EDI

Revista digital - edición n°28

Los Destacados del Año 2017

En esta edición

DICIEMBRE 2017

2018

Loading

LO IMPORTANTE QUE VIENE

ELDERECHOINFORMATICO.COM

Fernando Cervoni
Puerto Rico

Joel Gomez Treviño
México

Daniel Ortiz Lora
Mexico

Enmanuel Alcantara
República Dominicana

(EDI)

La Red
Puerto Rico
México
Rep. Dominicana
Guatemala
Venezuela
Ecuador
Costa Rica

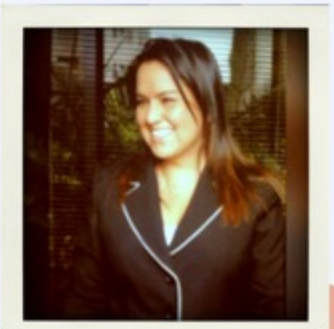
José Leonett
Guatemala

Rafael Martinez
Venezuela

Carlos Tudares
Venezuela

Rafael Montenegro
Costa Rica

Paulina Casares
Ecuador



Hildamar Fernandez
Venezuela

Alvaro Andrade Sejas
Panamá

Katiuska Hull Hurtado
Panamá

Yoselin Vos
Panamá

(EDI)

La Red

Panamá

Colombia

Alvaro Soto
Colombia

Victor Anttinoti
Panamá

Heidy Balanta
Colombia

Emanuel Ortiz
Colombia

Jefferson Espinoza Vera
Colombia

Ana Mesa Elneser
Colombia

Colombia

Humberto Carrasco
Chile

Elisabeth Bouvier
Uruguay

Jazmin Ibarrola
Paraguay

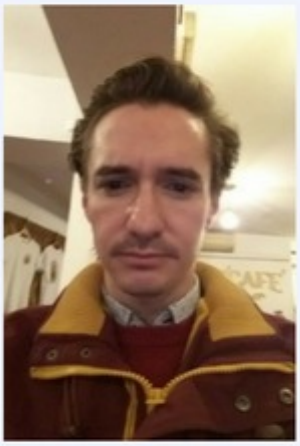
Gunter Krone
Paraguay

(EDI)

La Red
Chile
Uruguay
Perú
Paraguay
Brasil
España

Karen Céspedes
Perú

Wilson Furtado
Brasil

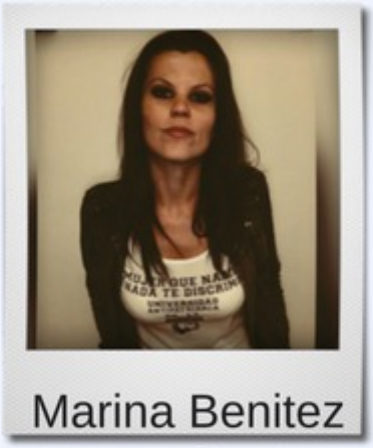


Pedro Macias
Esáña

Jorge Campanillas
España

Laine Souza
Brasil

Eugenia Lo Giudice
Argentina



Marina Benitez
Demtschenko
Argentina

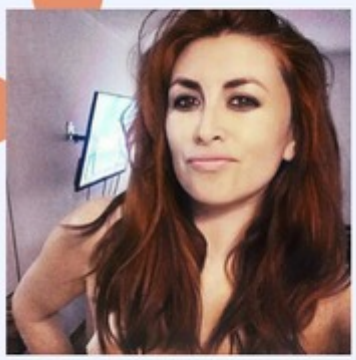
Natalia Toranzo
Argentina

Analía Martinez
Argentina

(EDI)

La Red

Argentina



Carolina Marín
Argentina

Sebastián Gamen
Argentina

Marcelo Lozano
Argentina

Fedra Fontao
Argentina

Eugenia Orbea
Argentina

Rubén Avalos
Argentina

Sonia Boiarov
Argentina

SOMOS EDI LA RED

EL CENTRO DE INFORMACIÓN

y contenidos
más grande iberoamerica

TWITTER: ELDERECHOINF

CONTENIDO

EDITORIAL

REVISTA DIGITAL EDICIÓN NRO 28 - EDI

Llegó la edición 28, por fin para mi por lo menos, la última del 2017 y primera del 2018, con 15 días de atraso pero con las mismas ganas de siempre. En esta edición contamos con invalorables aportes, les aseguro que no se van a defraudar con los contenidos, también les contamos quienes son los DESTACADOS DEL 2017 para la RED EDI. Verán gente conocida, gente mas o menos conocida y algunos que no tienen idea quienes son, bueno, la idea siempre ha sido que nuestros destacados sean aquellos que, por diferentes razones están siempre en el candelero. El criterio utilizado podría decirse que es simple, están quienes fueron muy votados (hubo más de 155 votos postulando candidatos), hubo otros que si bien no fueron tan votados, tuvimos conocimiento de su trabajo por diferentes vías a lo largo del año, hubo quienes a pesar de ser votados, no llegaron a justificar su aporte como más relevante que el de otros. Resumiendo, quienes están tienen su porqué, los que no, simplemente no se dio en esta oportunidad. LOS DESTACADOS DEL AÑO DE EDI, no es un premio, no es un concurso, es simplemente una "opinión" de unos cuantos o muchos que aportaron su criterio u propuesta.

Especial agradecimiento a la Dra Benitez Demtschenko por su colaboración en la maquetación

"Todo el mundo trata de realizar algo grande, sin darse cuenta de que la vida se compone de cosas pequeñas."

- Frank Clark

es un simple recordatorio para gente que nos consta trabajó mucho por lograr la difusión del derecho informático, nada más.-

Este año la Red tendrá novedades como siempre, hay nuevos convenios con Universidades que nos permitirán brindar capacitaciones de calidad, insistiremos con los Congresos haciendo especial énfasis en la injerencia y valor de la mujer en el mundo jurídico/tecnológico, no porque creamos que necesitan ser impulsadas de manera diferente, sino porque entendemos que es el momento de validar y poner de relieve su labor y empuje..-

No hace falta decir que continuaremos con la Revista, ampliaremos nuestra videoteca y buscaremos con afán seguir innovando en materia de congresos, tenemos como deuda pendiente el I CONGRESO MUNDIAL ONLINE DE DERECHO INFORMÁTICO con una modalidad de formato grabado y en vivo, seguiremos con entrevistas de un minuto en video, volveremos con los Podcast y no permitiremos que se olviden que lo mejor que nos da esta vida es la posibilidad de hacer, por eso, no debemos quedarse con ideas que parecen maravillosas, jueguensela, busquen hacer la diferencia, insistan, no abandonen,peleen por lo que creen, sigan adelante que la vida es eso, es hacer, porque

Nuevos Trabajos en la Red Las WebCamers

*** Lucrezia Vigliocco . Miembro de AGEIA DENSI**
+ Carlos Dionisio Aguirre

1) Introducción.

A Internet se le acusa de destruir empleo, se ha llegado incluso a decir que una compra por la red, implica que un dependiente que está en una tienda física, pierda su empleo. Pero esta sentencia es quizás demasiado exagerada y trataré de demostrar que tal afirmación carece de fundamento.

En primer lugar, recientes estudios de consultoras, demuestran que Internet genera una media de 2,6 empleos por cada trabajo físico que se pierden en el canal tradicional[1]. Y en segundo lugar, la Industria del Internet se convirtió en una de las principales fuentes de trabajo, en los países del primer mundo, ya que permite que personas de todo el mundo, trabajen en empresas vinculadas a la red.

2) Nuevas Formas de Trabajo:

Los trabajos en la Nueva Realidad son contratados, desarrollados y ejecutados en línea. La localización del trabajador no es importante y puede estar en cualquier lugar del planeta, con el solo requisito de tener un dispositivo conectado a Internet.

El trabajo se encuentra a escala global, y los precios del mismo son fijados también a escala mundial.

Pero, muchas personas del mundo, no acceden todavía a Internet, y esto por las numerosas causas de la brecha digital que impiden ese acceso.

Internet permitiría generar empleos para 4.000 millones de personas. Los países o sectores de la población global que no aún no tienen acceso a la red es porque aún se encuentran en desarrollo hacia esa conectividad, que deberían mejorar radicalmente, para poder crear una vida mejor y más sostenible para sus habitantes.

Cuando éstas personas logren el acceso a Internet, se encontrarán con una nueva forma de progresar, mejorar su economía y de hacer dinero, se conectarán con millones de personas de todo mundo, a través de las redes sociales y les surgirá la curiosidad de cómo ganar dinero a través de ellas. Y aquí, es donde empresas, mercados y servicios on-line, entran en juego, y se convierten en medios o caminos para salir de la pobreza, y por ende llevar una mejor calidad de vida.

[1] Cifra proporcionada por la consultora Worldwide Mobile Worker Population, año 2011-2015.

Con acceso a Internet, no importa donde alguien vive, no importa su condición socio económica, lo que importa es que a través de Internet las personas pueden acceder a educación gratuita (conocimientos) y generar fuentes de ingresos a través del mercado global.

Las regulaciones en este campo conocido como **teletrabajo,** también empiezan a ser discutidas en los diferentes países y de manera incipiente, se empieza a hablar de la agremiación de estos trabajadores fronteras adentro en los distintos Estados, aunque éstas regulaciones pierden virtualidad en el marco de la red global de alcance transnacional.

3) Regulación del teletrabajo en Argentina:

El Ministerio de Trabajo, busca regular por ley el teletrabajo, que incluirá a quienes trabajan desde el país para el exterior; y además, asegurar condiciones mínimas de trabajo y derechos para empleados que trabajan desde sus casas.

El **teletrabajo** es una modalidad cada vez más extendida en las empresas, pero **no existe aún una ley que lo regule**. Solo tenemos un **proyecto de ley de Teletrabajo**, que el Ministerio de Trabajo viene impulsando hace varios años, que está más cerca de llegar al Congreso. Se trata de una nueva versión, con modificaciones, de un proyecto elaborado en 2007 pero que no llegó a ser tratado en el Congreso. **El proyecto contempla que se aplique la ley del país que sea más favorable para el trabajador**.

Otro punto de la iniciativa, es el otorgamiento de un plus para el empleado que tele trabaje que le permita compensar los gastos, como la electricidad o la conexión a Internet, que le genera trabajar en su casa y, además, el cumplimiento de normas de seguridad e higiene en el domicilio. También contemplará la "reversibilidad" del teletrabajo: el empleado que comenzó en la empresa como trabajador presencial y luego optó por el teletrabajo tendrá la posibilidad de volver a su situación anterior.

El proyecto contempla una **igualdad entre un trabajador presencial y un teletrabajador que ocupen la misma posición**, por ejemplo, en el derecho a la formación y en las licencias. Y define al teletrabajo como una modalidad laboral que se puede llevar adelante desde el domicilio del trabajador o desde otro espacio ajeno a la empresa.

Desde 2008, el Ministerio de Trabajo cuenta con un Programa de Seguimiento y Promoción del Teletrabajo en Empresas Privadas (Propet) que hoy integran alrededor de 40 compañías, entre ellas YPF, Telecom, Cisco y Dell. En 2013, a través de una resolución, también comenzó a monitorear la aplicación de esta forma de trabajo en esas empresas.

4) Trabajo en la Internet:

Actualmente en la red, tenemos extensa gama de oportunidades laborales, por ejemplo: Traducción y transcripción; Experto en Big Data ; Programadores; Periodismo de datos; Redactores de contenidos; Gestión de comunidades online; Analistas web; Asistente virtual; Webcamers; Elaborar pronósticos Deportivos; Tarot On-Line, entre otros.

Pero he decidido hacer zoom, sobre las **webcamers**, porque particularmente, me ha

llamado la atención dicho mercado laboral.

4.1. Webcamers:

Ser webcamers en si es una vocación, no es para todo el mundo. Es un trabajo como cualquier otro, donde se exige esfuerzo y dedicación. Se puede realizar desde sus casas o estudios.

Webcamers es la persona que por medio de su cuerpo y carisma ofrece un servicio de entretenimiento para adultos (shows y conversaciones eróticas) por medio de páginas web, donde los usuarios pagan para interactuar con la webcamers.

Todo el **contenido realizado es erótico y fantasioso**, a través de la **red**. En ningún momento hay contacto físico REAL con el usuario que está accediendo al servicio de entretenimiento. Es decir, **es todo VIRTUAL**. No se pasan datos personales reales.

En estos tiempos, lo VIRTUAL es un dispositivo generador de un nuevo tipo de realidad. Una **RELACION VIRTUAL** entre dos personas, tiene las siguientes características:

*** Es actual**: pertenece a lo que cada persona es en este momento. Se conecta la memoria y el deseo.

***Es fantástica**: Se realiza nuevas experiencias, que en gran medida son inconscientes. Se satisface necesidades. Se inventa un nuevo personaje a medida de cada cliente o usuario.

***Es potencial:** Se crean nuevos "personajes", con nuevas fuentes de experiencia, a diferencia de las relaciones clásicas (cara a cara). En el mundo virtual es todo posible, pero no es llevado a la práctica.

Las relaciones virtuales, se crean de forma voluntaria y dentro los límites de la mente. Es un fenómeno, puramente psicológico.

Teatro Virtual: Las "modelos webcam" trabajan desde una cámara web encendida y realizan sus shows que duran de cuatro a seis horas diarias, donde personas de todo el mundo admiran un show en vivo. Todos cumplen sus fantasías y deseos mediante solo un click.

¿Qué es una página webcam?: Se trata de un espacio virtual, que permite que modelos y clientes se conecten para que chateen entre sí, acompañados de video (similar a una videollamada).

Los pagos a las modelos se realizan a través de plataformas, que permiten transacciones con tarjetas de crédito, para que los clientes puedan pagar por los servicios

El Video Chat es mundial: El negocio del video chat erótico, se mueve en distintas páginas de carácter mundial, donde los interesados deben registrarse, ya sea para ser webcamers o ser usuario o cliente.

La misión de las webcames es atrapar con sus encantos y sensualidad a los usuarios, para que paguen por pasar tiempo viéndolas. La ganancia de cada modelo, depende de cada página, puede ser en minutos o tokens.

Los países más consumidores de páginas webcam: Son EEUU y países donde reina el Euro. Y en menor escala, algunos países latinos como Chile, Perú y Ecuador. Los países latinos, son clientes en menor proporción, por el cambio de su moneda local con el dólar o euro.

Perfil de las webcamers: La mayoría son universitarias que realizan su labor antes o después de clases. También hay un alto porcentaje de madres que realizan este trabajo, cuando sus hijos duermen, concurren a los

colegios, clubes, etc. Es requisito esencial para trabajar como webcamers: ser mayor de edad (18 años), tener un ordenador, webcam y obviamente, acceso a la red; o trabajar desde un estudio.

Legalidad en el mundo webcam**: ¿Es legal ser webcam?** La respuesta es **SI**. Solo debe tener en cuenta que mientras **NO IMPLIQUE LA PARTICIPACION DE MENORES DE EDAD** es una actividad laboral y empresarial que se puede llevar a cabo sin ningún tipo de restricción.

