No. 139 Abril - Junio 2016 ISSN 0120-5919

SISTEMAS

Tarifa Postal Reducida Servicios Postales Nacionales S.A. No. 2016-186 4-72, vence 31 de Dic. 2016

Fraude informático: viejos trucos, nuevos entornos

ACIS
ASOCIACIÓN COLOMBIANA DE INGENIEROS DE SISTEMAS
Calle 93 No. 13 - 32 of. 102
Bogotá, D.C.
www.acis.org.co

UNIVERSIDAD EAN

CON ACREDITACIÓN INSTITUCIONAL DE ALTA CALIDAD

Formamos gerentes con capacidades para **liderar procesos** tecnológicos de información y comunicación, desarrollando competencias para la **innovación y definición de la estrategia tecnológica en las organizaciones.**

Maestría en Ingeniería de Procesos
Metodología Presencial
Con opción de doble titulación internacional:
Universidad EAN / Institut Supérieur de Gestion- ISG, Paris - Francia.
Código SNIES No. 102408 con Registro Calificado.

Maestría en Gerencia de Sistemas de Información y Proyectos Tecnológicos
Metodología Virtual
Código SNIES No. 104320 con Registro Calificado.

Especialización en Gerencia de Tecnología
Metodología Presencial
Código SNIES No. 1985 con Registro Calificado.

Carrera Profesional en Ingeniería de Sistemas
Acreditación de Alta Calidad otorgada por el Ministerio de Educación Nacional.*
Metodología Presencial y Virtual
Código SNIES No. 1984, 102139 con Registro Calificado.

* Aplica para el programa en metodología presencial.

FORMANDO EMPRENDEDORES
CREADORES DE EMPRESAS SOSTENIBLES

INSCRIPCIONES ABIERTAS
universidadean.edu.co

Centro de contacto en Bogotá: +(57-1) 593 6464
Línea gratuita nacional: 01 8000 93 1000
e-mail: informacion@universidadean.edu.co
Cl. 79 Nº. 11 - 45 El Nogal, Bogotá D.C. Colombia, Suramérica

Acreditación de la Engineering Accreditation Commission (EAC) de ABET a Ingeniería de Producción Metodología Presencial.
www.abet.org

ABET Engineering Accreditation Commission

ACBSP ACCREDITED

En esta edición

Publicación de la Asociación Colombiana de Ingenieros de Sistemas (ACIS)
Resolución No. 003983 del Ministerio de Gobierno
Tarifa Postal Reducida Servicios Postales Nacional S.A. No. 2016-186 4-72
ISSN 0120-5919
Apartado Aéreo No. 94334
Bogotá D.C., Colombia

Abril-Junio 2016
Calle 93 No.13-32 Of. 102
Teléfonos 616 1407 – 616 1409
A.A. 94334
Bogotá D.C.
www.acis.org.co

Globaltek Security

Conference 2016

Cybersecurity

Big Data

SOC - SaaS

EH - Pentesting

Risk Management

Si Ud. es el responsable por la Seguridad de la Información en su Organización, lo invitamos a estar pendiente del GLOBALTEK SECURITY CONFERENCE 2016, el evento de Seguridad en el mes de Octubre que reúne conferencias y conferencistas de primer nivel.

Busque información detallada y registrese tempranamente en nuestro sitio web http://www.globalteksecurity.com para compartir con colegas y profesionales del medio, una interesante jornada académica sobre tendencias y novedades de la industria.

www.globalteksecurity.com

Fraude informático: generoso caldo de cultivo

Enfrentarlo, se convierte en una tarea exigente y de visión multidisciplinar.

Jeimy J. Cano M., Ph.D, Ed.D(c), CFE

El fraude informático es una realidad multidimensional que afecta a todos los participantes de la sociedad. Su capacidad de adaptación y reinvención en contextos digitales, le permite asumir distintas formas y aproximaciones de tal manera que, establecer esquemas referentes para enfrentarlo, resulta una tarea exigente y de visión multidisciplinar.

En este sentido, la identificación y atención de patrones emergentes como la intersección de malas prácticas de las personas, las debilidades de seguridad y control en los procesos, las fallas o vulnerabilidades técnicas de las tecnologías de información, así como las limitaciones legales para actuar cuando corresponde, deben motivar el desarrollo de habilidades en los profesionales antifraude, para enfrentar el caldo de cultivo generoso y siempre fresco que crea esta realidad, donde la inevitabilidad de la falla y la creatividad de la mente criminal

tienen un sitio preferente donde operar.

De ahí que esta edición de la revista se ocupe de examinar el desafío del fraude informático, para motivar reflexiones conceptuales y prácticas conectadas con la realidad actual de los individuos y las organizaciones, en Colombia y en el mundo.

Dentro de ese contexto, el ingeniero Juan Carlos Reyes, columnista invitado, plantea sus análisis desde la cotidianidad del fraude y las encrucijadas actuales en un mundo digitalmente modificado e hiperconectado, en el que el sentido común que suele ser el menos común de los sentidos –valga la redundancia-, debe ser la práctica más habitual para hacernos más resistentes a las estrategias de los delincuentes.

A nivel internacional, la Asociación de Examinadores Certificados de Fraude (en inglés *Association of Certified Fraud Examiners* –ACFE-) es la entidad global que ofrece un cuerpo de conocimiento destinado a la lucha contra el fraude, en todas sus formas. En tal sentido, la entrevista realizada a la doctora Muna Dora Buchahin Abulhosn, fundadora y vicepresidente de la ACFE, Capítulo México, ilustra la dinámica del fraude informático en una dimensión internacional, así como los retos que deben encarar los especialistas antifraude en el reconocimiento y control de este tipo de conductas, en Latinoamérica y el mundo.

De manera complementaria, el ingeniero y magíster Andrés Almanza, continuando con la tradición de la Asociación Colombiana de Ingenieros de Sistemas –ACIS-, de ofrecer a la comunidad estadísticas neutrales y académicas en temas relevantes para el gremio y la nación, presenta los resultados de la XVI Encuesta Nacional de Seguridad Informática -ENSI-16-, basada en el conocimiento adquirido a lo largo de años de compilación y análisis de información, nos muestra las tendencias y los retos frente a las amenazas emergentes en la protección de la información, en la dinámica del contexto colombiano.

Teniendo en cuenta que el fraude informático es una problemática multidisciplinar, el foro que habitualmente se realiza para cada número de la revista, contó con la participación de la academia y la consultoría, profesionales especialistas en estos asuntos. El diálogo planteado por los abogados, los contadores públicos y los ingenieros de sistemas, sobre la realidad de fraude en el contexto digital, establece una postura integral que procura, no sólo ver los resultados de las actividades ilegales, sino el alcance de la conducta criminal que, asistida por la tecnología, crea una realidad que engaña y compromete millonarios recursos financieros que afectan tanto a las organizaciones como a la nación misma.

Finalmente, se presentan dos artículos que buscan explorar y conceptualizar la problemática del fraude informático.

Por un lado, el ingeniero y magíster Joshua González, profesor de la Universidad de los Andes, detalla las diferencias entre el cibercrimen, el fraude y otras conductas delictivas en el terreno digital, como funda-

mento para comprender las estrategias de seguridad y control inmersas en la dinámica de la inevitabilidad de la falla, en el contexto de las organizaciones a nivel nacional e internacional.

Por otra parte, este servidor, plantea un análisis del fraude informático como una realidad emergente, resultado de la interacción del tejido digital interconectado, disponible en una sociedad de la información y el conocimiento, para lo cual propone el pensamiento de sistemas como aproximación epistemológica, con el fin de motivar acciones convergentes orientadas a detectar y procesar conductas contrarias al ordenamiento jurídico y social, sobre plataformas de productos y/o servicios digitalmente modificados.

En resumen, cada uno de los contenidos planteados en este número de la revista representan una posibilidad de encuentros y desencuentros con la realidad del fraude informático, como quiera que esta actividad plantea en sí misma posturas enfrentadas, que generan tensiones entre los participantes de la dinámica social: personas, procesos, tecnología y supervisores, las cuales revelan la esencia misma de la pertinencia del tema, en medio de un mundo volátil, incierto, complejo y ambiguo.

***Jeimy J. Cano M., Ph.D, Ed.D(c), CFE**. Ingeniero y Magister en Sistemas y Computación por la Universidad de los Andes. Ph.D in Business Administration por Newport University, Especialista en Derecho Disciplinario por la Universidad Externado de Colombia y candidato a Doctor en Educación por la Universidad Santo Tomás. Cuenta con un certificado ejecutivo en gerencia y liderazgo del MIT Sloan School of Management, MA, USA. Profesional certificado como Certified Fraud Examiner (CFE) por la Association of Certified Fraud Examiners y Cobit5 Foundation Certificate por ISACA. Director de la Revista SISTEMAS de la Asociación Colombiana de Ingenieros de Sistemas – ACIS.*

XXXVI SALON DE INFORMÁTICA 2016
EMPRENDIMIENTO E INNOVACIÓN EN TI

LLAMADO A CONFERENCISTAS Y TRABAJOS

CUANDO	Octubre 27-28 de 2016
Formato de entrega	Contenido de la charla o ponencia en formato libre, incluyendo un resumen de la hoja de vida del conferencista
FECHA LÍMITE DE PRESENTACION DE PROPUESTAS	Agosto 1
Informe del Comité Académico	Septiembre 1
Entrega de la versión definitiva	Octubre 1

Objetivos

Este XXXVI Salón de Informática de ACIS, tiene por objetivos principales: 1) fortalecer las capacidades en emprendimiento e innovación del gremio, con miras a responder a los retos actuales de la economía nacional; 2) presentar casos y experiencias que ilustren a los asistentes con ejemplos de la realidad nacional, 3) contribuir a la divulgación de las oportunidades y políticas gubernamentales, orientadas al sector de TI, y 4) servir de foro de discusión de las temáticas relevantes al gremio y servir de canal de comunicación y transmisión de las mismas a los entes participantes.

Contenido

La charla o ponencia propuesta debe enmarcarse en temáticas directamente relacionadas con el emprendimiento y la innovación en las organizaciones:

- ¿Cómo lograr la innovación en las organizaciones actuales?
- Inhibidores de la innovación
- Mecanismos de apoyo a la innovación organizacional
- Retos y problemas típicos que enfrentan los emprendedores
- ¿Cómo convertir la innovación en emprendimiento?
- ¿Cómo preparar/adaptarse al mercado?
- ¿Cómo innovar con una estrategia digital para la organización?
- Perfil / Fórmula del emprendedor
- Oportunidades para los emprendedores en los ODS: objetivos de desarrollo sostenible.
- Emprendimiento social con TI
- Casos y ejemplos de enfoques
- Foro: economía del posconflicto en Colombia y oportunidades de emprendimiento en TI
- Foro: teoría y práctica en las oportunidades para los emprendedores nacionales

Fraude informático: preguntas y respuestas con Muna Dora Buchahin Abulhosn

Mencionar su nombre significa indagar entre los "pesos pesados" del fraude en el ámbito de las tecnologías de la información y las comunicaciones. A ella nada se le escapa.

Sara Gallardo M.

A Muna Dora Buchahin Abulhosn, abogada y doctora en Derecho, entrevistadora forense certificada, especialista en anticorrupción, conferencista por todo el mundo, perito auxiliar en Criminología del Tribunal Superior de Justicia del Distrito Federal en México, con todas las acreditaciones internacionales posibles, docente y autora del libro "Auditoría forense, delitos contra la administración pública", no le cabe un título más en su hoja de vida. Son tantos, que citarlos todos le quitaría espacio a la esencia de esta entrevista: compartir con los lectores su conocimiento y vasta experiencia al frente de 450 auditorías en los ámbitos público y privado y en más de 243

dictámenes de casos presentados ante autoridades penales y administrativas en México, país donde reside y es testigo de su arduo trajinar por los laberintos de la seguridad de la información.

La más reciente noticia en su laureado camino es el premio ACFE: "*Certified Fraud Examiner of the Year Award 2016*", entre los Certified Fraud Examiner – CFE-, Examinador Certificado de Fraude, de 208 capítulos en el mundo.

Semejante perfil, no podía producir nada distinto a una serie de respuestas al cuestionario enviado por correo electrónico, acompañadas de cifras, gráficos y conceptos.

Revista Sistemas: ¿Cuál es la definición que motiva el actuar de un profesional certificado en fraude?

Muna Dora Buchahin Abulhosn: es un especialista en la prevención, detección, disuasión y la investigación de fraude ocupacional, entendido como *el uso de la propia ocupación para el enriquecimiento personal, a través del mal uso o el uso indebido de los recursos o activos de la organización, con la intencionalidad de cometer un acto ilícito.* El "Manual del Examinador" lo define como: "... todos aquellos medios complejos que el ingenio humano puede concebir y a los que recurre un individuo para sacar ventaja de otro, por medio de falsas sugerencias o por supresión de la verdad. Incluye toda sorpresa, truco, astucia u ocultamiento, y cualquier forma injusta por la que el otro es engañado". Por lo tanto, el entorno y la importancia de su actividad lo obligan a una actualización permanente para acreditar su *experticia*, las competencias y las habilidades forenses para cualquier tipo de investigación como especialista antifraude. Su actuación se rige con los más altos estándares de ética, conocimiento y experiencia que contemplan el dominio de diversas técnicas forenses, dado que el examinador de fraudes certificado (CFE) se integra en cualquier organización pública o privada, independientemente de las distintas regulaciones legales a cada país.

RS: ¿Desde su experiencia, cuáles son los fraudes informáticos más comunes?

MDBA: los más recurrentes se vinculan con el llamado "robo de identidad" en sus diversas modalidades. A través de diferentes mecanismos como el envío de correos spam, donde se le solicita al destinatario con

un correo engañoso, acceder a una liga de un sitio "conocido seguro" (el cual en realidad es una copia del original), y cuyo propósito es que el usuario ingrese datos personales (usuario, contraseña, número de tarjeta bancaria, etc.), para que éstos sean robados y utilizados posteriormente para fines ilícitos, entre ellos el mercado negro o el robo o retiro de dinero de cuentas bancarias.

También sucede que a través del envío de correo spam, se puede anexar un archivo electrónico, de tipo PDF o video o cualquier otro de uso común. Una vez que el destinatario lo abre, puede descargar un archivo (*malware*) que se instala en la computadora y una vez instalado, puede estar enviando toda la información que el usuario teclea cuando visita sitios específicos, entre los más comunes referidos a bancos.

