IMPORTANCIA DE LA SEGURIDAD INFORMÁTICA Y CIBERSEGURIDAD EN EL MUNDO ACTUAL

Gamboa Suárez Jose Luis
holgs0203@gmail.com
Universidad Piloto de Colombia

***Resumen*—** Durante los últimos años el auge en los crímenes digitales o ciberataques ha puesto en jaque a los usuarios de internet, sitios web, empresas y corporaciones, generando pérdidas por miles de millones de dólares al año con tendencia al alza, debido a que cada día los cibercriminales mejoran o evolucionan sus métodos para lograr acceder a la información personal y confidencial de las víctimas y con ello poder obtener un lucro económico. Debido a esto es importante estar al tanto de las amenazas que se pueden conseguir día a día en la web o con solo encender el computador, sin embargo, no basta con ello, se debe tener un conocimiento mínimo de cómo contrarrestar dichas amenazas y tener las herramientas mínimas para no ser víctimas de robo de información, fraudes o estafas. Por lo antes expuesto es que la seguridad informática toma tanta importancia, no solo desde el punto de vista de resguardo de información, sino también económico, la inversión de tiempo para el adiestramiento y programas de protección son la única manera de hacerle frente a los cibercriminales y evitar mayores pérdidas monetarias en el futuro. En el último año se registraron más de 467.000 ciberataques, generando pérdidas que superaron los 3.990 MM$ a nivel mundial, siendo Estados Unidos el país con mayor afectación, no es de extrañar que haya asignado un presupuesto de 15.000 MM$ a ciberseguridad y países como Francia contratará más de 4.000 expertos de seguridad informática a mediano plazo con la finalidad de contrarrestar posibles ataques a futuro.

***Abstract*—** Over the past few years the increase in digital crimes has put internet users, websites, companies and corporations, generating losses of billion of dollars at year with a rising trend, due to each day the cybercriminals improve or evolve their methods to get access to personal and confidential information of the victims and thus obtain economic profit. Because of this it is important to be aware of the threats that can be obtain daily on the web or just to turn the computer, by the way it is not enough, it is necessary to have less knowledge of how counter these threat and at least have the tools to avoid being the victims of an information theft, fraud or scam. It is therefore that cybersecurity is so important, not just from the standpoint of the information safeguarding, also economic, the investment of time for training and protection programs, are the only way to deal with cybercriminals and to avoid greater monetary losses in the future. Over the past year more than 467.000 cyber-attack were recorder, generating losses that surpass $3,990 MM worldwide, the US has been the most affected country, not surprising that it has allocated a budget of $15,000MM to cybersecurity and countries such as Francie hire over 4,000 experts in the medium term to counter possible future attacks.

I. INTRODUCCIÓN

En una era digital como lo actual, en la que empresas, personas e incluso gobiernos poseen información importante y/o clasificada en dispositivos digitales (fijos o móviles), se hace de vital importancia conocer los riesgos existentes ya sea de ataques, espionajes o actos delictivos de los cuales se puede ser víctima, así como de las herramientas existentes para detectarlos, prevenirlos y contrarrestarlos. Si bien es cierto que con el paso del tiempo los ciberataques y delincuencia cibernética han evolucionado, no en menor medida los programas y herramientas para evitar ser víctima de dichos ataques también han evolucionado, por ello es importante mantenerse al día sobre la seguridad informática, ya sea mediante reseñas, cursos (online o presencial), lecturas autodidactas, o cualquier otro método de aprendizaje, lo importante es estar actualizado sobre las tendencias y métodos de protección de información digital.

II. SEGURIDAD INFOMÁTICA

La seguridad informática se trata sobre la protección de información de índole personal, empresarial o gubernamental contenida no solo en la red, sino también en los dispositivos de uso diario como teléfonos celulares, tabletas, computadoras de escritorio, laptop o cualquier dispositivo digital, de amenazas que puedan poner en riesgo la información almacenada o transportada en alguno de los dispositivos antes mencionados. Una buena Ciberseguridad no solo se debe basar en la prevención de ataques, sino también detección y corrección de los mismos, reduciendo los riesgos de exposición de la información, brindando confianza a los usuarios.

A. Categorías de Seguridad Informática

La seguridad informática puede dividirse en algunas categorías comunes como se muestra a continuación:

1) Seguridad de Red

Son medias que se toman con la finalidad de proteger una red informática de intrusos, ya sean atacantes dirigidos o malware oportunista. Involucra autorizar acceso a datos que se encuentran almacenados en la red, la cual es controlada por un administrador. Los usuarios eligen o se les asigna una identificación y contraseña para su autenticación que les permite acceder a información y programas dentro de sus autorizaciones.

2) Seguridad de las Aplicaciones

Es el proceso para hacer que las aplicaciones sean más seguras al encontrar, corregir y mejorar su seguridad. Gran parte de esto sucede durante la fase de desarrollo, pero incluye herramientas y métodos para proteger las aplicaciones una vez que se implementan. Este tipo de

seguridad se enfoca en mantener los dispositivos y el software libres de amenazas. Una aplicación afectada o mal diseñada podría brindar acceso a los datos que está destinada a proteger. La seguridad eficaz comienza en la etapa de diseño, mucho antes de la implementación de un programa o dispositivo.

3) Seguridad de la información

Es el conjunto de medidas preventivas y reactivas que permiten resguardar o proteger la información, manteniendo la confidencialidad, integridad y la autenticación de los datos, tanto en el almacenamiento como en el tránsito. Cabe aclarar que el término seguridad de información difiere a seguridad informativa, debido a que el primero abarca un rango más amplio, llegando a tener una importancia global en otros aspectos que no involucran a la Ciberseguridad.

4) Seguridad Operativa

Entendida como el conjunto de procedimientos destinados a minimizar los riesgos a los que están expuestos la información, software y equipos, incluyendo los procesos y decisiones para manejar los recursos de datos. Los permisos que tienen los usuarios para acceder a una red, así como los procedimientos que determinan cómo y dónde puede almacenarse o compartirse los datos se incluyen en esta categoría. El adiestramiento del personal acerca los riesgos y la manera de prevenirlos mediante la concientización y capacitación constituyen los pilares fundamentales de la Seguridad Operativa.

5) Recuperación ante Desastres y la Continuidad del Negocio

Definen la capacidad que tiene una organización de responder a un incidente de seguridad informática o a cualquier otro evento que cause que se detengan de manera parcial o total sus operaciones originando perdidas de datos o información. Las políticas de recuperación ante desastres dictan la forma en que la organización restaura sus operaciones e información para volver a la misma capacidad operativa que tenía antes del evento. La continuidad del negocio es el plan al que recurre la organización cuando intenta operar sin determinados recursos.

6) Capacidad de Usuario Final

Aborda el factor de seguridad informática más impredecible: las personas. Si se incumplen las buenas prácticas de seguridad, cualquier persona puede introducir accidentalmente un virus en un sistema que de otro modo sería seguro. Enseñarles a los usuarios desde eliminar los archivos adjuntos de correos electrónicos sospechosos, a no conectar unidades USB no identificadas y otras lecciones importantes es fundamental para la seguridad de cualquier organización.

Si bien cada uno de las categorías de seguridad mencionados se basa en un aspecto específico de los procesos desarrollados por equipos digitales de las empresas, personales o gubernamentales, se encuentran entrelazados entre sí y mantienen una continúa relación y convivencia de funcionamiento. Para llevar a cabo una adecuada seguridad informática todas las funciones de seguridad debe tener y cumplir los siguientes procesos:

- ***Protección:*** configuración de manera adecuada del software, sistema, aplicaciones y redes, desde su creación hasta su puesta en marcha para garantizar un perfecto funcionamiento.
- ***Detección:*** debe ser capaz de identificar en tiempo real si se ha cambiado la configuración de algún mecanismos o aspecto del sistema, equipo o si algún tráfico de red indica un problema
- ***Reacción:*** una vez identificado los problemas rápidamente, responder de manera eficaz, eliminando la amenaza y regresar a un estado seguro de funcionamiento.
- Sin dejar de lado los principios básicos de la seguridad informática manteniendo los siguientes aspectos de la información en cada uno de los aspectos y procesos.
- ***Integridad:*** toda información debe ser correcta sin modificaciones, ni alteraciones no autorizadas ni errores. Se protege frente a vulnerabilidades externas o posibles errores humanos.
- ***Confidencialidad:*** el acceso a las redes, aplicaciones e información solo debe ser permitido a personal autorizado. La información no debe llegar a personas o entidades que no estén dentro de esta clasificación.
- ***Autenticación:*** la información procedente de un programa, aplicación, carpeta de red o usuario, debe verificada y se debe garantizar que el origen de los datos es correcto y fidedigno.

