Riesgos cibernéticos: desafío para las aseguradoras

En la era digital actual, los ciberdelitos representan un desafío cada vez más complejo para las empresas. A medida que la tecnología avanza, las amenazas cibernéticas también evolucionan, adoptando métodos más sofisticados para acceder a la información, uno de los activos más valiosos de cualquier organización.

Lorena Paola Ayala Cubillos
Subdirectora de Gestión Institucional contra el Fraude de Fasecolda

Riesgo cibernético a nivel global

El riesgo cibernético se ha identificado como un desafío global significativo, según el Informe de Riesgos Globales 2024, publicado por el Foro Económico Mundial, está entre los cinco más severos, junto con el cambio climático, el uso de la inteligencia artificial (IA), la crisis del costo de vida y la polarización política; esta posición destaca la creciente amenaza que representa para diversos sectores.

Adicionalmente, la Federación Mundial de Asociaciones de Seguros (GFIA, por su sigla en inglés) ha documentado pérdidas económicas considerables derivadas de ataques cibernéticos (cerca de un billón de dólares); estas incluyen impactos financieros directos, daño a la reputación de las marcas y costos de recuperación.

Por ejemplo, IBM reportó, en su *Informe* sobre el coste de la *vulneración de datos de 2023*, que el costo promedio de una filtración fue de 4,45 millones de dólares, este dato subraya la sofisticación y magnitud de los incidentes de seguridad cibernética.

En Latinoamérica la situación no es diferente; según el Índice de *inteligencia de amenazas X-Force*, de IBM, la región experimentó cuantiosos ataques durante 2023, que representaron el 12% de los incidentes a nivel mundial. América Latina registra 7.160 ataques diarios, lo que supone un promedio de cinco infecciones por minuto (Kaspersky, 2023). Países como Colombia han sido especialmente afectados, con un elevado número de ataques dirigidos hacia sectores como el comercio minorista, las finanzas y los seguros.

Según el balance de ciberseguridad de 2023, del Centro Cibernético Policial de la Dirección de Investigación Criminal e Interpol, en Colombia se reportaron 59.033 denuncias por delitos informáticos en el año. Estos casos se concentran principalmente en Bogotá, con un 19% del total, le siguen Medellín, con el 9%, Cali, con un 5%, Barranquilla, con el 3%, Cartagena, con un 2%, e Ibagué, también con un 2%.

Las principales denuncias en 2023 están relacionadas con hurto de información, acceso abusivo y violación de datos personales.

Durante 2023, las cuatro modalidades de incidentes cibernéticos más frecuentes fueron *phishing*[1], estafas en la compra y venta de productos por internet, falsificación de identidad en entornos digitales y amenazas a través de redes sociales.

Según el reporte generado por el Índice Nacional de Seguridad Cibernética (NCSI, por su sigla en inglés), Colombia ocupa el puesto 69 entre 176 países en términos de preparación para prevenir amenazas y manejar incidentes de seguridad cibernética. Este dato refleja la urgencia de adoptar estrategias robustas de ciberseguridad en las organizaciones.

Gráfico 1:
Ciudades más afectadas por el delito informático

Fuente: Centro Cibernético Policial de la Dirección de Investigación Criminal e Interpol

El papel de la IA en la generación de ciberataques

La inteligencia artificial (IA) desempeña un papel crucial en el aumento de los ciberataques, al identificar, de manera efectiva y sigilosa, vulnerabilidades en los sistemas de información y aprovechar que el eslabón más débil en la cadena de seguridad son los usuarios. Los ciberdelincuentes están utilizando la IA para obtener credenciales de acceso y así poder infiltrarse en los sistemas sin levantar sospechas. En muchos casos, su objetivo no es solo secuestrar datos, sino operar en la sombra para extraer información.

Es por ello que los métodos tradicionales de defensa, como el de «murallas y fosos de los castillos medievales», en los que la murallas hacen referencia a los sistemas que bloquean accesos no autorizados y el foso representa capas adicionales de seguridad (como autenticación de múltiples factores y cifrado de datos) (Microsoft, 2024), se han vuelto más vulnerables, los ciberdelincuentes han encontrado maneras de evadir o superar estas barreras mediante métodos avanzados de *phishing* y el uso de *software* malicioso.