La sofisticación de las técnicas de los defraudadores para lograr mayor impacto en sus objetivos, es permanente. Existe una variación denominada *spear-phishing*, la cual realiza envíos de correos a personas específicas (está dirigido al ataque) y son envíos de remitentes o empresas que seguramente conoce el destinatario. Ante este escenario, es fácil que la víctima crea como válido el correo y proporcione la información solicitada, ingresando a las ligas que se indican en el correo o descargando un archivo puntual. El uso indebido de los datos personales es ahora un riesgo universal inminente, en un potencial mundo de fraudes cibernéticos que ha afectado a gran número de organizaciones y ciudadanos.

RS: ¿El ambiente de la tecnología móvil, la nube y otros desarrollos similares han hecho crecer el fraude?

MDBA: en el mundo globalizado se atrae el lado oscuro de los delitos cibernéticos. Según datos del *Informe 2016 de "Ciberseguridad: ¿Estamos preparados en América Latina y el Caribe?,* publicado por el Banco Interamericano de Desarrollo (BID), de una población de 125 millones de habitantes en México, el 44% tiene acceso a internet (55 millones de personas), terreno abonado para el desarrollo colectivo, al generar comunicación y mayor información en tiempo real. Pero, son mayores los riesgos tanto para los usuarios como para las empresas, por la vulnerabilidad de los sistemas operativos de los dispositivos móviles (Android, IOs o Microsoft), y de programas que pueden robar información y transmitirla para fines ilícitos.

Los modelos de servicios en la nube, entre los que se cuentan: *Software como Servicio (Software as a service – SaaS-); Plataforma como servicio*

(Platform as a Service –PaaS-) o *Infraestructura como Servicio (Infrastructure as a Service –IaaS-),* también han presentado vulnerabilidades que los delincuentes informáticos han explotado. Muchas de ellas, por el descuido del usuario al dejar sesiones remotas abiertas o accediendo desde redes no seguras, lo cual es aprovechado para accesos no autorizados y robos de información.

RS: ¿Qué tipo de entrenamiento deben tener las personas y empresas para enfrentar el fraude informático?

MDBA: desde el más alto nivel organizacional, resulta imprescindible implementar una cultura de seguridad de la información, comunicar y sensibilizar a todo el personal en línea vertical y horizontal, y no estrictamente en el sentido de "seguridad informática", sino incluir una sensibilización permanente, vinculada en las distintas áreas y con un protocolo de alerta a los posibles riesgos y vulnerabilidades, en caso de un incidente o contingencia.

La capacitación debe centrarse en modelos de seguridad de la información y normas internacionales que permitan seguir un marco de referencia, como las ISO/IEC 27001 (estándar para la implementación de un sistema de gestión de la seguridad de la información), ISO 27017 (estándar para la aplicación de controles de seguridad de información en sistemas o servicios basados en computación en nube) e ISO 27032 (Guía sobre ciberseguridad), por mencionar algunas.

Es muy importante mantener comunicación constante interna entre el personal de la organización, para conocer la recurrencia y los *modus operandi* de los fraudes informáticos. Esto servirá como insumo para actualizar las políticas de seguridad o configuraciones específicas de sistemas o la infraestructura de la organización. Estas actualizaciones deben ser permanentes y alineadas a la organización.

Debo decir que en México existen grandes oportunidades de trabajo para aquellos jóvenes que deciden estudiar estas carreras profesionales, y que hay escasez de personal en esta materia. Se asegura un futuro promisorio y lleno de actividad intensa para los talentos.

Siga la entrevista completa en el siguiente link:
http://acis.org.co/portal/content/entrevista-muna-dora-buchahin-abulhosn

Sara Gallardo M. *Periodista comunicadora, universidad Jorge Tadeo Lozano. Ha sido directora de las revistas "Uno y Cero", "Gestión Gerencial" y "Acuc Noticias". Editora de Aló Computadores del diario El Tiempo. Redactora en las revistas Cambio 16, Cambio y Clase Empresarial. Autora del libro "Lo que cuesta el abuso del poder". Ha sido corresponsal de la revista Infochannel de México y de los diarios "La Prensa" de Panamá y "La Prensa Gráfica" de El Salvador. Investigadora en publicaciones culturales. Gerente de Comunicaciones y Servicio al Comensal en Andrés Carne de Res, empresa que supera los 1800 empleados; corresponsal de la revista IN de Lanchile. En la actualidad, es editora en Alfaomega Colombiana S.A., firma especializada en libros universitarios y editora de esta revista.*

Reflexiones sobre el fraude personal y corporativo

El nuevo mundo interconectado genera tension en términos de seguridad y los controles terminan siendo los más simples, guiados por el sentido común.

Juan Carlos Reyes M.

El vocablo latino *fraus* es aquel de donde deriva la palabra fraude, y su significado más simple es el de la "acción que resulta contraria a la verdad y a la rectitud".

Partiendo de esta sencilla pero completísima definición, se ha desarrollado una impresionante cantidad de prefijos para indicar de qué manera se puede cometer cada tipo de fraude, hasta llegar a uno de los más recientes que es el anglicismo *ciber*, generalmente utilizado para referirse a lo que comprende el mundo digital de los sistemas de información, incluso el internet.

Podríamos señalar que es de esta forma como etimológicamente se configura el ciberfraude. Pero, nada más alejado de la realidad creer que el *ciberfraude* es sólo una formación de palabras, cuando nuestra sociedad actual es cada vez más *ciber* dependiente. Al final, vivimos en un mundo

que mantiene las más viejas costumbres (como el *fraus*), pero que tiene todas las oportunidades de las nuevas tecnologías (el *ciber*).

Una de las aristas más apasionantes en torno a este tema es darse cuenta de que la única diferencia entre hace 100 años y ahora, es sólo el medio por el cual se produce. Donald Cressey en su libro "The Theft of Nation" establece una de las teorías más comúnmente aceptadas hoy, sobre por qué la gente comete fraude, llamada "el triángulo de cressey" que se apuntala en tres conceptos básicos:

Motivación: ¿qué es lo que motiva al defraudador a cometer el ilícito? Tal vez tiene problemas económicos, alguna presión financiera, gasta en forma excesiva, mantiene un estilo de vida en contravía con sus ingresos o está forzado a conseguir dinero (para pagar alguna extorsión, por ejemplo).

Oportunidad: ¿el defraudador, además de la motivación, tiene la oportunidad de cometer el fraude? ¿Es alguien que tiene acceso al dinero, a los bienes o que tiene la autonomía para negociar con ellos y obtener un beneficio personal? ¿Es el administrador de un sistema transaccional, con los privilegios para eliminar registros o abrir la puerta a los datos?

Mucho hemos oído hablar en diferentes escenarios acerca de la motivación y la oportunidad y resulta lógico entender que si las dos existen, el fraude está hecho. Pero, la verdad es que no es así.

Lo más impactante de la teoría de Cressey, aquello que la aleja de la lógica es el tercer elemento que conforma el triángulo, porque es tan humano e inherente al ser, que incluso nos brinda una dimensión adicional, sin la cual aun cuando existiera la oportunidad y la motivación, el humano no cometería un fraude: la racionalización.

Racionalización: cuando el defraudador tiene la motivación y la oportunidad, debe vencer una última barrera, que es él mismo; debe auto convencerse de que el fraude que está a punto de cometer no es ilegal y tiene que justificarlo, no para sus jefes o sus compañeros sino para sí mismo. Esto es lo verdaderamente excitante de la teoría de Cressey. El defraudador debe pensar que se MERECE lo que hace, culpando al sistema, a la sociedad o a su entorno. Frases como "he trabajado mucho y no lo reconocen" o "nadie se dará cuenta" o "lograré compensarlo antes de que se enteren" están a la orden del día para satisfacer la necesidad de racionalización del individuo, como parte de la argumentación que usará si alguien se refiere al tema.

Bien sea que el defraudador tenga acceso al dinero físico o al sistema de información, esta conducta siempre es repetitiva, sea para fraudes tradicionales o informáticos. Al final no hay juez más duro que uno mismo.

La evolución de las tendencias de fraude presenta múltiples oportunidades a partir del desconocimiento y de la ingenuidad de las personas cuando de elementos informáticos se trata. Numerosos estudios demuestran que las poblaciones más afectadas por el fraude digital son las personas mayores, los ancianos, sobre todo, en cuanto al fraude financiero; y menores,

en lo relacionado con el acoso en línea. Estos resultados tienen sentido si tenemos en cuenta que la población que ha crecido conociendo internet y las nuevas tecnologías es más escéptica frente a lo que encuentran en línea, que aquellos que no están familiarizados con las mismas.

Entrando en materia, desde nuestro observatorio de fraude hemos podido evidenciar cómo se han vuelto más sofisticados los ataques hacia la población en general. Hace algunos años era muy evidente que los correos electrónicos de phishing buscaban su objetivo lo más directamente posible, al solicitar abiertamente la contraseña de acceso, mientras que hoy en día estos correos ni siquiera parecen estar interesados en ella, sino más bien en información común como datos de identificación o georeferenciación. Incluso es más probable que busquen instalar alguna clase de malware en el computador o en el teléfono, con miras a monitorear las actividades y/o crear redes zombis que atacan al unísono como botnets, una de las armas cibernéticas más letales debido a su estructura colaborativa.

Por supuesto el gran reto lo tiene el usuario común y corriente, pues cada vez le es más difícil identificar lo que puede ser *malware* o no; las aplicaciones que instala en su teléfono por ejemplo pueden ser las más inocentes y no saber cuáles son sus verdaderas intenciones: hemos encontrado aplicaciones para encender la linterna del teléfono que al instalarse piden permiso para acceder a la agenda de contactos del teléfono, lo cual es absolutamente innecesario. A mismo tiempo que el usuario se expone a la victimización, se convierte en un objetivo más apetecido por los ciberdelincuentes, pues al poder trazar al detalle sus actividades y perfilar sus rutinas es posible determinar su perfil económico, social, profesional y digital.

Los fraudes dirigidos a los usuarios de tecnología tienen como componente principal aprovechar la confianza creciente que experimentamos en las tecnologías de información, pues hoy toda nuestra vida está entre dos aparatos que son el computador y el teléfono. Nuestra música, nuestros intereses, nuestras relaciones, nuestra información, nuestras fotos, nuestra ubicación, y en algunos casos, hasta nuestro dinero pueden estar en esos dos aparatos, lo que los convierte en objetivos de alto valor para escalar hacia fraudes más globales, como, por ejemplo las corporaciones donde trabajamos. Y es ahí donde toma sentido el concepto del "valor digital" de una persona: qué hace dentro de su compañía, a qué tipo de información o activos tiene acceso, sumado a saber si tiene la necesidad y la motivación para cometer un fraude.

Las redes sociales juegan un papel clave hoy en día en la preparación de fraudes, con la entrada del concepto de OSINT (Inteligencia de fuente abierta) que se basa en la perfilación de las personas, a partir de su actividad en internet, principalmente en sitios sociales donde publican detalles de su vida diaria. En internet existen herramientas y personas que "cosechan" toda esa información para crear datos de tendencias en cuanto a intereses, información demográfica, geográfica y muchas otras que, al final, facilitan desde el envío de publicidad

altamente dirigida (*marketing*) hasta la sofisticación del *phishing* con datos bastante específicos que podrían llegar a engañarlo.

Por otro lado, no se puede separar el fraude personal del fraude corporativo, toda vez que cuenta con los mismos actores, sólo que en situaciones diferentes en donde la persona puede pasar de ser víctima a perpetrador, o simplemente terminar siendo un soldado en favor de organizaciones criminales complejas.

En razón del trabajo que desarrollamos en AntiFraude® hemos conocido de primera mano muchas situaciones de fraude que han sido facilitadas por la tecnología, bien sea porque ésta ha sido modificada de manera maliciosa por alguien que tenía el acceso a ella o simplemente porque funcionarios internos han aprovechado la oportunidad cuando hay problemas tecnológicos. En cualquier caso, los fraudes corporativos se siguen encuadrando en las tres grandes categorías sugeridas por ACFE, en su reporte a las naciones: Corrupción, apropiación indebida de activos y fraude en estados financieros, todos éstos facilitados por las cada vez más numerosas herramientas informáticas de que disponemos.

Si bien el fraude como conducta dentro de una organización puede ser muy difícil de acabar completamente, si es posible disminuirlo a través de los controles apropiados. Una efectiva estrategia de control involucra por una parte, las acciones preventivas que permitan disuadir el fraude como, por ejemplo, la ubicación de elementos de monitoreo (audio, video, informático) dentro del marco de la ley y de los derechos fundamentales, la promulgación de políticas de prevención de fraude y las técnicas para evitar la colusión.

El análisis adecuado de la cultura organizacional, la identificación de competencias de las personas clave en la organización y una adecuada gestión de cambio totalmente alineada con las competencias existentes y el estilo de cultura organizacional propio, son factores determinantes para disuadir las posibilidades de fraude e identificar de forma temprana dónde puede haber vulnerabilidades de carácter humano.

Por otro lado, el ambiente de control debe proporcionar los mecanismos para identificar los fraudes, bien sea mediante el uso de líneas o la asignación de recompensas por información o tal vez mediante las auditorías y otros mecanismos de investigación, que permitan establecer cómo se presenta una conducta fraudulenta.

Finalmente, se deben tener adecuados mecanismos de reacción, para que cuando se identifique una situación sea posible acceder rápidamente a la causa raíz de la misma para eliminarla y garantizar que no vuelva a suceder.

Hoy en día, la evolución tecnológica ha llevado inclusive a contar con herramientas adicionales para transferir el riesgo de fraude, como las pólizas de seguro, en las cuales ya hay aproximaciones muy detalladas acerca de coberturas para riesgo cibernético. Así mismo, la tercerización de procesos operativos toma un papel protagónico en la transferencia del riesgo, bajo la premisa de que puede ser más expedi-

to tomar acciones legales contra un proveedor que ha cometido fraude, que contra un empleado.

En conclusión, no podemos separar el fraude que afecta a las personas comunes y corrientes, del fraude que afecta a las organizaciones. Las herramientas tecnológicas para ejecutar diversos esquemas de fraude complejos están a la orden del día y la realidad es que se pueden conseguir a muy bajo costo en la red cuando se sabe a dónde buscar.

