UNIVERSIDAD DE XALAPA

Instituto Interdisciplinario de Investigaciones

Xalapa, Ver; 25 de enero de 2018
Asunto: El que se indica

A QUIEN CORRESPONDA
P R E S E N T E

El suscrito, Rector de la Universidad de Xalapa, me dirijo a usted(es) para hacer constar lo siguiente:

Los libros que se publican bajo el sello editorial de la Universidad de Xalapa, a través de su Instituto Interdisciplinario de Investigaciones, cursan por una rigurosa etapa previa de revisión, a cargo de la comisión dictaminadora de esta casa de estudios, la cual se integra por subcomisiones especializadas en las diferentes áreas del conocimiento, emitiendo un dictamen que puede ser favorable para publicación, recomendación para posterior publicación y no favorable.

La obra presentada para su dictamen y eventual publicación, por parte de los **Doctores Carlos Hernández Rodríguez y Raúl Manuel Arano Chávez** titulada **"10 Temas de Ciberseguridad"**, previa revisión y arbitraje de la comisión dictaminadora, de todos y cada uno de los capítulos que la integran y al encontrase que reunía los requisitos de fondo y forma exigidos para este tipo de publicaciones, decidió emitir el **dictamen favorable** para su publicación, tanto en lo general como en lo individual (capítulos del libro) por lo que dicha obra fue publicada bajo el sello editorial de la Universidad de Xalapa, a través de su Instituto Interdisciplinario de Investigaciones, en enero de 2017, con número de registro **ISBN 978-607-8156-55-9**, pudiéndose encontrar su versión digital en la página www.ux.edu.mx.

Sin más por el momento, se extiende la presente constancia para los fines legales y académicos a los que haya lugar.

ATENTAMENTE

Dr. Carlos García Méndez
RECTOR DE LA UNIVERSIDAD DE XALAPA

Kilómetro 2 de la Carretera Federal Xalapa-Veracruz,
Fraccionamiento Ánimas, C.P. 91190, Edificio Cedro, Tercer piso.
Tel.- (01) 228 841-72-85 Ext. 7256 drcarlosazuara@hotmail.com
www.facebook.com/III.UX www.ux.edu.mx

Autores

Alberto Brandon Báez Camarena
Antonio Berdeja Rivas
Carlos Antonio Vázquez Azuara
Carlos Hernández Rodríguez
Carlos Iván Téllez Gutiérrez
Daniel Armando Olivera Gómez
Daniel Reyna Ramos
Ignacio Olivares Linares
Jesús Escudero Macluf
José Martín Cadena Barajas
Karina Aurora Ybarra Martínez
Luis Alberto Delfín Beltrán
Milagros Cano Flores
Oliver González Barrales
Raúl De La Fuente Izaguirre
Raúl Manuel Arano Chávez
René Montero Montano
Teresa García López

ISBN: 978-607-8156-55-9

10 Temas de Ciberseguridad

10 Temas de Ciberseguridad

COORDINADORES

Carlos Hernández Rodríguez
Raúl Manuel Arano Chávez

10 Temas de Ciberseguridad

COORDINADORES

Carlos Hernández Rodríguez
Raúl Manuel Arano Chávez

Editorial Universidad de Xalapa, en coordinación con su Instituto Interdisciplinario de Investigaciones

Xalapa, Veracruz, México, 2017

UNIVERSIDAD DE XALAPA
Saber / Trascender

INSTITUTO INTERDISCIPLINARIO DE INVESTIGACIONES
Universidad de Xalapa

Primera Edición

El tiraje de esta obra, se realizó bajo el sello editorial de la Universidad de Xalapa A.C., a través de su Instituto Interdisciplinario de Investigaciones, en enero de 2017, constó de 1000 ejemplares, oficinas en Km. 2 Carretera Xalapa-Veracruz, C.P. 91190. Xalapa, Veracruz, México.

ISBN: 978-607-8156-55-9

Portada y diseño editorial:
Dr. Carlos Antonio Vázquez Azuara

OBRA CONMEMORATIVA DE LOS VEINTICINCO AÑOS DE LA FUNDACIÓN DE LA UNIVERSIDAD DE XALAPA.

CONTENIDO

PRÓLOGO

Iniciamos la 4ta era de la revolución industrial en nuestro planeta. Esta etapa se vincula con nanotecnologías, inteligencia artificial, drones e impresoras 4D.

En 1760, surgió la primera revolución industrial, las máquinas facilitaron la vida a las personas. Su expresión permitió, no tan solo la rapidez en la ejecución de acciones, sino además la multiplicidad de los operadores en otras actividades.

Para 1860, el mundo vivía la segunda revolución industrial que se caracterizó por la producción en cadena. Derivó en productos homologados. Incremento las plazas para trabajadores y por ende, el crecimiento de la industria.

Gran fortuna se tuvo en el siglo XX, ya que la tercera revolución industrial se ubicó como un cambio no sólo en la industria, sino en toda la actividad humana. Y esto sucedió, tan sólo hace 37 años de nuestra época actual, al aparecer los ordenadores portátiles.

Y así llegamos a la cuarta era. Que se distingue por un cúmulo de información a través de internet. Se rompieron las barreras del conocimiento. La globalización se materializó con gran fuerza. Pero, sobre todo, se creó un nuevo mundo: el ciberespacio. Así dentro de un entorno virtual se generan todas las actividades de nuestro planeta.

Se revela que existen tan solo en México 70 millones de usuarios conectados. Más de 50% de la población en nuestro país.

Y a nivel mundial, hay un alza del PIB del 0.5 que se afirma, fue resultado del crecimiento en las conexiones por internet. El alza de usuarios, no es solo en países europeos, ya que en regiones africanas aún con grandes retos, se manifiesta un aumento continuo de cibernautas.

El ciberespacio es considerado acorde a Neil Postman como "… una idea metafórica que se supone que es el espacio en el que se encuentra su conciencia cuando se está utilizando la tecnología informática a través del internet…".

Los cibernautas también son llamados ciberciudadanos. Y las actividades que en la red se desarrollan abarcan todos los ámbitos del quehacer humano: educación, cultura, arte, ciencia, sociedad, gobierno, historia, tecnología, pero principalmente negocios comerciales.

Aunado a esto, surgieron nuevos términos. Un lenguaje con códigos específicos que expresan las reglas del cibermundo.

Sin embargo, esta creciente comunidad, también es un espacio para las actividades que conllevan conductas antisociales. Entendiendo por estas a las que generan un daño. Y este daño se constituye en ciberdelito, cuando tiene un tipo que lo delimita.

Así, por la propia naturaleza humana, a la par del desarrollo tecnológico tan útil y trascendente se genera la anti versión de la conducta ideal en el ser… la que daña y lastima no tan solo a un sujeto, si no al mismo tejido social.

Es incuestionable entonces que, así como la conducta criminal se estudia como un fenómeno integral, los incidentes en el cibermundo deben ser muy puntualmente observados.

De tal forma que, considerando la tricotomía del actuar negativo en el ciberespacio, se conciben los siguientes elementos para su mayor comprensión:

a) La persona afectada
b) Quien la afecta y;
c) El resultado de esa afectación.

Dentro de la tricotomía ciberdelictiva, sería clave incluir un cuarto elemento: el contexto.

El escenario o contexto, contendría no solo la caracterización del fenómeno, sino además la descripción completa del mismo. Esto apoyaría con certeza, el estudio integral del ciberdelito.

Situación que derivaría, en un proceso de investigación eficiente, eficaz y oportuna. Dando un matiz multidimensional a la investigación del ciberdelito. Lo anterior, propiciaría la generación no tan solo de líneas de generación de conocimiento, sino propuestas precautorias efectivas y eficaces como basamentos para la ciberseguridad.

Los habitantes de esta era, somos afortunados. Y más aún, cuando una institución educativa como la Universidad de Xalapa asume un compromiso de calidad en la educación y realiza un esfuerzo al producir esta obra, que es garantía de calidad.

Se afirma calidad, dado que el estar tenazmente vinculada con la realidad y los esquemas de trabajo delineados tanto en el Plan

Nacional de Desarrollo 2013-2018, como en el Programa Nacional de Seguridad 2014-2018, se alinean con especial atingencia con respecto al ciberdelito y a la ciberseguridad.

Por lo antes expuesto se expresa: el mundo del ciberespacio si bien es virtual, representa hoy el contexto más amplio, plural y globalizado del quehacer humano.

No hay esfera de nuestra actual vida, que sea ausente o exceptúe el ámbito del cibermundo.

Es poco probable que en el futuro no se rescate, el gran esfuerzo que representa la actitud del ciberciudadano con respecto a la ciberseguridad y a la tipología ciberdelictiva que hoy en día es un reto a la imaginación y talento legislativo.

Y difícil es pensar, al mismo tiempo, que exista un alto o retroceso a la evolución que en materia de ésta área se genera con gran rapidez día a día.

Lo que significa que, la Ciberseguridad desde un entorno empresarial, jurídico y tecnológico sea un tema obligado y de total importancia para el desarrollo de cualquier profesional.

Por lo antes expuesto se felicita a la Universidad de Xalapa por estar siempre a la vanguardia. Su compromiso resalta cuando al apropiarse de los conceptos básicos contenidos dentro de la Estrategia Digital Nacional resuma en tres palabras: Compartir, Consolidar y Proteger, la intención de esta magnífica obra conlleva, de tal forma que:

- Comparta: conocimientos.
- Consolide: destrezas y;

- Proteja con este fabuloso texto al entorno, a través de propiciar el desarrollo de nuevas capacidades y competencias, que sean aplicables positiva y eficazmente.

Por ello celebro y afirmo una vez más, que la Universidad de Xalapa sin duda, propiciará con este legado escrito que quien lea sus valiosos contenidos se enriquezca y promueva su muy digno lema: Saber/Trascender.

Patricia Rosa Linda Trujillo Mariel

DEVICE LOCK, UNA ALTERNATIVA A LA SEGURIDAD INFORMATICA EN EL ORGANO DE FISCALIZACIÓN SUPERIOR PERIODO 2013-2015

Raúl De La Fuente Izaguirre*
José Martín Cadena Barajas&

INTRODUCCIÓN

La administración pública es la actividad que se desarrolla en el organismo del estado para el cumplimiento de los fines del mismo. Los organismos adscritos tienen una relación de dependencia con un nivel central siendo las tecnologías de la información y comunicación (Tic's) un canal por medio del cual existe esa comunicación convirtiéndose la información en un activo muy importante para ambos.

Según (Chiavenato, 2006) el concepto de información representa mensaje con significado en un determinado contexto, disponible para uso inmediato y que proporciona orientación a las acciones por el hecho de reducir el margen de incertidumbre con respecto a nuestras decisiones

Para (Ferrel & Hirt, 2004), la información comprende los datos y conocimientos que se usan en la toma de decisiones.

Desde la perspectiva de (Czinkota & Masaaki, 2001) la información consiste en datos seleccionados y ordenados con un propósito específico.

* Maestro en Tecnologías de la Información. Ingeniero en Sistemas Computacionales. radelafuente@uv.mx
& Maestro en Matemáticas. Licenciado en Matemáticas. jcadena@orfis.gob.mx

Desde un punto de vista informático la definición un dato es la unidad mínima de información, pero para (Toffler & Toffler, 2006) la diferencia radica en:

> Los datos suelen ser descritos como elementos discretos, huérfanos de contexto: por ejemplo, 300 acciones. Cuando los datos son contextualizados, se convierten en información: por ejemplo, tenemos 300 acciones de la empresa farmacéutica X.

Una de las principales problemáticas que enfrentan todas las organizaciones sean públicas o privadas es la administración de la seguridad de la información que viaja desde una red de área local (LAN) o bien tiene salida por medio de la Internet, desde una postura personal la seguridad de esta información es entendida como una ausencia de peligro o riesgo en la organización. Ante tal situación las Tic's son una pieza fundamental para evitar posibles amenazas hacia el principal activo de las instituciones.

Castells (1996) define a las Tic´s como el conjunto convergente de tecnologías de la microelectrónica, la informática, las telecomunicaciones, televisión, radio y la optoelectrónica.

Ávila (2007) define el concepto de internet como uno de los servicios principales y de más uso a nivel empresarial, el cual consiste de un conjunto de redes interconectadas a escala mundial con la particularidad de que cada una de ellas es independiente y autónoma.

Existen múltiples herramientas de tecnología que apoyan en la seguridad informática de la información, las cuales las podemos atacar desde cuestiones elementales como una configuración a los registro del sistema operativo, de manera física

desconectando componentes de la unidad centra de proceso (CPU) o de manera automatizada y remota vía una LAN o mediante servicios a través de internet, que no es otra cosa que la denominada nube informática.

EL ORFIS Y LA SEGURIDAD INFORMÁTICA

El Órgano de Fiscalización Superior es un organismo autónomo del Estado dotado de personalidad jurídica y patrimonio propios, autonomía técnica, presupuestal y de gestión, que apoya al Congreso en el desempeño de su función de fiscalización superior, y tiene la competencia que le confieren la Constitución Política de los Estados Unidos Mexicanos, la Constitución Política del Estado, la Ley de Fiscalización Superior y Rendición de Cuentas para el Estado y demás legislación aplicable (Orfis, 2016).

La visión del ORFIS es la consolidación de la imagen institucional con una dinámica estable y técnicamente fortalecida, que convalide la confianza de la Población y de los Entes Fiscalizables en los procesos y resultados de las auditorías, así como en las acciones posteriores que impactan favorablemente en la gestión pública. Su misión es hacer de la Fiscalización Superior el instrumento eficaz que estimule el control, la transparencia y la rendición de cuentas en los Entes Fiscalizables, dando cumplimiento al mandato legal que da origen a nuestra Institución (Orfis, 2016).

Además de contar con su política de integridad la cual garantiza la más alta probidad y confiabilidad en las funciones que desarrollan, dentro y fuera de la Institución, el personal del Órgano de Fiscalización Superior del Estado de Veracruz (ORFIS), deberá conducirse con independencia, objetividad y rigor técnico, enalteciendo la honestidad, la ética y el profesionalismo, debiendo ser intachables en el desempeño de su trabajo y preservar la transparencia de los asuntos que tienen bajo su encargo (Orfis, 2016).

El desarrollo tecnológico proporciona herramientas eficaces y seguras para la difusión de información, por lo que es de suma importancia para el ORFIS, las ventajas que ofrece la tecnología para garantizar que tanto la comunicación al interior como al exterior, se vea favorecida con el avance en dicha materia. En este sentido, el ORFIS dispondrá de la tecnología para desarrollar los procedimientos idóneos que nos permitan interactuar eficaz y oportunamente; primeramente al interior en el desarrollo de nuestras funciones, así como al exterior para lograr el cometido. Es por ello que en su plan estratégico 2012 -2019 señala los siguientes objetivos:

- Rediseñar e innovar la página web del ORFIS.
- Desarrollar una red interna de comunicación e información para las Unidades Administrativas del ORFIS. (Intranet)
- Implementar un "Sistema de Consulta Telefónica a Entes Fiscalizables", con registro de atención por Unidad Administrativa, mediante conmutador.
- Fomentar el uso de las tecnologías de información por parte de los Entes Fiscalizables para la transparencia y difusión de la información financiera.

El ORFIS se ha apoyado en la tecnología para desarrollar los procedimientos que permitan interactuar eficaz y oportunamente; para lograr el cometido de brindar seguridad en la información.

La seguridad informática mejora el sistema de información y el flujo de información de una organización. Los servicios están dirigidos a evitar los ataques de seguridad y utilizan uno o más

mecanismos de seguridad para proveer el servicio (UNAM, 2016).

La clasificación de la seguridad informática según la (UNAM, 2016) es:

- Confidencialidad
    - Servicio de seguridad o condición que asegura que la información no pueda estar disponible o ser descubierta por o para personas, entidades o procesos no autorizados. También puede verse como la capacidad del sistema para evitar que personas no autorizadas puedan acceder a la información almacenada en él.

    - La confidencialidad es importante porque la consecuencia del descubrimiento no autorizado puede ser desastrosa. Los servicios de confidencialidad proveen protección de los recursos y de la información en términos del almacenamiento y de la información, para asegurarse que nadie pueda leer, copiar, descubrir o modificar la información sin autorización. Así como interceptar las

comunicaciones o los mensajes entre entidades.

- Autenticación
    - Es el servicio que trata de asegurar que una comunicación sea auténtica, es decir, verificar que el origen de los datos es el correcto, quién los envió y cuándo fueron enviados y recibidos también sean correctos.
- Integridad
    - Servicio de seguridad que garantiza que la información sea modificada, incluyendo su creación y borrado, sólo por el personal autorizado.
    - El sistema no debe modificar o corromper la información que almacene, o permitir que alguien no autorizado lo haga. El problema de la integridad no sólo se refiere a modificaciones intencionadas, sino también a cambios accidentales.
- No repudio
    - El no repudio sirve a los emisores o a los receptores para negar un mensaje transmitido. Por lo que cuando un mensaje es enviado, el receptor puede probar que el mensaje fue enviado por el presunto

emisor. De manera similar, cuando un mensaje es recibido, el remitente puede probar que el mensaje fue recibido por el presunto receptor.

- Control de acceso
    - Un control de acceso se ejecuta con el fin de que un usuario sea identificado y autenticado de manera exitosa para que entonces le sea permitido el acceso.

    - Los componentes básicos de un mecanismo de control de acceso son las entidades de red, los recursos de la red y los derechos de acceso. Estos últimos describen los privilegios de la entidad o los permisos con base en qué condiciones las entidades pueden tener acceso a un recurso de la red y cómo estas entidades son permitidas para tener acceso a un recurso de la red.

    - El control de acceso puede ejecutarse de acuerdo con los niveles de seguridad y puede ejecutarse mediante la administración de la red o por una entidad individual de

acuerdo con las políticas de control de acceso.

- Disponibilidad
    - En un entorno donde las comunicaciones juegan un papel importante es necesario asegurar que la red esté siempre disponible.
    - La disponibilidad es un servicio que garantiza que los usuarios autorizados tengan acceso a la información y a otros activos de información asociados en el lugar, momento y forma en que es requerido. Un sistema seguro debe mantener la información disponible para los usuarios. El sistema, tanto hardware como software, debe mantenerse funcionando eficientemente y ser capaz de recuperarse rápidamente en caso de fallo.

El uso de las Tecnologías de la Información y Comunicación (Tic's) representa radicalmente una forma en que los gobiernos administran y ejecutan sus procesos, abriendo la posibilidad de mejorar e incrementar los canales de comunicación entre los miembros de la organización o externos, es de vital importancia que no exista fuga de información y que cumplan cabalmente las características de la misma.

Las filtraciones de datos puede iniciarse por empleados sin querer o usuarios con malas intenciones, dedicados a la copia de información sensible o de propietario desde sus equipos a

unidades de memoria flash, smartphones, cámaras, PDA, DVD, CDROM, u otras formas viables de almacenamiento portátil. O bien, las filtraciones pueden deberse a correos electrónicos de usuarios, mensajería instantánea, formularios web, intercambios de redes sociales o sesiones telnet. Los puntos de intercambio inalámbrico como Wi-Fi, Bluetooth e infrarrojos, así como canales de sincronización de dispositivos, suponen riesgos adicionales de pérdida de datos. Del mismo modo, los equipos terminales pueden verse infectados con software dañino que aprovecha pulsaciones de teclado y envía los datos robados a través de canales SMTP o FTP para terminar en manos de criminales. Aunque algunas de estas vulnerabilidades pueden evadir soluciones de seguridad para redes y controles nativos de Windows (DeviceLock, 2016).

Está herramienta tecnológica permite el control de contenidos y contexto para la mayor prevención de filtraciones, su motor de intercepción e inspección de varias capas proporciona un control minucioso sobre una gran variedad de posibilidades de filtración de datos desde el nivel de contexto. Para mayor confianza en evitar la fuga de datos sensibles, es posible aplicar el filtrado y análisis de contenidos para seleccionar intercambios de datos de terminales con medios extraíbles y dispositivos punto a punto, así como dentro de la red. Resultando para el administrador del centro de cómputo la completa seguridad para ajustar con precisión los derechos de usuarios a cada rol por lo que respecta a la transferencia, recepción y almacenamiento de datos en equipos corporativos (DeviceLock, 2016).

La herramienta ofrece un enfoque sencillo sobre la gestión, que permite a los administradores de seguridad utilizar Objetos de directiva de grupos de Microsoft directorio activo y consolas remotas para la administración dinámica de agentes terminales distribuidos, e imponer directivas de dominio bien definidas de forma centralizada en sus equipos anfitrión.

La figura 1 representa la manera lógica en que trabaja herramienta, es decir la forma que opera la misma mediante red local y los agentes que intervienen en ella.

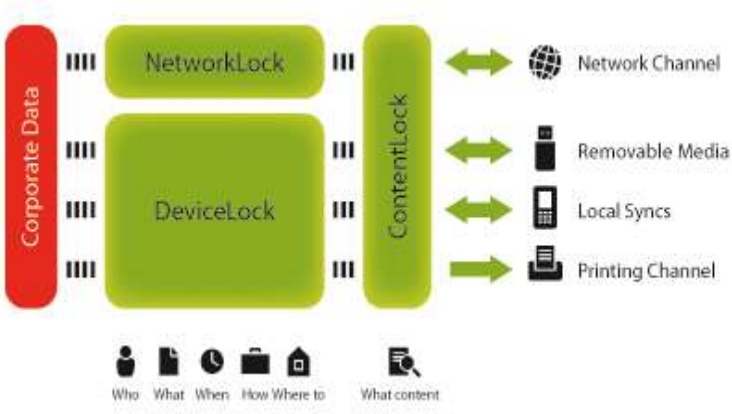

Figura 1
Fuente: http://www.devicelock.com/es/

La figura 2 describe cuales componentes son bloqueados por medio de DeviceLock asegurando así que se cumplan políticas de seguridad dentro de la organización, dichos elementos incluyen:

- Puertos USB
- Unidades Removibles
- Impresoras
- Tarjetas de Red Wifi
- Tecnología móvil.

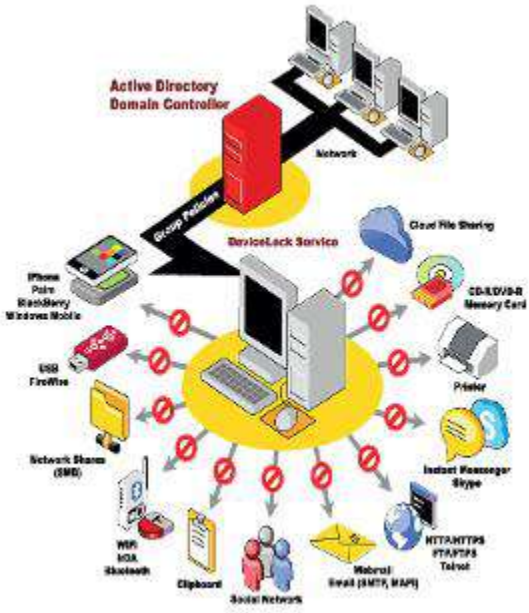

Figura 2
Fuente: http://www.devicelock.com/es/

Por lo antes mencionado el ORFIS opto por la implementación de dicho servicio tecnológico además que representa ventajas como:

- Control de acceso de dispositivos
- Control de comunicaciones de red.
- Filtrado de contenidos
- Protección de falsificación
- Integración con Active Directory
- True File Type Control
- Control del portapapeles
- Lista blanca USB
- Lista blanca de medios

- Lista blanca temporal
- Lista blanca de protocolos
- Auditoría
- Emulación

METODOLOGÍA

La metodología que se utilizó fue cualitativa, como indica su propia denominación, tiene como objetivo la descripción de las cualidades de un fenómeno. Adicionalmente se elaboraron figuras para la presentación y descripción de los resultados.

OBJETIVO GENERAL

Describir el uso de las Tic´s (DeviceLock) en proceso de seguridad informática en el Orfis durante el periodo 2013-2015.

RESULTADOS

Como antecedente a la seguridad informática en 2013, el ORFIS utilizaba la herramienta DeviceLock como parte de su protección y seguridad de la información, en esa fecha su uso era limitado, ya que se instalaba de manera independiente en cada equipo y no era administrada por una consola, además se bloqueaban puertos desde el bios de las computadoras limitando el uso de teclados y ratones usb (véase figura 3).

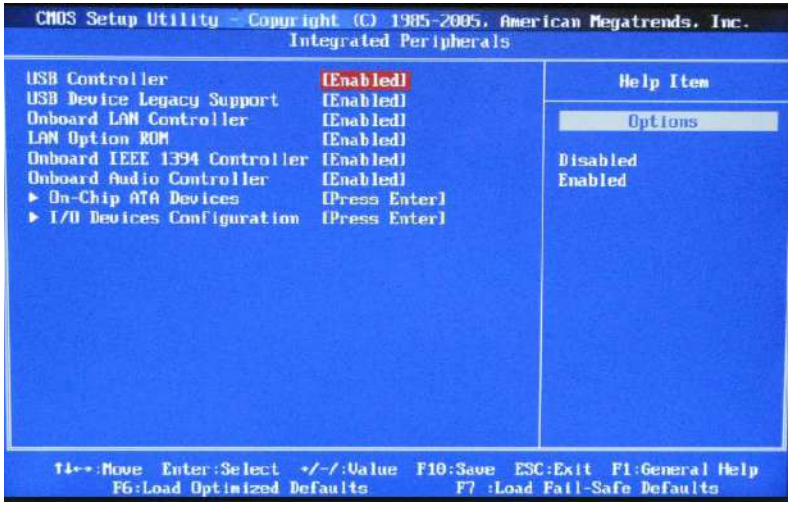

Figura 3
Fuente: Elaboración Propia

Otra herramienta que el ORFIS utilizó como parte de la seguridad informática era el antivirus, el cual fue administrado por 6 servidores instalados en distintas equipos de cómputo en el año 2013 y para el año 2015 se optimizo la administración de un solo servidor con 420 clientes (véase figura 4).

