LAS AMENAZAS CIBERNÉTICAS

Daniel Reyna Ramos*
Daniel Armando Olivera Gómez&

INTRODUCCIÓN.

Algunos autores consideran que el término "**ciberespacio"** se popularizó en la década de los 90´s por la rápida expansión de millones de usuarios que interactuaban en Internet con el propósito de otorgar productos y servicios o simplemente utilizando los productos "públicos" de esa época como los chats, portales web y otros sitios de interacción.

A través del **"ciberespacio"** es muy fácil y económico "convivir" con el mundo global, ya que hoy en día desde cualquier dispositivo que tenga conexión a internet podemos mandar alguna solicitud de compra o colocar algún producto para venta, así como, enviar tareas escolares e interactuar con alguna plataforma educativa o social; más aún con algún juego "on line", que permite a toda persona tener una convivencia con otros a través de sus consolas de juego.

Las redes sociales también son parte de este **"Ciberespacio"**, las cuales han tomado una popularidad increíble entre los millones de usuarios, lo cual ha permitido agrandar el universo del Internet, para dar paso a las telecomunicaciones y a la amplitud de aparatos electrónicos como las TV´s, Smart Phone y Tablets que facilitan la comunicación de sus usuarios.
El ciberespacio ha permitido la construcción de modelos o plataformas que ofrecen servicios a través del internet en el

* Académico del Instituto Universitario Veracruzano y Becario CONACYT en el Instituto de Investigaciones y Estudios Superiores de las Ciencias Administrativas de la Universidad Veracruzana daniel.reyna23@gmail.com

& Investigador del Instituto de Investigaciones y Estudios Superiores de las Ciencias Administrativas de la Universidad Veracruzana. Correo electrónico: dolivera@uv.mx.

sector público, privado, salud, educativo, etc., para que los millones de **"cibernautas"** puedan realizar cualquier actividad.

El término **"cibernauta"** es asociado a los millones de usuarios que utilizan las Tecnologías de la Información para **"navegar"** a través de la red pública de Internet.

En la actualidad ser un **"Cibernauta"** es tener presencia constante en el **"ciberespacio"**, desde leer noticias e interactuar con ellas a través de distintos canales de comunicación, ser estudiante en una plataforma educativa en el sector de la educación o tomando un curso que la empresa ha preparado para sus trabajadores o simplemente buscando algún producto o servicio de interés personal.

La naturaleza del ser humano también ha permitido que en estos espacios del Internet, día a día tengan un mayor crecimiento económico, social, político, educativo e interpersonal; este crecimiento desordenado tiene sus consecuencias a tal grado que como cualquier población del mundo, el ciberespacio también se vea rebasado en su ámbito social.

La falta de reglamentación permitió que personas se atrevieran a delinquir con la información que se contienen almacenados en todos los servidores, computadoras o equipos conectados a este **"Ciberespacio"**.

Obteniendo en algunos delos casos millones de dólares en ganancias como botín por el robo de la información de algunas empresas o cibernautas que se vieron involucradas en estos siniestros por no tener la seguridad requerida para evitarlos.
Esto tuvo como consecuencia la reorganización de todas las partes involucradas para tomar medidas de seguridad en su infraestructura, asi como la creación de software y hardware para prevenir y contraatacar las amenazas existentes en el Internet.

De igual manera se tuvo que crear la normatividad y legalidad necesaria para mitigar la comisión de delitos que tuvieran cabida en los ataques a empresas o a usuarios de esta red y determinar las sanciones correctivas a los delincuentes que realizan estos delitos creando el término **"Ciberseguridad"**.

La **"Ciberseguridad"** es definida POR LA UNIÓN INTERNACIONAL DE TELECOMUNICACIONES EN SU PORTAL WEB COMO: "CONJUNTO DE HERRAMIENTAS, POLÍTICAS, CONCEPTOS DE SEGURIDAD, SALVAGUARDAS DE SEGURIDAD, DIRECTRICES, MÉTODOS DE GESTIÓN DE RIESGOS, ACCIONES, FORMACIÓN, PRÁCTICAS IDÓNEAS, SEGUROS Y TECNOLOGÍAS QUE PUEDEN UTILIZARSE PARA PROTEGER LOS ACTIVOS DE LA ORGANIZACIÓN Y LOS USUARIOS EN EL CIBERENTORNO. LOS ACTIVOS DE LA ORGANIZACIÓN Y LOS USUARIOS SON LOS DISPOSITIVOS INFORMÁTICOS CONECTADOS, LOS USUARIOS, LOS SERVICIOS/APLICACIONES, LOS SISTEMAS DE COMUNICACIONES, LAS COMUNICACIONES MULTIMEDIOS, Y LA TOTALIDAD DE LA INFORMACIÓN TRANSMITIDA Y/O ALMACENADA EN EL CIBERENTORNO. LA CIBERSEGURIDAD GARANTIZA QUE SE ALCANCEN Y MANTENGAN LAS PROPIEDADES DE SEGURIDAD DE LOS ACTIVOS DE LA ORGANIZACIÓN Y LOS USUARIOS CONTRA LOS RIESGOS DE SEGURIDAD CORRESPONDIENTES EN EL CIBERENTORNO. LAS PROPIEDADES DE SEGURIDAD INCLUYEN UNA O MÁS DE LAS SIGUIENTES: DISPONIBILIDAD; INTEGRIDAD, QUE PUEDE INCLUIR LA AUTENTICIDAD Y EL NO REPUDIO; CONFIDENCIALIDAD." (ITU, 2010)

Es decir, proteger las tecnologías de la información y telecomunicaciones de las empresas y a los usuarios de Internet sobre ataques que estos pudieran ser objetos a través de herramientas tecnológicas, cuidando la integridad, autenticidad y confidencialidad de la información que contienen.

