado por modelos actuales, cuáles son los más usados, además de observar referentes para la construcción de sus programas de seguridad que los apoyen en la construcción de una cultura, gobierno y gestión de la seguridad en las organizaciones.

Por último y no menos importante, este estudio pretende determinar cuáles son las nuevas apuestas en materia de preparación del personal responsable de seguridad; dónde ven las organizaciones que sus grupos de trabajo pueden incrementar sus conocimientos; y, a través de cuáles estudios y/o certificaciones, pueden apoyar sus procesos internos.

Retos y desafíos

Las crecientes anomalías electrónicas, unas regulaciones vigentes, unas tecnologías de protección cada vez más limitadas y una mayor dependencia de la tecnología en la forma de hacer negocios, muestran cómo la

necesidad de proteger la información es más relevante.

En esa misma óptica se observan unos ejecutivos de la seguridad más preocupados por utilizar lenguajes cercanos a la organización, para proveer soluciones que armonicen las relaciones de funcionalidad y protección, dentro del marco del negocio.

Este estudio muestra el afianzamiento de la ciberseguridad, que ha permeado en las empresas como una visión hacia la redefinición de lo ya identificado, que saca de la zona de confort a las organizaciones y las lleva a plantear nuevos interrogantes acerca de la forma como deben ser tratados los riesgos a los que se ven expuestas.

En este contexto, cada vez más incierto, son necesarios 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 y el contexto en el que el mundo se desenvuelve.

Datos generales

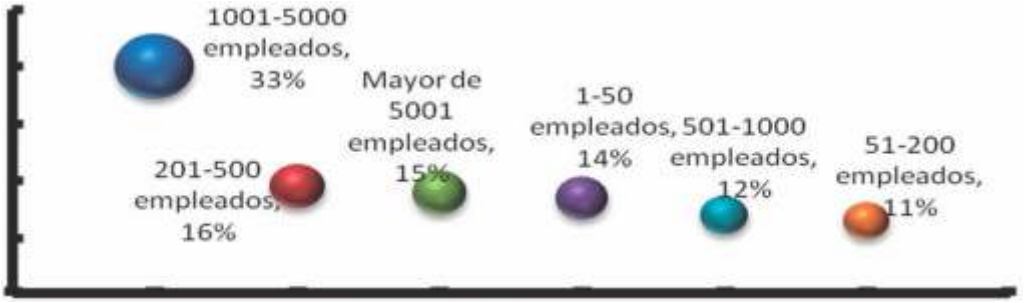
En esta sección están los datos más relevantes de la encuesta, relacionados con la demografía de los participantes y sus relaciones con la seguridad de la información.

La gráfica 1, muestra la comparación de los años 2016, 2015 y 2014 en relación con los participantes de la encuesta. Se puede observar que en el

Sectores

Gráfica 1. Sectores participantes

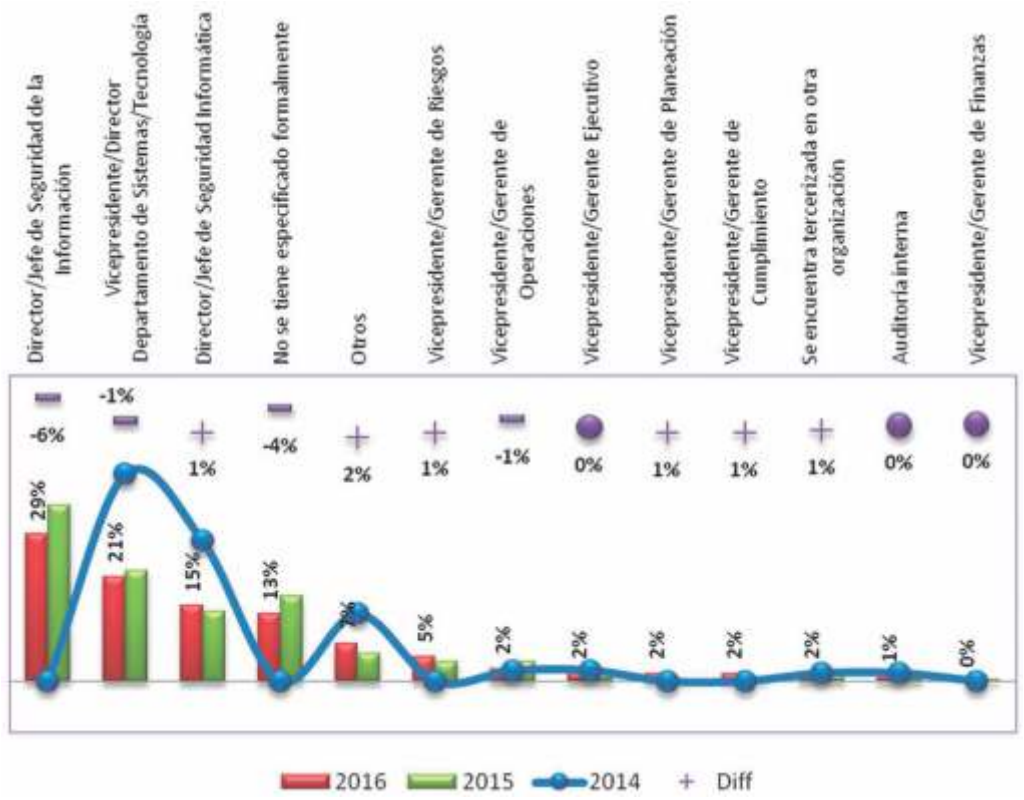
Tamaños



Gráfica 2. Tamaños de las empresas

año 2016 la participación del sector financiero fue la más nutrida y frente a años anteriores inclusive creció. Dos sectores que disminuyeron su participación fueron el sector del gobierno, que sólo obtuvo un 13% este año, y disminuyó en forma considerable, en un 7%, frente al año inmediatamente anterior, así como el sector de hidrocarburos, el cual disminuyó su participación en un 5%, frente a años anteriores.