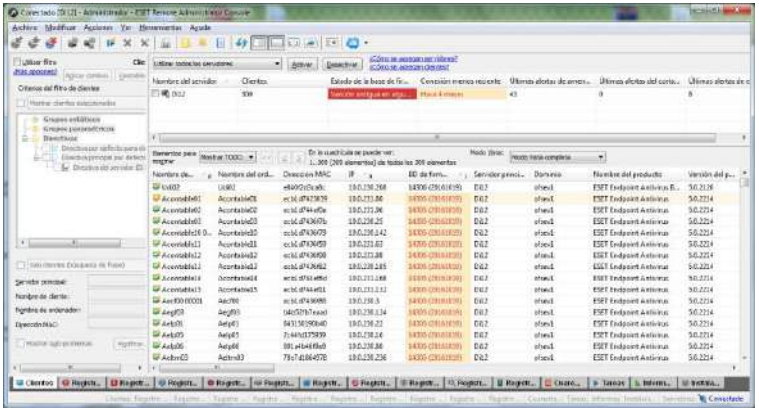

Figura 4
Fuente: Elaboración Propia

Para el año 2015 el ORFIS implementa la misma operación que se realizó con el antivirus con la herramienta DeviceLock la cual fue renovada y adquirida para 300 clientes, en su nueva implementación se incorporó al servidor principal del Directorio Activo de Windows y por medio del cual se realizan las operación de la seguridad informática, buscando que en todo momento dicha acción sea 100% transparente al usuario y no afecte sus actividades.

La figura 5 representa la consola de administración de DeviceLock, en la cual se busca a los equipos para bloquear determinados componentes.

La figura 6 indica los elementos que pueden ser bloqueados por el administrador de la herramienta de seguridad informática, así como el tipo de rol que cada usuario puede tener.

Figura 5
Fuente: Elaboración Propia

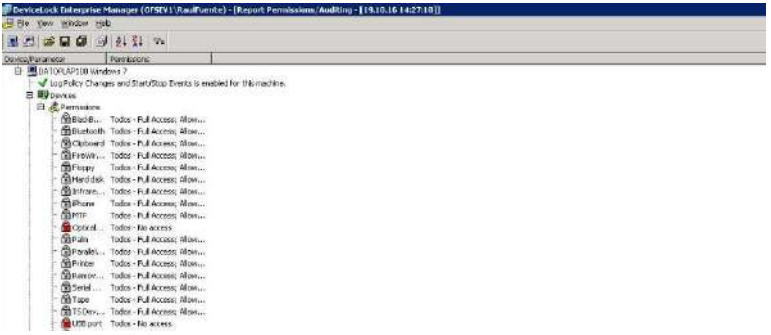

Figura 6
Fuente: Elaboración Propia

La figura 7 indica el permiso a cada uno de los usuarios, aunque esto podría considerarse repetitivo, bajo el esquema de red de dominio, cualquier usuario puede ocupar con su nickname y su contraseña un equipo de la organización. Por tal motivo se selecciona a quienes de estos se le aplica la política de seguridad.

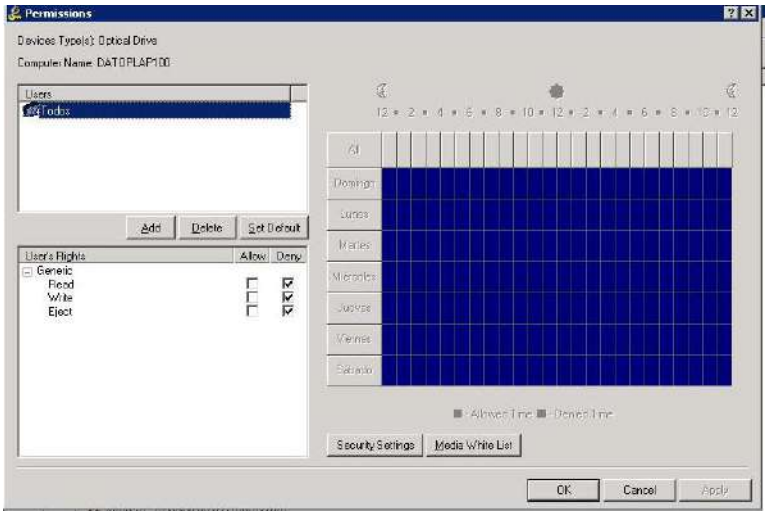

Figura 7
Fuente: Elaboración Propia

La figura 8 representa la posibilidad de permitir que dispositivos usb pueden utilizar los usuarios lo anterior porque en ocasiones hay dispositivos extraíbles que no representan una amenaza como el teclado, el ratón, etc.

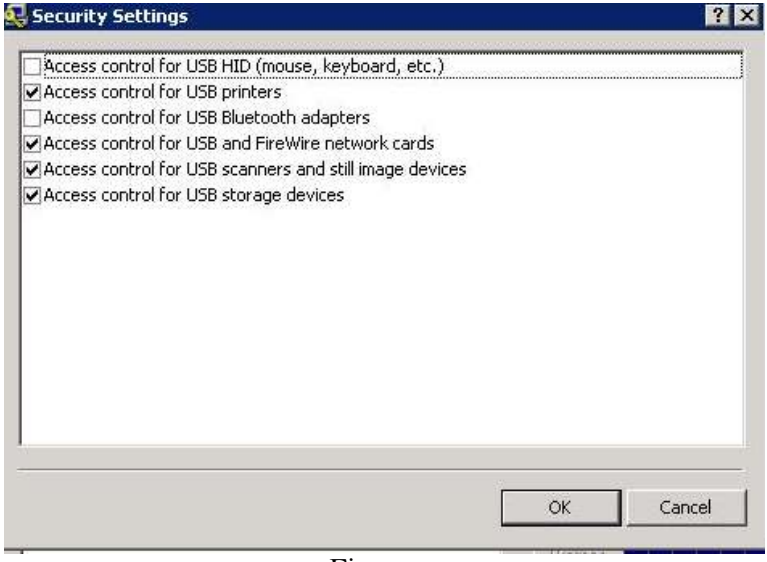

Figura 8
Fuente: Elaboración Propia

CONCLUSIONES

El Órgano de Fiscalización Superior (ORFIS) ha utilizado herramientas físicas tales como desconectar componentes del CPU y lógicas como lo ha sido el DeviceLock, el bloqueo por bios y modificación de registros del sistema operativo.
Los principales medios extraíbles que el ORFIS se ha preocupado por bloquear han sido los puertos USB, las unidades DVD y CD ROM así como también la tecnología móvil conectada al equipo de cómputo, lo anterior en un intento de salvaguardar la información de la organización.

La administración del antivirus es llevada a cabo por una sola persona, la cual es responsable de actualizar y verificar que las bases de datos de virus se encuentren al día para evitar que dichos fragmentos de código malicioso afecten la información y

se propaguen por la red, Actualmente se administran 420 clientes desde un solo servidor.
El 83% del equipo de cómputo del ORFIS tienen instaladas las seguridad informática por medio de políticas del DeviceLock y el 17% que no tiene instalada la herramienta de seguridad pertenece a la parte directiva de la institución.

Existe una diferencia entre el número total de clientes de antivirus y clientes de DeviceLock, lo anterior se debe a que todos los equipos de cómputo incluyendo la parte directiva y los servidores del site deben tener instalada la protección contra código malicioso.

De esta forma podemos concluir que las Tic's aunque no se apliquen de manera equivalente a todos los equipos de cómputo, las mismas benefician el proceso de seguridad informática

REFERENCIAS

Avila, A. (2007). *Iniciación a la red internet. Concepto, Servicios y Aplicaciones* . Vigo: IdeasPropias Ediciones.

Castells, M. (1996). *La Era de la Información. Economía Sociedad y Cultura.* Mexico: SigloXXI.

Chiavenato, I. (2006). *Introducción a la Teoría General de la Administración.* México: McGraw-Hill Interamericana.

Czinkota , M., & Masaaki, K. (2001). *Administración de Mercadotecnia.* International Thomson Editores.

DeviceLock. (19 de Octubre de 2016). *Seguridad y Control a Medios Extraibles* . Obtenido de http://www.devicelock.com/es/

Ferrel, O., & Hirt, G. (2004). *Introducción a los Negocios en un Mundo Cambiante.* México: McGraw-Hill Interamericana.

Orfis. (19 de Octubre de 2016). *Órgano de Fiscalización Superior del Estado de Veracruz.* Obtenido de http://orfis.gob.mx/orfis.html

Toffler, A., & Toffler, H. (2006). *La Revolución de la Riqueza.* Random House Mondadori.

UNAM. (19 de Octubre de 2016). *Seguridad Informatica.* Obtenido de http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/ServiciosSeguridad.php

DE LA CIBERSEGURIDAD A LA CIBERPOLÍTICA.

René Montero Montano*
Karina Aurora Ybarra Martínezα

La ciberseguridad y la construcción del concepto tiene su raíz en la visión de un mundo globalizado, apoyado en el desarrollo de la técnica y la tecnología como instrumento estratégico de control para la expansión de los mercados y el fortalecimiento de una economía centrada en un proyecto corporativo que aglutina a una "comunidad mundial". En ese sentido, estamos hablando de un discurso hegemónico y universalizado de la seguridad social, política y económica de todos los que habitan en este planeta, incluyendo en ello a quienes no están de acuerdo con los protocolos (hackers) que se instalan desde los organismos cupulares (gobiernos, corporativos empresariales) que toman decisiones sobre el propósito y modo de atender al aseguramiento humano, utilizando los recursos de *lo ciber*.

Digamos que la intencionalidad que da sentido al propósito de la ciberseguridad se instala en la búsqueda de la seguridad nacional/gubernamental, empresarial, y casualmente ciudadana -esta última circunscrita a los usuarios de un "bienestar digital"[1], propio de *lo ciber*-, que acota y excluye de su ámbito de definición a todos aquellos no usuarios, distantes de la necesidad de aseguramiento de este bienestar digital.

---

* Psicólogo social, Mtro. en Teoría Crítica, psicoanálisis y doctorante en teoría crítica. Fundador de Prospectiva y desarrollo sustentable S.C.

α Licenciada en Administración de Empresas, cursando actualmente Maestría en Alta Dirección y Gestión Administrativa.

[1] *"La ciberseguridad afecta al bienestar digital de la sociedad, de las organizaciones y de los países".* Caro, B. María J.- *Alcance y ámbito de la seguridad nacional en el ciberespacio*. Ciberseguridad, retos y amenazas a la seguridad nacional en el ciberespacio.- Instituto español de estudios estratégicos- Instituto Universitario General Gutierrez Mellado.- Ministerio de Defensa-España 2010.- pp. 80

Este rumbo de la reflexión y la acción del aseguramiento cibernético, por definición, ignora la diferencia de las condiciones nacionales y contextos económicos, sociales y culturales de las necesidades civiles de aseguramiento -aprovechando las fortalezas que para ello proporciona el desarrollo de las tecnologías de la información y las comunicaciones (TIC)-, para centrarse en el diseño de sistemas específicos derivados de las nociones de ataque/defensa, sean éstos de carácter político, económico, terrorista o delincuencial.

De esta manera, la posibilidad de aseguramientos nacionales (o estatales) incluyentes de los ciudadanos comunes, habitantes de un territorio "en riesgo", pasa de largo, sin que el esfuerzo tecnológico de una cierta ciberseguridad responda a intereses fundamentalmente humanitarios para el conjunto de quienes habitamos de este planeta, centrando su ejercicio en el plano de una *guerra ciber* que atiende propósitos distantes de una ciudadanía urgida de seguridad y que se encuentra más allá –o en los márgenes- de lo estrictamente relacionado con el bienestar digital.

¿Cuál sería entonces la intención de reunirnos para pensar la ciberseguridad en un estado de la República Mexicana como Veracruz, donde sus ciudadanos viven una de las condiciones más críticas de inseguridad en todos los ámbitos de la vida social, económica y cultural? ¿Qué experiencia podría dejarnos pensar en el aprovechamiento de las TIC's y *lo ciber* para el blindaje, el aseguramiento integral del buen vivir de los veracruzanos?

La exposición que a continuación se desarrolla toma sus ideas fuerza de la posibilidad de construir el buen vivir de los ciudadanos de un estado como el de Veracruz, a partir de la instalación de un aseguramiento endógeno, sustentable y sostenible, aprovechando las posibilidades de la planeación democrática de sus recursos y la transparencia en el ejercicio de

los mismos, con el soporte tecnológico de un modelo de ciberseguridad, que se despliegue más como una *ciberpolítica* incluyente, donde los actores principales son el gobierno y la sociedad civil. En esa medida se considera que los recursos de *lo ciber* y las TIC's pueden operar eficientemente si constituyen en un componente central de la participación ciudadana a través de comités ejecutivos y de contraloría social, habilitados para implementar un sistema de ciberseguridad ciudadana instalable en todo el territorio de la entidad donde existan poblaciones.

Esta propuesta de mirar la ciberseguridad, como una expresión *ciberpolítica*, abandona la mirada convencional globalizante, excluyente de la intervención ciudadana en la implantación de su aseguramiento por medio de la transmisión eficiente de la información y la transparencia de las políticas del buen vivir ciudadano, en la cual se prioriza la organización para la paz, con una distancia necesaria de la idea de la ciberseguridad para la guerra. Es una intención de construir un caso/ejemplo de seguridad ciudadana al margen de guerras, en las cuales no le corresponde intervenir enfrentándose con la delincuencia organizada desde *lo ciber*, ni de la competencia descarnada entre los mercados corporativos de circulación globalizante, considerando que estas son, o responsabilidad directa del estado/gobierno o una lucha específica de interés entre los actores beneficiarios de la competencia que se desata por el control de los mercados globales, y por lo tanto, de una ciberseguridad dirigida específicamente para el control y dominio del otro usuario, excluyente del conglomerado social no usuario del bienestar digital y desvinculado de la expansión de los mercados corporativos.

Nos interesa reflexionar sobre la construcción de una ciberseguridad que transite hacia una ciberpolítica de aseguramiento de la sociedad civil, para el buen vivir de sus ciudadanos y la construcción de sujetos en libertad, en una condición de respeto a sus derechos de propiedad

(PROUDHON, P), priorizando con esto su intimidad y distancia de técnicas de control instaladas para usos de manipulación, dominio y desarticulación de la posibilidad de ser, *estar-con-otros-en-el-mundo.*

Una "sí-verse-gür-y-dad", afirmación del verse o reconocerse boscoso (complicado o con abundantes dilemas), y fruto de ello, por ello mismo, por el hecho de atreverse a mirarse a sí mismos en su dificultad y complicación de ser, estar ya dispuestos para dar-compartir, dar el significado esencial de la conexión con el ser, simbolizado por la "y" griega, y así dar, la y-dad.
Vamos por insistir en que los sujetos que comparten un contrato social con su estado/nación tiene derechos fundamentales derivados de la función sustantiva de los gobiernos, que son la seguridad, la libertad y la propiedad, considerando que un estado incapaz de ofrecer seguridad a sus ciudadanos, es un estado fallido que debe ser relevado, sustituido por otra estructura que la garantice.

La seguridad, en este contexto contemporáneo, destaca como una necesidad imprescindible para que la libertad y la propiedad, como derechos, faciliten el buen vivir de cualquier sujeto/ciudadano existiendo en sociedad. Para el caso que nos convoca, de todos los que habitan en este territorio veracruzano.

La seguridad civil contemporánea, apoyada en el uso de las TIC's, puede ser concebida como estrategia de ciberpolítica, si se mira como una posibilidad para las naciones que se organizan como estados democráticos liberales, donde la participación ciudadana es un componente indispensable para que opere un sistema de aseguramiento que garantice una existencia armónica, orientada por un contrato social capaz de promover los intercambios necesarios para el sostenimiento de una política democrática de *estar-con-otros-en-el-mundo.*

Así, el tránsito de una ciberseguridad convencional a una estrategia ciberpolítica pone el acento en la participación ciudadana para la construcción de sistemas de planeación democrática y de ejercicio de los recursos nacionales disponibles -dedicados al aseguramiento del buen vivir-, con criterios de un enfoque de sustentabilidad social y sostenible del sistema, priorizando estructuras de participación y organización ciudadanas que, en una relación de horizontalidad ético-política con los integrantes de su gobierno, cumplan funciones de ejecución, seguimiento y validación de planes, programas, y proyectos de aseguramiento, social, económico, político y cultural.

Como un antecedente experiencial recuperable, en los años 80's, el gobierno de la República Mexicana diseñó los primeros ejercicios para el establecimiento de un sistema de planeación democrática, que se instaló y demostró algunas de sus bondades. Sin embargo, durante los últimos 20 años este sistema ha sido desarticulado –tal es el caso de Veracruz-, para reinstalar un modelo autoritario y centralizado, derivado de planes nacionales o estatales de desarrollo que se desvinculan de la consulta y la demanda de las poblaciones y comunidades beneficiarias de las funciones de sus respectivos gobiernos.

Esta marcha atrás de la democratización de la vida política nacional y de los estados -cuyo análisis y discusión no es motivo de este trabajo-, facilitó la desarticulación política de la participación social y la formación ciudadana, en prácticamente todo el territorio nacional, estatal y municipal, restituyéndose con ello la toma de decisiones unilaterales de la planeación y ejercicio de los recursos federales y estatales destinados al buen vivir ciudadano.

Paralelamente, al instalarse la autoridad ilimitada de los corporativos industriales, inmersos en el discurso de los mercados, y reducirse la intervención del estado/gobierno en la

regulación de la economía y la toma de decisiones de su rumbo, se formalizaron estructuras burocráticas cada vez más ajenas al cumplimiento del contrato social ciudadano-gobierno, asumiendo formas del ejercicio de la función pública orientada a una política de negocios para la acumulación de capitales personales y familiares, violando la normatividad vigente y al amparo de la ambigüedad y protección que las leyes vigentes otorgan a quienes se supone tienen responsabilidades de aseguramiento de los ciudadanos.

De este modo, las facilidades para un rápido y voraz enriquecimiento de los funcionarios públicos, establecieron condiciones de alto riesgo y vulnerabilidad para la población.

Así, la seguridad ciudadana alcanzará niveles extremos de fragilidad e indefensión en todos los niveles y ámbitos de la vida social, económica y cultural. Los grupos e individuos no podrán contar con posibilidades de defensa y protección, lo que construirá un consenso de vivir en un mundo y una realidad cotidiana permanentemente amenazante. Ante tales amenazas no habrá más que recurrir y confiar en el último recurso disponible desde una postura civil y pacífica: la democracia electoral.

Digamos entonces, que la decisión ciudadana reclama y convoca a un aseguramiento real y concreto, casi en los límites de la sobrevivencia, al cual se debe responder aprovechando los recursos disponibles y poniendo en marcha el mayor esfuerzo de invención, creatividad, compromiso y honestidad. Es aquí donde una *"sí-verse-gür-y-dad"*, apuntalada estratégicamente en las TIC's, puede desplegarse, aprovechando los avances alcanzados, poniendo en movimiento un ejercicio de traducción ciudadana de cada uno de los recursos de la informática y las telecomunicaciones desarrollados desde *lo ciber*, y destinarlos a la búsqueda del buen vivir de los veracruzanos.

Para lograr un propósito como el sugerido, es necesario:

1) Instalar un sistema de planeación democrática con amplia participación ciudadana.
2) Fortalecer las estructuras de administración territorial, actualizando la regionalización geográfica vigente.
3) Fortalecer los sistemas de geolocalización a nivel de AGEB.
4) Actualización de las bases de datos de representantes comunitarios por sector (agropecuario, salud, obras públicas, educación, etc).
5) Crear un sistema de redes informáticas con operación hasta el nivel comunidad-AGEB.
6) Instalar un modelo de organización comunitaria que opere con dos comités de participación ciudadana: a) de ejecución de obras y b) de contraloría social.
7) Desarrollar un sistema en red de información y comunicación disponible a nivel comunidad-AGEB, accesible a la ciudadanía organizada en torno a los comités ciudadanos.
8) Desarrollo de redes de información y comunicación que vinculen los comités de organización ciudadana con el sector correspondiente (salud, educación, obras públicas, seguridad pública, etc.)
9) Implantar un modelo de organización, capacitación y autoevaluación de los comités de participación ciudadana para el buen vivir.
10) Reuniones de evaluación periódicas: locales, municipales y regionales con participación ciudadana y gubernamental.

Instalar un sistema de planeación democrática con amplia participación ciudadana.- La estrategia de inclusión ciudadana para la identificación de necesidades reales de inversión en infraestructura y servicios a la población, permite una valoración mucho más efectiva de la asignación de acciones que el gobierno debe programar para su ejecución dentro de sus

Programas Operativos Anuales (POA). Implica una relación permanente y directa que en épocas pasadas –antes del desarrollo de las TIC's-, era imposible sostener, para "estar al día" de los avances y logros de lo programado, en proceso y ejecutado. Una red con equipos y tecnología instalados microregionalmente y a nivel comunidad permite que los ciudadanos beneficiarios establezcan niveles de confianza aceptables con las instituciones del sector correspondiente, vínculos seguros con las de seguimiento gubernamental, y entre ellos mismos, como organizaciones responsables de aseguramiento ciudadano.

Fortalecer las estructuras de administración territorial, actualizando la regionalización geográfica vigente.- Desconcentrar la administración sectorial en un estado tan grande como Veracruz es una acción urgente para la eficiencia y la eficacia del seguimiento y aseguramiento ciudadano, en tanto que los rangos de respuesta permiten la instalación de mayor compromiso por parte de las organizaciones ciudadanas y de las propias dependencias. Un sistema creado desde el aprovechamiento de las TIC's permite que la información se distribuya y organice local, regional y centralmente. Al mismo tiempo, las empresas participantes y ejecutantes se reconocen y prestigian de manera directa con los usuarios.

Fortalecer los sistemas de geolocalización a nivel de AGEB.- El uso de las comunicaciones satelitales y el seguimiento permanente de la institución responsable de la ciberseguridad, para que las cosas sucedan en cada comunidad y rincón del estado de acuerdo a lo programado, facilita una eficiencia financiera y administrativa de los recursos asignados y programados, evitando intentos de gestión fraudulenta y desfasada de los tiempos comprometidos para la ejecución.

Actualización de las bases de datos de representantes comunitarios por sector (agropecuario, salud, obras

públicas, educación, etc.).- Un primer y sustantivo ejercicio para validar en campo, es contar con una base de datos reciente de los diferentes representantes o responsables, por sector, de los enlaces con las dependencias gubernamentales. Esto facilitará la realización de reuniones comunitarias o asambleas informativas y posteriormente organizativas de un modelo de aseguramiento aprovechando *lo ciber* y las TIC's. Se trata de crear las condiciones para el pasaje, de una democracia electoral, a una democracia participativa, que se organice en torno a los comités de ejecución y contraloría, conformados por los expertos reconocidos y éticamente valorados por los integrantes de las poblaciones, colonias vecinales y estructuras basadas en territorialización urbana desde la AGEB.

Crear un sistema de redes informáticas con operación hasta el nivel comunidad-AGEB.- Es la implantación del aseguramiento apoyado en *lo ciber* y las TIC's, con una fortaleza originalmente endógena del sistema, aprovechando los avances que se han obtenido desde las tecnologías aplicadas en la ciberseguridad convencional, pero ahora aplicadas a propósitos y objetivos adecuados a lo sostenible de la organización ciberpolítica del estado-gobierno-sociedad civil. Ello con una capacidad de intercambio de información, transparencia y acceso que facilite una primera etapa de la instalación de un proceso de restauración económica social y cultural de un territorio tan devastado como el de Veracruz.

Instalar un modelo de organización comunitaria que opere con dos comités de participación ciudadana: a) de ejecución de obras y b) de contraloría social.- La decisión de la ciudadanía veracruzana, reflejada en unas elecciones por demás competidas, muestran una franca disposición de romper con el circulo vicioso tendido por más de 20 años en todo el territorio del estado. La participación y los consensos sociales, traducidos en los votos logrados por cuando menos dos partidos políticos diferentes al hegemónicamente dominante, son el indicador

duro de una disposición al cambio ante una gobernanza amenazante. Sin embargo, parece que la vía aún se funda en la esperanza y la fe. Por ello es necesario pasar al ámbito de las visiones compartidas y a la implantación de estrategias de co-gestión y en la medida de lo posible, de autogestión.

Las poblaciones de Veracruz viven bajo amenaza permanente, la inseguridad no se restringe al crimen organizado, sino a todas sus formas de manifestación adquiridas en los últimos 12 años de desgobierno. Como un tercero amenazante, la inseguridad promueve la organización en torno a objetivos comunes y este es el caso de un gran número de veracruzanos. De ahí la certeza que la participación ciudadana apoyada en las TIC para fortalecer la seguridad desde las estructuras democráticas, pueden ser una realidad si las condiciones se facilitan tecnológicamente.

La organización comunitaria, en contextos de libertad y defensa de sus derechos ciudadanos, se convierte en un soporte indeleble de un estado que responde positivamente a la necesidad de crear un modelo de seguridad eficiente y eficaz. Por ello, la creación, formación y capacitación de comités de participación social para crear una variante veracruzana de gobierno compartido es la respuesta idónea para dar los pasos indispensables ante la incertidumbre de sobrevivencia.

Desarrollar un sistema en red de información y comunicación disponible a nivel comunidad-AGEB, accesible a la ciudadanía organizada en torno a los comités ciudadanos.- Tecnificar el sistema de información en todo el territorio de la entidad es hoy una tarea fácil, lo difícil es tomar la decisión para hacerlo de manera incluyente. Los apoyos técnicos y financieros para ello no pueden ser en este momento un pretexto para realizarlo su efectivamente existe el interés de blindaje de la población desde una ciberseguridad tecnológica tendiente a la "sí-verse-gür-y-dad" humana.

Desarrollo de redes de información y comunicación que vinculen los comités de organización ciudadana con el sector correspondiente (salud, educación, obras públicas, seguridad pública, etc.).- Un sistema diseñado para atender las necesidades de organización, información, transparencia y efectividad en la realización de obras y acciones orientadas a la seguridad ciudadana, operando desde un servidor suficientemente robusto para incluir seguimiento de procesos a través de registros fotográficos e informes elaborados por los comités de participación, restablece valores asociados a la confianza, cooperación, responsabilidad compartida, optimismo y, por lo tanto, sentimiento de seguridad frente al porvenir.