Quienes se dedican al negocio de modelos webcams, son personas que están vinculadas al entretenimiento para adultos, actividad que está íntimamente relacionada con el **derecho constitucional a la intimidad** (art.19 CN) que reza: " las acciones privadas de los hombres, que de ningún modo ofendan al orden y la moral pública, ni perjudiquen a un tercero, están sólo reservadas a Dios, y exentas de la autoridad de los magistrados": Y por ello, le guste o no a la gente conservadora, el videochat es un negocio que puede llevarse a cabo, sin ningún tipo de inconvenientes.

¿Es legal ser webcamer? La respuesta es si

5. Bibliografía:

http://www.laopiniondezamora.es/blogs/por-internet/la-influencia-de-internet-en-la-economia-local-e-internacional.html

https://www.cronista.com/negocios/Buscan-regular-por-ley-el-teletrabajo-una-modalidad-cada-vez-con-mas-adeptos-20150406-0004.html

https://www.minutouno.com/notas/356855-internet-permitira-generar-empleos-4000-millones-personas

Retroceso de Derechos Humanos en tiempos tecnológicos. Visión Restaurativa.

RESEÑA AUTOBIOGRÁFICA

Romina Florencia Cabrera. Abogada egresada de la UNLP (Argentina). Investigadora-Docente en la UBA (Invitada de la Especialización en Derecho Informático), y en la USAL (Maestría en Ciencia de la Legislación). Estudios de Posgrado sobre Recursos Humanos (UNLP), en Diplomacia Digital (DiploFoundation, Ginebra, Suiza), y sobre Seguridad (ASCASEPP). Doctorando en la UNLP. Miembro del Observatorio Iberoamericano de Protección de Datos; del Instituto de Derecho Constitucional y Político de la Facultad de Ciencias Jurídicas y Sociales de la UNLP, y de otras instituciones Científico -Académicas.

Las conquistas sociales son maravillosas, pues permitieron un avance en el respeto a los Derechos Fundamentales y en el avance de la Humanidad, hacia el logro de la paz y convivencia social. Lo hemos observado en Tratados, Convenios de Cooperación Internacional e internos, en procesos judiciales, en la Academia, en el arte, en la vida cotidiana…

Una sociedad que no utiliza con frecuencia actitudes y términos discriminatorios, que integra de manera inclusiva a sectores vulnerables y diversifica sus políticas públicas hacia un enfoque más amplio y tolerante, avanza sin ninguna duda hacia un estado superior en estándares de respeto a los Derechos Humanos.

Las Tecnologías de las Información y la Comunicación son maravillosas para unir personas y proyectos, acortan distancias y mejoran la transmisión de los mensajes: pero que sucede cuando el discurso de odio y menoscabo de esos Derechos Fundamentales se hace presente en estos medios tecnológicos?...

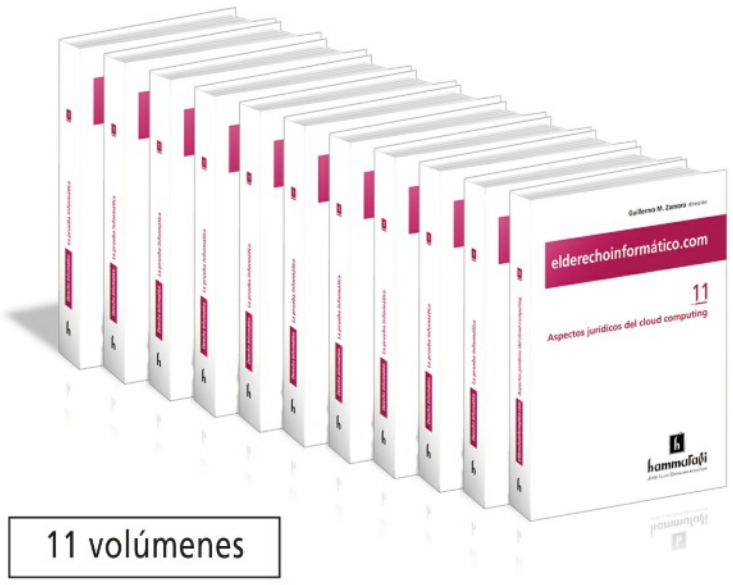
El caso de Internet y su mayor manifestación, las Redes Sociales, ha

librería | hammurabi

Talcahuano 440 - C1013AAI
CABA - Argentina
Tel.: (54-11) 4371-8179
info@libreriahammurabi.com.ar

en preparación

Colección «elderechoinformático.com»



11 volúmenes

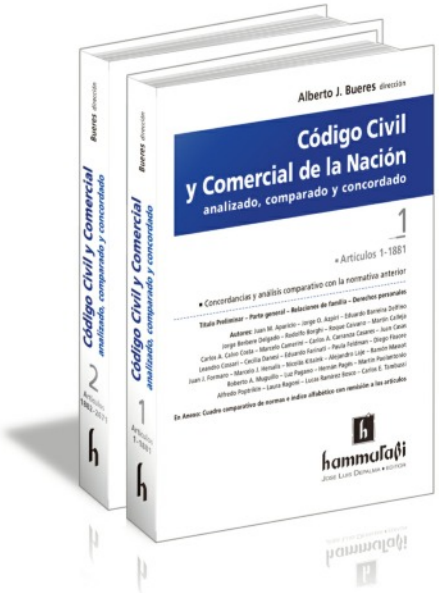
Guillermo M. Zamora dirección

1 — La prueba informática
2 — Negocios jurídicos en tiempos de Internet
3 — Delitos informáticos
4 — Propiedad intelectual en la era de la información
5 — Gobierno digital y gobierno abierto
6 — Datos personales, su protección
7 — ODR, Resolución de Disputas Online
8 — Firma digital
9 — Régimen jurídico de nombres de dominio
10 — Teletrabajo
11 — Aspectos jurídicos del *cloud computing*

Novedad

Código Civil y Comercial de la Nación

analizado, comparado y concordado



Alberto J. Bueres dirección

2 tomos | Artículos 1 - 2671

Análisis complementario de las principales normas que inciden en el «Derecho del trabajo» al cuidado de Juan J. Formaro

Contiene: Cuadro comparativo de normas. Indice alfabético de voces

• **Tomo 1. Arts. 1 a 1429.** **Autores:** Juan M. Aparicio – Jorge O. Azpiri – Eduardo Barreira Delfino – Jorge Berbere Delgado – Rodolfo Borghi – Martín Calleja – Marcelo Camerini – Carlos A. Carranza Casares – Rubén Compagnucci de Caso – Leandro Cossari – Cecilia Danesi – Paula Feldman – Diego Fissore – Juan J. Formaro – Marcelo J. Hersalis – Germán Hiralde Vega – Nicolás Kitainik – Alejandro Laje – Sabrina Luini – Ramón Massot – Luz Pagano – Hernán Pagés – Alfredo Popritkin – Laura Ragoni – Lucas Ramírez Bosco – Carlos E. Tambussi.

• **Tomo 2. Arts. 1430 a 2671.** **Autores:** Liliana Abreut de Begher – Beatriz Areán – Jorge O. Azpiri – Eduardo Barreira Delfino María I. Benavente – Gabriela Boquin – Roque Caivano – Carlos Calvo Costa – Marcelo Camerini – Juan Casas – Federico Causse Rubén Compagnucci de Caso – Leandro Cossari – Nelson Cossari – José Fajre – Eduardo N. Farinati – Juan J. Formaro – Andrés Fraga – Alberto Gabás Lidia Garrido Cordobera – Marcelo J. Hersalis – Gabriela Iturbide – Jorge Juliá – Alejandro Laje – Ricardo Nissen – Martín Paolantonio Christian R. Pettis – Lucas Ramírez Bosco – Javier Rosembrock Lambois – Luciana Scotti – Gabriel Ventura – Luis M. Vives.

aumentado la velocidad y frecuencia de esa trasmisión de mensajes. Estamos totalmente de acuerdo con una internet abierta, inclusiva, libre y diversa para todos los sectores. Pero la libertad de expresión no implica la lesión al honor y a la dignidad humana de Grupos sensibles, sujetos de persecución y discriminación, víctimas de manifestaciones neonazis o extremistas de todo tipo.

El avance logrado en materia de Protección y Promoción de los Derechos Humanos a través de mecanismos y Tratados Internacionales, se ve menoscabado por los mensajes ofensivos y discriminatorios en los medios digitales.

No estamos procurando censura en Internet. Eso sería el mayor error de todos los tiempos. Internet debe ser libre y abierta para todos los sectores, según el modelo de Múltiples partes interesadas en su gestión. Lo que se debe procurar, es un debido seguimiento, identificación y detección de estos grupos, para que debidamente retiren ese contenido violento de la Web, y además reciban una pena tipificada en los Códigos Penales, más un complemento de arrepentimiento diagramado dentro de la Justicia Restaurativa, para promover valores y lograr una mediación y respeto hacia las víctimas.

La Dra. Aída Kemelmajer de Carlucci (2004; p.10) precisa a la Justicia Restaurativa como "(...) a la variedad de prácticas que buscan responder al crimen de un modo más constructivo que las respuestas dadas por el sistema punitivo tradicional (...)" Esta vía lo que busca, tal como lo enuncia Zehr (2007) es "(...) involucrar, dentro de lo posible, a todos los que tengan interés en una ofensa particular, e identificar y atender colectivamente los daños, necesidades y obligaciones derivadas de esa ofensa (...)" En una sociedad que se encuentra en crisis, presentando hechos cada vez más violentos y que se presenta intolerante ante el otro, referirnos a la Justicia Restaurativa es una apuesta ardua, pese a ello emerge necesario ponerla en marcha, a los efectos de la construcción de un sistema de justicia que garantice la paz social.[1]

El infractor, que asume los hechos responsablemente y se hace cargo de sus propias acciones, es un motor que genera un triple incentivo optimista: a) para con él mismo, ya que es más fácil cumplir con el compromiso voluntariamente asumido que con una condena impuesta por el sistema punitivo tradicional, a la vez que le otorga una legitimidad mayor ante sí mismo y ante la sociedad, reconociendo su error y buscando reparar el daño causado; b) para con la víctima, que logra conocer del propio infractor las razones y la historia detrás del hecho que lo perjudicó, lo coloca en la situación de protagonista del procedimiento, evitando la situación de postergación que viviría en un proceso penal tradicional y, eventualmente, obtener un sincero pedido de disculpas; c) la comunidad logra mantener la

[1] "Justicia Restaurativa, Mediación penal y principio de Oportunidad: Nuevos caminos a la adopción de un sistemas pacífico de resolución de conflictos en el sistema penal". Sitio Web: http://www.saij.gob.ar/maria-victoria-cavagnaro-justicia-restaurativa-mediacion-penal-principio-oportunidad-nuevos-caminos-adopcion-sistema-pacifico-resolucion-conflictos-sistema-penal-dacf150826-2015-11-11/123456789-0abc-defg6280-51fcanirtcod . Fecha de Consulta del Sitio : 23/10/2017.

paz en su seno, con la posibilidad de participar en el procedimiento de resolución del conflicto y generar los canales para evitar futuros hechos similares.

El propósito principal que busca alcanzar la Justicia Restaurativa, como el mismo término indica, no es otro que el de "reparar", más no hay que dejarse llevar por la inercia de pensar que hace referencia a una mera compensación económica del daño causado, puesto que cuando en la Justicia Restaurativa se habla de "reparar", se apunta más allá y con un sentido más profundo y trascedente de lo que la teoría general del derecho de daños refiere.[1]

PRINCIPIO DE LEGALIDAD Y PRINCIPIO DE OPORTUNIDAD:

"Nullum crimen, nulla poena sine praevia lege", célebre axioma en latín, que plasma el denominado "Principio de Legalidad Penal", que consiste en el fundamento en virtud del cual ningún hecho puede ser considerado como delito sin que una ley anterior lo haya previsto como tal, que en nuestro país posee jerarquía constitucional

La ley penal in abstracto describe una conducta como punible y prevé una sanción. No obstante, es necesario que el Estado -quien tiene el monopolio de la fuerza- a través de sus órganos persecutorios impulse la investigación y verifique la existencia del hecho, la participación del imputado y, si corresponde, aplique la sanción al responsable. Esto, se conoce como "principio de oficialidad", que no debemos confundirlo con el "principio de legalidad procesal", según el cual tiene el Estado la obligatoriedad de la persecución, de todos los hechos punibles de los que se tome conocimiento. De este modo, nuestro país consagra el principio de legalidad (o indisponibilidad), que puede entenderse como "la automática e inevitable reacción del Estado a través de sus órganos predispuestos, para que frente a la hipótesis de la comisión de un hecho delictivo comiencen a investigarlo, reclamen luego el juzgamiento y si corresponde el castigo.[2]

Por otra parte, en materia de política criminal, cabe mencionar el "principio de oportunidad (o disponibilidad)", al que no debemos ver como antinomia del de legalidad -aunque mayormente así sucede- y que puede definirse "como la posibilidad que la ley acuerda a los órganos encargados de la investigación penal, por razones de política criminal o procesal, de no iniciar la investigación o suspender provisoriamente la ya iniciada, limitarla objetiva o subjetivamente, hacerla cesar definitivamente antes de la sentencia, aplicar penas inferiores a la escala penal fijada legalmente para el delito, o eximir a los responsables de ella ".

La mediación considera las causas reales del conflicto y las consecuencias del mismo, buscando la fórmula más idónea para satisfacer las necesidades personales de la víctima y del presunto infractor.[3]

[1] Óp. Cit. 1

[2] Óp. Cit. 1

[3] Óp. . Cit. 1

Al decir del Dr. Norberto Daniel Barmat (2000), la mediación aparece como "un procedimiento institucional, tramitado previamente a la celebración de un proceso penal, en el cual un funcionario público, denominado mediador, colabora para que los actores del conflicto derivado de un hecho delictivo, conocido por alguna de las agencias del sistema penal, busquen solucionar sus diferencias a través de una negociación. El cumplimiento de un acuerdo lícito logrado entre las partes, extingue la pretensión penal". Tanto en un juicio como en un proceso de mediación se presta un servicio de justicia, con la diferencia que en el primero, las partes pretenden que el juez (un tercero) decida qué es lo justo, mientras que en la mediación son los mismos participantes quienes se hacen cargo de un conflicto. Esto genera conciencia de responsabilidad y compromiso futuro para la resolución de otros conflictos que se presentan en cualquier orden de la vida.[1]

Los Discursos de Odio deberían prevenirse a través de la incorporación de esos sistemas de Control y Retribución social, para avanzar como Sociedad Integradora y Supera dora de Conflictos, hacia una Pacificación de las Disputas y a un orden en la Era Digital, para gozar de manera más eficiente y eficaz de los Derechos Fundamentales, y de las ventajas tecnológicas.

Autora: Romina Florencia Cabrera

[1] Óp. Cit. 1.

