8-10-2020

Estudio de la Evolución de los Incidentes de Seguridad Informática en Colombia: 2010-2020

Jeimy J. Cano M.
Universidad de los Andes, jcano@uniandes.edu.co

Andrés Ricardo Almanza Junco
Asociación Colombiana de Ingenieros de Sistemas (ACIS), andres.almanza@acis.org.co

Estudio de la Evolución de los Incidentes de Seguridad Informática en Colombia: 2010-2020

Artículo Completo

Jeimy J. Cano M.
Universidad de los Andes
jcano@uniandes.edu.co

Andrés Ricardo Almanza Junco
Asociación Colombiana de Ingenieros de Sistemas (ACIS)
andres.almanza@acis.org.co

Abstract

The evolutive study of information security incidents in Colombia is an effort made by the Colombian Association of Systems Engineers (ACIS), which for more than 10 years has been applying a national information security survey in order to study and understand the evolution of information security in the Colombian context. The analysis of the results of the last 10 years on the subject of incidents shows the most relevant trends in the country, based on the number of incidents, the types of incidents and how their presence in the organizations is noticed. The reflections that are proposed for each of these elements are contrasted with the readings of international reports in order to situate the specific challenges of the companies in the different sectors of the Colombian industry.

Keywords

Security, Evolution, Colombia, Analysis, Longitudinal, Incidents.

Resumen

El estudio evolutivo de los incidentes de seguridad informática en Colombia es un esfuerzo realizado por la Asociación Colombiana de Ingenieros de Sistemas (ACIS), quien durante más de 10 años ha venido aplicando una encuesta nacional de seguridad de la información con el fin de estudiar y entender el comportamiento de la seguridad en el contexto colombiano. El análisis de los resultados de los últimos 10 años en la temática de incidentes muestra las tendencias más relevantes en el país, basadas en la cantidad de incidentes, los tipos de incidentes y cómo se advierte su presencia en las organizaciones. Las reflexiones que se plantean para cada uno de estos elementos se contrastan con las lecturas de reportes internacionales con el fin de situar los retos concretos de las empresas en los diferentes sectores de la industria colombiana.

Palabras Clave

Seguridad, Evolución, Colombia, Análisis, Longitudinal, Incidentes.

Introducción

Los incidentes de seguridad son momentos de verdad para las organizaciones en general. Definen y revelan los puntos ciegos que las empresas tienen en sus modelos de seguridad y control, los cuales son aprovechados frecuentemente por los adversarios (Cano, 2020). Las fallas de seguridad son realidades inherentes en las compañías comoquiera que la inevitabilidad de la falla es una norma en todos los escenarios de la vida empresarial, lo que implica necesariamente romper con el imaginario ejecutivo de riesgo "cero" y seguridad ciento por ciento.

Si bien las vulnerabilidades presentes en los diferentes componentes de los modelos de seguridad y control son fuente de inestabilidad y "pérdida de control", de igual forma son fuente de conocimiento y

ventanas de aprendizaje que permiten conocer mejor la manera para hacer más resistente las estrategias de protección diseñadas al interior de las organizaciones. Cuando las debilidades de control se entienden como resultado de las condiciones del entorno de operación de una persona o componente, no se intenta buscar culpables o responsables de los eventos, sino comprender qué fue lo que llevó a que la situación se manifestara y establecer aquellos puntos de inestabilidad que se deben fortalecer de cara al futuro (Reason, 2000).

En este sentido, estudiar los incidentes más relevantes en la realidad de la práctica y gestión de la seguridad informática y de la información en un país, ofrece una vista general y orientaciones concretas sobre aquellos puntos de inflexión que son claves en la dinámica de control de la información de las empresas, con el fin de llamar la atención sobre las posibles cegueras cognitivas que pueden pasar inadvertidas, para ajustar los programas de seguridad y control de las organizaciones más allá del aseguramiento de las recomendaciones propias de los estándares y las buenas prácticas.

Los resultados de la Encuesta Nacional de Seguridad Informática (ENSI) ejercicio de exploración y análisis de las prácticas y gestión de la seguridad informática en Colombia, que se ha venido realizando en los últimos 20 años con el apoyo de la Asociación Colombiana de Ingenieros de Sistemas, establecen algunas tendencias en sus diferentes variables estudiadas. Particularmente, para este estudio se ha tomado la variable de los incidentes, entre los años 2010 a 2020, en los cuales se indaga sobre la cantidad de incidentes, tipo de incidentes, sectores productivos donde ocurren y cómo se enteran las organizaciones de estos.