Bajo estos términos el sector privado y gubernamental han tomado las medidas necesarias para que los transacciones de los servicios y productos que ofertan sean de forma segura o al menos tener la certeza de no ser sorprendidos por la **"Ciberdelincuencia"**, es decir, dar las condiciones necesarias para que estas se realicen de forma segura.
Se han creado algunas instituciones gubernamentales en México como la creación de la División Científica en la Policía Federal, que ayuda a prevenir o en su caso a darle seguimiento a los delitos cibernéticos reportados.

También cuenta con un Centro Nacional de Respuesta a Incidentes Cibernéticos (CERT-MX), los cuales a través de boletines advierten a los usuarios acerca de las amenazas que se presentan, más adelante platicaremos sobre estos CERT.

Es por ello que debemos conocer algunos de los modelos que se utilizan en el **"Ciberespacio"**, así como sus principales amenazas, los ataques que se han presentado y algunas de las mejores prácticas para mitigar estos ataques.

MODELOS QUE SE UTILIZAN EN EL "CIBERESPACIO".

En el Ciberespacio hay cabida para todo tipo de emprendimiento, así como la capacidad de crear cualquier noticia, dar a conocer alguna revista, periódico o libro, conocer otros lugares, conocer a otras personas en el modo virtual.

Es una comunidad en la que puedes llevar una vida virtual como si la tuvieras personalmente comprar una casa, vehículo, electrodoméstico, ropa, zapatos, en fin, toda una vida virtual.

Para ello se han instalado en el Internet modelos que permiten realizar diversas actividades mientras estas realizando físicamente una diferente.

Correo Electrónico.

Puedes enviar o recibir mensajes y/o archivos a través de un **"Correo Electrónico"** que es una herramienta que permite enviar y recibir documentos electrónicos y que millones de personas conectadas al Internet poseen, esta herramienta las podemos llamar en dos formas:

Correos Electrónicos "públicos" estos están regidos por instituciones que ofrecen su servicio a todo usuario de la Internet regidos a través de políticas de comunicación y uso para utilizar su plataforma.

La seguridad de estos correos, son administrados por la empresa que los representa, quienes invierten millones de dólares en este rubro, ya que son "blanco" de diversos ataques para destruir su "reputación", como ejemplos: @hotmail, @gmail;

Correos Electrónicos "privados" estos correos son creados para los trabajadores de empresas privadas y su seguridad es administrada por personal de la empresa o por otra empresa que hayan contratado, sus políticas y restricciones son generadas de manera interna, como ejemplos tenemos @pgr.gob.mx, @ux.edu.mx

Este modelo de comunicación diariamente recibe ataques de diferentes formas encontramos su vulnerabilidad en los usuarios que no siguen las normas y políticas preestablecidas, también la intrusión de algún virus informático tipo malware que vulnere la seguridad de su computadora.

Redes Sociales.

Como parte de la naturaleza de los seres humanos hemos aprendido a socializar con personas diferentes o afines a nosotros, lo cual ha permitido engrandecer el conocimiento de la humanidad.

Conociendo diferentes lenguas, gastronomía, cultura, tecnología, moda, salud, economía y educación, entre otros, y en el mundo globalizado del Internet descubrimos otras formas de pensar, construir y de realizar actividades cotidianas a como las realizamos.

Es por ello que en el **"Ciberespacio"** encontramos aplicaciones informáticas que nos permiten realizar estas actividades.

El observatorio Nacional de las Redes Sociales y de las SI, en su documento denominado "Las Redes Sociales en Internet" la define como: "un sitio en la red cuya finalidad es permitir a los usuarios relacionarse, comunicarse, compartir contenido y crear comunidades", o como una herramienta de "democratización de la información que transforma a las personas en receptores y en productores de contenidos". (Osigma, 2011).

Así también las tipifica en:

Redes Sociales Directas.

Son redes sociales directas aquellas cuyos servicios prestados a través de Internet en los que existe una colaboración entre grupos de personas que comparten intereses en común y que, interactuando entre sí en igualdad de condiciones, pueden controlar la información que comparten. Los usuarios de este tipo de redes sociales crean perfiles a través de los cuales gestionan su información personal y la relación con otros usuarios. El acceso a la información contenida en los perfiles suele estar condicionada por el grado de privacidad que dichos usuarios establezcan para los mismos.

LAS REDES SOCIALES DIRECTAS PUEDEN CLASIFICARSE DE DIFERENTE FORMA EN FUNCIÓN DEL ENFOQUE EMPLEADO COMO MUESTRA LA SIGUIENTE TABLA:

Tabla 1. Categorías de redes sociales directas en función del enfoque

Según finalidad	Según modo de Funcionamiento	Según grado de apertura	Según nivel de integración
De ocio	De contenidos	Públicas	De integración vertical
De uso profesional	Basada en perfiles: personales/profesionales	Privadas	De integración horizontal
	Microblogging		

Fuente: ONTSI

Según grado de apertura.

SE TIENE EN CUENTA LA CAPACIDAD DE ACCESO A LAS MISMAS POR CUALQUIER USUARIO ENTENDIDA ÉSTA COMO EL NIVEL DE RESTRICCIÓN QUE SE APLICA.