B. Tipos de Ciberataques

Existen una gran variedad de peligros a la seguridad de la información que poseen los usuarios en sus dispositivos o en la red. Muchas de dichas amenazas a veces son llevadas a cabo con éxitos en los conocidos Ciberataques mediante la utilización de códigos maliciosos para alterar o sustraer información de un ordenador o red, alterando la lógica de los datos generando consecuencias perjudiciales que pueden comprometer la información. Dichos ataque pueden ser llevados a cabo por un individuo u organización que intenta obtener el control de un sistema operativo para usarlo con fines maliciosos ya sea robo de información, fines económicos, políticos, religiosos o incluso con el propósito de generar terror o miedo generalizado en una población, clase dirigente o gobierno.

Existe una gran variedad de agentes maliciosos que pueden ser usados por los hacker para tratar de vulnerar sistemas informativos en el que desean irrumpir, a continuación se mencionan los más comunes.

1) Malware

Es un software malicioso que una vez que entra al ordenador puede causar todo tipo de daños, desde tomar el control del equipo, monitorear acciones e incluso enviar datos confidenciales a la base de origen del atacante. Con frecuencia es propagado a través de archivos adjuntos de correos electrónicos no solicitados o descargas en línea aparentemente legítimas. Hay una variedad malware entre los que se mencionan los siguientes:

- ***Virus:*** son programas informativos maliciosos que tienen como objetivo alterar el funcionamiento de un computador, sin que el usuario lo note, por lo general, infectan otros archivos del sistema con la intención de modificarlos para destruir de manera intencionada datos almacenados en un equipo o red. un programa capaz de reproducirse, que se incrusta un archivo limpio y se extiende por todo el sistema informático e infecta a los archivos con código malicioso.
- ***Troyanos:*** un tipo de malware que a menudo se camufla o disfraza como software legítimo. Los cibercriminales o hacker suelen emplear los troyanos para intentar acceder a los sistemas de los usuarios. Una vez activados estos malware permiten a los criminales espiarte, obtener datos e información personal y confidencial y obtener acceso a tu sistema, donde pueden causar terribles daños como: copia, modificación, eliminación y/o

bloqueo de datos, además de interrupción del rendimiento de ordenadores o redes.

- ***Spyware:*** software malicioso que registra y recopila información en secreto de una computadora, ordenador o red, para luego transmitirla a una entidad externa de los cibercriminales para que puedan hacer uso de esta información sin el conocimiento o consentimiento del usuario. Por ejemplo, el spyware podría capturar los detalles de las tarjetas de crédito.
- ***Ransomware:*** programa o software malicioso que infecta programas o archivos, teniendo la capacidad de bloquear la pantalla de una computadora o cifrar archivos importantes predeterminados con una contraseña. Por lo general muestra un mensaje exigiendo un pago de rescate para restablecer las funciones del sistema y no eliminar o borrar los archivos o datos infectados.
- ***Adware:*** software no deseado diseñado para mostrar anuncios publicitarios en la pantalla del ordenador o equipos móviles, normalmente en un explorador. Por lo general se disfrace de programas que parecen legítimos para ser instalados en la pc, tableta o dispositivo móvil.
- ***Botnets:*** nombre genérico que denomina a cualquier grupo de ordenadores o redes de computadoras con infección de malware controlados por un atacante o grupo de cibercriminales de manera remota para realizar tareas en línea sin el permiso del usuario.

2) Phishing

Es un programa malicioso enviado a las víctimas o usuarios a través de correos electrónicos que parecen ser de una empresa legítima, bancos u otra organización, solicitando información personal o confidencial. En muchas ocasiones dichos correos poseen enlaces a sitios web preparados por los cibercriminales. Estos ataques se utilizan a menudo para inducir a que las personas entreguen datos bancarios, de tarjetas de crédito, de débito u otra información personal.

Por lo general una persona no abre un archivo adjunto al azar, de cualquier correo o de origen desconocido, es debido a ello que a menudo simulan ser alguien conocido o una entidad de confianza, para conseguir que se realice la acción deseada. Estos ataques dependen en su mayoría de la curiosidad y los impulsos humanos, por lo tanto serán difíciles de detener.

Para combatir este tipo de ataques, es esencial comprender la importancia de verificar los remitentes de correo electrónico, archivos adjuntos y enlaces.

3) Ataque de inyección SQL

Un ataque de inyección SQL es un código malicioso con un lenguaje de programación de consulta estructurado, utilizado para comunicarse con las bases de datos de los servidores que almacenan información crítica para sitios web y de servicios, con la finalidad de tomar el control y extraer datos privados de clientes, tales como: nombres de usuario y contraseña, datos bancarios, números de tarjeta de crédito, entre otros. Los cibercriminales aprovechan las vulnerabilidades de las aplicaciones basadas en datos para insertar código malicioso en una base de datos mediante una instrucción SQL maliciosa. Esto les brinda acceso a la información confidencial contenida en la base de datos.

4) Ataque de Denegación de Servicio

Consiste en saturar de tráfico con fine maliciosos un sitio web o sistema informativo, sobrecargando las redes y los servidores, impidiendo que satisfaga solicitudes legítimas. Esto hace que el sistema sea inutilizable e impide que una organización realice funciones vitales, como publicar su contenido o dar respuesta a usuarios. En algunos casos, estos ataques son realizados por un gran número de ordenadores al mismo tiempo. Son muy difíciles de superar debido a que el atacante aparece simultáneamente desde diferentes direcciones IP en todo el mundo, lo que dificulta aún más la determinación del origen.

5) Ataque Cross-Site Scripting

Este tipo de ataque persigue al usuario y no al servidor, lo que implica la inyección del código malicioso en un sitio web, ya sea en un comentario o un script para que se pueda ejecutar automáticamente en el navegador del usuario cuando este accede al mismo.

Los frecuentes ataques de este tipo a usuarios de determinado sitio web pueden dañar significativamente la reputación del mismo al poner en riesgo la información de los usuarios sin ninguna indicación de que haya ocurrido algo malicioso.

6) Ataque BEC/EAC

Es un tipo de estafa sofisticada que se dirige tanto a empresas como a usuarios que realizan solicitudes legítimas de transferencia de fondos. Ésta se lleva a cabo cuando un atacante compromete cuentas de correo electrónico comerciales o personales legítimas, mediante la intrusión de computadoras, con lo cual crea cuentas de correos con dominios similares al de las personas o instituciones afectadas, o enmascara su cuenta de correo como legitima, para lograr realizar transferencias de fondos no autorizadas. No siempre está asociada con una solicitud de transferencia de fondos. Una variación implica comprometer las cuentas de correo electrónico comerciales legítimas y solicitar otro tipo de información sensible, datos personales, como elementos previos para este u otro tipo de ataques.

Aunque existen varios métodos para introducir un programa o software malicioso en un ordenador o red, en algún momento requiere que el usuario realice una acción para que pueda instalarse en el sistema, entre los más comunes se pueden mencionar:

- Mensajes de redes sociales como Twitter y Facebook.
- Archivos adjuntos en los mensajes de correos electrónicos.
- Sitios Web sospechosos.
- Insertar USBs. DVDs, o CDs con software maliciosos.
- Descargar aplicaciones o programas de internet.
- Anuncios publicitarios falsos.

De acuerdo a lo anteriormente dicho, una vez que es enviado el programa malicioso por el medio elegido por el cibercriminal, el proceso de infección más común del ordenador o red puede describirse de la manera siguiente:

- El usuario descarga un programa infectado en su computador.
- El archivo malicioso se aloja en la memoria ram de la computadora, aún si no se termina de instalar.
- El archivo malicioso infecta los archivos y programas en ejecución en ese momento.
- Al reiniciar la computadora, programa malicioso se carga nuevamente en la memoria ram y toma control del sistema operativo, lo cual hace más fácil su replicación para contaminar cualquier archivo que encuentre a su paso.

Ya instalado y propagado en el computador o red del sistema un programa malicioso puede causar grandes daños o efectos negativos en la información del usuario o en los datos del ordenador, permitiendo a los ciberdelincuentes entre otras cosas:

- Tener control remoto del ordenador infectado, permitiendo enviar, recibir, iniciar y eliminar archivos, mostrar datos y reiniciar el ordenador.
- Obtener de manera ilícita datos bancarios de sistemas de banca online, sistemas de pagos electrónicos, tarjetas de débito y de crédito.
- Robar datos de la cuenta de jugadores online.
- Obtener datos de inicio de sesión y contraseñas de mensajería instantánea de cualquier red social.
- Modificar o bloquear datos del ordenador o red, los cuales serán desbloqueados mediante el pago de un rescate.

C. Pérdidas Ocasionadas por Ciberataques a Nivel Mundial

Para poder comprender la importancia de la seguridad informática, se debe conocer los daños que han causado a lo largo del tiempo los ciberataques, además de las consecuencias económicas que han conllevado a las empresas y personas quienes lo han sufrido. Si bien con el paso del tiempo se han incrementado los mecanismos para la protección de los equipos y de la información contenida en ellos, no menos cierto es que el cibercrimen han evolucionado sus métodos para llevar a cabo los crímenes digitales.