Para este año, la distribución de las empresas es diversa. La mayor participación la tienen las empresas de 1001



Gráfica 3. Dependencia de la seguridad

a 5000 empleados (33%); le siguen lasempresas de 201 a 500 empleados (16%); luego las compañías mayores a 5000 empleados (15%).Por un lado, refleja la voluntad de los participantes en aceptar la encuesta y, por otro, indica que la ciberseguridad y/o seguridad de la información son temas interesantes, además de advertir sobre la importancia de conocer la realidad del país y la región.

Dependencia de la responsabilidad en seguridad

En la gráfica 3, se muestra de quién depende la responsabilidad de la seguridad en la organización. Se observa que cada vez más la seguridad de la información, deja de depender de las áreas de tecnología y pasa a otras áreas de la organización; así mismo, mientras decrece la dependencia de la seguridad de un director de seguridad de la información (6%), crece en 1% para las otras áreas, como director de seguridad informática, gerente de riesgos, gerente de planeación, gerente de cumplimiento. Indica también una tendencia a tercerizar la seguridad, como una alternativa en las organizaciones.

Cargo de los encuestados

La gráfica 4, muestra los cargos de las personas que han contestado la encuesta, divididos en cuatro áreas. Los cargos asociados a las áreas de tecnologías de información, 38%; los cargos relacionados con seguridad de la información, 38%; los que corresponden a las áreas de control, 16%; y, por último, los cargos de niveles ejecutivos equivalentes a un 8% del total de la población encuestada.

Para este año, el incremento es de un 2%,frente al período inmediatamente anterior, en lo que se refiere a los

Gráfica 4. Cargo de los encuestados

cargos en seguridad de la información y niveles ejecutivos de la organización. Este panorama muestra cómo ha ganado terreno la seguridad de la información, dentro de las empresas en la realidad colombiana. Ya tiene su propio espacio y madura con el tiempo. Así mismo, vemos cómo año tras año la encuesta muestra las diferentes interpretaciones de la seguridad de la información en las organizaciones colombianas.

Top de hallazgos

Esta sección muestra las variaciones más importantes de los resultados de la encuesta, desde las variaciones más positivas, hasta lo que más decreció, comparando los resultados de este año con el 2015.

En las tablas se encuentra descrito el ítem general, en la primera columna; la segunda columna describe las opciones y la tercera muestra la variación con relación al año anterior.

Las mayores variaciones positivas

(Tabla 1)

Análisis y comparaciones

De la tabla anterior se puede extraer lo siguiente:

1. El rol de primer respondiente se viene adoptando en las organizaciones para este año como una de las nuevas responsabilidades de los oficiales de seguridad.

1. En Colombia, el rol de Oficial de Seguridad Informática es lo que más predomina en las organizaciones, en el momento de crear el cargo para un responsable de seguridad; coincide con la tendencia mundial, según datos de la encuesta de Seguridad de la firma PwC [5], en la que el 54% de los encuestados tiene un responsable de seguridad a cargo. En Colombia, el 48% dice tener un CISO y el 27% un Oficial de Seguridad Informática. De esta manera, se ve reflejada la realidad global de tener un responsable a cargo que vele por los intereses relacionados con la protección de la información y le muestre a la organización los riesgos a los que se puede ver expuesta

3. Dentro del conjunto de nuevas actividades realizadas por los responsables de seguridad, está velar por la protección de la información personal, toda vez que las regulaciones nacionales como la ley 1581 en sus decretos reglamentarios así lo exige y cada vez más se ven enfrentados a responder por los entes de control en este sentido. Según informe de la firma PwC[6], el cibercrimen crece en un 32%, y uno de los factores claves está en el robo de información personal, razón por la cual es necesario que las responsabilidades del encargado de seguridad estén relacionadas con la protección de la información personal, como una de las nuevas responsabilidades de los encargados de la seguridad

4. Según datos de la encuesta de Ernst & Young[7], un 42% de los encuestados reconoce los activos de información como una pieza clave, en términos de la protección de la información, además del valor que tienen las declaraciones formales entorno a la identificación de activos de información; tendencia que se ve reflejada en Colombia. En este año, los encuestados el 71% de los encuestados reconoce la práctica de la formalidad de una directriz, establecida y reconocida