- ***REDES SOCIALES PÚBLICAS**. ESTÁN ABIERTAS A SER EMPLEADAS POR CUALQUIER TIPO DE USUARIO QUE CUENTE CON UN DISPOSITIVO DE ACCESO A INTERNET SIN NECESIDAD DE PERTENECER A UN GRUPO U ORGANIZACIÓN CONCRETA.*
- ***REDES SOCIALES PRIVADAS**. ESTÁN CERRADAS A SER EMPLEADAS POR CUALQUIER TIPO DE USUARIO. SÓLO SE PUEDE ACCEDER A ELLAS POR LA PERTENENCIA A UN GRUPO ESPECÍFICO U ORGANIZACIÓN PRIVADA QUE*

SUELE HACERSE CARGO DEL COSTE DE LA MISMA. LOS USUARIOS SUELEN MANTENER RELACIÓN CONTRACTUAL O DE OTRA ÍNDOLE CON DICHO GRUPO ESPECÍFICO U ORGANIZACIÓN.

Según nivel de integración.

SE TIENE EN CUENTA EL NIVEL DE AFINIDAD, INTERÉS E INVOLUCRACIÓN EN MATERIAS O ACTIVIDADES DE TIPO, PREFERENTEMENTE, PROFESIONAL.

- ***REDES SOCIALES DE INTEGRACIÓN VERTICAL**. SU EMPLEO SUELE ESTAR ACOTADO AL USO POR PARTE DE UN GRUPO DE USUARIOS A LOS QUE AÚNA UNA MISMA FORMACIÓN, INTERÉS O PERTENENCIA PROFESIONAL. NO ES INFRECUENTE QUE EL USUARIO ACCEDA A ELLAS PREVIA INVITACIÓN POR PARTE DE UNO DE SUS MIEMBROS Y LA VERACIDAD DE LA INFORMACIÓN CONTENIDA EN LOS PERFILES SUELE SER COMPROBADA Y VERIFICADA. PUEDEN SER DE PAGO, EL COSTE SUELE SOPORTARSE POR LOS PROPIOS USUARIOS DE LAS MISMAS CONTANDO CON UN NÚMERO DE USUARIOS MUY INFERIOR AL EXISTENTE EN LAS REDES DE INTEGRACIÓN HORIZONTAL.*
- ***REDES SOCIALES DE INTEGRACIÓN HORIZONTAL**. SU EMPLEO NO ESTÁ ACOTADO A UN GRUPO DE USUARIOS CON INTERESES CONCRETOS EN UNA MATERIA.*

ALGUNOS EJEMPLOS DE REDES SOCIALES DIRECTAS, INCLUIDAS EN EL ANEXO DEL PRESENTE ESTUDIO,
SON: FACEBOOK, YOUTUBE, WIKIPEDIA, HI5, LINKEDIN, MYSPACE. (Osigma, 2011)

Las Redes Sociales en México han tenido mucho éxito ya que un gran porcentaje de los cibernautas las utilizan como medio de comunicación, asi como para mostrarse ya que permiten el envío

de imágenes, vídeos, texto y la localización del lugar donde se encuentran.

La vulnerabilidad de esta modalidad se encuentra en la información que se publica ya que los **"Cibernautas"** de estas redes no dimensionan el gran peligro en el que se encuentran al incorporar información en estas redes, muchos de ellos no verifican las políticas de privacidad de las aplicaciones que instalan y hacen uso, ya que cualquier persona que este incorporada a esa red social puede hacer uso malintencionado de la información.

Por lo que se ha dado que a través de esta modalidad el "robo de identidad", el "hackeo", y la difamación, se vea a la alza en el uso de la "ciberdelincuencia" para que los usuarios sean "blancos" fáciles en los ciberataques.

Banca en Línea.

La modalidad de Banca en línea muestra grandes beneficios para los usuarios que utilizan este servicio como lo define la CONDUCEF en su portal web: ENTRE LOS MUCHOS BENEFICIOS DE LA BANCA EN LÍNEA DESTACAN DOS: LA SEGURIDAD Y LA COMODIDAD. CON ESTE SERVICIO NO TIENES QUE CARGAR EFECTIVO PARA REALIZAR COMPRAS QUE INVOLUCRAN MONTOS IMPORTANTES; POR EJEMPLO, EL ENGANCHE DE UN AUTO O UNA CASA, LO QUE REDUCE EL RIESGO DE QUE TE ASALTEN. ADEMÁS PUEDES REALIZAR CASI TODAS TUS OPERACIONES FINANCIERAS DESDE TU CASA U OFICINA LAS 24 HORAS DEL DÍA, SIN ACUDIR A LA SUCURSAL BANCARIA NI HACER FILAS.

EL TIPO DE OPERACIONES QUE PUEDES HACER A TRAVÉS DE LA BANCA EN LÍNEA VARÍA RESPECTO AL BANCO CON EL QUE MANEJES TU CUENTA DE CHEQUES O DE NÓMINA, LAS CUALES FUNCIONAN COMO CUENTA EJE (CUENTA A TRAVÉS DE LA CUAL

PUEDES HACER OPERACIONES COMO DEPÓSITOS O PAGOS), Y DEL TIPO DE SERVICIO QUE CONTRATES. (CONDUSEF, PROTEJA SU DINERO, 2016)

A través de esta modalidad se pueden realizar pagos de servicios, traspasos de efectivo, domiciliar los pagos y realizar inversiones, entre otros servicios, de acuerdo a la sucursal bancaria que lo oferta.

La vulnerabilidad en esta modalidad también consiste en el "usuario" ya que los bancos invierten grandes cantidades de dinero en la seguridad de sus aplicaciones, los usuarios son engañados a través de la "Ingeniería Social" (manipulación de una persona hacia su víctima para obtener información confidencial).