Por otro lado, todos los días, tanto a título personal como corporativo, producimos demasiada información hacia la red y siempre hay alguien que está tomándola para perfilar las actividades y conocer a los potenciales objetivos. Sin embargo, en medio de toda la preocupación que puede generar el nuevo mundo interconectado en el que vivimos, las soluciones siguen siendo las más simples, y están en el sentido común.

Juan Carlos Reyes Muñoz. *Director de la firma Grupo Schart Latinoamérica especializada en seguridad de la información aplicada al fraude, mediante la marca AntiFraude®. Miembro de la Asociación de Investigadores de Crímenes de Alta Tecnología (*www.htcia.org*), de ACFE (*www.acfe.com*), auditor líder de ISO 27001 y delegado para el comité JTC1/SC27 de ISO en representación de INLAC, con una experiencia de más de 15 años en seguridad de la información en diferentes instituciones financieras, de seguros, de servicios y gubernamentales alrededor de América Latina.*

RUEDA DE NEGOCIOS ACIS 2016
EMPRENDIMIENTO E INNOVACIÓN EN TI

Octubre 26 de 2016

Objetivos

En el marco del Programa en Emprendimiento e Innovación en TI de la Asociación, el 26 de Octubre se llevará a cabo la **Rueda de Negocios y Emprendimientos en TI**. Esta rueda de negocios se orienta y especializa en emprendimientos basados en las tecnologías de información, productos y servicios asociados.

Los objetivos de la Asociación con esta rueda de negocios son: 1) contactar emprendedores nacionales con inversionistas y empresas de capital de riesgo interesadas en el sector de TI; 2) fortalecer las capacidades de los emprendedores de TI asistentes, y 3) facilitar los procesos de selección y negociación a los inversionistas interesados.

Al desarrollarse la rueda de negocios durante la realización del programa en emprendimiento e innovación, los emprendedores inscritos podrán participar (un cupo) igualmente en el Salón de Informática, que se llevará a cabo los días 27 y 28 de Octubre.

Cronograma

Inscripciones a la rueda	Abril 1 – Septiembre 30
Servicios de análisis y evaluación de portafolio	Agosto 1 – Septiembre 30
Rueda de negocios	Octubre 26 2-6 pm
Salón de Informática en emprendimiento e innovación	Octubre 27-28

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

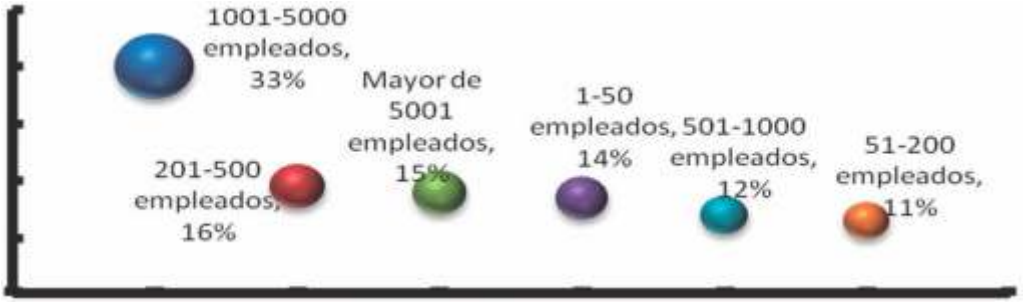
En esta sección están los datos más relevantes de la encuesta, relacionados con la demografía de los participantes y sus relaciones con la seguridad de la información.

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

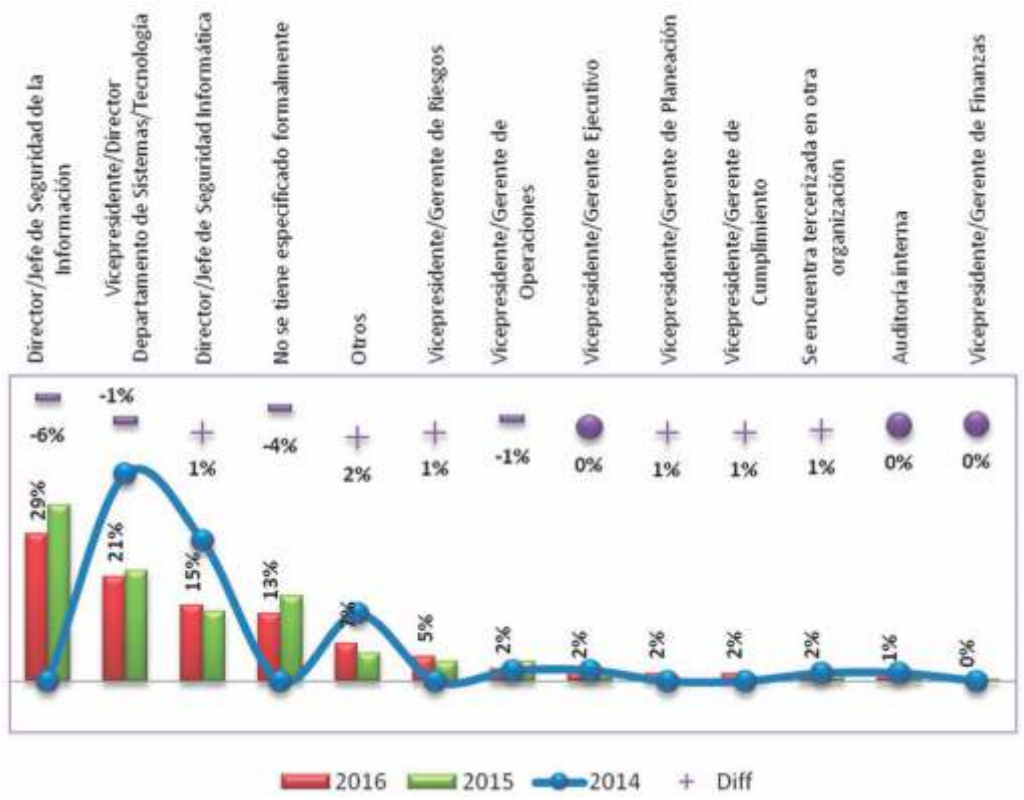
Tamaños



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.

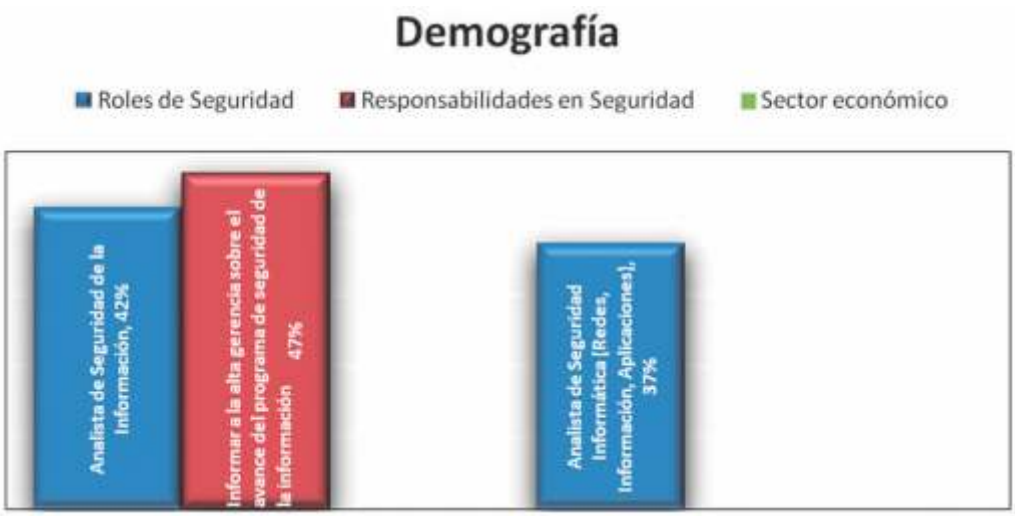
a. Informar a la alta gerencia sobre el avance del programa de seguridad de la información.

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

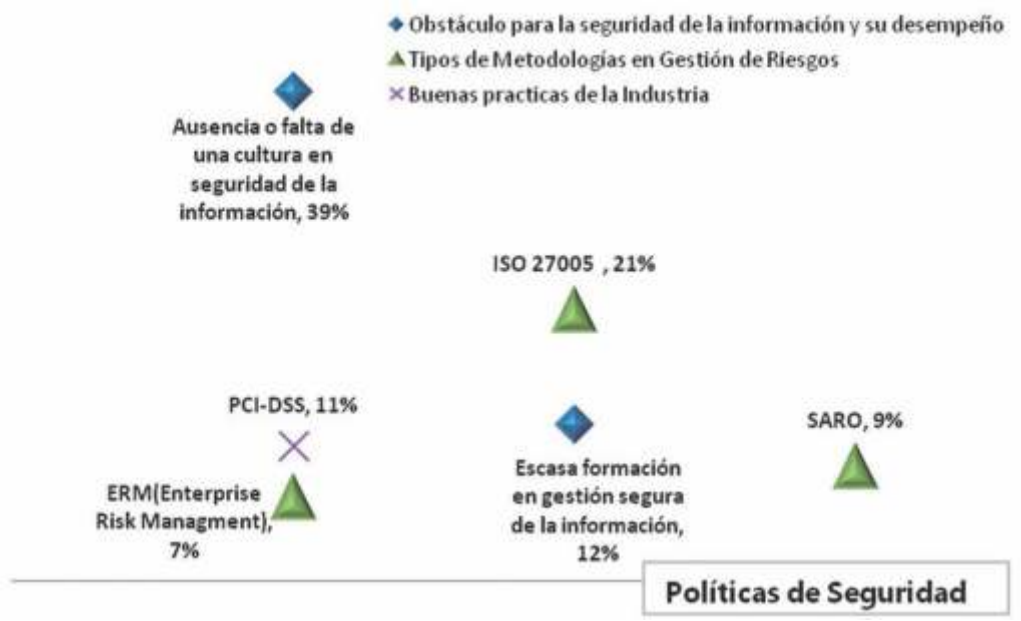


Gráfico 8. Políticas de Seguridad

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.

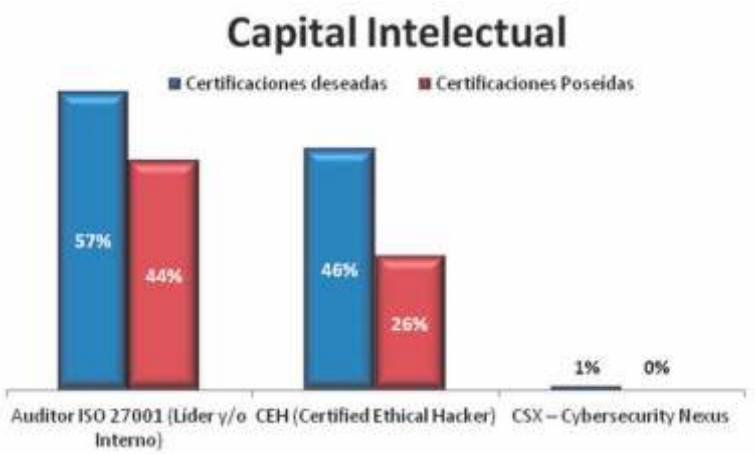
Por último, está la más reciente certificación creada para atender los temas de ciberseguridad de ISACA CSX (Cyber Security Nexus); en la actualidad, los participantes no poseen dicha certificación, pero el 1% sí considera que se debería tener, para poder desempeñar las funciones de seguridad en la organización.

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

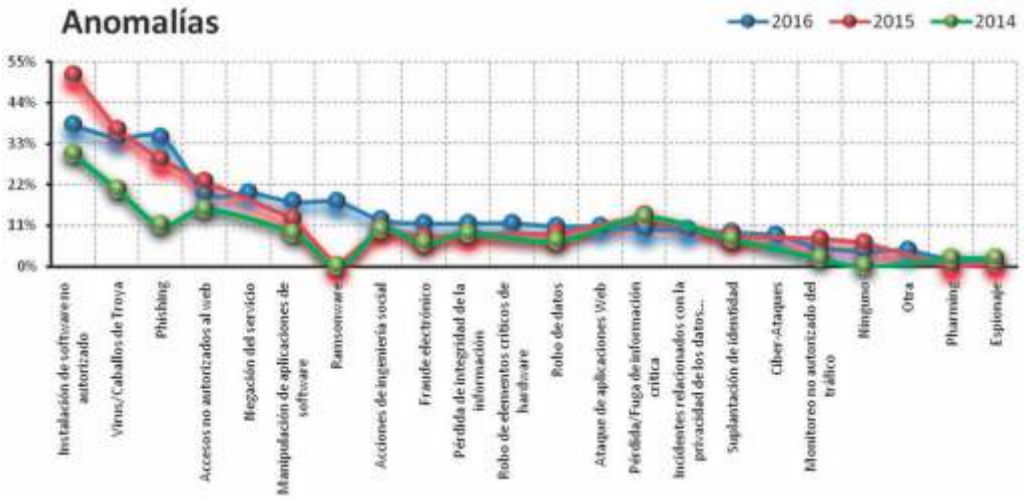


Gráfico 10. Anomalías

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.*

Fraude informático y el contexto colombiano

El ritmo que acompaña los avances tecnológicos en términos de fraude, no es el mismo de los controles ni de las alertas ni de la cultura de prevención y, menos aún, del marco jurídico que los cobija.

Sara Gallardo M.

El fraude informático avanza a un ritmo que supera todos los controles, las alertas, la cultura de prevención y ni qué decir del marco jurídico que lo rodea. Entorno que, según los futurólogos tecnológicos, no tiene nada de halagador.

Las predicciones de Scott Klososky, una de las voces más autorizadas en tales vaticinios, son para preocuparse y hacer un llamado a prestar más atención a un flagelo mundial que parece no tener límites. “Creo que estamos cerca de algún tipo de Pearl Harbor (1941). Una suerte de evento digital que acabe con numerosas compañías. Hasta que eso no ocurra, la gente no le prestará suficiente atención a la seguridad informática. Dicho evento podría suceder en los próximos cinco años”, le dijo al diario El Tiempo.

De ahí la necesidad de analizar con distintos expertos las condiciones del

presente, las tendencias y hasta el pasado. “Hace unos meses el Departamento de Defensa de los Estados Unidos liberó el documento denominado *Seguridad de los sistemas computarizados*[1], que conservaba como clasificado desde el 11 de febrero de 1970. Es decir, un documento de hace 46 años. Al revisarlo, se detectó que, en términos de los controles, pareciera que se hubiera quedado congelado en el tiempo, lo que me produjo la siguiente reflexión: -¿No hemos cambiado ni evolucionado?, manifestó Jeimy J. Cano M., director de la revista y moderador de la reunión convocada con tales fines.