Tabla 1

Ítem	Descripción	Variación frente al año (2015)
1. Roles en la organización		
➡ Primer respondiente / gestionador de incidentes de seguridad, este rol creció de manera importante frente al año inmediatamente anterior.		17%
➡ Es el rol de Oficial de Seguridad Informática (ISO), otro de los roles que la organización mas a desarrollado en Colombia y crece frente a años anteriores.		9%
2. Actividades realizadas por el responsable de seguridad		
➡ Velar por la protección de la información personal		13%
➡ Seguimiento de prácticas en materia de protección de la privacidad de la información personal		12%
➡ Evaluar la eficiencia y efectividad del modelo de seguridad de la información		8%
3. Activos de Información		
➡ Las organizaciones cuentan con declaraciones formales relacionadas con los activos de información		11%
4. Información de fallas de seguridad		
➡ Notificación de proveedores		9%
➡ Notificación de colegas		8%
5. Mecanismos utilizados		
➡ SIEM (Security Information Event Management)		8%
➡ Las herramientas Anti-DDOS		7%
6. Conciencia de la alta dirección		
➡ La alta dirección entiende y atiende recomendaciones en materia de seguridad de la información.		7%
7. Notificación de los incidentes de seguridad		
➡ Autoridades locales/regionales.		7%

en la organización como un buen ejercicio, para poder gobernar de una mejor manera los datos, la información, el conocimiento y con ello tener mejores capacidades de competencia en un entorno digital tan cambiante como el actual.

5. La cooperación ha introducido en el mundo de la seguridad una nueva dinámica que permite a las organizaciones, de una manera más consistente, enfrentar las amenazas de hoy en día. En este año estos ejercicios se ven reflejados a través de la forma en cómo se notifican las organizaciones de los fallos de seguridad. Por un lado, el 45% de los encuestados reconoce hacerlo por sus proveedores; el estudio indica el fortalecimiento de las relaciones con ellos. El 43% señala que se entera de las fallas de seguridad por sus colegas.

La tendencia global, según la encuesta de PwC [5], muestra los beneficios relacionados con la cooperación: con los pares de la industria, con la autoridad y con el Gobierno, lo que les permite mejorar sus capacidades para entender mejor la realidad en la que se desenvuelve el mundo de la ciberseguridad. En esta misma perspectiva, los encuestados en Colombia señalan como herramientas de control con mayor crecimiento

En Colombia las herramientas de control con mayor crecimiento a los SIEM (25%), y las herramientas Anti-DDOS (16%).Se observa un crecimiento significativo de su uso, frente al año inmediatamente anterior. Las tendencias internacionales mues-tran a los SIEM dentro del espectro, como lo hace el Reino Unido [7], a través de la encuesta de seguridad llevada a cabo por ellos, en la que un 19% de los encuestados dice tener un SIEM implementado completamente en sus organizaciones para el tema de control. Por su parte, la firma de EY en su informe anual, advierte que sólo el 21% de los encuestados tiene un SIEM para monitorear las redes frente a las anomalías. Esto confirma que en la realidad nacional se está viendo a los SIEM como un instrumento válido a la hora de pensar en un control que apoye la prevención de los riesgos digitales.

6. La conciencia de la seguridad es otro de los ítems que varió de manera importante este año para Colombia. El 29% de los encuestados manifiesta que sus niveles directivos entienden y atienden recomendaciones, en materia de seguridad. Tendencia que se ve reflejada en el informe de Ciberseguridad realizado entre ISACA y RSA[8], en el que se reporta que el 36% de los encuestados dice que sus miembros de alta gerencia están muy comprometidos con la seguridad. De la misma manera, lo expresa la firma PwC en su informe anual [5], en el que, cerca de 45% de los encuestados, considera que sus juntas directivas se encuentran participando en la realidad de la seguridad. Así las cosas, en Colombia la realidad contempla la un interés por la seguridad, más allá de un reto tecnológico y la ven como un aliado en las juntas, que consideran el término de riesgos de información, como una nueva responsabilidad que los acerca a la realidad actual.

Las mayores variaciones negativas (Tabla 2)

Son aquellos criterios considerados este año por los encuestados, como

los menos importantes. Su variación frente a años anteriores es negativa.

Análisis y comparaciones

De la tabla anterior vale la pena destacar lo siguiente:

1. Solo el 39% de los encuestados manifiesta que sus áreas de seguridad poseen recursos definidos entre uno y cinco, mientras que en el año 2015 en Colombia, el 64% de los encuestados reconoció esa misma cantidad de recursos. Los datos globales muestran una tendencia contraria, según datos de la encuesta global del Reino Unido [7]. Lo positivo de la lectura para este año está relacionado con dos temas. Primero, disminuyen en un 3% los encuestados que manifiestan no tener ningún recurso dedicado a la seguridad, reforzado con la tendencia mundial a tener áreas de seguridad, formadas y establecidas. Crecen en un 4% las áreas de seguridad de más de 15 personas y eso está cerca de la tendencia global cercana al 10%.

2. Para este año la gestión de riesgos no fue reconocida como una herramienta indispensable, dentro del ejercicio de la protección de la información en la realidad Colombiana. Solamente el 30% de los encuestados manifestó realizar un ejercicio de evaluación de riesgos al año, comparado con el 49% de los encuestados del año anterior, quienes manifestaron haber realizado el ejercicio. Así mismo, sólo el 11% manifestó realizar el ejercicio dos veces al año, frente al 27% del año anterior. Y la tercera situación es que al momento de indagar sobre las razones para no realizarlo, una de ellas es reconocer que se hace dentro de los ejercicios corporativos de gestión de riesgos. Sorprende el decrecimiento de esta respuesta, en la que sólo el 29% de los encuestados manifiesta que el ejercicio se realiza dentro de la visión corporativa de la gestión de riesgos. La tendencia global, según la firma PwC[5] está relacionada con que el 91% de los encuestados manifiesta tener un marco de gestión de riesgos y ve los beneficios de tenerlos, frente a la cirberrealidad a la que se enfrentan las organizaciones.