Comercio Electrónico

Como toda comunidad el **"ciberespacio"** representa un modelo económico transaccional donde los millones de cibernautas pueden realizar

De acuerdo al estudio realizado en "Comercio Electrónico" durante 2015 por la Asociación Mexicana de Internautas en México AMIPCI el resultado fue lo siguiente:

- DE ACUERDO A LA ACTIVIDAD DE COMPRA REGISTRADA DESDE ENERO A MARZO DE 2015, TRES CUARTOS DE LOS INTERNAUTAS MEXICANOS REALIZAN COMPRAS ONLINE.
- MÁS DE LA MITAD COMPRÓ FUERA DEL PAÍS DURANTE ESTE PERÍODO.
- EL VOLUMEN DE COMPRADORES HA CRECIDO FUERTEMENTE INFLUENCIADO POR LA COMPRA DE DESCARGAS DIGITALES DESDE DISPOSITIVOS MÓVILES

- El gasto trimestral promedio en todos los dispositivos y categorías que no se relacionan a viajes fue de MXN$ 5,575.00 pesos, alrededor de MXN$ 1,860.00 pesos gastados online por mes.
- Dos tercios de los compradores utilizan un dispositivo móvil (smartphone y/o tablet) para sus compras online, con tan sólo un tercio que utiliza exclusivamente PC/Laptop.
- A los mexicanos les gusta utilizar dispositivos móviles para un acceso a internet en cualquier lugar, y también por la posibilidad de utilizar la aplicación de los comercios, lo cual puede ahorrarles tiempo.
- Siete de cada diez usuarios realizaron compras desde las aplicaciones del comercio, y más de un tercio compró en las aplicaciones. (AMIPCI, "COMERCIO ELECTRÓNICO", 2015)

Ventas en línea:

- Tres de cada cuatro ventas en línea ocurren por medio de una PC/Laptop. Las cuatro categorías principales vendidas en línea son ropa, deportes, otras categorías no enlistadas y electrónicos de consumo.
- La gran cantidad de incidencias en "otras categorías no enlistadas", indica la diversificación de la oferta del comercio electrónico.
- Por valor de ventas, sin incluir viajes, las cuatro categorías principales son electrónicos de consumo, computadoras/dispositivos periféricos/PDAs, y boletos de eventos.

- LOS COMERCIOS ESPERAN QUE LAS COMPRAS AUMENTEN ALREDEDOR DE EL BUEN FIN, NAVIDAD Y HOTSALE.
- CASI NUEVE DE CADA DIEZ COMERCIOS ESTÁN CONSCIENTES DEL SELLO DE CONFIANZA DE AMIPCI, PERO SÓLO DOS DE CADA CINCO OFRECE EL SELLO DE CONFIANZA EN SU SITIO. CASI TODOS LOS COMERCIOS ESTÁN CONSCIENTES DE LOS EVENTOS EL BUEN FIN Y HOTSALE. (AMIPCI, "COMERCIO ELECTRÓNICO", 2015)

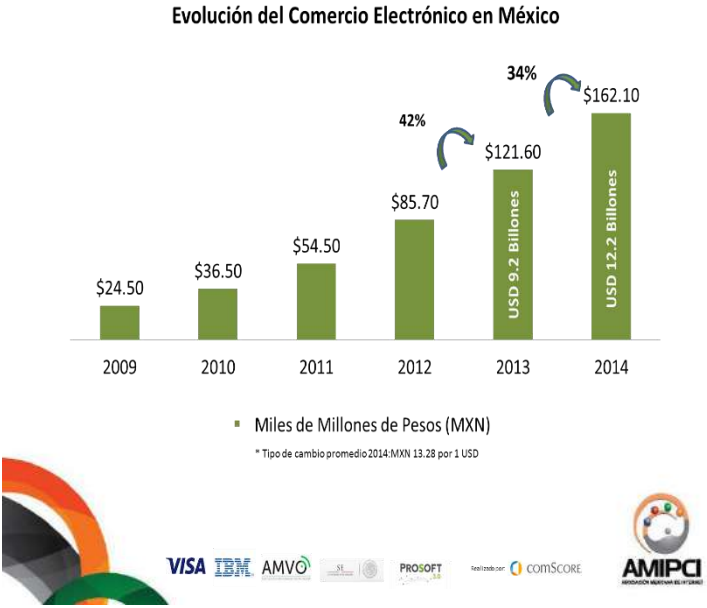

Figura 1.- Tabla de Evolución del Comercio Electrónico en México (AMIPCI, "COMERCIO ELECTRÓNICO", 2015)

En la figura 1 vemos la evolución en millones de pesos que ha tenido el Comercio Electrónico en Mexico, mostrando un aumento del 34% solo en los últimos años (2013-2014), lo que demuestra que a nivel económico genera grandes ganancias para las empresas que utilizan este modelo en el **"ciberespacio".**

Este modelo en particular ha sufrido las consecuencias de los mayores **"ciberataques"** en todo el mundo aunque no hay cifras reales ya que muchos usuarios que han sufrido estos ataques, no lo registran ante las instituciones encargadas de llevar la estadística delictiva en este tema, pero más adelante veremos algunos de los ataques relevantes que se han sufrido.

Juegos en línea

Hay una gran amenaza en esta modalidad ya que la mayoría de los **"Cibernautas"** que la utilizan son menores de edad, y no conocen los riesgos a los que se puedan enfrentar y para la **"Ciberdelincuencia"** se convierten en un "blanco" fácil para atacar.
La revista electrónica "Merca2.0" publica las 5 amenazas que acechan en los videojuegos, detectadas por la empresa Kaspersky, descritas a continuación:
1.- **PHISHING**. ÉSTA ES UNA TÁCTICA QUE DA BASTANTE RESULTADOS A QUIENES BUSCAN ATACAR EL MUNDO DE LOS JUEGOS EN LÍNEA, YA QUE MEDIANTE CORREOS FALSOS LOGRAN QUE EL USUARIO SE DIRIJA A PORTALES FRAUDULENTOS, SIMILARES A LOS ORIGINALES QUE PIDEN CONTRASEÑAS. CON ESTO, LOS ATACANTES INTENTAN APODERARSE DE DATOS COMO LOS DE LAS TARJETAS DE CRÉDITO.
2.- **CIBERACOSO**. ALGUNOS DE LOS JUEGOS TIENEN LA OPCIÓN PARA INTERACTUAR CON OTROS JUGADORES, ESTE MEDIO PUEDE SER EMPLEADO PARA INSULTAR A LOS DEMÁS, O BIEN PARA INDAGAR SOBRE LA VIDA PRIVADA DE LOS USUARIOS.