Cada una de las temáticas estudiadas alrededor de los incidentes manifiestan patrones de interés para las compañías en el país en sus diferentes sectores, donde se advierten que en promedio se tienen entre 1 y 3 incidentes anualmente, que la instalación de software no autorizado es el incidente de mayor puntuación, que si bien todos los sectores muestran evidencia de eventos no deseados, el sector financiero es el que frecuentemente manifiesta un alto nivel incidentes relacionados con el engaño y el fraude en línea (phishing) y que la manera más recurrente de la notificación de incidentes se hace directamente a los directivos de las organizaciones en Colombia.

En resumen, este artículo se desarrolla desde una vista general de antecedentes que contextualiza el estudio, seguidamente se detallan sus aspectos metodológicos, se hace una breve mención sobre el instrumento utilizado para la investigación, así como de la población encuestada, para finalmente terminar con los resultados, su análisis y las conclusiones más relevantes.

Antecedentes

Los incidentes de seguridad informática (ISI), como aquellas materializaciones de vulnerabilidades conocidas o desconocidas en los modelos de seguridad y control de las empresas, son momentos adversos que se presentan en todas las organizaciones, que implica el desarrollo de ciclos metodológicos que le permitan darle una adecuada gestión. Conocer cómo evolucionan, los tipos que se presentan, a qué sectores afecta y con qué frecuencia, resulta de interés para establecer estrategias de preparación que habiliten a las organizaciones para hacerle frente a dichos eventos contrarios.

Así mismo, el contraste de estos resultados con las tendencias internacionales configura un espacio de análisis extendido que enmarca la realidad de este estudio para situar los retos que las empresas tienen de cara a los incidentes. Es por ello por lo que dentro de los estudios estudios referentes que se consultaron y analizaron se encuentran el Managing Enterprise Risks in a Digital World realizado por la firma BakerHostetler (BakerHostetler, 2019), el Estudio de la evolución de la Seguridad de la Información en Colombia de ACIS (ACIS, 2020), el Incident Response & Data Breach Report de Crypsis (Crypsis,2020), ESET Security Report 2019 (ESET, 2019), el How does security evolve from bolted on to built-in? consolidado por la empresa Ernst &Young (EY, 2019), el Informe 23nd Annual Global CEO Survey de la compañía PwC (PwC, 2020), el reporte Data Breach Investigation Report de Verizon (Verizon, 2020), el reporte de Riesgos globales del Foro Económico Mundial (WEF,2020), la vista del CyberSecurity Report LATAM realizado por el Banco Interamericano de Desarrollo – BID y la Organización de Estados Americanos – OEA (OEA-BID, 2016), entre otros reportes de industria.

Metodología

En esta sección se presentan los aspectos metodológicos de esta investigación, describiendo los detalles del proceso realizado, la preparación del instrumento de recolección, la estrategia de recolección de la información, así como los ejercicios propios de la tabulación de los datos.

Perspectiva Metodológica

Este estudio, hace una lectura cualitativa del entorno basado en una encuesta de selección múltiple, cuyos resultados son revisados con apoyo de elementos cuantitativos de estadística básica para comprender los factores o fenómenos relevantes a la seguridad de la información en el contexto colombiano. En este sentido, se considera que la realidad de la seguridad de la nación se funda en las interacciones e interrelaciones que las empresas y las personas desarrollan para construir y revelar una realidad particular y propia del país, sin perjuicio de sus semejanzas con otras naciones en el mundo. Por tanto, bajo esta perspectiva se busca entender la experiencia que las personas comparten en ciertas temáticas consideradas claves en materia de seguridad y ciberseguridad. En particular, se toman las respuestas de la encuesta nacional de seguridad informática, en el componente de incidentes en las tres temáticas previamente mencionadas.

Instrumento de Investigación

Este estudio se realiza basado en una de las variables de la encuesta nacional de seguridad informática que consta de un cuestionario de 40 preguntas, con selección múltiple (incluida la opción abierta para otros, cuando es necesario), donde cada participante de la encuesta en línea puede indicar sus preferencias y establecer, basado en su experiencia, las respuestas con las que más se identifique. Lo anterior corresponde a la observación de fenómenos tal y como se dan en un entorno, sin la intervención directa de los investigadores, con el fin de examinar los cambios que se dan a lo largo del tiempo en grupos específicos que están vinculados con las labores relacionadas con la gestión y el gobierno de la seguridad de la información en Colombia.

En relación con el análisis de la gestión de incidentes en este estudio se consideran los siguientes elementos a revisar.

- Gestión de incidentes:
    - Cantidad de incidentes: Relacionado con evaluar el número de incidentes de seguridad que se pueden presentar en una organización en un año. Se usa una escala numérica para cuantificar.
    - Tipos de incidentes: Se toma la taxonomía de los distintos incidentes de seguridad disponibles a la fecha y que se reportan en el país, la cual evoluciona con el tiempo y se alimenta de las tendencias internacionales.
    - Notificación de incidentes: Relacionado con la forma en cómo los encuestados reportan los incidentes de seguridad en las organizaciones.