Implantar un modelo de organización, capacitación y autoevaluación de los comités de participación ciudadana para el buen vivir.- La formación de los miembros de las estructuras democráticas de participación ciudadana, con los enfoques de sustentabilidad social, igualdad de género, inclusión social y reconocimiento de la diferencia, integrando en los procesos de capacitación a la población adulta y joven de las localidades, permite aprovechar la experiencia y las competencias que ya existen entre ellos, al mismo tiempo que desarrollar nuevas habilidades genéricas, que faciliten a los participantes compartir funciones y responsabilidades en el mantenimiento de los equipos y la alimentación del sistema de información y seguimiento local y microregional, promoviendo la revaloración de las asambleas y reuniones vecinales de presentación de logros, así como el análisis de nuevos retos y la creación de escenarios de soluciones cada vez más sustentables y sostenibles.

Reuniones de autoevaluación y evaluación periódicas: locales, municipales y regionales con participación ciudadana y gubernamental.- El diálogo que propicia el intercambio sobre las dificultades, problemas, formas de solución y logros alcanzados en los procesos compartidos

gobierno-sociedad civil, es la estrategia clave para la apropiación y reconocimiento de una ciberpolítica efectiva. La presentación de datos sobre resultados y logros derivados de la participación ciudadana a través del uso y dominio de las TIC's, amplían la apropiación de los mismos como una estrategia tecnológica de ciberseguridad y una existencial de *"sí-verse-gür-y-dad"*. Hacer del uso de las TIC's de manera cotidiana en el ejercicio del aseguramiento ciudadano contribuye al descentramiento del individualismo y destaca lo virtuoso del vivir en sociedad.

A MANERA DE CONCLUSIÓN

Como una construcción social, la realidad que se propone es una utopía factible, siempre y cuando se conjuguen voluntades para un gobernar discreto e incluyente, en ese sentido, su cristalización efectiva es responsabilidad de gobiernos que ejerzan el poder de "mandar obedeciendo", es decir, instituciones que se apropian de una ética de servicio ciudadano, restableciendo los valores sustantivos que la función del estado debe propiciar para con todos sus ciudadanos: seguridad, libertad, igualdad y fraternidad.

Demos la vuelta al bucle, un giro de timón, vamos a torcer la tuerca de la ciberseguridad para apropiarnos de ella con el propósito de vivir mejor.

BIBLIOGRAFÍA:

De TOMAS, Morales Susana & otros.- (s/f).- Retos del derecho ante las nuevas amenazas.- Madrid.- Editorial Dykinson

GIANT,Niki (2016).- Ciberseguridad para la i-generación. Uso y riesgo de las redes sociales y sus aplicaciones.- Madrid, España.- Narcea S.A. Ediciones

HEIDEGGER, MARTIN (1997).- Ser y tiempo (1997) Chile.- Ed. Universitaria S.A.

-- (1994).- La pregunta por la técnica.- Conferencias y artículos.-Barcelona.- Ediciones del Serbal 9-37

JORDÁ, Capitán Eva & Verónica de Priego Fernández. (2014).- La protección y seguridad de la persona. Aspectos sociales y políticos.- Editorial Reus S.A.

INSTITUTO ESPAÑOL DE ESTUDIOS ESTRATÉGICOS (2010).- Ciberseguridad, retos y amenazas a la seguridad nacional en el ciberespacio. Cuadernos de estrategia 149.- España.- Ed. Ministerio de defensa.

MONTEMAYOR, Rogelio.- (s/f).- Sistema de Planeación democrática.- Revista de Administración Pública.

OCDE (2016).- Perspectivas de la OCDE sobre la economía digital 2015. México.- Microsoft México.

PROUDHON, J.P (2005).- ¿Qué es la propiedad? Investigaciones sobre el principio del derecho y el gobierno.- Buenos Aires.- Ed. Proyección

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/

México, E. S. (Marzo de 2016). *Hackearon página del SAT; Anonymous se adjudica el ataque.* Recuperado el Octubre de 2016, de https://www.elsoldemexico.com.mx/mexico/157113-anonymous-mexico-hackea-el-sitio-web-del-sat

Osigma. (Diciembre de 2011). *Observatorio Nacional de las Redes Sociales y de las SI.* Recuperado el Octubre de 2016, de Observatorio Nacional de las Redes Sociales y de las SI: http://www.osimga.gal/export/sites/osimga/gl/documentos/d/20111201_ontsi_redes_sociais.pdf

Symantec. (Abril de 2016). *Publicaciones de Security Response.* Recuperado el Octubre de 2016, de https://www.symantec.com/es/mx/security_response/publications/threatreport.jsp

UNA NECESIDAD EN LAS EMPRESAS: LA CIBERSEGURIDAD

[2]Raúl Manuel Arano Chávez
Jesús Escudero Macluf *
Luis Alberto Delfín Beltrán *

INTRODUCCIÓN

Con el uso de las tecnologías en las empresas se les facilitan tener un acercamiento con sus clientes de forma global a través de un correo electrónico donde se les envíe por ejemplo un catálogo de productos, felicitaciones de cumpleaños, un boletín de noticias, o muchos otros servicios más, sin que esto le represente un costo adicional. De la misma forma con la creación de un portal web donde podremos representar nuestra marca, servicios, productos y que nuestros clientes puedan realizar sus compras en línea en cualquier día de la semana en cualquier horario.

Es por ello, que una empresa al menos debe contar con un portal web, correo electrónico, un sistema de gestión de clientes y estar en permanente comunicación a través de las redes sociales, para conocer los valores que debe agregar a su producto y/o servicio con respecto a las características que sus clientes prefieren.

Una nueva forma de hacer negocio es el Comercio Electrónico, quien ha tenido gran relevancia en la actividad de una empresa ya que han tenido que incorporar herramientas para las transacciones bancarias o pagos en línea, así como la generación

* * Investigadores del Instituto de Investigaciones y Estudios Superiores de las Ciencias Administrativas de la Universidad Veracruzana. Correo electrónico: rarano@uv.mx, jescudero@uv.mx y ldelfin@uv.mx

de facturas electrónicas que demanda tener una infraestructura local o tercerizar el servicio.

En este sentido, cobra mayor impacto la seguridad en las tecnologías de la información y comunicación de una empresa, ya que al utilizar la internet como medio de comunicación interna y externa, en este mundo globalizado están expuestos a las amenazas de seguridad de su información.

Los objetivos de los "ciberdelincuentes" no solo se ven reflejados en ataques a empresas grandes o también basan sus ataques en pequeñas y medianas empresas, por lo que toda empresa sin importar su "sector" y/o tamaño deben poner mayor cuidado en la seguridad de sus datos, quizá lo más importante en las empresas no sea solo el cliente sino toda la información que genera el cliente.

LAS TECNOLOGÍAS DE LA INFORMACIÓN INCLUSTADAS EN LAS EMPRESAS.

El uso de las Tecnologías de la Información y Comunicación (TIC´s), en las empresas se ha vuelto en algo imprescindible en toda su estructura organizacional, tomándolas como herramientas tecnológicas que optimizan y mejoran sus procesos administrativos-operativos, agilizando sus operaciones administrativas, de toma de decisiones, procesamiento de datos y en el análisis de información.

Con el uso de la internet como aceleradora de procesos las empresas tienen que cambiar sus estrategias de trabajo al interior como al exterior y a continuación presentaremos las que desde nuestro opinión son más utilizadas por las empresas:

1) Internet en la nube (Cloud Computing)

Fernández morales en su libro "Computación en la nube para automatizar dice que **"**De acuerdo con Ioni y Ioni (2011), en la

actualidad, la mayoría de la infraestructura de computación en la nube se compone de servicios confiables a través de puntos llamados "centros de datos" y construidos en los servidores con varios niveles de tecnologías de virtualización. Los servicios son accesibles en cualquier lugar y permiten el acceso a la infraestructura de redes. Esta forma de acceso satisface todas las necesidades i**nformáticas de los consumidores".** (Fernández Morales, 2012)

2) Comercio Electrónico (E-Commerce)

La Procuraduría Federal del consumidor en su portal electrónico lo precisa como: *"El proceso de compra, venta o intercambio de bienes, servicios e información a través de las redes de comunicación."*

"Representa una gran variedad de posibilidades para adquirir bienes o servicios ofrecidos por proveedores en diversas partes del mundo. Las compras de artículos y servicios por internet o en línea pueden resultar atractivas por la facilidad para realizarlas, sin embargo, es importante que los ciberconsumidores tomen precauciones para evitar ser víctimas de prácticas comerciales fraudulentas" (PROFECO, 2016).

Este modelo de negocio electrónico garantiza a las empresas capacidad en la oferta de sus servicio y/o productos, bajo costo de operación, procesos comerciales agiles y eficientes, ingreso al mercado global, utilización de nuevas tecnologías y calidad en el servicio. Aunque no asegura el éxito puede ser un gran canal de distribución en las empresas.

3) Negocio Electrónico (E-Bussines).

Jorge Eliécer Prieto Herrera, en su libro "Investigación de Mercados" lo define como *"actividad o proyecto empresarial que tiene como escenario la utilización de un medio electrónico". (Prieto Herrera, 2009).*

Logra una mejor integración entre el proveedor-cliente, disminuye los costos de operación, integra un mejor conocimiento del mercado y permite entrar al mundo globalizado.

4) Big Data

De acuerdo con el análisis realizado por el AMIPCI (Asociación Mexicana de Internet) el término Big Data se refiere a "la acumulación masiva de datos. Esta tendencia se enmarca principalmente en actividades relacionadas con sistemas que manipulan grandes conjuntos de datos, que supera la capacidad de sistemas tradicionales para ser capturados, gestionados y procesados en un tiempo razonable" (AMIPCI, 2015).

La manipulación de grandes cantidades de datos personales se centra en un proceso de captura, almacenamiento, análisis, y visualización. La captura u obtención de los datos se pueden realizar a partir de diversos mecanismos, ya sean los generados por las personas, transacciones de datos, mecanismos de e-marketing y páginas Web.

El almacenamiento se realiza mediante plataformas o sistemas para extraer, homologar y generar bases de datos; el análisis que se puede realizar mediante asociaciones, análisis de textos, minería de datos (Data Mining) referida al análisis de comportamientos predictivos, o Clustering de datos, mediante la agrupación de grupos pequeños de individuos para identificar comportamientos similares; y su visualización a través de imágenes, gráficas, infografías, entre otros.

Este concepto se puede ser utilizado en una gran variedad de ámbitos, como el desarrollo de campañas de comercialización específicas para perfiles de usuarios de redes sociales; venta de nuevos productos y servicios basado en patrones de compra de usuarios, creando anuncios personalizados y boletines electrónicos.

En este sentido, representa grandes oportunidades para el desarrollo y crecimiento de nuevos negocios basados en datos personales, pero también comporta importantes riesgos. Por lo que las empresas deben ser cautas con los riesgos asociados a sus procesos de captura, identificación, re-identificación, análisis predictivo y recolección de información, concediendo especial atención en el tratamiento de datos de carácter personal.

5) Mercadotecnia Electrónica (E-Marketing)

La mercadotecnia en el internet es la posibilidad de promocionar y difundir los productos y/o servicios de forma global a través de la red de redes, mostrando como ventajas el contacto directo con los potenciales clientes, realizar campañas masivas a todos los usuarios del internet, innovación en la penetración de los productos ante los clientes y el ingreso al mercado global a bajo costo.

"La comunicación es importante para darnos a conocer y que conozcan nuestras intenciones, pero para generar resultados a lo largo del tiempo usted necesita tener acción permanente. Esta acción debe estar respaldada por una estrategia corporativa y ambos tipos de estrategias (corporativas y sectoriales) responden a la visión que usted se proponga. (Moncalvo, 2016)

LOS RIESGOS CIBERNÉTICOS EN UNA EMPRESA.

Como hemos visto las bondades que ofrecen las Tecnologías de la Información y Comunicación (TIC´s) a las empresas, estas han permitido que este sea un gran sector de oportunidades para todos aquellos que desean comercializar o difundir sus productos, pero esto ha llevado a que se tenga que reglamentar el uso de estas para no caer en "dificultades técnicas".

Pero esto también nos ha traído que personas ajenas quieran lucrar con nuestra información y sea una amenaza constante en el día a día de nuestros procesos informáticos.

La protección de los datos no ha sido bien valorada en México, sobre todo en las pequeñas y medianas empresas, creyendo que estas no son un objetivo importante para los "hackers", recordemos que estos "personajes" navegan todo el tiempo en la red en busca de sitios vulnerables y al encontrarlos no dudan en mostrar sus habilidades para sustraer su información.

Recordemos que un gran porcentaje de negocios se apoyan en bases de datos con conexiones remotas, software de gestión y el uso continuo de Internet, por lo que tener en tu empresa un posible fallo o deficiencia en la seguridad de tus "servidores" o equipo de telecomunicaciones representa un grave problema que puede significar la pérdida de datos importantes, afectando gravemente el desempeño y seguridad.

Como las amenazas más comunes encontramos las siguientes:

a) Phishing

De acuerdo a la publicación que realiza el portal web Panda Security el "phishing" consiste en "*el envío de correos electrónicos que, aparentando provenir de fuentes fiables (por ejemplo, entidades bancarias), intentan obtener datos confidenciales del usuario, que posteriormente son utilizados para la realización de algún tipo de fraude.*

Para ello, suelen incluir un enlace que, al ser pulsado, lleva a páginas web falsificadas. De esta manera, el usuario, creyendo estar en un sitio de toda confianza, introduce la información solicitada que, en realidad, va a parar a manos del estafador". (Secutity, 2016)

b) Ataques de fuerza bruta

Ataque por fuerza bruta es el método que se utiliza para averiguar una contraseña probando todas las combinaciones posibles hasta dar con la correcta. Los ataques por fuerza bruta son una de las técnicas más habituales de robo de contraseñas en Internet dado que no es necesario tener grandes conocimientos en seguridad informática para realizar uno y existen programas que realizan de forma automática esta labor. http://faqoff.es/que-es-un-ataque-por-fuerza-bruta/

c) Robo de identidad

La CONDUSEF en su revista "Proteja su dinero" lo describe "Cuando una persona obtiene, transfiere, posee o utiliza de manera no autorizada datos personales de alguien más, con la intención de asumir de manera apócrifa su identidad y realizar compras, obtener créditos, documentos o cualquier otro beneficio financiero en detrimento de sus finanzas.

Tu identidad la constituyen datos personales como: nombre, teléfono, domicilio, fotografías, huellas dactilares, números de licencia y seguridad social, números de tarjeta de crédito y cuentas bancarias, nombres de usuario y contraseñas." (CONDUSEF, 2016)

d) Ataques de negación de servicios (DoS)

Se entiende como que una persona "ajena" se apropie de un recurso o servicio de una empresa con la intención de evitar cualquier acceso de sus clientes. También, se incluyen los ataques destinados a colapsar un recurso o sistema con la intención de destruir el servicio o recurso.

e) Spyware o Keylogger

Software o hardware instalado en una computadora, generalmente sin el conocimiento del usuario, que recoge información de dicho usuario para más tarde enviarla por Internet a un servidor remoto.
http://www.internetglosario.com/828/spyware.html

f) Hackeo

Un hacker es aquella persona experta en alguna rama de las TIC´s, dedicado a intervenir y/o realizar alteraciones técnicas con buenas o malas intenciones sobre un producto o dispositivo.

http://cristianargelvergara.blogspot.mx/p/inicio.html

La palabra hacker es tanto un neologismo como un anglicismo. Proviene del inglés y tiene que ver con el verbo "hack" que significa "recortar", "alterar". A menudo los hackers se reconocen como tales y llaman a sus obras "hackeo" o "hackear".

http://www.definicionabc.com/tecnologia/hacker-2.php

CONCLUSIONES

Las empresas hoy en día requieren de establecer mayores medidas de seguridad en su infraestructura de las Tecnologías de la Información y Comunicación, y deben de contratar a personal especializado en seguridad ya sea interna y/o externa que le permita contar con un plan definido para prevenir o mitigar los posibles ataques que pudiera tener, no olvidemos que por el simple hecho de que las empresas utilicen sistemas de información o servicios de internet son vulnerables a todo tipo de ataque sin importar el tamaño de la empresa.

De suma importancia establecer en la organización políticas de seguridad con respecto a: utilización de antivirus corporativo y licenciado, disminuir los tiempos de navegación en la web de sus empleados, evitar la descarga de archivos desde sitios no legales, filtrar los correos electrónicos de dudosa procedencia y crear perfiles laborales con acceso restringido de información y sobre todo estar siempre alertas a que así como la tecnología en las empresas evoluciona, de la misma forma las medidas de seguridad deben de ser cada vez más complejos.

REFERENCIAS BIBLIOGRÁFICAS

AMIPCI. (2015). *ESTUDIO SOBRE EL VALOR ECONÓMICO DE LOS DATOS PERSONALES*. AMIPCI.

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

Fernández Morales, M. (2012). *Computación en la nube para automatizar unidades de información*. Red Universidad Nacional de Costa Rica.

Moncalvo, A. (2016). *Comercio Electrónico para Pymes*. Buenos Aires: Ugerman.

Prieto Herrera, J. E. (2009). *Investigación de Mercados*. Ecoe Ediciones.

PROFECO, P. F. (2016). *Profeco / Secretaría de Economía*. Recuperado el miércoles 12 de Octubre de 2016, de http://profeco.gob.mx/internacionales/com_elec.asp

Secutity, P. (12 de octubre de 2016). *Panda*. Recuperado el 12 de octubre de 2016, de http://www.pandasecurity.com/spain/homeusers/security-info/cybercrime/phishing/

CONSULTAS WEB

Aprendizaje Educativo del Desarrollo de las TIC. Obtenido de http://cristianargelvergara.blogspot.mx/p/inicio.html. (Consultado el 21 de octubre de 2016)

Definición ABC. Obtenido de http://www.definicionabc.com/tecnologia/hacker-2.php. (Consultado el 21 de octubre de 2016)

Glosario de I nformática e Internet. Obtenido de http://www.internetglosario.com/letra-s.html. (Consultado el 21 de octubre de 2016)
Consejos de seguridad para Pymes. Obtenido de http://www.all4sec.es/blog/consejos-de-seguridad-para-pymes/. (Consultado el 21 de octubre de 2016)
¿Qué es el Internet marketing? Obtenido de http://www.internet-marketing.es/que-es-internet-marketing.html. (Consultado el 21 de octubre de 2016)

IMPLEMENTACIÓN DE UNA HERRAMIENTA OPEN SOURCE COMO SISTEMA DE SEGURIDAD REACTIVA EN ESCENARIOS EMPRESARIALES PYMES, COMO SOLUCIÓN DE SEGURIDAD A BAJO COSTO

Carlos Iván Téllez Gutiérrez*

INTRODUCCIÓN

La rapidez con la que están absorbiendo tecnología las PYMES y que la están adaptando a su modelo de negocio para eficientar y automatizar procesos para diferenciarse de su competencia en servicio y prontitud de respuesta, organización y mejorar las transacciones comerciales y la integridad de la información de los clientes.

Las PYMES gracias a que los costos de tecnología y de acceso a Internet han ido en decremento con el paso del tiempo y los diferentes servicios hacia los clientes y procesos internos y externos como correo electrónico, pago de impuestos, servicios en la nube Internet, extranet, entre otros, se observa que se ha incrementado también el nivel de riesgos y ataques derivados de las vulnerabilidades y conocimientos técnicos que en esta época la brecha digital en las PYMES crezca debido a la implementación de nuevas tecnologías.

La gran diversidad de acceso a Internet de los ISP (Internet Service Provider, Proveedores de servicio de Internet), deja a la deriva a las PYMES con poca o nula protección en el acceso a una red local (LAN, Local Area Network) y hacia contenidos en Internet no alineados a los procesos de negocio en donde lleva

* Universidad Veracruzana,catellez@uv.mx, Xalapa, Veracruz

que este sea el punto ideal para accesos no autorizados, ataques del tipo Denial of Service (DoS) y virus informáticos.
Cualquier persona con conocimientos básicos de redes y protocolos de comunicación aunada a las herramientas y tutoriales disponibles en Internet de algún estudio o tutorial de vulnerabilidades de alguna marca comercial o abierta de sistema operativo de red, marcas de Routers dinámicos (ADSL), Switches, entre otros pueda accesar a una red de cómputo.

Por otro lado, para los Hackers, aumenta más la atención que las PYMES sean débiles en cuanto a su protección perimetral, Interna y sobre todo a su acceso de la red desde Internet.

La realidad de la PYME en el entorno de TI
Aunque mucho de las herramientas que se tienen hoy para poder tener contramedidas hacia un ataque, vulnerabilidad o un virus informático, los usuarios de las PYMES no poseen una cultura informática de habilidades, capacidades técnicas y el conocimiento de las amenazas a la seguridad y de las técnicas apropiadas de control a fin de proteger su infraestructura de red y comunicación (Edgar Tello Leal, 2008) han evolucionado muy rápido y paralelamente al desarrollo tecnológico, va también en aumento una gran complejidad de los ataques(HPE Security Research Cyber Risk Report, 2016) debido a la curva de aprendizaje de alguna vulnerabilidad o sobre todo de algún debilidad encontrada en el software o red.

Por lo anterior, Las empresas, especialmente las PYMES, deben mantenerse a la vanguardia sobre el correcto uso de las tecnologías, de cómo mantener a salvo al menos su presencia dentro de la red de Internet para garantizar su integridad digital.

El cómo protegerse es un tema el cual existe un gran abanico de posibilidades en hardware y software pero que, al momento de ver la realidad económica en cuestión de los costos, es un

problema. La otra cuestión, es de poder asesorarse con algún experto en la materia que pueda prestar la debida atención a lo que la PYME necesita como requerimiento mínimo en protección en amenazas de ataques, contramedidas de espionaje informático, accesos no autorizados, etc.

La importancia de las PYMES en salvaguardar su información.

Las Pymes se encuentran en la obligación tecnológica de proteger su volumen de información todas sus bases de datos de conocimiento de una manera ágil, generando a sus clientes la suficiente confianza y credibilidad para poder realizar sus transacciones comerciales de forma segura, rápida y eficiente.

Vulnerabilidades que se exponen las PYMEs hoy en día.

Toda organización maneja información crítica debe estar consciente que para poder hablar seguridad informática, se pueda identificar primero a los diferentes tipos de ataques y amenazas a los que se ven expuestas como:

- **Phising**: Es la suplantación de identidad y que se comete mediante el uso de un tipo de ingeniería social, caracterizado por intentar adquirir información confidencial de forma fraudulenta. Por ejemplo, la suplantación de un banco que solicita actualizar el pasword de acceso a una cuenta bancaria.
- **DDOS**(Distributed Denial of Service): Se traduce como ataque distribuido y denegación de servicio, consiste en atacar al servidor desde otras computadoras para que deje de funcionar.
- **Malware**: es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario
- **Spyware**: El spyware es un software que recopila información en una computadora y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del mismo.
- **Bugs**: Vulnerabilidades de un proveedor o falla mal intencionada por un problema técnico en algún Software

- **Spam:** . Correo basura o mensajes no solicitados, no deseados o de remitente desconocido.
- **Botnet**. Ataques que puede controlar todos las computadoras infectadas de forma remota
- **Fuga de Información**: Mediante medios electrónicos se roba información sensible de la empresa por parte de empleados o terceros usando métodos de transferencia electrónica.
- **Intrusión remota**. Ingreso externo no autorizado a un equipo de cómputo usando la infraestructura de conectividad de la empresa.
- **Fuerza Bruta**: Se emplea software automatizado para generar una lista larga de posibles contraseñas de acceso, para ingresarlas en la cuenta de un usuario .
- **LDAP** (Lightweight Directory Access Protocol): Es un Protocolo Ligero/Simplificado de Acceso a Directorios el cual que hace referencia a un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red
- **Inyección de SQL**. es una técnica donde un atacante crea o altera comandos SQL existentes para exponer datos ocultos, sobrescribir los valiosos, o peor aún, ejecutar comandos peligrosos a nivel de sistema en el equipo que hospeda la base de datos.

Internet, los riesgos en las PYMES

El incremento exponencial del crecimiento de Internet, ha permitido que las PYMES sean más competitivas y más eficaces en sus procesos que ahora se encuentran interconectados y que ayuda mucho a eficientar los procesos internos y publicar servicios a los clientes externos en Internet.

Como consecuencia de esto se han visto expuestas a una serie de riesgos y amenazas inherentes a la implementación de transacciones comerciales a nivel nacional e internacional. Este problema impacta de manera negativa a las PYMES ya que para

tener los mínimos requerimientos de seguridad de la información, se deben establecer y mantener acciones que cumplan con tres requerimientos (Borghello, 2001).

- **Confidencialidad**: Previene el acceso no autorizado ya sea en forma intencional o no intencional a la información. La pérdida de la confidencialidad puede ocurrir de muchas maneras, como por ejemplo con la publicación intencional de información confidencial de la organización.
- **Integridad**: Que no se realicen modificaciones no autorizadas por personal autorizado a los datos o procesos y sean consistentes tanto interna como externamente.
- **Disponibilidad:** Tiene que ver con asegurar un acceso confiable y oportuno a los datos o recursos para el personal apropiado.

Por qué implementar un SSR en una PYME

La seguridad hoy en día es un tema importante en las TI dentro del contexto de las PYMES, pero la mayoría no tiene tan claro que la seguridad ya debe ser parte la cultura organizacional. Dentro de los conceptos de la organización de empresa y asignación de presupuesto, debería asignarse como prioridad el dedicar recursos a la seguridad, pero en muchas es hasta nula, hasta que se presenta un evento o en el peor de los casos un desastre.

Ante los riesgos informáticos actuales, las PYMES necesitan empezar a tomar precauciones con el fin de impedir ataques o infecciones externas.