3.- **TRAMPAS.** HAY HACKERS QUE BUSCARÁN REALIZAR ESTAFAS A OTROS JUGADORES MEDIANTE LA VIOLACIÓN DE LAS REGLAS, AL UTILIZAR CUENTAS DE OTROS CLIENTES PARA JUGAR EN MEJORES CONDICIONES QUE AQUELLOS QUE REALIZAN EL PROCESO DE LOS JUEGOS DE MANERA NORMAL, LOS NOVATOS EN ESTAS ACTIVIDADES SON SUS PRINCIPALES BLANCOS.
4.- **ENVIDIAS**. SI UNA CUENTA TIENE UN PERSONAJE ALTAMENTE DESARROLLADO O ES PRESTIGIADO ENTRE LA COMUNIDAD DE CIBERPLAYERS PODRÁ SER UNO DE LOS PRINCIPALES OBJETIVOS DE ATACANTES QUE SE DEDICAN A DESTRUIR DICHOS PERFILES.
5.- **ENGAÑOS.** OTRA MANERA EN SER VULNERABLE A LOS ATAQUES ES A TRAVÉS DE LAS FALSAS ACTUALIZACIONES O UTILIDADES DE LOS JUEGOS. A TRAVÉS DE ESAS ACCIONES, LOS HACKERS INTENTAN ROMPER LA SEGURIDAD DE LAS COMPUTADORES O DE LOS DISPOSITIVOS MÓVILES PARA INSTALAR ALGÚN MALWARE. (Merca2.0, 2014)

PRINCIPALES ATAQUES

En este apartado conoceremos algunos de los ataques más recientes que se han realizado en el **"ciberespacio"** los cuales han servido para conocer la vulnerabilidad del hardware y software utilizado en su infraestructura de seguridad, así como, las mejores prácticas para mitigar ataques futuros.

Ciberataque a Dyn de octubre de 2016

El portal web Colarebo Internacional publicó el ataque que recibió esta empresa.

DYN ES UN PROVEEDOR DE DNS (DOMAIN NAME SYSTEM-SISTEMA DE RESOLUCIÓN DE NOMBRES), QUE PROPORCIONA EL SERVICIO DE MAPEO DE "NOMBRE DE DOMINIO" A USUARIOS FINALES, ES DECIR PROPORCIONA LA IP CORRESPONDIENTE.

EL ATAQUE FUE DEL TIPO CONOCIDO COMO DDOS (DENEGACIÓN DE SERVICIOS) FUE CONTRA LOS SERVIDORES DE DYN, UNA IMPORTANTE EMPRESA QUE ADMINISTRA EL RENDIMIENTO DE INTERNET Y EL ACCESO A SITIOS COMO TWITTER, PAYPAL, TWITTER, SPOTIFY, AMAZON, SOUNDCLOUD Y NETFLIX, QUE DEJÓ INACCESIBLES GRANDES PLATAFORMAS Y SERVICIOS DE INTERNET A GRAN CANTIDAD DE USUARIOS DE EUROPA Y NORTE AMÉRICA.

FUE UN ATAQUE MASIVO A LA INFRAESTRUCTURA BASE DE INTERNET, UTILIZANDO MILLONES DE DISPOSITIVOS IOT PARA EJECUTARLO. EL GRUPO NEW WORLD HACKERS SE DECLARÓ RESPONSABLE DEL ATAQUE. SE ESPECULA QUE FUE UN ATAQUE PARA ESTUDIAR, DE FORMA MALICIOSA, EL NIVEL DE VULNERABILIDAD DE LA INFRAESTRUCTURA MÁS FUNDAMENTAL DE INTERNET. (Colarebointernacional, 2016)

El 'hackeo' a Yahoo
La revista Expansión en alianza con CNN publicó
NUEVA YORK (CNNMONEY) - LOS EXPERTOS EN SEGURIDAD DICEN QUE LA INFILTRACIÓN EN LA CUENTA DE YAHOO ES "MASIVA".

YAHOO CONFIRMÓ EL JUEVES 22 DE SEPTIEMBRE QUE LES HABÍAN ROBADO MÁS DE 500 MILLONES DE CUENTAS DE SUS USUARIOS EN UNA INFILTRACIÓN OCURRIDA A FINALES DE 2014.

LOS EXPERTOS CREEN QUE PODRÍA SER EL HACKEO MÁS GRANDE DE LA HISTORIA.
PARA TENER UN PUNTO DE COMPARACIÓN, EL HACKEO A LINKEDIN OCURRIDO EN 2012 AFECTÓ A 117 MILLONES DE CUENTAS Y HACE UNOS MESES SE ANUNCIÓ QUE 360 MILLONES DE CUENTAS DE MYSPACE HABÍAN QUEDADO COMPROMETIDAS.

EN LA INFORMACIÓN QUE SE OBTUVO EN EL HACKEO A YAHOO PODRÍA HABER NOMBRES, DIRECCIONES DE CORREO ELECTRÓNICO, NÚMEROS TELEFÓNICOS, FECHAS DE NACIMIENTO Y, EN ALGUNOS CASOS, PREGUNTAS DE SEGURIDAD CIFRADAS O NO CIFRADAS CON SUS RESPUESTAS, SEGÚN UN COMUNICADO DE YAHOO.