De acuerdo al reporte anual del Centro de Denuncias de Delito de Internet de 2019 [1] los ataques cibernéticos incrementan gradualmente cada año, como se muestra en la Fig. 1.

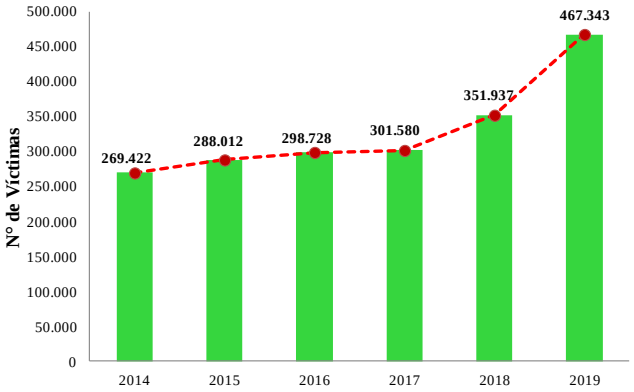

Fig. 1. Número de Víctimas de Ciberataques Anuales 2014-2019 (Fuente Reporte Anual IC3)

En el año 2019 hubo un total de 467.343 delitos cibernéticos reportados, lo que resulta en un promedio diario de 1280 ataques informáticos. Los ciberataques muestran un constante aumento cada año, observándose un repunte en el año 2019, durante el cual presentó un incremento de 115.406 ataques respecto al año anterior, lo que representa un 32,8% más que los ocurridos en el 2018.

Los ataques informáticos no solo representan riesgos a la seguridad de la información o integridad de los equipos, también representan pérdidas económicas para las personas, empresas y/o corporaciones, mientras mayor es el número de incidentes se traduce en un incremento de las pérdidas anuales generadas por estos ataque [1], como se muestra en la Fig. 2.

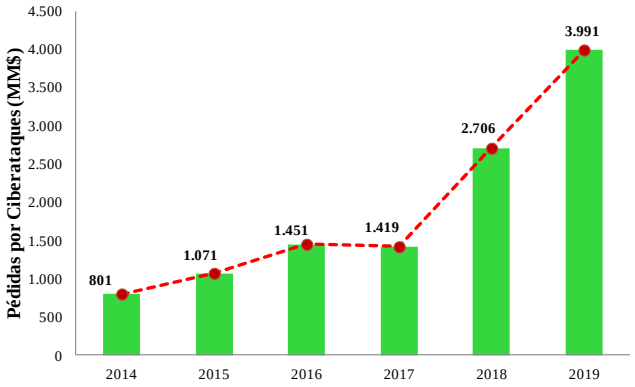

Fig. 2. Reporte de Pérdidas Anuales por Ciberataques 2014-2019 ((Fuente Reporte Anual IC3)

Las pérdidas generadas por los ciberataques a nivel mundial durante el año 2019 fueron de 3.991 MM$, el cual es un costo extremadamente alto si se tiene en consideración que los gastos asociados para la producción 680.000 barriles de petróleo de una empresa petrolera son de 3.971 MM$ al año. Estos valores representan un incremento del 47,5% al obtenido el 2018 el cual había mostrado un aumento del 90,8% respecto al año anterior, es decir, en dos años las pérdidas generadas por estos ataques suponen un crecimiento de 181%. Estos datos dejan en evidencia que los ataques basados en tecnologías web siguen causando estragos cada vez mayores a las organizaciones.

1) Distribución Porcentual por Tipo de Ataque

Según el reporte anual del Centro de Denuncias de Delito de Internet [1], se observaron un total de 467.343 ataques cibernéticos distribuidos en una variedad de tipos, los cuales se muestran en la Tabla I y. en la Fig. 3

Tabla I. Distribución de Victimas por Tipo de Ataque 2019 (Fuente Reporte Anual IC3)

Tipo de Ataque	Victimas
Phishing	114.702
Impago / Sin envío	61.832
Extorsión	43.101
Violación de Datos Personales	38.218
Suplantación de Identidad	25.789
BEC/EAC	23.775
Fraude de Confianza / Romance	19.473
Robo de Identidad	16.053
Acoso / Amenazas de Violencia	15.502
Pago Excesivo	15.395
Anticipo de Dinero	14.607
Oferta Falsa de Empleo	14.493
Fraude de Trajeta de Crédito	14.378
Suplantación Gubernamental	13.873
Apoyo Técnico	13.633
Bienes Raíces / Alquiler	11.677
Otro	10.842

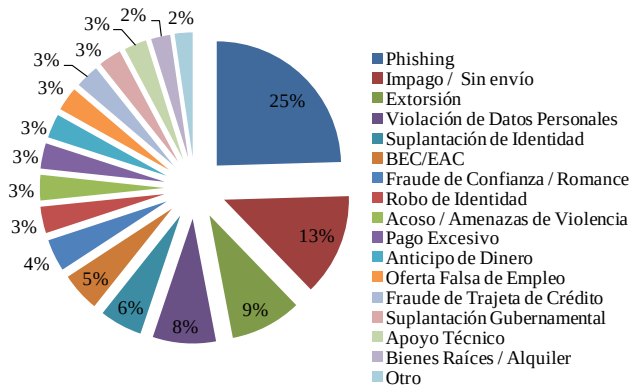

Fig. 3. Distribución Porcentual de Ataques Cibernéticos por Tipo (Fuente Reporte Anual IC3)

De los ataques perpetrados durante el año 2019, el Pishing ocupó el primer lugar con un mayor número de víctimas, a las cuales se les envió correos electrónicos haciéndose pasar por empresas o entidades bancarias, con la finalidad que los usuarios facilitaran información confidencial de sus cuenta bancarias, tarjetas de crédito u otra información con la cual pudiesen obtener un lucro económico a expensa de la víctima. Este tipo de fraude electrónico representó el 25% del total de las denuncias de ciberataques mundiales.

La otras dos modalidades más usadas durante el 2019 fueron las de compra o ventas fraudulentas por internet (Non Payment/No Delivery) en las cuales los criminales realizaban un pago falso para recibir una mercancía en venta o recibían cobros por un producto o articulo en venta el cual no enviaban una vez recibido el pago. Y las extorsiones, que es la solicitud de compensación económica a cambio de desbloqueo de equipos, aplicaciones y datos secuestrados por los delincuentes o con la amenaza de publicar alguna información personal obtenida del computador de la víctima.

Entre las 3 categorías antes descritas suman el 47% del total de delitos digitales ocurridos durante el año 2019, mientras que el resto se distribuye entre las otras 14 categorías que se muestran en la Tabla I.

2) Distribución de Pérdidas por Tipo de Ataque

Si bien hay tres categorías de ataques que tuvieron más cantidad de víctimas o fueron usadas en mayor proporción para llevar a cabo fraudes electrónicos, no significa que por tener un mayor número de denuncias sean las que generaron las mayores pérdidas monetarias durante el año 2019. De acuerdo al reporte anual del Centro de Denuncias de Delito de Internet [1], la distribución de pérdidas por tipo de ataque se puede verificar es la siguiente.

Tabla II. Distribución de Pérdidas por Tipo de Ataque 2019 (Fuente Reporte Anual IC3)

Tipo de Ataque	Pérdidas ($)
BEC/EAC	1.776.549.688
Fraude de Confianza / Romance	475.014.032
Suplantación de Identidad	300.478.433
Bienes Raíces / Alquiler	221.365.911
Impago / Sin envío	196.563.497
Robo de Identidad	160.305.789
Suplantación Gubernamental	124.292.606
Violación de Datos Personales	120.102.501
Fraude de Trajeta de Crédito	111.491.163
Extorsión	107.498.956
Anticipo de Dinero	100.602.297
Otro	66.223.160
Phishing	57.836.379
Pago Excesivo	55.820.212
Apoyo Técnico	54.041.053
Oferta Falsa de Empleo	42.618.705
Acoso / Amenazas de Violencia	19.866.654

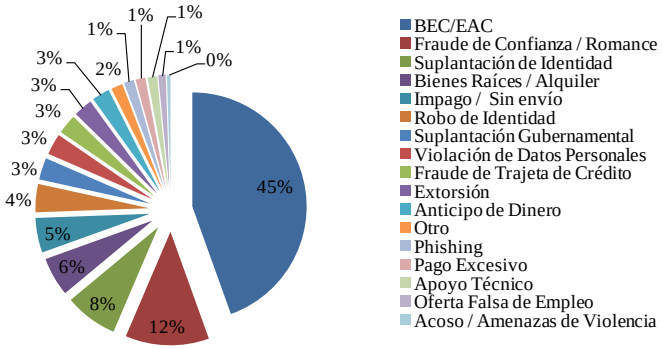

Fig. 4. Distribución Porcentual de Pérdidas por Tipo de Ataque (Fuente Reporte Anual IC3)

Durante el año 2019 los ciberataques generaron un total de pérdidas de 3.990 MM$, lo que representa un promedio diario de 10,9 MM$ robado a personas, empresas o corporaciones. El ataque que más pérdidas causó fue el BEC/EAC, el cual el atacante usa correos fraudulentos para obtener fondos ya sea de entidades o personas. Este tipo de fraudes generó perdidas por encima de 1,77 MMM$ lo que representa el 45% de las pérdidas totales del año 2019.