CySI

ESTUDIO DE INFORMÁTICA FORENSE

ASESORARSE CON UN PERITO INFORMÁTICO FORENSE

PUEDE SER VITAL PARA GANAR UNA DEMANDA
O EVITAR UNA CONDENA

NUESTROS SERVICIOS

- Asesoramiento Informático – Jurídico
- Peritos de Parte
- Obtención de evidencia
- Análisis forense digital

NUESTROS PRODUCTOS

- Duplicador / Bloqueador Forense
  - DITTO® FIELDSTATION FORENSE
  - DRIVEDOCKS AND FORENSIC DOCKS
- Software Forense de investigación
  - NUIX

CRU

nuix

Simple. Powerful. Precise.

info@cysi.com.ar
(+54 11) 5199 5535
(+54 9 11) 5463 4098 / 5257 8889

TOR EXIT NODES EN LA JUSTICIA ARGENTINA.

Autores: Dra. Johanna C. Faliero y Dr. Rodrigo S. Iglesias.[1]

INTRODUCCIÓN.

Iván Barrera Oro, sufrió una investigación judicial sobre el delito informático más estigmatizante del Código Penal Argentino, siendo notoria su investigación sobre sistemas electorales electrónicos y la exposición pública en diferentes ámbitos, un fiel defensor de derechos humanos y hacktivista argentino, fue investigado por producción y distribución de pornografía infantil.

El CASO.

En fecha 8 de agosto de 2013 se traficó una imagen de pornografía infantil en la RRSS 4chan, la dirección IP desde la cual se realizó la publicación es 190.17.31.178 proveniente de Argentina, Buenos Aires, Capital Federal, dicha red social realiza la denuncia del hecho a NCMEC el 6 de julio de 2015 mientras en la Argentina se realizan las elecciones a Jefe de Gobierno de la Ciudad Autónoma de Buenos Aires con el sistema de Voto Electrónico; el viernes anterior recibía un allanamiento en su domicilio Joaquín Sorianello a quien luego se le archivaría la causa judicial de oficio (propia desición) por parte del fiscal al no poder demostrarse delito alguno en contra de su persona. Como es de público conocimiento Iván Barrera Oro es uno de los investigadores informáticos que informaron distintas vulnerabilidades en dicho sistema de votación (colocar más de un voto por boleta, quemar los chips RFID, exponer sobre la problemática en El Honorable Senado de la Nación Argentina, etcétera), Iván además de investigador es hacktivista y desde hacía varios años tenía un nodo de salida de TOR funcionando en su domicilio.

El 6 de junio de 2016 Iván Barrera Oro, a raíz de la denuncia realizada por 4Chan en NCMEC y ésta enviada al Ministerio Publico Físcal de la Ciudad Autónoma de Buenos Aires y a solicitud del Fiscal Lopez Zavaletta y concedido por el Juez Aostri, recibe el allanamiento a su domicilio y el secuestro de sus equipos electrónicos (smartphones, notebook, DVDs, GoPro, modem), en cuya orden de allanamiento

[1] Ambos son Socios Fundadores del Estudio Faliero & Iglesias.

estipulaba el secuestro de estos equipos, pero cometieron el error de dejar en el domicilio dos estuches con DVDs con la inscripción “fotos” (recuerden que la denuncia es por la publicación de una “foto” de pornografía infantil), además de no proceder a revisar el domicilio de forma completa en busca de “cualquier dispositivo de almacenamiento informático” sino que dejaron todas las llaves físico-lógicas de cifrado, que una vez que los oficiales de la Policía Metropolitana se retiraron del domicilio Iván procedió a “quemarlos” en su horno a microondas por el temor y seguridad de sus equipos; en ese momento Iván trabajaba en el Enacom (Ente Nacional de las Comunicaciones) donde tenía información confidencial y de sumo resguardo por la sensibilidad de la información contenida en sus equipos que podrían ser utilizadas para inferir en las comunicaciones en el País.

Iván se pone en contacto con el Abogado Rodrigo Iglesias, especialista en Delitos Informáticos y quien ya había defendido con éxito a Joaquín Sorianello, viejos conocidos de los eventos del Flisol (Festival Latinoamericano de Instalación de Software Libre), quien acepta el cargo de abogado defensor sin dudar y la Perito de parte Licenciada Patricia Delbono en conjunto.

En el descargo que realizan ante la justicia se indica que en el horario indicado por 4Chan como hora de la publicación dicha dirección IP era utilizada como nodo de salida de Tor dado que así lo informa el Exonerator de Tor (https://exonerator.torproject.org/), donde además de corroborar el uso del nodo de salida de Tor en ese horario es evidente, el nombre del nodo era Bradley Manning (hoy sería Chealsy Manning).

En diciembre de 2016 comenzamos al pericia informática sobre los elementos secuestrados a Iván en el Centro de investigaciones Judiciales del Ministerio Publico Fiscal de la Ciudad Autónoma de Buenos Aires (CIJ), donde la intención de darnos una copia forense informática de todos los dispositivos de almacenamiento fue la medida indicada por el CIJ y rechazada de plano por la defensa, dado que de contener la imagen o material de cualquier tipo que implique pornografía infantil estaríamos ante el delito de distribución de pornografía infantil (parece que los fiscales especializados en delitos informáticos no entienden que ellos también pueden cometer delitos), solicitamos una Audiencia de Nulidad sobre la pericia en curso (sabiendo que al no estar concluida la pericial, el resultado de la audiencia iba a ser negativo) con el fin de explicarle los delitos que podría acarrear la distribución de material forense informático por parte del CIJ y los derechos que amparan a realizar la pericia en conjunto tanto del perito de la defensa (la Licenciada Delbono) su abogado (Dr. Rodrigo Iglesias) como de los peritos oficiales del CIJ. Esto último es lo que ocurrió, ambos profesionales pudieron realizar la pericia y la Licenciada Delbono realizo en conjunto con los peritos oficiales del CIJ el informe pericial, sin antes solicitar colaboración a Iván para poder acceder al Root del equipo de escritorio que pudo rescatar una de las llaves físico-lógica para poder acceder a esa parte del sistema, y dado que no era posible realizar el encendido del equipo para descifrar la copia forense

realizada se solicito la colaboración de Iván (quien además de colaborar con dicha llave indico como utilizar la misma) dado que de no realizarse dicha colaboración la causa judicial no tendría un resultado favorable y sería solo una prescripción por falta de elementos fáctico para realizar la debida pericia forense informática.

Demostrar que lo indicado en la declaratoria realizada por Iván era una cuestión de tiempo, cuanto? el tiempo que pueden demorar en realizar una pericia informática de forma correcta y esperar el informe pericial, obviamente el resultado fue favorable a la defensa e Iván, y solicitamos el correspondiente sobreseimiento, no solo dieron por prescrita la causa judicial y además el sobreseimiento de Iván sino que sumamos algunos puntos en la investigación de delitos informáticos para que se puedan agilizar procesos en la investigación judicial sobre distribución de pornografía infantil en Argentina, brindando conferencias en distintos lugares (como en Ekoparty), donde se explico el error del accionar de Mariano Manfredi, Enrique Del Carril (ambos pertenecientes al Centro de Investigaciones Judiciales del Ministerio Publico Fiscal de la Ciudad Autónoma de Buenos Aires) que deberían entender que el accionar tiene que ser los mas expeditivo posible y verificar si el mismo se encuentra siendo un nodo de salida de Tor (con ingresar los datos en https://exonerator.torproject.org/ con la fecha del hecho es suficiente) y no secuestrar los equipos sino solicitar la colaboración correspondiente para investigar el delito cometido, no entregar copias forenses de evidencia informática dado que la misma puede no solo conllevar a un delito sino que la pericial debe ser realizada en conjunto, para no generar ningún tipo de inconvenientes.

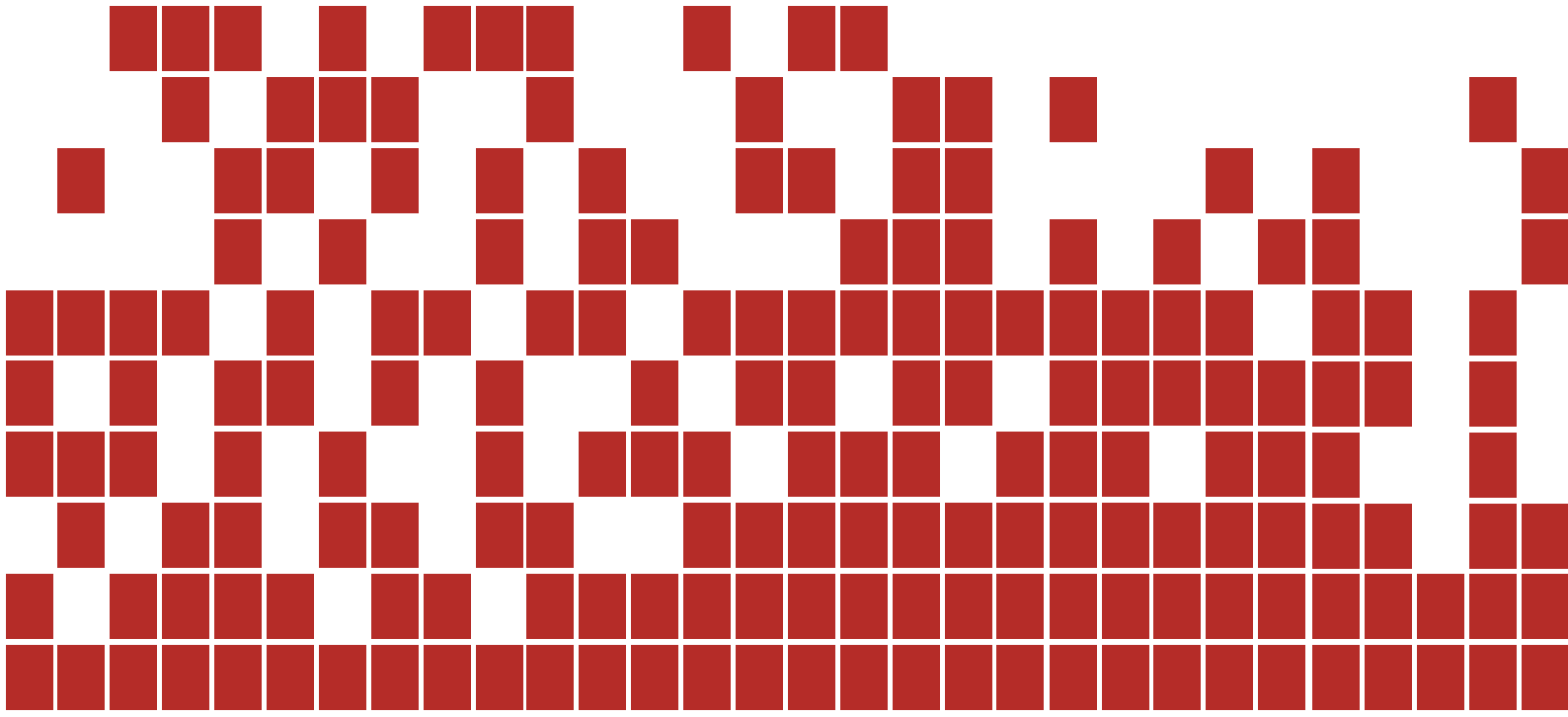
Así mismo, los Derechos Humanos son garantizados en la Constitución Nacional Argentina y habiendo adherido a varios Tratados de Derechos Humanos es que debemos garantizar y asegurar la libertad de expresión, la intimidad y privacidad de las personas, la confidencialidad de las comunicaciones entre las personas, es por esto que Tor en a Argentina es legal e Iván Berrera Oro es evidencia que una dirección IP no es necesariamente una persona física, y que ser un nodo de salida de Tor no evita los delitos, no los realiza, es solo una herramienta para garantizar Derechos Humanos, el resto es una utilización ilegal de una herramienta.

Iván siempre fue defensor de Derechos Humanos y luego de ver una conferencia de Jacob Appelbaum es que decide contribuir de una forma activa sobre el ejercicio y defensa de estos Derecho siendo un nodo de salida de Tor, la persecución a personas que se encuentran defendiendo la democracia de su País, la igualdad entre las personas, la libertad de expresión y privacidad de las personas en Internet lo realizó de esta forma, exponiéndose a ser perseguido judicialmente y generar un fallo judicial sin precedentes.

CONCLUSIONES.

Hemos analizado el caso de forma objetiva y vemos que en el accionar judicial existen

falencias graves de interpretación y actualización de la tecnología, las formas de investigación y basar la misma es “El Estado del Arte” que solo lleva a cometer errores en la investigación y generar problemas judiciales a personas que utilizan las herramientas tecnológicas de forma correcta o con fines altruistas (como la protección de la libertad de expresión, protección de la intimidad y privacidad), generando investigaciones obsoletas por cuestiones de tiempos reales y la falta de celeridad en casos donde la perdida de la evidencia digital o la pronta colaboración necesaria, la falta de instrucción y capacitación del sector judicial revela que no solo investigan a personas honestas sino que las reiteradas violaciones de los códigos de procedimiento penales por falta de conocimientos técnicos hacen que quienes sean los que llevan adelante el proceso sean los peritos y no los fiscales (que nunca estuvo presente en ninguna pericia). Es por esto que necesitamos un manual de procedimiento o protocolo para realizar pericias informáticas forenses que sea actualizable en cuanto a la tecnología y los requisitos técnicos, donde la presencia de profesionales de la Fiscalía o Juzgado Interviniente sean obligatorias. Y fundamentalmente, entender que una dirección IP no es un número identificador único (como el DNI), por el contrario, podría tomarse como la dirección de un edificio pero que el mismo pueda ser del tamaño de miles de departamentos. Por suerte, defender los derechos humanos mediante un TOR Exit Nodes en Argentina es legal.




elDerechoInformatico.com
"IL CIELO DEI SOSPIRI"

Revista Red Latinoamericana de Derecho Informático

"Malware: Sus propósitos y su finalidad en la investigación del Cibercrimen"

Autor: Emanuel Ortiz Ruiz

El software malicioso se convierte actualmente en uno de los intereses del delincuente cibernético para realizar actividades criminales, por tanto ha sido de gran interés de estudio en su temática y desarrollo a partir de los escenarios jurídico –legales en los cuales se puede individualizar una posible acción delictiva; esto enmarcado en el artículo 269E *"Uso de software malicioso"* en donde se evalúe la pertinencia de su uso adecuación típica por parte de la Fiscalía General de la Nación, de acuerdo a sus principales características y modalidades delictivas en las que se presenta.

Actualmente las amenazas informáticas crecen según los parámetros en los que se evalúe las nuevas tecnologías en el mercado, para *Gartner (2015),* las tecnologías emergentes para el año 2020 crearán una relación muy familiar entre el ser humano y las máquinas, cerca del 20% de los negocios estará dominado en este escenario por diferentes avances en materia tecnológica, el uso del [1]BYOD y los recientes avances en inteligencia artificial nos ponen frente a un escenario de ser posibles víctimas ante ataques o infecciones frente al [2]malware a nivel mundial; en ese sentido mediante esta monografía se pretende explicar los aspectos fundamentales para abordar el contexto criminal en donde se presenta el fenómeno delictivo y pretende explicar las principales tendencias en materia cibercriminal de la comisión de las conductas que se encuadren dentro del tipo penal de "*Uso de software malicioso*", dando observancia a las principales modalidades y tipologías en las que se cometen atentados contra los principios de seguridad en la información: *Integridad, Disponibilidad y Confidencialidad*.