Por otro lado, el proteger a la LAN desde fuera de la red de la empresa, ayuda a evitar accesos no autorizados, con el objetivo de minimizar vulnerabilidades en los sistemas de la LAN.

Las grandes Empresas tienen el poder económico y técnico para poder implementar seguridad (Deloitte, 2007) y enfrentarse a una crisis de seguridad de información ya sea Interno o externo a la Red.

El poder proteger la LAN de una PYME y proveer seguridad de la información ya no es una opción más de inventario de la empresa, si no que surge ahora la necesidad de una estrategia de seguridad, bajo costo y una implementación alineada con los controles que se definan e instaurar una política clara al respecto.

Ni las empresas grandes se salvan de implementar seguridad, ya que en los últimos años, se han visto diferentes ataques a empresas como PlayStation de Sony, PayPal, Paginas gubernamentales, entre otros incidentes que se han reflejado en el robo de identidad de los usuarios, robo de información financiera(cuentas, claves bancarias, claves de seguridad de tarjetas de crédito), robo por mensajes de correo del tipo Phising, y que para los clientes y usuarios han dejado una mala imagen de estas empresas y accionistas, cuestionando el manejo de seguridad que se le está brindando a los datos.

Una de las soluciones que se han desarrollado para contrarrestar las amenazas tecnológicas han sido los Firewalls, Anti-spam, AntiMalware, Antivirus, etc pero el crecimiento de amenazas y los diferentes tipos de ataque, hacen que estas soluciones sean caros adquirirlas una por una y que sea poco accesibles en el presupuesto para las PYMEs.

Para el caso de una LAN de una PYME, el poder instalar una herramienta que pueda cubrir los aspectos de Confidencialidad, Integridad y Disponibilidad a un bajo costo,

Protegiendo a la seguridad física y lógica de una PYME un SSR.

Una de las preguntas que se debe de hacer una PYME es: ¿qué se debe proteger?.

Es claro mencionar que en cuestión de continuidad de negocio, los elementos a proteger sean primeramente los DATOS.

En segundo lugar, el hardware en donde estos residen, se modifican, resguardan y se accesan, es decir; el conjunto de componentes que integran la parte física de la red LAN y el hardware de cómputo.

Como tercer elemento, la parte LÓGICA, que es el conjunto de aplicaciones, sistemas operativos y programas de red que ayudan a los procesos de negocio de las PYMES.

Para poder proteger a una PYME brindándole una herramienta de seguridad que cumpla con los requisitos de bajo costo, fácil instalación, requerimientos de hardware de costo accesible y velocidad y de cobertura (NETGEAR, 2011)

Con una herramienta de seguridad se necesita un que cumpla con ciertos requisitos de:

- Filtrado de origen a destino de IP, protocolo IP, puerto de origen y destinación para TCP y UDP tráfico
- Balanceador de carga por terminales para conexiones simultaneas con reglas de base
- Politicas de enrutamiento con alta flexibilidad para la seleccion del gateway sobre las reglas de base para el

equilibrio de banda, failover, WAN multiple, backup sobre mas ADSL, etc…
- Filtracion transparente en capa 2.
- Posibilidad de inhabilitar la **filtración** (firewalling) o la opción de solo **router**

En el ambiente de herramientas OPEN SOURCE, pfSense cumple mucho de estas características y tiene una gran ventaja para una PYME, es una distribución gratuita. Basada en FreeBSD, tiene el potencial de ser un Firewall y Router a la vez, sustituyendo las cajas de enlaces que los ISP instalan. Incluye una gran lista de paquetes que permiten expandir fácilmente las funcionalidades sin comprometer la seguridad del sistema.

Pfsense(https://pfsense.org/), cuenta con un gran respaldo de descargas e instalaciones por todo el mundo ya que cuenta con más de 1.000.000 descargas y innumerables instalaciones en todo el mundo y puede ser instalado en una gran variedad de equipos.
Dentro de sus características cuenta con firewall que sirve como un área de la LAN que audita todo el tráfico de Internet entrante y saliente y que permite circular, permitiendo controlar el tráfico y que bien configurado y administrado evita en gran medida que los hackers lo superen y por supuesto ayuda a mantener a salvo los datos confidenciales de las PYMEs y permite la monitorización y registro de las bitácoras de los servicios utilizados internos y externos al usar Internet y demás protocolos requeridos.

Pfsense por ser una distribución basada en BSD, se adaptan muy bien a los niveles de seguridad actuales ofrece ventajas de seguridad informática que las PYMES pueden adquirir.

Caso de éxito de PYME BUSINESS CENTERS Xalapa.
BUSINESS CENTERS Xalapa, es una PYME que ofrece servicios de oficina virtual y oficinas físicas localizadas en la

ciudad de Xalapa. Dentro de los usuarios que requieren velocidad, seguridad y disponibilidad de los servicios se encuentran: Nestlé, Profuturo, Asistek, entro otros.

Se utilizó una computadora Intel Celeron Core 2 Duo 1.8 Ghz, 4 GB Ram, HDD 250 GB y 2 tarjetas de red Realtek. Enlace de Internet Telmex FTTH 20 Mbps, Switch LAN Linksys de 16 puertos y AP Linksys.
Módulos Instalados:
-Portal Cautivo y Radius
-Antivirus, proxy y filtrado de contenido.
-Módulo HAVP, que es un módulo integrado de proxy y antivirus para el contenido Web
-Squid y Ligtsquid para generación de estadísticas para analizar reportes de consumo de ancho de banda, páginas visitadas y número de ingresos, entre otros, con el fin de tomar decisiones y para procesos de auditoría.
- Firewall, con reglas para que garanticen la mayor protección posible sin afectar el rendimiento, por ejemplo: permitir que los usuarios que vengan de una WAN accedan a una Intranet mediante protocolo https por el puerto 443.
- VPN, para acceso remoto a oficinas
- Squidguard, que ayuda a las usuarios de las PYMES de modo seguro, que los contenidos de navegación en internet, se haga correcto uso de los recursos alineados al modelo de negocio de los procesos de la empresa.

CONCLUSIONES

Uno de los retos de las Pymes es poder adaptarse a los requerimientos de seguridad informática para evitar las diferentes amenazas y las diferentes protecciones que se pueden hacer en las aplicaciones de red de servicio como correo, transacciones electrónicas, contenido válido de tráfico de Internet, entre otros.

El tema del poder adquirir una herramienta SSR y que Pfsense permite a las Pymes dentro de sus inversiones, considerar que no tiene costo y que su mantenimiento es bajo sobre la maquinaria que se instale

Pfsense sirve para el concepto que llamamos SSR, como una herramienta de aseguramiento de LAN y acceso a Internet, siendo una plataforma que le ayuda a una PYME a tener un punto de equilibrio económico y operativo.

Trabajos a futuro

Describir y Analizar una herramienta que PfSense acaba de liberar y es el **p0f**, la cual es una avanzada herramienta de red para huellas dactilares digitales que habilita la **filtración** a travez el sistema operativo al inicio de la conexión. Permitiendo saber realmente quién es el usuario que esta atrás del dispositivo.

REFERENCIAS

- (Edgar Tello Leal, 2008), "Las tecnologías de la información y comunicaciones (TIC) y la brecha digital: su impacto en la sociedad de México", http://www.uoc.edu/rusc/4/2/dt/esp/tello.pdf)
- (HPE, Security Research Cyber Risk Report 2016), https://ssl.www8.hp.com/mx/es/ssl/leadgen/secure_document.html?objid=4AA6-3786ENW&siebelid=560016101&sectionid=pdf&returnurl=%2Fmx%2Fes%2Fsecure%2Fpdf%2F4aa6-3786enw.pdf&simpletitle=cyber%20risk%20report&subbu=tsg.software&parentPageName=3.0&analytics_page_name=3.0&parentUrl=http%3A%2F%2Fwww8.hp.com%2Fmx%2Fes%2Fsoftware-solutions%2Fcyber-risk-report-security-vulnerability%2F&compURI=tcm%3A230-

1906136&fv=FLEX2%20SW3&metrics_asset_value=eb&bu=tsg&st=%2Fmx%2Fes%2Fsoftware-solutions%2Fcyber-risk-report-security-vulnerability&as=software&wsi=r11374&cu=false)

- (Borghello, 2001) "Seguridad Informática: sus implicaciones e implementación". Tesis de Licenciatura en Sistemas, Universidad Tecnológica Nacional, Argentina, 2001
- (Deloitte, 2007), I. Brightman, J. Buith. "Treading Water. The 2007 Technology, Media & Telecommunications Security Survey", Deloitte, 2007.)
- (NETGEAR, 2011) "Dispositivo ProSecure Para la gestión Unificada de las amenazas". Online [Mar. 2011]. [11]G

UN MARCO DE REFERENCIA PARA LA AUDITORÍA DE SISTEMAS DE INFORMACIÓN BASADOS EN WEB

Alberto Brandon Báez Camarena

INTRODUCCIÓN

La llegada de las principales técnicas de auditoría permite a los auditores identificar los riesgos y evaluar los controles sobre los sistemas de información críticos en sus organizaciones, tiene profundas consecuencias para muchas áreas de las actividades de las empresas. Aunque tales técnicas de auditoría están todavía en las primeras etapas de desarrollo, el impulso hacia su mejora es tal que se ha cambiado el carácter de la investigación llevada a cabo principalmente por la comunidad de investigación industrial. Una gran proporción del esfuerzo de investigación actual se limita a los investigadores que normalmente están ligados a asociaciones profesionales y organizaciones relacionadas con la auditoría de sistemas de información (Champlain, 1998). Argumentamos que la evaluación de los sistemas de información basados en Web (WBIS) es relevante para la industria y la academia, como consecuencia de ello, el trabajo relacionado con el desarrollo de metodologías y herramientas de auditoría se lleva a cabo ahora por sistemas científicos de la información (Akoka et al, 2000;. Atzeni et al, 2002;. Nicho 2008). El desarrollo teórico necesario para comprender las metodologías de auditoría está dando lugar a grandes avances y se espera que tengan repercusiones en los sistemas de información así como en las herramientas y técnicas de auditoría puesto que las metodologías de auditoría son cada vez más importantes ya que las organizaciones dependen en gran medida de estos sistemas información. La última década ha visto el desarrollo a un ritmo sin precedentes de los sistemas de información basados en Web (WBIS) que ha abierto la oportunidad para que se desarrollen cada vez más WBIS muy sofisticados, tales como portales, juegos en línea, portales de

gestión de información y entretenimiento, buscadores, aplicaciones de comercio electrónico, CRM (Customer Relationship Management) y aplicaciones EAI (Enterprise Application Integration).

SISTEMAS DE INFORMACIÓN BASADOS EN WEB

Durante la última década, el impacto de la web ha transformado el papel de las tecnologías de la información de sistemas apoyo en las organizaciones a sistemas estratégicos de recolección y entrega de datos que permiten la gestión estratégica de las organizaciones apoyándose en los mismos, permitiendo a las empresas por ejemplo, determinar los hábitos de compra de los clientes y darles un mejor servicio. Por lo general, se admite que las tecnologías aplicadas al comercio electrónico han reducido el costo de la recolección de datos de los compradores (Dewan et al. , 2000). Los sistemas de información basados en Web (WBIS) son sistemas de información específicos que toman ventajas de las tecnologías web, están integrados por cinco componentes principales: el sitio web, el sistema de procesamiento de negocios en línea, la gestión del conocimiento, la base de datos, y los agentes de software. Va mucho más allá de las oportunidades y los servicios ofrecidos por los sitios web mediante el apoyo a los procesos de negocio.
Teniendo en cuenta la necesidad de auditar este tipo de sistemas basados en Web, consideramos que se deben tener en cuenta dimensiones específicas en la forma y los medios para llevar a cabo dicho proceso de auditoría.

Auditoría para Sistemas de Información

El objetivo principal del auditor de sistemas de información es formular una opinión objetiva sobre la eficacia y la contribución de los sistemas de información a la empresa (Collier et al. , 1995). Su juicio puede ser influenciado por factores tales como su conocimiento sobre los sistemas de información de la

organización, y el grado de riesgo de cometer errores a través de esta evaluación. El propósito de una auditoría en tecnologías de información es evaluar los controles de TI (Mahnic et al., 2001), un auditor de TI evalúa y asesora sobre los siguientes aspectos de las tecnologías de la información: eficacia, eficiencia, exclusividad, etc (Hermanson, 2006). Se han propuesto un gran número de métodos de evaluación de los sistemas y tecnologías de información, así como de los WBIS, los que reciben una atención especial incluyen el cuadro de mando integral Balanced Score Card (Barrow et al., 2001), el método de desarrollo de sistemas dinámicos (Deschoolmeester et al., 2000), sistemas de simulación (Anderson, 2000), etc. Estos métodos son de carácter multidisciplinario, se basan en las teorías de evaluación tales como la teoría económica (Svavarsson, 2002), el enfoque interpretativo (Abu- Samaha, 2000), el enfoque crítico (Jones et al. , 2002), la teoría de la estructuración (Jansen et al. , 2004), la teoría de suelo (Jones et al., 2001), el enfoque de contingencia (Turk, 2000), la teoría de la opción (Svavarsson, 2002), y la teoría social (Berghout et al., 1996). La variedad de enfoques , tales como COBIT, ITIL, ValIT, etc. (ITGI, 2005) ilustra la falta de consenso (Chang et al, 2005;. Simonsson et al, 2007). Aunque no existe un entendimiento común sobre una teoría de evaluación adecuada hay tres conceptos principales que estructuran el proceso de auditoría (ITGI 2005): Procesos y dominios , criterios de auditoría, y el marco de la auditoría de sistemas de información.

Procesos y Dominios de los Sistemas de Información

Para asegurarse de que los sistemas de información están funcionando de manera eficiente y eficaz para ayudar a la organización a alcanzar sus objetivos estratégicos, se debe realizar un proceso de auditoría, esta tarea implica el análisis de los procesos de los sistemas de información. Las actividades individuales dentro de un sistema de información se pueden agrupar en procesos. El marco COBIT (ITGI 2005) identifica

34 procesos de tecnología de la información. Este último se agrupan en cuatro dominios (figura 1).

MONITOREAR Y EVALUAR
ME1 Monitorear y evaluar el desempeño de TI.
ME2 Monitorear y evaluar el control interno
ME3 Garantizar cumplimiento regulatorio.
ME4 Proporcionar gobierno de TI.
PLANEAR Y ORGANIZAR
PO1 Definir el plan estratégico de TI.
PO2 Definir la arquitectura de la información
PO3 Determinar la dirección tecnológica.
PO4 Definir procesos, organización y relaciones de TI.
PO5 Administrar la inversión en TI.
PO6 Comunicar las aspiraciones y la dirección de la gerencia
PO7 Administrar recursos humanos de TI.
PO8 Administrar calidad.
PO9 Evaluar y administrar riesgos de TI
PO10 Administrar proyectos.
ADQUIRIR E IMPLANTAR
AI1 Identificar soluciones automatizadas.
AI2 Adquirir y mantener el software aplicativo.
AI3 Adquirir y mantener la infraestructura tecnológica
AI4 Facilitar la operación y el uso.
AI5 Adquirir recursos de TI.
AI6 Administrar cambios.
AI7 Instalar y acreditar soluciones y cambios.
ENTREGAR Y DAR SOPORTE
DS1 Definir y administrar niveles de servicio.

DS2 Administrar servicios de terceros.
DS3 Administrar desempeño y capacidad.
DS4 Garantizar la continuidad del servicio.
DS5 Garantizar la seguridad de los sistemas.
DS6 Identificar y asignar costos.
DS7 Educar y entrenar a los usuarios.
DS8 Administrar la mesa de servicio y los incidentes.
DS9 Administrar la configuración.
DS10 Administrar los problemas.
DS11 Administrar los datos.
DS12 Administrar el ambiente físico.
DS13 Administrar las operaciones.

Fig. 1. Dominios y procesos de TI de acuerdo a COBIT 4.0

Los sistemas heredados (o Legacy), así como los sistemas de información basados en la Web incluyen tanto componentes técnicos como de gestión, las tareas de auditoría se pueden llevar a cabo a lo largo de las dimensiones relacionadas con los dominios de los Sistemas de Información (figura 2):

Dimensión de Gestión y Organizacional	**Dimensión Tecnológica**
Sistemas de información de planeación estratégica Sistemas de información funcionales (marketing, recursos humanos, logística, sistemas de información contable, etc.) Sistemas de procesamiento de datos y	Seguridad informática Operaciones de procesamiento de datos Aplicaciones actuales Nuevos proyectos de sistemas de información Costos de sistemas de información Compras y subcontratación

procedimientos de la organización Normas de contabilidad y regulación	Telecomunicaciones y sistemas de redes de cómputo

Fig. 2. Dominios de los sistemas de información.

Cualquier enfoque de auditoría se puede realizar en uno de los 34 procesos de COBIT o uno de los doce dominios descritos anteriormente.

Criterio de Auditoria

Para satisfacer los objetivos del negocio los sistemas de información deben cumplir con ciertos criterios que permitan medidas de control adecuadas. El conjunto de criterios considerados por las diferentes metodologías no son estrictamente equivalentes pero a menudo se superponen. En general, los criterios de auditoría son generalmente segmentada de acuerdo con tres puntos de vista (Nicho , 2008; Olsina et al, 2001):

- Los requisitos de calidad de productos que abarca, por ejemplo, la eficiencia y el rendimiento.
- Los requisitos de seguridad descritos en los criterios de coherencia, seguridad, conformidad y fiabilidad.
- Requisitos de legibilidad que comprende viabilidad, auditabilidad y la capacidad de evolucionar.

Marcos de referencia de Auditoría

Los marcos de auditoría de TI buscan cumplir el concepto de seguridad y permite la alineación de los objetivos de TI con los objetivos empresariales (Grembergen et al, 2005;. Yip et al, 2006) con el fin de satisfacer las necesidades de información del

negocio y los objetivos de las organizaciones. Los conceptos de dominios de sistemas de información y los procesos de TI, así como los criterios de auditoría juegan un papel central en el proceso de auditoría que permite a las empresas reforzar los objetivos de control interno. Se han propuesto varios marcos de control interno (o marcos de auditoría): COSO, COCO, Cadbury, COBIT y eSAC (Brown et al, 2005.). El marco COSO (COSO, 1992) ha sido diseñado para proporcionar seguridad respecto al logro de los objetivos de la información financiera y en el cumplimiento de las leyes y reglamentos. El marco COCO (COCO, 1995) es muy similar a COSO pero presenta conceptos adicionales no incluidos en COSO tales como los controles que permiten a los auditores identificar los riesgos en la capacidad de las organizaciones para explotar oportunidades. El marco de Cadbury (Cadbury, 1994) tiene como objetivo proporcionar una garantía de la disposición y el mantenimiento de registros contables adecuados. A diferencia de los tres marcos descritos anteriormente, el informe eSAC es el primer marco que tiene por objeto proporcionar "una buena orientación sobre el control y la auditoría de los sistemas de información y tecnología" (Stott, 2008).

En el contexto de la era del Internet, los nuevos sistemas de información basados en la web están diseñados, desarrollados e implementados con gran rapidez. Como consecuencia de ello, cada vez es más difícil de realizar auditorías eficaces de sistemas de información basados en la web utilizando metodologías tradicionales de auditoría tales como COBIT.

El proceso de auditoría de sitios web sólo está comenzando a hacer sentir su presencia más allá de la comunidad de investigación industrial, como se puede ver, hay muy pocos trabajos que tratan explícitamente la auditoría de los sitios web más allá de los aspectos de calidad. Se define a continuación un enfoque específico para la auditoría de un WBIS.

El objetivo de esta metodología es contribuir a la base de conocimientos existente en la evaluación de sistemas de información ofreciendo una metodología de auditoría basada en los dominios de los sistemas de información y los criterios combinados para formar un árbol jerárquico ponderado, esto permitirá:

- Reducir al mínimo el tiempo y los esfuerzos necesarios para llevar a cabo el proceso de auditoría. Esto sólo se puede lograr si la metodología tiene un modelo teórico subyacente (en nuestro enfoque es un modelo de análisis multicriterio jerárquico)
- Adaptar esta metodología a nuevas aplicaciones tales como sistemas de información basados en la web.
- Implementar una herramienta de auditoría asistida por computadora, lo que aumenta la eficacia y la eficiencia del proceso de auditoría.

La Auditoria de un sistema de información basado en Web – Un método basado en dominios

La característica fundamental de este marco, llamado INFAUDITOR, es que los dominios de auditoría y criterios de auditoría se pueden combinar para formar un árbol jerárquico que se define como un conjunto finito de nodos de tal manera que:
los nodos no terminales representan los dominios de auditoría y subdominios (por ejemplo, las aplicaciones heredadas, las aplicaciones basadas en web, metodología de desarrollo, las características del sistema y la documentación, la seguridad del sistema, el sistema de información de marketing , etc.), los nodos terminales representan dominios elementales a las que se deben aplicar las pruebas de control.

INFAUDITOR considera dos tipos de árboles:

- Un árbol general que abarque todos los ámbitos del sistema de información y pruebas de control.
- Varios sub- árboles que no son independientes correspondientes a la auditoría de determinados dominios de información del sistema, como un WBIS.

Cuando la auditoría de un dominio particular tal como en un WBIS, los pesos se atribuyen a los nodos del árbol en general, lo que lleva a un sub-árbol personalizado. Para cada prueba de control se da a los nodos terminales del sub-árbol un grado (o una apreciación cualitativa). Los pesos y las calificaciones que el auditor pueda determinar, resultará de diferentes dominios, dando lugar a una puntuación global de auditoría . Basándose en estas evaluaciones, el auditor puede escoger la opinión que mejor clasifica los sistema de información del cliente. La estructura del árbol jerárquico de auditoría se representa de la siguiente manera (figura 3), donde D indica dominio, SD para el subdominio, T para la prueba de control, G para el grado y W para el peso. Por ejemplo , la prueba de control T1 , 2 da como resultado un grado G1 , 2 , el dominio D1 puede entonces ser evaluada para W1 , 1 * G1 , 1 + W1 , 2 * G1 , 2 . Entonces la evaluación D1 se pondera por W1 en el grado de evaluación global.

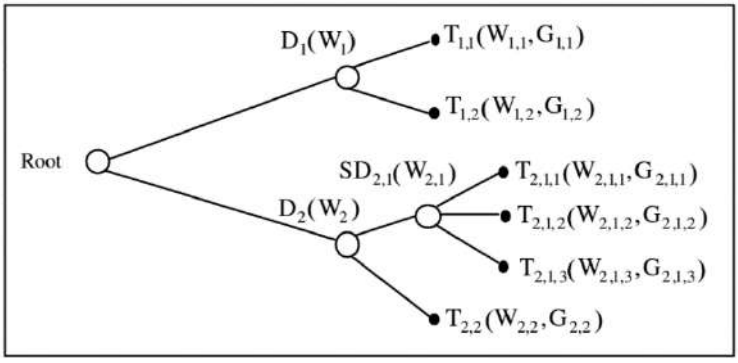

Fig. 3. Estructura del árbol jerárquico de decisiones.

Todos los resultados se dan en una escala cuantitativa. En cualquier nivel del árbol, la suma de los pesos de los hijos de un nodo es igual a 1. Los pesos de los nodos indican no sólo su participación en la evaluación final, sino también las pruebas que el auditor debe realizar.

El árbol de auditoría general es muy amplio, ya que el sistema de auditoría de información involucra a muchos dominios. Una originalidad de INFAUDITOR es que abarca todos los aspectos del sistema de auditoría de la información, mientras que otros métodos por lo general se centran tanto en los aspectos de gestión (marketing, recursos humanos, sistemas de información logística, etc.) o en los aspectos técnicos (red informática, la seguridad del sistema, las aplicaciones, nuevos proyectos, etc.) INFAUDITOR incorpora así el conocimiento de los diferentes ámbitos de sistemas de información.

El árbol de auditoría en general se lleva a cabo por las reglas. Para cada nodo del árbol (que representa el dominio o subdominio a auditar), una regla representa el vínculo entre este nodo y su padre. El manejo del árbol por las normas hace que sea fácil de mantener y favorece un enfoque de creación de prototipos. El enriquecimiento del árbol requiere sólo la adición de nuevas normas, sin tener que volver a escribir toda la estructura.

Esta capacidad de personalización a través de reglas es una importante contribución de INFAUDITOR. Este proceso de personalización se ha aplicado a los WBIS resultantes en la auditoría sub-árbol proporcionada a continuación (figura 4). Argumentamos que los tres criterios (calidad, seguridad, facilidad de lectura) mencionados anteriormente son adecuados para la evaluación de los WBIS. Estos criterios se han descompuesto en varios sub- criterios, teniendo en cuenta las características específicas de WBIS. La primera columna representa los criterios globales (calidad, seguridad, facilidad de

lectura). La segunda columna representa sus respectivos sub-criterios. Por ejemplo, la conformidad, la facilidad de uso, etc. son los sub -criterios de calidad. Este proceso de descomposición se repite para cada sub-criterio que conduce a la sexta columna.

Este enfoque de la auditoría puede ser utilizado en diferentes niveles de detalle (dominio, dominios sub-dominio, elementales) como herramienta de auditoría de los auditores y los usuarios finales (figura 4).