3. Cada vez más los encuestados reconocen el valor de las certificaciones como un plus o mecanismo adicional de soporte para validar competencias, a la hora de llegar a los cargos de seguridad. Por ello, sólo el 19% de los encuestados respondió que dentro de los perfiles existe personal certificado en seguridad de la información; en comparación con el año anterior que el 37% manifestaba no poseer ninguna certificación para desempeñar el rol relacionado con la protección de la información.

4. En materia de presupuestos se tienen respuestas interesantes. Por una parte, sólo el 25% de los encuestados manifiesta no saber cuál es el monto asignado para la seguridad al año, comparado con 2015 que fue de un 42%. La lectura que se hace de esto es que cada vez más los responsables de seguridad tienen la responsabilidad y manejo del control de un presupuesto sólo para la seguridad. De la misma manera, sólo el 12% de los encuestados afirma que lo asignado en materia de seguridad, del total del presupuesto de la organización está entre el 0% y 2%, comparativamente con 2015, en que el 26% de los

Tabla 2

Ítem Descripción	Variación frente al año (2015)
Recurso humano dedicado a la seguridad.	
➡ Para este año sólo el 39% de los encuestados manifiesta tener áreas de seguridad con recurso humano entre 1-5, con dedicación exclusiva a dichas responsabilidades.	-25%
Gestión de riesgos.	
➡ Este año sólo un 30% de los encuestados manifiesta realizar una vez al año el ejercicio de riesgos.	-19%
➡ De igual manera, sobre la realización de dos pruebas al año, el estudio actual registra un 11%.	-17%
➡ Sólo el 29% de los encuestados, manifestó tener un modelo integral de riesgos para analizar y visualizar los riesgos de seguridad.	-15%
Certificaciones poseídas.	
➡ Este año bajó a un 19%, el grupo de personas que manifiesta no poseer algún tipo de certificación.	-18%
Presupuestos de Seguridad	
➡ Sólo el 25% de los encuestados manifestó no conocer o contar con la información acerca de los montos asignados a la seguridad.	-17%
➡ Este año solamente el 12% reconoce que sus inversiones, en materia de seguridad de la información, están entre el 0% y el 2% de los presupuestos de la organización, comparados con el 26% del año 2015. Es interesante ver la tendencia de contemplar un recurso financiero suficiente para una inversión, frente a la protección de la información.	-14%
➡ Este año, sólo el 12% de los encuestados reconoce que sus presupuestos asignados para la protección de la organización, están por debajo de los US$20.000 dólares americanos.	-14%
Políticas de seguridad	
➡ Para este año, sólo el 42% de los encuestados reconoce que la organización posee formalmente una política de seguridad	-17%
Regulación digital	
➡ Esteaño el 22% de los encuestados manifiesta no estar sujeto a regulación de ningún tipo.	-16%
Incidentes de seguridad	
➡ Este año el incidente instalación de software autorizado, sólo se registro en el 38% de los encuestados.	-13%

encuestados afirmaba que ese era el valor del presupuesto. Por último, un 12% de los encuestados afirma que el presupuesto de seguridad asignado para el año 2015 estaba por debajo de los $US 20.000 dólares americanos. Al comparar con los datos de períodos anteriores, el 25% de los encuestados manifestaba que sus presupuestos asignados estaban en esos rangos. Así las cosas y frente a las tendencias mundiales, tenemos organizaciones más comprometidas con las inversiones en seguridad de acuerdo con las tendencias internacionales. Según la firma PwC[5], el promedio de los presupuestos en seguridad crece en un 24%. De igual manera, al revisar la información del informe de seguridad realizado por la firma ISMG[9], el 57% indica que sus presupuestos cambiarán y aumentarán y, el 34%, afirma que se mantendrán estables. En Colombia, el crecimiento de los presupuestos asignados para este año, está un 4% por encima de los $US130.000 dólares americanos.

5. Este año solo el 42% de los encuestados reconoce tener una política escrita, aprobada por la dirección e informada a todo el personal, comparado con el período anterior, en que el 60% de los encuestados reconoció esta realidad. Se observa lo contrario en la formalidad de los procesos de seguridad de la información en las organizaciones, si se reconoce la necesidad por entender la seguridad pero, sin el formalismo que requiere. Tendencia que a nivel global se mantiene igual como se ve en el informe de Ernst & Young que indica que la madurez de sus encuestados en este tema es baja. El informe describe que las organizaciones reconocen la seguridad, además de entender los riesgos de la ciberseguridad como un factor clave, pero se ven poco maduras en el sostenimiento de un *framework* de políticas y están-dares que le ayuden en la construcción de un modelo de gobierno y gestión alrededor de la seguridad. Una realidad muy similar es la que plantea la encuesta de seguridad realizada en el Reino Unido, donde el 72% de los encuestados considera la madurez de sus políticas y *frameworks* de seguridad no adecuados, y sólo un 26% considera maduras sus políticas de seguridad de la información. Así las cosas, es necesario que las organizaciones refuercen y redoblen sus esfuerzos por mantener sus políticas de seguridad y *frameworks*, como parte de sus elementos claves en materia de protección de la información.