SEGÚN PER THORSHEIM, ASESOR EN SEGURIDAD CIBERNÉTICA QUE TRABAJA EN NORUEGA, EL HACKEO "TENDRÁ REPERCUSIONES EN LA RED DURANTE VARIOS AÑOS". (CNN, 2014)

Hackearon página del SAT; Anonymous se adjudica el ataque

21 de marzo de 2016

CIUDAD DE MÉXICO.- DESPUÉS DE ESTAR FUERA POR ALREDEDOR DE DOS HORAS Y MEDIA, ESTE LUNES LA PÁGINA WEB DEL SERVICIO DE ADMINISTRACIÓN TRIBUTARIA (SAT) QUEDÓ RESTABLECIDA EN SU SERVICIO A LOS USUARIOS.

Y ES QUE PASADA LA 1:00PM EL SAT REPORTÓ FALLAS PARA INGRESAR A SU PORTAL, Y USUARIOS PREGUNTARON SOBRE EL RESTABLECIMIENTO DEL SISTEMA DE SU PÁGINA.

EL GRUPO ANONYMOUS MÉXICO SE HABÍA ADJUDICADO EL HACKEO Y EN UN BREVE COMUNICADO SEÑALÓ QUE LO HABÍA HECHO PARA REAFIRMAR QUE SU ORGANIZACIÓN "SIGUE MÁS FUERTE QUE NUNCA". (México, 2016)

Hackean a la actriz Scarlett Johansson

1 de junio de 2016

El portal de Excelsior publicó el hackeo a la cuenta de correo de la actriz Scarlett Johanson.

ANOCHE EL NOMBRE DE SCARLETT JOHANSSON SE VOLVIÓ TENDENCIA EN TWITTER, POR UNA SENCILLA RAZÓN: NUEVAMENTE SE FILTRARON FOTOS DE ELLA TOTALMENTE DESNUDA.

DE MANERA INMEDIATA LAS IMÁGENES SE PROPAGARON POR LA RED EN DONDE SE PUEDE VER A LA ACTRIZ NEOYORQUINA DE 31 AÑOS RECOSTADA EN UN CAMA Y TOMÁNDOSE FOTOS MUY AL NATURAL, APENAS ENSEÑANDO EL "PUBIS ANGELICAL", COMO LO DEFINIERA EL DESAPARECIDO ESCRITOR MANUEL PUIG EN SU NOVELA HOMÓNIMA DE 1979.

ESTA ES LA SEGUNDA OCASIÓN EN QUE LA DESINHIBIDA RUBIA SUFRE DE ATAQUES CIBERNÉTICOS, YA QUE EN 2011 TAMBIÉN FUE VÍCTIMA DE LA FILTRACIÓN DE COMPROMETEDORAS IMÁGENES POR PARTE DEL HACKER CHRISTOPHER CHANE, ACTUALMENTE CONDENADO A 10 AÑOS DE PRISIÓN POR INVADIR Y DIFUNDIR LA PRIVACIDAD DE LA ARTISTA.

ESA VEZ EL PIRATA INFORMÁTICO INGRESÓ A LAS CUENTAS DE CORREO DE JOHANSSON Y VIRALIZÓ EN INTERNET SUS FOTOS SIN ROPA, COMO TAMBIÉN LO HIZO CON OTRAS FAMOSAS DEL CALIBRE DE CHRISTINA AGUILERA Y MILA KUNIS. (Excelsior, 2016)

Estos ciberataques en México de acuerdo al portal web "El Economista" han costado 24 millones de dólares al año:

AL AÑO, MÉXICO PIERDE ALREDEDOR DE 24 MILLONES DE DÓLARES DERIVADO DE CIBERATAQUES, ESTIMÓ GUADALUPE DE LA TORRE, DIRECTORA DE DAÑOS DE LOCKTON MÉXICO.

AL AÑO, MÉXICO PIERDE ALREDEDOR DE 24 MILLONES DE DÓLARES DERIVADO DE CIBERATAQUES, ESTIMÓ GUADALUPE DE LA TORRE, DIRECTORA DE DAÑOS DE LOCKTON MÉXICO.

BRASIL, MÉXICO Y COLOMBIA SON LOS PAÍSES MÁS AFECTADOS POR ESTOS DELITOS CIBERNÉTICOS, AÑADIÓ.

POR LO ANTERIOR, ES DE GRAN IMPORTANCIA QUE LAS EMPRESAS COMIENCEN A PROTEGERSE Y BLINDARSE EN TODOS LOS PUNTOS DE VULNERABILIDAD QUE TIENEN.

MARCELA FLORES, DIRECTORA GENERAL PARA MÉXICO DE LOCKTON, DIJO QUE EL SECTOR FINANCIERO ES DE LOS MÁS VULNERABLES EN CUANTO A DELITOS CIBERNÉTICOS SE REFIERE; SIN EMBARGO, TAMBIÉN ES DE LOS QUE TRABAJA MÁS PARA BLINDARSE CONTRA ÉSTOS Y ASÍ DISMINUIR -EN LA MEDIDA DE LO POSIBLE- LAS PÉRDIDAS MONETARIAS.

KASPERSKY LAB, COMPAÑÍA DE SOFTWARE ANTIVIRUS, RECIENTEMENTE INFORMÓ QUE, DURANTE EL SEGUNDO TRIMESTRE DEL 2016, BLOQUEÓ MÁS DE 1 MILLÓN 132,000 ATAQUES DE MALWARE FINANCIERO; ESTA ACTIVIDAD TUVO UN AUMENTO DE 15.6% EN COMPARACIÓN CON EL PRIMER SEMESTRE DEL 2015.