Las siguientes dos modalidades que mas generaron pérdidas fueron el Fraude de Confianza o Romance, en el cual el atacante usa páginas de citas para obtener datos personales o confidenciales de los usuarios, dicho fraude causó pérdidas por un monto de 475 MM$ lo que representa el 12% del total. Y el fraude de suplantación de identidad en el cual personas recibían un mensaje de correo electrónico, de texto o en las redes sociales de un supuesto amigo, familiar o colega en el que se incluía una solicitud de información personal o financiera valiosa, con este tipo de ataque se acumularon pérdidas por encima de los 300 MM$, lo que significa el 8% del total del año 2019.

Entre las 3 categorías mencionadas acumularon un 65% de las pérdidas mundiales generadas por los ataques digitales, el resto se distribuyó entre las otras 14 categorías.

Tabla III. Pérdidas por Ataque y Promedio Diario 2019 (Fuente Reporte Anual IC3)

Tipo de Ataque	Pérdidas por Evento ($)	Pérdidas Diarias($)
BEC/EAC	74.723	4.867.259
Fraude de Confianza / Romance	24.393	1.301.408
Bienes Raíces / Alquiler	18.957	606.482
Suplantación de Identidad	11.651	823.229
Robo de Identidad	9.986	439.194
Suplantación Gubernamental	8.959	340.528
Fraude de Trajeta de Crédito	7.754	305.455
Anticipo de Dinero	6.887	275.623
Otro	6.108	181.433
Apoyo Técnico	3.964	148.058
Pago Excesivo	3.626	152.932
Impago / Sin envío	3.179	538.530
Violación de Datos Personales	3.143	329.048
Oferta Falsa de Empleo	2.941	116.764
Extorsión	2.494	294.518
Acoso / Amenazas de Violencia	1.282	54.429
Phishing	504	158.456

El fraude BEC/AEC fue el tipo de ataque que mayores daños generó durante el año 2019, causando un costo promedio de 74.723$ por cada víctima, presentando una media diaria de 4,9 MM$ de pérdidas generadas a los usuarios. Este tipo de estafa es la que ha mostrado un mayor crecimiento en los últimos 5 años pasando de un total de 1.495 afectados durante el año 2014 a los 23.775 registrados durante el año pasado, lo que significó un incremento del 1.490%. Respecto a las pérdidas generadas se observa un crecimiento exponencial en los últimos años teniendo un reporte de 60 MM$ en el 2014 y de 1.777 MM$ en el 2019, lo que se traduce en un salto de 2.846%, por lo que este tipo de estafa se ha convertido en una empresa de mil millonaria. Estos crecimientos pueden observarse en las Fig. 5 y Fig. 6.

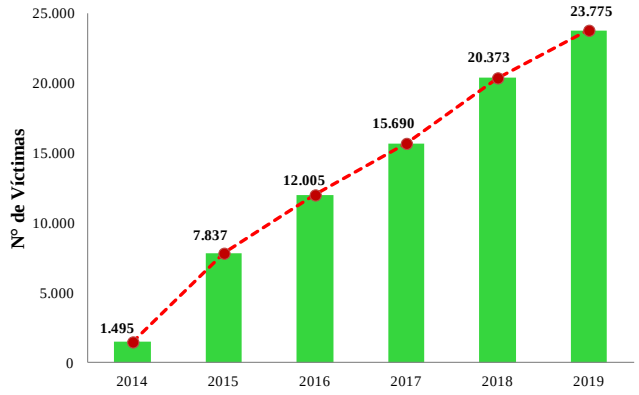

Fig. 5. Número de Víctimas Anuales de Ataque BEC/EAC 2014-2019 (Fuente Reporte Anual IC3)

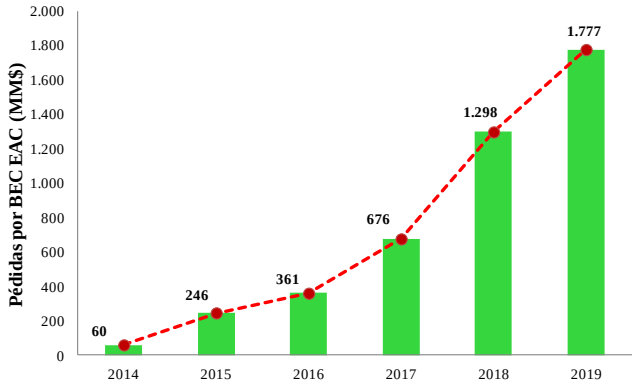

Fig. 6. Pérdidas Anuales de Ataque BEC/EAC 2014-2019 (Fuente Reporte Anual IC3)

3) Clasificación de Víctimas por Rango de Edad

Los cibercriminales no discriminan a sus víctimas, atacan a niños, jóvenes, adultos y ancianos por igual con la finalidad de obtener un lucro económico. Es por ello que personas de todas las edades deben estar atentas y concientizarse sobre la seguridad informativa para evitar ser víctimas de fraudes o ataques digitales.

Si bien se ha visto la cantidad de ataques realizados y las pérdidas generadas por los mismos durante el 2019, hasta ahora no se ha especificado que sector poblacional ha sido el más vulnerado. Nuevamente se recurre a los datos reportados por el Centro de Denuncias de Delito de Internet [1], para obtener la Fig. 7 y Fig. 8, en la primera se puede observar la distribución porcentual de ataques por rango de edad de las víctimas.

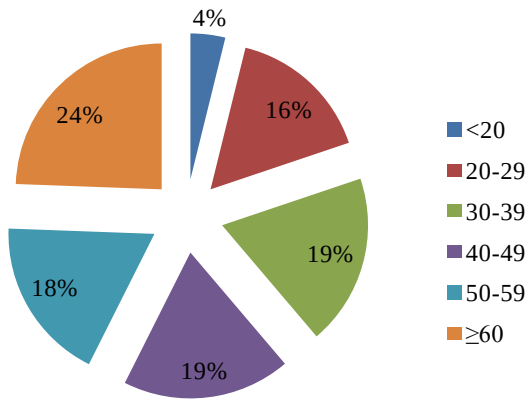

Fig. 7. Distribución Porcentual de Ataques por Rango de Edad (Fuente Reporte Anual IC3)

De acuerdo a los datos suministrados por la IC3 [1], durante el 2019 el sector más vulnerable a los ciberataques fueron las personas de la tercera edad, es decir, los adultos mayores a 60 años, los cuales representaron el 24% del total de las víctimas durante este período. Si a estas estadísticas se le suman los ataques sufridos por la población con edades comprendidas entre 50-59 años, se obtiene que las personas con rangos de edad mayor a 50 años representó el 42% del total de los afectados por ataques digitales durante el año pasado, lo que significa que las personas mayores son los más propensos a este tipo de ataques fueron las personas con edades de 20 años o menos, con apenas el 4% del total de los casos reportados.

Ya se ha visto el rango de edad de las personas que sufrieron mayor cantidad de ciberataques durante el 2019, pero también es de importancia constatar en cual sector se generaron los mayores costos económicos, lo cual puede verse en la Fig. 8, donde se muestra la distribución porcentual de pérdidas por rango de edad.

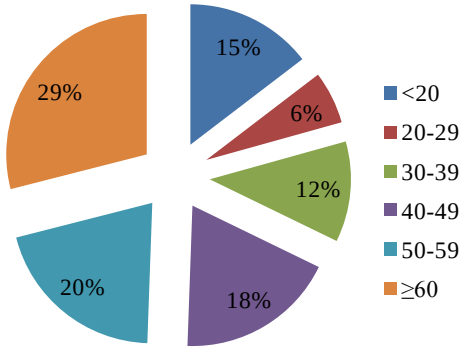

Fig. 8. Distribución Porcentual de Pérdidas Rango de Edad (Fuente Reporte Anual IC3)

En lo que respecta a las pérdidas, de igual manera el sector más afectado fueron las personas mayores a 60 años, quienes representan el 29% del total de los daños económicos, seguidos por las personas con edades comprendidas entre 50-59 con el 20%, lo que significa que los afectados con edades mayores a 50 años conforman el 49% del total de todas las pérdidas generadas durante el 2019. Por otra parte, las personas menos afectadas económicamente fueron los jóvenes con edades comprendidas entre 20-29 años.