En ese sentido es importante destacar que las circunstancias de la adecuación de la condcuta toman importancia desde el punto de vista de aplicabilidad; cuya imputación formal realiza la Fiscalia General de la Nacion debe enfocarse en los principios generales y convencionales del cibecrimen a nivel internacional; sin embargo este argumento sigue ambiguo frente a la titulación del ciberdelincuente en aspectos tecnológicos; estas circunstacias ameritan que muchas de estas conductas se puedan encuadrar dentro de aspectos principales de la conducta, sin embargo, todavía no son de mayor importancia para jueces y fiscales lo que indica falencias en materia de aprehensión y entendimiento de la sofisticación del delito; por

[1] BYOD: Bring your Own Device traducción al español: Traiga su propio dispositivo

[2] Malware: Software Malicioso, como lo define la guía de atención a incidentes de Malware, NIST SP 800-83 (Recomendaciones del Instituto Nacional de Estandar de Tecnologías, es un programa que insertado en un sistema puede afectar y comprometer la confidencialidad, integridad y disponibilidad de la información en un sistema informático.

tanto la importancia de abordar mecanismos de aprendizaje en Tic para la recaudación, presentación y formalización de los medios probatorios posibles para la consecución de la validez en la apreciación de un delito informático.

Para este escenario se debe realizar un análisis integral en donde se documente en el cual se documente las principales modalidades delictivas y se incurre en la conducta de del uso del software malicioso, estas incidencias en razón a la tipicidad dentro del código penal colombiano, con el fin de delimitar las acciones en la que realmente es desplegada la acción del sujeto agente frente a la labor cibercriminal; esta misma propuesta muestra los aspectos técnicos en los cuales orbita los componentes de la voluntad y la finalidad criminal del Ciberdelincuente.

En ese mismo sentido se pretende realizar una introspección de cómo se están adelantando los respectivos procesos judiciales por parte de los Fiscales en esta temática como componente verídico de la carencia de conocimientos en la utilización del artículo en mención.

Algunos aspectos pueden evidenciarse en la construcción de un mecanismo en que el Sistema actual interiorice la utilización y adecuación de conductas que han sido no exploradas o nuevas, pero el tema en cuestión, se ha evidenciado la mala práctica en la adecuación por parte de los Fiscales y directores de la investigación en no aplicar de manera correcta algunos apartes de la Ley 1273 del 5 de enero de 2009 en este es preciso recalcar se encuentra la inoperancia de nuevas formas de demostrar que un ciberdelincuente.

En amplio sentido este esquema ha subvalorado la función sancionatoria del uso de software malicioso, de manera que se vuelve inequívoco el problema por parte del rector de la investigación y el ente acusador sobre esta problemática, pues el desconocimiento de los tipos penales que acompaña la Ley 1273 no reúnen los factores externos que ponen en manifiesta la conducta punible. La escasa preparación ha sido consecuente de forma negativa con los retos en materia de cibercrimen (Editor y Centro Criptológico Nacional, 2014).

De la misma manera el abordaje de estas conductas suele ser pragmático ante los errores judiciales que se cometen dentro del Sistema Penal Oral Acusatorio porque no dibujan o esquematizan las actuaciones procesales y la búsqueda verdadera de la situación fáctica y real del asunto. Así pues es importante señalar que las actividades técnicas asociadas a la respuesta ante un incidente informático que pueda convertirse en condcuta cibercriminal son subjetivas frente al análisis exhaustivo en otros asuntos de carácter de examinación forense.

Es importante señalar que las consecuencias son fehacientes cuando se trata de dilucidar las circunstancias rodearon el hecho y los elementos con los que el cibercriminal o ciberdelincuente ejecutó la acción, de esta manera también es determinante valorar aspectos de pertinencia y conducencia para

saber cómo instrumentalizar esa adecuación típica.

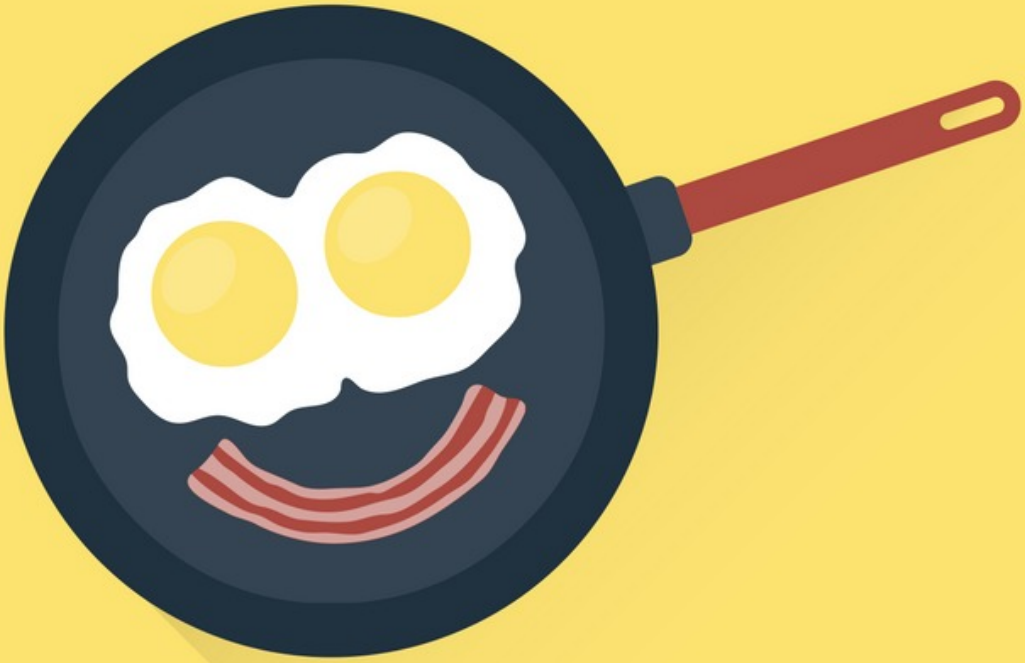
En ese mismo sentido los Fiscales actuales desconocen las herramientas para poder encauzar este tipo de conductas, dejándose ver falencias en materia de investigaciones penales y que tienen que ver con el indiciado cuando se va a realizar una imputación de cargos en las que se evidencian un sin número de errores en materia de interpretación.

Estos errores de interpretación no son causales de acuerdo a la conducta procesada si no a la relación de la conexión entee el bien juridico y la construcción del lenguaje del código malicioso; en ese sentido se observa la fundamentalidad de los aspectos relacionales en virtud de la calificación de la conducta.

Estructuración de un nuevo concepto de adecuación típica frente a una conducta de tipo sofisticado o "Maliciosa"

En este sentido se han citado diferentes doctrinantes para tal efecto; sin embargo sigue siendo escaso indicar que el concepto clásico de la adecuación tipica cubre totalmente el panorama; indudablemente se debe reconocer que la extperiencia nos dicta una extensión hacia lo práctico, en el que se debe indagar los aspectos formales de la conducta y su convergencia desde lo virtual a lo físico; así puues se deberá trazar una línea disruptiva para afirmar su univocidad formal y adecuada para los casos que ofrece el cibercrimen actualmente.

Respecto al "uso" que aborda el mismo artículo de ese mismo software para la consecución de la finalidad no se relaciona con la utilización del medio para la consecución del fin; en un hecho de una comisión que afecte la información y los datos es una situación cada vez más inquietante indagar el porque sucede y como sucede la materialización del "uso" del software malicioso cuya actividad se limita a la función lógica o ejecución lógica de tareas para llegar a una determinada labor; sin embargo en este caso, se debe agregar con cierta importancia la relevancia de la efectividad del daño frente a cualquiera de los componentes del sistema informático como ápice de verdad. Así mismo el efecto y la voluntad del delicuente ante ese sistema informático; concibiendo con esto el grado de margen de impacto sobre la Disponibilidad, Integridad y Confidencialidad.
Una vez proponemos que los datos e información procesados en ese ecosistema informático son de valoración semántica en su adecuación; respondemos de manera acuánime al cambio de perspectiva y su mirada holística de su función, ejecutabilidad y el daño que puede causar el uso del software malicioso frente a otras víctimas.



EDIPODCAST, COSAS QUE HACEN FELIZ A LA GENTE

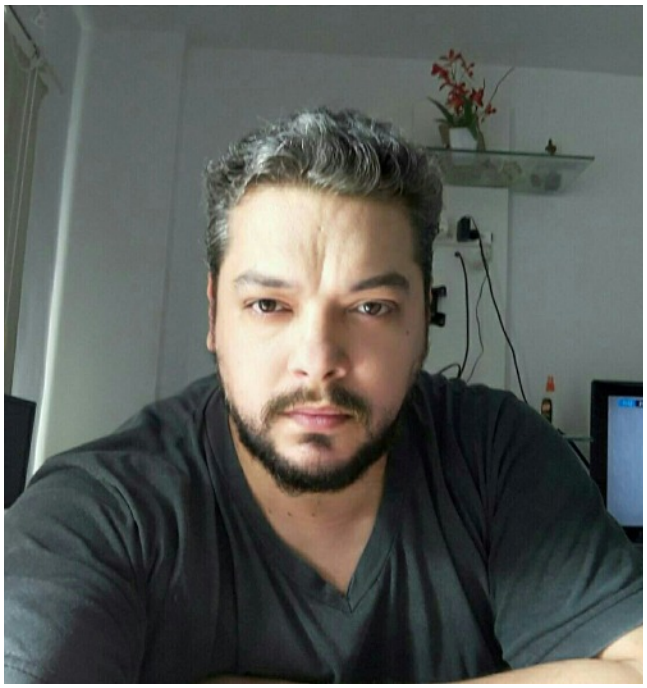
ELDERECHOINFORMATICO.COM

TENENCIA DE MATERIAL PORNOGRÁFICO DE MENORES PARA CONSUMO PERSONAL

Autor: Edgardo Villordo

Introducción

Sin lugar a dudas que la regulación de los delitos informáticos, los cuales se encuentran en un universo mas complejo el derecho informático, hasta la fecha no tiene una regulación específica; lo que implica un problema para los Estados que deben regular esta actividad, que cada vez es mas abarcativa de las relaciones comerciales y personales, de los ciudadanos entre si y con el mundo. Este nuevo ámbito jurídico relacionado con las tecnologías, comprende infinitas posibilidades, que por lo general exceden a la previsiones técnicas que el legislador establece en las regulaciones.



Todo esto debido a que el derecho informático mas precisamente el delito informático, tiene particularidades -velocidad de nuevas modalidades criminales debido al avance tecnológico- que no admiten en muchos casos regularlo con facilidad, como con otras ramas del derecho penal y asi lo vuelven complejo para nombrar algunas de ellas: su interacción, la posibilidad de comunicaciones sincrónicas y asincrónicas, operadores de servicios automáticos y la posibilidad de realizar actividades sin presencia física, o la comunicación con cualquier parte del planeta y su velocidad, tanto en las redes sociales, servicios bancarios, comerciales, etc, sumado a los nuevos adelantos en la comunicaciones con aplicaciones cada vez mas complejas que se insertan en la vida de las personas.

Este cúmulo de cuestiones que no son fáciles de comprender por aquellos que no son nativos digitales (y mucho menos por aquellos que no estan formados en una rama del derecho totalmente nueva), como se denominan a los ciudadanos que reciben estas tecnologías desde su nacimiento, merecen estudio y regulación progresiva y constante, ya que las mismas influyen en la vida y valores de las personas, y por otro lado no se mantienen estàticas por el contrario son dinámicas a velocidades inusitadas y muchas veces no previstas por las regulaciones.

Empero, entiendo que dichas regulaciones en materia criminal, como asi también en otras, deben ser siempre con un norte preestablecido, tal es el respeto de las garantías

constitucionales que constituyen el principio rector de las regulaciones legales en las distintas ramas del derecho incluída la informática. Desde la reforma de 1994 que acentúa y refuerza su constante evolución con la incorporación de los **Tratados Internacionales y el respeto por los ddhh, regulado en el Art. 75 inc. 22 de la Constitución Nacional**. Es indudable que el respeto por los derechos humanos es el principio rector por el cual debemos bregar en esta materia criminal, sumado al **principio pro homine**, y el principio de progresividad y no regresividad de los ddhh.

El presente artículo no pretende ser un análisis doctrinario en profundidad de la situación de la regulación informática de la tenencia de material pornográfico para consumo personal, porque la extensión de la temática excede el límite de este, sino tan solo un orden de ideas de algunos aspectos que a primera vista, pareciera ser deben ser analizados con mayor profundidad, para su correcta regulación y por último su introducción si correspondiere al Codigo Penal Argentino.-

La Necesidad.-

Habiendo establecido de una forma muy resumida algunos de los aspectos complejos del derecho informático en el cual se encuentra inserto el tipo penal, pretendo esbosar algunas consideraciones sobre el artículo **"La necesidad de sancionar la tenencia de la pornografía infantil para consumo personal en la Argentina"**, publicado en Pensamiento Penal cuya autoría le corresponde a María Milagros Roibón, que me llamo la atención, por su título y por otro lado, entiendo que la finalidad perseguida es buena en su génesis. Pero, me genera algunas dudas respecto a sus fundamentos técnicos, los que en mi modesto entender han quedado con un análisis deficitario y solamente pretendo en forma sucinta plantear algunos interrogantes como colaboración a publicación realizada, que no los veo del todo resueltos, que requieren mayor profundidad en su estudio, para de última poder desentrañar si corresponde tipificar o no una nueva figura dentro del Código Penal Argentino.

El primer aspecto a destacar es lo que se considera **"necesidad"**, si bien el artículo hace referencia a un alerta que proviene de una oficina extranjera (F.B.I.) de los EEUU, entiendo que el hablar de este tipo de hechos, vale decir, material pornográfico con niños, implica una actividad morbosa, la que deviene imperativamente repugnante, porque implica a niños sosteniendo relaciones sexuales explícitas o exponiéndose en hechos de índole netamente sexual con otras personas, debe ser regulada y previsto por el derecho argentino y en su caso, ver si corresponde su penalidad.

Ahora dicho esto, y no contándose con estadísticas precisas de casos que permitan revelar la necesidad de una política criminal y solo hacer referencia a casos o alertas de oficinas extranjeras, en una población de mas de 30 millones de personas, me parece apresurado -desde esa perspectiva- por poner un adjetivo.