6. Resulta interesante este año observar que en la realidad nacional sólo el 22% de los encuestados manifiesta no estar sujeto frente a una regulación o normativa, en términos de seguridad de la información, comparado con el año anterior, en que el 38% de los encuestados manifestó no estar sujeto. La interpretación para la realidad nacional es ver cómo las organizaciones van entendiendo de una mejor manera su contexto y cómo las regulaciones nacionales o internacionales les permiten tener una visión en lo relacionado con la seguridad de la información. Marcos normativos como la Ley 1581 o de protección de datos personales, la Ley 1712 o Ley de transparencia, así como el nuevo CONPES de ciberseguridad, son marcos que ponen de manifiesto una atención plena en las organizaciones, frente a los actuales escenarios tan exigentes, relacionados con los riesgos en entornos cibernéticos.

Lo nuevo

Esta sección contempla los nuevos ítems de esta versión de la encuesta; en este año no se incluyen sino opciones nuevas dentro del cuerpo de preguntas existentes.

A continuación se relacionan por categoría los ítems incluidos, y las gráficas muestran los resultados de las opciones adicionadas.

La sección de demografía contempla:

1. En la pregunta relacionada con los roles de seguridad de la información se agregan dos nuevas opciones, con el fin de poder saber con mayor precisión el tipo de roles que las organizaciones han venido implementando en relación con la protección de la información. Estos son:

a. Analista de seguridad de la información
b. Analista de seguridad informática

2. En la pregunta relacionada con la responsabilidad en materia de seguridad de la información, se agrega una opción, como resultado del estudio del 2015, donde se evidenció la necesidad de incluirla.

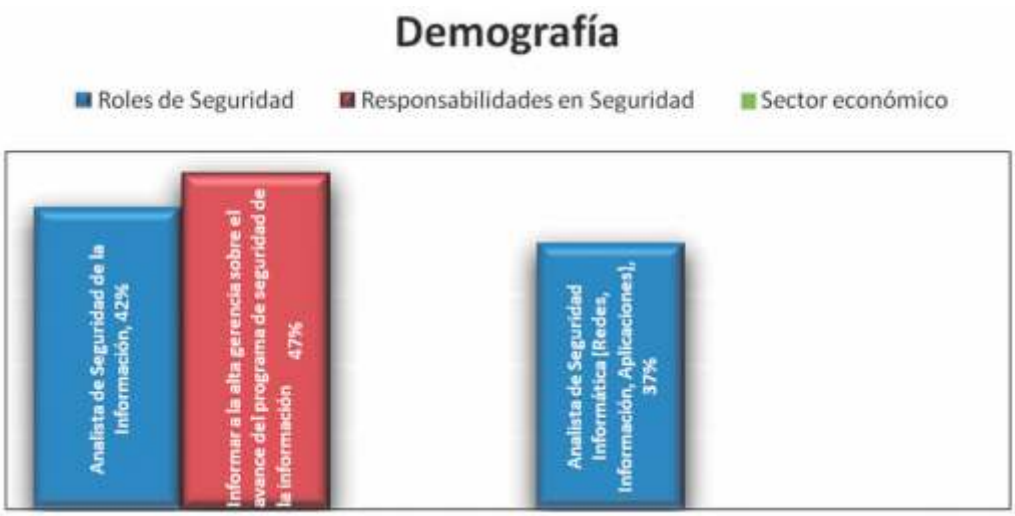
a. Informar a la alta gerencia sobre el avance del programa de seguridad de la información.

3. Por último, en la pregunta relacionada con los sectores económicos, se adiciono una opción.

a. Sector de Retail / Consumo masivo.

En el grafico 5, están representados los valores obtenidos este año en estos temas.

En la sección de fallas de seguridad, se incluyo la opción de *Ransomware*, como lo evidencian las tendencias mundiales de amenazas y los informes de amenazas de Cisco [2], Forcepoint



Gráfica 5. Demografía

[3], IBM [3]. Forcepoint[3], estima que el negocio alrededor del Ransomware está en $US325 millones de dólares.

Cisco Security [2], considera el *Ransomware* como una tendencia de anomalías que debe ser entendida y abordada. Los datos de Cisco revelan que Angler, en un 60% de su distribución, contenía algún tipo de *Ransomware* y los ingresos totales por tal concepto son cercanos a los $US34 millones de dólares.

En el caso de Colombia se tienen los siguientes datos.

Gráfico 6. Fallas de Seguridad

Se quiso evaluar la presencia del malware tipo *Ransomware* dentro del conjunto de incidentes de seguridad en las empresas y, efectivamente, se confirma la tendencia mundial de considerarlo como una de las anomalías presentada en nuestra realidad, con un 17%. Con ello se confirma que las tendencias se aplican de manera global y no discriminan regiones ni horizontes.

En la sección de herramientas y prácticas de seguridad, se incluyó un mecanismo nuevo que está siendo utilizado en la industria y son los servicios de inteligencia de amenazas [3], en donde algunas organizaciones van más allá de un SIEM y los proveedores han construido a través del aprendizaje y el Big Data, modelos más inteligentes para la detección de las amenazas de la organización

Gráfico 7. Herramientas y prácticas de seguridad.

Así las cosas, la realidad nacional identificó en un 11% que sí es utilizado este mecanismo de control como una alternativa válida para la detección temprana en pro de la prevención, mejorando así sus ambientes reactivos y permitiendo conocer de una mejor manera a sus adversarios digitales.

En la sección de políticas de seguridad de la información se agregaron las siguientes opciones.

En la pregunta relacionada con los obstáculos para lograr una adecuada seguridad de la información:

a) Ausencia o falta de cultura en seguridad de la información.
b) Escasa formación en gestión segura de la información.