Llama la atención que el sector con menor cantidad de ataque (edad<20) no sea el que tenga menores costos asociados, esto se debe a que a pesar de haber sufrido menos ciberataques los gastos económicos por cada uno de ellos fue mayor a los sufridos por los demás sectores evaluados.

4) Distribución de los Ataques por Países

Puede decirse que el año 2019 fue desastroso para la ciberseguridad, teniendo un total de 467.343 ciberataques que se tradujeron en pérdidas económicas que sobrepasaron los 3.991 MM$, mostrando un incremento de 32,8% en el número de ataques y de 47,5% en los costos generados. Los ataques fueron generados a lo largo del mundo, según datos del reporte anual del Centro de Denuncias de Delito de Internet [1], el país más afectado fue Estados Unidos seguido del Reino Unido, tal como se muestra en la Fig. 9.

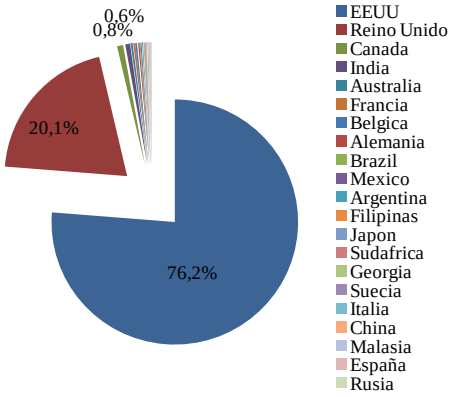

Fig. 9. Distribución de Ataques por Países (Fuente Reporte Anual IC3)

El país más afectado por los ciberataques fue Estados Unidos con un 76,2% del total de los incidentes mundiales reportados, seguido por Reino Unido con un 20,1%. Entre ambos países representan el 96,3% de la totalidad de los reportes de ciberataques producidos durante el año 2019, el restante se distribuye en los 19 países restantes, quedando en evidencia que el país más vulnerado desde el punto de vista digital es Estados Unidos.

D. Ciberataques más Famosos de la Década

La seguridad de la información ha sido uno de los temas más importantes durante la última década. Los acontecimientos relacionados con los ciberataques, brechas de datos personales y ataques informáticos a empresas o instituciones han pasado de ser noticias puntuales u ocasionales a titulares de los periódicos casi a diario. Hoy en día ocurre un nuevo caso cada semana, por lo que se ha tenido que aprender a afrontar las consecuencias de estos ataques a medida que su impacto aumenta y afecta a más víctimas.

De acuerdo a un estudio realizado y publicado por Redacción TICPymes [2], estos fueron los principales ciberataques perpetrados en el mundo en los últimos 10 años.

1) Wikileaks (Noviembre 2010)

Creada en 2006 por el australiano Julian Assange, ganó popularidad en 2010 cuando se publicaron una serie de documentos filtrados de interés público con material comprometedor de diferentes índoles, preservando el anonimato de sus fuentes. Entre los archivos publicados por esta organización destacan el vídeo de tiroteo a periodistas de Julio 2007, documentos sobre la Guerra de Afganistán entre los años 2004 y 2009, registros de la Guerra de Irak filtrados desde el Pentágono, telegramas del Departamento de Estado estadounidense con sus embajadas por todo el, el cual se convirtió en la mayor filtración de documentos secretos de la historia.

2) Sony PlayStation Network (Abril 2011)

PlayStation Network, es un servicio de PlayStation que permite la compra de juegos online, durante el ataque resultaron comprometidos los nombres, correos electrónicos, datos de acceso y otros datos personales de aproximadamente 77 millones de personas y este servicio dejó de funcionar durante una semana. En ese momento, la empresa japonesa no descartó la posibilidad de que los datos bancarios de los usuarios hubieran sido robados.

3) Dropbox (Agosto 2012)

Dropbox es un servicio de almacenamiento de datos en la nube, durante el 2012 sufrió un ataque en el cual los correos electrónicos y contraseñas de más de 68 millones de usuarios fueron expuestos o

robados, robadas las contraseñas. Los atacantes lograron entrar en sus cuentas debido a que uno de los empleados de Dropbox usó la misma contraseña profesional en su perfil de LinkedIn, cuando a principios de ese año LinkedIn sufrió un ataque, los hackers tuvieron acceso a la contraseña del empleado y la usaron para acceder a la red interna de Dropbox. Aunque el ataque tuvo lugar en 2012, la magnitud del mismo se conoció cuatro años más tarde.

4) Target (Diciembre 2013)

El gigante estadounidense de venta minorista Target fue objeto de un ataque durante el 2013, en el cual se obtuvo de manera ilícita la información personal (nombres, direcciones, números de teléfono y correos electrónicos) de 70 millones de clientes, además del robo datos bancarios de al menos 40 millones de víctimas. Los cibercriminales ingresaron al sistema de Target a través de un malware PoS, afectando los dispositivos del punto de venta, en este caso, lectores de tarjetas de crédito/débito y cajas registradoras. El ataque adquirió proporciones aún mayores al estar diseñado para la temporada de compras previas a la Navidad.

5) eBay (Mayo 2014)

En mayo de 2014, eBay emitió un comunicado en el que pedía a sus 145 millones de usuarios que cambiaran su contraseña tras descubrir que su red había sido objeto de un ciberataque. Los piratas informáticos pudieron entrar en el sistema de la empresa mediante el acceso no autorizado a las contraseñas de algunos empleados, y se hicieron con nombres de clientes, contraseñas cifradas, correos electrónicos, direcciones, números de teléfono y fechas de nacimiento.

6) Elecciones en los Estados Unidos (Diciembre 2015)

Durante este ataque los perpetradores lograron acceder a la información de 191 millones de votantes estadounidenses, alrededor del 60% de la población. Dichos datos fueron expuestos en Internet debido al error de una empresa de marketing contratada por el Comité Nacional Republicano durante la campaña de Donald Trump. Esto hizo que los registros de los votantes, incluyendo nombres, direcciones, números de teléfono, afiliaciones políticas, fechas de nacimiento, incluso religión y posicionamiento en temas controvertidos, fueran accesibles en la web.

7) Friend Finder (Noviembre 2016)

Este ciberataque afectó a más de 412 millones de cuentas en la red de sitios para adultos y pornografía, quedando expuestos en el mercado negro correos electrónicos y contraseñas. Como estos datos estaban asociados a sitios de contenido para adultos, el impacto del ataque también implicó la extorsión y vergüenza de los usuarios afectados.

El caso se hizo público por LeakedSource, que lo clasificó en su momento como el mayor robo de datos de la historia.

8) Uber (Noviembre 2017)

El ataque incluyó la exposición de nombres, correos electrónicos y números de teléfono de 57 millones de clientes en todo el mundo, así como la información personal de 7 millones de conductores de esa empresa de transporte. La noticia destacó en los medios de comunicación, no sólo por el número de víctimas afectadas, sino también porque Uber pagó cien mil dólares a dos hackers para eliminar los datos robados y ocultar el ciberataque, manteniéndolo en secreto.

9) Cambridge Analytica (Marzo 2018)

Cambridge Analytica - una empresa de análisis de datos que trabajó con el equipo de Donald Trump, utilizó sin consentimiento la información de 50 millones de perfiles de Facebook para identificar los patrones de comportamiento y gustos de los usuarios para utilizarlos en la difusión de propaganda política. De esta manera quedó demostrado que el robo de datos puede ser usado en política, en este caso, para influir en las elecciones presidenciales de Estados Unidos en 2016.

10) Facebook (Marzo 2019)

Un año después del escándalo de Cambridge Analytica, Facebook fue víctima una vez más de un ataque, en el cual los datos de unos 419 millones de usuarios quedaron expuestos, entre ellos números de teléfono e identificación. Esto fue posible debido a que la data era almacenada en un servidor online que no estaba protegido por contraseña. Los Estados Unidos, el Reino Unido y Vietnam fueron los países más afectados. La información obtenida puede ser utilizada por los cibercriminales para spam, phishing o fraudes asociados a la tarjeta SIM.

Los ciberataques perpetrados durante la última década, han dejado en evidencia que no importa lo grande sea una empres u organización o cuan poderoso sea una Nación o gobierno, los cibercriminales siempre logran conseguir una brecha para llevar a cabo sus ataques, lo que hace que sea una amenaza latente a nivel mundial, y que se requieren mecanismos para poder prevenir, minimizar y contrarrestar las consecuencias de ser víctimas de los ataques digitales.