Población Encuestada

La ENSI año tras año es distribuida a través de correo electrónico, a una comunidad de más de 3000 profesionales registrados en la Asociación Colombiana de Ingenieros de Sistemas (ACIS), redes sociales y grupos o comunidades de ciberseguridad/seguridad de la información en Colombia, más de 10 grupos y/o comunidades de alrededor de 500 personas o más, para ser diligenciada de manera virtual, a través de un formulario en la Web configurado a través de la plataforma Surveymonkey. La población seleccionada responde a la comunidad de seguridad de la información que se tiene en Colombia, que se coordina desde la ACIS hace 20 años, quienes están al frente de las operaciones y gerencia del área en el país, de los cuales, en promedio participan 186 profesionales a nivel nacional.

Planificación del Documento

Año tras año se hace una revisión y análisis del cuestionario utilizado por parte de los investigadores que apoyan el proceso de ejecución y análisis de la encuesta, con el fin de efectuar los ajustes que sean necesarios y así contar con un instrumento más depurado y acorde con la evolución de las temáticas en seguridad de la información.

Luego de estas adecuaciones y modificaciones se procede a utilizar la plataforma virtual destinada para tal fin, para realizar las pruebas de funcionalidad y de cohesión en relación con la dependencia de las preguntas. Seguidamente se hace el despliegue de la encuesta en todas las comunidades que se han definido.

Procesamiento

Una vez concluida la encuesta se extraen las respuestas totales del cuestionario en una hoja cálculo, para adelantar el estudio de los datos planeados utilizando otras herramientas de analítica de datos que permitan generar reflexiones particulares a cada una de las temáticas del cuestionario, así como vistas cruzadas de algunos de los temas de interés. En particular, se presentan a continuación los resultados para la variable de los incidentes de seguridad en Colombia.

Limitaciones del Estudio

El estudio realizado sobre los incidentes de seguridad informática en las organizaciones colombianas en la última década busca perfilar la dinámica de esta realidad y establecer marcos de acción concretos para las empresas. En este sentido, establecer los impactos de estos en cada sector y su correlación con otras variables, si bien puede resultar de interés, no se adelantaron toda vez que no se identificaron reportes estadísticos concretos confiables consolidados por sectores en el país en esta temática y por las limitaciones propias de los tiempos previstos para la realización del estudio.

Resultados

Los resultados que se presentan a continuación corresponden a los valores promedios más importantes y relevantes de la encuesta en la dimensión relacionada a la gestión de incidentes de seguridad informática de los últimos diez años.

Incidentes

Cantidad de incidentes: Los resultados establecen que, en el contexto colombiano, el promedio de incidentes de seguridad informática se presenta en el segmento de 1 a 3 con un 28% en promedio durante los 10 años de análisis, entre 4 a 7 incidentes el promedio es de 15%, más de 7 incidentes está en un 16%, ninguno está en un 9% y un 33% manifiesta en promedio no contar con esa información para responder.

Tipos de incidentes: En este estudio se consideran 24 tipos de incidentes, que se han venido estudiando durante los 10 años. Los datos se muestran en la tabla 1.

Tipos de Incidentes	Promedio
Instalación de software no autorizado	38%
Virus/Caballos de Troya	34%
Phishing	22%
Accesos no autorizados al web	22%
Acciones de ingeniería social	14%

Tipos de Incidentes	Promedio
Negación del servicio (DOS/DDOS)	12%
Robo de elementos críticos de hardware (notebooks, discos, etc.)	11%
Errores Humanos	11%
Manipulación de aplicaciones de software	11%
Pérdida/Fuga de información crítica	11%
Ataque de aplicaciones Web (XSS, SQL Injection, Directory Transversal, etc.)	10%
Fraude electrónico	10%
Pérdida de integridad de la información	9%
Suplantación de identidad	8%
Ninguno	7%
Ransomware	7%
Robo de datos	6%
Incidentes relacionados con la privacidad de los datos personales (publicación de información personal, solicitudes de eliminación de datos personales, etc.)	6%
Monitoreo no autorizado del tráfico	5%
Ciberataques (APT o ataques dirigidos, denegación de servicios masiva)	5%
Otra (Por favor especifique)	3%
Espionaje	2%
Pharming	2%
Brecha de seguridad provocada por terceras partes (p.e Cloud Access Security Broker)	1%

Tabla 1. Tipos de Incidentes y Promedios de Frecuencia

Notificación de los incidentes: En cuanto este ítem, lo que se identifica es que el 50% reporta a los Directivos de la organización en primer lugar, seguido de los equipos de atención de incidentes (CSIRT) con un 29%, 13% no informa o denuncia la situación, el 12% lo reporta a las áreas legales, 15% a las autoridades nacionales, un 8% utiliza otras opciones y el 7% lo reporta a autoridades regionales o locales.

Análisis de Resultados

Incidentes de seguridad, constante de las empresas.