En la pregunta relacionada con los tipos de metodologías de gestión de

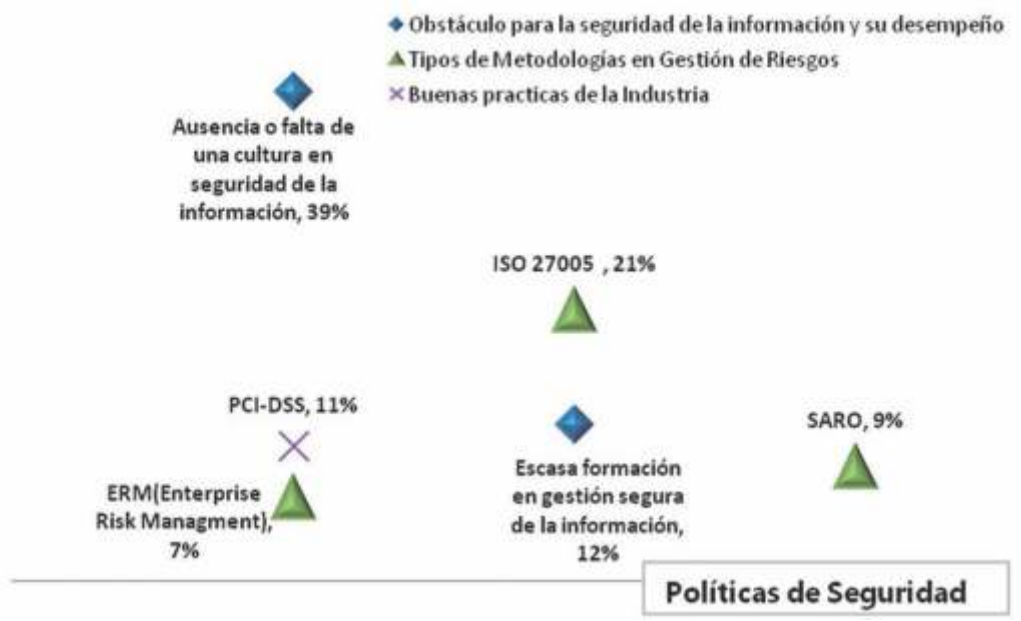


Gráfico 8. Políticas de Seguridad

riesgos se incluyeron las siguientes opciones:

a) ISO 27005
b) SARO
c) ERM

Por último, en la pregunta relacionada con la utilización de buenas prácticas en materia de seguridad de la información se incluyó, la siguiente opción:

a) PCI-DSS

Estas opciones deciden incluirse luego del estudio realizado año anterior, donde se evidenció que encontraban identificadas por los participantes como otras alternativas.

La Gráfica 8,muestra los resultados de los tres elementos incluidos.

Los resultados son los siguientes:

1. Obstáculos para el desempeño de la seguridad de la información en la organización, reflejada en un 39% de las respuestas de los encuestados. Además de la escasa información en gestión segura de la información.

2. Tipos de metodologías en materia de gestión de riesgos. En ella se incluyeron ISO 27005(21%), SARO (9%) y ERM (7%) como nuevos mecanismos utilizados por las organizaciones para realizar sus ejercicios de gestión de riesgos. Los datos muestran que ISO 27005 e ISO 31000 son los utilizados por las organizaciones en Colombia en la identificación de sus riesgos en materia de seguridad de la información.

3. Buenas prácticas de la industria. En este ítem se incluyó a PCI-DSS como parte del conjunto de opciones, teniendo como resultado que el 11% de los encuestados lo usa frecuentemente

como conjunto de buenas prácticas, en materia de protección de la información.

La sección de capital intelectual contempla los siguientes elementos:

Sobre las certificaciones de los profesionales de seguridad:

a) Auditor ISO 27001 (Líder y/o Interno)
b) CEH (Certified Ethical Hacker)
c) CSX – Cybersecurity Nexus

La Gráfica 9, muestra que hoy la certificación de Auditor Líder/Interno ISO 27001 es tenida por los profesionales de seguridad con un 44% de aceptación. A la pregunta de si sería importante esta certificación para el desarrollo de las funciones de seguridad, un 57% considera que sí es así y que por tanto es deseable que los profesionales la tengan.

El otro ítem evaluado es la certificación CEH (Certified Ethical Hacker), hoy el 26% de los encuestados manifiesta poseer dicha certificación; el 46% considera que debería tenerla para el desarrollo de las funciones de seguridad de la información.

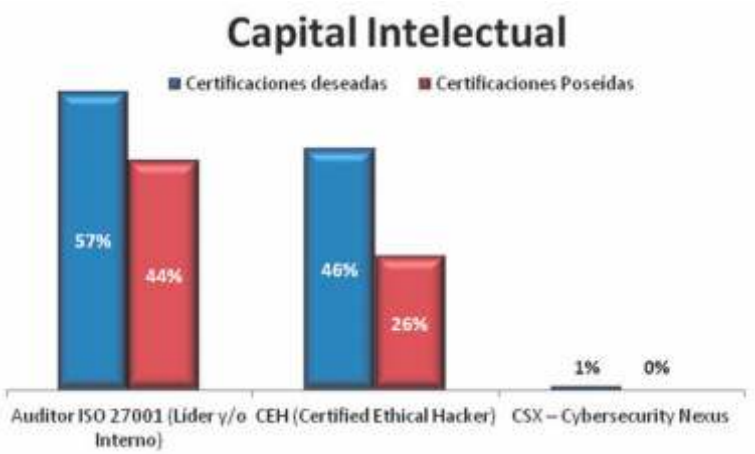
Por último, está la más reciente certificación creada para atender los temas de ciberseguridad de ISACA CSX (Cyber Security Nexus); en la actualidad, los participantes no poseen dicha certificación, pero el 1% sí considera que se debería tener, para poder desempeñar las funciones de seguridad en la organización.