E. Cibercriminales más Famosos

Hay que recordar que el malware no surge de la nada ni nace de forma espontánea en la red, todas las amenazas cibernéticas e informativas que existen fueron creadas por una persona o un grupo de individuos, ya sea a mano o mediante la rápida edición de un código existente. Todo con la finalidad de burlar sensores de antivirus antiguos. Sin embargo, aunque el número de ciberdelincuentes que existe en Internet es innumerable, existe una selecto grupo que se ha hecho famoso por sus "logros" en el área de burlar la seguridad de grandes empresas, corporaciones e incluso gobiernos. Según Venture Beat [3] estas son las 10 personas, grupos u organizaciones más peligrosas o famosas en el mundo de los hacker de la actualidad.

1) "Cracka"

En 2016, este adolescente británico apodado como Cracka y perteneciente a un grupo llamado "Crackas with Attitude", defensor del Movimiento Palestino, fue detenido por hackear la CIA y la Casa Blanca. Tan solo con 16 años consiguió hackear los correos personales del Director de la CIA, el director del FBI y el Director de Inteligencia Nacional. De este último también logró acceder a sus cuentas telefónicas y reveló la identidad de 31.000 agentes del gobierno de Estados Unidos.

2) Evgeniy Mikhailovich Bogachev

También apodado Fantomas, es el cibercriminal por cuya captura el FBI ofrece una recompensa de hasta tres millones de dólares desde el año pasado. El crimen que se le imputa este cracker es el robo de 100 millones de dólares de cuentas bancarias estadounidenses. Se le atribuye la creación del virus Game Over Zeus, que ha infectado a más de un millón de ordenadores de todo el mundo y de CryptoLocker, un sistema de cifrado de archivos utilizado para extraer pagos de rescates en las estrategias de ciberextorsión.

3) Nicolae Popescu

Es otro de los delincuentes informáticos más buscados del planeta, cabecilla de una trama de estafa a nivel global que operaba mediante la implantación de anuncios falsos en webs de subastas que nunca llegaron a los ganadores. El FBI estadounidense ofrece un millón de dólares por él, y pese a que desmantelaron su banda en una macro

operación en 2012 -con dinero, armas y vehículos de lujo de por medio, a día de hoy Popescu sigue con paradero desconocido.

4) Ourmine

Por citar un grupo estrictamente actual y de los más temidos en los tiempos que corren, a este grupo de supuestamente tres crackers le atribuyen miles de robos de perfiles en redes sociales, y el ingreso de medio millón de dólares en pocos meses mediante la extorsión a las víctimas. Desde Ourmine habrían tratado de extorsionar a los CEOs de Facebook, Google o Twitter, además de youtuber famosos como "El Rubius" y "Julian Assange" En algunos ataques los integrantes de han asegurado que sus acciones están destinadas a concienciar a los usuarios e instruirlos acerca de la protección online.

5) Adrian Lamo

Nativo de Boston, se dio a conocer como el 'hacker vagabundo' ya que viajaba a diversos puntos con acceso a Internet como cibercafés para realizar sus ataques "en diversas jurisdicciones" y exponiéndose lo menos posible. Irrumpió en redes informáticas de alta seguridad, detectando fallos en The New York Times, Microsoft, Yahoo!, Fortune 500 y Bank of América. También delató a Chelsea Manning, el soldado que presuntamente filtró a WikiLeaks el vídeo que mostraba a soldados estadounidenses asesinando a un fotógrafo de Reuters y a otros civiles en Afganistán, junto a diversos documentos clasificados del ejército de los EE.UU. que mostraban actitudes delictivas. Por robar información del New York Times, Lamo fue sentenciado a seis meses de arresto domiciliario.

6) Vladimir Levin

Conocido por ser todo un experto en el arte de robar dinero, Levin fue capaz de hacerse, desde su apartamento en San Petersburgo, con 10 diez millones de dólares hurtados a clientes del banco Citibank. Una vez capturado, tuvo que devolver el dinero y cumplir con tres años de cárcel, además de una multa económica de un cuarto de millón de dólares.

7) Alexsey Belan

Este joven ruso es el tercer cibercriminal más buscado por Estados Unidos, es acusado de hackear los sistemas de las tres mayores empresas de comercio electrónico del mundo, así como robar y vender bases de datos con información sensible a millones de usuarios a otros piratas informáticos. En estos momentos se encuentra en busca para su captura, se han seguido sus pasos por Europa del Este, Maldivas y el Sudeste asiático. La recompensa que se ofrece por Belan es de 100.000 dólares.

8) Elliott Gunton

Comenzó su carrera de ciberdelincuente a los 16 años, cuando fue descubierto pirateando TalkTalk, una empresa de telecomunicaciones, a partir de ahí se le ha acusado de una serie de delitos desde robo de información personal hasta falsificación, lavado de dinero con criptodivisa, trabajo como hacker al mejor postor, pirateo de cuentas de Instagram de famosos, venta de dichas cuentas a otros hackers y alojamiento de fotos indecentes de niños en el ordenador de su casa.

9) Soupnazi

Su auténtico nombre es Albert González, rey de la técnica conocida como phishing. Este pirata informático robó 170 millones de cuentas bancarias de todo el mundo, fue declarado culpable en 2008 y actualmente continúa la pena de 20 años de cárcel.

10) The Equation Group y The Shadow Brokers: Yang y Yang

The Equation Group es el nombre informal de la unidad Tailored Access Operations (o TAO) de la Agencia de Seguridad Nacional (NSA) de EE. UU. Su función es recopilar información relacionada con la guerra cibernética. Fundado en 2001, este grupo fue un secreto de Estado bien oculto hasta que se descubrió en 2015, cuando se relacionaron con la organización dos tipos de malware de espionaje: EquationDrug y GrayFish. También se sabe que se abastecieron de vulnerabilidades conocidas para asegurarse de que sus actividades como hacker no se detectasen y se ha especulado con que estuvieron detrás de Stuxnet, el gusano que afectó al programa nuclear iraní durante un tiempo.

F. Profesionales de Ciberseguridad más Famosos

No todos los especialistas en inteligencia tecnológica (conocidos como hacker éticos) son enemigos públicos, la mayoría son hábiles programadores capaces de identificar las debilidades de los programas más blindados. Otros se dedican a proteger los datos en internet, cuentas bancarias, y privacidad de los usuarios. También corrigen 'bugs', descubren fallos de seguridad y los tapan. Persiguen delincuentes, la pornografía infantil en Internet, entre otros delitos importantes.

Un informe de Infoempleo y Deloitte [4] sitúa a los hackers éticos como el perfil mejor pagado en el sector de información tecnológica, con salarios de entre 75.000 y 115.000 euros brutos anuales en Europa. La ciberseguridad se erige como una de las prioridades en todos los sectores de actividad. Entre los casos más conocidos del empleo de hacker éticos para mejorar la seguridad informativa de una compañía o empresa se pueden mencionar:

1) Chema Alonso

De nombre real José María Alonso Cebrián, es considerado uno de los mejores hackers y experto en ciberseguridad de España. Ha recibido diferentes reconocimientos, en 2005 y hasta 2016 Microsoft le concedió el prestigioso galardón Microsoft MVP (Microsoft Most Valuable Professional) en el área de seguridad corporativa. Actualmente es chief data officer de Telefónica. En este cargo lidera la estrategia de 'big data', Publicidad y Cuarta Plataforma de Telefónica. Como parte del trabajo de definición de la Cuarta Plataforma, también lidera el equipo de Banco de Datos Personales y es el patrocinador principal interno del Data Transparency Lab. Es asimismo responsable de la ciberseguridad global y de la seguridad de los datos, creando la nueva Unidad de Seguridad Global con la Information Security Global Business en B2B & B2C e Eleven Paths.

2) Kevin Mitnick

También conocido como "el Condor", es uno de los hackers que cambiaron la historia mundial de la seguridad informática, Mitnick hoy es un importante asesor de ciberseguridad, se dedica a la creación de sistemas de seguridad para importantes compañías en los Estados Unidos. Es experto autodidacta en mostrar las vulnerabilidades de sistemas operativos complejos y dispositivos de telecomunicaciones.

3) Kevin Poulsen

También conocido como Dark Dante, un ex Sombrero Negro, grupo de piratas informáticos que se dedicaban a destrozar los sistemas de seguridad más eficaces del mundo. En octubre de 2006, Kevin Poulsen publicó valiosa información sobre pederastas registrados con la red social MySpace. Su investigación ayudó a identificar 744 personas registradas con perfiles falsos y condujo a la detención de uno de ellos: Andrew Lubrano. Actualmente, trabaja como jefe editor de Wired News, una revista estadounidense.

4) Michael Calce

Otro adolescente convertido en cracker de primera categoría, responsable del ataque que afectó a tres pesos pesados de la industria online: eBay, Amazon y Yahoo!, tras que se le condenó a un uso limitado de Internet. Es otro de los que se ha cambiado de bando, en la actualidad dedica a asesorar empresas sobre seguridad digital y se convirtió en autor con su galardonado libro "Mafiaboy: A Portrait of the Hacker as a Young Man".