Los incidentes de seguridad informática evolucionan en cada uno de los rangos establecidos durante los años del estudio. La figura 1, muestra la forma como cambian, resaltando que los incidentes entre los rangos de 1 a 3, más de 7 y entre 4 y 7 incidentes, tienen un movimiento similar durante los 10 años analizados, mientras se mantiene una tendencia decreciente de la variable ningún incidente de seguridad en el mismo periodo. De igual manera, en dicha figura se observa un patrón creciente de la variable "no cuento con esa información", lo que se traduce en un llamado de atención a las empresas colombianas y sus profesionales de seguridad para fortalecer la monitorización de vulnerabilidades y la gestión de incidentes que permitan identificar y comunicar a todas las partes interesadas la información respectiva relativa a los incidentes y sus implicaciones en las organizaciones.

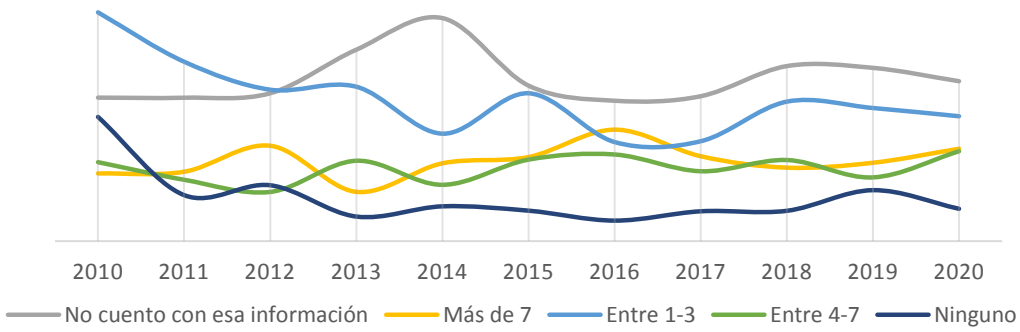

Figura 1. Evolución de la Cantidad de Incidentes

En la consolidación y análisis de los datos de los 10 años recolectados, como se observa en la figura 2, todos los sectores han experimentado incidentes de seguridad y cabe resaltar que la categoría denominada "ningún incidente", es la más baja en resultados con solo un 9% como valor promedio. Por otro lado, el 33% en promedio de todos los sectores manifiestan que aún se desconoce esa información, lo que sugiere que no hay claridad si los incidentes son identificados y en qué cantidad en sus organizaciones.

Este desconocimiento puede explicarse por varios elementos. Primero que no existen líneas claras de comunicación en el proceso de la gestión de incidentes. Esto es, quien identifica la falla, puede no estar notificando a las partes interesadas sobre la incidencia detectada. Segundo, que los procesos de gestión de incidentes no se estén llevando de manera ordenada y sistemática, lo que implica una ejecución parcial del mismo. Tercero, que los equipos de respuesta a incidentes están desconectados de los otros equipos que apoyan la gestión en la organización. Cuarto, la organización cuenta con limitadas capacidades tecnológicas para monitorizar, identificar, y reportar los incidentes y, por último, puede estar asociado con los profesionales encuestados, que posiblemente no han sido incluidos en los procesos de gestión de incidentes y por tanto no conocen la dinámica que se maneja al interior de la organización.

De cara al reto del adversario digital y los efectos que producen los incidentes de seguridad que estos generan, se hace necesario que el proceso de la gestión de incidentes sea una pieza fundamental de la postura y estrategia de ciberseguridad de las empresas, propendiendo por atender, y gestionar de manera ordenada y sistémica los eventos digitales que puedan crear inestabilidad en la operación de las empresas.