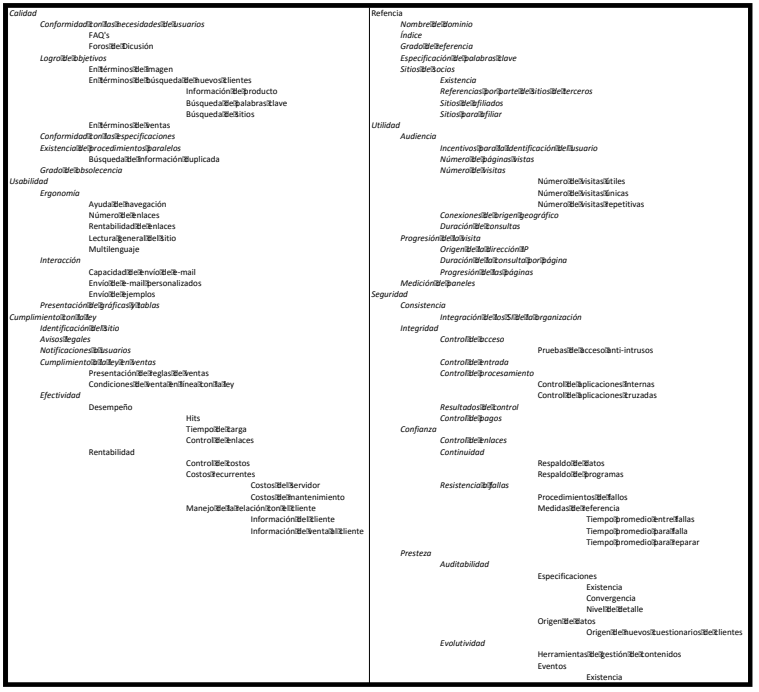

Figura 4. Árbol de auditoría de WBIS

CONCLUSIONES

La auditoría de sistemas web ofrece una importante ocasión de volver a evaluar la afirmación de que los marcos tradicionales de auditoría no son adecuados para la evaluación del sitio web. Hemos definido un enfoque basado en dominios para que los auditores realicen de forma eficaz y eficiente un proceso de auditoría de sitios web, tomándolo como un enfoque de ahorro de costos en la práctica de auditoría de WBIS. Con el uso de un proceso analítico jerárquico, el proceso de auditoría se estructura como un árbol jerárquico de evaluación, por lo tanto los controles de auditoría sólo se realizan en los nodos terminales, minimizando el tiempo y el esfuerzo necesarios para evaluar todo el dominio (recordemos que COBIT no tiene ninguna estructura jerárquica) por lo tanto, se deben realizar todas las pruebas de auditoría. Finalmente, nuestro enfoque ha sido ampliamente utilizado para auditar varios dominios que ofrecen una alternativa a COBIT. Una limitación fundamental de todo el enfoque de auditoría de WBIS tal como se presenta en este trabajo es la falta de consideración de las interdependencias entre los criterios. Estas interdependencias se pueden manejar mediante el uso de enlaces entre los criterios. Otra limitación es la falta de instrumento de orientación que permita a los auditores para decidir la mejor forma de proceder durante un proceso de auditoría, la forma de acceder a las explicaciones sobre lo que ha ocurrido durante las misiones de auditorías anteriores y la forma de acceder a la cada vez mayor información histórica que puede ser utilizada, por ejemplo al momento de decidir los valores que se asignan a los diferentes criterios. Por último, una limitación conocida es el relacionado con el proceso de jerarquía analítica subyacente de múltiples criterios de toma de decisiones.

REFERENCIAS

Akoka J., Comyn-Wattiau I. (2000) Auditing Computer and

Management Information Systems –Concepts, Methodologies and Applications, en Encyclopedia of Library and Information Science, Kent A. (Editor), Marcel Dekker, Inc. New York.

Atzeni P., Merialdo P., Sindoni G. (2002) Web Site Evaluation : Methodology and Case Study, DASWIS 2001, , Notas de lectura en Computer Science, N° 2465, Springer-Verlag, 2002.

Brown, W., Nasuti, F. (2005). What ERP Systems can Tell us about Sarbanes-Oxley. Information Management and Computer Security, 13(4), 311-327. Cadbury Report (1994) "Internal Control and Financial Reporting.

Champlain J.J (1998) Auditing Information Systems – A Comprehensive Reference Guide, John Wiley & Sons, Inc., New York.

Chang, J. C.-J., & King, W. R. (2005). Measuring the Performance of Information Systems: A Functional Scorecard. Journal of Management Information Systems, 22(1), 85-115.

Collier P., Dixon R., (1995) "The Evaluation and Audit of Management Information Systems", Managerial Auditing Journal, Vol. 10.

Danna E., Laroche A., (2000) "Auditing Web Sites Using Their Access Patterns", http://www9.org/final-posters/poster25.html, 9th WWW Conference, Amsterdam.

Deshpande Y., Chandrarathna A., Ginige A. (2002) "Web Site Auditing – First Step Towards Reengineering", Proceedings of SEKE'02.

Dewan R., Jing B., Seidmann A. (2000) "Adoption of Internet Based Product Customization and Pricing Strategies, Journal of Management Information Systems, Fall 2000, Vol. 17, N°2.

Grembergen, W. V., Haes, S. D., & Moons, J. (2005). Linking Business Goals to IT Goals and COBIT Processes. Information Systems Control Journal, 4, 18-22.

Hermanson, D. R. (2006). Internal Auditing: Getting Beyond The Selection 404 Implementation Crisis. Internal Auditing, 21(3), pp. 39-41. InDIMENSIONS Consulting Group, Web Site Audit, http://www.indimensions.com.

Lewin J., "Web Site Audit and Evaluation", http://www.lewingroup.com.

Nicho M. (2008) "Information Technology Audit: Systems Alignment and Effectiveness Measures", Ph.D Dissertation, AUT University.

Simonsson, M., Johnson, P., & Wijkstrom, H. (2007). Model Based IT Governance Maturity Assessments With COBIT. Paper presentado en la 15ª Conferencia Europea de Sistemas de Información, Suiza.

Singleton, T. W. (2006). COBIT- A Key to Success as an IT Auditor. Information Systems Control Journal, 1.

Wang S. (2001). "Toward a General Model for Web-Based Information Systems", International Journal on Information Management, Vol. 21.

LA UNIVERSIDAD Y SU RELACIÓN CON LA CIBERSEGURIDAD

Carlos Hernández Rodríguez[*], Milagros Cano Flores[&], Teresa García López[&]

INTRODUCCIÓN

Actualmente nuestro País enfrenta altos índices de inseguridad, lo cual origina a la sociedad mexicana una gran preocupación, pero se ha añadido a ese gran problema un motivo más para sentirnos inseguros, y es a través el uso del internet y redes sociales.

Debido a esta situación el Sistema Nacional de Seguridad Pública, a través de sus instancias competentes e instituciones de colaboración, se esfuerza por dar solución a los actos ilícitos que perturban la paz y tranquilidad social.

Cabe destacar, que el Sistema Nacional de Seguridad Pública es la encargada de planear y aplicar acciones que conlleven a una seguridad social, pero también es preciso resaltar que todos los ciudadanos como miembros activos de la sociedad también debemos contribuir al logro de las mismas. Sin embargo, hoy en día no solo estamos expuestos a un asalto, robo entre otro ilícito,

[*] Doctor en Administración y en Educación
[&] Doctora e Investigadora del Instituto de Investigaciones y Estudios Superiores de las Ciencias Administrativas
[&] Doctora e Investigadora del Instituto de Investigaciones y Estudios Superiores de las Ciencias Administrativas

si no que estamos expuesto al robo de datos que almacenamos en dispositivos que ahora son vulnerables.

Las instancias que se encuentran dentro del Sistema Nacional de Seguridad Pública, no deben ser las únicas promotoras de la seguridad, las universidades a través de su primordial función de formación académica, investigación y difusión en diferentes áreas del conocimiento pueden contribuir de manera significativa en la búsqueda de soluciones, en relación a la gestión de soluciones que conlleven a evitar ilícitos a través del uso de los desarrollos tecnológicos.

Prácticamente nada escapa a la digitalización y las personas, las empresas y las instituciones se ven abocadas a vivir y funcionar cada vez más en la red. Obviamente esto constituye un escenario de oportunidades de todo tipo, pero, también trae consigo nuevas amenazas relacionadas con la vulnerabilidad del usuario de la red.

El objetivo esencial de este trabajo consiste en mencionar la importancia de establecer un vínculo Universidad-Sociedad, para que en conjunto se elaboraren proyectos estratégicos que conlleven a entender y mejorar la Ciberseguridad.

¿QUÉ ES LA CIBERSEGURIDAD?

La ciberseguridad es el conjunto de herramientas, políticas, conceptos 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. [Unión Internacional de Telecomunicaciones (UTI), 2010).

El número y el grado de sofisticación de los ciberataques están aumentando al mismo tiempo que crece nuestra dependencia de Internet y de otras redes para obtener servicios e información críticos. De acuerdo con la compañía de seguridad McAfee, en 2011 se produjo el mayor número de amenazas descubiertas. Se supone que existen aproximadamente unos 70 millones de programas malware circulando en todo el mundo y los teléfonos inteligentes ("smartphones") se han convertido en el principal medio de su difusión. Los analistas consideran que al menos el 70% de los correos electrónicos son spam. Mientras tanto, las redes eléctricas inteligentes, la computación en nube, las redes de automatización industrial, los sistemas de transporte inteligentes, la ciberadministración y la banca electrónica, entre otros tipos de infraestructura, se están interconectando. (UTI, 2012)

Sin embargo, la mayor facilidad de conexión y la mayor eficacia en las comunicaciones traen consigo una mayor vulnerabilidad frente a los ciberataques. Aún no existe una definición de ciberseguridad aceptada en todo el mundo y ello obstaculiza los esfuerzos de protección que deben emprenderse a nivel nacional e internacional teniendo presente el carácter transfronterizo que tienen hoy en día las redes y sistemas informáticos. Para el año 2015 más del 60% de la Población mundial hace uso del internet, esto ha aumento significativamente los ataques cibernéticos, el robo de información, de identidad, entre otros.

El problema es que aunque el usuario presenta preocupación por su ciberseguridad, a menudo no es capaz de identificar cuáles son realmente los peligros y por tanto no sabe cómo enfrentarse

a ellos. Por ejemplo, gran parte de los internautas piensa que la mayor amenaza en la red es que te roben datos personales y las claves, pero el cibercrimen evoluciona constantemente, de forma que un atacante puede querer acceder a los recursos del usuario para aprovecharse del poder de procesamiento con el fin de realizar tareas que requieran gran poder de computación, o bien puede robarle su ancho de banda para que su sistema actúe como un zombi dentro de una *botnet* y poder realizar ataques masivos. (Rodríguez, 2016)

Por otro lado, el **Cloud Computing** se ha convertido en poco tiempo en una importante tendencia tecnológica, pero entraña numerosos riesgos relacionados con la seguridad, como la pérdida de control en el uso de las infraestructuras de la nube, la falta de garantía de la seguridad de los datos y las aplicaciones cuando se lleva a cabo la portabilidad a otro proveedor, los fallos de aislamiento, los problemas a la hora de realizar certificaciones externas de seguridad o calidad de los servicios de la empresa que opera en la nube o la exposición que supone el llevar a cabo la gestión de las interfaces a través de Internet. Por su parte, en el caso del **Big Data**, el almacenamiento y tratamiento de enormes cantidades de datos es en sí un riesgo para la seguridad, puesto que las filtraciones o robos de información pueden tener importantes efectos legales y reputacionales para una organización. (Rodríguez, 2016)

Por otra parte, actualmente las **apps** constituyen el medio preferido para conectarse a la red desde dispositivos móviles. Para valorar su importancia, es importante saber que el 90% del tiempo de conexión a Internet a través de un dispositivo móvil se destina a su uso y cada mes se lanzan al mercado unas 40.000 nuevas apps. La principal ciberamenaza en este caso es la capacidad que tienen de recolectar datos personales y de comportamiento lo que las convierte en un foco de posibles fugas de información que afecten a la privacidad del usuario. A esto hay que sumarle que su carácter global choca con las

distintas legislaciones sobre la protección de la privacidad que existen en los distintos países. (Molano, 2016)

Las soluciones de seguridad pueden pasar por el uso de software específico de privacidad en los teléfonos móviles, pero realmente resulta fundamental informar y concienciar al usuario sobre la adecuada gestión de su privacidad en las redes.

Hasta ahora se han visto una gran cantidad de ataques y tendencias que indican que los ataques M2M están a la alza, por lo que las preocupaciones por la seguridad del Internet de las Cosas están bien fundamentadas. Gartner ha estimado que 6.4 mil millones de nuevos dispositivos para el IoT se incorporarán al Internet durante el 2016. (Manky, 2016)

También podemos ver la posibilidad de que este tipo de ataques se expandan más allá del crimen informático para convertirse en terrorismo o guerra cibernética. De acuerdo con la Base de Datos Nacional sobre Vulnerabilidades (NIST), estamos en camino de ver un número, sin precedente, de CVEs (Vulnerabilidades Comunes y Exposición). La información más reciente de NIST sobre CVE muestra que cerca de 4.200 de vulnerabilidades comunes se han encontrado en software disponible al público, las mismas que ya han sido divulgadas y publicadas, por lo que nuestra predicción es que aún faltan muchas más por ser descubiertas. (Manky, 2016)

Así como los cibercriminales se vuelven objetivo de investigaciones y enjuiciamientos dentro del sistema de justicia criminal, los hackers que son cuidadosos han desarrollado una nueva variante de malware llamado 'ghostware', diseñado para cumplir con su misión y después borrar cualquier huella antes que las medidas de seguridad puedan detectar que el sistema ha sido comprometido.

Este tipo de ataques sobrepasan las técnicas y herramientas de prevención. La detección en tiempo real es esencial, ésta requiere un enfoque de arquitectura de seguridad integrada, que permita que los dispositivos compartan información sobre el ataque, en tiempo real, correlacionen y generen inteligencia de amenazas accionable y coordinen una respuesta para aislar el malware para, de esta manera, poder identificar todas las instancias del ataque desplegado en cualquier lugar de la red. (Manky, 2016)

Se esperan ver más ataques basados en 'Ghostware' que han sido rediseñados para explotar el doble desafío que representan, por un lado, el incremento en la brecha de habilidades de seguridad y, por el otro, los dispositivos aislados de seguridad heredada. (Manky, 2016)

De acuerdo con el estudio 'Market Pulse Suvey', el 69% de las personas que fueron alguna vez empleados pero ya no hacen parte de la nómina de las compañías, todavía tiene acceso a la información corporativa. Así mismo, un 83% de las personas que accede a las nubes corporativas también tiene instalado en sus dispositivos lo que se conoce como 'shadow IT', o tecnología sombra, que puede ayudar a resolver tareas cotidianas pero no cuenta con el aval del área TI.

Las cifras anteriores debieron activar una alarma de seguridad entre todos aquellos que valoran los datos de sus organizaciones, y no es para menos, cuando entre tanta información aquella que servirá para la toma de decisiones que agregarán valor a un negocio. (Molano, 2016)

Por lo tanto la Ciberseguridad es un tema que está cobrando relevancia y trascendencia y aunque para muchas personas, el término no es familiar aún, en poco tiempo quizás estemos

pagando a una empresa especial dedicada a la vigilancia de nuestra información en la red, tal y cual cuidaran nuestra casa.

LAS UNIVERSIDADES COMO GENERADORAS DE CONOCIMIENTO

El término universidad se aplicaba a toda comunidad organizada con cualquier fin, cuando los profesores de las escuelas formaron comunidades para proteger sus intereses, el término "Universidad" comienza a aplicarse por excelencia a las comunidades de profesores y estudiantes, se pasa de la escuela a la universidad como institución autónoma. El proceso de transformación fue gradual y se llevó a cabo de manera diferente para cada universidad. (Tunnermann, 2003)

La institución universitaria, durante su larga vida que se aproxima a los ocho siglos, ha sufrido profundas transformaciones a origen de los distintos movimientos culturales. La sobrevenida más importante a fines del siglo XVIII, fue la secularización de la enseñanza el Estado sustituyó a la iglesia en la alta dirección de la empresa docente. (Tunnermann, 2003)
La problemática actual se encuentra en el debate acerca de los fines de la universidad. En el siglo pasado se manifestó un fuerte contraste entre las instituciones educacionales inglesas y las del continente. Donde las primeras plasmaron el tipo humano, donde se dedicaron a la formación de la personalidad. En el continente, sobre todo en los países latinos, la universidad asumió la misión principal de conservar y transmitir los conocimientos y suministrar a la vez una sólida base para el ejercicio de las profesiones (abogados, médicos, ingenieros, farmacéuticos, entre otros) a cuyo fin expedía los correspondientes títulos.

Ambos ideales, la formación integral humana y la conservación del saber, pertenecen a las finalidades imprescriptibles de la

institución universitaria. Pero esta enfrenta ahora nuevas exigencias como consecuencia de la profunda transformación social a que estamos asistiendo. La mera transmisión del saber no satisface ya; a la universidad se le pide que promueva la obtención de conocimientos nuevos y contribuya al incesante incremento de la ciencia. Al empuje de esta necesidad, junto a las cátedras universitarias y a título de complemento obligado a ellas, se organizan seminarios y laboratorios en los que florece la especulación pura. Por esta razón la función investigadora ha pasado a ser primordial en la universidad de hoy. (Tunnermann, 2003)

Otro problema que ha de resolver la universidad de hoy es el de la fijación de sus fronteras, el progreso científico requiere de una creciente especialización. La vinculación usual entre función docente y la investigadora encauza esta antítesis hacia una solución; a la primera se le reserva la integración de los conocimientos en visión sintética y unitaria, en tanto que la segunda permite ahondar el análisis y la especialización hasta donde sea posible.

Las Universidades son instituciones de educación superior, centros con cierta complejidad organizativa, que integran diversas facultades de artes, ciencias y escuelas profesionales las cuales poseen autoridad para conferir títulos en varios campos del saber. Son organizaciones dedicadas a hacer avanzar el saber, que enseñan e investigan, esto es, generan, enseñan y difunden el saber.

En México, la universidad durante muchos años, se configuraba de acuerdo con el modelo francés, el cual tiene como ideal: (lograr la estabilidad política del Estado; su procedimiento es de una enseñanza profesional uniforme confiada a un cuerpo organizado; su función es crear un motor intelectual a través de una función asignada por la sociedad), sin embargo, el surgimiento de las universidades privadas y la incidencia es

éstas para cubrir la demanda laboral muestran indicios de un cambio radical en el esquema universitario, tanto en sus ideales como en sus procedimientos.

A partir de 1968 hay una búsqueda por la democratización en la que se pretende una mayor participación de los alumnos en las decisiones. Un giro en la conformación del sistema universitario lo ha dado el hecho de que el gobierno va perdiendo papel protagónico en su financiamiento, así como en sus funciones, orientación y control, y va ganando terreno la autonomía en la generación y difusión del conocimiento en el nivel superior dentro de la enseñanza formal.

Los sistemas universitarios actuales tienen una marcada tendencia a la especialización que se acentúa que se acentúa por el gran auge que se le da a la actividad económica y al individualismo, el cual deriva un espíritu utilitarista; sin embargo, por otro lado ¿existe un ansia por saber y entender el todo que rodea al hombre, lo que puede propiciar el mantenimiento de la idea de una formación más generalizada y una enseñanza de carácter holístico a pesar de la tendencia a hacer de las universidades entidades generadoras de profesionistas que surtan la demanda del carácter laboral. (Tunnermann, 2003)

La universidad pública, considerada como una institución eminentemente cultural, tiene como metas la producción y transmisión de formas de saber, y la formación de intelectuales (profesionales e investigadores) con conciencia crítica y posición activa sobre su desempeño social, lo que responde así a los intereses globales de amplios sectores de la nación, y no sólo a los del gobierno o la empresa. (ANUEIS, 2014)

El conocimiento forma parte de la realidad. El conocimiento puede generarse dependiendo del contexto donde esté involucrada un problema en particular. Esa realidad puede ser

entendida dependiendo de la formación del investigador o disciplina desde donde se estudie el problema. En la generación del conocimiento, juega un papel importante el contexto donde esté involucrada la realidad, y de acuerdo a los resultados obtenidos de puede actuar en lo social, lo cultura, lo económico y lo histórico, tratando de obtener un beneficio colectivo.

Por ello la Universidad está obligada a generar conocimiento que permita administrar en forma eficaz la información almacenada en la red, pero también a desarrollar programas que permitan contrarrestar una amenaza cibernética, si bien es cierto que en las universidades se han formado individuos que han provocado el avance de la tecnología, hay otros que han desarrollado su conocimiento de manera informal.

Por lo anterior, la gestión del conocimiento es una toma de conciencia del valor del conocimiento como recurso y producto en la sociedad. El conocimiento es uno de los valores más preciados que pueda tenerse y buscarse. No debemos olvidar que esta búsqueda y hallazgo se dio en primer lugar en las organizaciones empresariales. En ellas se reconoce la necesidad imperante de acelerar flujos de información desde los individuos hacia la organización y vice-versa con la intensión de producir un valor agregado para la organización. La información se convierte a través de los individuos en un activo de conocimiento para la organización y éste, a su vez, en un "activo de capital humano" (Minakato, 2009).

LA UNIVERSIDAD Y SU RELACIÓN CON LA CIBERSEGURIDAD

El primer problema de este tema, es la conceptualización del término seguridad al que se le han intentado agregar campos que no le corresponden. La Seguridad Pública, es la función a cargo del Poder Ejecutivo, mediante la cual, a través de acciones

efectivas de información, disuasión y actuación firme, se logra la prevención de conductas delictivas, garantizando con ello, la tranquilidad e integridad de cada uno de los integrantes de la sociedad. Esta función forma parte de todo un sistema penal, que involucra diversos sectores y a los tres poderes de la Unión, en el afán de combatir el delito y castigar a sus autores. (Aguayo, 1999)

La Seguridad Pública es tan sólo una de las funciones concretas que tiene a su cargo el Ejecutivo para prevenir los delitos, más no la única. Quinientos años antes de Cristo, Confucio escribió lo siguiente: "Cuando se le conduce al pueblo mediante disposiciones y órdenes administrativas, y cuando por medio de castigos se procura meterle en razón, ciertamente que el pueblo evitará los delitos, mas no tomará conciencia de que la comisión de delitos es algo de lo que tiene que avergonzarse. Cuando mediante la fuerza de unos principios morales se le guía exteriormente hacia el bien y se vinculan sus actividades externas a un extenso catálogo de formas de comportamiento ritualizadas, entonces tendrá el sentimiento de vergüenza, se apartará del mal y marchará por el camino correcto". (Aguayo, 1999)

> La Doctrina de la Seguridad Nacional tiene sus orígenes en la necesidad que el gobierno tiene de evitar problemas en la conducción del país. (CNS, 2015)

La educación, es uno de los medios por excelencia para enseñar normas y valores a las personas para alejarlas del delito, es un elemento fundamental para transmitir de manera implícita en los planes curriculares de las instituciones educativas, una cultura de valores que propicie en los sujetos una participación sólida ante su sociedad, en aspectos relativos a la sociedad.

Dentro de la seguridad pública, también ha existido una adaptación a las nuevas formas de delito que se pude cometer en la sociedad, y es a través del uso de recursos tecnológicos, mejor llamados "cibernéticos", por lo tanto, los Gobiernos han tenido que diseñar estrategias para proteger a la sociedad de ilícitos que cada vez más se dificultad en atrapar al delincuente, pues ahora se enfrentan a entes digitales, que pueden provocar un problema de seguridad estando a miles de kilómetros donde se cometió el delito. (CNS, 2015)

Por lo anterior, la educación no escapa de los continuos avances tecnológicos, y aunque mucho se ha mencionado del divorcio o alejamiento de la educación formal con estos desarrollos, definitivamente la afectan positiva o negativamente. Hoy en día la educación está rodeada de un nuevo lenguaje y de nuevas modas presentes en los hogares, en las calles, en las escuelas etc., en pocas palabras, la forma o manera de educar ha cambiado de un momento histórico a otro.

Hacemos reflexión consiente de la función de la Seguridad Pública y del impacto que tiene en la sociedad mexicana respecto a la carencia de ética, métodos y compromisos en el cumplimiento de su función. Se hace indispensable pensar que la Universidad es una instancia alternativa para que a través de su función y servicio establezca un vínculo de la Seguridad Pública desde nuevos paradigmas de formación disciplinaria en el área específica de este sistema y también inmiscuir a las que no están en relación directa al área.

Partimos de que las funciones sustantivas de la Universidad son la docencia, la investigación, la difusión de la cultura y extensión de los servicios y que se realizarán a través de las entidades académicas, se desprenden las siguientes propuestas como apoyo y promoción a la Ciberseguridad:

- Las Universidades, establezcan convenios con las instancias de seguridad pública, para determinar a través de qué acciones la primera puede promover a la segunda.
- Formar los recursos humanos necesarios para hacer frente a los problemas de seguridad cibernética.
- Elaborar programas estratégicos de comunicación, concientización, capacitación y servicio social a la comunidad universitaria, para inmiscuirla desde su formación a participar en las funciones de Ciberseguridad
- Ubicar a prestadores universitarios de servicio social en actividades de ciberseguridad, de acuerdo a las especialidades disciplinarias del sistema y a aquellas que desempeñen actividades relativas al mismo.
- Las Universidades, de acuerdo al área disciplinaria de la Seguridad Pública, pueden organizar cursos de especialización que sean necesarios de cubrir competentemente en las dependencias de seguridad, así mismo cursos y diplomados, que fomenten en los sujetos una mayor preparación en el áea de ciberseguridad.
- Que la Universidad conciba en su función, no sólo formación disciplinaria del área de especialización, sino que promueva una dimensión integral en la formación de los universitarios, no precisamente en lineamientos establecidos dentro del curriculum formal, sino a través de la promoción de valores respecto a la participación en la seguridad pública, donde intervenga la labor conjunta de la comunidad universitaria (Directivos-Docentes-Estudiantes).

CONCLUSIONES

Cada época ha tenido distintos problemas que resolver, y hoy en día la preocupación de las empresas no es directamente relacionada con la inversión en infraestructura, compra de maquinaria y equipo, de capacitación, manejo de inventarios, entre otros, sino en cómo cuidar la información que se tiene

almacenada en la red, en cómo evitar el robo de identidad y lo más complejo, cómo estar al margen de un desvío de dinero.

Al hablar de Ciberseguridad, casi de inmediato se asocia el concepto de "amenaza". Si hasta hace poco tiempo, la mayor preocupación era proteger algún bien, pero hoy cambia y la prioridad es prevenir los riesgos de ataques cibernéticos.