Los invitados Recaredo Romero, director regional para América Latina de la División de Investigaciones y Disputas de KROLL; Natalia Baracaldo, directora del Departamento de Ciencias Contables –CIJAF- y Luis Eduardo Daza, especialista en fraude informático, del Departamento de Ciencias Contables de la Universidad Javeriana, asistieron puntuales a la cita.

“La idea es que profundicemos en las diferencias que rodean esa tendencia que está afectando y dando vueltas entre las organizaciones y el público general: el fraude informático, el ciberdelito y las otras modalidades del cibercrimen”, puntualizó Jeimy J. Cano, para dar comienzo al debate con la primera pregunta:

¿Cuál es diferencia entre un delincuente informático y un fraude informático? ¿Qué es delincuencia informática por fraude informático? ¿Existe alguna diferencia?

Recaredo Romero
Director Regional para América Latina de la
División de Investigaciones y Disputas
KROLL

[1] Department of Defense (1970) Security controls for computer systems (U). Report of Defense Science Board Task Force on Computer Security. Febrero. Recuperado de: http://seclab.cs.ucdavis.edu/projects/history/papers/ware70.pdf

El delincuente informático es el perpetrador y el fraude informático, la conducta. Y me atrevería a orientar la pregunta a la función que le damos al fraude informático. Existe una larga variedad de definiciones, una de ellas referida a quien usa el engaño a través de medios informáticos. Esa sería una diferencia entre el fraude informático y el delito informático. El primero, es un delito específico y el segundo contempla una variedad de acciones ilegales, que no son necesariamente fraude. Lo que quiere decir que el delito informático es un concepto más amplio que el fraude informático.

Luis Eduardo Daza Giraldo
Especialista en Fraude Informático
Departamento Ciencias Contables
Pontificia Universidad Javeriana

El delincuente informático, es el sujeto, el perpetrador, también identificado en otro tipo de delitos y fraudes. Es esa persona envuelta en los grandes mitos y realidades que más adelante tendremos oportunidad de precisar. A veces, es muy difícil poder identificar el delincuente informático, principalmente por las características de anonimato de su actividad. El segundo aspecto es diferenciar entre fraude y delito informático. Este último está tipificado por cada país como una conducta punible. En otras palabras, hay situaciones –que aunque son fraude, no están contempladas como delito. De ahí algunos asuntos en nuestra legislación colombiana, que aunque no son tipificadas como delito, sí caben en la categoría de fraude. Para dar un ejemplo muy sencillo, en Colombia, la evasión tributaria no es un delito, es una conducta reprochable desde el punto de vista administrativo. Eso mismo pasa en el tema informático, hay unas conductas específicas tipificadas en la ley como delito informático y otras que no alcanzan a quedar ahí, que uno podría catalogar como fraude informático.

Natalia Baracaldo
Directora Departamento Ciencias Contables –CIJAF-
Pontificia Universidad Javeriana
Mi respuesta la oriento desde la jurisdicción actual. Con el fraude financiero, sucede lo mismo. En algunos países está tipificado en los códigos penales y en otros no es así. En Colombia existe una normatividad específica, que ayuda a tipificar específicamente los temas relacionados con delitos informáticos. Sin embargo, puede haber conductas enmarcadas en asuntos de fraude, tales como el engaño, que ni siquiera pertenecen a la categoría de delitos informáticos. De ahí que la respuesta sea muy amplia y dependa del contexto desde el cual se mire. En nuestro país, se trata de un asunto incipiente, muy nuevo y prácticamente desconocido. Quienes están más salvaguardados están en el sector financiero. Allí es donde existen las mejores medidas, para cuidar ese precioso activo que es la información. En ese orden de ideas, ellos protegen la información ya sea del delito informático o de malas prácticas en su contra. Pero, cualquier persona puede cometer algo en contra de la información y ni siquiera está tipificado ni siquiera existe. De ahí que no podamos referirnos a un delincuente informático.

Jeimy J. Cano M.
Director Revista Sistemas
ACIS
¿Este tipo de conductas (fraude informático) están tipificadas en la legislación colombiana? ¿Hay casos con fallos concretos? De no ser así, ¿cuál es la razón?, ¿por qué?, ¿cuáles son las carencias para que no lo estén?

Natalia Baracaldo
En nuestro país, la tipificación de los delitos no es un tema exclusivo del ambiente informático y considero que el Código Penal se queda corto en muchísimos aspectos. No sabría decir si por quienes emiten este tipo de

Luis Eduardo Daza señala las nueve categorías de delitos informáticos tipificadas en la ley colombiana.

normas o si falta que la Academia se pronuncie. Lo que sí es evidente es que hay una falencia. Dentro de la Ley 273 de 2009, se quedan por fuera infinidad de asuntos. Pensando la pregunta desde otro contexto, en el sentido de las responsabilidades frente al control interno de la información, se exige a muchas empresas que los revisores fiscales sean quienes dictaminen sobre la tecnología de la información orientada a protegerla. Un revisor fiscal es un contador de profesión, ¿qué puede saber de delitos y de fraudes informáticos, inclusive de seguridad de la información? En mi opinión, no sólo existen vacíos normativos, también en quienes manejan estos temas, en términos de conocimiento y buenas prácticas.

Jeimy J. Cano M.
¿Está tipificado o no el delito informático?

Luis Eduardo Daza
Está tipificado; por lo menos así se llama dentro de la ley colombiana, la 1273 de 2009.

Sara Gallardo M.
Editora Revista Sistemas
Pero, ¿no específicamente el fraude?

Luis Eduardo Daza Giraldo
En la ley colombiana están tipificados como nueve categorías de delitos, incluso hasta daños físicos en equipos, daño informático y acceso no autorizado. Sí existen fallos concretos, pero siguen siendo muy pocos. Uno de los aspectos a tener en cuenta con relación a nuestras autoridades en el país, es que como se trata de temas relativamente muy recientes, la preparación técnica de los funcionarios para atender tales hechos es escasa y deficiente. Quienes combaten ese tipo de delitos enfrentan el reto de actualización y de una formación más avanzada. En los diferentes expedientes judiciales –doscientos, para citar una cifra-, que manejan los fiscales figuran casos de robo, hurto, lavado de activos, estafa y tal vez sólo uno es delito informático y, en consecuencia, la prioridad para su investigación será, probablemente, una de las últimas. Y

además se preguntan: "¿qué hago con este proceso?, ¿a qué investigador se lo asigno?". En otras palabras, se trata de un tema que genera angustia y, por lo tanto, deciden trabajar sobre lo conocido y aplazar lo demás. Esta situación explica por qué se conocen muy pocos fallos o condenas. Su complejidad y la falta de preparación técnica en lo penal la determinan.

Sara Gallardo

¿Existen cifras sobre el porcentaje de cuántos casos de los que manejan los fiscales, corresponden a delitos informáticos?

Luis Eduardo Daza

Hay algunos informes con bajos resultados finales de productividad. En las noticias se informa sobre algunos casos muy connotados acerca de acciones de *hacking*, pero son la excepción. Y, lo grave de todo esto, es que la gran mayoría de delitos informáticos quedan en la impunidad. En el caso, por ejemplo, de un fraude financiero a través de una tarjeta de crédito, si la entidad bancaria devuelve el dinero al tarjetahabiente, hasta ahí llega el asunto. Se cometió el delito, pero no se hizo nada para iniciar una acción legal, porque la víctima (el tarjetahabiente) al final no sufrió una pérdida. Tal hecho, por los montos individuales menores, no incentiva los procesos penales y obstaculiza su éxito de investigación y sanción.

Recaredo Romero

Con relación a si está o no tipificado el fraude, me gustaría "medir el vaso, medir el hielo". En otras palabras, la tecnología va a una velocidad muy distinta a la de las normas. Eso sucede en la normatividad nacional e internacional. El fraude informático no está tipificado en la ley. Algunas conductas sí lo están, con las cuales en un caso de fraude informático, se podrían apalancar la investigación y el proceso.

Recaredo Romero indica que la tecnología va a una velocidad muy distinta a la de las normas y, por tal razón, el fraude informático no está tipificado en la ley.

Según Recaredo Romero (derecha), el fraude no está tipificado, pero se le puede conectar con delitos informáticos que sí lo están.

Jeimy J. Cano M.
¿En lo penal?

Recaredo Romero
Exactamente y con conexión al delito informático. El fraude, específicamente, no está tipificado, pero se le puede conectar con delitos informáticos que sí lo están. Por ejemplo, con el delito de acceso abusivo a un sistema informático. Ese delito está presente en muchas conductas y fraudes. Así que la norma tiene carencias, pero es algo natural, mientras el ritmo de la tecnología y el sistema normativo sean distintos. Ya, por lo menos, tenemos en Colombia unas conductas tipificadas como delitos informáticos.

Jeimy J. Cano M.
¿Existen en Colombia estadísticas sobre fraude informático? ¿Cuáles son las conductas más habituales?

Recaredo Romero
Con relación a estadísticas, cito los resultados del informe global de fraude que elabora KROLL anualmente. En el año 2015, de las once tipologías de fraude que mide el estudio, el "robo de información, pérdida o ataque" se ubicó en tercer lugar como tipología más frecuente a nivel internacional. En Colombia, esa tipología fue la número uno y afectó al 27% de las empresas que participaron en el estudio.

Sara Gallardo
¿De cuántas empresas?

Recaredo Romero
Del total de la muestra, el 27%. Es preciso anotar que el estudio mide específicamente el fraude detectado. El fraude real, que incluye el no detectado, es probablemente significativamente más alto. Dentro de las tipologías más comunes en el ámbito empresarial está la captura y robo de información para venderla y hacer uso de la misma; también el robo de identidad es prevalente. En el sistema financiero, los datos personales, cuen-

tas bancarias, claves de acceso a tarjetas, entre otros aspectos, tienen una alta demanda en el mercado negro. Se trata de actividades de bajo riesgo y alta retribución para el delincuente, lo cual incentiva la actividad ilícita. La transnacionalidad de esas tipologías, dificultan investigar el delito informático. Dentro de las tendencias, estamos ante unos encadenamientos productivos, por llamarlos de alguna manera, donde tenemos muchos eslabones que participan en la cadena; desde los desarrolladores de los *softwares* maliciosos, hasta los que capturan datos, los que los comercializan y los que hacen uso de esos datos para obtener un beneficio económico. Entonces, tenemos una multitud de actores ubicados en distintos países. Afortunadamente, la colaboración judicial es creciente y está aumentando la eficacia en la persecución de estos delitos, la cual ha sido tradicionalmente muy baja. Algo que se ha vuelto tremendamente frecuente y que se espera siga en aumento es el *ransomware*, o secuestro de información; una tendencia global que está afectando también a Colombia. Esta es una actividad que va a ser difícil de contrarrestar, mientras existan empresas y personas dispuestas a pagar "el rescate". Frente a lo que se ve a futuro, *Internet de las cosas* tendrá gran incidencia, por la interconexión al gran *software* y el boom de los bienes electrónicos; los carros, las casas y los sistemas del hogar estarán conectados. Así que podrá resultar lo mismo que estamos viendo ahora, el secuestro de información, a cambio de un rescate, además de pasar a metodologías todavía más sofisticadas.

Jeimy J. Cano

Adicionalmente al planteamiento de Recaredo Romero, el ransomware ha sufrido una evolución. Ya no sólo se pide rescate, sino que con el pasar del tiempo sin pagarlo, los atacantes comienzan a borrar los archivos retenidos. En otras palabras, queda capturado el equipo.

El director de la revista y moderador del foro Jeimy J. Cano se refiere a la evolución del ransomware.

Luis Eduardo Daza (segundo de derecha a izquierda) advierte sobre la dificultad para medir la acción criminal en la red.

Recaredo Romero
Agregaría que con el *ransomware* está sucediendo lo mismo que ocurría con la extorsión y los secuestros tradicionales. Hay casos en que la gente paga el rescate y se le piden pagos adicionales. O casos en que las víctimas vuelven a ser atacadas por ser percibidas como proclives al pago. Adicionalmente, lo más común hasta el momento es, yo retengo tu información hasta que me pagues el rescate. Pero se empiezan a presentar incidentes en los que se amenaza a la víctima con hacer pública la información, a no ser que se pague rescate.

Sara Gallardo
¿Con relación a las tendencias mencionadas, que en muchos lugares ya son un hecho, hay cifras específicas?

Luis Eduardo Daza
Cuando se habla de estadísticas, el problema es medir la acción criminal en la red. Esta acción es muy difícil de realizar. En teoría hay dos tipos de delitos informáticos: los que no contemplan una intención financiera, conocidos como *hacking* y los que sí la tienen, reconocidos como *cracking*. ¿Cuál es medible? Generalmente, las estadísticas apuntan al *cracking* porque se trata de cifras asociadas a montos de dinero; mientras que las acciones de acceso a sistemas o datos no autorizados resultan difícilmente medibles. Lo más difícil en este tipo de delitos es medir. Como dije antes, las conductas de los delitos informáticos se podrían dividir entre las que son con una intención de provecho financiero y las que no. Las primeras, de alguna manera se podrían medir, o por lo menos estimar, con base en encuestas a las víctimas, ya sean personas o empresas. Al contrario, resulta casi imposible estimar los delitos informáticos no financieros, que sólo buscan acceder a unos datos o sistemas de información sin consentimiento de su titular. Algunas entidades han realizado dichas mediciones, en forma anual y otras bianual y la gran mayoría a través de encuestas en las que se

definen ciertas categorías y una metodología de estimación para cada una. De esta forma, la empresa o persona que fue víctima del ciberdelito financiero manifiesta la modalidad, el número de incidentes, el monto involucrado y demás características. Pero no hay de *hacking*.