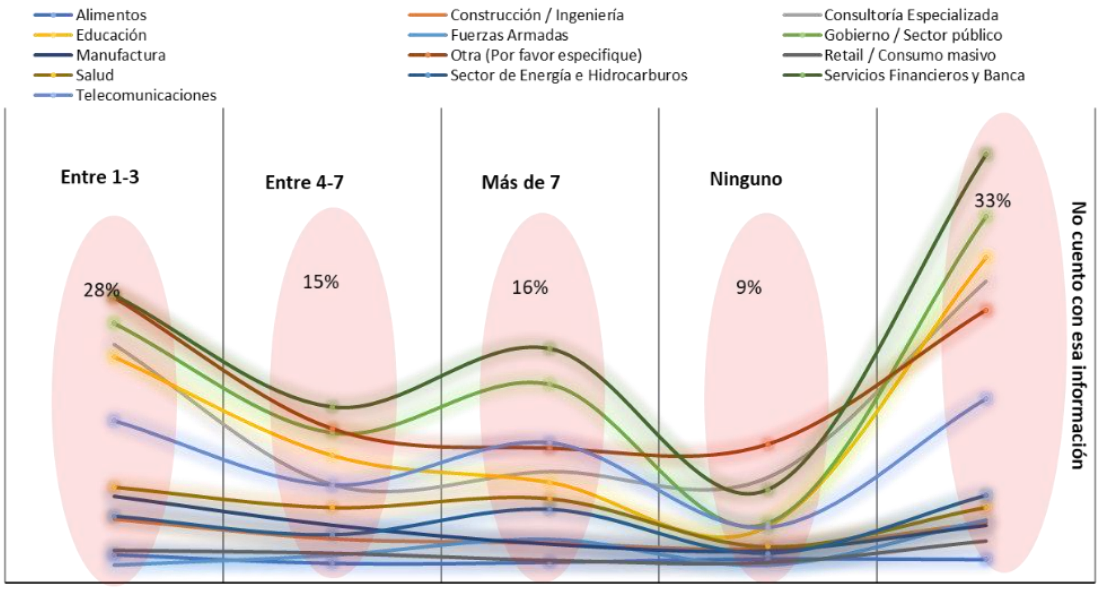

Figura 2. Sectores y Presencia de Incidentes

Los datos de Colombia muestran que entre 1 y 3 incidentes de seguridad se presentan en los distintos sectores de la industria, afirmación que se confirma en el informe de ESET (2019), el cual manifiesta que en Latinoamércia dos de cada tres empresas sufrieron un incidente de seguridad durante el 2018.

Al revisar, con mayor detalle los sectores analizados se identifica, que aquellos donde hay mayor presencia de incidentes, como son el financiero, el gobierno, los servicios de consultoría especializada y las telecomunicaciones, es donde se han desarrollado mayores capacidades para la detección de incidentes (Cano & Almanza, 2020).

De esta forma, Colombia se adhiere a la realidad global en materia de incidentes de seguridad digital; tendencias que se ven reflejadas en el informe del Foro Económico Mundial en su XX edición WEF (2020), que cataloga a los ciberataques como una realidad global. De la misma manera, el estudio de EY (2019) manifiesta que 6 de cada 10 organizaciones, que equivale al 59%, ha enfrentado durante el año al menos un incidente, los cuales serán cada vez más notorios en las organizaciones según manifiestan sus ejecutivos.

Tipos de incidentes, más que solo un caso

Los datos de Colombia muestran que son diversos y variados los tipos de incidentes que se presentan. En estos últimos 10 años, aunque los incidentes son distintos y aparecen muchos más en tiempos más cortos, hay tendencias marcadas que se mantienen. Según un estudio reciente realizado por Cano & Almanza (2020), las instalaciones de software no autorizado 28%, la ingeniería social 26%, el phishing 23% y el ransomware 18%, son los de crecimiento sostenido en Colombia entre los años 2000 y 2018.

La figura 3, muestra el comportamiento de los 24 tipos de incidentes que se han monitoreado a través de la encuesta y su comportamiento durante los 10 años de estudio. Todas sin excepción, con las variaciones respectivas propias de los adversarios digitales, tienen presencia dentro de la realidad de las empresas colombianas.

Algunos de los datos relevantes identificados en este estudio, están relacionados con la evolución de los tipos de incidentes durante el marco de tiempo definido para la investigación. De ellos se resalta que el tipo de incidente Pharming, ha tenido un crecimiento equivalente al 47%, seguido de los incidentes relacionados con la privacidad con un 25%, los ciberataques y el phishing en tercer lugar con un 24%, la pérdida de integridad de la información es el siguiente con un 23% de crecimiento, seguido del espionaje que tiene un 21%, los ataques de ingeniería social y el monitoreo del tráfico no autorizado con un 19%, el fraude electrónico con un 17% y la suplantación de identidad con un 16%.