LA EMPRESA ASEGURÓ QUE LAS AMENAZAS A LOS DISPOSITIVOS MÓVILES TAMBIÉN HAN AUMENTADO, PUES DURANTE EL SEGUNDO TRIMESTRE DEL AÑO PASARON DE 31.6 A 45.1 POR CIENTO.

DE ACUERDO CON GUADALUPE DE LA TORRE, EL RIESGO QUE PARA LAS EMPRESAS SIGNIFICA EL INTERNET PARA ESTÁ DENTRO DE LAS NUEVAS TENDENCIAS EN RIESGOS DE LAS LÍNEAS FINANCIERAS DE LAS ASEGURADORAS (DISEÑADAS PARA PROTEGER LAS COMPAÑÍAS DE RIESGOS FINANCIEROS QUE PUEDEN DERIVAR EN DEMANDAS Y PÉRDIDAS MONETARIAS ALTAS).

DESTACÓ QUE EL MERCADO DE LÍNEAS FINANCIERAS EN MÉXICO TIENE UN VALOR DE 50 MILLONES DE DÓLARES EN PÓLIZAS Y SE ESPERA UN CRECIMIENTO PARA ESTE AÑO DE 20 POR CIENTO.

DESDE EL 2010, ENTRÓ EN VIGOR LA LEY DE PROTECCIÓN DE DATOS QUE OBLIGA A LAS EMPRESAS A ESTAR AMPARADAS PARA PODER RESPONDER ANTE AFECTACIONES OCASIONADAS POR CIBERATAQUES.

"SIN EMBARGO, NO TODAS LAS EMPRESAS ESTÁN PREPARADAS PARA ESTOS MECANISMOS, POR LO QUE AÚN HAY COMPAÑÍAS QUE ESTÁN ENFRENTÁNDOSE A MULTAS Y A DEMANDAS IMPORTANTES QUE DEBEN CUBRIR SI EXISTE UNA VULNERABILIDAD DE DATOS. ES IMPORTANTE QUE SE HAGA CONCIENCIA, PUES ESTA PRÁCTICA CONTINÚA AUMENTANDO", DIJO DE LA TORRE.

OTRO SECTOR QUE ES AFECTADO CONSTANTEMENTE, ASEGURÓ MARCELA FLORES, SON LAS EMPRESAS FAMILIARES, PUES ÉSTAS MUCHAS VECES NO CUENTAN CON LA INFORMACIÓN O RECURSOS NECESARIOS. (Economista, 2016)

La empresa Symantec a través de su portal web publicó un informe sobre amenazas a la seguridad en Internet 2016.

EN EL 2015, SYMANTEC DETECTÓ MÁS DE 430 MILLONES DE EJEMPLOS NUEVOS Y DIFERENTES DE SOFTWARE MALICIOSO. ESTE NÚMERO NO NOS SORPRENDE. LOS ATAQUES CONTRA EMPRESAS Y NACIONES APARECEN EN LAS NOTICIAS TAN A MENUDO QUE NOS HEMOS ACOSTUMBRADO TANTO A LA GRAN CANTIDAD COMO A LA VELOCIDAD DE LAS CIBERAMENAZAS. LA MAYORÍA DE LOS INFORMES SOBRE AMENAZAS SOLO TRATAN SUPERFICIALMENTE EL PANORAMA DE AMENAZAS, PERO LA GRAN CANTIDAD DE DATOS DE SYMANTEC PERMITE AL INFORME SOBRE AMENAZAS A LA SEGURIDAD EN INTERNET ANALIZAR DIVERSOS FACTORES, COMO LAS TÁCTICAS DEL ATACANTE, LOS MOTIVOS Y LOS COMPORTAMIENTOS. A CONTINUACIÓN, SE PRESENTAN SEIS CONCLUSIONES Y TENDENCIAS CLAVE DE 2015.

CONCLUSIONES CLAVE:

- SE DETECTÓ, EN PROMEDIO, UNA VULNERABILIDAD DE DÍA CERO POR SEMANA. LOS ATACANTES AVANZADOS SIGUEN APROVECHANDO LAS FALLAS EN LOS NAVEGADORES Y LOS PLUGINS DE SITIOS WEB.
- SE PERDIERON O ROBARON QUINIENTOS MILLONES DE INFORMES PERSONALES. CADA VEZ MENOS EMPRESAS ELABORAN INFORMES SOBRE EL ALCANCE TOTAL DE LAS FUGAS DE DATOS.
- LAS VULNERABILIDADES DE SEGURIDAD MÁS IMPORTANTES EN EL 75 % DE LOS SITIOS WEB MÁS POPULARES NOS PONEN A TODOS EN PELIGRO. LOS ADMINISTRADORES WEB TODAVÍA TIENEN DIFICULTADES PARA MANTENER LA VIGENCIA DE LOS PARCHES.
- LAS CAMPAÑAS SOBRE SPEAR-PHISHING DESTINADAS A EMPLEADOS AUMENTARON UN 55 %. LOS CIBERATACANTES APUNTAN A LOS DATOS DE LAS GRANDES EMPRESAS EN EL LARGO PLAZO.
- EL RANSOMWARE AUMENTÓ UN 35 %. LOS CIBERCRIMINALES USAN EL CIFRADO COMO ARMA PARA RETENER DATOS CRÍTICOS DE LAS EMPRESAS Y LAS PERSONAS.
- SE BLOQUEARON CIEN MILLONES DE SERVICIOS DE SOPORTE TÉCNICO FALSOS. AHORA, LOS CIBERESTAFADORES LO ENGAÑAN PARA QUE LOS LLAME Y LES ENTREGUE SU DINERO. (Symantec, 2016)

Como hemos visto a través de estos ejemplos cualquier institución, empresa y usuario del Internet esta propenso a una amenaza cibernética en donde los **"Ciberdelincuentes"** en cada instante están realizando ataques a la vulnerabilidad de los **"Cibernautas"** es por ello, que debemos extremar la seguridad en la infraestructura de nuestra empresa, escuela o incluso de nuestros equipos personales teniendo actualizado nuestro

software y sobre todo contar con alguna herramienta para mitigar ataques como pueden ser los "Antivirus".