Y esa, en mi opinión es una de las conductas, para llegar a la pregunta sobre ¿Cuáles son las más habituales? Sin tener una cifra concreta, creo que el *hacking* es una de las conductas más habituales en ese tipo de delitos, pero no se puede medir exactamente. Es como hablar de otros fenómenos como el narcotráfico, hay cifras, hay datos, hay estimaciones, pero no hay una cifra exacta. No hay una medición exacta. Se trata de hacer ejercicios o aplicar modelos para medirlo. Nosotros desde la academia ¿qué hacemos? Revisamos y seguimos estadísticas que publican algunas firmas como KROLL, KPMG y PriceWC que se aventuran a medir el fenómeno. Y ahí lo que uno ve es que hay unas tendencias, las cuales permiten medir, según sus metodologías, en dónde se puede ir clasificando y midiendo el delito informático y qué tendencia marca. KPMG venía haciendo una encuesta de fraude en las empresas para los años 2011 y 2013. Algo interesante es que para el 2013, incluyó la variable, cibercrimen. Esto es muy valioso porque hace una primera medición en las empresas colombianas. Lástima que no apareció la versión 2015 para comparar dicha medición. Esperábamos que fuera cada dos años, pero KPMG no lo hizo. No sé si lo estarán pensando hacer o retomar. El tema de estadísticas o medición de actividades ilegales, en este caso los delitos informáticos, resulta muy complejo porque se trata de medir algo que sabemos que existe, pero es clandestino.

Natalia Baracaldo

La firma KPMG ha venido haciendo lo que ellos denominan *Encuesta de fraude*, versiones 2011 y 2013. En la primera, realizaron mediciones rela-

Por primera vez en la historia de esta sección de la revista, ninguno de los invitados a la reunión era ingeniero de sistemas.

cionadas con el árbol del fraude que proponía tres categorías y en ésta medían impactos de corrupción, malversación de activos, e información financiera fraudulenta. En la encuesta del año 2013, contemplan la ramificación del cibercrimen, en donde entran las conductas a las que nos hemos referido. En ese estudio de 2013 vale la pena destacar que el impacto económico de estos actos vandálicos está representado en una cifra cercana a los 550 millones de dólares, sin tener en cuenta lo no cuantificado. De dicha encuesta sale el cibercrimen. En el año 2011, el valor total de los fraudes cuantificados fue de 950 millones de dólares; para el año 2013, la cifra de lo cuantificado ascendió a 3.600 millones de dólares. Sin embargo, no quiere decir que en ese lapso hubiesen ocurrido esos fraudes. Más bien, es que se venían gestando y lo que salió a la luz en esos períodos, fue lo que venía de atrás. Por ejemplo, Interbolsa y Saludcoop, para citar algunos. Tales casos no fueron específicamente gestados por el cibercrimen, pero sí fueron utilizadas herramientas informáticas. Es importante entonces, verificar la incidencia que tiene el tema de lo informático. Las cifras de lo que propone KPMG en su encuesta versión 2013, es que el 23% de los ataques cibernéticos, obedece a deslealtad de empleados. Es decir, que en ese porcentaje, se están gestando desde el nivel ocupacional y personas dentro de la organización, fraudes relacionados con el cibercrimen. Allí hay otras cifras importantes de mencionar, como que el 39% de los ataques cibernéticos fueron detectados de manera accidental. Digamos que en esa cifra, se mencionan dos cosas, el impacto o la incidencia de cómo se detectaron ataques cibernéticos. No es común que los delitos informáticos se denuncien a través de los canales organizacionales, obedece más a un tema de accidente -como veíamos en noticias recientes- a que la persona tuvo mala ortografía o escribió mal el *password.* Se podría decir entonces que no hay controles en la tecnología de informa-

ción, a través de un canal de denuncias. En los ataques cibernéticos, no es efectivo un canal de denuncias para detectarlo, lo cual es muy preocupante. Incluso, están las cifras, del Rasmussen College (2012), las cuales señalan que el delito cibernético ha venido creciendo tanto en los últimos años, que llegará un momento, en el cual tenga muchísima más incidencia que el narcotráfico, la trata de personas u otro tipo de delitos y ante la opinión pública sean más graves.

Jeimy J. Cano

¿Existe un modus operandi del defraudador informático? ¿Cuáles podrían ser los síntomas que revelen un posible fraude informático?

Luis Eduardo Daza

En buena parte de estos asuntos aplica la teoría general del fraude. El modus operandi del defraudador se presenta interna y externamente, hechos que coinciden con la teoría del fraude en general. Es decir, afuera de las organizaciones están los defraudadores interesados en vulnerar u obtener beneficios de la compañía. Dentro del ámbito interno de las empresas, yo diría, que los fraudes se pueden dar en todos los niveles, desde la alta dirección, digamos, desde un nivel directivo y medio, hasta un nivel netamente operativo. ¿De qué depende? Según la teoría general del fraude, un enfoque tradicional de finales de los años 60 propuesto por Donald Cressey, los funcionarios cometen fraude por motivación, oportunidad o racionalización. Sin embargo, luego se añade el concepto de la capacidad a estos tres elementos. Sin duda, es un aspecto fundamental en este tipo de conductas asociadas a los delitos informáticos, porque la capacidad del sujeto determina el alcance que pueda tener para acceder a la información o datos. Entonces, dependiendo de la modalidad del fraude de que estemos hablando se pueden identificar diferentes perfiles y modos de actuar. Por ejemplo, un alto directivo tiene mucha más capacidad de acceso a cierta información, que muchos otros

Jeimy J. Cano (fondo) indaga sobre el modus operandi del defraudador informático.

funcionarios de la empresa no lo tienen. Hay muchos altos directivos que tienen acceso a todo. Algunos, por buena práctica, renuncian a dichos privilegios y dicen, “yo no quiero tener claves de nada”, “yo no quiero tener acceso a ningún sistema”, “a mí pásenme la información requerida”. En cambio, hay otros funcionarios que su capacidad es limitada al nivel de acceso que se haya fijado según las políticas o protocolos de seguridad. Digamos, por ahora, que diferenciar el acceso a los sistemas de información es una de las buenas prácticas que existen porque delimita la capacidad y establece perfiles diferentes.

¿Cómo se ven los síntomas? También yo diría, hay que aplicar la teoría general del fraude. ¿Cómo sabe uno que de pronto alguien está involucrado en ese tipo de fraudes? Hay que revisar los temas y las conductas personales; por ejemplo, los cambios repentinos o injustificados de estilo de vida, aquellas personas que se quedan siempre hasta altas horas de la noche, o en horarios no habituales o en fines de semana; relaciones muy cercanas con ciertos proveedores o clientes. Yo aplicaría la teoría del fraude. Los síntomas son esos comportamientos inusuales, son aquellas conductas que podrían ir descubriendo ese tipo de fraude, según el área de desempeño laboral o funcional de la persona. Sin duda, hay que volver a poner la lupa en aquellas personas que tienen cierta capacidad y además están ubicados en áreas críticas o de alto impacto. Porque cada categoría de fraude tiene sus propias condiciones.

Natalia Baracaldo

KPMG tiene en cuenta una tipificación dentro de su nuevo árbol de fraude: la piratería, los accesos no autorizados y el vandalismo. En el tema de piratería, creo que todos nos hemos hecho una idea desdibujada, desde el señor que está en el mercado informal o que quienes la realizan manejan unos perfiles muy bajos. Puede que sea esa la línea final de toda la cadena, pero la

verdad, es que en términos de piratería, todo obedece a grandes cabezas, a grandes corporaciones. Si miramos el tema de la música, hoy en día existen plataformas como *Napster*, o *Spotify*, que se han visto inmersas en temas de piratería, en términos de derechos de autor. Desde la óptica en que se mire es necesario hacer una diferenciación. Si se trata de la reproducción no autorizada, piratería hecha por una organización grande o si se refiere a distribución, la cual cae en mercados más oscuros, densos y sobre los que el control finalmente se pierde. Los accesos no autorizados, podrían darse directamente en las organizaciones. Por ejemplo, con los accesos abusivos a sistemas informáticos de las entidades. Por ejemplo, la persona que su puesto de trabajo era en el área contable y luego pasó a tesorería, a quien se le presenta una necesidad familiar y ve la oportunidad de cometer un acto ilegal, en el marco de un acceso no autorizado. ¿Cuál sería el modus operandi de la persona? Ellos lo hacen una vez, dos veces y se dan cuenta que lo pueden repetir y le proponen al amigo. Un caso muy sonado el del tesorero de Bavaria, quien cometió uno de los actos de fraude financiero de miles de millones de pesos, de mayor repercusión en nuestro país, hace aproximadamente ocho años. Por otro lado, los robos de identidad, también a través de accesos abusivos a la información o a través de las páginas de internet con las entidades financieras. Y por último, podemos hablar de un tema de vandalismo, donde apenas voy a mencionar los temas de suplantación de destrucción de la información y de *software* malicioso. En ese ambiente es posible encontrar personas muy capaces, a veces ni siquiera profesionales, pero sí muy hábiles con los asuntos de sistemas. Particularmente, participo en investigaciones de fraude financiero, donde uno se ve inmerso en escenarios con personas discapacitadas o mujeres embarazadas.

Recaredo Romero

A la hora de revisar el modus operandi para establecer el perfil del perpetrador, es oportuno diferenciar entre el

Recaredo Romero (derecha) explica las diferencias que rodean a los actores internos y externos, en términos del fraude informático, dentro de una organización.

actor interno y el externo. Y dentro de los actores internos, aquellos que actúan de manera maliciosa y los que son negligentes. Al contrario de lo que pudiera pensarse, un número significativo de incidentes de seguridad informática son generados por actores internos. Es importante fortalecer la conciencia de seguridad informática en los empleados y hacer que todo el mundo sea responsable de crear un entorno seguro. Los empleados con escasa cultura de seguridad, aquellos que por desinformación o porque no les gusta la inconveniencia que genera la seguridad e intentan evadir las políticas de la empresa, facilitan mucho la actuación de los *hackers*. El factor humano es usualmente el eslabón débil en cualquier programa de seguridad informática. Respecto a los actores externos, nos encontramos los *hackers* criminales, los cuales buscan generalmente un beneficio económico, los *hacktivistas*, cuyo propósito es principalmente generar daño o avergonzar a la víctima, y los *hackers* patrocinados por gobiernos. Es importante tener presente que las tácticas de los *hackers* han ido evolucionando. Se ha pasado del "golpear y correr" al "infiltrar y permanecer". Una medida de protección de uso creciente en las organizaciones es la gestión de incidentes de seguridad informática con agentes inteligentes. Estos agentes ayudan a detectar incidentes o alertas en tiempo real y proporcionan soluciones inmediatas en forma automática para controlar los incidentes.

Jeimy J. Cano

En un mundo digitalmente modificado como lo establecen los académicos Michael Porter y James E. Heppelmann[2] (2015) la seguridad y el control se convierten en un elemento clave que genera valor a los productos y servicios. En este sentido, ¿qué tipos de controles se deben tener en cuenta para prevenir el fraude informático? ¿Son los mismos que se aplican en seguridad de la información o como controles generales de TI?

[2] Porter, M. y Heppelmann, J. (2015) How Smart, connected products are transforming companies. Harvard Business Review. Octubre.

Natalia Baracaldo

En mi concepto, el tema del control tiene que analizarse como un todo. El control interno es un proceso organizacional y existen los controles que pueden ser compartidos. Por ejemplo, al modelo COSO, relacionado con el control interno, la organización para cumplir sus objetivos debe determinar los ámbitos de cumplimiento, financiero y operativo. Lo informático está implícito en los tres. En la Ley *Sarbanes Oxley*, en el año 2002, posterior a fraudes financieros, en la sección 404 de Control sobre información financiera, se obliga a que las organizaciones contemplen un control interno sobre ésta. Aunque allí no se está hablando específicamente de fraude informático, sí vemos la necesidad de que tengan controles internos de tales características. En ese orden de ideas. ¿qué efecto tiene esto en el ámbito colombiano? Pues que eso va aplicar para aquellas empresas colombianas que coticen en bolsa. ¿Pero cuántas empresas colombianas cotizan en bolsa? Un mínimo porcentaje de la economía. Es decir, que por normatividad, las empresas no están obligadas a tener unos sistemas informáticos muy fuertes. En las empresas de familia, las pymes y las microempresas, piensan que el riesgo informático más grande es un virus que afecte el computador. Tales compañías no cuentan con un back-up de la información. ¿Cuál es el tema crucial? Regulación, porque las empresas no tienen la obligatoriedad en Colombia de contar con un sistema de información fuerte; ni desde la seguridad de la información ni desde el fraude informático. ¿Dónde es palpable el tema del fraude informático? En las grandes organizaciones con prácticas de gobierno corporativo y de control interno. Tales empresas comienzan a tener dependencias antifraude. ¿Y cuál es el porcentaje de estas compañías en el país? Un porcentaje muy pequeño.

Recaredo Romero

Las bases y los conceptos básicos son los mismos. Pero sí hay algunos matices dentro de la seguridad informática, donde es importante un grado

Recaredo Romero (derecha) dice que "no hay sistemas de protección infalibles".

de especialización, sobre todo en los profesionales. Ahí, principalmente en temas como el monitoreo o la respuesta a amenazas dinámicas, sí existe una marcada diferencia, al tener profesionales con una formación y experiencia práctica, atendiendo incidentes y ataques informáticos. Así mismo, la oferta de herramientas especializadas para prevenir, monitorear, detectar y responder a las amenazas de seguridad es cada vez más amplia y sofisticada y requiere profesionales con los adecuados conocimientos técnicos. Una tendencia creciente en cuanto a controles, es el endurecimiento por parte de las organizaciones de la política de uso aceptable de tecnología de la información. Específicamente, las restricciones de acceso a sitios *web* desde computadores conectados a la red corporativa, incluyendo proveedores de servicios de email, redes sociales, chats y motores de búsqueda.

Sara Gallardo

¿Lo que quiere decir que la tecnología ha fallado? ¿Si la solución se cifra en determinar: "usted no use", "usted no acceda", "usted…", quiere decir, que los controles en términos tecnológicos fallaron?

Recaredo Romero

Ese es el desafío de esta temática. No hay sistemas de protección infalibles. Siempre se está en riesgo y la tolerancia al mismo influirá en los controles que cada uno deberá establecer. Obviamente, el sistema financiero es muy restrictivo. Habrá otro tipo de actividades económicas, en las que pueden manejar el riesgo con criterios más flexibles. Dependiendo de la naturaleza del trabajo, de los requerimientos para la esencia del negocio o la actividad realizada se establecerán políticas diferentes. La tendencia dominante es establecer restricciones generales de uso aceptable de tecnología de la información para toda la organización y permitir excepciones para personas o grupos según lo amerite la necesidad del negocio. Las amenazas son crecientes y cambiantes y hay que adaptar los controles en la misma medida.