El ciberespacio tiene una característica jamás nunca vista hasta ahora, que es la exposición. Esa inmensa capacidad de comunicación y de acceso, de intercambio de información con otros individuos y empresa, es un doble problema. Los mismos procesos y las mismas tecnologías pueden dar lugar de igual modo a un nuevo negocio o a una nueva amenaza, alcanzando miles de millones de potenciales clientes o de potenciales víctimas.

Cuando inicio el uso de internet, primero en lo militar y después en la educación, pocas personas aventuraron a pronosticar el gran riesgo que existe por el uso, intercambio, manipulación, compra de información, en realidad no hay privacidad en la red,

La universidad puede y deben jugar un papel importante en la vinculación con la Ciberseguridad, primeramente haciendo conciencia en las personas sobre los riesgos que hay en la red, y después desarrollando conocimiento que permita hacer frente a estas amenazas.

BIBLIOGRAFÍA

Aguayo Quezada, Sergio. *Los usos, abusos y retos de la Seguridad Nacional Mexicana. 1946-1990.* Artículo en el libro *En busca de la seguridad perdida.* Siglo XXI Editores. Primera Edición, 1990. México.

Bunge, M.(2006). La ciencia, su método y su filosofía. México. Nueva Imagen.

Manky Derek (2016). Más ataques y mayor sofisticación, Artículo recuperable en https://colombiadigital.net/actualidad/articulos-informativos/item/9260-mas-ataques-y-mayor-sofisticacion.html.

Minakato Arceo Alberto (2009). "Gestión del conocimiento en educación y transformación de la escuela. Notas para un campo en construcción", en *Sinéctica, revista electrónica de educación*, núm. 32, enero-junio de 2009, ISSN 1665-109X

Molano Adriana (2016). Datos en riesgo: la solución preinstalada en la mitad de los dispositivos del mundo. Archivo recuperable en https://colombiadigital.net/actualidad/articulos-informativos/item/9242-datos-en-riesgo-la-solucion-preinstalada-en-la-mitad-de-los-dispositivos-del-mundo.html

Rodríguez Cafranc Pablo (2016). Ciberseguridad, cómo proteger la información en un mundo digital, Artículo Recuperables en http://blogthinkbig.com/ciberseguridad-como-proteger-la-informacion-en-un-mundo-digital/. Consultado el 20 de octubre de 2016.

Tunnermann Bernheim Carlos (2003). La Universidad Latinoamericana antes los retos del siglo XXI. Colección UDUAL, México.

Páginas web consultadas

http://www.cns.gob.mx (2015)

http://www.itu.int/net/itunews/issues/2010/09/20-es.aspx

PANORAMA GENERAL DE LA CIBERSEGURIDAD INTERNACIONAL Y NACIONAL

Antonio Berdeja Rivas
Ignacio Olivares Linares

INTRODUCCIÓN

Hoy hablar sobre temas referentes a la Ciberseguridad en México nos obliga a realizar una revisión de los casos y los probables autores de estos sucesos, no sólo para conocer y adoptar los muy sofisticados sistemas de seguridad, sino también para estar preparados ante ataques que cada vez serán más poderosos y con consecuencias graves. Particularmente porque México se encuentra en una posición débil tanto en materia tecnológica como legal.

De ser verdad que, muchos de los poderosos hackers del ciberespacio están obedeciendo a intereses políticos que en el fondo son una guerra silenciosa contra las grandes corporaciones no sólo del ámbito tecnológico, sino también financieras y principalmente, contra las grandes potencias del mundo occidental. Si bien es cierto que a finales de los años 80s del siglo pasado terminó la denominada guerra fría, surgieron nuevos esquemas de lucha por el poder global, en este sentido las nuevas tecnologías de la información, junto con las redes sociales, han jugado un papel fundamental. La información sigue siendo un elemento clave de poder, los datos intangibles se han convertido en grandes tesoros mundiales, y la idea de apoderarse de ellos o destruirlos es la nueva guerra fría o soft (suave) de estos últimos años.

Tan sólo hace una semana los medios de información daban cuenta del ciberataque más grande ocurrido en los últimos 10 años. Pablo David Livsit calificó así este episodio: "Un ataque cibernético golpeó a algunos de los gigantes de internet y afectó

las operaciones de varios sitios como Twitter, Netflix, Spotify, The New York Times y The Guardian.
"El ciberataque contra el proveedor de infraestructura de internet Dyn interrumpió el servicio en importantes firmas afectando sobre todo a usuarios en la Costa Este de Estados Unidos.

"No quedó claro quién es el responsable. Funcionarios dijeron que el Departamento de Seguridad Nacional y la Oficina Federal de Investigaciones (FBI) están investigando "todas las posibles causas" del ataque.

"Los sitios de Airbnb, Spotify, Soundcloud, The New York Times, The Guardian y Vox Media también se vieron perturbados en sus servicios.

"Por otro lado, aunque los investigadores expertos en seguridad se apresuraron a ponerlo en duda, seguidores de WikiLeaks también se atribuyeron el ataque: el grupo Anonymus dijo que estaba detrás del 'apagón', indicando que lo hacía en respuesta a la decisión del gobierno de Ecuador de cortar el acceso a internet a Jualian Assange, fundador de WikiLeaks." [3]

Sin embargo, días después se publicó la siguiente información en otros medios de información digital: "La empresa china Hangzhou Xiongmai, fabricante de webcams y reproductores DVD, se ha responsabilizado de la caída masiva de internet ocurrida el pasado viernes (21 de octubre).

"A través de un comunicado, los representantes de la compañía explicaron que sus productos habían sido infectados con el

[3] Pablo David Livsit, periodista con un posgrado en Periodismo Digital, su portal informativo se denomina "Tecnología sin Fronteras".

malware Mirai, el causante del ciberataque, para ser utilizados en el ataque contra los servidores DNS de Dyn.
"Con el ataque a los servidores, se generó la caída de sitios como Twitter, Amazon, Spotify y Netflix, entre otros. El problema fue ocasionado debido a que los usuarios de las cámaras web no hicieron el cambio de la contraseña preestablecida.
"Buscando evitar un ataque similar, Hangzhou Xiongmai pedirá a los usuarios devolver los primeros productos que estaban disponibles en Estados Unidos, mientras que para los productos hechos antes de abril de 2015 se liberará un parche que solucionará el problema de seguridad.

"Aunque la solución propuesta por Hangzhou pretende solucionar una parte del problema, esto no evitaría que se vuelva a repetir un escenario similar a futuro. Días antes del ataque, fue publicado en la red el código de hackeo Mirai, desde ese entonces, expertos en seguridad informática han rastreado varios intentos de reactivarlo. El proveedor de servidores Dyn aseguró que al menos 10 millones de direcciones IP estuvieron relacionadas con el ataque."

Aunque el pasado 23 de octubre, el diario digital paraguayo La Nación, publicó que "El grupo de hackers 'New World Hackers´, distribuidos en China y Rusia, se adjudicó la responsabilidad por el ataque al proveedor de internet Dyn. Mediante un mensaje de Twitter, ´New World Hackers' explicó que el ciberataque se hizo a través de las redes de computadoras 'zombies' (como refrigeradores y lavadoras inteligentes, y otros enseres hoy dotados de sistemas de cómputo) que lanzaron en simultáneo 1,2 terabits de datos por segundo a los servidores gestionados por Dyn, firma que ofrece servicio en EEUU a compañías como Twitter, Spotify y medios de comunicación como CNN y The New York Times.

Al respecto los atacantes, de acuerdo a dicha nota informativa, dijeron: "No hicimos esto para atraer a los agentes federales,

sólo para probar nuestro poder", así lo declararon dos miembros del grupo de piratas informáticos, identificados como "Profeta" y "Zain".

Así este ataque fue tan sólo hace unos días y aunque no ha habido mayor información que permita ratificar o acusar a dichos personajes y confirmar si la empresa china fabricante de cámaras web fue la responsable de este grave "descuido", lo cierto es hoy estar cada vez más atentos a estos sucesos para que a partir de ellos podamos encontrar una posición de equilibrio para nuestro país. Es decir, se debe crear mayor conciencia en los usuarios de estas tecnologías en nuestro país, puesto que los atacantes sólo están esperando un descuido o una provocación para que de inmediato inicie un ataque.

Javier Arreola, hace unos meses escribía para Red Forbes "¿qué es la ciberseguridad y qué tan importante es? La seguridad cibernética (o ciberseguridad) se refiere a la protección de las computadoras, redes, programas y datos contra el acceso o modificación no deseada o no autorizada. Para ello se utilizan herramientas, políticas, medidas de seguridad, directrices, enfoques de gestión de riesgos, acciones de formación, conceptos de seguridad, mejores prácticas e incorporación de tecnologías (Danilak & Thomas, 2016).

Areola informaba que el valor en juego de la información es cada vez más grande. De acuerdo con Brand Financer, de los 71.0 billones de dólares (trillions, en inglés) que concentran las 58 mil compañías más valiosas del mundo, 37.5 billones –más de la mitad– son activos intangibles como propiedad intelectual o información que están almacenados en computadoras. Más aún, el Foro Económico Mundial espera que robustecer la protección en contra de los riesgos cibernéticos podría añadir hasta 22 billones de dólares (trillions, en inglés) a la economía antes del 2020. (Jessop & Kerber, 2015)."

Coincidimos con Arreola cuando indica que desafortunadamente, como consecuencia del siempre cambiante y complejo entorno tecnológico, de los inevitables descuidos humanos, y de la continua sofisticación de los ciberataques, no existe alguna protección infalible para estar 100% seguros en la internet. Ni las compañías más grandes del mundo, ni los gobiernos de las economías más grandes podrán evitar ser víctimas de ataques cibernéticos.

Ya en el año 2015 algunos expertos en la materia visualizaban que conforme las organizaciones y los países engrosan sus defensas digitales, los cibercriminales siguen desarrollando maneras más sofisticadas y elaboradas de poder penetrar hasta las infraestructuras tecnológicas más robustas. Además hoy se está generalizando la idea de que algunos de los ciberatacantes son parte de programas del gobierno, es un hecho que a cualquier compañía le va a resultar imposible prevenir un ataque cibernético desarrollado con los casi ilimitados recursos del gobierno. Esta idea de Arreola, nos hace recordar lo que en los años 70 y 80s cuando era creciente los ataques terroristas, que se trataba de un Terrorismo de Estado, es decir se sospecha de la abierta participación de gobiernos en estos operativos, cuyo efecto era doblemente magnificado al tener como cámara de resonancia a los medios de comunicación.

Para el caso de los ciberataques, la razón puede ser porque criminales, terroristas y países que quieren dañar a otros individuos, organizaciones y naciones han comprobado que es más sencillo hacer daño al adversario atacando vía cibernética que de manera presencial. Es decir, como sosteníamos al inicio, los tesoros intangibles son el blanco favoritos de ellos.

Tan sólo el año pasado, refiere el propio Arreola, 594 millones de personas en el mundo fueron víctimas de la ciberdelincuencia, lo cual ha orillado a varios gobiernos a tomarse en serio el asunto. Pero el continuo cruce de fronteras tecnológicas y los

dilemas éticos que este tema presenta hacen que los gobiernos participen igualmente en la protección de ataques cibernéticos a sus ciudadanos e instituciones, que desarrollen programas de hackers cuya función es romper encriptaciones de países adversarios o espiar la actividad en línea de ciudadanos considerados sospechosos.

Por ejemplo, el presidente estadounidense ha creado la posición de "Jefe de Seguridad Informática de la Casa Blanca", quien se encargará de endurecer la seguridad informática interna de las agencias federales, así como de modernizar los sistemas de tecnologías de la información del gobierno federal. También ha establecido la Comisión Nacional para la Mejora de la Ciberseguridad, que hará recomendaciones de acciones que se puedan tomar la próxima década para proteger la privacidad y mantener la seguridad pública, así como otros datos de seguridad nacional. Todas estas acciones son parte del Plan Nacional de Ciberseguridad, que en caso de que lo apruebe el Congreso, expandiría el presupuesto del rubro a 19 mil millones de dólares. (Calmes, 2016)

Por otro lado, el mismo Congreso estadounidense acaba de aprobar la controvertida Ley de Seguridad Cibernética e Intercambio de Información (CISA, por sus siglas en inglés), bajo la cual se compartiría información privada de ciudadanos con compañías contratistas, agencias de investigación, espionaje y criminalidad, y se seguiría a ciudadanos sospechosos de cometer delitos. Esta ley fue combatida fuertemente por los cabilderos de Amazon, Apple, Dropbox, Google, entre otras empresas tecnológicas. (Caldwell, 2016)

En años recientes, el Ejército Popular de Liberación (PLA, por sus siglas en inglés) de China ha invertido grandes recursos en su departamento especial de ciberinteligencia, que no solamente realiza vigilancia y espionaje avanzado, sino que posee malware capaz de destruir infraestructura de interés nacional como redes

de distribución eléctrica e hidráulica en el extranjero. (Stone, 2013).

Con respecto a Rusia, se sospecha que tiene ciberarmas aún más avanzadas que las del gobierno chino. La milicia rusa también cuenta con unidades especiales dedicadas al ciberespionaje, que además de hacer espionaje para robar secretos de otros países, complementan a su ejército en ataques de guerra. En el 2014, Rusia utilizó ataques de denegación de servicio distribuido (DDoS, en inglés) para apagar las comunicaciones móviles de Ucrania, previo a comenzar un ataque tradicional de campo de batalla (Weedon & Galante, 2014).

Cabe destacar que el Servicio Federal de Protección ruso compró en 2013 cientos de máquinas de escribir que se usan para salvaguardar las comunicaciones entre el Kremlin y el presidente. El objetivo es evitar la fuga de documentos, ya sea por parte de su personal o por parte de hackers. Cada máquina de escribir ha sido modificada para que tenga un patrón único que permite identificar rápidamente los documentos que produce. Eso sí, este sistema no está exento del robo o fotografía de papeles, ni de incendios. (Irvine, 2013)

Al ser un país emergente con una amplia población, México ha incrementado significativamente su acceso a banda ancha e internet. Es preocupante que los cibercrímenes han crecido aún más rápido, y un factor clave es la pobre educación cibernética de la población y sus organizaciones. De acuerdo con estimaciones de Symantec, el 40% de los internautas mexicanos, unas 54.9 millones de personas, ha sufrido al menos un crimen.

De ellos, el 58% de los delitos son suplantación y robo de identidad, seguidos por el 17% por fraudes y el 15% por hackeo. Todo esto convierte a México en el tercer lugar mundial en crímenes cibernéticos, después de China y Sudáfrica. De acuerdo con la Comisión Nacional de Seguridad, en los últimos 5 años,

el 53% de los ataques fueron contra dependencias gubernamentales, 26% contra recintos académicos y 21% contra el sector privado. (López, 2016)

¿Qué es el robo de identidad?

Cuando alguien roba tu información personal y financiera, con la finalidad de suplantar tu identidad para obtener beneficios de forma fraudulenta, se dice que comete robo de identidad.

Tus datos pueden ser utilizados para solicitar créditos o usar los que ya tienes de forma exagerada, crear cheques falsos con tu número de cuenta e incluso obtener a tu nombre algún documento oficial. Cuando esto sucede, no sólo pierdes dinero, también se daña tu reputación financiera. Si solicitan un crédito a tu nombre sin que te des cuenta y por consiguiente nunca se paga, esto dañará tu historial crediticio y es probable que en el futuro las instituciones financieras te nieguen algún crédito. En casos más graves puedes tener problemas con las autoridades, derivados de algún fraude o infracción que el ladrón cometa a tu nombre.

Por lo general, a las víctimas les lleva mucho tiempo darse cuenta de que su identidad ha sido robada y cuando se percatan del fraude, el ladrón ya ha hecho estragos.

En México, el delito de robo de identidad va en aumento día con día, según datos del Banco de México, nuestro país ocupa el octavo lugar a nivel mundial en este delito; en un 67% de los casos, el robo de identidad se da por la pérdida de documentos, 63% por el robo de carteras y portafolios, y 53% por información tomada directamente de una tarjeta bancaria.

Comúnmente, el delito de robo de identidad se usa de manera ilegal para abrir cuentas de crédito, contratar líneas telefónicas, seguros de vida, realizar compras e incluso, en algunos casos,

para el cobro de seguros de salud, vida y pensiones. Al respecto se debe escuchar las diversas recomendaciones que sobre este tema en su oportunidad ha emitido la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF).

México también es el segundo lugar mundial con más ataques tipo phishing, que es el intento de adquirir información sensible mediante comunicaciones electrónicas. Esto no es de extrañar debido a que apenas el 35% de los mexicanos usan contraseñas seguras y además comparten datos sensibles con mucha facilidad. Muchas veces nos causa una terrible pereza modificar desde nuestro NIP en los cajeros electrónicos o elaborar contraseñas más complejas para asegurar nuestros datos personales.

La Policía Cibernética, perteneciente al área de seguridad del gobierno, es la principal unidad de combate al cibercrimen. Además, el Instituto Politécnico Nacional cuenta con el único equipo de especialistas digitales forenses en México, así como con el Centro de Investigación en Computación, que desarrolla sistemas para proteger la transmisión de la información digital. (Notimex, 2015)

Dependencias como Gobernación, Seguridad Pública y la Procuraduría General de la República informaron haber sido blanco de ataques orquestados por delincuentes cibernéticos que intentaron y a veces lograron penetrar sus defensas, pese a que hay secretos de Estado en sus redes.

Incluso la Presidencia de la República aceptó no ser inmune y advirtió que el gobierno federal se encuentra en riesgo frente a un "arsenal de armas" virtuales en manos de bromistas así como la delincuencia común y organizada.

Gobernación admitió que los ataques cibernéticos que se han presentado se limitan a peticiones múltiples a los sistemas informáticos, aunque insistió en que este tipo de agresión "no representa un riesgo" para la seguridad informática de Bucareli.

Un total de 106 equipos en la dependencia, que tiene conexiones con áreas tan sensibles como el Centro de Investigaciones sobre Seguridad Nacional (CISEN) y el Instituto Nacional de Migración, han sido infectados con programas dañinos.

En tanto, la Secretaría de Seguridad Pública repuso que en mayo de 2009, registró un récord de 509 ataques a sus servidores, mientras que la Procuraduría General de la República admitió haber detectado una infección con el virus klif, un spyware capaz de retransmitir información de una computadora a otro usuario. La PGR sostuvo que su información es altamente protegida porque, de ser penetrada por terceros, "la delincuencia puede tener acceso directamente a los bancos de información, a fin de manipular, destruir total o parcialmente y descargar los datos reservados y confidenciales".
La Presidencia de la República clasificó como reservada por 12 años toda la información referente a ataques a sus servidores, los más visitados dentro de todo el gobierno federal.

En los Pinos argumentaron que dar a conocer información sobre el número de ataques a sistemas informáticos, terminales de cómputo, servidores y redes, así como cuántas computadoras han sido infectadas "comprometería la seguridad y la defensa nacional".

"Esta información se encuentra clasificada como reservada", expuso la Presidencia, que se amparó en los artículos 15, 16 y 17 de la Ley Federal de Transparencia para negar los datos, bajo el argumento de que revelarlos "proporcionaría información respecto de las vulnerabilidades de la red institucional".

Sobre la situación de la Ciberseguridad en México, Daniel Kapellmann y Benjamín Reyes, difundían recientemente que según el reporte "Tendencias de Seguridad en América Latina y el Caribe" de la Organización de los Estados Americanos (OEA), tan sólo en México los costos anuales generados por ciberdelitos en 2014 ascendieron a $3,000 millones de dólares, afectando al sector público, privado y civil. Los riesgos en materia de seguridad cibernética que fueron denunciados incluyen desde malware, phishing y hackeos, hasta incidentes de fraude y extorsión, difamación, amenazas, robo de contraseñas, suplantación de identidad y acoso.

Si bien ya existen esfuerzos a nivel nacional para impulsar este tipo de seguridad, como la creación del CERT-MX (Equipo de Respuesta a Incidentes de Seguridad Cibernética) o la operación de la División Científica de la Policía Federal, entre otras cosas, México aún sigue rezagado en este tema con un creciente impacto negativo. De acuerdo con el "Índice Global de Seguridad 2014" liberado a inicios del año en curso por la Unión Internacional de Telecomunicaciones (UIT), el país cuenta con un bajo nivel de preparación ante ciberamenazas.

Este reporte evalúa la respuesta general de más de 100 países ante la inseguridad cibernética, utilizando una escala de evaluación entre 0 y 100 puntos. De este modo, cada país cuenta con una calificación que puede repetirse, derivando en un ranking con 29 posiciones, entre las cuales México ocupa la 18, a la par de Perú, Vietnam y Burkina Faso.

México cuenta con una calificación global de 32.4 sobre 100, lo cual implica que se encuentra 12.3 puntos por debajo del promedio global. A nivel Latinoamérica, esto implica que México se encuentra por encima de países como Paraguay y Venezuela, pero muy por debajo de otros como Brasil, Uruguay, Argentina, Costa Rica, Chile y Colombia.

En específico, el Índice Global de Ciberseguridad se centra en cinco principales indicadores o áreas, que son las medidas legales, técnicas, orgánicas, capacitación y cooperación tanto nacional como internacional.

Daniel Kapellmann y Benjamín Reyes, aseveran: "Las principales fortalezas de México se encuentran en las medidas técnicas, mientras que su principal debilidad son las orgánicas. Esto indica que se cuenta con algunas instituciones y marcos técnicos de ciberseguridad, incluyendo equipos contra incidentes cibernéticos, pero se no cuenta con una planificación y estructuras orgánicas que promuevan la implementación de medidas de este tipo de seguridad entre distintos sectores e instituciones."

Aunado a lo anterior México registra bajos niveles en materia de marcos legales e instituciones encargados de tratar la seguridad en línea, así como en programas de capacitación, certificación, desarrollo de profesionales y certificación de organizaciones de carácter público en esta materia. Este patrón se refleja nuevamente en una falta de mayor desarrollo en materia de marcos para cooperación nacional e internacional y redes de divulgación de información.

Ante esta situación México debe trabajar más en la búsqueda de estrategias articuladas, donde haya una planeación a fondo para hacer de las redes sociales y demás tecnologías digitales, espacios de crecimiento y desarrollo que tanto necesita nuestro país.

Asimismo, debemos alejarnos de blanco concéntrico que buscan los hackers y nuevos luchadores sociales internacionales que buscan la menor provocación para lanzar sus ataques planeados y destructivos. Las razones o sin razones de estos atacantes también es porque buscan decirnos algo que posiblemente no está bien según la óptica de ellos, debemos agradecer que al

menos en lo que va de este Congreso Internacional de Ciberseguridad, no hayamos tenido, ni lo deseamos, al menos un apagón.

Trabajos citados

— Arreola, J. (26 de abril de 2016). Padrón electoral en la nube: ¿ciberproblemas a la mexicana? Obtenido de Forbes México.
— Caldwell, G. (07 de febrero de 2016). Why You Should Be Concerned About The . Obtenido de TechCrunch.
— Calmes, J. (09 de febrero de 2016). Obama's Last Budget, and Last Budget Battle With Congress. Obtenido de The New York Times.
— López, J. (07 de febrero de 2016). Cibercrimen ataca a 40% de internautas mexicanos. Obtenido de El Financiero.
— Danilak, M., & Thomas, D. (23 de marzo de 2016). What is Cybersecurity? Obtenido de Quora.
— Jessop, S., & Kerber, R. (28 de agosto de 2015). Investors still in the dark as cyber threat grows. Obtenido de Reuters UK.
Kapellmann, Daniel & Benjamín Reyes, Retos de Ciberseguridad en México. Obtenido en http://the-ciu.net/nwsltr/381_1Distro.html
— Kushner, David. "The Real Story of Stuxnet." IEEE Spectrum: Technology, Engineering, and Science News. N.p., 26 Feb. 2013. Web. 16 May 2016.
— Notimex. (28 de diciembre de 2015). México, tercer lugar mundial en ataques cibernéticos; equipo de IPN los combate. Obtenido de Aristegui Noticias.
— Office of the National Counterintelligence Executive. "Foreign Spies Stealing US Economic Secrets in Cyberspace." Counterintelligence (n.d.): n. pág., Oct. 2011. Web.
— Stone, Richard. "A Call to Arms." Science Mag 339.6123 (2000): n. pag. 1 Mar. 2013. Web.
— The White House. (09 de febrero de 2016). Fact Sheet: Cybersecurity National Action Plan. Obtenido de The White House Office of the Press Secretary.

— Weedon, Jen, and Laura Galante. "Intelligence Analysts Dissect the Headlines: Russia, Hackers, Cyberwar! Not So Fast. « Executive Perspective." Atom. N.p., 12 Mar. 2014. Web. 17 May 2016.
— Wikipedia. (07 de mayo de 2016). List of cyber-attacks. Obtenido de Wikipedia.
-- www.forbes.com.mx/ciberseguridad-casi-prueba-del-enemigo-invisible/Benjamín Reyes

LOS DELITOS BINARIOS EN MÉXICO

Carlos Antonio Vázquez Azuara*

¿Por qué delitos binarios? y no informáticos, cibernéticos o electrónicos.