En contraste, la estrategia de «confianza cero» *(zero trust)* es una nueva norma en ciberseguridad, más

Gráfico 2:
Principales delitos informáticos

Fuente: Centro Cibernético Policial de la Dirección de Investigación Criminal e Interpol

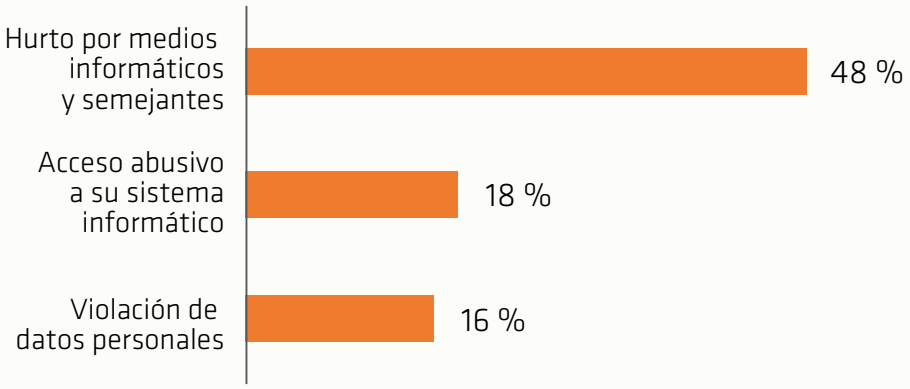
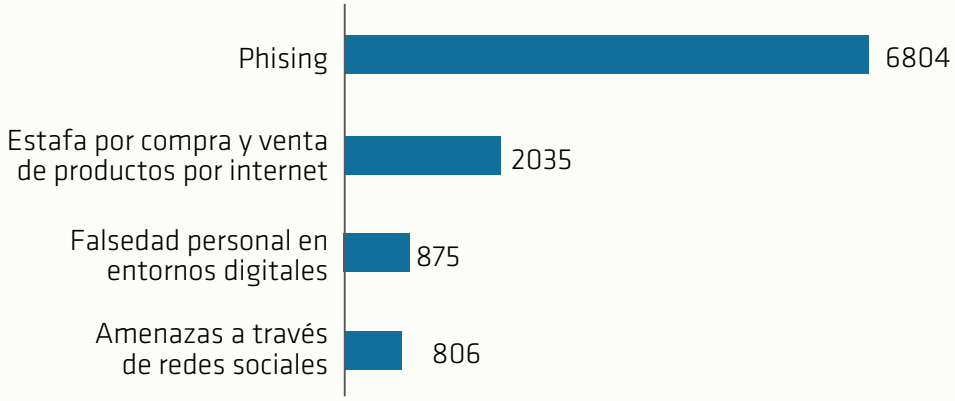


Gráfico 3:
Número de casos reportados por modalidad de incidentes cibernéticos

Fuente: Centro Cibernético Policial de la Dirección de Investigación Criminal e Interpol



adaptada a los desafíos actuales, asume que ningún usuario o dispositivo dentro o fuera de la red puede ser confiable de manera predeterminada. Por lo tanto, todos los usuarios, dispositivos y aplicaciones deben ser verificados y autenticados continuamente antes de permitir el acceso a los sistemas, para asegurar un trabajo seguro desde cualquier lugar, proteger los datos y minimizar el impacto de los actores malintencionados (Microsoft, 2024).

Este enfoque dinámico no solo permite adaptarse mejor a los desafíos actuales de ciberseguridad, sino que también puede fortalecer la protección contra los ciberdelincuentes.

Desafortunadamente, la IA también se utiliza para mejorar y automatizar modalidades de amenaza como el *phishing*, en el que antes era común ver errores gramaticales y de ortografía que delataban los correos electrónicos maliciosos; ahora, con el uso de la IA, estos correos son muy convincentes, pues se han eliminado incongruencias en los mensajes para poder engañar a los usuarios de manera más efectiva y obtener su información.

Un desafío adicional surge cuando la misma IA que identifica vulnerabilidades es utilizada por sistemas de defensa que también dependen de IA; esto plantea una paradoja interesante: ¿cómo pueden los sistemas defenderse de amenazas que utilizan la misma tecnología para atacar?