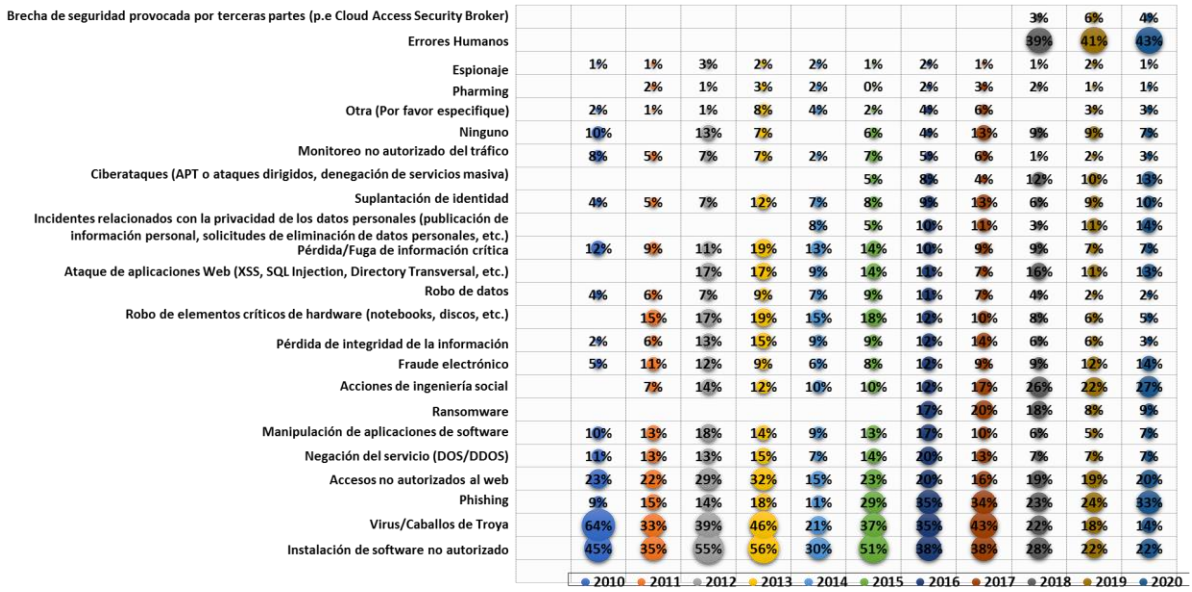

Figura 3. Evolución de los Tipos de Incidentes

Colombia no es ajena a la realidad mundial. Según BakerHostetler (2019), el 39% de los incidentes están relacionados con casos de Phishing, datos que coinciden con los resultados presentados en este artículo, donde los ataques de Phishing crecen de manera significativa con un 24% en los 10 años analizados. Así mismo Secureworks (2019), manifiesta que el Ransomware es uno de los incidentes que registra incrementos de 21%, dato que contrasta con los resultados de este estudito, donde en 5 años de medición de la extorsión con datos, se advierte un aumento del 4%. Si bien, esta temática no crece de la misma manera que lo refleja el informe internacional, si se revela una tendencia sostenida de crecimiento frente a las demás anomalías.

Sectores, no todos sufren de lo mismo

Al revisar la forma como cada industria se ve afectada por los tipos de incidentes durante el periodo de tiempo analizado, se evidencian dinámicas no uniformes que se advierten en la figura 4. Los datos revelan que los incidentes que más se presentan en todas las industrias están relacionados con la instalación de software no autorizado, los virus y los caballos de troya. Sin embargo, en la banca, el phishing resulta ser el más relevante como se indica en la figura 4.