Diversas propuestas han existido, para reformar los ordenamientos punitivos tanto de los estados como el federal, a fin de establecer un capítulo que pueda dar cobertura jurídica y protección a los bienes jurídicamente tutelados que se pudieran vulnerar mediante las nuevas tecnologías y las cuales se han ido fortaleciendo con base en postulados tales como los que corren a cargo de los siguientes autores:

Carlos Sarzana, en su obra Criminalitá e tecnología, los crímenes por computadora comprenden "Cualquier comportamiento criminógeno en el cual la computadora ha

* Licenciado en Derecho, Licenciado en Ciencias de la Comunicación, Doctor en Derecho Público con mención honorifica, miembro del Sistema Nacional de Investigadores del CONACYT, Docente doblemente Certificado en Juicios Orales, por la SETEC-SEGOB, Diplomado en Sistema Penal Acusatorio desde la perspectiva de la reforma constitucional, por parte del Instituto de la Judicatura Federal del Poder Judicial de la Federación, Diplomado en Sistema Penal Acusatorio y Adversarial y Diplomado en Medios Alternativos para la Solución de Conflictos y Justicia Restaurativa, ambos por la Universidad de Xalapa y validados por la SETEC, Diplomado en Educación y Tecnologías de la Información, por la Universidad de Xalapa.

estado involucrada como material o como objeto de la acción criminógena, o como mero símbolo"[4]

Nidia Callegari define al "delito Informático" como "aquel que se da con la ayuda de la informática o de técnicas anexas"[5]

Rafael Fernández Calvo define al "delito Informático" como la realización de una acción que, reuniendo las características que delimitan el concepto de delito, se ha llevado a cabo utilizando un elemento informático o telemático contra los derechos y libertades de los ciudadanos definidos en el título 1 de la Constitución Española"[6]

María de la Luz Lima dice que el "delito electrónico" "en un sentido amplio es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, el delito Informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin"[7]

Julio Tellez Valdes conceptualiza al "delito Informático" en forma típica y atípica, entendiendo por la primera a "las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin" y por las segundas

[4] SARZANA, Carlos. "Criminalita E Tecnologia – Computer Crimes, Rasegna Penitenziaria E Criminologia", Nos 1-2, Anno 1, Gennaio – Giugno, Italia, 1979. P. 59

[5]http://www.coladic-rd.org/cms/wp-content/uploads/2008/07/los_delitos_informaticos_peter_read.pdf

[6] http://www.tribunalmmm.gob.mx/tribunalm/biblioteca/almadelia/Cap3.htm

[7] http://www.aadat.org/delitos_informaticos20.htm

"actitudes ilícitas en que se tienen a las computadoras como instrumento o fin"[8]

Como podemos darnos cuenta en líneas anteriores, los autores refieren definiciones de delitos atendiendo a una naturaleza electrónica, informática, y como en el caso de nuestro país, cibernética, pero en ninguno de los conceptos, estamos hablando de un verdadero campo de estudio que alcance siquiera a comprender todo lo que los delitos relacionados con las nuevas tecnologías infieren.

Para empezar, se analizará, que se entiende en cada concepto que antecede a los delitos que se vienen refiriendo.

Electrónica:

La electrónica es el campo de la física que se refiere al diseño y aplicación de dispositivos, por lo general circuitos electrónicos, cuyo funcionamiento depende del flujo de electrones para la generación, transmisión, recepción o almacenamiento de información. Esta información puede consistir en voz o música como en un receptor de radio, en una imagen en una pantalla de televisión, o en datos como una computadora. La electrónica como tal tiene una gran variedad de aplicaciones para la vida del hombre, como por ejemplo: las telecomunicaciones, la computación, la medicina, la mecánica entre otras[9].

Como se advierte de esta simple definición, la electrónica, es un campo que involucra los aparatos *per se*, por los cuales se podrían cometer los delitos, pero no involucra la realidad virtual que

8 http://www.delitosinformaticos.com/delitos/delitosinformaticos.shtml

9 http://www.viasatelital.com/proyectos_electronicos/definicion_electronica.htm

vivimos, es decir, cuando estamos en internet, lógicamente accedamos mediante un ordenador, pero una vez en el ciberespacio, se atiende a un leguaje que va más allá de la electrónica, es decir un leguaje binario, que rebasa el aspecto de la electrónica y pasa a un plano constituido por unos y ceros, que debe ser regulado jurídicamente y cuando un delincuente comete un delito haciendo uso de las nuevas tecnologías, no lo hace apoyándose en sus conocimientos sobre la electrónica, lo hace apoyándose en sus conocimientos sobre la utilización de las nuevas tecnologías, el cual solo puede manifestarse mediante el código binario, que es el lenguaje que las nuevas tecnologías entienden para traducir los actos de individuo, en funciones que afectan el ciberespacio u otros sistemas lógicos. Por tanto, no es recomendable o suficiente hablar de delitos electrónicos.

Informática:

La informática es la ciencia que tiene como objetivo estudiar el tratamiento automático de la información a través de la computadora. Esta definición, si bien es bastante amplia, se debe a que el concepto de informática también es amplio. Para referirse a esta ciencia, también suele utilizarse el término Computación o Ciencia de la Computación, con la diferencia de orígenes. En cuanto al contenido de la Informática, se encarga de estudiar todo lo relacionado con las computadoras que incluye desde los aspectos de su arquitectura y fabricación hasta los aspectos referidos a la organización y almacenamiento de la información. Incluso contiene las cuestiones relacionadas con la robótica y la inteligencia artificial[10].

Si se analiza el concepto de Informática, se puede aludir que, se va a un plano que involucra el tratamiento de la información mediante las computadoras, e incluso todo lo relacionado con

[10] http://www.mastermagazine.info/termino/5368.php

estas, y se aterriza únicamente en lo concerniente al comportamiento del individuo respecto a esas computadoras o centro de almacenamiento de información, por tanto, cuando se habla de delitos informáticos, se infiere que son aquellos que el individuo comente con relación a las computadoras o a la información que se pudiera almacenar dentro de las mismas, pero no infiere, dada la naturaleza y alcances del concepto, el análisis de las conductas delictivas realizadas mediante las nuevas tecnologías y la internet, que solo son posibles mediante el código binario, es decir, un mensaje amenazador por celular, sería un delito binario, pero no está al alcance del campo de estudio de la informática, porque no se está vulnerando ningún ordenador o sistema de datos lógico, por tanto, se entiende que la única manera de conectar los actos del individuo con los ordenadores, las nuevas tecnologías y el ciberespacio, es el código binario, el cual se utiliza cuando hacemos uso de las nuevas tecnologías, previo conocimiento sobre la utilización de las mismas.

Es decir, el comportamiento del individuo, verbigracia en el ciberespacio, que se logra mediante el código binario, es un aspecto que rebasa a la informática, porque no se está vulnerando un sistema lógico o de información digital, se utiliza el código binario para delinquir y si bien es cierto el código binario es objeto de estudio de la informática, no menos cierto es que el referido código, es lo que le permite a la informática su desarrollo, por tanto, tiende a ser este código la herramienta que tiene la informática para existir y por tanto se advierte como un concepto más amplio y adecuado para los delitos que involucran las nuevas tecnologías tales como los delitos binarios y es en este sentido que tampoco se recomienda el término delitos informáticos.

Cibernética

La Cibernética es la ciencia que se ocupa de los sistemas de control y de comunicación en las personas y en las máquinas, estudiando y aprovechando todos sus aspectos y mecanismos comunes. El nacimiento de la cibernética se estableció en el año 1942, Norbert Wiener uno de los principales fundadores de esta ciencia, propuso el nombre de cibernética, derivado de una palabra griega que puede traducirse como piloto, timonel o regulador. Dentro del campo de la cibernética se incluyen las grandes máquinas calculadoras y toda clase de mecanismos o procesos de autocontrol semejantes y las máquinas que imitan la vida[11]

Los alcances del campo de estudio de la cibernética son muy amplios y van enfocados a establecer el comportamiento de las maquinas, alineado a imitar la vida humana, perfeccionarla y por supuesto facilitarla, pero indudablemente está fuera del alcance de los aspectos que interesan como disciplina de estudio que podría definir los delitos que involucran las nuevas tecnologías, puesto que, si bien es cierto, la cibernética involucra el estudio de la inteligencia artificial, que es la que da vida a los delitos que se tratan de conceptualizar, no menos cierto es que esta disciplina requiere como hilo conductor entre el hombre y la máquina, al código binario, es decir, actualmente las nuevas tecnologías están basadas en inteligencia artificial, pero hasta el momento, ésta se encuentra supeditada a la voluntad del hombre, quien brinda las instrucciones que se traducirán en actos que las máquinas realizan y la única manera en que estas instrucciones pueden ser entendidas por el ordenador, son mediante el código binario, por tanto, los delitos cibernéticos, son un concepto que quedaría cubierto por el ámbito de estudio de los delitos binarios, siendo este último el único hilo conductor entre la cibernética y el delincuente, por tanto, el concepto de

[11] http://robothumano.galeon.com/productos774285.html

delitos cibernéticos, quedaría superado y por ende, tampoco se recomienda.

Retomando lo establecido en capítulos anteriores, el Derecho Binario, es la rama del derecho que se encarga del estudio de las normas que regulan la relación entre los individuos y de ellos con su entorno social, basada en las nuevas tecnologías y la Internet.

Del ámbito de estudio anterior, se puede decir que, los Delitos Binarios, son aquellos delitos tradicionales cometidos con el uso de las nuevas tecnologías y/o el Internet, como un medio o canal, como el objetivo o finalidad y como el soporte o coadyuvante, para la comisión del acto antijurídico, antisocial, típico, culpable y punible.

La comisión a la que se refiere la definición anterior, puede ser por acción, o por omisión, asimismo, al hablar de delitos tradicionales, nos referimos a los delitos tipificados como tales en los ordenamientos punitivos vigentes.

De igual forma, cuando se habla del uso de las nuevas tecnologías y el Internet, nos referimos a tres perspectivas de los Delitos Binarios: como un medio o canal para cometer el acto delictivo, como el objetivo o finalidad del acto delictivo y como el soporte o coadyuvante del acto delictivo.

Por todo lo anterior, es necesario establecer que el concepto que abarcaría todos los supuestos que pudieran ser objeto de la comisión de algún delito mediante las nuevas tecnologías y el internet, es el de Delitos Binarios.

Propuesta de reforma a las Leyes Punitivas.

La reforma que se plantea quedaría de la siguiente manera:

TÍTULO…
DELITOS BINARIOS

CAPÍTULO I
CONSIDERACIONES PRELIMINARES DE ESTE TÍTULO

Por delito binario, se entenderá, la comisión de un acto antijurídico, antisocial, típico, culpable y punible basado en los delitos tradicionales o independientes de estos, cometidos con el uso de las nuevas tecnologías y/o el Internet, como un medio o canal, como el objetivo o finalidad y como el soporte o coadyuvante, pudiendo causar una afectación o no, a la propiedad y/o posesión binaria de que se trate, por tanto:

Se entenderá por delitos binarios basados en los delitos tradicionales, la comisión de un delito ya previsto por este código, cometido con el uso de las nuevas tecnologías y/o el Internet, como un medio o canal, como el objetivo o finalidad y como el soporte o coadyuvante.

Se entenderá por delitos binarios independientes de otros delitos, la comisión de un delito que no se basa en uno tradicional, pero contemplado en el presente título, cometido con el uso de las nuevas tecnologías y/o el Internet, como un medio o canal, como el objetivo o finalidad y como el soporte o coadyuvante, pudiendo causar o no una afectación a la propiedad y/o posesión binaria.

Se entenderá por delito binario en perjuicio de la propiedad y/o posesión binaria, la comisión de un acto que cause una afectación a las mismas.

La comisión a la que se refiere este título, puede ser por acción, o por omisión y cuando se habla de delitos

tradicionales, se hace referencia a los delitos tipificados como tales en éste código.

Por nuevas tecnologías se entenderán los últimos desarrollos tecnológicos y sus aplicaciones.

Para efectos del presente título, se entenderá el uso de las nuevas tecnologías y el internet, como un medio o canal para cometer el acto delictivo, cuando se utilicen las mismas, como conductor entre el sujeto activo y el sujeto pasivo del delito tradicional.

Se entenderá el uso de las nuevas tecnologías y el internet, como el objetivo o finalidad del acto delictivo, cuando se utilicen las mismas, como el receptor de la actualización del tipo penal que se configure.

Para efectos del presente título, se entenderá el uso de las nuevas tecnologías y el internet, como soporte o coadyuvante del acto delictivo, cuando se utilicen las mismas, como apoyo para la consumación del acto ilícito sin ser necesariamente un medio o la finalidad.

Para efectos de este título, por propiedad binaria, se entiende, el derecho que se tiene de uso, goce, usufructo y disfrute sobre bases de datos, sistemas de red, carpetas de información, archivos, programas, cuentas de correo electrónico, cuentas de redes sociales, sitios de internet, espacios virtuales y toda aquella información digital o sitios digitales, resguardados en el ciberespacio o en algún medio de almacenamiento, sin que necesariamente se tenga la posesión de las mismas.

Por posesión binaria, se entiende el derecho que se tiene de uso, goce, usufructo y disfrute sobre bases de datos, sistemas de red, carpetas de información, archivos, programas, cuentas de correo electrónico, cuentas de redes sociales, sitios de

internet, espacios virtuales y toda aquella información digital o sitios digitales, resguardados en el ciberespacio o en algún medio de almacenamiento, sin que necesariamente se acredite la propiedad de las mismas.

Para efectos de este título, se entenderá como afectación a la propiedad binaria, la alteración, daño, modificación, uso sin autorización, reconfiguración, desconfiguración, intrusión no autorizada, interceptación, y/o todo aquello que tienda al deterioro y/o aprovechamiento y/o difusión indebida de la propiedad binaria.

También se entenderá como afectación a la posesión binaria, la restricción del acceso que haga una o más personas en un sitio virtual, base de datos, archivo, carpeta y/o sistema operativo ubicado en internet o en un ordenador o sistema de cómputo, a quien tenga derecho para tener dicho acceso.

CAPÍTULO II
DELITOS BINARIOS
BASADOS EN LOS DELITOS TRADICIONALES

Artículo...- A quien cometa un delito de los ya previstos por este código, con el uso de las nuevas tecnologías y/o el Internet, como un medio o canal, como el objetivo o finalidad y como el soporte o coadyuvante, serán sancionado con la pena prevista por el delito tradicional del que se trate, incrementándose hasta en una mitad.

CAPÍTULO III
DELITOS BINARIOS EN PERJUICIO DE
LA PROPIEDAD Y LA POSESIÓN BINARIA

Artículo...- A quien cometa un acto que cause una afectación a la propiedad y/o posesión binaria, se le impondrán de seis

meses a doce años de prisión y multa hasta de trescientos días de salario.

Si la afectación a la que se refiere este título, es con ánimo de lucro y/o en perjuicio de terceros, las penas previstas en el párrafo anterior, se incrementarán hasta en una mitad.

CAPÍTULO IV
DELITOS BINARIOS
INDEPENDIENTES DE OTROS DELITOS

Artículo…- Se impondrán de seis meses a doce años de prisión y multa hasta de trescientos días de salario al que actualice alguno de los siguientes supuestos:

I.- Recolección no autorizada de datos. - Comete este delito binario, quien, con cualquier fin y sin autorización de quien deba otorgarla, desarrolle, utilice, adquiera o propague, en cualquier sistema operativo conectado a un sistema de red interna o a la internet, un software que recolecte información ubicada en dicho sistema operativo o en cualquier otro.

II.- Instalación no autorizada de software. - Comete este delito binario, quien sin autorización de quien deba otorgarla e independientemente del fin, instale cualquier tipo de software o descargue algún tipo de archivo en un ordenador, sistema operativo o sistema lógico de cómputo.

III.- Almacenamiento no autorizado de información. - Comete este delito binario quien, sin contar con autorización de quien debiera otorgarla, almacene, en algún tipo de medio de almacenamiento o en internet, cualquier tipo de información digital.

IV.- Suplantación de identidad. - Comete este delito binario quien, con el ánimo de recolectar datos,

independientemente del fin, hospede en internet un dominio igual o similar a otro con las diferencias suficientes en el nombre del sitio para generar en los cibernautas la creencia de que se encuentran en el sitio original, propiciando que de manera voluntaria el sujeto pasivo otorgue sus datos o revele información.

También comete este delito, quien con autorización o sin ella, ingrese a una cuenta de correo electrónico, pagina web, cuenta de red social, o cualquier sitio web, realizando actos a nombre de quien tenga el derecho sobre las mismas, siempre que dichos actos causen una afectación al sujeto pasivo y/o un beneficio al sujeto activo de este delito.

V.- Secuestro de cuentas de correo, sitios web y redes sociales. - Comete este delito, quien, con autorización de quien deba darla o sin ella, ingrese a una cuenta de correo electrónico, sitio web o red social y cambie la contraseña o código de acceso, generando que quien tenga derecho a ingresar quede impedido de hacerlo.

VI.- Implantación de Software o archivo malicioso.- Comete este delito binario quien, mediante algún tipo de medio de almacenamiento digital, memoria USB, o mediante una transferencia de datos digitales, instale, propague, difunda o haga circular, en un ordenador, sistema lógico de computo, en el internet o en una red interna, un virus, un software o archivo que, al ser abierto, o al ser instalado, implante un virus digital en un ordenador, sistema operativo, base de datos o sistema lógico de computo.

VII.- Neutralización de seguridad y antivirus. **-** Comete este delito binario quien, sin autorización de quien deba darla, por medio de internet o directamente en un ordenador, sistema operativo o sistema lógico de computo, desactive un antivirus, una pared de fuego o cualquier sistema de seguridad que se encuentre activado.

VIII.- Implantación de archivos espías. - Comete este delito binario, quien envíe mediante internet o instale directamente un archivo espía en un ordenador, sistema operativo o sistema lógico de computo, con el fin de conocer todo aquello que acontezca en los mismos.

IX.- Manipulación de ordenadores o programas. - Comete este delito binario, quien, mediante un ordenador, sistema operativo o sistema lógico de cómputo, manipule, configure, desconfigure, altere, utilice o modifique un ordenador, sistema operativo o sistema lógico de cómputo, inhabilitando el uso de quien tenga derecho a hacerlo.

X.- Transferencia de correos electrónicos basura. - Comete este delito binario, quien, de manera reiterada, mande correos electrónicos a través de la internet, a uno o más destinatarios, cuyos contenidos, sean cadenas, publicidades u otros considerados perjudiciales o improductivos para el usuario, con el fin de causar una afectación a los destinatarios. Este delito se perseguirá por querella de parte.

Si la afectación a la que se refiere este título, es con ánimo de lucro y/o en perjuicio de terceros, las penas previstas en este artículo, se incrementarán hasta en una mitad.

CAPÍTULO V
CONSIDERACIONES RELATIVAS A LOS DELITOS BINARIOS

Los delitos binarios, se actualizan independientemente de que causen una afectación o no, pero en caso de existir, la reparación del daño se basará en el daño ocasionado o las consecuencias que traiga consigo la perdida de la información, los archivos, programas o cualquier daño lógico del que se trate.

Al sujeto activo del delito binario basado en los delitos tradicionales, se le aplicará la pena a la que haya lugar según lo establecido por este título, sin que proceda aplicarle adicionalmente la pena que el delito tradicional de origen contemple.

Al sujeto activo del delito binario independiente de otros delitos, se le aplicará la pena a la que haya lugar, independientemente de la sanción que pudiera existir, en caso de actualizarse alguna otra conducta delictiva prevista por este código.

Cuestiones anexas a la reforma.

La reforma que se viene planteando, involucra necesariamente una trasformación de la visión que actualmente se tiene sobre los delitos y se debe comenzar a entender que estamos en medio de una evolución sin precedentes, que requiere adaptar las leyes a las nuevas necesidades que enfrentamos y evidentemente la era digital, es el principal reto.

Asimismo, esta reforma, requiere el establecimiento de nuevas leyes que permitan la salvaguarda de la propiedad binaria y de la realidad virtual, puesto que actualmente, no existen mecanismos jurídicos de salvaguarda para ello.

Requiere también, el reconocimiento por parte de los doctrinarios, de nuevas normas que rebasan lo establecido por Eduardo García Máynez entre otros juristas destacados, quien establecía la existencia de normas jurídicas, morales, religiosas, de trato social y técnicas, pero ahora, debemos incorporar las normas binarias.
Las normas binarias, son aquellas que regulan la conducta del individuo y de él con otros individuos en la realidad virtual.

Se ha establecido, que es la realidad virtual, entendiendo por ésta, una realidad que vivimos a la par de nuestra realidad material, intangible y transportable, basada en un código binario y en muchos casos es una realidad en la que interactuamos la mayor parte de nuestro tiempo y refiere aquella donde realizamos todas nuestras actividades sociales, familiares, emocionales, laborales, de recreación, entre otras, mediante las nuevas tecnologías y la Internet.

Por lo anterior, una de las cuestiones que deben de surgir con la reforma propuesta, es la regulación de la realidad virtual mediante normas binarias, ya que no es posible tutelar nada en el ciberespacio y para muestra nos podemos remitir a los siguientes ejemplos:

Una cuenta de correo electrónico, nos atrevemos a decir que es nuestra, pero ¿cómo acreditamos la propiedad de la misma?, si alguien vulnera nuestra cuenta e ingresa de forma ilegal a ella hackeandola, además de la intrusión no autorizada a sistemas lógicos de los que hablan los delitos informáticos, pero ¿por qué no autorizada?... también debemos tener presente que se está invadiendo la privacidad y se está allanando un espacio virtual, pero todo lo anterior, no es posible acreditarlo si no es posible primero acreditar la propiedad de la cuenta o la posesión siquiera.

De quien es propiedad la información que se sube al ciberespacio, es decir, si subo una fotografía y alguien la toma, y yo no lo autorizó, ¿puedo exigir jurídicamente algo?, la verdad es que no, porque sabido es por los cibernautas, que lo que se sube a internet sin las precauciones de los derechos de autor, se vuelve del dominio público, pero esto ¿Quién lo estableció?

Cuáles son las políticas de navegación que debemos observar o que pasa si alguna página, mediante engaños, me hace descargar

un virus perjudicial a mi máquina, que puedo hacer jurídicamente hablando, si los virus no son otra cosa que programas diseñados para causar afectaciones lógicas. ¿Puedo proceder por daños? Que dice el tipo penal de daños en Veracruz:

Artículo 226.- A quien, en perjuicio de tercero, por cualquier medio destruya o deteriore una cosa, total o parcialmente ajena o propia, se le impondrán de seis meses a ocho años de prisión y multa hasta de ciento cincuenta días de salario.
Este delito se perseguirá por querella. (Reformado, primer párrafo; g.o. 24 de agosto de 2004)

Artículo 227.- Si el daño se ocasiona con motivo del tránsito de vehículos y el conductor se hallare en estado de ebriedad o bajo el influjo de estupefacientes u otras sustancias tóxicas, se sancionará con prisión de tres a nueve años, multa hasta de trescientos días de salario y suspensión del derecho para conducir vehículos hasta por tres años. Esta conducta se perseguirá de oficio.

Artículo 228.-La prisión podrá aumentarse hasta diez años y la multa hasta trescientos días de salario, si el daño recae en bienes de valor científico, artístico, cultural o de utilidad pública.

En el tipo penal descrito con antelación, se habla de la destrucción o deterioro de una cosa total o parcialmente ajena… para empezar, regresamos al problema de la acreditación de la propiedad, pero también nos enfrentamos al problema de la definición de cosa, puesto que cosa, jurídicamente hablando, puede ser un bien, una obligación o un derecho, pero si hablamos de bien, ¿cómo establecemos que tipo de bien?

Para efectos de la presente investigación se deben acuñar también como parte de la clasificaron a los bienes binarios, que no son ni los bienes incorpóreos, ni los intangibles, puesto que

estos dos últimos, hacen referencia a la realidad material mientras que el primero de los mencionados, hace referencia a la realidad virtual.

Pero esto que se comenta en el presente apartado, no es ni la punta del iceberg de lo que se tiene que enfrentar en tratándose del Derecho binario, puesto que el ciberespacio involucra infinidad de nuevos retos que solo se podrán ir subsanando con el trascurso de la actual evolución.

Finalmente nos permitimos presentar en este apartado, algunas medidas que pudieran mejorar algunos de los problemas más comunes jurídicamente hablando, con respecto al ciberespacio.

- Implementar como forma de acceso al correo electrónico u otras páginas de internet la huella digital para efectos de identificar al usuario sin lugar dudas.
- En páginas para adultos, solicitar el número de folio de la credencial de elector para acreditar la mayoría de edad de los visitantes
- Establecer una cuenta de correo electrónico oficial por cada ciudadano, de un servidor de gobierno, para un mayor control y diversos usos tales como las notificaciones personales.
- Establecimiento de una división política y por ende de competencia por naciones en el ciberespacio.
- La creación de un registro nacional de cibernautas
- La creación de una base de datos nacional de páginas de internet con registro de los que tiene derechos sobre los respectivos dominios y hospedajes.

Somos conscientes en el presente trabajo, las recomendaciones aquí expresadas, son complicadas de llevarse a la práctica, pero de hacerse, tenderían a mejorar las conductas del individuo en el ciberespacio.

Expectativas de la reforma.

La reforma tiene las expectativas de que se tienda a mejorar la persecución de los delitos binarios, actualmente conocidos como informáticos y cibernéticos.

Pero esto involucra, capacitación al personal encargado de la procuración de justicia mediante programas de mejora continua, además involucra también la creación de agencias especializadas en delitos binarios, puesto que como ya ha quedado demostrado en capítulos anteriores, los que se encuentran al frente del aparato de administración de justicia en el Estado, manifiestan que es necesario que se establezca personal especializado para la atención a este tipo de delitos.

También involucra, que en las universidades preparen a los estudiantes ante los retos jurídicos que involucran las nuevas tecnologías y el internet, pues prácticamente todas las disciplinas de estudio que se desprenden de la ciencia del derecho, son objeto de las nuevas tecnologías y la internet, por ejemplo, en el ámbito del comercio, tenemos el comercio tradicional y el comercio electrónico, en el ámbito civil, tenemos los contratos tradicionales y los contratos electrónicos revestidos de una firma electrónica, en el ámbito fiscal, tenemos incorporado el pago de impuestos por internet, en el ámbito bancario tenemos las trasferencias electrónicas y en suma, prácticamente en todas las ramas del derecho es posible la incorporación del enfoque de nuevas tecnologías y el internet, y todo esto es campo de estudio del derecho binario.

Por lo anterior, se espera que la reforma, traiga consigo el reconocimiento de una nueva rama del derecho como lo es el derecho binario y que consecuencia de esto se mejoren los mecanismos jurídicos de protección para los derechos binarios, siendo estos últimos aquellos inherentes al individuo en el ciberespacio.

Consideraciones finales

Se demostró que el término adecuado para vislumbrar el campo de acción que infieren los delitos que involucran las nuevas tecnologías y la internet es el de Delitos Binarios, toda vez que abarca toda la actividad humana, tendiente a delinquir, relacionada con las nuevas tecnologías y el internet.