En México como en todo el mundo se han preocupado por tener Centro Nacional de Respuesta a Incidentes Cibernéticos (CERT-MX), construidos con la finalidad de prevenir y mitigar amenazas y ataques cibernéticos.
A continuación mostraremos en América Latina que países cuentan con estos Centros de Respuesta a Incidentes Cibernéticos.

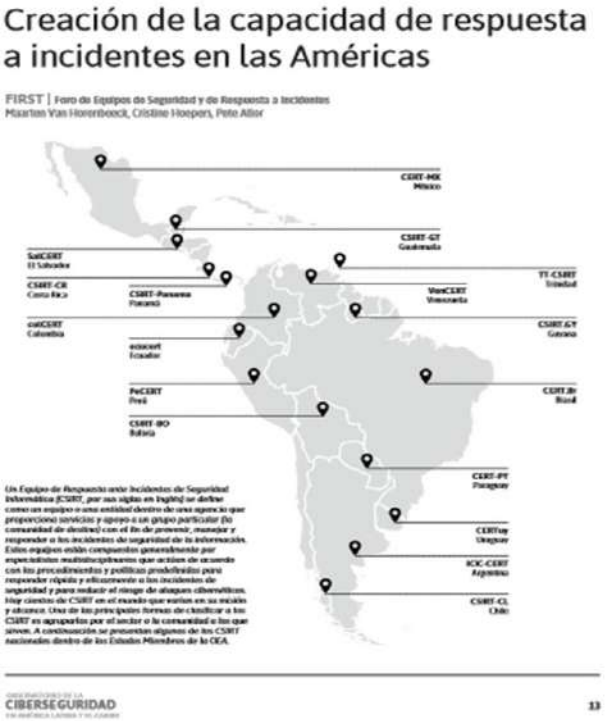

Figura 2. Creación de la Capacidad a incidentes en las Américas. (Ciberseguridad, 2016)

CONCLUSIONES

El **"Ciberespacio"** se ha convertido en un gran nicho de oportunidades para la construcción de negocios que permite difundir sus productos y/o servicios a bajo costos, hoy en día las empresas grandes o pequeñas, asi como, los usuarios, deben invertir dinero en hardware y software de **"Ciberseguridad"**, ya que esto le permitirá prevenir o mitigar las **"Amenazas Cibernéticas"** a las que están expuestas.

Así como, conocer las instituciones creadas para apoyar y mitigar estas amenazas a través de comunicados o boletines de medidas de seguridad, como también las empresas encargadas en este rubro, conocer la normatividad y legislación vigente para no caer en trampas de la **"Ciberdelincuencia"**

Como ya hemos visto a lo largo de este artículo las **"Amenazas Cibernéticas"** segundo a segundo tratan de poner en riesgo los bienes informáticos, a través de los diferentes modelos de comunicación de los **"cibernautas"** y empresas, por lo que estos deben de tomar muy en serio las recomendaciones de los expertos, y aprender de cómo se han perpetrado los ataques por parte de estos **"Ciberdelincuentes"** para no caer en estas **"Amenazas Cibernéticas".**

REFERENCIAS

AMIPCI. (2015). *"COMERCIO ELECTRÓNICO"*. Recuperado el OCTUBRE de 2016, de https://amipci.org.mx/estudios/comercio_electronico/Estudio_de_Comercio_Electronico_AMIPCI_2015_version_publica.pdf

Ciberseguridad, O. d. (2016). *Ciberseguridad ¿Estamos preparados en América Latina y el caribe?*. Recuperado el Octubre de 2016

CNN, E. e. (Septiembre de 2014). *El 'hackeo' a Yahoo tendrá repercusiones durante años: expertos.* Recuperado el Octubre de 2016, de http://expansion.mx/tecnologia/2016/09/23/el-hackeo-a-yahoo-tendra-repercusiones-durante-anos-expertos

Colarebointernacional. (Octubre de 2016). *¿Qué es un ataque de denegación de servicio?.* Recuperado el Octubre de 2016, de https://colarebointernacional.wordpress.com/2016/10/22/que-es-un-ataque-de-denegacion-de-servicio/

CONDUSEF. (12 de OCTUBRE de 2016). *PROTEJA SU DINERO.* Obtenido de http://www.condusef.gob.mx/Revista/index.php/usuario-inteligente/consejos-de-seguridad/563-robo-de-identidad

Economista, E. (Agosto de 2016). *Ciberataques en México cuestan 24 millones de dólares al año: Lockton.* Recuperado el Octubre de 2016, de http://eleconomista.com.mx/finanzas-publicas/2016/08/18/ciberataques-mexico-cuestan-24-millones-dolares-ano-lockton

Excelsior. (Junio de 2016). *De nuevo hackean fotos de Scarlett Johansson al desnudo.* Recuperado el Octubre de 2016, de http://www.excelsior.com.mx/funcion/2016/06/01/1096106

ITU, U. I. (Noviembre de 2010). *Unión Internacional de Telecomunicaciones.* Recuperado el 10 de Octubre de 2016, de http://www.itu.int/net/itunews/issues/2010/09/20-es.aspx

Merca2.0. (13 de Mayo de 2014). *5 amenazas que acechan en los videojuegos.* Recuperado el Octubre de 2016, de http://www.merca20.com/5-amenazas-sobre-los-juegos-online/