Tendencias

Variaciones en tipos de incidentes

La gráfica10 muestra las variaciones de los tipos de anomalías que se manejan y cómo han evolucionado desde el año 2014, hasta la fecha. Dentro de la gráfica hay tres datos interesantes:

1. El *Ransomware* como una de las anomalías.



Gráfica 9. Capital Intelectual

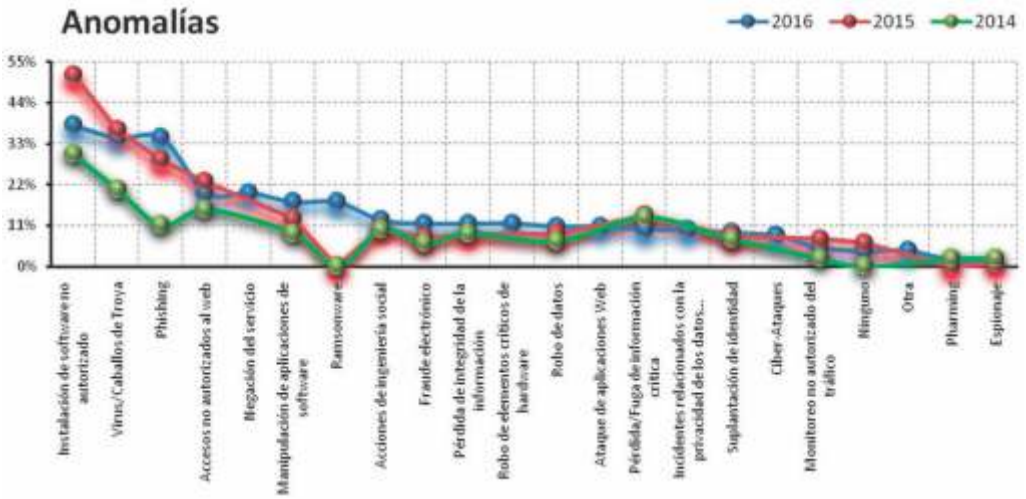


Gráfico 10. Anomalías

2. La disminución frente al año anterior, de la instalación de *software* no autorizado, mostrando que las organizaciones han mejorado los controles, con relación a este tipo de prácticas.

3. Continúa el crecimiento del *Phishing*, como una de las anomalías más usadas, inclusive para este año, ratificando con ellas las tendencias mundiales como una de las técnicas de ataque más común en la actualidad.

Herramientas de protección

En la gráfica11, se muestra la evolución de los mecanismos de protección y su revisión con el año inmediatamente anterior. Vale la pena señalar los siguientes puntos:

1. Siguen siendo las soluciones *AntiMalware*, sistemas de contraseñas, Vpns, y *firewalls* tradicionales, los mecanismos de control más usados en la realidad nacional.

2. Hay una disminución frente al año anterior de los mecanismos estándar.

3. Existe un crecimiento en ciertas tecnologías. Entre ellas, los sistemas biométricos; los SIEM como herramientas integrales de monitoreo; los *firewall* de bases de datos que su crecimiento se puede relacionar con la aplicación de los marcos regulatorios nacionales; las herramientas Anti-DDOS, toda vez que estos tipos de ataques están dentro del conjunto de ataques retadores en su control. Y por último, los ciberseguros, una tendencia que sigue emergiendo como mecanismo frente a las ciberamenazas a las que las organizaciones se enfrentan en su día a día.

En resumen, la seguridad de la información exige un enfoque multidimensional para ver desde todas las aristas, no sólo las técnicas a la protección de la información como un instrumento que le permita a la organización avanzar de una manera más consistente en los nuevos entornos

Gráfico 11. Mecanismos de protección.

digitales, sino tener en cuenta su permanente transformación. De esa forma, los riesgos y amenazas que van mostrando las nuevas realidades, llevan a las organizaciones a proteger su recurso más valioso, la información.

Conclusiones

1. Se sigue afianzando la transformación de paradigmas de la seguridad de la información en las organizaciones y su relación con los directivos de las mismas, las juntas directivas cada vez más se involucran y participan en la toma de decisiones. Esto se ajusta a la realidad mundial sobre los temas que se encuentran en el radar de los ejecutivos. Así mismo, encontramos más CISO's con capacidades de venta y de lenguaje, en torno a los riesgos. Son catalizadores para hacer entender los temas de la seguridad en los directivos de la organización.

2. Dentro de la encuesta se indaga sobre la conciencia de los directivos y su nivel de involucramiento y responsabilidad a la hora de participar en las tomas de decisiones con relación a la seguridad. Por tal razón, se adapta la matriz de Covey [1], para relacionar las dos variables identificadas con la responsabilidad y compromiso de las

altas direcciones, en materia de seguridad de la información, como lo muestra la Gráfica 12.