Luis Eduardo Daza
Parto de una analogía. El tema de los controles es similar a los "cachos" o a la infidelidad. No importa cuántos controles usted coloque, si de verdad una persona tiene la intención de ser infiel, lo va a hacer. Esa persona buscará muchas maneras para lograrlo. Las organizaciones, los auditores, las áreas de riesgo, siempre están buscando imponer o verificar el cumplimiento de los controles y más controles, para minimizar el riesgo. Esa es una de sus tareas. Y se convierte en un círculo vicioso. En mi opinión, la solución no está en enfocarse en esa dirección. El reto está en crear una cultura y tener en cuenta los cambios generacionales. Por ejemplo, hoy una persona de las últimas generaciones, *millenials*, es quien dentro de una organización necesita estar conectado con el mundo o por lo menos con sus contactos. El mundo no tiene sentido si no es globalizado e intercomunicado. Esto es muy importante hoy en las organizaciones, porque la tendencia en los controles a la seguridad de la información es cada vez más restrictiva para los accesos a redes sociales e internet.

Jeimy Cano
¿Entonces, la cultura es un control?

Luis Eduardo
La cultura se vuelve en una forma complementaria del control. Volviendo a la infidelidad, si en mi casa me enseñaron a respetar, a decir la verdad, a ser honesto, etc., etc., pues al final seguramente no voy a caer en ella. Y pasa lo mismo en las organizaciones. Si la cultura dentro de la empresa es relajada, vulnerable y no está bien cimentada, si los accesos contemplan fines personales y no institucionales, hay riesgo. En muchas ocasiones la información de algunas empresas tiene niveles muy altos de confidencialidad, es decir, no es posible compartirla ni con la familia. Hace poco supe de un atraco en un banco del país, porque un empleado de esa oficina divulgó fotos en sus cuentas personales de redes sociales

Hoy, las organizaciones ponen en práctica más y más controles, según Luis Eduardo Daza (izquierda).

El uso de las redes sociales y los smartphones, de acuerdo con Natalia Baracaldo, pueden ser la mayor fuente de riesgo.

y con esa información los delincuentes supieron dónde estaban las bóvedas o caja fuerte y la ubicación. Se trata de un tema de cultura y un reto generacional.

Jeimy J. Cano M.

¿Qué tendencias futuras se ven en el fraude informático? ¿Se apalancan en las tendencias de la delincuencia digital moderna?

Recaredo Romero

Algunos ejemplos ya los hemos anotado. Agregaré que crecen las amenazas a los teléfonos inteligentes. Los dispositivos móviles actuales contienen mucha información personal y cada vez más son objeto de ataques. Por ejemplo, hay aplicaciones que camuflan en juegos aparentemente inofensivos que posteriormente descargan un componente malicioso. Las vulnerabilidades siguen siendo frecuentes en *Android*, el sistema operativo más utilizado del mundo, a pesar del lanzamiento de nuevas versiones que ponen énfasis especial en la seguridad. Sin duda, los teléfonos inteligentes son un área de atención, toda vez que su uso es extendido y cada vez somos más dependientes de ellos.

Natalia Baracaldo

En escenarios en perspectiva, el uso de redes sociales, *smartphones*, entornos a los que nos hemos vuelto adictos, esclavos, pueden ser la mayor fuente de riesgos en los sistemas de delitos informáticos. En sentido contrario a tal perspectiva sobre el futuro del delito informático, los temas de piratería tienden a disminuir, porque hoy se han creado empresas para descarga de música, películas, videos, etc. Ahora las personas tienen la música en sus móviles, sin pagar ni exponer los equipos a virus. Esto también depende de la jurisdicción. En China, en Asia se tipo de aplicaciones no se pueden tener.

Luis Eduardo Daza

La tendencia de la delincuencia informática va en dos vías. Una, la denominaría como la irreverencia o el irrespeto al *status quo* y está basada en tecnología. Es decir, con la aparición de ciertos fenómenos como la

economía colaborativa hemos cambiado los principios de riqueza que ya no están en la cantidad de propiedades, sino en la facilidad para acceder a bienes o servicios, apoyados en los desarrollos tecnológicos. Algunos ejemplos notables de esta nueva forma de acceder a la economía colaborativa o *sharing economy* es Uber ó Airbnb. El caso de Uber es muy significativo para entender cómo este negocio, basado en una plataforma tecnológica desarrolla un servicio de transporte sin tener la propiedad de un solo vehículo; esto se ha convertido en todo un reto para los taxistas tradicionales, autoridades, usuarios y otros jugadores. Para volver a la respuesta, cito este ejemplo para ilustrar que los negocios lícitos hoy no tienen fronteras, pero al mismo tiempo las organizaciones criminales y ciberdelincuentes se aprovechan de las mismas ventajas tecnológicas.

La segunda tendencia la podría denominar como la asimetría regulatoria. Es decir, los ciberdelincuentes saben perfectamente que en la red tienen un panorama inmenso, casi ilimitado, de posibilidades para reali-zar actividades que resultan claramente ilegales según las normas penales de cada país. Sin embargo, la red no tiene una jurisdicción penal específica. Esta situación es aprovechada por los delincuentes para favorecer sus intereses y evadir las posibles acciones legales que debieran asumir.

Conclusiones

Recaredo Romero

El mundo está cada vez más interconectado y dependemos de la tecnología en los negocios y nuestra vida cotidiana. Esto nos expone a riesgos crecientes e infortunadamente no existen métodos infalibles de protección. No obstante, podemos mitigar en forma significativa el riesgo de fraude y otros riesgos informáticos mediante la implementación de estrategias adecuadas orientadas a prevenir la ocurrencia de incidentes y a responder de manera rápida y efectiva cuando estos suceden. Defender el perímetro sigue siendo necesario, pero no es suficiente. Un buen programa de seguridad informática requiere prestar atención a estos tres pilares fundamentales: personas, procesos y tecnología.

Natalia Baracaldo

Queda de manifiesto que en todos los sectores de la economía, el ciberdelito debe ser contemplado como un riesgo, frente al cual se debe dar una respuesta, que desde mi experiencia debería ser la mitigación; lo mejor en materia de mitigación es la imposición de controles, los cuales deben formar parte de la cultura organizacional. Es importante que las empresas y hasta los ciudadanos del común sean conscientes sobre cómo el conocimiento y la prevención en estos temas, se vuelve un arma para combatir los delitos cibernéticos.

Luis Eduardo Daza

Para concluir, quisiera decir que los ciberdelincuentes se aprovechan del anonimato que se puede dar en la red y también saben de las debilidades técnicas de las autoridades para investigar estas conductas. Por lo tanto, debemos asumir una gran responsabilidad en el manejo de nuestros propios datos y cuidar la información que manejamos de las empresas o negocios a nuestro cargo. En cuanto a los delitos informáticos en las empresas, se requiere un trata-

miento con enfoque basado en riesgo para distinguir mecanismos de prevención y controles acordes con el nivel de riesgo identificado. Por último, las organizaciones deben tener en cuenta los cambios en su estructura por el avance tecnológico y de comunicaciones, los cambios culturales de las personas que llegan al mundo laboral y los tipos de controles, según el diferente rol de sus empleados.

Sara Gallardo M. *Periodista comunicadora, universidad Jorge Tadeo Lozano. Ha sido directora de las revistas "Uno y Cero", "Gestión Gerencial" y "Acuc Noticias". Editora de Aló Computadores del diario El Tiempo. Redactora en las revistas Cambio 16, Cambio y Clase Empresarial. Coautora del libro "Lo que cuesta el abuso del poder". Ha sido corresponsal de la revista Infochannel de México y de los diarios "La Prensa" de Panamá y "La Prensa Gráfica" de El Salvador. Investigadora en publicaciones culturales. Gerente de Comunicaciones y Servicio al Comensal en Andrés Carne de Res, empresa que supera los 1800 empleados; corresponsal de la revista IN de Lanchile. En la actualidad, es editora en Alfaomega Colombiana S.A., firma especializada en libros universitarios, y editora de esta revista.*

Fraude informático, una amplia mirada

Diferencias de conceptos e implicaciones entre fraude, crimen cibernético y otros.

Joshsua González

Introducción

En la actualidad, simplificamos nuestras expresiones sobre el ámbito informático, reduciéndolas a la preposición "ciber" (cibercrimen, ciberterrorismo, ciberguerra, cibercomercio, cibereducación), cayendo en una definición utópica. El Departamento de Defensa de los Estados Unidos define el ciberespacio como *el entorno teórico en el que se comunica la información digitalizada, a través de redes informáticas*. Por otro lado, la Estrategia Nacional Militar para operaciones ciberespaciales del mismo país, define el ciberespacio como *el dominio que se caracteriza por el uso de la electrónica y del espectro electromag-nético para almacenar, modificar e intercambiar datos, mediante sistemas de redes e infraestructuras físicas*. Tiempo después, El Departamento de Defensa (en publicación junto al organismo de Operaciones Conjuntas, el 17 de septiembre 2006, incorporaron un cambio el 22 de marzo de 2010), define el ciberespacio como *un ámbito global en el entorno de la información. Se trata de la red interdependiente de infraes-*

tructuras tecnológicas de la información, incluida Internet, redes de telecomunicaciones, sistemas informáticos y procesadores embebidos. Tales medios utilizados en el ciberespacio como lo son la electrónica y el espectro electromagnético para almacenar, se enfocan en acciones como modificar e intercambiar datos, por medio de los sistemas en red. Las operaciones en el ciberespacio emplean las capacidades de este medio, principalmente para lograr dichos objetivos y contemplan operaciones de redes informáticas y actividades para operar y defender a la Red de Información Global.

Una nueva manera de delinquir

A casi 10 años de uno de los incidentes de seguridad mayor nombrados en el año 2008, donde un hombre conocido como Michael Largent fue arrestado por un proceso fraudulento en la creación de aproximadamente 58.000 cuentas bancarias, las cuales usó para el recaudo de dinero en transacciones electrónicas. Básicamente, Largent realizó una burla al sistema de Google Checkout, Paypal y otros sitios de transacciones, donde a través de transacciones mínimas de centavos logró acumular cerca de USD$50.000. Más allá del caso, las transacciones electrónicas en sí fueron válidas, no se halló delito punible en el acto de llegar a depositar centavos de dólar, por lo que a Largent no se le inculpó por este acto. El fraude se declaró en el hecho de llegar a falsificar nombres, números sociales y asociarlos a las cuentas bancarias, delito conocido como fraude bancario.

Lo que el crimen cibernético ha hecho es tomarse una gran cantidad de delitos ya existentes, con un vector diferente. La delincuencia informática es conocida hoy en día como un crimen o delito que utiliza ordenadores, dispositivos móviles, redes y computadores entre otros. Sin embargo, hay tres hechos distintos de estos crímenes, donde los equipos informáticos tienden a ser un objetivo, un arma, o simplemente un facilitador del acto.

En el primer caso, los sistemas informáticos son el objetivo del delito y foco de actividades tales como robo, destrucción, alteración de la información, sistemas de información y *software*. En el segundo caso, los equipos informáticos pretenden ser el arma que implica el uso para lanzar ataques, entre los que se cuentan: el acoso cibernético (*ciberbullying*), pornografía infantil, correo no deseado, *spoofing* (en calidad de suplantación de varios vectores, como sitios *web*, correo electrónico), DoS (Denegación de Servicio). De igual manera, en sus diferentes acciones (*Distributed Denial of Service DoS, Economic Denial of Service EDoS*). En el tercer caso, los sistemas de información, computadoras y elementos informáticos son el facilitador y apoyo a la delincuencia tradicional, tales como el robo, el asesinato y terrorismo, entre otros.

Generalmente, la ciberdelincuencia es considerada como un crimen regular con una nueva modalidad de realización y un medio que, de una u otra manera, es vinculado al uso de Internet, pero difiere un poco. Pues bien, la diferencia es la escala y el alcance de la delincuencia, que utilizando herramientas de escaneo automático pueden ser lanzadas a través de millones de personas en cuestión de minutos. Se opta por dichos medios, debido a las

acciones de los delincuentes y ofrece mayor seguridad e integridad física para éstos, con un nivel de exposición menor, capacidad de existencia de testigos y algo mucho más llamativo, la clandestinidad y persecución jurídica. Por ello, es posible que en cuestión de horas, todo el mundo podría ser cubierto con el mismo virus, gusano o cualquier otra cosa. ¿Cómo evolucionó? Realmente, la ciberdelincuencia comenzó como un *hobby* de informáticos aburridos y jóvenes estudiantes, cuyo objetivo principal era demostrar su destreza y mostrar sus habilidades como *hackers* a la comunidad de sus compañeros. Fueron personas con conocimientos un poco más avanzados, tratando de superarse unos a otros. A pesar de que algunos de los ataques causarían un grave perjuicio económico, los autores rara vez obtenían alguna remuneración económica de los ataques. Y en la mayoría de los casos, las víctimas son al azar, sin objetivos específicos.

Sin embargo, desde la década de los años 2000, se ha venido produciendo un cambio gradual hacia las redes del crimen y criminales más organizados, más que los piratas informáticos individuales. La delincuencia informática se ha convertido en un gran negocio. Y como se puede ver a partir de una serie de delitos informáticos y las violaciones que han ocurrido recientemente, ellos se están enfocando en las empresas que tienen bolsillos profundos financieros, de los que pueden obtener dinero. Un ejemplo que afecta a muchos es la información financiera y su hurto, como los números de tarjeta de crédito/débito. Hay un enorme mercado donde se pueden comprar números de tarjetas de crédito robadas. Y cuando la de tarjeta de crédito no funciona o se ha cerrado, en realidad se puede obtener un reembolso de vuelta.

Figura 1: Extraído de sitio web a través de la Deep web. Disponible en: 7jv2q5zyz4ij6yuf.onion

Se trata de un negocio real con diferentes características de delito cibernético. Uno de los principales fines es recopilar información financiera, secretos comerciales, sobre la disidencia, y cómo involucrar a las grandes corporaciones en situaciones que les representen riesgos.

Y, para cometer un delito no hay que tener grandes conocimientos tecnológicos. De ahí que la extorsión se ubique en el segundo grupo, cambiando sus vectores e ataque en el marco de tecnologías de uso diario, convertidas en un método infalible para el acto. Los casos más conocidos perpetrados por bandas criminales y exempleados poco conformes, quienes logran traspasar los mecanismos y controles de seguridad para amenazar con destruir los datos o revelar información privada, en caso de que no se llegara a pagar dinero por su silencio o protección.