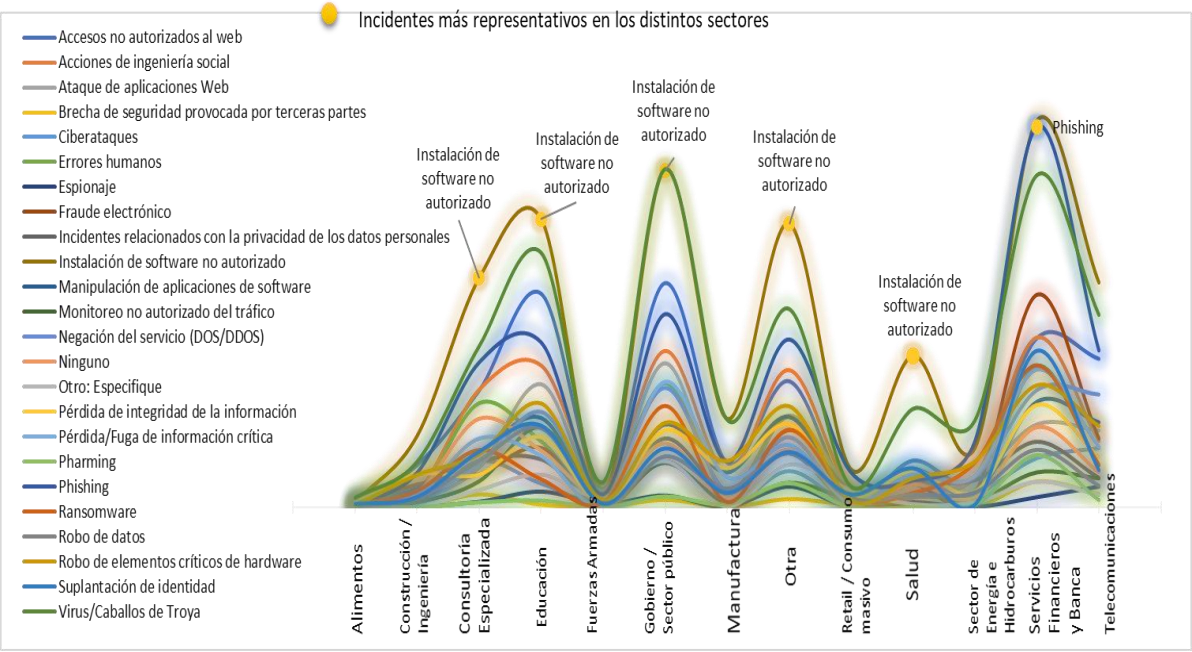

Figura 4. Sectores vs Tipos de Incidentes

En su informe Checkpoint (2020), resalta que el sector financiero es uno de los sectores con mayor presencia de incidentes de seguridad. Los datos acumulados de la evolución de la seguridad de la información de Colombia muestran la misma tendencia. Por su parte, Cripsys (2020), manifiesta como dato adicional que el sector de la Salud durante el año 2019 reportó mayor presencia de incidentes de seguridad, lo que igualmente se empareja con los datos históricos de Colombia, donde se puede evidenciar, una tendencia creciente en el número de incidentes en la franja entre 4 y 7, que representa un 11,37%, así como entre 1 y 3 incidentes con un crecimiento de 1,31%.

Los reportes internacionales como el de Ponemon-IBM (2020), evidencian que las vulnerabilidades relacionadas con el software representan el 86% de los casos de incidentes, resultados que se ratifican a través de la historia de los datos de Colombia, en donde los incidentes relacionados con el software están presentes. Así mismo, el mencionado reporte resalta que al menos 55% de las empresas a nivel global ha sufrido de brechas de seguridad donde se han comprometido al menos 1000 registros de datos con información confidencial y datos sensibles de los clientes.

Conclusiones

Los incidentes establecen una realidad inevitable en la dinámica de las organizaciones modernas. Todas las industrias están siendo afectadas habida cuenta de la mayor exposición digital y la hiperconectividad creciente que se demanda por parte de una sociedad cada vez más conectada y exigente de nuevas experiencias que cambien la manera de hacer las cosas, donde la agilidad y la versatilidad son la base de los nuevos productos y servicios que se implementen.

Durante las últimas décadas, el sector financiero, ha sido pionero en incorporar mayor interacción digital con sus clientes, para lo cual las tecnologías móviles y sus aplicaciones se han convertido en un factor clave para establecer una perspectiva omnicanal con mayor alcance y experiencia. En consecuencia, la economía colombiana se ha venido dinamizando, con una banca más digital con nuevos servicios y tecnologías, las cuales no solamente han creado nuevas oportunidades, sino han incrementado la superficie de ataques (ESRB, 2020). Esta dependencia incrementa el potencial del apetito de los adversarios digitales para continuar creando nuevos inciertos sobre esta acelerada dinámica digital de la banca.

Los datos del estudio sugieren que en Colombia el phishing, el ransomaware y la instalación de software no autorizado, son los incidentes que mayormente se presentan en todas las industrias del país, y que

deben ser atendidos de forma prioritaria toda vez que los datos y tendencias internacionales, muestran que siguen creciendo de manera sostenida en el tiempo.

Llama la atención el caso particular del pharming, una amenaza que busca redirigir el tráfico hacia un sitio particular establecido por el agresor, explotando vulnerabilidades del sistema de nombre de dominio, la cual manifiesta el mayor crecimiento sostenido a lo largo de los 10 años de estudio. Este dato, demanda una reflexión y análisis en profundidad de las estrategias de aseguramiento de los sitios web de las empresas, para no convertirse en puentes de los agresores que, por lo general, usan esta estrategia para capturar información y engañar a los clientes.

Es por ello que el llamado es a la preparación de las organizaciones con el fin de aumentar sus capacidades de monitorización y prospectiva con el fin de puedan atender con mayores y mejores elementos las inestabilidades propias de la realidad digital en la cual están inmersas (BakerHostleter, 2019).

Según ESRB (2020), la presencia de los ciber incidentes en los ambientes organizacionales puede desencadenar crisis sistémicas en las organizaciones. Esto es, un incidente de seguridad digital no solo es un incidente relacionado con las tecnologías de la información, sino un evento que puede producir distintas implicaciones en la organización y afectar de manera sistémica su dinámica empresarial, con impactos adversos para sus planes estratégicos, y consecuencias importantes en el desarrollo de sus negocios.

El Foro Económico Mundial (WEF, 2020), igualmente manifiesta que los ciberataques hacen parte de los riesgos más significativos y de importancia global, y por lo tanto, requieren de la atención no solo de las áreas técnicas, sino de los equipos directivos, como lo manifiesta PwC (2020), en su estudio de las preocupaciones de los ejecutivos a nivel global.

Las áreas de seguridad de la información de las organizaciones están experimentando cambios permanentes en la forma de atender los incidentes de seguridad que se presentan (BID-OEA, 2016). No es solo atender los incidentes, sino entender mejor como estos evolucionan y la dinámica propia de los adversarios digitales. Si bien en Colombia, se vienen desarrollando y aplicando las buenas prácticas de atención de incidentes, es necesario que tanto los distintos sectores de la industria, y la nación en general, aceleren sus esfuerzos para desarrollar mayores capacidades dinámicas para atender, gestionar y manejar los incidentes actuales y futuros.