G. Inversiones en Ciberseguridad a Nivel Mundial

Con la constante crecida de las amenazas cibernéticas y riesgos de seguridad digital, las organizaciones y empresas se han visto en la necesidad de invertir en ciberseguridad como mecanismos protección, con la finalidad de salvaguardar su información y activos. De igual manera los Estados se han unido a la campaña de inversión en seguridad informática y digital, como método de protección de diversos sectores que incluyen desde el sanitario hasta el militar, como el resguardo de las redes eléctricas hasta redes de comunicaciones.

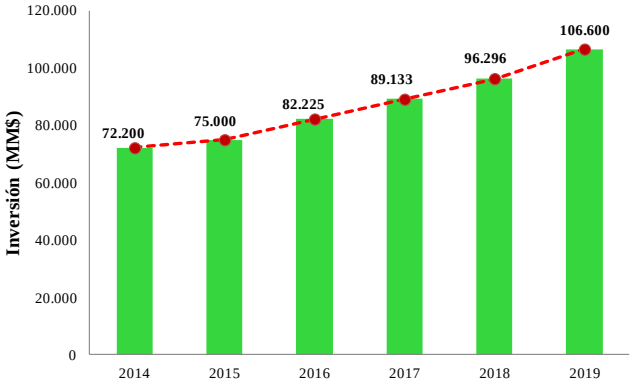

Fig. 10. Distribución de Inversión por Países (Fuente Precise Security)

Según la investigación de Precise Security [6], la inversión en ciberseguridad a nivel mundial durante el 2019 fue de 106.600 MM$, lo que significó un incremento del 10,1% respecto al realizado el año 2018, mostrando un constante durante los últimos cinco años presentando un aumento del 46,8% en relación al año 2014, esto se debe a la concienciación de las organizaciones, empresas y entes gubernamentales sobre la importancia de la seguridad digital y de las consecuencias sobre la vulnerabilidad de la misma. Además estima que la inversión mundial en esta área para el 2023 sea mayor a los 151.000 MM$.

De acuerdo a la misma investigación Precise Security (2020), la mayor parte de la inversión en seguridad se centró en lo referente a servicios de seguridad gestionada, de integración, consultoría y educación, así como capacitación en seguridad de integridad tecnológica. El software fue la segunda área de destino de los gastos en seguridad, como lo son software de seguridad, los de gestión de identidades y confiabilidad, análisis de seguridad, inteligencia y respuesta ante eventos. El resto de la inversión se centró en el hardware, de los cuales en su mayoría fueron destinados a productos de seguridad de red. En la Tabla IV se observa las cantidades de inversión por cada rubro y en la Fig. 11 se desglosan en porcentajes para tener una mejor idea de la división de los gastos.

Tabla IV. Inversión Mundial en Ciberseguridad por Áreas 2019 (Fuente Precise Security)

Area	Inversión (MM$)
Servicios	47.600
Software	38.000
Hardware	21.000

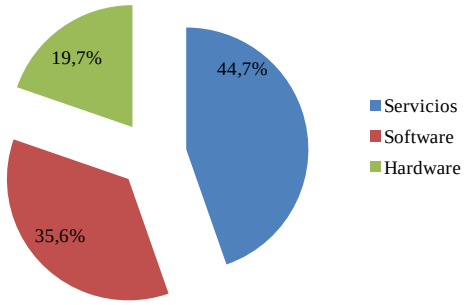

Fig. 11. Distribución porcentual de Inversión 2019 (Fuente Precise Security)

Con el constante aumento de los dispositivos digitales interconectados, además del incesante incremento de los ataques cibernéticos, la seguridad cibernética se ha convertido en una necesidad a nivel mundial. Es por ello que se ha vuelto atractiva para los inversores con un horizonte a largo plazo, quienes han sido atraídos a este campo durante varios años, y con razón, debido a que es un sector de alto crecimiento (8 a 10% anual), llegando a obtener un rendimiento bursátil del 130% en los últimos cuatro años, antes de la caída del 25% presentada en febrero del corriente año. Aún así sigue siendo de vital importancia más aún en estos tiempos de la crisis del COVID-19 cuando ha incrementado la demanda del uso de internet debido al confinamiento de las personas en sus hogares.

De nada sirve realizar grandes inversiones en ciberseguridad si no se fortalece el eslabón débil de la cadena: El usuario. Para ello hay que adiestrar y fortalecer la cultura de seguridad informática, puesto que es la falta de cultura y las carencias en formación la principal base del problema. Los usuarios aún no poseen la concienciación adecuadas en materia de ciberseguridad. Según un informe de CHECK POINT, uno de cada cinco empleados es causal de una brecha de seguridad mediante el mal uso de su computador, laptop o dispositivo móvil.

Es por ello que los ciudadanos en general, los profesionales y empleados en particular, son hoy en día el "eslabón más débil" de la cadena en la ciberseguridad. El phishing y la ingeniería social son las técnicas más empleadas para llegar hasta ellos. Es por ello, que mientras no cuenten con la formación y conocimiento adecuados, el problema puede volverse cada vez más complejo, ya que los ciberdelincuentes tienen espacios abiertos a través de los que pueden vulnerar y explotar cualquier dominio o dispositivo. Dicho en palabras sencillas es de vital importancia que los usuarios y empleados reciban la formación adecuada sobre los riesgos y amenazas, así de cómo prevenir ser víctima y sus consecuencias.

H. Ranking de Ciberseguridad a Nivel Mundial

Para poseer una excelente ciberseguridad, no solo basta con realizar grandes inversiones en el área de seguridad informativa, se debe cumplir con una serie de criterios para poder ser considerado entre los países mas ciberseguros del mundo, entre ellos están la capacidad de

enjuiciar a los cibercriminales, capacidad técnica para prevenir ataques cibernéticos, la cooperación con otros países, fortaleza que tiene la industria local en materia de ciberseguridad y la forma en que está organizada la agencia u organismo Nacional dedicado a la de seguridad cibernética del gobierno.

En una investigación realizada por una compañía británica de Comparitech [5], en la cual se calificó y analizó el comportamiento de diversos patrones y vulnerabilidades cibernéticas en todo el mundo, entre los cuales están la cantidad de infecciones de malware, la cantidad de ataques de malware financieros, la capacidad de reacción ante ataques cibernéticos y la legislación sobre ciberseguridad, se obtuvo así, según sus cifras, los países más seguros en materia cibernética así como los más vulnerables.

Los resultados obtenidos por la compañía revelaron que Dinamarca es el país con mayor ciberseguridad del mundo, subiendo desde el cuarto lugar que tuvo el año pasado, desplazando a Japón del sitial de honor, el cual cayó a la quinta posición. Completan la lista de los primeros 5 países de alto rendimiento: Suecia, Alemania, Irlanda y Japón. Países como Francia, Canadá y Estados Unidos fueron expulsados de los cinco países con mayor seguridad cibernética y se ubicaron en el noveno, sexto y 17º lugar, respectivamente.

De igual manera el estudio reveló que Argelia es el país con peor ciberseguridad del mundo, revalidando ese lugar respecto al año 2018, seguido por Tayikistán, Turkmenistán y Siria como los países con menor índice de seguridad cibernética del planeta.

Según el informe Riesgos regionales para hacer negocios 2019 del Foro Económico Mundial. En una encuesta realizada a cerca de 13.000 líderes empresariales la principal preocupación de la Región de Europa y Norteamérica son los ciberataques, seguidos de ataque terroristas y crisis fiscales.

Tabla V. Riesgo Empresarial Europa y Norteamérica 2019 (Fuente Comparitech)

Región	Riesgo #1	Riesgo #2	Riesgo #3
Europa	Ciberataques	Crisis Fiscal	Burbuja de Activos
Norteamérica	Ciberataques	Fraude o Robo de Datos	Ataque Terrorista

Es contradictorio el hecho que al pesar que con el pasar del tiempo las empresas, organizaciones y gobiernos han incrementado las inversiones en el tema de ciberseguridad de igual manera han ido en aumento los ciberataques y pérdidas generadas por fraudes digitales.

I. Métodos para mejorar la Ciberseguridad a Nivel Mundial

En los últimos años las amenazas cibernéticas se han convertido en uno de los principales riesgos para los usuarios, compañías, empresas y gobiernos a nivel mundial, mostrando un crecimiento tanto en el número de víctimas como en las pérdidas generadas. Es de entender que ninguna persona, compañía, empresa o ente gubernamental puede estar seguro de que nunca va a sufrir un ataque que ponga en peligro su ciberseguridad, pero lo que sí puede hacer es tomar las medidas adecuadas para reducir las probabilidades y evitar los daños siempre que sea posible. Si se tiene en cuenta el impacto causado por un ciberataque contra la infraestructura crítica de un país, cualquier mejora en la estrategia de ciberseguridad será fundamental. Teniendo en cuenta esto se muestran algunos consejos y recomendaciones para prevenir y/o evitar futuros desastres informáticos.