La IA como herramienta para la prevención de ciberataques en el sector asegurador

A pesar de que son muchos los desafíos en materia de riesgo cibernético, la IA puede ser una aliada de las aseguradoras, pues, así como se usa para acceder a los

Los ciberdelincuentes están utilizando la IA para obtener credenciales de acceso y así poder infiltrarse en los sistemas sin levantar sospechas.

1. «El phishing alude a una técnica fraudulenta en internet con la que se pretende captar datos privados de los usuarios: nombres de acceso a cuentas bancarias, contraseñas, datos de las tarjetas de crédito, etc.» https://www.fundeu.es/consulta/phishing-6/

sistemas de información, su constante aprendizaje la convierte en una herramienta importante para agilizar la identificación de vulnerabilidades. Por ejemplo, puede analizar rápidamente grandes volúmenes de datos y detectar movimientos sospechosos, lo que le permite anticiparse y mitigar posibles ataques; además, esta tecnología proporciona información crucial para corregir los puntos críticos más vulnerables de manera oportuna.

El monitoreo constante de anomalías es otra ventaja significativa de la IA, complementa la labor humana al facilitar la detección temprana de comportamientos inusuales que podrían indicar una intrusión; de ahí la importancia de contar con equipos capacitados para interpretar los datos recopilados y tomar decisiones informadas en tiempo real.

Además de su papel en la detección y respuesta ante amenazas, la IA mejora notablemente los procesos de autenticación de usuarios y la gestión de accesos; esto es especialmente relevante en el contexto actual de teletrabajo, en el que la flexibilidad de conexión desde múltiples ubicaciones requiere sistemas aún más robustos para garantizar la seguridad de la información.

Promover la concientización y la educación

Para contribuir efectivamente a la protección contra los ataques cibernéticos, no basta con invertir en tecnología avanzada; también es crucial priorizar la educación. En la era digital actual, las personas están cada vez más conectadas y dependen de la tecnología, lo cual las hace más vulnerables. Aunque muchos sean conscientes de los frecuentes ataques cibernéticos, tienden a subestimar el riesgo de que su información personal pueda estar comprometida.

¿Cuántos de ustedes han considerado que si los datos de sus empresas se exponen, también se podría divulgar su información personal?, ¿Cuántas veces ha accedido a cuentas bancarias, comprado tiquetes de avión, pagado facturas de servicios o diligenciado formularios con sus datos personales desde redes corporativas? Es esencial ser conscientes y responsables con la información que se expone.

La colaboración activa no solo fortalece la protección de datos y la seguridad cibernética, sino que también construye una comunidad digital más consciente de los riesgos del ciberespacio.

Otro punto crítico y frecuentemente pasado por alto es la saturación de información que enfrentan los clientes. En un entorno en el que la línea entre lo real y lo ficticio es cada vez más difusa, las noticias falsas y la desinformación representan un riesgo significativo para la reputación de cualquier empresa.

Es necesario que las organizaciones desarrollen campañas educativas dirigidas a sus clientes, ayudándolos a discernir entre información veraz y engañosa.

Facilitar una experiencia de usuario segura en las plataformas digitales, compartir información sobre incidentes de seguridad y actuar como un canal informativo confiable para prevenir amenazas emergentes en el mercado son pasos fundamentales.

Esta colaboración activa no solo fortalece la protección de datos y la seguridad cibernética, sino que también construye una comunidad digital más consciente de los riesgos del ciberespacio.

¿Seguros? ¿Asesorias?¿Proveedores?

DIRECTORIO DIGITAL FASECOLDA

AUTOADMINISTRABLE

¡WOW! 📻📖📗❤️

Inscriba su empresa ahora y obtenga los siguientes beneficios

- Visibilidad y posicionamiento de su compañía en la industria de seguros
- Actualización inmediata. Herramienta autoadministrable.
- Fácil navegación
- Enlaces a su sitio web
- Conozca su competencia
- Encuentre proveedores
- Conecte con potenciales clientes

Administre su información en tiempo real y descubra la red de negocios de la industria de seguros

fasecolda.com/servicios/directorio/

Más información y tarifas

ANA FELISA PÉREZ

344 3080 ext: 1803 fperez@fasecolda.com

fasecolda
Federación de Aseguradores Colombianos