En consecuencia, prepararse para los incidentes resulta un ejercicio mandatorio de cara al entorno digital que se tiene en la actualidad. Por tanto, no sólo la tecnología se configura como la protagonista de los eventos adversos, sino la educación, la creación de una cultura de seguridad en todos los niveles (liderada a través del ejemplo), así como el fortalecimiento de la inteligencia digital y la cultura de ciberseguridad, se configuran como piezas claves que ayudan en el desarrollo de posturas de seguridad más resilientes y consistentes con los retos que imponen las dinámicas empresariales en medio de la transformación digital.

Los incidentes que vienen reportando las empresas y en especial aquellos que están relacionados con la privacidad, por lo general son catalogados como brechas de seguridad (Verizon, 2020). En Colombia, este tipo de eventos manifiesta un 25% de crecimiento sostenido en el tiempo, lo que implica que las áreas de seguridad de la información empiecen a entender la protección y la privacidad de los datos como una temática interdisciplinar, en donde se adelanten esfuerzos conjuntos y reflexiones complementarias, de tal manera que le permitan a las organizaciones construir perspectivas enriquecidas que den cuenta de las expectativas propias de los negocios y sus clientes.

Finalmente, es necesario entender que los adversarios digitales, siguen y seguirán desarrollando nuevas formas de materializar sus acciones, para lo cual estarán innovando en la forma de generar retos que afecten a las organizaciones de todos los sectores; ya no solamente con preferencia por el sector financiero, sino en otros sectores como el gobierno, la salud, las grandes superficies (*retail*), la educación entre otros, los cuales estarán sometidos a las mismas presiones. Por tanto, las áreas de seguridad de la información estarán mucho más ocupadas buscando no solo reaccionar ante los adversarios, sino tratando de anticiparlos (PwCb, 2020). De esta forma, es clave que ésta áreas fortalezcan sus capacidades vigentes, incrementen sus esfuerzos técnicos, administrativos y estratégicos para establecer programas de

prospectiva que les permita atender el reto de proteger, defender y anticipar algunos movimientos de los renovados agresores digitales.

REFERENCIAS

BakerHostetler (2019). Managing Enterprise Risks in a Digital World. Recuperado de: https://f.datasrvr.com/fr1/019/33725/2019_BakerHostetler_DSIR_Final.pdf

Cano, J. & Almanza, A. (2020). Estudio de la evolución de la Seguridad de la Información en Colombia: 2000 - 2018. *Revista Iberoamericana de Sistemas y Tecnologías de Información*. E27. Marzo. 470-483.

Cano, J. (2020). Modelo SOCIA. Una reflexión conceptual y práctica desde la perspectiva del adversario. *Actas X Congreso Iberoamericano de Seguridad Informática 2020*. Universidad Politécnica de Madrid - Universidad del Rosario. Enero. Doi: 10.12804/si9789587844337.09

Crypsis (2020). Incident Response & Data Breach Report. Recuperado de: https://cdn2.hubspot.net/hubfs/4266002/Threat%20Report%202020/Crypsis_2020%20Incident%20Response%20and%20Data%20Breach%20Report_FINAL.pdf

ESET (2019). ESET Security Report 201. Recuperado de: https://www.welivesecurity.com/wp-content/uploads/2019/07/ESET-security-report-LATAM-2019.pdf

ESRB (2020). Systemic cyber risk. Recuperado de: https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf

EY (2019). How does security evolve from bolted on to built-in?. Recuperado de: https://www.ey.com/Publication/vwLUAssets/2020_GISS_pdf/$FILE/ey-global-information-security-survey-2020-report.pdf

OEA-BID (2016). Ciberseguridad: ¿Estamos preparados en América Latina y el Caribe? Recuperado de: https://publications.iadb.org/es/publicacion/17071/ciberseguridad-estamos-preparados-en-america-latina-y-el-caribe

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

PwCb (2020). Digital Trust Insights Pulse Survey. Recuperado de: https://www.pwc.com/us/en/services/consulting/cybersecurity/library/pwc-covid-19-ciso-pulse-survey.html/?WT.mc_id=CT2-PL200-DM2-TR1-LS2-ND30-PR5-CN_DTI-PULSE-SURVEY-2020-next-move-june2020-survey-edition

Reason, J. (2000). Human error: models and management. *British Medical Journal*. 320, 768-770

Secureworks (2019). Incident Response Insights Report. Recuperado de: https://apexassembly.com/wp-content/uploads/2019/08/Secureworks_SECO1240N_IncidentResponseInsightsReport2019.pdf

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

WEF (2020). Global Risks Report 2019. World Economic Forum. Recuperado de: http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf