EDI

Colaboran en esta edición:

Milagros Roibon - Ana Brian
Sebastian Gamen - Franco Vergara
Fabian Descalzo - Pedro J Macias T.
Marina Benitez D. - M. Eugenia Orbea
Franco Giandana

LOS DESTACADOS DEL AÑO 2016 ELDERECHOINFORMATICO.COM

El Derecho (Informático) las voces nuevas

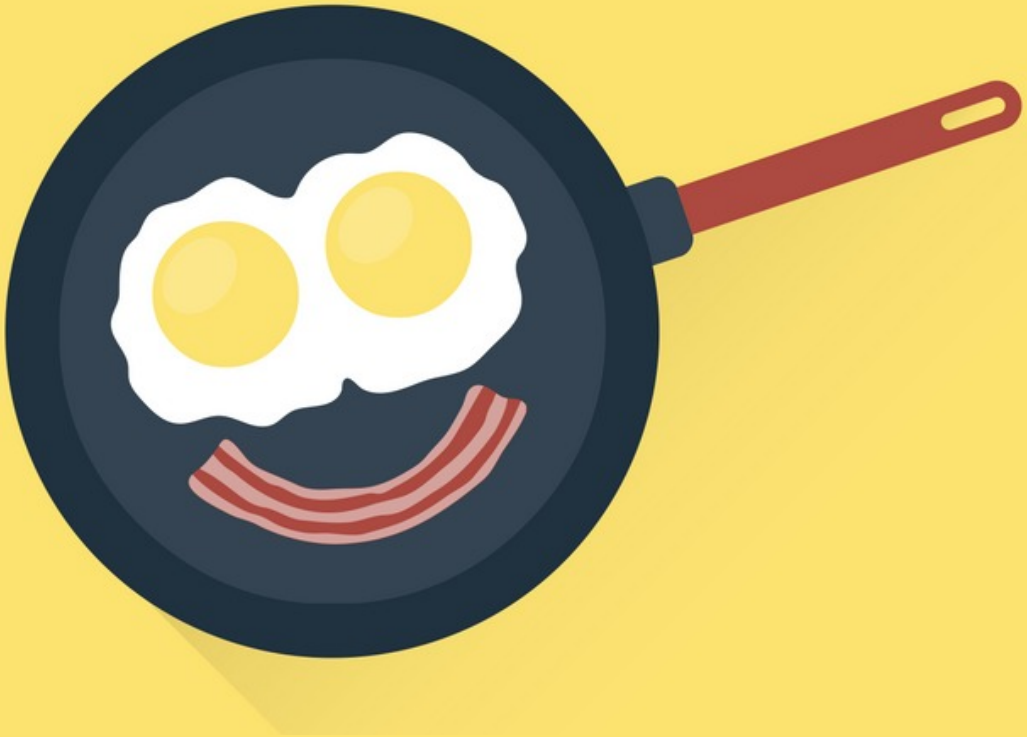
LA RED

REVISTA DIGITAL DE LA RED IBEROAMERICANA ELDERECHOINFORMATICO.COM

DICIEMBRE 2016 | EDICIÓN Nº 25 - DISTRIBUCIÓN GRATUITA

Arte de tapa: Florencia Cadario/Mariana Andersen/Mariano Rivero

Algo nuevo se está cocinando en La Red



ELDERECHOINFORMATICO.COM

EDI

contenido

Red Iberoamericana EDI

Edición N° 25 - Diciembre 2016
Distribución Gratuita

www.elderechoinformatico.com

librería | hammurabi

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

en preparación

Colección «elderechoinformático.com»

11 volúmenes

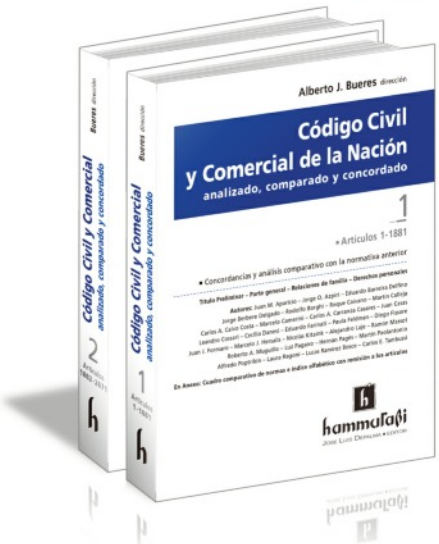
Guillermo M. Zamora dirección

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.

EDITORIAL

Edición n° 25 - Diciembre de 2016

Red Iberoamericana ElDerechoInformatico.com

Guillermo M. Zamora
Director EDI

CORRESPONSALES:

- Fedra Fontao / Marina Benitez Demtschenko - Argentina

- Laine Souza - Brasil

- Ana Mesa Elneser - Colombia

- Carlos Reusser Monsalvez - Chile

- Rafael Montenegro - Costa Rica

- José Leonett - Guatemala

- Hildamar Fernandez - Venezuela

- Elizabeth Bouvier - Uruguay

- Joel Gomez Treviño - México

- Enmanuel Alcantara - R. Dominicana

- Jorge Campanilla C. - España

La creatividad es inventar, experimentar, crecer, tomar riesgos, romper las reglas, cometer errores y divertirse -
Mary Lou Cook

ACTIVIDADES

Congresos en Uruguay, Colombia, Guatemala, Argentina, EDINoticias en 1 minuto, La Revista, Concursos hechos y proyectados al 2017, el Café Informático , Charlas, cursos, Proyectos de ley elevados, nuevos convenios de colaboración y reciprocidad con Universidades y distintas entidades de Iberoamerica, puntapie inicial para la Colección de libros de derecho informático de la Red junto a Editorial Hammurabi, fracasos, triunfos, hubo de todo, y para todos, 2016 no fue un año más definitivamente.-

Lo que no mata engorda y yo definitivamente estoy muy vivo (anonimo)

FUTURO:

Dificil es hablar de futuro en cuestiones que tienen relación con la tecnología, por suerte, el derecho informático, y esta Red es mucho más que algo tecnológico.-

En cada congreso que tenemos la oportunidad de compartir, nos convecemos más que no hay videoconferencia que valga lo que un abrazo y mucho menos un cafe compartido, no existe correo, video, o audio que pueda siquiera estar cerca de la increible experiencia de escuchar en primera persona la risa del compañero de ruta.-

Indudablemente, me siento afortunado, cada año que pasa, crecemos, mutamos, nos reconvertimos, buscamos más, pero un más de ambición sino de ansias, un más que nos enseña a repetir la charla y el café.-

La vida es un sinnumero de momentos, es la tristeza y la alegría de cada expresión que nos acerca, queda en nosotros ver como los manejamos.-

En infinidad de oportunidades me han preguntado, como hacer para pertenecer a la Red, lamentablemente no tengo una respuesta, no hay una forma mágica, ni un requisito, simplemente es estar, es querer, es hacer, lo he dicho mil veces, la Red somos todos, la Red es todo aquel que quiera estar, y sume, y empuje, y tire para adelante.-

La Red es todo aquel que quiera estar y haga cosas, porque no duden que el hacer es la forma mágica, no solo de pertencer, sino de crecer, solo o acompañados, busquen, estudien, lean, piensen, sean amigos, sean docentes, no se queden, porque el que se queda, muere. FELIZ AÑO!

Más que un blog.
Toda la actualidad jurídica.

información jurídica ágil, eficiente y relevante

aldiaargentina.microjuris.com

Llámenos (5411) 5031-9300

microjuris.com
inteligencia jurídica

La pornografía de venganza: la violencia de género por Internet y su tratamiento en el Código

Autor: María Milagros Roibón. Abogada, egresada de la UCA (2002). Ex abogada de la AFIP-DGI (por concurso). Empleada del Ministerio Público Fiscal (Rosario)

Introducción

En la actualidad, existen diversos enfoques sobre qué se considera un delito informático, incluso hay quienes niegan la existencia de los delitos informáticos como una categoría autónoma del Derecho. Pero la mayoría de los autores entiende que los delitos informáticos son aquellas conductas ilícitas que se cometen a través de un medio informático o electrónico.

Asimismo, los delitos informáticos presentan algunas características que -por el medio en donde se realizan- los diferencian de otros delitos. En ese sentido, se encuentra la trasnacionalidad, ya que sus efectos pueden esparcirse por toda la red o en un país distinto al lugar en donde se perpetró el ilícito. También, son delitos que se caracterizan por el anonimato que permiten los entornos virtuales, particularidad que favorece la comisión y proliferación de estos ilícitos.

Por otro lado, la complejidad y el avance vertiginoso de la tecnología conllevan a que algunas conductas disvaliosas -que se efectúan mediante un dispositivo informático- no se encuentren tipificadas en la legislación penal, quedando impunes o que su esclarecimiento resulte difícil. A esto se suma la poca capacitación de los operadores judiciales, la reticente colaboración de las empresas con la justicia local y que en muchas ocasiones la víctima se entera mucho tiempo después de que ha sido víctima de un delito, lo que retarda la investigación. Si bien concurren otros factores que problematizan la investigación de este tipo de criminalidad, entiendo que con lo mencionado es más que suficiente para el objeto del presente artículo.

En la Argentina, las Leyes 26.388 (2008) y 26.906 (2013) sustituyeron e incorporaron figuras típicas al Código Penal, regulando las conductas criminales que surgieron con la tecnología o aquellas conductas delictivas que se valen de los medios

electrónicos como nuevos medios de comisión, pero que ya se encontraban reguladas por el código de fondo.

¿Qué es la violencia de género de tipo sexual y cómo se manifiesta en Internet?

La facilidad con la que los usuarios pueden publicar contenidos en las redes sociales favorece la violencia de género contra la mujer, ya que cualquiera -valiéndose de una identidad real o ficticia- puede compartir fotos o videos de carácter sexual en segundos, y sin ningún tipo de censura. Las plataformas digitales también permiten que los contenidos se reproduzcan en poco tiempo, siendo vistos por miles de usuarios.

Por otro lado, la ley 26.846 (2009) distingue diferentes tipos de violencia contra la mujer, entre la que figura la sexual. El art. 5 de la norma concibe a la violencia sexual como "*Cualquier acción que implique la vulneración en todas sus formas, con o sin acceso genital, del derecho de la mujer de decidir voluntariamente acerca de su vida sexual o reproductiva a través de amenazas, coerción, uso de la fuerza o intimidación, incluyendo la violación dentro del matrimonio o de otras relaciones vinculares o de parentesco, exista o no convivencia, así como la prostitución forzada, explotación, esclavitud, acoso, abuso sexual y trata de mujeres*".

La Dra. Daniela Dupuy, Fiscal a cargo de la Fiscalía de Delitos Informáticos de la Ciudad Autónoma de Buenos Aires, señaló recientemente que en su fiscalía suelen recibir *"innumerables consultas de mujeres mayores de edad sobre quienes han publicado en Internet fotos o videos con contenido sexual. En la mayoría de estos casos, los acosadores suelen ser ex o actuales parejas, y pueden tratarse de situaciones aisladas o formar parte de un círculo de violencia hacia la mujer".*[1]

Estas acciones que -se conocen como pornografía de venganza o pornovenganza- consisten en que el agresor difunde las imágenes o videos sexuales de su víctima, sin que esta haya prestado su consentimiento. El victimario comparte esos contenidos en las redes sociales, en WhatsApp, por correo electrónico, etc. con la finalidad de humillar a la víctima. En la mayoría de los casos, son los hombres quienes realizan estas conductas. El hombre se venga de sus ex parejas, publicando fotos o videos de estas en situaciones sexuales, sin la autorización de la mujer.

En un primer momento, dos mayores de edad consintieron **libremente** filmarse o tomarse fotografías sexuales, pero con posterioridad una de ellas publica o difunde esos contenidos, sin la aprobación o la anuencia de la otra parte. Es decir que el consentimiento fue dado para grabar o tomar fotografías de carácter sexual, no para distribuirlos. La finalidad que motiva estas conductas es la represalia, el resentimiento, la extorsión o la venganza de un hombre contra su ex pareja.

La pornografía de venganza lesiona el derecho a la intimidad de la persona, cuyos videos o fotos sexuales se difunden si su consentimiento. Este derecho, tutelado por numerosa legislación, también fue tratado por la jurisprudencia. La Corte Suprema de Justicia de la Nación sostuvo que *"El derecho a la privacidad e intimidad, fundado en el artículo 19 de la Constitución Nacional, protege jurídicamente en relación directa con la libertad individual un ámbito de autonomía personal, así como acciones, hechos y datos que, conforme a las formas de vida acogidas por*

[1] Pornografía infantil y grooming representan el 87% de los delitos informáticos Consultado en http://www.eldia.com/informacion-general/pornografia-infantil-y-grooming-representan-el-87-de-casos-de-delitos-informaticos-179327 el 25/11/2016

la sociedad, están reservadas al individuo, y cuyo conocimiento y divulgación por extraños implica peligro real o potencial para la misma intimidad" (CSJN, 11-12-84, E. D. 112-239).

Cuando estas conductas son cometidas por el hombre -con la única intención de degradar a su ex mujer- conforman una modalidad de la violencia de género de tipo sexual, pero en el ámbito virtual o digital, en donde el hombre ejerce una posición de poder sobre la víctima, al exponer contenidos íntimos de ésta, pero sin su autorización. Hay que destacar que las mujeres también realizan estos actos, pero en proporción muy inferior a los casos en que los hombres son los victimarios.

Este tipo de violencia provoca efectos devastadores en quien la padece, al ver violada su intimidad, siendo expuesta a miles de desconocidos. En muchas ocasiones, las víctimas sufren ofensas, insultos o acoso por parte de quienes vieron sus fotos o videos.

El padecimiento de la mujer no finaliza con la publicación del video, sino que con posterioridad debe soportar las injurias y los ultrajes de quienes lo vieron. A través de un gravísimo atentado a la privacidad de la víctima, se la mortifica psicológica y socialmente; razones más que suficientes para que estas agresiones no sean ajenas a la consideración jurídica.

La pornografía de venganza en el Derecho Penal argentino

Si bien el Código penal argentino no castiga la pornografía por venganza, el 23 de noviembre pasado el Senado de la Nación dio media sanción al proyecto de ley de la senadora Marina Riofrío sobre la penalización de la publicación o difusión de imágenes no consentidas de desnudez parcial o total. Esta iniciativa incorpora el artículo 155 bis al Código Penal, el que establece penas de 6 meses a 4 años de prisión a quien publique o difunda imágenes o videos de contenido sexual o erótico de personas, a través de medios de comunicaciones electrónicas, aun habiendo existido acuerdo entre las partes involucradas para la obtención o suministro de esas imágenes o video.[1]

Si la Cámara de Diputados de la Nación convierta en ley este proyecto, la Argentina habrá avanzado significativamente en una materia, en donde confluyen los delitos informáticos, la violencia de género y la protección del derecho a la intimidad. De esta forma, una innumerable cantidad de conductas que antes permanecían impunes -con las consecuencias perjudiciales para las víctimas- serán denunciadas y posiblemente condenadas por los tribunales, evitando que las mujeres queden desamparadas frente a este tipo de violencia.

Con el uso indebido de la tecnología, la intimidad de una persona puede resultar tan fácilmente vulnerada, que su protección se convierte en una prioridad para los Estados de derecho y para la pacífica convivencia de las personas que diariamente se conectan a Internet. El Estado debe velar -a través de la ley- para que las personas no sean mortificadas ni flageladas en su integridad sexual ni en su libertad individual, impidiendo hostigamientos y acosos de personas que -con el único fin de dañar- ejercen violencia detrás de una pantalla o desde la comodidad de un dispositivo informático.

[1] Aprobaron el proyecto contra la "pornovenganza" consultado en http://www.parlamentario.com/noticia-97017.html el 25/11/2016

2017
La Red EDI

En crecimiento constante

EDI - La RedIBEROAMERICA

Facebook.com/elderechoinformatico | www.elderechoinformatico.com
Twitter: elderechoinf

“NOCIONES BÁSICAS DEL NUEVO DELITO DE PHISHING EN EL DERECHO ESPAÑOL”

Autor: **Pedro Jesús Macías Torres**
Sevilla/España

Muchas veces se ha afirmado y nunca con falta de razón que las tecnologías muestran una doble cara; una de ellas que permite una calidad de vida mejor, más llevadera, rápida y sencilla y otra, no tan positiva contra la que debemos repeler sus consecuencias. El ser humano tradicionalmente se ha decantado en no pocas ocasiones por determinadas conductas al margen de lo que la sociedad, sobretodo el Derecho consideran licitud. Para el mundo de los penalistas, mucho se ha tenido que esperar para que el ordenamiento jurídico español tipificara lo que es delito de phishing, rellenando las lagunas que siempre existen ante un avance inconmensurable de los instrumentos que la técnica innova.

Recordando lo que en esencia es la estafa, nuestros profesores nos mostraban una realidad formada por cuatro actos escalonados para que el delito como tal llegara a consumirse y ser objeto de reproche por ley: el engaño, el error, la disposición patrimonial y el perjuicio a favor de un tercero y con el que la finalidad defraudatoria se había logrado. Pero con el phishing, ¿ocurre lo mismo?, ¿qué hay de común y de novedoso respecto de la estafa?

En esencia y ajustándonos a lo que constituye la cotidianidad muchos días hemos recibido e-mails con ofertas de trabajo bastante suculentas por las que a través de una labor efectuada desde casa y sin excesivas complicaciones, percibiríamos unos emolumentos difíciles de obtener, aun desempeñando un trabajo que requiera horas de esfuerzo, sacrificio, buena preparación y una considerable responsabilidad. En resumidas palabras, el phishing es una nueva modalidad de comisión delictiva por la que empleando las nuevas tecnologías, el verdadero defraudador quiere un beneficio económico; casi siempre una gran cantidad de dinero. El Código Penal español en su artículo 248.2 afirma que además de lo que viene siendo la estafa tradicional, también se consideran reos de la misma: “*Los que con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro*”. Es fácil deducir tras la lectura de este párrafo que el bien jurídico protegido es precisamente el patrimonio en sí. Las actuaciones de defraudadores que emplean herramientas cada vez más pulidas y que generan una credibilidad difícil de superar tienen su freno en el Código Penal a raíz de la modificación sufrida por la Ley Orgánica 5/2010, de 22 de Junio, reformándose de nuevo en 2015, por la Ley Orgánica 1/2015, de 30 de Marzo. Existen diversas variantes

defraudatorias con peculiaridades que las diferencian del resto y todas con una terminología anglosajona; pongamos por ejemplo: el denominado whaling. Para diferenciarlo de lo que es el phishing, debemos atenernos a la víctima que lo padece. Con el primero el usuario de una entidad bancaria recibe un correo electrónico pensando que procede del banco donde tiene ingresado todo o parte de su dinero. El defraudador solicita unas claves a la víctima de estafa informática y ésta se los manda por medio de un archivo adjunto HTML enviado previamente por la supuesta entidad bancaria; de esta manera resulta más difícil si cabe el realizar un rastreo por parte de la policía al inicio de las investigaciones que se efectuasen. Con el whaling el grupo de víctimas tiene un carácter reduccionista, circunscribiéndose a los empleados o trabajadores del mundo de las finanzas incorporados a grandes empresas.

Con la estafa informática, modalidad phishing (o pesca de incautos), el defraudador recibirá esas claves necesarias para la extracción involuntaria o inconsentida de su titular. La cuestión se complica aún más; aparentemente el esquema conceptual no reviste dificultad alguna pero hay que saber que el autor material del delito no trabaja sólo, sino que junto a él intervienen unos cooperadores que nuestro modo de ver son cooperadores necesarios para la comisión del delito, por tanto, ele elemento doloso se encuentra presente, a menos que quepa desconocimiento por parte de estos cooperadores o intermediarios que reciben de manera popular y en lenguaje policiaco el nombre de “muleros” o “muleros bancarios”.

El verdadero defraudador, cabeza intelectual de la trama encarga al mulero que se ponga en contacto con las víctimas a fin de obtener dichas claves que sólo el titular de la cuenta puede y debe saber. Cuando la víctima de phishing proporciona inocentemente lo solicitado a quien se lo envía es al propio cooperador (que cobrará un porcentaje de lo acordado) y esta cantidad defraudada emprenderá un segundo viaje que por regla general va dirigida al extranjero, lugar donde se sitúa el defraudador autentico y que no tiene por qué mantener relación alguna con la víctima, a la que ya se ha desposeído de su patrimonio. Es obvio afirmar que la intervención de estos muleros son elementos esenciales para que el delito de phishing se efectué y además que se haga sin levantar ningún tipo de sospechas. No sólo debemos saber que la técnica empleada a través de los ordenadores es esencial para que el delito vaya “edificándose”; también la existencia de una cuenta corriente en el extranjero con la que cobrar las cantidades trasladadas en el menor tiempo posible nos puede dar una ligera idea de la rápidez con la que estos sujetos activos se emplean a fondo; la construcción de una web simulando a modo de ejemplo una entidad bancaria dista y mucho de los primeros intentos que allá por lo años noventa del pasado siglo se realizaban y por ello supone una dedicación de cara a generar una confianza en la que será la próxima víctima.

De cara a intervenciones por parte de la policía, resulta más difícil detectar al cooperador necesario, al mulero como tal que generalmente residirá en el mismo país que el sujeto pasivo, coincidan o no las poblaciones en las que habiten. Frente a un juicio de competencia, diversos pronunciamientos judiciales muy recientes colocan el lugar de residencia y actuación del mulero como el idóneo para que el juzgado correspondiente conozca del caso para su instrucción y parece viable que así fuera, pues si hablamos de un “circuito bancario”, expresión acertada a mi modo de ver por parte de los

penalistas, este cooperador o intermediario evitará con su actuación la no reversión de ese dinero, es decir, un patrimonio económico considerable que probablemente nunca recuperará. La víctima tiene como opción preferente comunicarlo al banco del que es cliente y en virtud de nuestra Ley de Servicios de Pago, la entidad financiera debería devolver esas cantidades sustraídas sin su beneplácito pero para ello es conveniente la comunicación con el banco con inmediatez absoluta y la ausencia de un ánimo fraudulento con la empresa; el mismo mínimo fraudulento que el estafador y el mulero (no en todas las ocasiones) han tenido para elaborar esta modalidad delictiva. Regresando a las primeras líneas de este trabajo, hemos mencionado que la estafa se caracteriza por un engaño, posteriormente un error más tarde la entrega o disposición patrimonial y el perjuicio ocasionado a la víctima. Si éste no existe, no debemos hablar de un delito de estafa. Con la estafa informática los dos primeros elementos, es decir: engaño y error no suelen estar igual de definidos que la estafa tradicional recogida en el artículo 248.1 del Código Penal español. La intervención de las computadoras, les da un aire de autonomía, más que nada por el contenido del programa que incorporan éstas. Si el programa confeccionado se hace para defraudar, en mi opinión, sí cabe la existencia de una "colaboración de la víctima" en el mismo instante en el que en la mente del usuario de las claves se forja una realidad no ajustada a lo que es y accede por tanto al fraude. Si una falsa web de un banco solicita las claves que el cliente pudiera tener, al programa informático no se le puede exigir una concreta responsabilidad penal. Es el defraudador el que con mala fe elabora el programa para que la potencial víctima descargue el archivo adjunto e introduzca los datos requeridos.

El último de los aspectos que deseo destacar dentro de lo que es una explicación sucinta de esta nueva vertiente de delitos contra el patrimonio se encuentra en lo que se conoce como "ignorancia deliberada", un tanto criticada por la doctrina del Tribunal Supremo, pero que la mayor parte de nuestras Audiencias Provinciales la han apoyado. Consiste básicamente en la calificación de partícipe con existencia de dolo al tener constancia de que la actuación desempeñada sea algo ilícito, por parte del mulero. Para los jueces no es necesario el conocimiento exhaustivo de toda la operativa: cuando empieza, cuando se pretende concluir, identidad del defraudador, motivos que conducen a una actividad defraudatoria, etc. No es necesario a mi modo de ver que el mulero posea una basta formación académica; puede deducirse sencillamente que emitir una solicitud de trabajo con grandes contraprestaciones para integrarlos en una cuenta corriente que después pasa a otra del extranjero no forma parte de lo cotidiano. En palabras del Tribunal Supremo, los muleros "*tienen un conocimiento necesario para prestar su colaboración y la ignorancia del resto del operativo no borra, ni disminuye su culpabilidad porque fueron conscientes de la antijuricidad de su conducta*". Algunos casos en España en los que el recurso de apelación del mulero ha sido completamente desestimado y consideran que de manera efectiva había un dolo necesario y como consecuencia debería aplicarse el artículo 248.2 del Código Penal. En definitiva y cerrando este tema, el mulero siempre responderá cuando tenga conocimiento de los resultados que pudieran preverse y que su conducta conformara un hecho delictivo.

Si tuviéramos que hacer un comentario como conclusión en un supuesto de este tipo (delito de

phishing) deberíamos decir que en puridad, todos son perjudicados: en primer lugar la propia víctima como el perjuicio que se le causa, ha confiado ella en la credibilidad que la web falsa expone en su pantalla y con su buena fe envía esas claves numéricas (o alfanuméricas), creyendo que el banco los necesita por ejemplo para el envío de promociones nuevas de productos con determinada rentabilidad, pero salen perdiendo también autores y participes interviniente en lo que a la tecnología se refiere. Como recomendación máxima se aconseja el cierre de todas las aplicaciones antes de acceder a la web del banco, escribir la URL en el navegador prescindiendo de cualquier tipo de enlace que se ofrezcan, cerciorarse que la web comienza por https://, de esta manera los datos que circulan por Internet estarán dotados de mayor seguridad, pues van cifrados y no acceder a los servicios de banca on line a través de ordenadores públicos. Si no se siguen estos pasos muy difícil será atajar una lacra como la que este trabajo exponemos.

Pedro Jesús Macías Torres

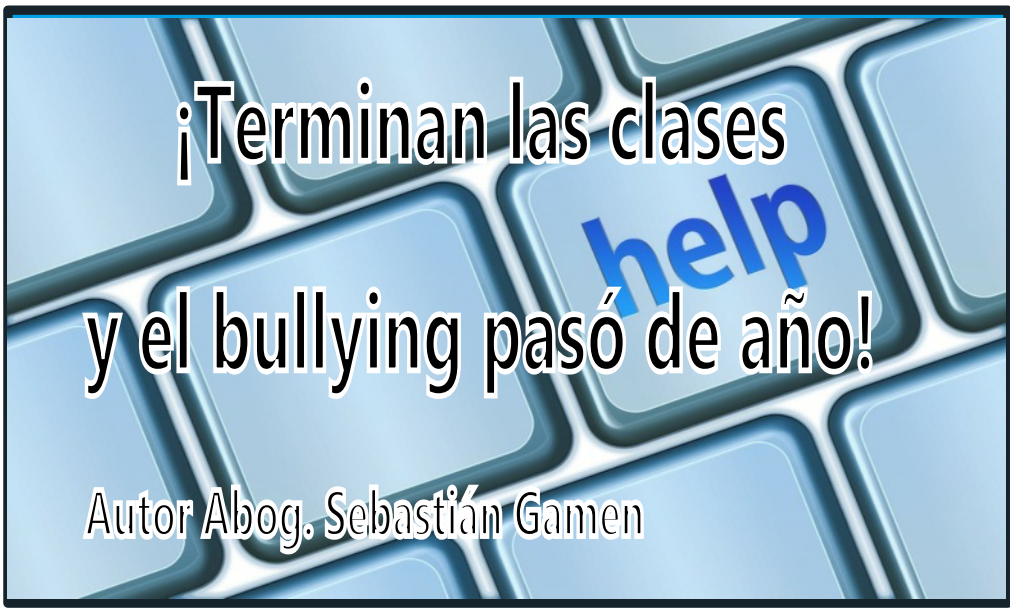
Licenciado en Derecho. Itinerario Derecho de la Administración de Justicia (Privado).Universidad Pablo de Olavide de Sevilla.

Alumno del Máster Oficial de Derecho de las Nuevas Tecnologías, impartido por la Universidad Pablo de Olavide, de Sevilla en el curso académico 2015-2016

Ha asistido a numerosos Congresos, Conferencias y Seminarios en temas vinculados con el Derecho de las Nuevas Tecnologías, así como cursos entre ellos: : Programa de Cursos TIC,s 2004 de la Junta de Andalucía: "Experto en Derecho y Nuevas Tecnologías". Modalidad Semipresencial

ESTAMOS EDIficando

RESPONSABLE
SEBASTIÁN
GAMEN



Pelea de gallos se llama un grupo de WhatsApp creado por chicos madrileños (España) y que busca que un par de participantes se humillen uno a otro, y los observadores deciden finalmente el ganador, el más cruel. La edad de sus creadores es de apenas 10 años.

La mayoría de las redes sociales, Facebook, Twitter, Instagram, WhatsApp, Snapchat prohíben su uso para menores de 13 pero los niños se las rebuscan, muchas veces con la anuencia de sus padres, para estar presentes.

El bullying es el acoso u hostigamiento o todo acto de maltrato y/o violencia física, verbal y/o psicológica al que es sometido de manera repetida y sostenida en el tiempo una persona. Este acoso cuando se traslada del mundo físico a internet se le llama ciberbullying. Dos nombres para un mismo problema.

Las formas del bullying son de las más variadas con la ayuda irremplazable de los smartphones, la Victorinox del abusador. Los nuevos teléfonos filman, sacan fotos, dan acceso a las redes sociales, a los mensajes, a comentar, a publicar, a llamar, a dejar mensajes. Hubo denuncias de malos tratos verbales, referidos a condiciones de religión, raza, defectos físicos. Hubo denuncias por filmar o sacar fotos de compañeros desnudos en el baño, o simplemente por sacar fotos por debajo de las faldas de las compañeras para luego, con un solo clic viralizar sin el menor control posterior sobre la imagen.

En Argentina los últimos datos son preocupantes. Según el informe del Observatorio para la República Argentina de Bullying Sin Fronteras (3er Trimestre de 2016) el aumento de las denuncias en escuelas primarias y secundarias aumentaron un 33%. En 2015 hubo 1184 casos, frente a los 1561 del presente año. Siempre estos números esconden una realidad aún peor, considerando todos los casos que no fueron denunciados.

Este informe nos brinda información interesante en la Argentina, que podría replicarse en otros países iberoamericanos. Dice que “Las chicas más bonitas y más femeninas siguen siendo el colectivo escolar más atacado. Los motivos contra las chicas son la belleza y comportamiento sofisticado en un 50%, el rendimiento escolar superior 22%, los defectos físicos 12%, rendimiento escolar inferior en un 8%, rendimiento deportivo inferior 4%. ¿Qué ocurre con los chicos? Belleza y comportamiento sofisticado: 22%, rendimiento escolar superior 24%, defectos físicos un 28%, rendimiento escolar inferior en un 12% y rendimiento deportivo inferior 8%.

El problema del bullying actual es que no cesa, sigue a la víctima a todas partes y eso agota, genera una desesperación de no encontrar en el mundo un lugar seguro, un lugar libre de ofensas, de maltratos, de humillaciones. Esa misma desesperación lleva a las víctimas a tomar la decisión más radical, el suicidio.

En la Argentina el caso que llevó el bullying a los medios (2004) fue el del chico de Carmen de Patagones, Junior, que usó un arma en el colegio para disparar a mansalva a sus compañeros del aula. Después llegó la triste noticia del homicidio de Nayra Cofreces, asesinada por sus compañeras en Junín el 2 de mayo. A lo que hay sumarle los casos de suicidios en La Pampa de Milton y en el barrio porteño de Nuñez de Francisco, en una secuencia de muertes que ya no son hechos aislados.

Legislar y educar.

En un mundo interconectado no mirar que pasa en otros países es una bobera. Solo para hacer una pequeña comparación con otros países vemos que en Estados Unidos hay legislaciones en California (1999), Florida con su norma HB 479 (2003) y Misuri (2006) con sus estatutos sobre acoso para incluir el acoso y el acecho mediante comunicaciones electrónicas y telefónicas, así como el ciberacoso escolar después del Suicidio de Megan Meier (2006). A nivel federal cuentan con el Acta Violence Against Women Act (2000) que incluyó el ciberacoso en una parte del estatuto interestatal sobre el acoso. Finalmente, existe la ley federal que hace referencia al ciberacoso en Estados Unidos, la 47 USC sec. 223.

En otros países existen legislaciones para la prevención, cuyo éxito habrá que estudiarse dentro de algunos años.

En Argentina La Ley Nacional Nro. 26.892 trata el tema, aunque carece de reglamentación, lo que la torna en absolutamente ineficiente. A nivel provincial Buenos Aires y la Ciudad Autónoma de Buenos Aires con la ley votada el pasado 07 de diciembre del corriente año, apuntan a la prevención, la educación, la contención de la víctima y la realización de campañas de concientización.

Pero al margen de las legislaciones nacionales o provinciales, debemos tener tatuado en nuestras vidas la Declaración universal de los derechos humanos que en su Artículo 5 expresa que “Nadie será sometido a torturas ni a penas o tratos crueles, inhumanos o degradantes".

La Declaración ha sido considerada en varias oportunidades por la Suprema Corte de Justicia de la Nación como operativa y aplicable, siendo que desde el año 1994 tiene carácter constitucional. Si nos remitimos a los antecedentes específicos podemos comenzar en la década del 80 cuando dijo que “el art. 2 de la CADH es bien claro en el sentido que los derechos y libertades mencionados en el artículo precedente – que son todos los que consagra la Convención- deben ser específicamente incorporados al derecho interno de los Estados partes, en caso de no encontrarse ya garantizados en ellos, mediante las disposiciones legislativas o de otra índole...”. En ese sentido, la CSJN continuó diciendo que “carecería de sentido esta obligación que asumen los Estados que suscriben el tratado en cuanto a adoptar las

disposiciones de derechos internos que se requieran para garantizar la tutela de los derechos que en él se enuncian", si el contenido no fuere operativo.

La discusión sobre el carácter programático u operativo de los tratados de derechos humanos terminó con la sentencia "Ekmedjian".

En conclusión, las declaraciones y tratados internacionales sobre derechos humanos forman parte del derecho interno, y deben ser aplicables por los jueces. Y lo más importante, la interpretación de los instrumentos internacionales sobre derechos humanos deben realizarse a partir del principio pro homine, privilegiando siempre a la persona humana.

Parece exorbitante usar la declaración Universal de los derechos humanos para casos de bullying pero, cuando pensamos en que los chicos se están suicidando la respuesta es un no rotundo.

Volviendo al ordenamiento legal vigente en Argentina, en mi opinión tenemos herramientas suficientes para controlar el acoso. Desde el punto de vista penal, muchas de las conductas de los abusadores encuadran en los delitos de lesiones, amenazas, coacciones, calumnias e injurias.

Desde el plano de la responsabilidad civil, la situación se facilita mucho. Aun cuando estemos hablando de menores la letra de la ley cae como un baldaso de agua fría, la ley no protege a quién causa un daño a otro.

Porque las malas costumbres familiares, o la falta de educación en casa nunca debe ser soportado por un tercero inocente. La familia sigue siendo la célula de la sociedad y el estándar del "buen padre de familia" sigue más vigente y con más fuerza que nunca.

Los padres del abusador son civilmente responsables por los daños que ocasionan sus hijos, imputación que se le atribuye por culpa in vigilando o por inculcar una educación insuficiente, situación que se presume por el actuar ilícito del menor. Cabe la aclaración que el bullying no es un acto aislado, sino una conducta ilícita continuada y prolongada en el tiempo.

El flamante Código Civil y Comercial de la Nación en el Título V, sección 6º del libro III, que se titula "Responsabilidad por el hecho de terceros", dispone el Art. 1754. Hecho de los hijos que "Los padres son solidariamente responsables por los daños causados por los hijos que se encuentran bajo su responsabilidad parental y que habitan con ellos, sin perjuicio de la responsabilidad personal y concurrente que pueda caber a los hijos".

Esta responsabilidad de los padres se traslada a los establecimientos educativos mientras permanezcan en ellos. Entonces, encontramos en el ordenamiento vigente dos responsables por los actos ilícitos del abusador, y el bullying es sin dudas un acto ilícito.

Las herramientas existen, lo que hay que preguntarse es si los jueces tienen la voluntad de aplicar la ley, cuidar los derechos de las personas y revalorizar el concepto de responsabilidad, tan enflaquecido por nuestros días.

Sebastián A. Gamen
Abogado especialista en derecho informático y Nuevas tecnologías.
Contacto: sag@sebastiangamen.com

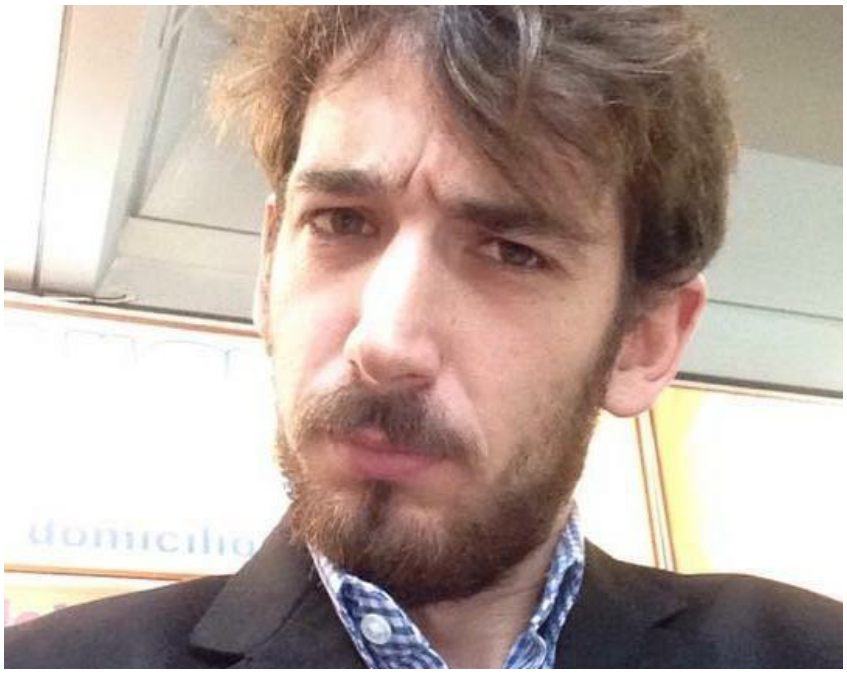
DIPLOMATURA

POSGRADO EN DERECHO INFORMÁTICO
ORGANIZA: ELDERECHOINFORMATICO.COM

1. Delitos Informáticos
2. Informática Forense
3. Aspectos Legales Datos Personales
4. Gobierno Digital
5. Aspectos Legales Cloud Computing
6. Régimen Jurídico Nombres de dominio
7. Aspectos legales del e-commerce
8. Teletrabajo
9. Propiedad Intelectual
10. Certificaciones Digitales

CERTIFICA UNIVERSIDAD NACIONAL
DE RIO NEGRO/ARGENTINA

EL SOFTWARE LIBRE COMO EXPRESIÓN DE CULTURA



Autor: Franco Giandana
Abogado e investigador especialista en Informática y en "Nueva Economía" .
Coordinador general en Ageia Densi
Promotor de la Sociedad de la Información y la Cultura Libre

"El código abierto es inequívocamente el motor de la innovación: ya sea potenciando la tecnología como en sistemas operativos, big data o IoT, o empoderando nueva generación de código abierto y entregando contundentes soluciones para el mercado"

Paul Santinelli - General Partner - North Bridge

Todas las empresas mas grandes de internet y la mayoría de los gobiernos actualmente utilizan Software Libre y la tendencia es creciente. Organizaciones como la NASA lo eligen por sus beneficios, es decir que este nuevo tipo de tecnología esta creando una nueva plataforma para el desarrollo tecnológico de innovación a nivel revolución industrial, causando impacto a nivel político y jurídico con una rapidez y fuerza que nos permite, ya en el año 2016, afirmar que nos encontramos ante un nuevo paradigma socio-productivo.

El Software libre es el elemento central de la Cultura Libre, aquella que según wikipedia.com se define como una corriente de pensamiento que promueve la libertad en la distribución y modificación de trabajos creativos basándose en el principio del contenido libre para distribuir o modificar trabajos y obras creativas, usando Internet así como otros medios. Este movimiento se opone principalmente a las medidas restrictivas del Derecho de Autor, por considerarlas principalmente un obstáculo para el desarrollo de la cultura y las ciencias. En orden de entender mejor la relevancia de este conjunto de normas, cabe mencionar que son considerados uno de los Derechos Fundamentales en la Declaración Universal de los Derechos Humanos. Estos Derechos están conformados por el conjunto de normas jurídicas y principios que afirman los derechos morales y patrimoniales que la ley concede a los autores (los derechos de autor), por el solo hecho de la creación de una obra literaria, artística, musical, científica o didáctica, esté publicada o inédita. En Argentina, estos derechos se encuentran regulados en la Ley 11.723, la cual, en su artículo 2° establece: "El derecho de propiedad de una obra científica, literaria o artística, comprende para su autor la facultad de disponer de ella, de publicarla, de

ejecutarla, de representarla, y exponerla en público, de enajenarla, de traducirla, de adaptarla o de autorizar su traducción y de reproducirla en cualquier forma".

En primer lugar, debe tenerse en cuenta que el software libre no es necesariamente gratuito, sino que – a diferencia del software no libre o propietario – puede ser usado, copiado, estudiado, modificado y redistribuido libremente. Esto quiere decir que el software libre puede ser vendido comercialmente sin dejar de ser libre. La Cultura Libre si bien se opone a las medidas restrictivas del descripto marco jurídico, no se opone totalmente a su regulación, ya que encuentra sustento en los artículos 17, 19 y 27 de la Declaración Universal de los Derechos del Hombre en la que se afirman los derechos que se protegen y se valoran en la Sociedad de la Información, esto son los de propiedad colectiva, libertad de expresión, formar parte de la vida cultural de la comunidad y a que se protegen sus obras cualquiera sea su naturaleza. Claramente estos objetivos tan sublimes solo pueden intentarse a través de una libre circulación de la información y a una integración progresiva de la comunidad. Estos son los valores predominantes en el nuevo paradigma, y ya que nos encontramos frente a nuevas demandas sociales, y estas a su vez deben enmarcarse en la regulación actual, que es antigua y en muchas casos no permite innovar (caso del co-working, que carece de seguridad Jurídica, o la actual ley de Sociedades Comerciales) debemos encontrar mecanismos que contemple la ley a los fines de asegurar el constante intercambio y circulación de la información. Ante esto, el Estado no debe ser indiferente, ya que en su afán de desarrollar la Sociedad y en su herramienta financiera que es el presupuesto, tiene la obligación de elegir aquellos recursos que faciliten la administración correcta por parte del Gobierno. Actualmente America Latina se encuentra progresando en cuanto a implementación de Software Libre se refiere, aunque aun existe ignorancia por parte de los "policymakers" de aquellos aspectos fundamentales que hacen a la decisión por un tipo de licencia libre o privativa. Es necesario entonces asegurar que aquellos encargados de la creación de las normas que rigen la conducta social, cumplan con su obligación de saber, frente esto, existen organizaciones como AGEIA DENSI, que se encuentran en el centro de este fenómeno con el afán de gestionar una mejor transición a través del asesoramiento a Instituciones. La dificultad que reviste una correcta lectura del sistema normativo y comercial justifican su existencia, ya que se necesita un enfoque multidisciplinario al momento de adoptar medidas sustentantes a nivel tecnológico.

Este fenómeno se ha desarrollado tanto que autores como Kevin Kelly ya sostienen que nos encontramos ante una Nueva Economía, la cual tiene rasgos propios y son lo de centrarse en los servicios y en el conocimiento, incorporando al sistema productivo a la información como un recurso. Esta nueva economía a su vez, prioriza la innovación y lo intangible sobre lo tangible. A nivel jurídico, esto se presenta como un desafío a nivel regulación, ya que las leyes deben acompañar a la generación de nuevas invenciones sin disminuir ni desalentar el proceso creativo. Esta economía tiene como rasgos fundamentales los de centrarse en la información y el conocimiento como bases de la producción y la competitividad. Además, es una economía global donde el sistema de organización es la Internet.

Por su vinculación directa con modos de producción cooperativa, resulta evidente el rol

protagonista del software libre en el cambio de la matriz productiva y, desde allí, en la configuración de un nuevo tejido socio productivo de carácter tecnológico en el ámbito de la economía social y solidaria. El proceso de desarrollo del software libre ha dado pruebas de éxito, debido al número de gente involucrada y al número de proyectos de código abierto que se han producido. No es del todo descabellado afirmar, como hace Vidal (2000), que el software libre, tomado como un todo, sería la empresa de software más productiva y poderosa del mercado.

Se trata entonces, de una filosofía en el que los individuos colaboran entre si para producir mas y mejores soluciones tecnológicas, permitiendo la comunicación entre diferentes regiones del mundo y sosteniendo un principio de comunidad cada vez mayor. Siguiendo a Alexander Bard, se supera el individualismo promulgado por Rene Descartes y Kant. En contraposición, nos encontramos en el paradigma relacionista, en la Sociedad de la Información, donde el individuo deja de ser el elemento central a desarrollar, y es reemplazado por la comunidad, es decir, los individuos no tienen existencia per se, si no que son reconocidos como elementos de un "red" superior. La sociedad es entonces un conjunto de redes mas que de personas. En este nuevo esquema productivo, la Cultura Libre y la generación de información, son el combustible que permite que cada día nos encontremos frente al cambio, ya se este real o potencial, podemos estar seguro que lo único permanente es el cambio. Es entonces que se sostiene que ante tanto dinamismo, la información no puede encontrarse protegida o priorizarse los intereses de un solo individuo por los de la sociedad en general.