En el eje X se encuentra representado el compromiso de la alta dirección, y en el eje Y está identificada la responsabilidad de la alta dirección, seguido de esto están las zonas definidas las cuales representan los siguientes conceptos:

Zona de rendimiento y resiliencia de la seguridad, donde el compromiso y la responsabilidad de la alta dirección son altas. En esta zona se ha identificado que los directivos de la organización están involucrados en la toma de decisiones relacionadas con los riesgos asociados a la protección de la información.

Zona de Supervivencia de la seguridad, donde el compromiso es bajo y la responsabilidad alta. En esta zona la alta dirección atiende y entiende las recomendaciones en materia de protección de la información, y, si bien no se involucra, sí tiene claro que es necesario entender los riesgos en materia de seguridad de la información.

Zona de fatiga de la seguridad: en esta zona hay un bajo compromiso y baja responsabilidad de la alta dirección con relación a la seguridad de la información y los riesgos involucrados. La alta dirección no se involucra en los procesos y toma de decisiones sobre la protección de la información.

Zona de receptividad de la seguridad: En esta zona hay baja responsabilidad y alto compromiso por parte de las altas direcciones de las organizaciones. En esta zona las altas direcciones lo que hacen es delegar las responsabilidades a otros, pero sí esperan ser informados de lo que sucede en mate-

Gráfica 12. Diagrama de Covey adaptado

Gráfica 13. Matriz de Conciencia de la Seguridad.

ria de la seguridad y cómo se avanza en este tema.

La Gráfica 13 muestra las variaciones entre el estudio de 2015 y este de 2016:

3. Seguimos en el camino de entender la seguridad de la información como un mecanismo para asegurar la organización. En esta visión existen aproximaciones para entenderla como un orientador de negocio. No obstante, algunos todavía ven en la seguridad de la información sólo herramientas y tecnologías de apoyo.

4. Los temas emergentes como la ciberseguridad y mecanismos como los ciberseguros son herramientas y contextos que hacen más complejo el ambiente de protección de las organizaciones. Los sucesos no sólo mundiales, sino regionales y locales, acrecientan los vectores de trabajo de los responsables de seguridad, los cuales deben propender por mantener en niveles adecuados, el ambiente de incertidumbre en el que las organizaciones hoy conviven.

5. Por otro lado, también se entienden las nuevas anomalías, entre ellas el *Ransomware*, como un desafío que debe ser analizado y visto de manera cuidadosa, toda vez que este entorno cada vez más volátil, incierto, complejo y ambiguo requiere de mayor observación, atención y capacidad de entender de manera profunda las interrelaciones corporativas y lo selectivo que puede llegar a ser un adversario digital.

6. Las regulaciones nacionales e internacionales son mecanismos que apoyan el fortalecimiento de los sistemas de gestión de seguridad de la información. Hoyexisten en Colombia normativas como la regulación en los sectores financieros y la ley de protección de datos personales. Las regula-

ciones internacionales inclinan la balanza hacia la seguridad de la información y nos enfrentan a un panorama todavía denso, en materia de ataques informáticos.

7. Los estándares internacionales de la industria se ven reflejados en Colombia en las buenas prácticas en seguridad de la información, De ahí que ISO 27000, ITIL y Cobit se consoliden como marcos para construir arquitecturas de seguridad de la información. Por otro lado, los participantes reflejan con énfasis la necesidad de utilizar algún marco de referencia, que les permita construir modelos adaptados a las necesidades de las empresas.

Referencias

[1] Los cuatro cuadrantes de Stephen Covey. http://www.zetasoftware.com/2015/02/administracion-del-tiempo-los-4-cuadrantes-de-stephen-covey/ .

[2] 2016 Global Threat Report Forcepoint. https://www.forcepoint.com/resources/whitepapers/forcepoint-2016-global-threat-report

[3] CISCO 2016. Informe anual de seguridad. http://globalnewsroom.cisco.com/es/la/press-releases/informe-anual-de-seguridad-de-cisco-revela-una-dis-1239705

[4] IBM X-Force Threat Intelligence Report 2016. https://securityintelligence.com/media/xforce-tir-2016/

[5] The Global State of Information Security® Survey 2016. *Turnaround and transformationinCybersecurity.* http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html

[6] The Global Economic Crime® Survey 2016.Adjusting the Lens on Economic Crime. http://www.pwc.com/gx/en/services/advisory/consulting/forensics/economic-crime-survey.html

[7] Information Security Maturity Report 2015 Current information security practice in European organizations. http://clubciso.org/quotable-statistics/

[8] State of Cybersecurity implications for 2016 An ISACA and RSA Conference. http://www.isaca.org/pages/cybersecurity-global-status-report.aspx

[9] 2016 Enterprise Security Study How Prepared Is Your Organization to Defend againsttoday's Advanced Threats? Information Security Media Group. http://www.bankinfosecurity.com/whitepapers/2016-enterprise-security-study-w-2499
http://www.isaca.org/pages/cybersecurity-global-status-report.aspx

**Realizada por la Asociación Colombiana de Ingenieros de Sistemas (Acis).*

Andrés Ricardo Almanza Junco, M.Sc. CISM, ITIL, ISO 27001, LPIC1. *Ingeniero de Sistemas, universidad Católica de Colombia. Especialista en Seguridad de Redes de la Universidad Católica de Colombia. Máster en Seguridad Informática de la Universidad Oberta de Cataluña, España. Codirector de las JornadasInternacionales de Seguridad Informática. Coordinador en Colombia de la Encuesta Nacional de Seguridad Informática. Coordinador del grupo CISO's-COLy CISO's-LATAM en Linkedin.*