Destinar la regulacion de este tipo de actividades al derecho penal en un tipo penal, me obligan a preguntarme si el **principio de ultima ratio** se encuentra analizado debidamente, o si nuevamente como sociedad sentimos el alivio de incriminar este tipo de hechos por parte de legislador que no tiene mucha iniciativa, y se ve inmerso en un problema de difícil estudio, y que resulta prima facie de complicada resolución. Pero que traído al escarnio público este tema, demanda respuesta, y la manera mas fácil de calmar este clamor, es utilizar el derecho penal, para mostrar soluciones facíles, lejos de un analisis del siglo XXI, que exige mayor discusión y análisis científico.-

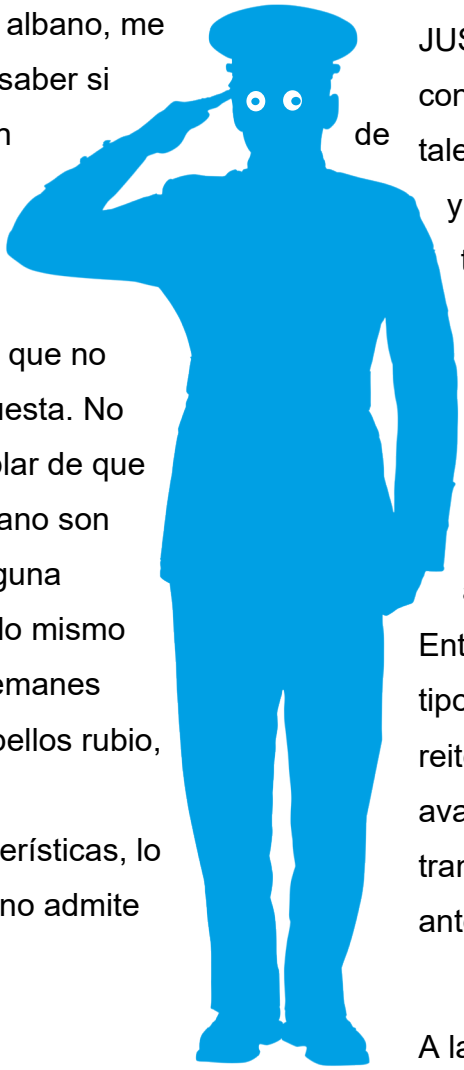
Por otro lado, me surgen fuertes dudas respecto a otros elementos que se mencionan en el artículo; coincido con la autora cuando hace mención que la cooperación internacional se hace necesaria, pero también es un problema debido a que no se esta hablando de países de legislación homogéneas lo cual sería un elemento a tener en cuenta para la regulación; debido que las distintas regulaciones de los paises, no siempren son coincidentes con las nuestras, y en algunos casos difieren sustancialmente. Sin dejar de lado que EEUU y otros países del mundo estan mucho mas adelantados que el nuestro en materia de espionaje informático, esto es una variable a tener en cuenta para la implementaciòn de este tipo de politicas públicas, ya que deja una puerta abierta para la obtención de datos sensibles en materia de seguridad informática e internacional, no hay que olvidar de los escandalos de la CIA con wikileaks, y los informes que se dieran a conocer públicamente de este tipo de ataques.-

Niño no tan niño, ¿y esto sería un problema para el tipo penal?

Sería pecar de etnocéntristas pensar que el derecho argentino es siquiera similar en todos los países del planeta. Es este punto donde prentendo mirar con detenimiento a otro elemento del artículo; que me llama la atención, seguramente es el motivo central de la regulación por su destinatario, el concepto de “niño”, que según nuestra normativa se encuentra regulado por la CONVENCION DE LOS DERECHOS DEL NIÑO en su Art. 1 , el cual define que es niño toda persona desde su concepción hasta que cumple 18 años, regulación que es compartida por muchos paises adherentes a dicha Convención.

Dicha institución jurídica no es similar en todos los paies la cual se regula de forma diferente en relacion a la franja etaria que se considera que una persona deja de ser niño. La mayoría de edad se puede adquirir antes de la edad establecida legalmente en nuestro país, esto puede ser por contraer matrimonio, por el consentimiento de los padres o por decisión judicial. A veces, difiere la edad en el caso de los hombres o de las mujeres, situaciones en que sea declarado incapaz o edades especiales. Ahora la mayoría de edad en algunos países se obtiene, cuando aquí según nuestra normativa nacional todavía son menores, por ejemplo: las personas en Albania a los 14 años adquieren la mayoría de edad , y

en otros países continúan siendo menores de edad. Aquí la ley ha determinado que luego de los 18 años ya son mayores de edad, y he aquí un problema de tipo jurídico penal, si la persona a la cual se le secuestra (mediante un proceso penal) contenido pornográfico (concepto que no es pasible en la doctrina, ni es de fácil determinación) de personas de 14 años de edad que mantienen relaciones sexuales, las cuales han sido filmadas en otro país de origen como por ejemplo el albano, me inquietud estriba en saber si se estaría frente a un de lito, y aquí encuentro un dilema para la regulación argentina que no resulta de fácil respuesta. No considero válido hablar de que los rasgos de un albano son determinados, de alguna forma, porque sería lo mismo que decir que los alemanes son personas de cabellos rubio, y ojos verdes, o con determinadas características, lo cual en el siglo XXI, no admite dicha presunción.-



Por otro lado, el artículo habla de sancionar la tenencia de pornografía infantil para el consumo personal. En tal sentido hay que recordar lo establecido por el Art. 19 de la CN, y los Tratados Internacionales en el Art 5 de la Declaración de los Derechos del Hombre y el Ciudadano, este derecho que equivale a la privacidad, tiene fundamento nada mas y menos que en el Principio de Reserva, en pocas palabras a ser dejado a solas, dice Cooley, lo cual constituye un ámbito de gobierno personal, propio de la dignidad del hombre, que rige con independencia del poder política y que impide la intervención del Estado en la esfera de la vida privada.

Asi en consonancia con lo antes mencionado se encuentra la CSJN (CORTE SUPREMA DE JUSTICIA ARGENTINA) que en su fallos, considera que un gobierno que no reconozca tales derechos y mantenga las vidas, la libertad, y propiedad de los ciudadanos sujetas en todo tiempo a la absoluta disposición e ilimitada revisión, aún de los mas democráticos depositarios del poder, es nada mas que un despotismo, el cual encuentro al señalar que violar el ambito privado de la persona constituye un avasallamiento que no admite justificación. Entiendo que el mercado que consume este tipo de material necesita regulación, pero -reitero- con un mayor análisis. Considero que avanzar en materia de la privacidad no se transforma en el camino correcto sin revisar antes otras alternativas conjuntamente.

A la hora de aportar claridad en materia penal, el artículo 19 de la CN (Constitucón Nacional), veda clara y categóricamente toda posibilidad de sancionar ideas, pensamientos, sentimientos, intenciones (actos internos), la vida psíquica, hechos privados, íntimos, personales, propios de su esfera privada conductas que no afecten -por daño o peligro

SALA 1a. , 11/2/2000).-

Ahora bien, atendiendo a mi primera afirmación sobre la dificultad de dicha materia en derecho criminal informático, encuentro parámetros técnicos juridicos que refuerzan mi tesitura incial, como es el caso “M., E. s/recurso de casación”, donde la Cámara de Casación revirtió el sobreseimiento dado a un médico que había enviado dos mensajes electrónicos con pornografía infantil a un foro de Internet, de los que usualmente son conocidos como newsgroups, entendiendo, correctamente, que el envío de un mensaje a tales foros constituía una forma de distribución. Pero lo que demostró ese caso fue la necesidad de una norma más inclusiva que pueda ser usada por jueces que, como los de la Cámara Nacional de Apelaciones en los Criminal y Correccional, desconocieran que de ninguna forma el envío de correos electrónicos a un newsgroup, cuya finalidad es distribuir información entre todos los miembros con un solo mensaje, puede ser interpretado como que no constituía “la realización del verbo típico”, esto es, la distribución.

El bien jurídico protegido en el tipo penal, resulta de dificil justificación, cuando el tenedor del material de contenido sexual explícito con un niño, puede o no haber sido partícipe indirecto del acto sexual con el menor, por lo cual penarlo por la afectación de dicho bien jurídico resulta al menos desproporcionado, debido a que la vinculación del consumo de este tipo de material multimedial es condenable desde un punto de vista moral; determinar si el consumidor de este material informático, tiene alguna relación con el menor, y con la producción del mismo sería materia de investigación y que de tratarse de un material internacional se dificulta mas aún; ni que hablar si el material que se secuestra, se encuentra con algun tipo de efecto especial diseñado por computadora, resulta a todas luces mas dificil aun determinar la veracidad del acto penado, y a su vez determinar como material verídico.

Por otro lado en caso de no poder determinar la identidad de la persona (niño) que parece según sus características físicas un puber; esto resulta de imposible determinación la afectación del bien jurídico protegido debido a la acreditación de la edad e identidad del menor víctima protagonista del material secuestrado, y que este niño se encuentre en la franja etaria que se establece como niño según la normativa argentina.-

Como corolario, sin ser un especialista en informática (ingeniero en sistemas o licenciado en sistemas), estimo que la mayoría de las personas que se conectan a la red, fácilmente pueden ser victimas de hackeos a sus ordenadores, y/o bien se podría insertar dentro de sus ordenadores imágenes, y material de este tipo. Esto también es materia de investigación y de difícil probanza en muchos casos. Dicha situación puede darse cuando una persona sin acceder a la red, lleva su ordenador a una reparación técnica, y la misma regresa con la carga de dicho material, y luego es

denunciada; resulta imposible que el usuario de un sistema operativo al día de hoy, tenga conocimiento de la totalidad de sus archivos y las capacidades que ocupan los mismos. Estas son algunas de las infinitas posibilidades que se pueden dar. El tratamiento de las mismas exceden la extensión del presente artículo que solo pretende ser un mínimo aporte para poder repensar la orientación de la regulación de un tema que me parece mas que preocupante, y que necesita un análisis constante debido a la mutabilidad de los avances tecnológicos.-

EDGARDO RUBEN VILLORDO

ABOGADO

LA CIBERCRIMINOLOGÍA. Nueva rama de la Criminología

Autor: Carlos Tudares

Cuando cursaba mis años en la carrera de Derecho, siempre vi con asombro lo interesante que era el estudio de la Criminología, como elaborar los Perfiles Criminales, y estudiar diversos asesinos en serie no sólo en nuestro país sino incluso a nivel internacional. Son más los casos acerca de homicidios y violaciones a los que se elaboran perfiles y pues no faltaba las Series de Tv como “Criminal Minds” e inclusive una serie que duró muy poco en tv como lo fue CSI CYBER que llegaron a tocar muy por encima el tema los perfiles criminales para los Ciberdelincuentes.

Pero desde hace año y medio he demostrado interés en todo lo referente a esa nueva rama de la Criminología como lo es ***LA CIBERCRIMINOLOGÍA***. Pero para poder entrar de lleno en este tema debemos definir primeramente lo que es la CRIMINOLOGÍA: *Ciencia que estudia el comportamiento delictivo y la reacción social frente a tal comportamiento Delincuencia, delincuentes y víctimas (Criminal o delincuente, cuya responsabilidad debe quedar establecida por un Tribunal, pero cuya “imputabilidad” es informada por la Psicología y Psiquiatría Forense. Estas disciplinas también estudian la dinámica personal que se resuelve en la motivación del acto delictivo, estudiando las consecuencias del acto antijurídico (víctima del Delito).*

Luego que hicimos un pequeño repaso acerca del concepto de Criminología nos sumergirnos en el mundo de la Cibercriminología, comenzando por su definición:

Es una parte de la Criminología que tiene como objeto el estudio de la delincuencia y la conducta antisocial en el ciberespacio y sus implicaciones en el espacio real.

Actualmente la mayor parte de la población tiene una vida en el ciberespacio, lugar en el que se producen las mismas relaciones que en la vida real, con los mismos riesgos de victimización y potenciales riesgos delictivos. Aunque no existe mucha investigación al respecto, empezamos a conocer las dinámicas que se producen y las herramientas que tenemos a nuestro alcance para poder prevenir esta problemática.

Dentro de los tópicos estructurales de internet en términos criminológicos tenemos: El diseño de Internet no fue pensado en términos de la seguridad de las comunicaciones, los datos y la información que se transmite, sino en la seguridad física de las redes. En la actualidad –aunque mejorados- los protocolos de comunicación son los mismos.

Durante la década de los años 60 en influenciada con la obra «1984» comienza a cuestionarse el uso de la informática en términos de privacidad e intimidad de las personas y con la recolección, el

almacenamiento y transmisión de datos e información a través de dispositivos informáticos aparecen las primeras conductas indebidas y hechos ilícitos relacionados con las computadoras.

Haciendo una retrospección en algunas décadas nos encontramos con los primeros pasos de la Cibercriminología entre los cuales algunos estudios identificaban a los delitos informáticos como Delitos de cuello blanco, término acuñado por el sociólogo estadounidense Edwin Sutherlan en 1939 Refiere a los delitos cometidos por los hombres de negocios a partir de la suposición de poder que ocupan desde las corporaciones

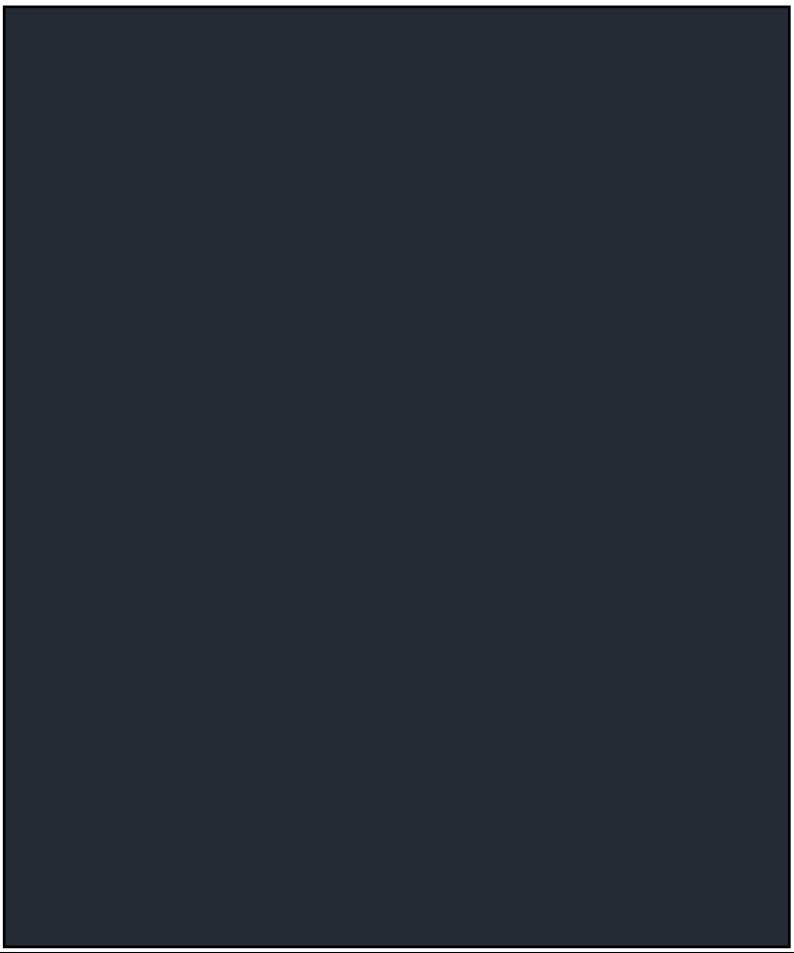
Hasta principios de los años 80, los usuarios de informática debían tener conocimientos específicos para el manejo de computadoras. El funcionamiento de los dispositivos estaba basado en programas que operaban mediante comandos complejos que requerían de formación y capacitación específica.

Entonces ya algunos países estudiaban el comportamiento de ese “delincuente especial”, del cual se ha especulado mucho debido a las películas de tv, series, entre otras, lo que permitido creer que el ciberdelincuente es siempre igual. Ese joven adolescente que se esconde detrás de una sudadera negra sin rostro y en muchas ocasiones mal llamados “hackers”

Pero cuando te enfrentas con un ignoto y descubre la variedad de facetas que éste tiene y de los impulsos que lo llevan a delinquir en el ciber espacio se caen todos esos mitos y paradigmas que todavía circulan. Si hacemos una comparación entre un asesino en serie y un ciberdelincuente lo único que quizás pueda haber una similitud en lo que podría ser “la firma” como tal, porque eso si es una condición innata de cualquier delincuente.

En una próxima entrega conversaremos acerca de cómo elaborar perfiles criminales de Ciberdelincuentes.

Abg Carlos Tudares T
Director de la Red Venezolana de Derecho Informático
e-mail: revederin@gmail.com



LA RED EDI

INFORMACIÓN QUE SUENA BIEN

WWW.ELDERECHOINFORMATICO.COM


AL
UNIVERSIDAD
AUTÓNOMA
LATINOAMERICANA
UNAULA

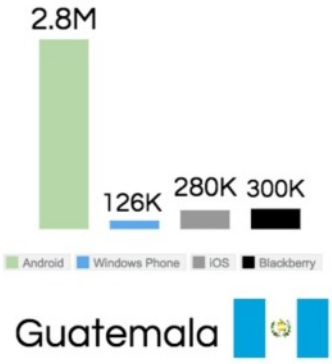
CIBERCRIMEN: LOS DESAFÍOS DE LA CIBERSEGURIDAD EN GUATEMALA

Autor: José Leonett

El auge de la tecnología ha realizado un gran impacto en la población mundial. Guatemala, como país pionero de la región Centroamérica y quien aporta una gran cantidad de startup, es una nación que tiene un alto consumo en tecnología que lo reflejan las estadísticas del Observatorio de la Ciberseguridad en América Latina y el Caribe (OEA & BID), donde la cantidad de personas con acceso a internet es de 3,683,564 y de abonados con teléfonos celulares de 16,911,811 lo cual refleja una penetración del internet en el país de un 23% que adicionalmente lo cual convierte en el País de Centroamérica con el mayor número de usuarios presentes en las redes sociales, distribuidos (estadísticas de http://www.internetworldstats.com/central.htm)

Guatemala cuenta con 1.400.000 usuarios registrados en Instagram de los cuales 680.000 son hombres y 670.000 mujeres.

Mientras que el sistema operativo de mayor diffusion sigue siendo los de los smarphone (fuente: latamclick.com)



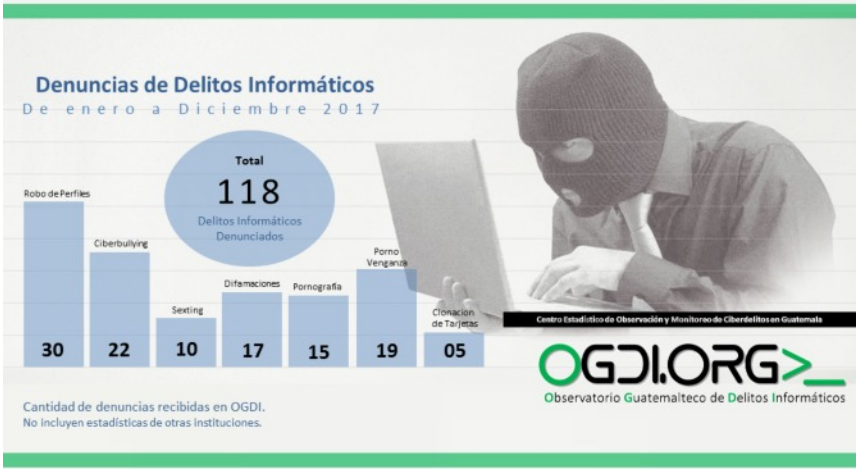
Con estas pocas estadísticas podemos ver la cantidad de personas e instituciones conectadas las 24 horas del día a internet; pero nos hemos planteado la pregunta: ¿Cuáles son los desafíos de la seguridad tecnología en materia de CIBERCRIMEN con este auge tecnológico?

Según el Informe sobre Desarrollo Humano en Guatemala, la cantidad de usuarios que utiliza Internet pasó del 10% de la población a 16%, en dos años, lo cual nos indica que 16 de cada 100 guatemaltecos usan Internet. (Fuente: Prensalibre)

El crimen organizado ha visto en este sector un nicho, con un crecimiento exponencial enorme, donde no existe ningún tipo de control, regulación o legislación que impida y sancione a estos grupos cometer sus fechorías no solo atacando a instituciones e inclusive sus insfraestructuras, sino también al ciudadano común quien se ha convertido en el banco predilecto de estos ciberdelincuentes.

La vulnerabilidad la cual se está evidenciando día a día por los medios de comunicación (estadísticas blancas) debe de alertar a las instituciones, personas y gobierno de tomar medidas urgentes para combatir este nuevo flagelo. Pero debemos de romper muchas barreras, entre ellas, la falta de estadísticas por parte de las instituciones que incluye al sector bancario nacional, para poder no solo mitigar y combatir los cibercrimenes, si no también, para tener estadísticas reales de que está afectando a dicho sector en temas de cibercrimenes y asi, tener unidades preparadas, equipos e infraestructura bajo una mística de disciplina investigativa contra el combate frontal de los cibercrimenes. Necesitamos compartir y crear inteligencia de ciberseguridad en el sector bancario, rompiendo las barreras de ciertas informaciones que al final de día no son confidenciales y que son de suma importancia para crear planes y estrategias reales y efectivas, contra los Ciberdelitos y cibercrimenes.

Las cifras estadísticas (aunque escasas) son alarmantes. Para el año 2016 la unidad de combate contra los delitos informáticos de la Policía Nacional Civil nos deja ver la fragilidad de los usuarios que navegan en internet y principalmente en las redes sociales:



- Ingeniería social y suplantación de identidad - 49%
- Redes Sociales - 35%
- Pornografía Infantil - 31%
- Amenazas y Ciberacoso - 27%
- Ataques a páginas del gobierno y privadas - 3%
- Maltrato Infantil - 2%

El observatorio guatemalteco de delitos informáticos –O.G.D.I- (www.ogdi.org), recientemente lanzo una proyección de solo denuncias recibidas por esa institución en donde podemos observar que la mayoría de estos Ciberdelitos tienen una tendencia con ataques directamente sobre el usuario y la vulneración de su intimidad y en casos extremos, su propia vida física.

Hacia el sector bancario nacional, vemos un incremento de cibercrimenes que nos reporta la superintendencia de bancos –S.I.B- en su Informe Estadístico 2015 y 2016. La SIB nos deja ver el crecimiento a nivel nacional de Cibercrimen relacionados con el tema de suplantación de identidad y tarjetas.

AÑO 2015: Superintendecia de Bancos de Guatemala -SIB-

- *Usurpación de identidad – 03%*
- *Clonación de Tarjetas de Crédito – 04%*

- **Apertura de operaciones por usurpación de identidad**
  Los 315 casos por usurpación de identidad representan el 8% del total en 2016 (111 casos, 3% en 2015), de los cuales las entidades han resuelto favorablemente 173 casos que representan el 55% de los mismos (67 casos,60% en 2015), por haber concluido que efectivamente se utilizó la documentación del usuario para tramitar tarjetas de crédito que luego fueron utilizadas para efectuar consumos no reconocidos por este.

al cobro de morosidad los cuales terminan almacenando y creando bases de datos que luego desconocemos el uso de las mismas o a donde irán a parar, violando el Habeas datas tipificado por las leyes de Guatemala de cada cliente, creando desde la óptica de ciberseguridad, un sistema completamente frágil en el activo de la información y protección de datos.

Sistema Financiero Supervisado: Casos atendidos por tipología, durante el período del 1 de enero al 31 de diciembre de 2016.

No.	TIPO DE CASO	CASOS ATENDIDOS	%	RESULTADO FAVORABLE DE LA GESTIÓN			
				SI	%	NO	%
1	Inconformidad con el historial crediticio en el SIRC	1,113	29%	958	86%	155	14%
2	Negativa en la concesión de convenio de pago	762	20%	640	84%	122	16%
3	Inconformidad con registros efectuados en el estado de cuenta	396	11%	224	57%	172	43%
4	Inconformidad con el cobro de intereses o en las condiciones pactadas	317	8%	152	48%	165	52%
5	Apertura de operaciones por usurpación de identidad	315	8%	173	55%	142	45%
6	Cargos fraudulentos no reconocidos - clonación de tarjeta	127	3%	60	47%	67	53%
7	Cierre, cancelación o bloqueo de la cuenta sin justificación aparente	91	3%	52	57%	39	43%
8	Solicitud de información sobre operaciones de seguros o depósitos	89	2%	43	48%	46	52%
9	Negativa en el pago de la cobertura de contratos de seguros	87	2%	21	24%	66	76%
10	Cargos por tiempos compartidos	80	2%	54	68%	26	32%
11	Cheques pagados con firma diferente a la registrada	76	2%	19	25%	57	75%
12	Inadecuada forma de cobro	71	2%	29	41%	42	59%
13	Inconformidad por la cancelación de cobertura de contratos de seguros	62	2%	18	29%	44	71%
14	Inconformidad por la no entrega de finiquito o de la carta de pago	51	1%	33	65%	18	35%
15	Inconformidad con la demanda planteada y las medidas precautorias decretadas	49	1%	26	53%	23	47%
16	Otros	138	4%	70	51%	68	49%
TOTAL		3,824	100%	2,572	67%	1,252	33%

- **Cargos fraudulentos no reconocidos – clonación de tarjeta**

  En 2016 se observan 127 casos de quejas que se relacionan con cargos no reconocidos, que representan el 3% del total de casos atendidos (188 casos, 5% en 2015), de los cuales 60 casos, que representan el 47%, han sido resueltos por las entidades a favor del usuario (107 casos, 57% en 2015), por haber determinado que dichos cargos no fueron efectuados por él; sin embargo, 67 casos, que representan el 53% (81 casos, 43% en 2015) fueron resueltos desfavorablemente, toda vez que las entidades consideraron, entre otros, que sí hubo presencia física de la tarjeta de crédito relacionada y que el plástico con el cual se realizaron las transacciones reclamadas no fue utilizado en puntos o lugares identificados de riesgo; sí como que el reclamo fue presentado de manera extemporánea según el plazo fijado en el contrato.

Fuente: Informe Estadístico 2016 SIB

El Renap registra 29 mil casos de usurpación de identidad en el año 2015 (fuente:publinew) mientras que cada día son robados 700 celulares, según la SIT (fuente; prensa libre)

A este emergente problema, debemos de sumarle la incursión de las pandillas en muchas estructuras de nuestra sociedad. Las ciberpandillas, modalidad de presencia de las pandillas en internet y redes sociales, han podido inyectar personal pasando muchos filtros de control en las instituciones, empresas y entes gubernativos desde donde la información de estas, se convierte en un activo de mucho valor a la hora de efectuar secuestros, extorsiones y asesinatos.

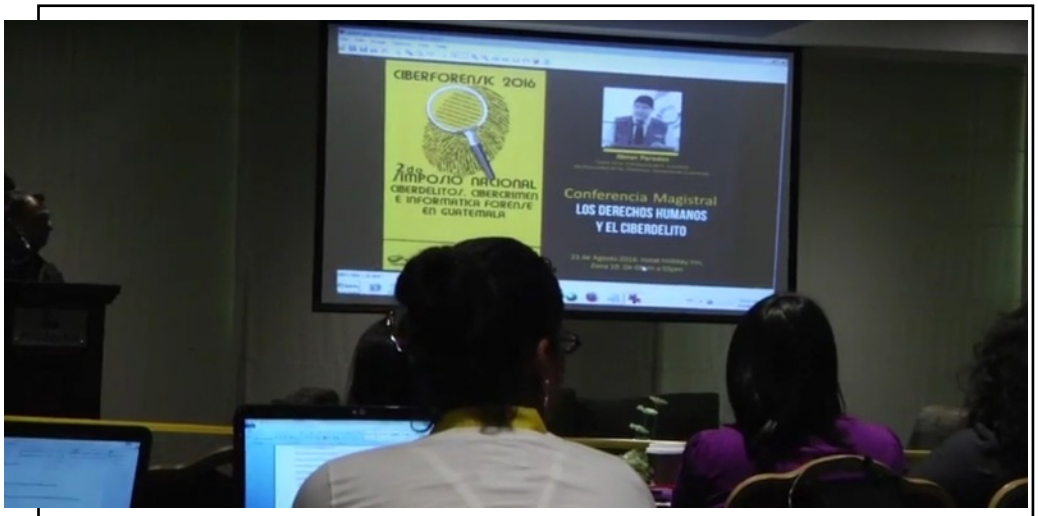
Las bases de datos son y seguirán siendo el blanco de predilecto de estos grupos, así como fuentes directas de información que pueden servir para crear modus vivendis, proveniente de los famosos buros crediticios, que simplemente con hacer un pago por medio de un tercero (política de pandillas), ya se tiene acceso a un sin número de información por parte del victimario. A estos debemos de sumarle, los traspasos de expedientes e información a terceras empresas dedicadas

Sumémosle a todo esto el robo y fuga de información de estas mismas instituciones por parte del personal de confianza. En este momento que usted está leyendo este artículo, cuantas personas en Guatemala, en los buros, cooperativas y entidades bancarias se han conectado de manera remota a las bases de datos, sufridos ciberataques, usurpación de identidad, clonación de tarjetas de crédito y debido, estafas electrónicas y un sinfín de ciberdelitos y cibercrimenes en tan poco tiempo. Me pregunto ¿realmente mantenemos un control sobre la fuga y venta de información en las instituciones? ¿Nos amparamos sobre ciertos reglamentos y leyes para no publicar estos hechos y mantenernos aislados en el combate de los Ciberdelitos? ¿Comunicamos estos hechos a nuestros superiores o solo callamos los incidentes? ¿Utilizamos empresas terceras que administran nuestra información sin saber el perfil de sus usuarios y el uso que le darán a esta? ¿Mantenemos informados y creamos simulacros de fuga y robo de información en nuestras instituciones y con qué periodicidad?

La mayoría de los Ciberdelitos y cibercrimenes hasta en un 85% la realizan personas que no son profesionales en sector de tecnología, simplemente son delincuentes. La contraparte, quienes aseguran y monitorean los principales activos del siglo XXI, la información, son personas preparadas y que muchas veces no tienen la menor idea de cómo se comenten dichos delitos, y dejo en claro que no busco denigrar sino dar a conocer una gran realidad que estamos viviendo y entonces ¿en qué estamos fallando? Porque no podemos educar para prevenir hechos ilícitos que están afectando a las instituciones.

El anonimato, la carencia de una ley contra el combate de los Ciberdelitos, la falta de educación y promoción educativa de cómo prevenir los Ciberdelitos, la constante capacitación sobre temas de Ciberdelitos y cibercrimenes en el sector bancario, el manejo de incidentes que requieran procesos que van más allá de los extrajudiciales y las personas que deben de estar en las exhibición de estos

informes son los grande desafíos para uno de los sectores que manejan todo el poder económico de la nación. Debemos de llegar a un consenso de cooperación de estadísticas entre instituciones y generar un centro de monitoreo y estadística para saber hacia dónde apuntan los Ciberdelitos y cómo debemos de enfrentarlos, claro está, en el marco de una cooperación franca entre todas las unidades de seguridad, análisis de riesgos, auditoria, jurídico y sistemas.



Los controles aunque sean más estrictos, siempre existirá una mente delincuencial o investigativa que plantea una solución al mismo. Al final del día, son plataformas creadas por seres humanos y violadas por seres humanos que han sido llamadas, Delitos de alta tecnología.

Creo en lo personal, que debemos de sentarnos sin burocracias y no buscando un interés único y egoísta, sino, buscando un bienestar y solución común que nos afecta a todos en cualquier estrato de la sociedad Guatemalteca y mundial. Penar en consciencia colectiva de datos y allí, fundar las bases de cooperación multidisciplinaria en manos de expertos que combaten en primera persona, estas nuevas modalidades de cometer delitos con el uso de la tecnología. Guatemala cuenta con muchos y muy buen recurso humano, claro algunos viciados, otros no comprometidos y un

pequeño grupo entusiasta que cree en una nación prospera y equitativa y que hoy por hoy, es un faro de la tecnología en Centroamérica y del mundo. Ahora queda mi última pregunta ¿Cuándo nos reuniremos en una mesa con un café, libreta, lápiz y ganas de crear planes y políticas en contra de la lucha del Cibercrimen en el país? No buscando solamente marketing que es bueno, pero no tiene nada que ver con la ciberseguridad. Cuando abordaremos francamente este tema en el sector.

Recuerda esto: siempre hay alguien, que te está vigilando.

José R. Leonett

Gerente de Ciberseguridad en INFO Y MAS Guatemala
CEO/Founder del Observatorio Guatemalteco de Delitos Informáticos –OGDI-.
Ponente de la Comunidad de Inteligencia, Seguridad y Ciberdefensa – COINSECI Europa.
CO Red Iberoamérica El Derecho Informático y CO Red Latinoamérica de Informática forense REDLIF Guatemala.
Miembro activo del Consejo Consultivo Internacional de la Red Venezolana de Derecho Informático (REVEDERIN).

LA RED EDI LES DESEA

FELIZ

2018

ELDERECHOINFORMATICO.COM
ESTAMOS DONDE ESTAS VOS

Ethical Hacking Consultores

Nuestros Servicios

- Security Penetration Testing
- Auditoria y Certificación de ATM's
- Informática Forense
- Auditorias Especializadas
- Asesoramiento en Derecho Informático
- Inteligencia Informática
- Entrenamiento en Seguridad
- Soluciones Big Data

Nuestros Productos

pentest365

- Pentesting Persistente desde la Nube
- Identificación automatizada de Tecnologías, Vulnerabilidades y Exploits
- Monitoreo de Seguridad 24x7x365
- Alertas en tiempo real
- Escaneo de puertos Programable
- Dashboard Perzonalizable
- Reportes con cumplimiento PCI v3

KAS

- Reducción del fraude en ATMs
- Monitoreo y Seguridad en tiempo real
- Servicios y Salud del ATM 24x7
- Alertas en tiempo real ante incidentes
- Agilidad en la investigación Forense
- Reportes con cumplimiento PCI v3
- Dashboard 100% personalizable
- Protección Multivendor

TMFdesk

- Call Center por Redes Sociales
- Sistema distribuido de mensajes
- Administración de multiples Redes Sociales al mismo tiempo
- Administración de histórico de Chats
- Estadisticas de atención por Agente
- Respuestas Automáticas y Enlatadas
- Reportes automáticos.

Firmaza

- Firma Electrónica
- Correo Electrónico Certificado
- Firma de Documentos Online
- Testigo Digital Online
- Sello HTTP Seguro
- Factura Electrónica
- Firma de Transacciones

Visitanos: www.ehcgroup.io Contactanos: (+507) 3873850 | info@ehcgroup.io

LA PROTECCION DE LOS DATOS EMPRESARIOS [1*]

María Eugenia Lo Giudice

La tecnología en la vida cotidiana ya es un hecho ordinario, pero no impide la posibilidad de riesgos que nos lleva a prevenir los posibles efectos negativos.
Las tecnologías de la información y la comunicación (TIC) nos transmiten una dicotomía de aspectos: a) un aspecto positivo señala un sinnúmero de contribuciones a la ciencia y sociedad en general. b) en su aspecto negativo podemos ejemplificar conductas disruptivas como el *phubbing* (del inglés *phone* más *snubbing*) acto de ignorar a alguien por mirar el teléfono móvil; o *nomofobia* (del inglés *no mobile pone)*, miedo a estar sin el teléfono móvil. Y así se podría abundar los efectos nocivos de químicos usados en tecnología, aparición de síndromes en el ser humano (túnel carpiano, sordera, obesidad) o desastres naturales ocasionados por el uso de elementos tecnológicos, etc. etc.

Actualmente se ha avanzado de la sociedad de la información a la sociedad del conocimiento, donde se comprende el valor asignado al dato en sí mismo como base del desarrollo tanto en lo económico como en lo social.

Lo anterior implica trabajar sobre una cultura de la seguridad que monitoree almacenamiento y comunicación de la información corporativa, restando incertidumbre ante el riesgo, en este caso ante la probabilidade de *fuga de datos.*

Cómo se vincula "riesgo" con "información"?

Del tratamiento que se le dé a los datos derivará la responsabilidad sobre los sujetos de derecho (personas físicas o personas jurídicas).

De acuerdo a estadísticas[1] un 81 % de las grandes organizaciones identifican los propios empleados como responsables de violaciones a la información. ¿Será pues este un factor posible de riesgo en determinadas circunstancias?

Factor humano – Ingeniería social

Más allá de las legislaciones en general que suelen considerar el deber genérico de no dañar a otro y su consecuente obligación de reparación integral del daño causado, es necesario observar la conducta de los

[1] Departamento para Negocios, Innovaciones y Habilidades del Gobierno de Gran Bretaña, 2015.

integrantes de las organizaciones pudiendo diferenciarse lo físico (amenazas que incumben lo humano y lo natural) de lo tecnológico (se refiere a la estructura del sistema pudiendo influir en lo humano y/o lo físico).

Asi, partimos de la necesidad de propulsar una cultura de seguridad para su aplicación interna que abarque posiciones tanto administrativas como ejecutivas y no confiar la seguridad solamente a un departamento técnico especializado en seguridad informática.

El factor humano dentro de una empresa se considera crítico en seguridad de la información. Justamente y parafraseando "los atacantes en lugar de centrarse en los servidores, se han percatado de que suele ser más sencillo atacar a los usuarios en el terreno del navegador y el correo electrónico".[1]

Nos estamos refiriendo a la "ingeniería social". Es decir, la influencia del accionar humano permeable o estrategia mediante la cual puede ser sometida una persona por otra, independientemente del *hardware*, para obtener de ella determinada conducta.
Si bien el recurso humano en la empresa es crítico, correctamente encauzado colaboraría en prevención de riesgos, evitando daños. Para ello se deben tomar medidas concretas, definiendo un plan de acción de prevención, extremando asi el control de la seguridad informática.

El concepto de ingeniería social, no es nuevo. Por nombrar algunos ejemplos podemos mencionar que ya se lo mencionó aplicado por el siglo VII a.c., según la historia del caballo de Troya de *La Odisea*.

Cercanos en nuestros tiempos mediante estrategias de ingeniería social, según KrebsonSecurity (2013)[2], se comprometieron 1.200 millones de contraseñas y direcciones de correo electrónico en el mundo con lo que se permitía conectarse a unos 420.000 portales de internet. La información era ofrecida por *hackers* rusos que llegaron a disponer de millones de cuentas con dominio pertenecientes a Rusia, de Yahoo, Microsoft y Gmail[3]. Otro ejemplo en 2014, el Banco JP Morgan Chase, fue víctima de piratas internacionales que atacaron cibernéticamente provocando la pérdida de datos sensibles de aproximadamente 83 millones de cuentas bancarias, provocando variaciones en el precio de acciones del mercado bursátil.

Otro conocido caso de fuga de datos se dio con la agencia de citas Ashley Madison[4], cuando ciberpiratas publicaron datos sensibles de usuarios, acarreando chantaje y hasta dos suicidios. Más reciente aún recordemos el caso Snowden[5], quien reveló datos del espionaje en

[1] http://www.cisco.com/c/dam/global/es_es/assets/pdf/asr_final_os_ah_es.pdf

[2] Krebs, B. (3 de octubre de 2013). Adobe To Announce Source Code, Customer Data Breach. Obtenido de https://krebsonsecurity.com/2013/10/adobe-to-announce-source-code-customer-data-breach/

[3] Angulo, S. (mayo, 2016). Un hacker ruso robó más de 273 millones de credenciales. Obtenido de http://www.enter.co/chips-bits/seguridad/un-hacker-ruso-robo-mas-de-273-millones-de-credenciales/

[4] Albors, J. (20 de julio de 2015). Ataque a Ashley Madison comprometería a 37 millones en citas extramatrimoniales. Obtenido de https://www.welivesecurity.com/la-es/2015/07/20/ataque-ashley-madison/

[5] Márquez, W. (2 de julio de 2013). Lo que Snowden ha revelado hasta ahora del espionaje de EE. UU. Obtenido de http://www.bbc.com/mundo/noticias/2013/07/130702_eeuu_snowden_revelaciones_espionaje_wbm

sistemas de información que perpetraba Estados Unidos sobre China, Rusia y la Unión Europea.

FUGA DE INFORMACIÓN O DATOS

Listando de mayor a menor frecuencia, posibles factores que darían lugar a fuga de información, consideramos: 1) negligencia o impericia en el manejo de la seguridad de la información, (ejemplo, el correo electrónico sin cifrar, envío a dirección equivocada, almacenamiento de archivos en servicios basados en la *nube*), 2) ataques internos (ejs. realizado por empleados infieles), 3) delincuentes informáticos (aplicación de técnicas capaces de robar información de dispositivos no conectados).

Corroborando lo expuesto, según el proveedor ruso de seguridad informática Kaspersky Lab, casi la mitad de las empresas españolas han sufrido en alguna ocasión un robo atribuido al negligente accionar del comportamiento de sus empleados. Por lo que el 50 % de esas empresas han restringido o prohibido el uso de servicios de intercambio de archivos y el 47 % ha impuesto reglas para regular la conexión de dispositivos externos en los equipos corporativos.

SEGURIDAD INFORMÁTICA Y GESTIÓN DE RIESGO

A. La empresa

La seguridad informática desde la óptica de un lego, es un proceso complejo que está fuera del alcance de todo profesional no especializado. Mientras que desde la *empresa*, se entiende que es una especialización del área de sistemas de información. No se comparte esta visión, entendiendo que el compromiso y responsabilidad debe ser de todas las áreas de la organización.

Estamos ante un cambio de paradigma sobre nuevos comportamientos sociales que impacta también en el ámbito laboral. Como las posibilidades de teletrabajo desde el exterior de la empresa permiten la conectividad desde dispositivos personales. Para ello, las áreas de sistemas aplican normativas internacionales (ISO 27000[1]) que enmarca la gestión de seguridad de la información usada con el objetivo de mejorar prácticas o regular este tipo de actividades.

Jurídicamente a efectos preventivo para el caso de las empresas se podría tener en cuenta las siguientes herramientas:
1) Contar con un Manual de gobierno corporativo donde se trate la protección de datos, basados en los principios de buena fe, compromiso y lealtad. 2) Tener el control sobre el personal de la empresa (selección y contratación, estado de satisfacción en ella, etc.). 3) Al momento de la contratación, incluir cláusulas dejando aclarados los parámetros exigidos en cuanto a la seguridad de la información. 4) Disponer de un Manual de uso de herramientas informáticas, con protocolos jurídicos de seguridad, cláusulas de responsabilidad en el tratamiento de la información y uso de las herramientas. 5) Aplicación de estándares de seguridad, como la norma ISO 27000.

B. El usuario final

[1] International Organization for Standardization. ISO 27000. Obtenido de http://iso27000.es/iso27000.html#section3b

En cuanto, factor humano, debemos resaltar la cultura de la concientización que suele generar frecuentes problemas en la administración de seguridad.
Se exigen conductas que brinden seguridad como a través de diferentes métodos de autenticación. Generalmente combinamos tres factores: algo que *conozco,* ejemplo una clave; algo que *tengo,* el uso de una credencial; y algo que *soy*, referido a un aspecto biométrico del individuo.

A pesar de ello es frecuente que con la "colaboración y desconocimiento" de la propia victima se llega a atentar contra la seguridad de los datos, como robo de claves, p*hishing, key loggers*, etc. Las organizaciones que han sido víctimas de estas prácticas no publican generalmente sus estadísticas dado que supondría un descrédito en los clientes.

PROTECCION DE DATOS

En la seguridad informática se deben distinguir dos objetivos de protección: 1) la seguridad de la información y 2) la protección de datos.

La primera se ocupa de protección de los datos mismos, teniendo en cuenta confidencialidad, integridad y disponibilidad, pero enfatizamos especialmente *autenticidad*.

Al asociar seguridad debe entenderse medidas de prevención de daños que se genere sobre la información. Primeramente, determinar procesos y medidas de protección que garanticen un tratamiento adecuado de acuerdo con el principio de neutralidad tecnológica (los procesos de las TIC son tan dinámicos que implican inversiones en actualización y capacitación continua).

Se deben implementar, con la participación de todos los sectores de la organización, medidas de protección preventiva suficientes mediante un plan de gestión de riesgo. Caso contrario, se deberá asumir responsabilidades jurídicas tanto civiles como penales, contractuales y extracontractuales.
Desde la perspectiva jurídica, la seguridad informática se refiere a las características y condiciones de sistemas de procesamiento de datos y su almacenamiento, para garantizar su confidencialidad, integridad y disponibilidad, características propias de los datos, exigidas en numerosas legislaciones.