Y, el tercer grupo contempla el fraude en Internet con diferentes modalidades. Por lo general, consiste en facilitar información falsa a un individuo específico o para toda la comunidad. Por ejemplo, las cotizaciones bursátiles pueden ser manipuladas, mediante la fabricación de información positiva o negativa para difundirla entre los participantes y generar subidas y bajadas en los mercados que afectan las acciones. Otra parte de la delincuencia acude al robo de identidad, en el cual los piratas informáticos pueden asumir la identidad de la víctima y asumir su *personaje* en Internet para hacer transacciones en línea o cualquier otro tipo de acciones. El verdadero problema más allá del delito es realmente la víctima, borrar el nombre de ellas de las listas de morosos, para obtener su historial de crédito restaurado, es un problema terrible.

Aun así, en nuestro país existen delitos cibernéticos poco típicos, que se ven como una conducta no delictiva, debido a la falta de una legislación más estricta. Es el caso de la piratería y aquellas acciones que van en contra de la propiedad intelectual.

La ciberdelincuencia también puede clasificarse con base en la sofisticación del medio utilizado. Técnicas criminales implican la intrusión en los ordenadores y las redes, además de *phishing/spoofing*, robo de identidad, denegación de servicio, ataques de suplantación, la manipulación de los servicios de datos, o el fraude. Y las características de estos crímenes incluyen un evento singular o discreto, siempre desde la perspectiva de la víctima, facilitado por *software* malintencionado, como los registradores de pulsaciones (*keyloggers*), *bots*,

Figura 2: Ejemplo de CryptoLoker, Extraído de Malwarebytes. Disponible en: http://images.techhive.com/images/article/2014/01/cryptolocker-100222101-orig.png

spyware, *backddors*, o troyanos. Las características de la delincuencia social contemplan el uso de herramientas legítimas como foros de los medios sociales, aplicaciones de mensajería y sitios *web* de citas. Y las actividades tales como el acoso, la depredación de los niños, la extorsión, el chantaje, el espionaje corporativo complejo y el ciberterrorismo son tipificados como delito.

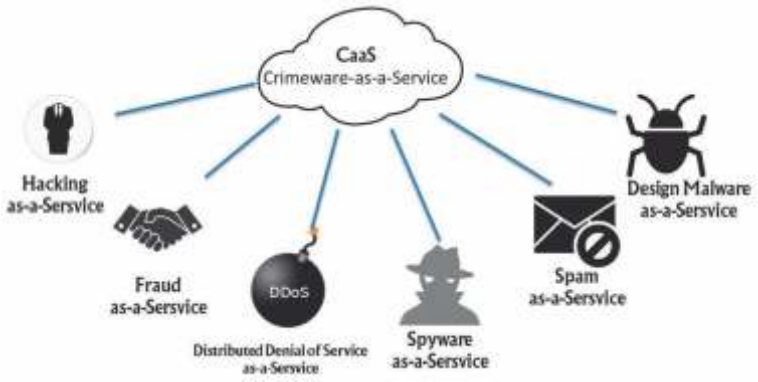
Crimeware, lo que es viejo es nuevo

En aspectos informáticos tenemos que cada tipo de *software*, según su propósito final, tiene un nombre característico. El *crimeware* debe ser diferenciado del *spyware*, *adware* y *malware*. El *crimeware* ha llegado a ser diseñado mediante técnicas de ingeniería social y de fraude, tanto *online* como *offline*, con el único propósito de robo de identidades para acceder a cuentas de compañías que tienden a pertenecer al sector financiero, compañías de comercio por internet y empresas de transacciones electrónicas. Se considera parte de fraude o crimen, debido a que estos programas están diseñados para robar o suplantar la identidad de una persona o usuario.

Hoy se utiliza tecnologías de punta, como lo son los servicios en la nube; de ahí que el *crimeware* sea identificado como *CaaS (Crimeware as a Service)*, donde las personas pueden llegar a escoger el tipo de servicio requerido. La característica más importante de dicho modelo de "negocio" es la clandestinidad que Internet llega a ofrecer, donde los esfuerzos en la parte legal llegarán a ser pieza clave para la persecución de los responsables.

Ciberterrorismo, nuevo campo de batalla

No sólo los fraudes, engaños, acosos, robos y accesos no autorizados se pueden considerar un crimen cibernético. Más allá, existe una amenaza estratégica, el ciberterrorismo. Según Denning, éste puede llegar a entenderse en la convergencia entre lo que es el terrorismo común, pero en un ámbito ciberespacial. Hecho que se basa en fallas, vulnerabilidades y riesgos tecnológicos para lograr intimidar o presionar a un Estado y su sociedad civil. La directiva presidencial Norteamericana No.13010 de 1998, define ocho sectores críticos con servicios vitales para el funcionamiento de la nación, cuya incapacidad de operación o destrucción tendría un



impacto directo en la defensa o en la seguridad económica:

1. energía eléctrica,
2. producción, almacenamiento y suministro de gas y petróleo,
3. telecomunicaciones,
4. bancos y finanzas,
5. suministro de agua,
6. transporte,
7. servicios de emergencia
8. operaciones gubernamentales (mínimas requeridas para atender al público)

El ciberterrorismo puede afectar infraestructuras críticas de un país: sistemas eléctricos, producción, almacenamiento y suministro de combustibles, telecomunicaciones, servicios financieros, sistema de suministro de agua, transporte, en todos sus ámbitos (aéreo, fluvial y terrestre).

Aspectos legales, no todo es tecnología

Es posible llegar a determinar que el ciberespacio se considera una nación globalizada extendida en un ámbito incorpóreo. La expresión comercio electrónico puede tomarse de manera genérica en su significado, mientras que el error que podemos llegar a cometer con el prefijo “ciber”, integra todo aquello intangible en ese meta-espacio.

En Colombia, el uso de un entorno digital y su desarrollo como nación en un ambiente ciberespacial presenta incertidumbres y exposición a riesgos en seguridad. Nuestro país ha hecho esfuerzos enormes en temas legales y procedimentales como lo son la ley de delitos informáticos 1273 del 2009, ley 1581 del 2012 protección de datos personales, ley 1623 de 2013 de inteligencia y criterios de seguridad y el documento CONPES 3854 sobre política nacional de seguridad digital, entre otros.

Sin embargo es posible que las normas nacionales sean inocuas, por ejemplo, para atacar la pornografía infantil o para proteger la confidencialidad de los datos personales. Este espacio global no sólo corresponde a la economía, sino también a otros aspectos sociales como la cultura, la religión, la raza y la política.

Actualidad y hacia dónde vamos

Considerando el ciberespacio como un nuevo sitio, un lugar donde prácticamente desaparece el paradigma de que lo real debe ser físico y tangible, persiste la sensación de cosas imaginativas debido a su particularidad de ser incorpóreo, un lugar diferente al mundo que conocemos. Por ese cambio de ambiente, también se percibe un cambio a nivel de competencias y un ordenamiento distinto. Tales razones llevan a considerar la

necesidad de una Constitución que le de vida a un nuevo Estado dentro de un marco normativo con reglas de incuestionable cumplimiento.

Es necesario tener avances en el proceso antes de lograr un nuevo estado global, y explorar formas más reducidas que agrupen diferentes naciones, hacia una sociedad global. El enfoque de la política de ciberseguridad y ciberdefensa, hasta el momento, se ha concentrado en contrarrestar el incremento de las amenazas cibernéticas bajo los objetivos de defensa y lucha contra el cibercrimen. Los esfuerzos del país han posicionado a Colombia entre los líderes regionales, pero es necesario estimular la gestión del riesgo en el ciberespacio junto con el desarrollo y evolución del marco jurídico.

Referencias

[1] Irvine, Cynthia (2014) *Security Education and Critical Infrastructures*

[2] Ventre, Daniel (2015) *Chinese Cybersecurity and Defense*

[3] Goodman, Marc (2016) *Future Crimes: Inside the Digital Underground and the Battle for Our Connected World*

[4] CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL (2016) Política Nacional De Seguridad Digital. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

[5] Denning, D (2000) *Cyberterrorism*. Disponible en: http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html

[6] Suñé, Emilio (2012) *Declaración de Derechos del Ciberespacio* Disponible en: http://portal.uexternado.edu.co/pdf/7_convencionesDerechoInformatico/documentacion/conferencias/Los_Derechos_Humanos_en_el_Ciberespacio.pdf

[7] Gragido, Will & Pirc, John (2011) *Cybercrime and Espionage*

[8] Andress, Jason & Winterfeld Steve (2011) *Cyber Warfare*

Joshsua J. González Díaz, MSc. *Ingeniero de Sistemas de la Pontificia Universidad Javeriana, especialista en seguridad de la información de la Universidad de los Andes; especialista en Derecho Informático de la Universidad Externado de Colombia y Magíster en Seguridad de la Información de la Universidad de los Andes. Actualmente, se desempeña como profesor instructor de la maestría en Seguridad de la Información de la Universidad de Los Andes y CEO de la empresa de consultoría Stark Industries SAS.*

Fraude informático: una realidad emergente en un mundo digitalmente modificado

Jeimy J. Cano M., Ph.D, Ed.D(c), CFE

Introducción

Los temas de seguridad y control se han convertido en un tema prioritario para las organizaciones [1]. Las diversas formas de controvertir las medidas de protección, por parte de terceros no autorizados o de personal interno de las empresas, establecen verdaderos retos de monitoreo y seguimiento que los encargados de la seguridad o del control de fraude deben afrontar para poder determinar que algo está fuera de un patrón normal [2].

Las conductas engañosas mediadas por estrategias digitales o informáticas, revelan una faceta distinta del fraude, aumentando su capacidad de influencia, sus impactos y, sobre todo, aprovechando ahora la movilidad y las nuevas propuestas de servicios, pueden ser usados por terceros para crear escenarios creíbles y motivadores de actuaciones en las personas, para conducirlas a un artificio [9].

El fraude con componente digital o tecnológico es ahora la evolución natural de las conductas falaces, que

encuentran en el fenómeno técnico un aliado de su actuar, como quiera que el anonimato, la inestabilidad de los rastros y los vacíos jurídicos fundan una dinámica base para desarrollar actividades que permitan lograr defraudar a un tercero, generar una ganancia y desaparecer sin advertir presencia [4].

El fraude como conducta abiertamente contraria al contexto social y que afecta claramente la confianza en las instituciones, es una realidad sistémica que no se encuentra en la tecnología, los procesos o las personas, sino que es una combinación de ellas, tendiente a afectar la buena fe y por ende crear una zona de zozobra para el afectado, con el fin de lograr un beneficio ilegítimo como fruto de sus acciones engañosas y contrarias al orden establecido.

Detectar y procesar conductas de fraude digital o informático, implica comprender la dinámica de la inevitabilidad de la falla, por lo menos en cuatro dominios: las personas y sus comportamientos; los procesos y sus riesgos; la tecnología y sus fallas; además de los cuerpos normativos y sus vacíos, habida cuenta que es allí, en la convergencia de estos cuatro elementos donde se configura la posibilidad de una falacia que lleva consigo la semilla de un delito mayor [7].

Este documento hace una breve introducción a la temática del fraude informático, como una primera mirada sistémica de la problemática, entendiendo que aún existen muchos aspectos por resolver e investigaciones que desarrollar, con el fin de dar cuenta de una realidad que aparentemente sabemos dónde se encuentra, pero no necesariamente conocemos de donde surge.

Fraude: algunas definiciones básicas

El fraude es una condición de engaño, situación que revela una ilusión creada y planeada con determinación para motivar un comportamiento particular en una persona. Este ejercicio crea una ventana de vulnerabilidad -no percibida por la víctima-, donde el defraudador aprovecha su “halo de confianza” para envolver a la persona y materializar su objetivo principal: obtener un beneficio personal o para un tercero.

Cualquiera que sea la técnica de engaño utilizada, es la tecnología la que potencia sus efectos y aumenta su impacto, como quiera que la superficie de acción de la misma, está determinada por artefactos técnicos de uso masivo, que generan suficiente confianza en los suscriptores para que una campaña bien diseñada, basada en gustos y expectativas de las personas tenga éxito [8].

Basta un clic para comprometer la información de un individuo; para generar un vacío de seguridad de la información y para concretar un robo de identidad o materializar un ciberataque de grandes proporciones. Detrás de él, debieron existir meses de revisión y estudio de gustos y rutinas de las personas; inteligencia de fuentes abiertas sobre sus aficiones y preferencias, perfiles de navegación, inclinaciones sociales, académicas o políticas, para definir los vectores de ataque y afectar a la persona objetivo.

Defraudador digital: habilidades sociales, técnicas y de exploración

Los defraudadores digitales son personas hábiles con la tecnología, las relaciones sociales y las estrategias de búsqueda en internet. Estas habilidades llevadas con propósitos contrarios desarrollan contextos enriquecidos y creíbles, crean escenarios fértiles para que individuos desprevenidos caigan en las trampas que los llevan a perder activos de información claves, los cuales pueden ser usados por los delincuentes para cometer otros ilícitos con sus credenciales.

El defraudador digital, no es necesariamente un experto en tecnología, no tiene edad ni condición social ni género específico, pero lo que sí lo identifica es su capacidad para ver la realidad conectada de la persona o personas objetivo, con lo cual determinan su patrón de acción y en forma escalonada acumulan y relacionan información, para fundamentar su estrategia de engaño, elaborada y concreta.

La dinámica de las redes sociales y los constantes bombardeos de la publicidad en línea, crean una vitrina privilegiada para los delincuentes en internet, toda vez que se camuflan detrás de una de estas estrategias legítimas de los comerciantes, para establecer un perfil de invisibilidad capaz de engañar hasta el cibernauta más especializado. En este sentido, contar con el apoyo de la tecnología de información y su capacidad de correlación es clave para aumentar la expectativa de detección y acción sobre actividades ilícitas que comprometan la esfera personal, social, económica y política de las personas. La mentalidad causal de los analistas de fraude, contrasta con la mentalidad relacional de los defraudadores. Mientras unos buscan perfiles de actuación que respondan a patrones de actividad sospechosos, detectados con anterioridad, los delincuentes usan la dinámica de la realidad para crear versiones ligeramente modificadas, que los hagan pasar desapercibidos frente a las tendencias. En tal sentido, el defraudador estará tratando de evaluar la realidad y definir la cotidianidad, como factor clave de éxito para lograr su objetivo con un bajo nivel de detección.

Conexión consciente. Aprender de la dinámica del fraude

Si sabemos que no podemos anticipar muchas de las estrategias de los delincuentes para superar o sabotear los mecanismos de control dispuestos, es necesario desarrollar habilidades complementarias orientadas a aprender y conectar la realidad del fraude, para detectar la frecuencia de su intencionalidad y comenzar a seguirle el rastro más de cerca.

En este sentido, el analista del fraude informático debe ser lo suficientemente abierto para desaprender y quebrar sus modelos mentales, de manera de entrar en una conexión consciente con la realidad del fraude, que lo lleve a experimentar nuevas propuestas y a ampliar su visión estratégica de detección, usando realidades alternativas antes inexploradas.

En este sentido, parafraseando las prácticas de conexión consciente de un *Chief Information Security Officer* –CISO-, Oficial de Seguridad de la Información [3], en la lectura del analista o ejecutivo de control y

prevención del fraude, se proponen las siguientes acciones:

- **Dejar de luchar, aprender y anticipar**. El fraude no es una lucha contra el engaño; se trata de encontrar formas diferentes de mejorar las prácticas de prevención, detección, monitorización y control. Mientras más lucha se ejerza contra el oponente, menor capacidad de acción habrá para estudiarlo y superarlo (o anticiparlo). Siempre es posible dar un paso adelante del fraude, si el afectado es capaz de conectarse con él. Es decir, aprender y desaprender de su dinámica.

- **Escuchar la voz interior**. No importa lo hábil que el usuario se haya vuelto para identificar y afrontar retos en la detección, prevención y monitorización del fraude, pues siempre habrá momentos de incertidumbre y confusión. Meditar en los mensajes de voz interiores y en los diferentes análisis y reflexiones frente a la situación difícil, es una alternativa. Así mismo, detenerse en el silencio de la conexión con el fraude, para superar los límites mentales autoimpuestos y poder actuar en consecuencia.

- **Retar los límites**. Buscar dentro de sí aquellos paradigmas que parecen haber funcionado y ponerlos en práctica frente a la realidad existente. No es necesario hacer grandes cambios de estándares y prácticas, sino tomar aquellos que son claves, cuyas transformaciones pueden leer mejor las expectativas de los clientes y aumentar la confianza de estos frente a la detección, prevención y monitorización del fraude.

- **Permanecer centrado, en equilibrio**. Estar centrado es estar conectado con la propia fuente de equilibrio. En la detección, prevención, monitorización y control del fraude es necesario estar en constante exploración y conocimiento, conscientes de la ambigüedad permanente y en movimiento con el engaño. El responsable antifraude está centrado, cuando su atención está en el fluido del presente y su energía concentrada en la dinámica del cambio. No se dispersa; por el contrario, identifica la incertidumbre estructural presente en la realidad.

- **Superar las creencias personales**. Entre más fuertes sean las creencias, más estrecho será el punto de vista [5]. El ejecutivo antifraude que quiera tener éxito deberá ser flexible, conjugar los distintos puntos de vista y combinarlos con la perspectiva de riesgos. En la medida en que es posible reconocer otras miradas sobre la misma realidad de la amenaza identificada, es posible superar y confrontar los límites que imponen los propios paradigmas.

- **Capturar información de todas las fuentes posibles.** Cuando se advierten situaciones donde se configuran dilemas, es preciso consultar diferentes puntos de vista, aceptando lo que todos tienen que ofrecer. La lectura del riesgo es relativa al contexto y cada persona lo puede leer según la propia experiencia. En este sentido, es necesario configurar una vista agregada de opiniones para revelar aquellos intereses inmersos, para poder tomar una decisión conforme a lo que requiere el momento y la situación, sin dejarse invadir o

seducir por una postura en particular.

- **Aprender a tener intenciones claras**. En la detección y prevención del fraude, una intención clara, significa tener un propósito. Una afirmación que contempla la dinámica de la organización y los objetivos de negocio, para hacer congruente la práctica antifraude con las necesidades y retos de la empresa. Un ejercicio que permanece alerta a las señales del entorno, para tener conciencia de cada paso en la dirección que confirma dicho propósito.

Reflexiones finales

La dinámica del fraude informático o hiperconectado en el contexto de un mundo digitalmente modificado, comporta un proyecto de transformación social y cultural contrario a la sociedad, que busca desestabilizar y tensionar el orden existente, no de forma preferente y directa, sino con acciones discretas y poco visibles, de tal forma que los miembros de esta comunidad con intencionalidad criminal, independientemente de su condición personal, económica, política, religiosa, social, aportan capacidades distintivas que capitalizan de forma integrada, cuando se concretan los engaños para una empresa, persona o grupo de interés.

En este entendido, los defraudadores digitales comparten información y analizan datos de forma colectiva, para detectar las tendencias más sobresalientes, habida cuenta de que ellas servirán de puente y apoyo necesario para coordinar actividades o intentos de nuevas formas de trampas. De esta forma, estas comunidades crean un proceso de cambio de percepción, con una secuencia asimétrica de intenciones aparentemente llenas de "luz", las cuales terminan en resultados que enriquecen sus bolsillos, dejando al vaivén de las otras variables del entorno, las marcas cognitivas, afectivas, personales y sociales en sus víctimas.

Frente a esta realidad es necesario un diálogo transdisciplinar orientado a una reflexión desde la persona, los procesos, la tecnología y las regulaciones, para facilitar la construcción de fundamentos conceptuales de forma holística [6], adaptados a la realidad de un mundo digital y conectado, con el fin de crear una red de conocimientos complementarios que valore las contradicciones impuestas por la realidad del fraude y haga de ellos, una capacidad clave que considere las estrategias disponibles a la fecha para su prevención, monitorización, detección y control en las organizaciones modernas.

Referencias

[1] Bughin, J., Lund, S. y Manyika, J. (2016) Five priorities for competing in an era of digital globalization. *Mckinsey Quarterly*. Mayo. Recuperado de: http://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/five-priorities-for-competing-in-an-era-of-digital-globalization.

[2] Álvarez, M. (2016) Insider Attacks May Be Closer Than They Appear. Recuperado de: https://securityintelligence.com/insider-attacks-may-be-closer-than-they-appear/.

[3] Cano, J. (2015) Conexión consciente. Siete prácticas para habilitar una visión

trascendente en seguridad de la información. Recuperado de: https://www.linkedin.com/pulse/conexi%C3%B3n-consciente-siete-pr%C3%A1cticas-para-habilitar-en-jeimy.

[4] Cano, J. (2016) Cinco premisas de la delincuencia digital en un mundo digitalmente modificado. Recuperado de: https://www.linkedin.com/pulse/cinco-premisas-de-la-delincuencia-digital-en-un-mundo-jeimy.

[5] Chopra, D. (2014) *El alma del liderazgo. Descubre tu potencial de grandeza*. Bogotá, Colombia: Punto de Lectura.

[6] De Geus, A. (2011) *La empresa viviente. Hábitos para sobrevivir en un ambiente de negocios turbulento*. Buenos Aires, Argentina: Gránica.

[7] Kessem, L. (2016) 2016 Cybercrime Reloaded: Our Predictions for the Year Ahead. Recuperado de: https://securityintelligence.com/2016-cybercrime-reloaded-our-predictions-for-the-year-ahead/.

[8] Vax, S. (2016) Mobile Malware on Smartphones and Tablets: The Inconvenient Truth. Recuperado de: https://securityintelligence.com/mobile-malware-on-smartphones-and-tablets-the-inconvenient-truth/.

[9] Verizon (2016) 2016 Data breach investigations report. Recuperado de: http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/.

Jeimy J. Cano M., Ph.D, Ed.D(c), CFE. *Ingeniero y Magíster en Sistemas y Computación por la Universidad de los Andes. Ph.D in Business Administration por Newport University; Especialista en Derecho Disciplinario por la Universidad Externado de Colombia y candidato a Doctor en Educación en la Universidad Santo Tomás. Cuenta con un certificado ejecutivo en gerencia y liderazgo del MIT Sloan School of Management, MA, USA. Profesional certificado como Certified Fraud Examiner (CFE) por la Association of Certified Fraud Examiners y Cobit5 Foundation Certificate de ISACA. Director de la revista "Sistemas", de la Asociación Colombiana de Ingenieros de Sistemas –ACIS-.*

PREMIO COLOMBIANO DE INFORMATICA 2016

EMPRENDEDOR COLOMBIANO EN TI

Este año 2016, la Asociación quiere hacer un reconocimiento especial al emprendedor en Tecnologías de la Información (TI) destacado, a nivel nacional. Para merecer el PREMIO COLOMBIANO DE INFORMÁTICA 2016, un emprendedor presentado deberá cumplir con los siguientes criterios:

1. Ser nominado por uno o varios miembros de la Asociación a través de la página de ACIS.

2. Ser nacional colombiano.

3. Ser un emprendedor destacado en el ámbito nacional o internacional, y presentar al Jurado del Premio 2016 (directamente o por intermedio de su postulante) un resumen de sus emprendimientos y contribuciones al desarrollo de la Ingeniería de Sistemas y sus aplicaciones prácticas. Énfasis en sus logros, impacto en la comunidad, su entorno y la sociedad en general, así como su aporte al desarrollo del país, son requeridos.

4. Aceptar los criterios de evaluación del jurado, su calificación y resultados del proceso de selección.

Los emprendimientos relacionados NO pueden corresponder a trabajos académicos, como tesis de pregrado o postgrado puesto que el Premio se dirige a emprendimientos que denoten una considerable experiencia profesional (las tesis tienen por su parte otros espacios académicos en donde pueden concursar).

Fechas y mayor información

Fecha de apertura de la convocatoria: Marzo 30 de 2016.
Fecha de cierre de la convocatoria: Agosto 15 de 2016.

DIGIWARE
Su aliado en seguridad de la información

¿Conoce los riesgos que atraviesa su organización?

Es indispensable conocer el estado actual de su compañía, hacer una proyección a futuro y obtener una visión de los retos que enfrentará en la protección de sus activos de información.

1. Los ataques continúan siendo exitosos
2. Presupuesto de seguridad limitado
3. Gestión de riesgos conocidos, pero no de desconocidos
4. El cibercrímen es un negocio y no va a parar

CONSULTORÍA

Definición, implementación y oportuno mantenimiento de programas estratégicos de seguridad de la información, que se integren con la estrategia del negocio de cada organización.

SOLUCIONES TECNOLÓGICAS

Digiware provee las mejores soluciones de tecnología del mercado, ajustándolas a las necesidades puntuales de los clientes y brindando en cada herramienta, el respaldo y soporte constante.

SEGURIDAD GESTIONADA SOC

Gestionamos inteligencia en seguridad de la información para convertirla en una estrategia de negocio con ROI y la visibilidad necesaria para prevenir incidentes oportunamente.

FORMACIÓN DEL TALENTO HUMANO

Actualícese con nuestro grupo experto de I+D, comprometido con las problemáticas existentes en seguridad de la información y conviértase en un especialista en la materia.

Construyendo inteligencia en seguridad de la información

Information Security Trends Meeting 2016

El evento de seguridad de la información más importante de Latinoamérica

Agosto 11 / 2016
Club El Nogal / Bogotá, Colombia

Información e inscripciones

+(57)1 7443666 Ext. 2124
mercadeo@digiware.net
+(57) 3214900508
www.istmconference.org

www.digiware.net

• Centroamérica y El Caribe • Chile • Colombia • Ecuador • E.E.U.U. • Perú

Universidad Externado de Colombia

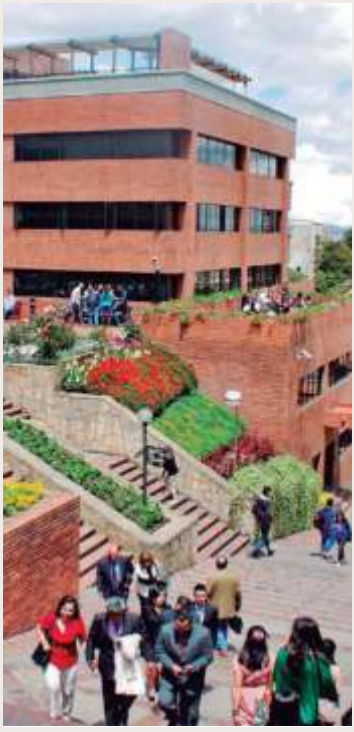
FACULTAD DE CONTADURÍA PÚBLICA

PROGRAMA DE PREGRADO

- **Contaduría Pública**
  CÓD. SNIES 1117
  Acreditación de alta calidad por seis años

PROGRAMAS DE ESPECIALIZACIÓN

- **Administración de Riesgos Informáticos**
  Bogotá CÓD. SNIES 15900
- **Auditoría Forense**
  Bogotá CÓD. SNIES 52169 / **Cartagena** CÓD. SNIES 102931
  Tunja CÓD. SNIES 102857 / **Villavicencio** CÓD. SNIES 103786
- **Control Gerencial Corporativo**
  Bogotá CÓD. SNIES 15901 / **Barranquilla** CÓD. SNIES 102960 / **Bucaramanga** CÓD. SNIES 102959
- **Gerencia y Administración Tributaria**
  Bogotá CÓD. SNIES 15860 / **Pereira** CÓD. SNIES 90828 / **Villavicencio** CÓD. SNIES 103779
  Tunja CÓD. SNIES 105144
- **Revisoría Fiscal y Auditoría Internacional**
  Bogotá CÓD. SNIES 4747



DESARROLLO EMPRESARIAL Y EDUCACIÓN CONTINUADA

DIPLOMADOS

- Normas Internacionales de Información Financiera
- Normas Internacionales de Auditoría y Aseguramiento
- Actualización Tributaria

SEMINARIO

- Actualización Tributaria

CURSOS

- Curso Taller Adopción por primera vez de las NIIF en PYMES
- El Despacho Profesional en la Contaduría Pública

UNIVERSIDAD EXTERNADO DE COLOMBIA
Calle 12 n.º 1-17 este. Bogotá - Colombia
PBX (1) 353 7000 / 342 0288 / 341 9900

FACULTAD DE CONTADURÍA PÚBLICA
Exts. 1351, 1359, 1355, 1346, 1357, 1349
faccontaduria@uexternado.edu.co
poscontaduria@uexternado.edu.co
dir.dempresarial@uexternado.edu.co

ADMISIONES Y PROMOCIÓN UNIVERSITARIA
Edificio A, piso 4.º, exts. 4301 a la 4309
admisiones@uexternado.edu.co