Se estableció una reforma que logra cubrir con todos los supuestos delictivos que se pudieran actualizar, con el uso de las nuevas tecnologías y el Internet.

Se argumentó que anexo a la reforma, se requieren otras reformas que tutelen los derechos en la realidad virtual tales como los que involucran la propiedad binaria, que se alberga en las redes, bases de datos y el propio ciberespacio.

Se demostró que es necesaria la incorporación de una nueva rama del derecho denominada Derecho Binario, la cual trae como campo de estudio todo el orden jurídico tendiente a regular al individuo con relación a su entorno y a otros individuos, basado en las nuevas tecnologías y el internet.

CIBERSEGURIDAD, RETOS Y PROSPECTIVA

Oliver González Barrales

INTRODUCCIÓN

Con el nacimiento de la era espacial, las computadoras y el internet, la sociedad global ha sufrido una evolución tecnológica sin precedentes, llamada hoy en día la tercera revolución industrial. Durante las últimas tres décadas del siglo XX, el desarrollo de las Tecnologías de Información y Comunicación (TIC) y el incremento en el uso de Internet, ha estado evolucionando hacia un mundo "híper-conectado", en el que las personas viven conectadas de forma permanentemente a la información a través de diferentes dispositivos como la radio, la televisión, el internet y el teléfono celular.

Es un hecho que estamos transitando hacia la sociedad de la información, cada día más servicios son ofrecidos vía internet, más información es almacenada en la nube y un mayor número de dispositivos son conectados alrededor del mundo. Las empresas dependen cada vez más de su operación en esta plataforma internacional para mejorar la experiencia de compra, permitiendo a sus clientes acceder desde sus dispositivos móviles a información en tiempo real de sus productos, inventario y costos a la par que observan físicamente los artículos.

El uso de las tecnologías de la información y la incorporación del Internet al mundo real, sin duda han sido un factor de desarrollo global, incluso nos están llevando hacia la cuarta revolución industrial mediante la inclusión del concepto del "Internet de las Cosas" donde su uso se incorporará a la industria en la producción, distribución y manejo de los

productos adaptando servicios a los clientes en cualquier parte del mundo.

De esta forma, han surgido conceptos como "Ciudad Inteligente", que se caracteriza por el uso intensivo de las TIC en la creación y el mejoramiento de los sistemas que componen la ciudad para crear, recopilar, procesar y transformar la información que incida en mejores servicios y calidad de vida mediante el uso eficiente de sus recursos.

Empero, la innovación tecnológica ha ido acompañada de un aumento en la delincuencia informática, en donde el alcance de los ataques cibernéticos y el daño económico combinado de la ciberdelincuencia ha llegado a un nivel tal que en algunos países la ciberdelincuencia puede haber superado a la delincuencia tradicional. Se ha identificado un aumento en la agresividad de los delitos informáticos[12].

En los últimos años ha tomado auge el término "Crime as a Service" que sustenta que el cibercrimen proporciona herramientas y servicios a través de todo el espectro de la delincuencia en Internet, a los atacantes cibernéticos de bajo perfil hasta terroristas cibernéticos.

LA TRICOTOMÍA DEL CIBERDELITO

A la par de la evolución del Internet se han ido generando las circunstancias propicias para aquellos que buscan un beneficio personal a costa de ciberusuarios, las afectaciones derivadas comparten un origen y una serie de características comunes de la actividad delictiva, tal es el caso del bajo grado de riesgo para el delincuente y el alto grado de efectividad e impacto, así como la facilidad de ejecución y el anonimato, ya que se puede delinquir prácticamente desde cualquier lugar del planeta donde

[12] Internet Organised Crime Threat Assessment, EUROPOL, 2016

exista acceso a Internet y afectar a Instituciones o individuos de cualquier parte del mundo. En algunos casos, no es imprescindible grandes conocimientos por parte del delincuente para efectuar algún delito cibernético.

Al respecto, el Foro Económico Mundial considera las fallas de la infraestructura crítica, los ciberataques y el fraude o robo de datos como parte de los principales riesgos globales, incluso entre los primeros diez lugares[13]. Este último ligado al robo de datos personales.

La teoría denominada la tricotomía del ciberdelito[14] describe la relación estrecha entre el volumen de atacantes, la ganancia por ataque y el volumen de víctimas. Estas tres estrechamente relacionadas con las medidas a tomar para prevenir o investigar, según sea el caso, las afectaciones por ciberdelitos.

Existe un gran volumen de atacantes que no necesariamente tienen grandes habilidades, un nivel alto de confianza o técnicas de ataque innovadoras, sin embargo, por la falta de concientización en ciberseguridad y protección de un alto volumen de víctimas, pueden generar un alto porcentaje de efectividad con ganancias mínimas por ataque. Esto se traduce en un alto volumen de ganancias obtenidas por la afectación a un alto volumen de víctimas que se puede prevenir en gran medida con una estrategia de concientización en materia de ciberseguridad.

Por otro lado nos encontramos con atacantes más sofisticados, estos cuentan con grandes capacidades y técnicas de intrusión innovadoras, sus ganancias por ataque son altas y regularmente sus ataques están dirigidos a víctimas con un alto perfil

[13] World Economic Forum, Global Risks 2013 [en línea], [fecha de consulta: Abril 2016]. Disponible en: http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2013.pdf

[14] Internet Organised Crime Threat Assessment, EUROPOL, 2016

económico que a su vez tienen un nivel de concientización, protección y seguridad elevado, por ende, las ganancias son bastas aunque en un bajo volumen de víctimas. Esto se traduce en un alto volumen de ganancias obtenidas en un bajo volumen de víctimas que en muchos casos se tiene que llegar a una investigación cibernética para identificar a los atacantes.

En 2014, los ataques más comunes en el Internet de las Cosas han sido a los sistemas de terminales de punto de venta (POS por sus siglas en inglés), cajeros automáticos y dispositivos de acceso a Internet en los hogares[15].

Un estudio realizado por la firma de software Symantec reveló que, a nivel global, la cifra de víctimas es de aproximadamente 12 víctimas por segundo: 1 millón diarias y 378 millones al año. El reporte indica que las pérdidas económicas anuales oscilan entre los 375 y 575 mil millones de dólares[16].

En Latinoamérica, y conforme al estudio realizado por la Organización de Estados Americanos (OEA) en colaboración con la firma de software Trend Micro, se presentó un incremento entre el 8% y el 40% en ataques durante 2012, siendo México el mercado más problemático. Dicho aumento se generó en ciberataques y acciones "hacktivistas", lavado de dinero y ataques a infraestructuras críticas[17].

[15] Internet SecurityThreat Report, Symantec (2015)
[16] Norton by Symantec, Reporte Norton 2013 [en línea], [fecha de consulta: Abril 2016]. Disponible en: https://www.symantec.com/content/es/mx/about/presskits/b-norton-report-2013-final-report-lam-es-mx.pdf
[17] Trend Micro, Latin American and Caribbean Cybersecurity Trends and Government Responses [en línea], [fecha de consulta: Abril 2016]. Disponible en: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-latin-american-and-caribbean-cybersecurity-trends-and-government-responses.pdf.

Quizá esta sea una de las razones por las que la actividad de programas de cómputo maliciosos (malware) también fue una de las principales afecciones, registrándose un incremento del 40% en incidentes cibernéticos en 2012[18]. Se estima que en 2013 la pérdida económica anual en México fue alrededor de los 3 mil millones de dólares según los datos del Reporte Norton de 2013[19].

El Estudio sobre los hábitos del Internet en México realizado por la AMIPCI (2014) indica que 18.4 millones (36%) de cibernautas son personas menores de edad, un gran número de posibles víctimas de delitos contra menores. El estudio arrojó que el promedio en el tiempo de conexión a Internet de los cibernautas en México es de más de cinco horas al día y que el uso es principalmente para el correo electrónico, redes sociales (9 de cada 10 lo utilizan) y búsqueda de información, en ese orden[20].

De acuerdo a la Encuesta Nacional de Disponibilidad y uso de las TIC en los Hogares, realizada por el Instituto Nacional de Estadística y Geografía en 2015, 55.7 millones de personas son usuarios de una computadora y 62.4 millones utilizan Internet en México. Dicha encuesta indica que el 9.7% de los usuarios de internet lo utiliza para ordenar o comprar productos en línea y el 9.3% para realizar operaciones bancarias. El 12.8% de los

[18] Trend Micro, Latin American and Caribbean Cybersecurity Trends and Government Responses [en línea], [fecha de consulta: Abril 2016]. Disponible en: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-latin-american-and-caribbean-cybersecurity-trends-and-government-responses.pdf.

[19] Norton by Symantec, Op. Cit., [fecha de consulta: Abril 2016]. Disponible en: https://www.symantec.com/content/es/mx/about/presskits/b-norton-report-2013-final-report-lam-es-mx.pdf

[20] Asociación Mexicana de Internet, Estudio Comercio Electrónico en México 2015 [en línea], [fecha de consulta: Abril 2016]. Disponible en: https://amipci.org.mx/estudios/comercio_electronico/Estudio_de_Comercio_Electronico_AMIPCI_2015_version_publica.pdf

usuarios de internet declaro haber realizado al menos una transacción electrónica (compra o pago por internet) dentro de los 12 meses previos a la entrevista[21].

A partir del contexto anterior, es posible establecer que el diagnóstico presenta tendencias en favor del uso de la tecnología, del acceso a la información y de la reducción de la brecha digital, es también posible notar que los gobiernos mantendrán una política de apoyo al uso de las tecnologías como mecanismo de desarrollo económico, político y social.

Empero, se ha visualizado un crecimiento de la actividad ilícita en el uso de las tecnologías y el Internet así como la constante evolución de éstos últimos, la actividad de la ciberdelincuencia se moverá a la par de dicho desarrollo en gran volumen, por lo que, es imprescindible que las políticas públicas y la legislación nacional consideren a la ciberdelincuencia como un aspecto prioritario nacional.

Así, el término ciberseguridad ha sido objeto de estudio y definición, tal como se expresa en la Recomendación UIT–T X.1205, de la Unión Internacional de Telecomunicaciones[22], quedó establecido como:

> *Es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas,*

[21] Instituto Nacional de Estadística y Geografía, 2015. [fecha de consulta: Mayo 2016] http://www.inegi.org.mx/saladeprensa/boletines/2016/especiales/especiales2016_03_01.pdf

[22] Unión Internacional de Telecomunicaciones, UIT 2009, Aspectos Generales de la Ciberseguridad [fecha de consulta: Abril 2016]. Disponible en PDF en: https://www.itu.int/rec/T-REC-X.1205-200804-I/es

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, y la confidencialidad.

RETOS EN MATERIA DE CIBERSEGURIDAD

De acuerdo con la Unión Internacional de Telecomunicaciones (UIT), a nivel global hay alrededor de 3 mil 200 millones de cibernautas (44% de la población mundial) con una tasa de crecimiento anual aproximada de 14%[23].

Con base en los Objetivos de Desarrollo del Milenio establecidos por la Organización de las Naciones Unidas a partir del año 2000, la revolución tecnológica de los últimos 15 años ha propiciado un progreso tecnológico, el despliegue de infraestructura y la caída de los precios en los bienes y servicios tecnológicos, lo que ha contribuido al crecimiento en el acceso y conectividad de miles de millones de personas en todo el mundo. A la fecha, existen más de 7 mil millones de abonados a servicios

[23] Unión Internacional de Telecomunicaciones, ICT Facts & Figures 2015 [en línea], [fecha de consulta: Abril 2016]. Disponible en: http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf.

de telefonía móvil en todo el mundo, frente a los menos de mil millones en el año 2000[24].

El escenario en México, de acuerdo con datos de la Asociación Mexicana del Internet (AMIPCI), es notable incremento en la cifra de cibernautas, pasando de 51.2 millones en 2013 a 53.9 en 2014. La AMIPCI identificó que en México se incrementó el comercio electrónico en 2014, llegando a movilizar más de 160 mil millones de pesos, lo que representa un 34% más que en el año anterior[25].
Otro dato relevante de México es la importancia que tienen las micro, pequeñas y medianas empresas (MIPYMES) en el desarrollo económico y social de la nación, ya que datos de Promexico refieren que existen cerca de 4.2 millones de MIPYMES que generan el 52% del Producto Interno Bruto (PIB) y el 72% de los empleos formales. El 95% de ellas son particularmente pequeñas y medianas e impulsan de manera relevante el crecimiento económico digital del país con el fortalecimiento de sus infraestructuras tecnológicas[26].

Por otro lado, los delincuentes cibernéticos han evolucionado desde el nacimiento de las Tecnologías de la Información y Comunicación, en la década de 1970, se inició con la experimentación e investigación de las nuevas tecnologías, durante la década de 1980 nace el termino hacer motivados por la curiosidad, en su mayoría experimentación de carácter

[24] Organización de las Naciones Unidas, Objetivos de Desarrollo del Milenio [en línea], [fecha de consulta: Abril 2016]. Disponible en: http://www.undp.org/content/undp/es/home/sdgoverview/mdg_goals/
[25] Asociación Mexicana de Internet, Estudio Comercio Electrónico en México 2015 [en línea], [fecha de consulta: Abril 2016]. Disponible en: https://amipci.org.mx/estudios/comercio_electronico/Estudio_de_Comercio_Electronico_AMIPCI_2015_version_publica.pdf
[26]PRODEIIN 2013-2018, Censos Económicos (2009). Micro, pequeña, mediana y gran empresa : estratificación de los establecimientos : Censos Económicos 2009 / INEGI, c2011. 2013 [en línea], [fecha de consulta: Abril 2016]. Disponible enhttp://www.institutopyme.org/index.php?option=com_content&view=article&id=134&,

benigno. Llegando la década del 2000, los script kiddies intentan causar daños y hacerse famosos pero aún sin objetivos claros, evolucionando en 2005 en cibercriminales con objetivos específicos y motivos comerciales, utilizando nuevas técnicas como el phishing, malware y redes de botnets. En la década de 2010 los ciberatacantes son ya profesionales con equipos sofisticados, nacen los grupos hacktivistas con motivos políticos y estratégicos. En los últimos años, se han generado estructuras de ciberdelincuencia organizada para realizar ataques y proveer servicios mediante la utilización de métodos y herramientas sofisticadas.

Derivado de los datos anteriores, se establecen como retos en materia de ciberseguridad las iniciativas que impulsen las capacidades en la investigación, la formación y desarrollo de capacidades en ciberseguridad, la prevención como mecanismo de combate al cibercrimen, la cooperación nacional e internacional, y la armonización legislativa en la materia.[27]:

A. Investigación

Incrementar las capacidades de investigación de los delitos cibernéticos con el objetivo de llegar a los ciberdelincuentes, lo anterior aunado a la cooperación en materia cibernética, hará cada vez más efectiva nuestras capacidades de identificación de los responsables.

- Las entidades que aplican la ley deben tener las herramientas, técnicas y conocimientos para combatir el uso delictivo del cifrado y el anonimato en internet. Se debe seguir centrándose en la atribución y el desarrollo de la inteligencia con el fin de identificar, localizar

[27] Internet Organised Crime Threat Assessment, EUROPOL, 2016

y procesar a individuos criminales clave para lograr un mayor impacto permanente en la comunidad criminal.

- Es esencial asignar recursos suficientes para investigar el malware y otros servicios que permiten generar ataques cibernéticos.

- Se debe contribuir y participar en actividades operativas y de prevención relacionados a los ataques cibernéticos. Esto dará lugar a un impacto mayor y más extenso en la lucha contra la criminalidad.

- El intercambio de inteligencia es esencial, esto ayudará a evitar la duplicación de esfuerzos, facilitar el intercambio de tácticas y herramientas, y aumentar la comprensión de las amenazas cibernéticas.

- Debe haber un esfuerzo continuo de todos para dar prioridad a las víctimas en las investigaciones.

B. Formación y desarrollo de capacidades

Especializar a los profesionales en materia de ciberseguridad, incluyendo el uso de monedas electrónicas y darknets para ampliar la cobertura de investigación de los delitos cibernéticos.

- Garantizar que se cuente con la capacitación y los recursos necesarios para el manejo de la evidencia digital en sitio utilizando técnicas como análisis forense de datos.

- Invertir en la formación especializada adecuada requerida para investigar con eficacia los ataques cibernéticos altamente técnicos.

- Dada la naturaleza cambiante de la ciberdelincuencia y el ritmo al que evoluciona la tecnología, existe una necesidad de un enfoque más adaptable y ágil a la investigación y el desarrollo, con miras a la obtención de resultados relevantes de una manera más oportuna.

- A medida que el uso criminal de monedas virtuales continúa ganando impulso, es cada vez más importante garantizar que los delitos informáticos y los investigadores financieros tienen una formación adecuada en la localización, la incautación e investigación de monedas virtuales.

- Un esfuerzo coordinado debe ser tomado por la policía para colaborar con los países donde se compren bienes y servicios con tarjetas de crédito comprometidas.

- La capacitación en Darknets debe ser un tema es un tema transversal para el apoyo de especialistas en múltiples tipos de delitos.

- No es factible o práctico que todos los delitos sean tratados por las unidades de delitos informáticos cuando el delito predicado está relacionado con drogas, armas de fuego o alguna otra mercancía ilícita. Es esencial, por

tanto, que el entrenamiento apropiado y soporte de la herramienta se extienda a las personas que trabajan en estas áreas para proporcionarles los conocimientos y la experiencia necesaria.

C. Prevención

Se deben desplegar campañas de sensibilización y concientización en materia de ciberseguridad, invertir en prevención se vuelve un tema de eficiencia sobre la inversión en investigación, después de ocurrido el delito cibernético.

- La inversión de recursos en actividades de prevención puede ser más eficiente que la investigación de los incidentes individuales. Además de la sensibilización y consejos de prevención del delito, las campañas deben aconsejar al público sobre cómo reportar los crímenes cibernéticos.

- Las campañas de prevención no deben centrarse únicamente en la prevención de los ciudadanos y las empresas que puedan llegar a ser víctimas de los delitos informáticos, sino también en la prevención de las consecuencias legales a delincuentes cibernéticos potenciales que se involucren en dicha actividad.

- Las campañas de prevención deben coordinarse con otras organizaciones nacionales e internacionales.

- Se debe fomentar el uso de software de seguridad y la denuncia de los ataques cibernéticos.

- Se debe mantener un enfoque en el desarrollo y la distribución de campañas de prevención y sensibilización. Estas campañas deben actualizarse para abarcar las tendencias actuales.

D. Cooperación

Se debe mantener una cooperación nacional e internacional en materia de ciberseguridad, tanto en el sector público, privado y académico para sumar esfuerzos en la lucha contra el cibercrimen.

- Se deben forjar y mantener la colaboración en materia de ciberseguridad con el mundo académico, el sector privado y el gobierno.

- Se requiere un esfuerzo adicional, a través del intercambio de información más centrado en cumplimiento de la ley, para vincular los casos de fraude de tarjetas. Esto facilitaría la identificación de los grupos del crimen organizado involucrados en el fraude de tarjetas de crédito.

- Se deben llevar a cabo operaciones a gran escala en materia de prevención e investigación del ciberdelito.

- Debe existir una colaboración activa con el Centro Especializado en Respuesta Tecnológica

(CERT-MX), para dar seguimiento a las investigaciones criminales derivadas de incidentes cibernéticos.

- Se deben establecer relaciones de trabajo con otras naciones para operar bajo jurisdicciones extranjeras.

- A medida que el uso criminal de monedas virtuales continúa ganando impulso, es cada vez más importante construir y mantener relaciones con la comunidad de moneda virtual, en particular los centros de cambio de moneda virtual.

E. Legislación

Se deben impulsar proyectos de armonización legislativa en materia de delitos electrónicos..

- Se requiere un enfoque armonizado para las investigaciones encubiertas en otras naciones. al respecto, la adhesión al convenio de Budapest (convenio sobre criminalidad) puede ser una opción para la armonización legislativa.

- Se deben sumar esfuerzos para asegurar que las infraestructuras críticas de TICs se encuentren protegidas por la legislación nacional aplicable.

- La armonización legislativa debe tipificar ciertas conductas para no permitir los refugios donde los delincuentes cibernéticos pueden evitar la investigación en su contra y el procesamiento judicial.

- Se debe permitir el intercambio de información y un enfoque coordinado para dar respuesta eficaz a los ataques cibernéticos graves. En este término, la asistencia legal mutua cobra suma importancia.

DECÁLOGO DE CIBERSEGURIDAD

Para incrementar nuestro nivel de seguridad de la información, a continuación se emiten una serie de recomendaciones generales.

1. Mantener actualizados los sistemas y aplicaciones de cómputo.

2. Utiliza contraseñas robustas con al menos 10 caracteres alfanuméricos y símbolos.

3. Utiliza doble factor de autenticación para servicios en línea, como las de correo electrónico y bancos.

4. Realiza respaldos de manera periódica y guárdalos en discos externos.

5. No abras documentos adjuntos y enlaces que vienen en correos de origen desconocido.

6. No realices depósitos antes de verificar que la operación sea legítima.

7. Desconfía de correos y páginas con ofertas atractivas de artículos y servicios.

8. Comprueba el nivel confiabilidad de los sitios web y la seguridad de su conexión ("https:// ").

9. Configura los parámetros de seguridad y privacidad en cuentas de correo electrónico y redes sociales.

10. Concientiza entre familiares, amigos y compañeros de trabajo la importancia de la seguridad de la información.

CONCLUSIONES

- Dentro de los retos del nuevo entorno operativo, se ampliarán los servicios a través del Internet con el impulso del **"Internet de las Cosas"** y las **"Ciudades Inteligentes"**, lo que implicará nuevas amenazas y ataques en el ciberespacio, por lo que el fortalecimiento de las capacidades operativas para la prevención e investigación de los ciberdelitos representa un área de oportunidad para los gobiernos quienes deberán establecer sus estrategias a fin de contrarrestar el fenómeno delictivo.

- Existe un gran volumen de atacantes que no necesariamente tienen grandes habilidades, un nivel alto de confianza o técnicas de ataque innovadoras, sin embargo, por la falta de concientización en ciberseguridad y protección de un alto volumen de víctimas, pueden generar un alto porcentaje de efectividad con ganancias mínimas por ataque. Esto se traduce en un alto volumen de ganancias obtenidas por la afectación a un alto volumen de víctimas que se puede prevenir en gran medida con una estrategia de concientización en materia de ciberseguridad.

- Los atacantes más sofisticados cuentan con grandes capacidades y técnicas de intrusión innovadoras, sus ganancias por ataque son altas y regularmente sus ataques están dirigidos a víctimas con un alto perfil económico que a su vez tienen un nivel de concientización, protección y seguridad elevado, por ende, las ganancias son bastas aunque en un bajo volumen de víctimas. Esto se traduce en un alto volumen de ganancias obtenidas en un bajo volumen de víctimas que en muchos casos se tiene que llegar a una investigación cibernética para identificar a los atacantes.

- Se establecen como retos en materia de ciberseguridad las iniciativas que impulsen las capacidades en la investigación, la formación y desarrollo de capacidades en ciberseguridad, la prevención como mecanismo de combate al cibercrimen, la cooperación nacional e internacional, y la armonización legislativa en la materia.

- Es de suma importancia la asistencia legal mutua con otros países del orbe, por lo que se considera revisar la importancia que tiene la adhesión de México al Convenio de Budapest en términos de armonización legislativa a nivel internacional, con la finalidad de allanar el camino a la investigación transfronteriza, la incursión de cibercriminales se ha hecho presente en los últimos años y requiere de una atención integral.

FUENTES DE CONSULTA

- Internet Organised Crime Threat Assessment, EUROPOL, 2016

- World Economic Forum, Global Risks 2013 [en línea], [fecha de consulta: Abril 2016]. Disponible en: http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2013.pdf
- Internet SecurityThreat Report, Symantec (2015)
- Norton by Symantec, Reporte Norton 2013 [en línea], [fecha de consulta: Abril 2016]. Disponible en: https://www.symantec.com/content/es/mx/about/presskits/b-norton-report-2013-final-report-lam-es-mx.pdf
- Trend Micro, Latin American and Caribbean Cybersecurity Trends and Government Responses [en línea], [fecha de consulta: Abril 2016]. Disponible en: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-latin-american-and-caribbean-cybersecurity-trends-and-government-responses.pdf.
- Norton by Symantec, Op. Cit., [fecha de consulta: Abril 2016]. Disponible en: https://www.symantec.com/content/es/mx/about/presskits/b-norton-report-2013-final-report-lam-es-mx.pdf
- Asociación Mexicana de Internet, Estudio Comercio Electrónico en México 2015 [en línea], [fecha de consulta: Abril 2016]. Disponible en: https://amipci.org.mx/estudios/comercio_electronico/Estudio_de_Comercio_Electronico_AMIPCI_2015_version_publica.pdf
- Instituto Nacional de Estadística y Geografía, 2015. [fecha de consulta: Mayo 2016] http://www.inegi.org.mx/saladeprensa/boletines/2016/especiales/especiales2016_03_01.pdf
- Unión Internacional de Telecomunicaciones, UIT 2009, Aspectos Generales de la Ciberseguridad [fecha de consulta: Abril 2016]. Disponible en PDF en: https://www.itu.int/rec/T-REC-X.1205-200804-I/es

- Unión Internacional de Telecomunicaciones, ICT Facts & Figures 2015 [en línea], [fecha de consulta: Abril 2016]. Disponible en: http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf.
- Organización de las Naciones Unidas, Objetivos de Desarrollo del Milenio [en línea], [fecha de consulta: Abril 2016]. Disponible en: http://www.undp.org/content/undp/es/home/sdgoverview/mdg_goals/

PRODEIIN 2013-2018, Censos Económicos (2009). Micro, pequeña, mediana y gran empresa : estratificación de los establecimientos : Censos Económicos 2009 / INEGI, c2011. 2013 [en línea], [fecha de consulta: Abril 2016]. Disponible enhttp://www.institutopyme.org/index.php?option=com_content&view=article&id=134&,