SUGERENCIAS PARA LA PREVENCIÓN DE IMPACTOS GENERADOS POR DAÑOS

Dentro del ámbito corporativo y habiéndose investigado material proporcionado por empresas que trabajan con seguridad informática,[1] para evitar las principales causas de fuga de información se sugieren los siguientes puntos:
1) Tener la suficiente información para clarificar una programación segura que no dé lugar a filtrado de datos. Para ello es importante tener una acabada valoración de los datos con que se cuenta en el activo y la forma en que se deben preservar y/o eliminar. 2) Educar y concientizar al personal sobre los impactos dañosos que generaría la falta de

[1] Como por ejemplo ESET, quien brinda soluciones de software de seguridad proveyendo protección de última generación contra amenazas informáticas. Bortnik, S. (30 de mayo de 2011). 10 mandamientos de la seguridad de la información en la empresa. Obtenido de https://www.welivesecurity.com/la-es/2011/05/30/10-mandamientos-seguridad-empresa/

responsabilidad en el manejo de la información. 3) No considerar solo el área técnica como única responsable de la seguridad de la información. 4) Invertir en la actualización de la tecnología que brinde seguridad técnica, acogiéndose a la actualización permanente de las normas ISO de seguridad de la información. 7) Las áreas de recursos humanos y legal deben trabajar conjuntamente para ser claros en la política de confidencialidad de la empresa.

IX. CONCLUSIÓN

Conjuntamente con la tecnología, se deben extremar los cuidados en el tratamiento de los datos, donde es fundamental la responsabilidad de la *ingeniería social*.

Se deben redefinir parámetros de conducta social como generación de riesgos, para lograr que el nuevo mundo tecnológico no sea percibido como “riesgoso”.

Se concluye en la necesidad de educar y concientizar el recurso humano a cargo del tratamiento de datos, y extremar condiciones tanto técnicas como legales adecuadas para su protección.

10 PASOS PARA HACER MARCA PERSONAL EN INTERNET

Autora: Carolina Marin

Las marca personal o “Personal Branding” es una tècnica enfocada en gestionar la imagen de una persona como si fuera una marca. Surgiò como una tècnica para la búsqueda de empleo. En la actualidad, desarrollar la marca personal es fundamental para saber diferenciarse en un mercado tan competitivo como es Internet.

1) Elige un nombre de usuario único para todas tus redes sociales, este ayudará a tu posicionamiento. Lo ideal es que sea tu nombre real, por ejemplo @carolinamarinok es mi usuario en todas las redes, tuve que agregar “ok” ya que estaba en uso mu nombre. Y cuando digo “todas tus redes” significa que hasta tu correo deberìa tener el mismo usuario.

2) Selecciona en què redes vas a estar. No, no puedes estar en todas si no tienes tiempo. Si eres abogado te recomiendo: Linkedin y Twitter. Si vas a estar en facebook que sea una Fan Page y no un perfil personal. **No hagas marca con tu perfil personal.**

3) Foto de perfil: sè que me pongo intensa con este tema pero es que es muy importante, l**a foto de perfil es como el DNI**, debe ser una foto de ti ¡solo! y en lo posible primer plano. No sirve los lentes de sol, ni las fotos con adulteraciones, tipo emoticones.

4) En la portada no sirve poner foto en primer plano, más bien conviene algo que cuente un poco màs de ti. Se permite: charlas, congresos, oficina, ¿paisajes? no, almenos que seas paisajista. ¿foto de la familia? eso dèjalo para tu facebook personal, **si vas a trabajar tu marca personal debes enfocarte en tu profesiòn.**

5) No hay mejor herramienta para hacer marca que un blog, allì podràs ayudar a personas con tu contenido. Se trata de crear contenido de valor que sirva para forjar y fidelizar una comunidad. Elige tu pùblico, tu tono de comunicaciòn y no olvides: hacer SEO, Usar las redes para llevar tràfico y tener Google Analytics para ver estadísticas.

6) Networking: en internet tambièn se puede crear nuestras propìai red de nogocios y què mejor que Linkedin y Twitter para hacerlo. En la ediciònNº 26 de esta revista hablo sobre ello.

7) Anuncios: Si bien es cierto que con contenido de valor es posible crear una comunidad de adeptos, no es fàcil. Si queremos llegar a grandes audiencias debemos hacer publicidad. En Facebook, por ejemplo, el alcance orgànico es de apenas el 3 %, es decir, de 2000 fans solo ven tus publicaciones 60, puede ser más o menos, depende de otros factores: frecuencia, contenido, cantidad de fans.¡ cuàndo se recomienda? para difundir eventos, cursos, charlas, promociones, etc.

8) Contenido: no todo pasa por informar o convertirnos en una agenda parlante de todo lo que hacemos dìa a dìa. Te recomiendo contenido ùtil que sirva para ayudar a tu comunidad. Recuerda primero elegir a tu pùblico.

9) Formatos: el formato que crece dìa a dia es el video, ya sea en vivo o grabado. Le siguen gif y fotos. Si vas a usar textos trata de que no sean muy largos. Usa siempre titulares llamativos, emoticones y fotos que acompañen tus notas.

10) Recuerda que en internet no solo compites con otros abogados sino que con todo el contenido que está circulando. Antes de crear tus publicaciones piensa en el formato que sea más útil para captar la atenciòn de los usuarios. Te recomiendo mirar otras marcas, fijate buenas prácticas.

LOS DESTACADOS (EDI) DEL AÑO

ELDERECHOINFORMATICO.COM

LA RED.

• ABOGADOS •

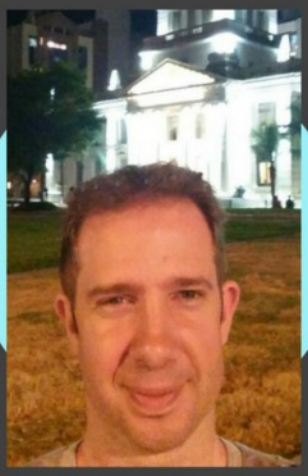
DESTACADOS EDI 2017

JOEL GOMEZ TREVIÑO MÉXICO

Presidente de AMDI - creador de abogadodigital.tv - Destacada labor en la difusión del derecho para COMAP

MIRIAM GUARDIOLA ESPAÑA

Presidenta Asoc. Safe Teens, artículos y participación en Foros, congresos y el Tribunal Europeo de derecho humanos



RODRIGO IGLESIAS ARGENTINA

Litigante destacado - Luchador contra el mal uso de las tecnologías en el sistema electoral

KAREN CESPEDES PERÚ

Directora de Comunicaciónes e Informática Jurídica del Colegio de Abogados de Lima - Organización de eventos y participación en foros

ROBERTO LEMAITRE COSTA RICA

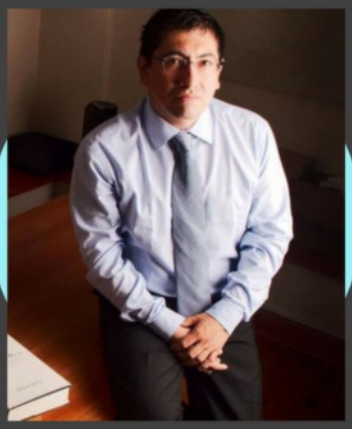
Abogado en Viceministerio de Telecomunicaciones Costa Rica - Conferencista - Docente

• TRAYECTORIA •

DESTACADOS EDI 2017

MARCELO BAUZA
URUGUAY

Diplomado en Derecho Informático e Informática Jurídica Universidad de Montpellier (Francia)
Doctor en Derecho y Ciencias Sociales por la Universidad Mayor de la República Oriental del Uruguay.



ERICK IRIARTE
AHON - PERÚ

Magister en Ciencia Política y Gobierno con mención en Políticas Públicas y Gestión Pública (PUCP). Fue Primer General Manager LACTLD, asociación de ccTLDs de América Latina. Director Ejecutivo de Alfa-Redi

BIBIANA LUZ CLARA
ARGENTINA

Creó y dirige el Instituto de Derecho Informatico del Colegio de Abogados de Mar del Plata, libros publicados, Creacion del CIIDDI, Directora del Grupo de Investigacion en Informatica y Derecho de UFASTA

JULIO TELLEZ VALDÉS - MÉXICO

Doctorado en Informática Jurídica y Derecho de la Informática por el Instituto para la Investigación y Tratamiento de la Información Jurídica (I.R.E.T.I.J.), Montpellier, Francia 1981.

• SITIO WEB/BLOG •

DESTACADOS EDI 2017

DERECHOINFORMATICO.CO (HEIDY BALANTA)

Sitio especializado en Derecho nformático y temáticas afines

EVENTOSJURIDICOS.COM (JORGE CAMPANILLAS)

Sitio dedicado a la difusión de todo tipo de eventos jurídicos teniendo este año especial én Derecho Informático

FFNEWS.COM.AR (FEDRA FONTAO)

Sitio revelación con contenido múltiple y artículos de relevancia en materia de Derecho y tecnologias

AB21.ORG.BR (ASOCIACIÓN BRASILERA LEGALTECHS-LAWTECHS)

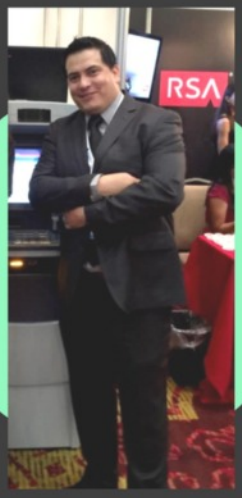
Sitio con noticias y novedades de relevancia en idioma portugués

ALGORITMOLEGAL.COM (RICARDO OLIVA LEÓN)

Sitio con contenido de actualidad en derecho informático con asiento en la Ciudad de Madrid España

• INFORMÁTICO •

DESTACADOS EDI 2017



ALVARO ANDRADE SEJAS
BOLIVIA/PANAMÁ

Titular de Ethical Hacking
Conferencista

MARCELO ROMERO
ARGENTINA

Perito informático - investigador digital
Conferencista

EZEQUIEL TOSCO
ARGENTINA

Secretario General del Sindicato de Informáticos de Argentina

ANDRÉS VELAZQUEZ
MÉXICO

Experto en seguridad Informática - Conferencista

JEIMY CANO
COLOMBIA

Experto en Seguridad informática - Conferencista - Doctrinario

• ORGANISMOS GUBERNAMENTALES •

DESTACADOS EDI 2017

MINTIC

Gobierno de Colombia

MINISTERIO TIC COLOMBIA

Dirigido por Juanita Rodriguez Viceministra de economía digital

Autoridad Nacional para la Innovación Gubernamental

innovamos para ti

INNOVACION.GOB.PA PANAMÁ

Entidad competente del Estado para planificar, coordinar, emitir directrices, supervisar, colaborar, apoyar y promover el uso óptimo de las TIC´s en el sector gubernamental para la modernización de la gestión pública

MINISTERIO PÚBLICO FISCAL

PROCURACIÓN GENERAL DE LA NACIÓN

REPÚBLICA ARGENTINA

UFECI (UNIDAD FISCAL ESPECIALIZADA EN CIBERCRIMEN) ARGENTINA

Dirigido por el Dr Horacio Azzolin - Coordina de manera articulada el combate contra el cibercrimen

• APORTES ACADÉMICOS •

DESTACADOS EDI 2017

MARINA PAULA BENITEZ DEMTSCHENKO
ARGENTINA

Conferencista - Presidenta de la Fundación Activismo Feminista Digital

CARMEN VELARDE KOECHLIN
PERÚ

Consultora en Gestión, Desarrollo Social y Derecho de las tecnologías

UNIVERSIDAD AUTÓNOMA LATINOAMERICANA - UNAULA

UNIVERSIDAD AUTONOMA LATINOAMERICANA
COLOMBIA

Entidad que organiza hace 4 años uno de los Congresos más importantes en Derecho Informático de su pais

ASOCIACIÓN DE ESCRIBANOS DEL URUGUAY

ASOCIACIÓN DE ESCRIBANOS DE URUGUAY
URUGUAY

Entidad que da soporte, apoyo y coorganiza hace 3 años el Congreso más importante de Uruguay en Derecho Informático

CONCIENCIA EN RED

CONCIENCIA EN RED
ARGENTINA

ONG dedicada a la concientización en el uso de las tecnologías coordinada por la Lic Analia Martinez

LORENA NARANJO
ECUADOR

Directora Nacional de Dirección Nacional de Registro de Datos Públicos - Ecuador

• EVENTOS •

DESTACADOS EDI 2017

I CONGRESO ARGENTINO DE CIBERCRIMEN E INVESTIGACIÓN DIGITAL (RUBÉN AVALOS)

Coordinado por el Dr Rubén Avalos - más de 360 participantes Rosario/Santa fe

I JORNADA DE DERECHO Y TECNOLOGÍA COLEGIO ABOGADOS DE LIMA (EDDA KAREN CESPEDES BABILON)

Coordinado por la Dra Karen Céspedes el más grande desarrollado en Perú

I CONGRESO LATINOAMERICANO DE DERECHO INFORMATICO (CARLOS D. AGUIRRE)

Coordinado por el Dr Carlos D Aguirre, más de 280 Participantes - Córdoba/Córdoba

• MENCIONES ESPECIALES •

DESTACADOS EDI 2017

OBSERVATORIO GUATEMALTECO DE DELITOS INFORMÁTICOS

Observatorio Dirigido por el Lic José Leonett, emite informes sobre el estado de situación en materia de delitos informáticos en Guatemala

ANALÍA MARTINEZ ARGENTINA

Consultora en Gestión, Desarrollo Social y Derecho de las tecnologías

EMANUEL ORTIZ RUIZ COLOMBIA

Académico de la Universidad Externado de Colombia - Doctrinario

DANIEL LOPEZ CARBALLO ESPAÑA

Director del Observatorio Iberoamericano de Protección de Datos Personales

APANDETEC PANAMÁ

Asociación Panameña de Derecho y Nuevas Tecnologías Organizadores de congresos, t jornadas de capacitaciones

NATALIA TORANZO ARGENTINA

Lic en Informática Coordinadora Congreso de Cibercrimen Neuquen/Argentina

VACACIONES CUIDADOS ON LINE

SI SALIS DE VACACIONES

¿Dejás sola tu casa?

* Nunca anuncies que tu casa está sola.
* No publiques FOTOS o VIDEOS con ubicación.
* No subas la geolocalización en tus Redes
* Activá el desvío de llamadas de tu teléfono fijo a tu celular.
* No cuentes planes de viajes a contactos que poco conoces por chat.

Si decidís publicar en las redes

* Configurá los niveles de Seguridad de tus cuentas.
* Que no sea PÚBLICO ningún contenido.
* Resguardá a niños y niñas en las redes.
* Sé cuidadoso con las publicaciones, no des datos sensibles: fotos de pasaportes o pasajes con datos como códigos de barra o códigos QR, patentes de vehículos, direcciones postales, tarjetas de crédito, etc.

REDES SOCIALES

DISPOSITIVOS MÓVILES

* Vinculá tus dispositivos con una cuenta de mail y contraseña que recuerdes.
* En caso de extravío del dispositivo, bloquealos para evitar robo de información: fotos, videos, datos bancarios, contactos, entre otros.

www.concienciaenred.org
cer-argentina@concienciaenred.org
@CERargentina

CER
CONCIENCIA EN RED

PIENSA EN TU ACTIVIDAD

(EDI)

LA RED

ELDERECHOINFORMATICO.COM