1) Adiestramiento de Personal

Se debe entrenar al personal sobre temas de seguridad informática y establecer políticas sobre el uso del e-mail, aplicaciones y páginas web, puesto que muchos ataques perpetrados se desencadenaron a través de un correo electrónico enviado al buzón de un empleado. Si se cuenta con la formación adecuada, este tipo de ataque no se puede llevar a cabo. Por este motivo en la actualidad un gran número de empresas están cambian su enfoque, de mejora de infraestructura a perfeccionamiento del factor humano en el área de ciberseguridad.

2) Reducción de Vulnerabilidad

La gestión de contraseñas y la administración de accesos privilegiados no se deben tomar a la ligera, por lo tanto se deben tomar medidas para proteger adecuadamente los equipos, información de la empresa y datos personales, incrementando la ciberseguridad. Para ello se pueden realizar las siguientes acciones:

- ***Gestión de Contraseñas:*** Con el aumento del uso de la fuerza bruta para intentar descubrir contraseñas, conviene reforzar los sistemas de verificación de los dispositivos. Las contraseñas largas y aleatorias previenen ataques de fuerza bruta y usar contraseñas diferentes por cada cuenta evita comprometerlas todas cuando se produce una violación de datos. Y aunque la autenticación de doble factor no es infalible, sí ayudará a complicarle las cosas a los ciberdelincuentes.
- ***Cifrado:*** Debido a que entre los principales objetivos de los ciberataques es el acceso a información delicada o confidencial, se deben tomar las medidas oportunas para cifrarla debidamente, de modo que, incluso aunque logren acceder a ella, la labor de des-encriptación sea más compleja.
- ***Control de procesos:*** La mejor forma de saber si se están produciendo accesos sospechosos a un sistema informático es medir su actividad en todo momento. En este sentido, existen programas y aplicaciones que monitorizan todos los procesos en tiempo real, detectan actividad inusual y, con todo ello, evitan el peligro antes de que llegue a producirse.
- ***Aislamiento:*** parte significativa de las vulnerabilidades se producen en infraestructuras a las que los ciberdelincuentes acceden de forma remota. Por ello es esencial que tanto los procesos como sistemas más delicados sean convenientemente aislados y, a ser posible, en redes sin conexión a internet.

3) Instalación y Actualización de Sistemas y Medidas de Seguridad Básicas

Los usuarios deben garantizar que sus computadores u ordenadores tengan debidamente instalados y actualizados los programas y recursos disponibles para su protección, tales como:

- ***Antivirus:*** existen una gran gama de antivirus que se encargan de detectar y eliminar las potenciales amenazas. Es de vital importancia mantener el software actualizado para obtener el mejor nivel de protección. El tipo de antivirus a utilizar depende de necesidades o requerimientos de cada usuario.
- ***Cortafuegos:*** Es un sistema que ejecuta una política de seguridad establecida, con el cual se filtra accesos de red y

bloquea el acceso a personas no autorizadas. Una vez instalado se debe mantener el Firmware actualizado en todo momento.

- ***Proxy:*** se considera un complemento del firewall ya que hace la función de intermediario, permitiendo el control de acceso, registro del tráfico, la mejora de rendimiento y el anonimato de la comunicación.
- ***Listas de control de acceso:*** Estas listas permiten determinar los permisos de acceso apropiados a usuarios y grupos concretos. Por ejemplo, puede definirse sobre un Proxy una lista de los usuarios a quienes se les permite el acceso a Internet.
- ***Redes privadas virtuales:*** Una extensión de red segura que se crea sin que los dispositivos estén conectados entre sí físicamente. Cuando utilizamos una VPN nos conectamos a los servicios de Internet de nuestro proveedor y no de manera directa. La VPN garantiza la confidencialidad de los datos.
- ***Sistema de prevención de intrusos:*** Es un sistema que soporta los dispositivos inalámbricos para evitar los puntos de acceso no autorizados y otras amenazas inalámbricas.

3) Utilización de Lave de Seguridad de Hardware

Para cuentas y datos vitales, en especial para entornos profesionales y empresariales, es conveniente hacer uso de un refuerzo adicional para protegerlos usando un mecanismo de seguridad de hardware, por lo general es un dispositivo en formato USB con un motor de cifrado de alta seguridad. Este proceso se realiza dentro del hardware para aumentar en gran medida la seguridad general frente a las soluciones por software.

4) Sentido Común

Como se ha dicho en reiteradas oportunidades, de nada sirven grandes inversiones en materia de ciberseguridad si el usuario no toma consciencia de la importancia de actuar con prudencia ante posibles amenazas. Algunas recomendaciones para evitar ser víctimas de ataques cibernéticos son:

- No abrir archivos adjuntos de correos electrónicos de remitentes desconocidos.
- No hacer clic en los vínculos de los correos electrónicos de remitentes o sitios web desconocidos.
- Evitar el uso de redes Wi-Fi no seguras en lugares públicos.

Si bien estas recomendaciones son importantes, no son una guía definitiva. La instalación de parches y actualizaciones, la protección de los puntos finales y la gestión integral de las distintas áreas del ambiente de ciberseguridad, son otras opciones para mantener lejos estas amenazas y proteger la información corporativa. Hay que recordar que lo más costoso no es mantener la red a punto y con toda la protección disponible, más costoso es no hacerlo. Si lo duda, basta con observar las pérdidas presentadas por las organizaciones, empresas y usuarios mencionados con anterioridad.

III. CONCLUSIONES

Con la globalización digital de las empresas, compañías y gobiernos, los usuarios se han convertido cada día en blancos más atractivos para los criminales cibernéticos, quienes aprovechan la web para mantenerse en el anonimato mientras realizan sus ataques. Con la finalidad de minimizar las probabilidades de ser víctimas de ciberataques, han incrementado la inversión en ciberseguridad. A pesar de ello los cracker han conseguido la manera de burlas las medidas de seguridad para lograr acceder a información confidencial o delicada de los usuarios para con ello alcanzar un lucro económico.

Las amenazas más devastadoras para la economía empresarial y de los usuarios durante el 2019 fueron los scams (engaños), compromiso de cuentas de email corporativas (BEC) y el fraude con argumento sentimental, representando el 47% de los delitos totales y el 65% de las pérdidas económicas., siendo el sector más vulnerable a los ataques digitales los adultos mayores a 50 años, quienes representaron el 42% de las victimas totales y el 49% de las pérdidas generadas durante el año pasado. El país con mayor porcentaje de ataques durante el 2019 fue Estados Unidos con 76,2% del total de reportes, seguido del Reino Unido con el 20,1% de los casos registrados. La inversión en ciberseguridad ha mostrado un incremento del 46,8% en los últimos 5 años hasta alcanzar la cifra de 106.600 MM$ durante el 2019.

De igual manera a pesar de todos los gastos en mejoras de software, hardware y servicios de seguridad, la mayor prevención para evitar ser víctima de ciberataques es el adiestramiento y concienciación del usuario final, con ello evitar el acceso de las amenazas a computadores u ordenadores y de esta manera mantener la confidencialidad de la información almacenada en ellos y en la red.

IV. REFERENCIAS

[1] M. Gorham, “2019 Internet Crime Report”, Federal Bureau of Investigation, Washington D. C., Int. Crim. Comp. Cent. 20. Dic. 2019.

[2] Redacción TICPymes. (2020, Feb 13). Los 10 ciberataques más grandes de la década [Online]. Disponible: https://www.computing.es/seguridad/noticias/ciberataques-mas-grandes-de-decada.1.html

[3] Kaspersky Lab. (2020, May 18). Los 10 hackers más infames de todos los tiempos. [Online]. Disponible: https://latam.kaspersky.com/resource-center/threats/top-ten-greatest-hackers

[4] elPeriódico. (2018, Nov 22).Quienes son los genios de la ciberseguridad en el mundo. [Online]. Disponible: https://www.elperiodico.com/es//hablemos-de-futuro/20180910/genios-ciberseguridad-mundo-7018808

[5] M. Hernández. (2020, Mar 05). Radiografía | Estos son los países más ciberseguros del mundo. [Online]. Disponible: https://forbes.co/2020/03/05/tecnologia/radiografia-estos-son-los-paises-mas-ciberseguros-del-mundo/

[6] Redacción Muycanal. (2020, Abr 15). La inversión en ciberseguridad crece un 10,7% en 2019. [Online]. Disponible: https://www.muycanal.com/2019/10/21/inversion-ciberseguridad-2

Jose Luis Gamboa Suárez
Tecnólogo en Diseño y Administración de sistemas de las Unidades Tecnológicas de Santander, Ingeniero de Sistemas egresado de la Universidad de Investigación y Desarrollo.