Citando a Santiago García Gago el "conocimiento puede fluir libremente al igual que ocurría antes de la imprenta cerrándose así el paréntesis de más de 500 años que abrió Gutenberg". Este conjunto de prácticas construidas en red, de forma distribuida y a lo largo del tiempo conforman un nuevo protocolo de gobernabilidad que podría, según de la Cueva (2012), escalarse hacia las políticas públicas y el Estado. Otros autores como Antonio Lafuente (Gutiérrez, 2012) aseguran que

«los hackers son los científicos de la nueva Ilustración», lo que fortalece la tesis de que el software libre no es apenas un ejercicio de soberanía tecnológica o de ahorro de recursos, sino un ejercicio de ciudadanía virtuosa y de democracia. Emerge entonces una suerte de nueva clase social, el cognitariado auto organizado (Berardi, 2003), del que forman parte los/as hackers, en contradicción frontal con la organización capitalista del trabajo, en manos del Estado o la corporación. En cuanto al proceso creativo, ha quedado demostrado que un mayor volumen de información y acceso acelera la innovación, por lo que apostamos a que se continúe liberando obras a los fines de empedrar cada vez mas a las sociedades y a enriquecer las relaciones estructurales que la soportan.

Es preciso conceptualizar a los bienes comunes como aquellos de acceso universal, de titularidad colectiva, cuyo uso se sostiene en el tiempo. No es un bien privado ni público. Este concepto comprende una serie de recursos, tanto físicos como intangibles, que son gestionados por una comunidad que puede ser física o virtual. La noción de bien común implica que todos los individuos de la comunidad tengan derecho a su uso y a obtener beneficios de esos recursos, lo que implica que el uso de una persona no impida que el resto lo utilice. Es decir que no es excluyente. De esta forma, podrían ser bienes comunes un bosque gestionado comunitariamente como también el conocimiento. Que un bien sea común no tiene que ver con su característica intrínseca sino más bien con la gestión que se haga de ese recurso. Debemos destacar el trabajo que ha realizado por Elionor Ostrom, Premio Nobel de Economía en el año 2009 por su trabajo sobre el "gobierno de los comunes". La labor investigadora de la profesora de la Universidad de Indiana logró recoger multitud de experiencias, muchas de ellas situadas en el área iberoamericana, que demostraban que la existencia de espacios y bienes comunales, es decir la no atribución de propiedad específica a sus usuarios, no conllevaba inevitablemente la sobreexplotación de los recursos y la pérdida y erosión de ese patrimonio. Ostrom demuestra que las formas de explotación comunal pueden proporciona mecanismos de autogobierno que garanticen equidad en el acceso, un control radicalmente democrático, a la vez que proporciona protección y vitalidad al recurso compartido por lo tanto, ante la posibilidad de la sobre explotación, la respuesta de Ostrom es "incrementar las capacidades de los participantes para cambiar las reglas coercitivas del juego a fin de alcanzar resultados distintos a las despiadadas tragedias". Este es el objetivo de la Cultura Libre.

La legislación relativa a derechos de autor concede al programador (o, en el caso de que se trate de un programador asalariado, a su empresario) un alto grado de control sobre el programa que ha creado. En concreto, es ilícito que un tercero distinto al titular de los derechos ejecute, copie, transforme o distribuya el programa, salvo con previa autorización del titular de los derechos. Por lo tanto, siempre será necesaria la previa autorización del titular de los Derechos de Autor para ejecutar, copiar en cualquiera de sus formatos, modificar o distribuir el programa, esto aplica incluso a los Estados. Básicamente este marco jurídico se opone a los lineamientos básicos de la Nueva Economía, ya que dificulta el desarrollo de Software que pueda ser compartido a los fines de generar competitividad en la calidad de las soluciones y no en su mero desarrollo.

El software libre se caracteriza por hacer uso de la legislación de copyright para definir la licencia de uso y explotación del código informático, con el objetivo de garantizar la liberta de uso, copia, modificación (que exige acceso al código fuente de programación) y la publicación de modificaciones. Esta versión de Copyright es también conocida como Copyleft. El artículo 27 de la Declaración Universal de los Derechos Humanos establece que "toda persona tiene derecho a tomar parte libremente en la vida cultural de la comunidad, a gozar de las artes y a participar en el progreso científico y en los beneficios que de él resulten". A su vez determina que "la persona tiene derecho a la protección de los intereses morales y materiales que le correspondan por razón de las producciones científicas, literarias o artísticas de que sea autora". También, el convenio

de Berna sobre la protección de obras literarias y artísticas de 1886, y los tratados de la OMPI sobre Internet en 1996, sentaron las bases de protección del contenido del derecho de autor, las limitaciones del mismo y su promoción mediante las tecnologías para la distribución y el uso de esos contenidos creativos. El titular de la creación u obra cuenta con una importante protección establecida en la normativa internacional, la OMPI regulo contratos de cesión de derechos como un acuerdo de licencia y lo definió de la siguiente manera: "un acuerdo de licencia es una asociación entre el titular de derechos de propiedad intelectual (licenciante) y otra persona que recibe autorización de utilizar dichos derechos

(licenciatario) a cambio de un pago de antemano (tasa o regalía), aunque también puede tener el carácter de gratuito". Para hacer realidad la necesidades de compartir, se han desarrollado herramientas jurídicas que benefician a los Autores pero también a los usuarios. Estas herramientas continúan creciendo en popularidad y en sus efectos. Los instrumentos mas utilizados para liberar obras en general son:

Creative Commons es una organización sin fines de lucro que permite usar y compartir tanto la creatividad como el conocimiento a través de una serie de instrumentos jurídicos de carácter gratuito. Dichos instrumentos jurídicos consisten en un conjunto de "modelos de contratos de licenciamiento" o licencias de derechos de autor que ofrecen al autor de una obra una manera simple y estandarizada de otorgar permiso al público y en general de compartir y usar su trabajo creativo bajo los términos y condiciones de su elección. En este sentido, las licencias Creative Commons permiten al autor cambiar fácilmente los términos y condiciones de derechos de autor de su obra de "todos los derechos reservados" a "algunos derechos reservados". El servicio prestado por Creative Commons Argentina cuenta con herramientas legales estandarizadas que se denominan "licencias", permitiendo que en una obra determinada se reserven todos los derechos, sólo algunos o se liberen todos ellos.

Otro sistema internacional de gestión y cesión de los derechos autorales es ColorIuris, que tiene validez mundial y con efectos legales de registro en 25 países entre ellos Argentina. Funciona mediante un contrato de cesión que celebran las partes, donde el primero le transfiere todo o parte del derecho sobre una obra o creación objeto del contrato, contando el titular de la misma con herramientas jurídicas que puede hacerlas valer en contra del cesionario en caso de una indebida utilización del contenido objeto de la cesión. Se prevé, a los fines de garantizar mayor seguridad e imparcialidad, la existencia de una tercera persona, que puede ser una entidad pública o privada, que tiene a su cargo la custodia y guarda de la copia de los contratos y tiene la obligación emitir, si se

solicita, el certificado con indicación de la fecha y hora de la celebración del contrato.

En cuanto al licenciamiento del Software libre, el principal instrumento utilizado es la Licencia Pública General de GNU (o simplemente sus siglas del inglés GNU GPL) y garantiza a los usuarios finales la libertad de usar, estudiar, compartir (copiar) y modificar el software. Su propósito es declarar que el software cubierto por esta licencia es software libre y protegerlo de intentos de apropiación que restrinjan esas libertades a los usuarios. Esta es la primera licencia copyleft para uso general, lo que significa que los trabajos derivados sólo pueden ser distribuidos bajo los términos de la misma licencia. La GPL puede ser usada por cualquiera, ya que su finalidad es proteger los derechos de los usuarios finales (usar, compartir, estudiar y modificar), y otorgar a los beneficiarios de un programa de ordenador de los derechos de la definición de software libre. La GPL, al ser un documento que cede ciertos derechos al usuario, asume la forma de un contrato, por lo que usualmente se la denomina contrato de licencia. Sus términos y condiciones deben estar disponible para cualquiera que reciba una copia de la obra al cual ha sido aplicada esta licencia. Con esta licencia, está permitido cobrar por la distribución de cada copia, o no cobrar nada.

Software Libre significa que el Código fuente se encuentra disponible, es decir, que cualquiera de los usuarios puede ingresar a las lineas de programación para entenderlas y si es su deseo, modificarlas. Siempre que el código compilado esté disponible y que haya "instrucciones claras" sobre dónde encontrar el código fuente la cláusula se considera cumplida. Se ha masificado tanto la existencia de códigos abiertos que hay discrepancias dentro de la comunidad de desarrolladores, por ejemplo, La Free Software Foundation tiene una diferencia filosófica con el Open Source Software, la diferencia entre estos dos perspectivas del Software Libre es su abordaje, mientras que la FSF tiene motivos éticos y morales para el licenciamiento de las obras creativas, sosteniendo el ideal de la libre circulación de la información, el código abierto apunta a aquellos beneficios que se derivan del desarrollo comunitario de este tipo de tecnología, es decir, que sostienen una postura meramente técnica, sin detenerse en sus aristas filosóficas. Por otro lado, el código abierto resguarda sobre todas las cosas la disponibilidad de acceder al código fuente, mientras que para que un software sea considerado libre, debe respetar las cuatro libertades promulgadas por la FSF. Estas son la libertad de usarlo, de tener acceso al código para estudiarlo y adaptarlo, de redistribuir copias y la libertad de mejorarlo. Se añade ademas de estas libertades, la restricción de que cualquier obra derivada de un Software libre debe respetar estas libertadores, y es entonces cuando con efecto multiplicador, el nuevo programa de computación con su respectivos formatos de código, es publicado bajo la misma licencia. En definitiva, siempre que el código fuente se encuentre disponible para su uso libre estaremos frente a valores morales y técnicos dignos de protección. La gran mayoría de nuestra actividad es alojado en servidores que utilizan códigos abiertos, también Google, Twitter, Facebook, Amazon, la NASA, la supercomputadora mas poderosa del mundo, los ejércitos, la casa Blanca, el FBI, y la mayoría de los países alrededor del mundo lo utilizan.

Por otro lado, el software libre dejó de ser cosa de locos de la programación en el momento en que las empresas se percataron de que contratar licencias millonarias de software a Oracle o a Microsoft

reforzaba el gasto y aumentaba su dependencia de esas compañías. Esta tecnología ha elevado su implantación empresarial. Es algo real y sostenible. En la web Linux.com, Brian Proffitt ha hecho público un estudio de implantación de software libre en empresas de todo el mundo y según los datos recogidos Europa es el continente con la adopción más completa con países como Francia con un 67% de los usuarios que admiten utilizar software libre, un 60,6% en Alemania (gracias sobre todo a empresas como SUSE), y un 41% en el Reino Unido. En EEUU, la adopción es del 56% mientras que en China es del 72,6%. El principal motivo por el que muchas empresas eligen software libre es por su bajo coste. Existe todo un mercado alrededor del software libre, empresas que ofrecen soporte, comunidades de desarrollo y, lo más importante, casos de éxito en empresas y administraciones públicas, estas son la bandera que definen software libre como algo real.

La consultora argentina (Re)ingenia ha hecho público un decálogo llamado “10 Razones para usar Software Libre en la empresa”. El Software Libre y de código abierto (FOSS, por sus siglas en inglés) tiene muchas otras ventajas convincentes para las empresas, particularmente las pymes:

1. Seguridad: los problemas de seguridad en el caso de Software Libre se resuelven en cuestión de horas. En cambio, en el mundo del software propietario, los parches de seguridad tardan considerablemente más en resolverse.

2. Calidad. un estudio reciente elaborado por la Linux Foundation ha demostrado que la superioridad técnica suele ser la razón principal por la que las empresas eligen el software de código abierto.

3. Personalización. Dado que el código es abierto, es simplemente una cuestión de modificarlo para añadir la funcionalidad que se desee.

4. Libertad. Cuando las empresas recurren al Software Libre, se liberan de las restricciones que impone el proveedor de software.

5. Flexibilidad. Cuando la empresa utiliza software propietario, entra en un proceso que requiere mantener la actualización de software y hardware hasta el infinito.

6. Formatos abiertos: Interoperabilidad. El software de código abierto es mucho mejor en la adhesión a los estándares abiertos que el software propietario.

7. Posibilidad de “auditar” el código. Con el software de código cerrado lo único que asegura la calidad y confiabilidad del software es la palabra de la empresa o del vendedor.

8. Opciones de Soporte. Para empresas que desean una garantía adicional, es posible contratar (a precios muy competitivos) equipos de soporte profesionales para la mayor parte de los sistemas de código abierto.

9. Costo. Entre el precio de compra del software en sí, el costo exorbitante de protección contra virus, los gastos de soporte, los gastos de actualización, los gastos asociados con estar bloqueado… el software propietario cuesta más al empresario de lo que él probablemente sepa.

10. Probar antes de comprar. Si el empresario está considerando el uso de software de código abierto, no le costará nada probarlo primero.

Existe en cada país ademas, el desafío de impulsar la soberanía tecnología y de mejorar la seguridad informática. Estas cuestiones encuentran una gran ventaja en este tipo de tecnología, ya que el Estado en cualquiera de sus niveles puede desarrollar soluciones eficientes, asegurándose la libertad de mejorar estos sistemas cuando sea necesario a un menor costo. El razonamiento economicista tiene un peso muy importante en las decisiones sobre compras públicas, el uso privilegiado o exclusivo de software libre en Administraciones Públicas ha sido sustentado en argumentos de tipo cuantitativo, en términos del ahorro que supone en el mediano plazo. En este sentido, es importante recordar que se ha calculado que el software libre o de código abierto ha supuesto un ahorro para la economía de la Unión Europea de, al menos, ciento catorce millones de euros al año (Daffara et al., 2013).

Con respecto a la confidencialidad de la información privada, esta no puede garantizarse como Acto Público sin la posibilidad de analizar el funcionamiento de los sistemas que la manipulan. Vuelve a hacerse presente aquí la necesidad de contar con el código fuente de los programas y el derecho a realizar su inspección. Las prácticas del software libre han creado también prototipos de dispositivos democratizantes, tanto respecto a una actividad económica concreta, como a la propia práctica de la política y de la actividad de Gobierno.

De hecho, si revisamos la decisión favorable a su uso en las Administraciones Públicas, es evidente que dicha decisión, además de los económicos, también se encuentra fundamentada en argumentos de carácter político e, incluso, ontológico, relativos a la activación de movimientos sociales y a la conquista de la independencia y la liberación. Con el apoyo público que ahora se destina a la adquisición de soluciones de software privativo, estos criterios podrían florecer como una industria del conocimiento con externalidades positivas y sostenibles en el tiempo.

En conclusión, existen variados argumentos que indican las ventajas en la inversión en tecnología libre, ademas de contar con herramientas jurídicas que permiten el crecimiento de una comunidad cada vez mas involucrada. Las decisiones que se adoptan en la Administración Publica son por demás relevantes ya que deben guiar a la Sociedad en su conjunto. En su fin pedagógico, el Estado debe introducir la programación en las escuelas, con el fin de preparar las futuras generaciones para responder con criterio desde un abordaje multisectorial, en palabras de David Rushkoff “en el emergente escenario futuro de masiva programación, o creas el Software, o eres el Software”. El software libre ya se encuentra presente en todos los ámbitos imaginables, desde hospitales a bases militares, universidades, empresas, asociaciones civiles o el internet que habitualmente utilizamos. La oposición existente entre licencias privativas y libres es meramente una expresión de la transición en la que nos encontramos, que tendrá como resultado una Sociedad de la Información competitiva y sobre capacitada. En el

futuro, enfrentaremos enormes dificultades a nivel global, el calentamiento global, la super población, la vigilancia como política de Estado e incluso el manejo de la inteligencia artificial. Aumentar entonces el nivel de conciencia es una preparación impostergable, facilitando la comunión entre los diferentes sectores económicos para que inviertan en la actualización que necesariamente deben realizar. Desde otro punto de vista, los Poderes Públicos deben reconocer la Nueva Realidad para continuar siendo relevantes. Si el Estado no busca crear puentes y achicar la brecha digital, se vera rezagado no solo a participar desde un rol secundario en la comunidad internacional, si no que vera disminuida su influencia en la gente, al no poder utilizar su mismo lenguaje. Luego de abordados los conceptos up supra, concluimos que la información necesaria para la implementación política de sistemas abiertos se encuentra disponible, así, esperamos que actores sociales tan importantes como empresarios y funcionarios políticos se encuentren a la altura del desafío.

Autor: Franco Giandina

De las formas de controlar la adecuada protección de los datos personales: El principio de Responsabilidad Demostrada (Accountability).

La Delegatura para la Protección de Datos Personales de la Superintendencia de Industria y Comercio de Colombia tiene una forma de ejercer el control sobre los datos personales con rasgos específicos, que se aplican desde 2015, época en que se realizó el lanzamiento de las Guías para la Implementación del Principio de Responsabilidad Demostrada (Accountability).

-I- ¿Qué es el principio de Responsabilidad Demostrada (Accountability)?

El principio de Accountability establece que toda entidad que recolecta y trata datos personales debe responsabilizarse por el cumplimiento efectivo de las medidas que implementen los principios de privacidad y protección de datos.

Son sus antecedentes normativos las Guías sobre Protección de la Privacidad y los Flujos Transfronterizos de Información de OCDE[1], que fueron actualizadas en 2013. En sus orígenes, el trabajo previo a la presente Guía fue llevado a cabo por la Oficina del Comisionado de Privacidad de Canadá, la Oficina del Comisionado de Privacidad e Información de Alberta y los Comisionados de Privacidad e Información de Columbia Británica[2] y complementado en el sector privado[3] [4].

-II- ¿Qué importancia tienen las guías para su implementación?

Conforme dichas Guías, todo responsable del tratamiento del dato debe contar con un programa integral de gestión de datos y, además, debe estar preparado para demostrar a la autoridad pertinente cómo implementa efectivamente dichas medidas en su organización.

Numerosos instrumentos jurídicos han incluido este concepto. Entre ellos cabe mencionar la Personal Information Protection and Electronic Documents Act (PIPEDA) de Canadá, la Directiva 95/46/CE, las Cross Border Privacy Rules (CBPR) de APEC, el procedimiento de “Safe Harbor” vigente entre Estados Unidos y la Unión Europea, los estándares de Madrid de 2009.

---

[1] http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#comments

[2] Ver https://www.priv.gc.ca/information/guide/2012/gl_acc_201204_e.pdf

[3] Centre for Information Policy Leadership (Secretariat) “The accountability project. The essential elements of accountability.”, 2009

[4] Nymity Privacy Management Accountability Framework. Toronto, Canadá, 2014.

En Colombia, la ley N° 1581 de 2012 y el Decreto N° 1377 de 2013, implementan este sistema de accountability, al que denominan Responsabilidad Demostrada, que marca estándares que se traducen en una mayor y más adecuada protección de los datos personales de los individuos. Se establece que el Responsable del Tratamiento de los datos tiene la obligación de demostrar que se han implementado medidas apropiadas y efectivas para cumplir con las especificidades de la ley colombiana. Además de la asignación de responsabilidades para el responsable del tratamiento, se privilegia la gestión de los riesgos.

La relevancia de esta Guía está dada porque trae implícito que la autoridad de control de protección de datos realiza un reconocimiento expreso a aquellas organizaciones que le puedan demostrar que una eventual falla en el tratamiento de la información de un titular corresponde a una situación aislada que se ha dado en el marco de un Programa Integral de Gestión de Datos Personales. Esto implica que cuando se opera una irregularidad en la protección de los datos, ante una inspección de la Autoridad de Control, el hecho de que la organización inspeccionada pruebe que tiene puesto en marcha un Programa Integral de Gestión de Datos Personales es un indicador trascendente de que tal incidente es un hecho aislado.

-III- ¿Cuáles son los fundamentos básicos para el desarrollo de un Programa Integral de Gestión de Datos Personales?

Se parte de la base de que las empresas adoptan políticas internas efectivas que fueron aprobadas en el decurso de un proceso realizado con la diligencia debida en el ámbito interno de una organización. El tratamiento del dato, por tanto, debe garantizar la existencia de una estructura administrativa para implementar las políticas de la ley de protección de datos, que sea proporcional a la estructura y al tamaño de la empresa, así como que existan mecanismos internos de implementación de las

herramientas de protección de datos, cursos de entrenamiento, programas de educación, y procesos para la atención de consultas, peticiones y reclamos que refieran al tratamiento de datos personales.

El programa integral de gestión de datos personales implica un compromiso de la organización en su totalidad a la adopción de políticas y procedimientos para cumplir con lo que indican las normas, y trae aparejada la implementación del programa, comprometiendo recursos económicos y materiales al efecto.

Este proceso debe comenzar desde los cargos jerárquicos más importantes de la empresa. Esto demuestra su apoyo y compromiso para generar el respeto a la protección de datos personales. Tiene su eje en una persona que asumirá la función de responsable o encargado de los datos personales dentro de la organización, implementará el sistema a efecto, supervisará los entrenamientos correspondientes, revisará que las trasmisiones internacionales de datos se hagan conforme a la ley y se ocupará del seguimiento y la auditoría de todo el

sistema, presentando los informes correspondientes ante violaciones a la seguridad o riesgos relacionados con los datos personales.

Es necesario generar políticas internas que dispongan obligaciones relacionadas con la protección de datos personales y que deben ser dadas a conocer a los empleados. Estas políticas deben establecer reglas sobre recolección, almacenamiento, uso, circulación, supresión, disposición final de la información personal; acceso, corrección, conservación y eliminación de datos personales; uso responsable de la información; controles de seguridad; inclusión de una cláusula de confidencialidad en todos los medios contractuales; presentación de quejas, denuncias y reclamos; en general, todo aquel elemento necesario para cumplir con la normativa sobre protección de datos personales.

-IV-¿Cómo se controla el Programa?

En tal sentido, las políticas generales de la empresa deben transparentarse en sus procedimientos administrativos y debe haber un adecuado manejo de los riesgos que se relacionan con el tratamiento de los datos personales. Para ello es necesario que exista un previo inventario de las bases de datos que contienen información personal y que existan políticas internas dentro de las organizaciones que dispongan obligaciones al respecto que sean adecuadamente dadas a conocer a todos los empleados. Estas reglamentaciones internas abarcarán temas como la recolección, almacenamiento, uso, circulación y supresión, conservación y eliminación de los datos personales, el acceso y la corrección de dichos datos, el uso responsable de los mismos, los controles de seguridad legales, físicos, administrativos y tecnológicos, la presentación de reclamos, etcétera.

Un programa efectivo de protección de datos debe ser comprensivo de políticas que se encuentren en consonancia con los ciclos internos de protección de datos dentro de la empresa y, a su vez, que generen resultados medibles que permitan probar el grado de diligencia.

-V- ¿Cómo se realiza la evaluación y revisión del Programa?

Tan importante como el desarrollo del Programa Integral de Protección de Datos Personales es su implementación, manteniendo su eficacia, el cumplimiento del programa y los estándares de Responsabilidad Demostrada. De ahí que se otorgue fundamental importancia al desarrollo de un plan de supervisión y revisión, que está a cargo del Oficial de Protección de Datos y debe establecer las medidas de desempeño y los controles necesarios para medirlo.

Asimismo, dicho plan de supervisión y revisión debe ser constantemente evaluado y supervisado teniendo en cuenta riesgos y amenazas al tratamiento de datos personales, las quejas más recientemente recibidas, la protección de datos personales en los servicios que se van incorporando, el grado de eficacia de la capacitación, el grado de actualización del programa.

-VI- ¿Cómo se demuestra el cumplimiento con el Plan?

Un factor importante para tener en cuenta en caso de que la autoridad realice una actuación administrativa es el de acreditar que se ha adoptado un Programa Integral de Gestión de Datos Personales y que el mismo está siendo aplicado con la diligencia debida. La demostración de la implementación del Programa es un elemento fundamental que tendrá en cuenta la autoridad de

el principio de transparencia hacia los titulares del dato, lo cual contribuye a generar confianza en el mercado.

-VII-

Colofón

La República de Colombia, con el lanzamiento en 2015 de las Guías para la Implementación del Principio de Responsabilidad Demostrada (Accountability) asume una postura interesante que propicia formas responsables y novedosas en Iberoamérica para proteger adecuadamente los datos personales dentro de las organizaciones. Siguiendo los estándares internacionalmente consensuados en la materia, propone una forma responsable de propender hacia la adecuada protección de los datos.

Ana Brian Nougrères. / Uruguay.

GOBIERNO

&

CUMPLIMIENTO

RESPONSABLE

ING FABIÁN DESCALZO

Respuestas al cumplimiento ¿Cada vez más complejas?

Las regulaciones globales y locales están creciendo en volumen y en complejidad, y como resultado, la demanda de responsabilidad legal se ha intensificado, a la vez que la administración de los costos asociados a la gestión de riesgo y cumplimiento continúa siendo un reto.

¿Debe la estrategia de cumplimiento de una empresa ser parte de la estrategia de seguridad? ¿Debe ser independiente o estar más cerca del área legal? ¿Cómo elige mejorar el cumplimiento en su empresa? En una organización la gestión de cumplimiento puede tornarse compleja y difícil de realizar, no solo por razones técnicas sino también por razones organizativas y funcionales. Coordinar todos los esfuerzos encaminados a asegurar un entorno de cumplimiento corporativo requiere de un adecuado control que integre los esfuerzos de toda la organización, empleando mecanismos reguladores de las funciones y actividades desarrolladas por cada uno de sus empleados.

Por ello deben establecerse pautas para la integración de capacidades de gobierno, aseguramiento y gestión del desempeño, riesgo y cumplimiento que integren estos esfuerzos de una manera conjunta, y que luego se representarán a través de las políticas y normas organizacionales, que formaran un marco normativo como medio de comunicación en el cual se establecen las reglas y controles reflejados en los diferentes procedimientos de la organización, para asegurar el cumplimiento de leyes y regulaciones del negocio apoyando a la confidencialidad, integridad y disponibilidad de la información previniendo y manejando los riesgos de seguridad en diversas circunstancias. Tengamos en cuenta que las pautas establecidas deben representarse en un programa que defina el objetivo, dirección, principios y reglas básicas para la gestión del cumplimiento y la seguridad.

En el mundo actual, no hay forma de asegurarnos contra el robo o el fraude si no podemos controlar o gobernar los procesos de negocio desde la tecnología que les brinda servicios y a su vez, si no capacitamos y concientizamos a las personas que los gestionan. Toda persona que intervenga en los diferentes procesos de negocio y a su vez utilice los servicios informáticos que ofrece la organización, debe conocer el marco normativo que regula las actividades de la organización, teniendo en cuenta que su desconocimiento no lo exonera de responsabilidad, ante cualquier eventualidad que involucre a la organización y a la seguridad de la información.

El objetivo de un programa de cumplimiento es el crear una mejor imagen de mercado y reducir los daños tangibles o intangibles ocasionados por los potenciales riesgos; esto determina que las necesidades de cumplimiento se centren en dar respuesta a la gestión riesgos, el control de los procesos y el control de accesos a la información y a los sistemas, siendo cada una de estos puntos módulos fundamentales para el entorno de GRC (Governance, Risk & Compliance) de cualquier organización, y el medio para dar respuesta puede ser representado, por ejemplo, a través de la gestión de seguridad de la información alineada con los objetivos comerciales de la organización para asegurar su negocio.

Tomando como guía este sistema de gestión, se tiene la posibilidad de cubrir una respuesta tanto a requerimientos legales o de industria (SOX, PCI-DSS, LFPDP, BCRA, SBIF, SBS, etc.) como el demostrar la adopción de prácticas comunes desde la visión de seguridad de la información (ISO9001, ISO27001, ITIL, COBIT, ISO20000, etc.) y las prácticas internas o la interacción con diferentes funciones y terceros. Los retos de cumplimiento han llevado a un incremento del espectro de responsabilidades, que abarcan aspectos relacionados con la administración de riesgos, la administración de cumplimiento y seguridad de la información, continuidad del negocio y la protección de datos.

Este incremento de responsabilidades ha llevado a lo largo del tiempo a integrar dentro de las organizaciones áreas específicas para su gestión, siendo el CSO o CISO (Chief Security Officer o Chief Information Security Officer) el responsable de supervisar el cumplimiento de los objetivos del sistema de gestión de seguridad y, al mismo tiempo, de establecer nuevas metas.

Debemos tener en cuenta que, para una buena comprensión de las pautas establecidas por la organización, la normativa debe ser organizada de manera sencilla para que pueda ser interpretada por cualquier persona que ostente un cargo de empleado o terceros con un contrato de trabajo por servicios en la organización, con conocimientos informáticos o sin ellos. Las políticas deben ser creadas según el contexto de aplicación, organizadas por niveles de seguridad y siguiendo un entorno de desarrollo, sobre la problemática de la compañía o previniendo futuras rupturas en la seguridad y el cumplimiento, aplicada sobre sus diferentes recursos o activos de información.

Dentro de la práctica de la seguridad de la información, los objetivos para controles individuales de seguridad o grupos de controles deben ser propuestos por el Comité de Seguridad y aprobados por la Dirección en la declaración de aplicabilidad; los cuales son revisados al menos una vez al año. El Comité de Seguridad de la Información debe estar destinado a garantizar el apoyo manifiesto de la Dirección a las iniciativas de seguridad, siendo sus principales funciones:

1. Revisar y proponer a la Dirección para su consideración y posterior aprobación, las políticas de seguridad de la información y las funciones generales en materia de seguridad de la información que fueran convenientes y apropiadas para la organización.
2. Monitorear cambios significativos en los riesgos que afectan a los recursos de la información de la organización frente a posibles amenazas, sean internas o externas.
3. Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes, relativos a la seguridad, que se produzcan en el ámbito de la organización.
4. Aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada sector, así como acordar y aprobar metodologías y procesos específicos relativos a la seguridad de la información
5. Evaluar y coordinar la implementación de controles específicos de seguridad de la información para los sistemas o servicios de esta organización, sean preexistente o nuevos.
6. Promover la difusión y apoyo a la seguridad de la información dentro de la organización, como así coordinar el proceso de administración de la continuidad del negocio.

Teniendo en cuenta las necesidades de cumplimiento, el programa definido para la gestión de la seguridad de la información, debe tomar como lineamientos principales cuatro dominios relacionados con el Gobierno Corporativo:

- **Seguridad Organizacional**
  Estableciendo el marco formal de seguridad que debe sustentar la organización, incluyendo servicios o contrataciones externas a la infraestructura de seguridad, Integrando el recurso humano con la tecnología, denotando responsabilidades y actividades complementarias como respuesta ante situaciones anómalas a la seguridad.

- **Seguridad Lógica**
  Estableciendo e integrando los mecanismos y procedimientos, que permitan monitorear el acceso a los activos de información, que incluyen los procedimientos de administración de usuarios, definición de responsabilidades, perfiles de seguridad, control de acceso a las aplicaciones y documentación sobre sistemas, que van desde el control de cambios en la configuración de los equipos, manejo de incidentes, selección y aceptación de sistemas, hasta el control de software malicioso.

- **Seguridad Física**
  Identificando los límites mínimos que se deben cumplir en cuanto a perímetros de seguridad, de forma que se puedan establecer controles en el manejo de equipos, transferencia de información y control de los accesos a las distintas áreas con base en la importancia de los activos.

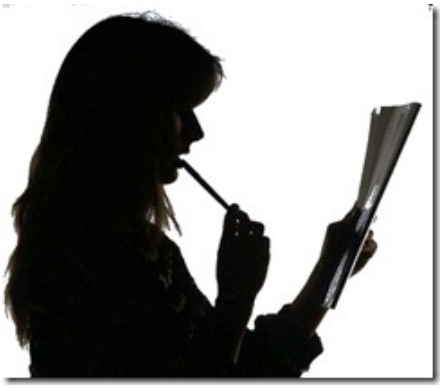
- **Seguridad Legal**
  Integrando los requerimientos de seguridad que deben cumplir todos los empleados, socios y terceros que interactúan en procesos de negocio y la información de la compañía,

bajo la reglamentación de la normativa interna de políticas y manuales de procedimientos de la organización en cuanto al recurso humano, sanciones aplicables ante faltas cometidas, así como cuestiones relacionadas con la legislación del país y contrataciones externas.

Para la práctica de estos cuatro dominios, y según lo mencionamos en párrafos anteriores, se debe establecer una metodología para determinar el proceso para la administración de riesgos, asegurando cubrir las siguientes etapas que llevan a completar su tratamiento:

- Identificación de los procesos de Negocio y servicios de TI y seguridad que lo soportan
- Identificación de riesgos de Negocio y servicios de TI y SI que lo soportan
- Análisis de riesgos de Negocio y servicios de TI y SI que lo soportan
- Evaluación de riesgos de Negocio y servicios de TI y SI que lo soportan
- Tratamiento de riesgos de Negocio y servicios de TI y SI que lo soportan
- Documentación, control y revisión

Los diferentes riesgos al cumplimiento deben ser evaluados sobre cada conjunto de actividades o procesos definidos, teniendo en cuenta su interrelación de forma ordenada y consecutiva para identificar los factores de riesgo que puedan involucrar a una o más unidades de negocio. Estos factores de riesgo pueden involucrar aspectos de cumplimiento al producirse un evento determinado que influya negativamente en el normal funcionamiento y operación de los procesos de TI de la organización, afectando de esta forma tanto a la privacidad o disponibilidad de datos como a la integridad que puede conllevar a hechos delictivos, ya sea por robo o fraudes. La organización debe considerar dentro de la definición de Riesgos de TI aquellos eventos relacionados con los sistemas de información y con la infraestructura de TI propia y de terceros que soporta el funcionamiento de dichos sistemas, y con cualquier otro recurso relacionado empleado por la función de TI de la organización para brindar sus servicios. De la misma forma, deben tenerse en cuenta los riesgos resultantes de la falta de adecuación o fallas en los procesos internos, de la actuación del personal o bien de aquellos que sean producto de eventos externos.



La organización debe considerar estos riesgos como componentes importantes a tener en cuenta en su programa de cumplimiento. Por lo tanto, independientemente de las normas y procedimientos específicos para la administración de riesgos, se debe aplicar un esquema en el cual las salidas del proceso de administración de riesgos se integren con el conjunto de la documentación de los procesos de negocio, con el fin de poder disponer de documentación acerca del perfil de riesgos operativos que enfrenta la organización en forma integrada y completa. El enfoque utilizado para identificar riesgos y factores debe incluir, entre otros, lo siguiente:

- Juicios basados en la experiencia y conocimiento de la organización y de los procesos y funciones de TI con los cuales está involucrado
- Observaciones formuladas en informes de Auditoría Interna, Auditoría Externa, y otras auditorías a las que esté sometida la organización.
- Resultados de estudios de vulnerabilidad llevados a cabo por la organización, ya sea en forma interna como mediante la contratación de terceros especializados.
- Conocimiento de incidentes registrados en el área, conocimiento de incidentes ocurridos en otras organizaciones del sector, aporte de las áreas usuarias
- Nuevos proyectos encarados por la organización, mediante los cuales se afecte a procesos de negocio o a la infraestructura de TI, los sistemas de información, o cualquier recurso relacionado.
- Cambios organizacionales, tales como reestructuración de áreas tecnológicas o funcionales, o la tercerización de actividades vinculadas con la administración y/o procesamiento de los sistemas de información o cualquier tipo de tratamiento de información de la organización.
- Clasificación de activos: En la clasificación de activos de información se define la criticidad de los activos en base a su disponibilidad, confidencialidad e integridad. Esta información es de gran utilidad a la hora de identificar riesgos de cumplimiento en relación a los activos críticos.

Adicionalmente a esto, las áreas de legales de las organizaciones, deben estar en conocimiento no solo de las actualizaciones legislativas y regulatorias, sino también de las necesidades de gobierno sobre las tecnologías actuales y nuevas que pueden influir negativamente en el cumplimiento de las organizaciones. Las áreas tecnológicas, de seguridad y riesgos deben conformarse como un núcleo consultivo que, en conjunto con las áreas legales y de control interno, permitan establecer un blindaje equilibrado a las organizaciones. Revise cualquier industria y encontrará que su entorno regulador se encuentra en un proceso constante de cambio, provocando alertas de cumplimiento a las cuales debe darse respuesta constante y en línea.

Establecer controles e identificar riesgos nos permite determinar un seguimiento de las actividades más importantes dentro del programa de cumplimiento que son relevantes para cada función en la organización, y obtener datos procesables con los que se pueden medir y remediar las brechas rápidamente y de manera eficiente. Tener estos datos significativos a su alcance no sólo ayuda a comprender el nivel actual de madurez de cumplimiento, sino que también ayuda a tomar decisiones acerca de la priorización para su tratamiento. Es necesario que establezca una metodología de medición en función de datos que representen el nivel de cumplimiento interno, representados en un proceso que refleje en forma periódica el alineamiento a las políticas internas de la organización y sus desvíos.

También puede hacerse mediante encuestas internas a usuarios finales, con preguntas referentes a puntos vitales de las normas, para evaluar el nivel de conocimiento como instancia previa a evaluar el cumplimiento en los procesos. Respecto de los indicadores, los mismos deben ser dinámicos en función de nuevas regulaciones o cambios en los procesos (lo que los hacen variables en el tiempo); además que también se pueden establecer distintos niveles de indicadores en función del nivel de madurez de la organización, lo que también hace que puedan variar en el tiempo teniendo en cuenta el crecimiento futuro en el nivel de cumplimiento de la misma.

Conclusión: Adopte una guía que responda a sus necesidades de cumplimiento, y desde el conocimiento de sus procesos no solo identifique aspectos legales o regulatorios, sino que también contemple los diferentes procesos secundarios o de servicios que pueden afectar al cumplimiento en los procesos principales, como por ejemplo la tecnología y la seguridad de la información.

FABIAN DESCALZO: fabiandescalzo@yahoo.com.ar

Gerente de Servicios y Soluciones en el área de Gobierno, Riesgo y Cumplimiento (GRC) en Cybsec by Deloitte, con amplia experiencia en la implementación y cumplimiento de Leyes y Normativas Nacionales e Internacionales en compañías de primer nivel de diferentes áreas de negocio en la optimización y cumplimiento de la seguridad en sistemas de información, Gobierno de Seguridad de la Información y Tecnologías de la Información..

Es certificado en Dirección de Seguridad de la Información (Universidad CAECE), IRCA ISMS Auditor, Lead Auditor ISO/IEC 27001, instructor certificado ITIL Fundation v3-2011 (EXIN) y auditor ISO 20000 (LSQA-Latu), profesor del módulo 27001 del curso de “TI Governance, Uso eficiente de Frameworks”, y de la “Diplomatura en Gobierno y Gestión de Servicios de TI” del Instituto Tecnológico Buenos Aires (ITBA), profesor en Sistemas de Gestión TI y Seguridad de la Información para entidades certificadoras y Auditor ISO 20000 / ISO 27001 para TÜV Rheinland Argentina.

Columnista especializado en áreas de Gobierno, Seguridad y Auditoría, Informática en Salud y Compliance en las revistas CISALUD, PERCEPCIONES (ISACA Montevideo Chapter), El Derecho Informático, CXO-Community y MAGAZCITUM; y disertante para CXO-COMMUNITY, Consejo Profesional de Ciencias Informáticas, ISACA Buenos Aires Chapter, ISACA Montevideo Chapter.

Miembro del Comité Académico E-GISART de ISACA Buenos Aires Chapter, del Comité Directivo del “Cyber Security for Critical Assets LATAM Summit” para Qatalys Global sección Infraestructura Crítica (Gobiernos y empresas de América Latina en el sector de la energía, química, petróleo y gas), del Comité Científico ARGENCON del IEEE (Institute of Electrical and Electronics Engineers), y del Comité Organizador CYBERSECURITY de ISACA Buenos Aires Chapter.


TE DESEAMOS UN
FELIZ
2017
LA RED EDI
ESTAMOS DONDE ESTAS VOS
ELDERECHOINFORMATICO.COM

Qué nos deja el 2016....

Autora: Marina Benitez Demtschenko

Corresponsal por Argentina de la Red EDI

Una agenda política dispersa, desentendida de cuestiones relacionadas con la ciberseguridad y el derecho informático. Varios eventos novedosos (Ekoparty en la Ciudad Autónoma de Buenos Aires; el "Campus Party" en Tecnopolis, Buenos Aires; el CIIS-16 ("1er Congreso sobre Ciudades Inteligentes, Innovaciones Tecnológicas y Sustentabilidad"), en Córdoba; el InfoSecurity Tour 2016 en Buenos Aires, y otros), pero como si fuesen aún una realidad paralela y externa en la que nuestro país no recaba: políticas públicas que desentonan, algunas que retrasan y otras que muestran que Argentina dista de estar a la altura de regiones y Estados con *ciber-conciencia*. La ley en torno a la recepción de avances tecnológicos y problemáticas en torno a las conductas dañosas online existentes, permanece inocua, desde hace digamos…unos cuantos años. Cada vez que hablo de la necesidad de legislar sobre ciberdelitos que en son moneda corriente en gran parte del mundo y que ya tienen acogida legal suficiente y creciente, (mientras aca los vemos ocurrir en total impunidad), me preguntan: "Y qué obsta, doctora, a que se sancionen leyes sobre esto?"…Mi única respuesta es: desinterés y desconocimiento.-

Hemos visto el debate ocurrido en torno a la reforma electoral para el ciclo 2017 y la batahola de intercambios contrapuestos entre legisladores y gestión actual, contra especialistas en informática y abogados por la implementación del voto electrónico. Tanto insumió a nivel político e intelectual de nuestros representantes que parece que no pudieron abocarse a otras cuestiones vinculadas con la ciberseguridad y el cibercrimen. La ley y las alternativas al voto electrónico finalmente se suspendieron en el tratamiento del Congreso.-

Una reforma vociferada y puesta en el refrigerador de proyectos "dificultosos" fue la de reforma a la ley de Grooming, que a principio de año fue puesta en conocimiento popular con bombos y platillos y luego se esfumó al notarse que no era unívoca la visión ni técnica ni conceptual del planteo para su modificación. Otra suerte corrió el proyecto presentado a mitad de año en el Senado para la tipificación de la mal llamada "pornovenganza" y bien llamada "difusión no consentida de imágenes íntimas", que fue aprobada casi por

trámite en dicho Recinto y que espera su encarnizado debate al llegar a Diputados, donde hay varios proyectos sobre la problemática y acá sí me detengo por ser mi metiére: ninguno con perspectiva de género; todos con nimios y vagos términos; la mayoría conteniendo una pena que da risa (incluso algunos con pena de multa: arruinás la vida entera de una persona pero podés vender el auto y seguir tu camino sin mayor poder punitivo por parte del Estado), y lo que es peor, ninguno contemplando la cantidad de variantes que supone dicha conducta: sin agravantes, sin especificaciones, sin estudio técnico, sin consulta a especialistas.- De más está decir que sancionar por sancionar, es un habitual estilo en nuestro Congreso, y que la puja que generan los especialistas y los sectores ajenos al poder público estatal (ejemplo: ONGs), no gusta, para nada, es más, se intenta correr del medio y tapar con medios periodísticos amansados al interés de la bandera que los costee, y siempre será así hasta que los funcionarios no resistan más al conocimiento y el tecnicismo de los que sabemos en serio y proponemos desde la óptica del bien común, del derecho efectivo, del poder publico en manos de quienes no usamos corbata.-

En lo que va del año que ya termina, nos encontramos con un país que poco dio a su comunidad digital. El ingreso de Uber también quedó en el éter de los temas sin debatir ni regularizar; cuestiones de e-commerce y plataformas extranjeras ofreciendo servicios por Internet a muy ventajosos costos para los usuarios, fueron rápidamente frenados (aerolíneas, hospedajes turísticos, importaciones). Otro hito no-tan-hito, es que se dio a conocer el primer informe estadístico de los delitos informáticos denunciados en nuestro país, a cargo del Ministerio de Justicia y Derechos Humanos de Nación. Un interesantísimo documento, esbozado por profesionales de renombre pero resultado de un relevo del año 2013… sí, publicado ahora -tres años después-, donde dichos índices perdieron toda capacidad de reflejo de la actualidad: una muestra más del retraso de nuestro país en la respuesta frente a la demanda sobre la materia…no?

Y cierro esta columna haciendo hincapié en la necesidad –dejada de lado negligentemente-, de legislación y políticas públicas que recepten a los nuevos tipos penales que si bien no son incipientes, resultan exigidos por la comunidad digital al punto que, habiendo realizado una encuesta (muy amateur, aunque bastante representativa del contexto geográfico, social y económico del usuario promedio en Argentina/ No así en edad, ya que respondieron personas de variadas franjas etarias) a través de las redes sociales Facebook y Twitter durante el mes de Noviembre de este año 2016, surgieron resultados llamativos, al menos para mí, que me considero una aficionada en el tema por sobre mi preparación intelectual, y de la cual me sorprendió sobremanera (imagino que tanta o más sorpresa causaría en el sector de la dirigencia política). La premisa fue:

- “Sufriste alguna de estas situaciones como usuarix de Redes Sociales? Cual?: Opciones: a) Robo de Identidad; b) Cyberbullying; c) Difusión de Imágenes Intimas; d) Injurias Calumnias”

De un total de casi 300 usuarixs, de los cuales el 70% que respondió fueron mujeres y el 30% hombres; y casi el 95% oriundos y residentes en la provincia de Buenos Aires, los totales aproximados fueron: Robo de Identidad: 21 %; Cyberbullying: 14 %; Difusión de Imágenes intimas: 10%; Injurias/ Calumnias: 55%. Y por una cuestión de orden en la encuesta y fidelidad de los resultados, dejé de lado a

casi 40 personas que acusaron haber sido víctimas de varios de las conductas dañosas online referidas, de forma conjunta o sucesiva.-

La realidad es que salvo por la ley referida sobre la difusión no consentida de imágenes intimas y su media sanción, Argentina atravesó un año mas de la era digital sin adecuarse a la misma y para peor: pretendiendo que nada ocurre y prestándole tan solo indiferencia como si de repente todo lo que ocurriera, pudiera ser tratado durante el año electoral que avecina, generando entonces marquesinas partidarias de políticas sin pensar demasiado, y convenientes a los fines que los legisladores que poco y nada hicieron este año, conserven su lugar en la banca.

Uno de los debates que se viene en estas condiciones, será la reforma de la ley de Propiedad Intelectual. Tendremos demasiado para oponernos y para proponer en el año que entra. Habrá que prepararse, por sobre todo, al embate.- Y en virtud del espacio conferido, grito al cierre de "***Lo personal es político!***" como dejara asentado hacia la eternidad, la maravillosa Carol Hanisch en cuanto el Estado debe garantizar a sus habitantes el bienestar, la integridad física y psíquica, la dignidad, la privacidad e intimidad, el honor y el acceso a la información. Políticas en serio para el resguardo y la libertad de lxs usuarixs de esta gran comunidad digital, y políticas de género que tiñan a la comunidad digital y física entera!

**La autora se desepeña en el estudio jurídico compuesto por las Dras. María Eugenia Orbea, Marina Benitez Demtschenko y Julieta Luceri; constituido en la ciudad de La Plata, Provincia de Buenos Aires, Argentina, se ha conformado para receptar y dar asesoramiento legal a los nuevos desafíos que surgen en la era digital.-

Dra. Benítez Demtschenko:

Derecho Informático y Nuevas Tecnologías.

Identidad digital y reputación online. Delitos informáticos. Injurias, calumnias y difamación online; medidas autosatisfactivas en el fuero federal; Redes Sociales. Presentaciones judiciales y extrajudiciales ante organismos reguladores y empresas proveedoras de Internet. Acciones civiles por responsabilidad en Internet. Protección de datos personales judicial y extrajudicial/ habeas data. Violencia de género online.-

Dra. Orbea:

Derecho de las Marcas y Patentes. Marketing digital y E-commerce.

Asesoramiento especializado sobre diseños, marcas y nombres comerciales para tiendas on line, showrooms, páginas de comercio electrónico; Protección de datos de modelos, contactos y trabajadores; Protección ante actos de Competencia Desleal y Publicidad; Asesoramiento legal sobre organización de desfiles y eventos de moda. Cesión de derechos de imagen para books, publicidad y catálogos; Adecuación y blindaje legal de páginas web de Moda y Belleza; community management (Social Media); Publicidad engaños; asesoramiento y abordaje de las distintas modalidades de contratación de trabajadores. Tratamiento migratorio de modelos, fotógrafos. Comercio exterior. Importación y exportación; Asesoramiento en contratos de franquicia, agencia, concesión, distribución, canje de productos, servicios publicitarios.-

Ofrecemos la perspectiva legal y el tratamiento de los espacios nuevos que las Nuevas Tecnologías propician, procurando al cliente no sólo la seguridad y la seriedad de una respuesta ajustada a la actualidad, sino también que se vean protegido y resguardado de un acuciante contexto que exige creatividad, rapidez y especialización por parte de los profesionales que lo asistan.-


AL
UNIVERSIDAD
AUTÓNOMA
LATINOAMERICANA
UNAULA

EL CONSULTOR EN SEGURIDAD INFORMÁTICA

Esp. Franco Vergara

Protegiendo la red hogareña

Autor : Lic. Franco Vergara

Tener una red informática en nuestra casa es algo que hace 20 años podía parecer impensado pero hoy es algo tan normal como leer el diario en internet cada mañana. Cabe aclarar que cuando me refiero una red informática en casa estoy hablando de una topología de red compuesta, generalmente, por un router y distintos tipos de dispositivos de usuario final; PC, notebooks, celulares, tablets, impresoras, etc, conectados a este.

Ahora, haciendo una análisis superficial de nuestra red es fácil darse cuenta que el router es el intermediario entre la red interna (LAN) y la externa (Internet) por ende es a quien deberíamos prestarle especial atención y así evitar ataques o accesos indebidos a nuestra red.

Estableciendo seguridad en el Router

Para empezar lo primero que deberíamos hacer es cambiar la contraseña de administrador del router, una recomendación que parece algo trivial pero que pocos hacen, ya que un ciberdelincuente con acceso al panel de administración del equipo podría modificar la configuración de servidores DNS y toda nuestra navegación sería redirigida a la computadora del delincuente o a donde él lo prefiera sin que lo detectemos ni notemos alguna anomalía.

Otra buena práctica de seguridad es deshabilitar cualquier tipo de acceso administrativo al router desde internet y en el caso que sea necesaria dicha gestión establecer una contraseña robusta al usuario administrador y bloqueos temporales de la cuenta al tercer o al quinto intento fallido para contrarrestar ataques de fuerza bruta desde internet.

Ahora, para los usuarios más avanzados o para los que les guste ir un paso más adelante otra buena práctica es la de actualizar el firmware (el sistema operativo) del router cada vez que sea necesario ya que muchas veces hay fallos de seguridad que únicamente se corrigen de esta manera.

El site www.routersecurity.org tiene mucha información relacionada a vulnerabilidades de routers y muchas herramientas para realizar escaneos y comprobaciones de seguridad.

Red WiFi

La red WLAN, conocida comúnmente como WiFi, es otro punto fuerte a atacar en lo que a seguridad de la red hogareña respecta ya que por lo general suelen ser vulnerables a posibles intrusiones de usuarios externos no autorizados.
A todos nos habrá tocado pasar por esa experiencia incómoda y a veces hasta insufrible de la navegación lenta. Generalmente aparece cuando más apurados estamos y resulta que si bien muchas veces el culpable es el mal servicio que nos brinda nuestro ISP muchas otras el problema está en nuestra red de área local.

Para estos casos lo primero que tenemos que hacer es corroborar si realmente el problema está en nuestro

ancho de banda utilizando alguna herramienta que sea capaz de medirlo como speedtest (www.speedtest.net).

Si los resultados del test de ancho de banda se condicen con el servicio contratado y la navegación sigue siendo lenta seguramente nos encontramos con un intruso en la red.

Detectando Intrusos en la red

Dos buenas herramientas para ver lo que pasa en nuestra red son: Air Snare y Netscan, la primera es

una tool con más funcionalidades que la segunda, pero si lo que estamos buscando es detectar intrusos cualquiera de las 2 nos va a servir. Basta con descargar, instalar el software y encontrar ver cuál es el equipo que no corresponde que esté conectado a nuestra red.

Cerrando puertas

La seguridad de la red WiFi se basa en 2 claves; la del router y la del acceso a la red inalámbrica. Como ya se vió el tema router queda por aclarar que para la red WiFi no deberíamos utilizar la contraseña que deja por defecto el ISP ya que muchos de estos proveedores de servicios usan patrones conocidos para definir las contraseñas, como el número del documento o el número de cliente del titular, facilitándole la tarea de llegar a nuestro password al ciberdelincuente.

Adicionalmente del cambio de contraseña es importante utilizar un tipo de cifrado reconocido como el WPA/WPA2.

A modo de mención comparto como novedad la pintura anti-WiFi. Fabricada por la compañía Pilkington y que ya se utiliza en algunos países del mundo. Se trata de un tipo de pintura especial que permite bloquear todo tipo de conexiones inalámbricas, no sólo de redes Wi-Fi, sino también Bluetooth y WiMax.

Medidas de seguridad inútiles

Al detectar la presencia de un intruso en la red muchos usuarios acuden a la medida más fácil; **apagar el router**. Si bien es cierto que con el router apagado es imposible que los intrusos accedan a nuestra red, también es cierto que nosotros tampoco tendremos acceso, y no termina ahí porque al encender el router el intruso recuperará la conectividad que había perdido.

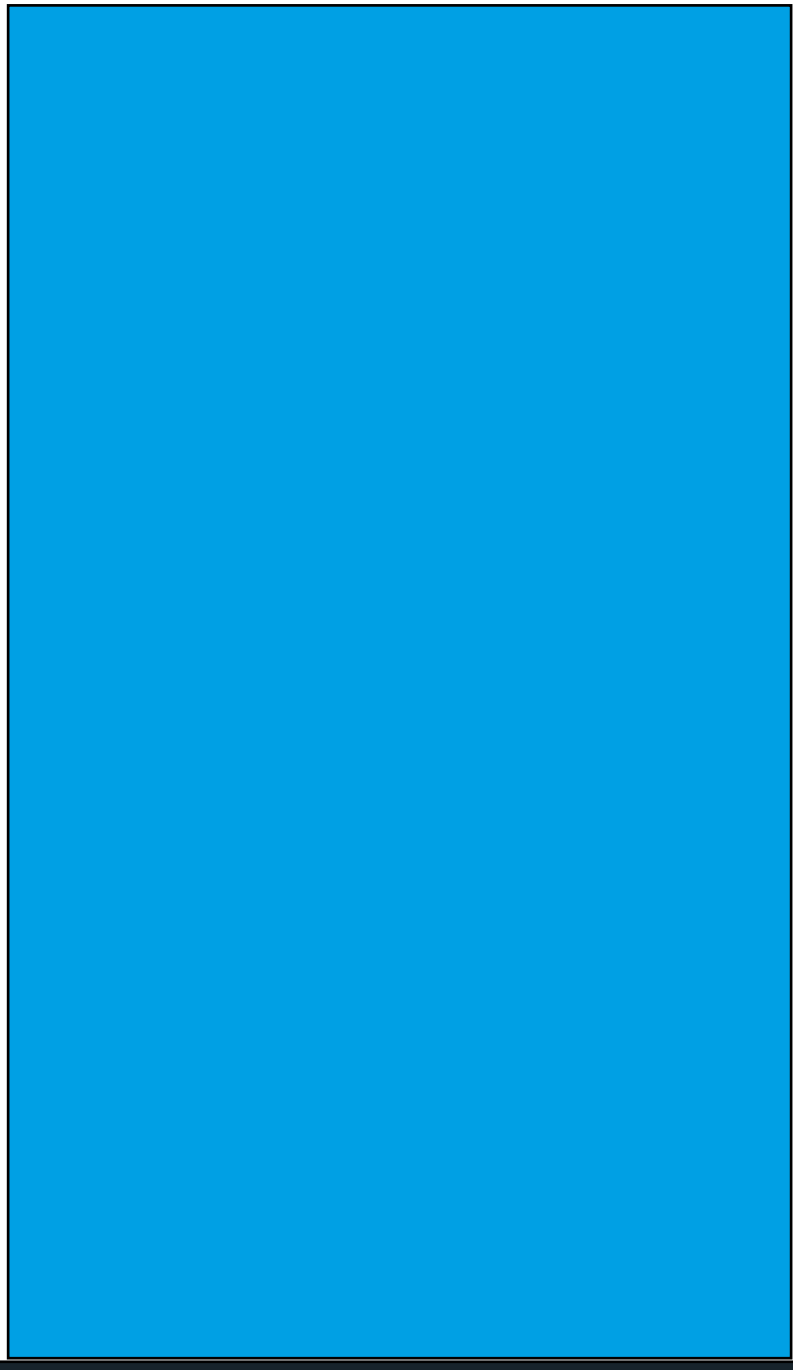
Otra medida bastante utilizada y que puede ser fácilmente vulnerada es el **Filtrado de equipo por MAC**. O sea, dar acceso a la red restringiendo por dirección física del dispositivo. En la teoría suena muy seguro pero esta restricción es fácilmente evadible con mecanismos de suplantación o cambios de dirección física más conocidos como MAC spoofing.

Por último, Si bien es importante y recomendable utilizar contraseñas robustas también es muy importante utilizar un tipo de cifrado seguro. Muchas personas se quedan en la primera parte, en la de utilizar una contraseña robusta, pero se olvidan que si utilizan algún tipo de cifrado débil como el **WEP** está clave puede ser descifrada en cuestión de segundo con herramientas como Aircrack.

Conclusión

Mantener la seguridad de nuestra red hogareña no es algo complejo, aunque sí un poco laborioso, pero es un esfuerzo que nos puede ahorrar muchos dolores de cabeza a futuro.

Lic. Franco Vergara
Especialista en Seguridad Informática



E-COMMERCE

AUTORA: María Eugenia Orbea

EL GIGANTE QUE NO LOGRA DESPERTAR

Hoy no podemos desconocer que el comercio por vía electrónica está en auge por las facilidades que ofrece internet como publicidad a muy bajo costo, difusión ilimitada, inmediatez del contacto, disminución de costos de intermediación y distribución sin embargo como la legislación no ha avanzado con la rapidez con que lo han hechos las nuevas tecnologías encontramos como principal valladar al despegue definitivo del e commerce en nuestro país, extensas lagunas de derecho que al generar desconfianza en el potencial consumidor impiden un sin número de intercambios mercantiles. Mientras el mercado ha crecido en forma vertiginosa, el derecho aún se encuentra en deuda en la finalización de un nuevo año.-

La venta on line sin duda ha cambiado los métodos que operaban en el tradicional mundo de los negocios y el comercio y con ello se ha modificado sustancialmente la forma y prueba de los contratos, pero también la forma de cumplimiento de los mismos y la formalización de los reclamos en casos donde el contrato no ha llegado a cumplir su finalidad en forma satisfactoria. Asimismo las ofertas cyber days, hot sales, black days, entre otras han venido a representar cambios en las operaciones comerciales, dando lugar a lo que se llama post e-commerce. Estos cambios vertiginosos, no se encuentran acompañados del correspondiente marco legal e irrogan pérdidas incuantificables.-

Por citar sólo un ejemplo, hace poco mas de un mes se dio a conocer el caso de un hombre que adquirió vía on line mas de 30 pasajes aéreos con tarjetas de crédito de otras personas, quienes impugnaban el cargo por la compra de esos pasajes, deviniendo en un pago rechazado para el aerolínea estafada. Estas maniobras irrogan pérdidas enormes a las empresas y dañan aún más al pequeño emprendedor quien carga

con las consecuencias de haber vendido su producto o servicio sin recibir su contraprestación a cambio.-

En Nuestro País la reciente reforma al Código Civil y Comercial Nacional, que comenzó a regir el 1 de agosto de 2015, ha introducido novedosamente esta modalidad de contratación a través de medios electrónicos, sin embargo, y más allá de representar un avance respecto de la obsoleta legislación, aún adolece de numerosos vacíos, principalmente en materia de la prueba informática a producirse sea en el fuero civil, comercial o penal.-

Hoy tan solo contamos con un puñado de pocas normas que a pesar de reconocer esta nueva modalidad adolecen de elementos esenciales: no logran reconocer al documento electrónico el carácter de instrumento con valor jurídico como una tercer categoría conjuntamente con los instrumentos privados y públicos (en sentido si bien la ley mal llamada “de firma digital” avanzó un poco al respecto resulta insuficiente); carecemos de normas claras que delimiten aquellos casos en los que el intermediario resulta o no responsable; no tenemos un marco de prevención de fraudes, ni resguardo de datos personales dejando librado al consumidor a las políticas de privacidad de cada sitio; carecemos de regulación de un sistema eficaz de arbitraje y mediación electrónica, rápido, de bajo costo y ágil como lo fue el proceso de compraventa. (E-resolutions); otro de los grandes flagelos que trae aparejada esta nueva modalidad contractual deviene de todo lo relacionado con las constantes violaciones a la propiedad intelectual (marcas, patentes, modelos industriales, derechos de autor), respecto de los cuales si bien contamos con la ley 11.723 que modificada por la ley 25.036 ha extendido la protección a la informática, no contempla expresamente el entorno digital; otro problema derivado de la extraterritorialidad deviene impuesta por las situaciones de doble imposición o ausencia de imposición tributaria que dificultan el desarrollo del e-commerce.-

Una regulación normativa específica regulatoria del e-commerce, que otorgue seguridad a la totalidad de los players del mercado, no sólo contribuiría a resolver los problemas suscitados en su consecuencia sino que al mismo tiempo, al brindar confianza a los interesados, facilitaría una eclosión positiva de esta modalidad mercantil en Argentina, principalmente en lo que atañe a las relaciones B2C (abreviatura de Business to Consumer: del negocio al consumidor) que son las que hoy marcan mayor presencia en el mercado. Por otro lado, sería conveniente también armonizar las legislaciones a nivel mundial, mediante convenios de cooperación o a través de los organismos internacionales ya instaurados que abandonen los principios de territorialidad propio de las legislaciones nacionales que poca aplicación tienen en el ámbito globalizado del comercio electrónico, principalmente en los aspectos relaciones con la propiedad intelectual y el tributario. Tal vez el 2017 sea el año en que se aborde finalmente el Anteproyecto de Comercio Electrónico. Lo cierto es que todavía queda mucho camino por andar.-

LA RED EDI

INFORMACIÓN QUE SUENA BIEN

WWW.ELDERECHOINFORMATICO.COM

¿LOS ABOGADOS NECESITAN MARKETING DIGITAL?

Autora: Carolina Marín

twitter @carolinamarinok Facebook @carolinamarinok www.marincarolina.com

¿Puede un abogado trabajar sin oficina? Como se trata de servicios no creo que sea un inconveniente, sin embargo, no es lo mismo citar a un cliente en un café que hacerlo en un estudio jurídico. Cada elemento de tu estudio va a influir en la percepción: el tamaño, la decoración, la ubicación, los muebles, incluso la cantidad de empleados y la atención al público. De acuerdo a la primera impresión (o reunión) el potencial cliente tomará la decisión de volver o no. Pero antes de llegar a la oficina (o al café) el cliente de un abogado hace un pedido a sus amigos y conocidos: "¿necesito un abogado, conocés uno bueno?" Y es aquí donde tu reputación debe ganarle a tu competencia y, en tiempos de internet, tu imagen y reputación pueden llevarte al éxito o al fracaso en un santiamén.

Imagen y reputación online

Todo el tiempo estamos construyendo nuestra imagen en internet, con lo que hacemos, decimos o con lo que callamos. Por otro lado, la opinión que otros vierten sobre nosotros construye nuestra reputación ¿cómo es esto? En Internet se generan miles de conversaciones detrás de personas, esas conservaciones, que pueden ser positivas y/o negativas, se generan en todas las plataformas digitales y, diferencia de la publicidad, no podemos manipularla tan fácilmente. Lo ideal es que haya una coherencia entre la imagen y la reputación, es decir, que lo que proyectemos sea lo mismo que los que los usuarios perciben, ergo, la reputación en el siglo XXI es la gallina de los huevos de oro.

"yo no tengo redes sociales ni web, así que no tengo problemas de que hablen de mi"

Grave error, el hecho de no estar en internet no te garantiza que no hablen de tu firma ¿y si alguien está hablando mal de tus servicios? lamentablemente no vas a poder defenderte. No estar en internet no te permite saber qué se dice de ti, por ende, no vas a saber qué mejorar. Tampoco te permite espiar a tu competencia o capitalizar los buenos comentarios.

El momento cero de la verdad

El momento cero de la verdad es el momento previo a estar cara a cara con un producto o servicio. Es el primer contacto del consumidor con la marca ¿dónde se da? Antes se hacía publicidad (estímulo) para persuadir en la decisión de compra de los consumidores, éstos llegaban al punto de venta y allí decidían si compraban o no. Hoy los consumidores ante un estímulo entran a internet y toman la decisión de compra antes de llegar a la tienda.

Cómo aprovechar el momento cero

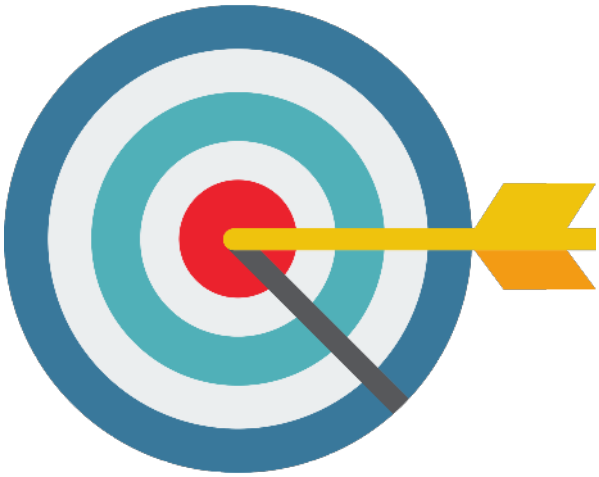
Más del 70% de los latinoamericanos que usan internet, utilizan buscadores online en sus decisiones de compra, ergo, en lo primero que debes invertir es un sitio. La web es la pieza más importante de toda tu estrategia digital. Es allí donde se concentran todos tus esfuerzos y objetivos de marketing digital. Dicho en otras palabras: tu oficina digital. Todas las estrategias deben llevar al consumidor a tu sitio. La interacción en las redes sociales, el SEO, las

campañas de publicidad en redes sociales o en los buscadores, las campañas de malings, etc. Hoy voy a hablarte de dos factores que debes tener en cuenta para tu marketing digital:

- **Contenido**

- Target

A quiénes nos dirigimos



Conocer a tu público te permitirá llegar a él de manera más rápida

Uno de los grandes errores en la comunicación es no saber a quienes les hablamos, creamos un mensaje común a todos, donde nadie se siente identificado ¿qué debes hacer? definir tu público. No solo con variables duras, como la edad, el sexo y clase social, sino con variables blandas; como intereses, gustos, miedos. Tratar de sacar una radiografía de tu cliente, esto te permitirá hablar de cosas que tu público necesita o le guste.

Ejemplo: Un abogado civil, especializado en familia, puede tener como público a madres solteras o divorciadas, mujeres jóvenes, independientes. Salen a comer afuera, hacen actividad física. Aprovechan los fines de semana para disfrutar con sus hijos. Les gusta viajar. Entonces, a estas madres puedes atraerlas a tu sitio o redes con contenido relacionado a su mundo: "Qué aspectos legales debe tener en cuenta si quiere viajar con su hijo menor de edad" o "cuántos días de vacaciones le corresponde a cada progenitor", etc. Puedes acercarles un pdf descargable con los requisitos para realizar diferentes trámite en juzgados, etc

Contenido útil

Tal como dicen el Manifiesto Cultrain: El contenido es el Rey, por ello, debes atraer y retener a tus clientes con contenido útil e inteligente en la web, blog y redes sociales. La mejor opción es tener un blog, que a mi criterio, es la pieza indicada para hacer marca en internet. Un blog te permitirá posicionarte como experto en una temática. Además, te ayudará posicionar tu web en Google. Los buscadores indexan páginas no sitios, esto quiere decir que cada entrada o página de tu web puede ser indexada por los motores de búsqueda, de esta manera aparecerá cuando los usuarios busquen determinado tema. Por lo tanto, si actualizas con frecuencia tu blog, tienes más posibilidades de aparecer en Google.

¿Los abogados necesitan Marketing Digital? Puedes ser el mejor abogado del mundo sin hacer marketing digital, la diferencia es que cuando utilizas el marketing todo el mundo se enterará que lo eres.

Hay una regla que se llama 80/20. El 80 % de tu contenido debe ser útil y solo el 20% de venta

Por segundo año consecutivo, la **Red Iberoamericana ElDerechoInformatico.com**, está reconociendo la labor de quienes a criterio de la postulación de la gente, la selección de los integrantes de la **Red EDI** así como algunos de los Ganadores de la EDICIÓN 2015, este año 2016, han entendido merecen ser R**ECONOCIDOS POR SU LABOR EN EL TRANSCURSO DEL AÑO** .-

Como todo reconocimiento su otorgamiento puede decirse es subjetivo, los que están, a nuestro criterio lo tienen bien merecido, encontrarán gente e instituciones que desde su punto de vista no lo merecen, o lo merecen menos que otros, lo que sea que sea, se debe justamente a la labor independiente de quienes han participado en la votación final,.-

Los **DESTACADOS DEL AÑO**, no tiene otro fin que el de pretender ser una modestísima palmada en la espalda destinada a aquellos que han desarrollado una labor meritoria en pos de esta materia que tanto nos apasiona.-

Para los que deberían haber sido merecedores de alguno de los RECONOCIMIENTOS y que no figuran en esta oportunidad, vayan nuestras más sinceras disculpas, trabajaremos para Mejorar, para los que si han tenido su merecido premio, vayan nuestras felicitaciones y esperamos que sirva de impulso para seguir trabajando y mejorando.-

FELIZ 2017

Guillermo M Zamora

Director

LOS DESTACADOS EDI DEL AÑO - ABOGADOS

LORENA DONOSO ABARCA-CHILE

Directora y fundadora del primer programa de Magíster en Derecho Informático en América Latina.

JORGE CAMPANILLA C. - ESPAÑA

Fundador Iurismática - Eventosjuridicos.com
Docente - Orador

DAVID MAETZU - ESPAÑA

Colaborador de Creative Commons España y miembro de la Junta Directiva de la Asociación de Usuarios de Linux de La Rioja - Orador

RODRIGO IGLESIAS - ARGENTINA

Impulsor preponderante en la concientización en contra del uso de voto electrónico en Argentina

EDI - LA REDIBEROAMERICA

LOS DESTACADOS EDI DEL AÑO - ABOGADOS

DANIEL CARBALLO - ESPAÑA

Director del Observatorio Iberoamericano de Protección de Datos Personales Socio ECIJA

HEIDY BALANTA - COLOMBIA

Heidy Balanta. Abogada, especialista en Derecho Informático y Nuevas Tecnologías. Magister en Derecho Económico

FRANCISCO GONZALEZ CALERO - ESPAÑA

Consejero Nacional por España del Observatorio Iberoamericano de Legislación y Políticas TIC (OLEPTIC) y miembro del Observatorio Iberoamericano de Protección de Datos

EDI - LA REDIBEROAMERICA

LOS DESTACADOS EDI DEL AÑO - EVENTOS

XI CONGRESO DE DERECHO INFORMÁTICO – CORINA IUALE

Responsable: Dra Corina Iuale - Lugar Bahia Blanca - Argentina

1ER CONGRESO PROVINCIAL DE DERECHO INFORMÁTICO,

Responsable: Jorge Deserio - Lugar Necochea - Argentina

XX CONGRESO IBEROAMERICANO DE DERECHO E INFORMÁTICA

Resposanle: Federico Bueno de Mata - Lugar: Salamanca España

ROBOTIURIS

Resposable: Alejandro Sánchez del Campo - Lugar: Madrid - España

LOS DESTACADOS EDI DEL AÑO - EVENTOS

VI CONGRESO IBEROAMERICANO CIIDI

Resposanble: Mg María Laura Spina - Lugar: Santa Fe Argentina

II ENCUENTRO DE DERECHO INFORMÁTICO

Resposanble: Elisabeth Bouvier - Lugar: Montevideo Uruguay

III CURSO INTERNACIONAL DERECHO INFORMÁTICO Y TIC´S" BIG DATA

Responsable: Ana Mesa - Lugar: Medellín Colombia

CIBERFORENSIC - II SIMPOSIO NACIONAL DE CIBERDELITOS

Resposable: José Leonett - Lugar: Guatemala

LOS DESTACADOS EDI DEL AÑO - EVENTOS

I ENCUENTRO INTERNACIONAL DE DERECHO INFORMÁTICO

Responsanble: Karen Céspedes -
Lugar: Lima - Perú

LOS DESTACADOS EDI DEL AÑO - ABOGADOS SUB40

JEFFERSON ESPINOZA VERA - COLOMBIA

Por su labor como colaborador en congresos, y aportes académicos

LIA HERNANDEZ - PANAMÁ

Fundadora del Instituto Panameño de Derecho y Nuevas Tecnologías (IPANDETEC). Representante de la sociedad civil e impulsora de la Comisión de Gobernanza de Internet para Panamá

LOS DESTACADOS EDI DEL AÑO - ABOGADOS SUB 40

LAINE MORAES SOUZA - BRASIL

fundadora LMSTREINAMENTO - ORADORA conferencista

ENMANUEL ALCANTARA - REPÚBLICA DOMINICANA

Ganador premio jóvenes innovadores -

MARCELO TEMPERINI - ARGENTINA

Titular de ASEGURARTE - Becario CONICET

EDI - LA REDIBEROAMERICA

LOS DESTACADOS EDI DEL AÑO - INFORMÁTICOS

ALVARO ANDRADE - BOLIVIA/PANAMA

Ingeniero de Sistemas Certificado por Microsoft, catorce años dedicado a la Seguridad informática e informática forense

JOSÉ LEONETT - GUATEMALA

Especialista en seguriad informática Ingogtm - OGDI

ALVARO SOTO - COLOMBIA

ASOTO - seguridad Informática - Conferencista

MARCELO ROMERO - ARGENTINA

Informático Forense - Grooming Argentina

EDI - LA REDIBEROAMERICA

LOS DESTACADOS EDI DEL PERIODISTAS/BLOGS/ SITIOS

COMUNIDAD VINTEGRIS

Responsable: Facundo Rojo
http://www.vintegris.info

NEGO2CIO

Responsable: Oscar Schmitz
http://www.nego2cio.com

LADOB.NET

Responsable: Irina Sternik
http://www.ladob.net

JURIDIA.CO

Resposanble: Camilo Escobar
http://www.juridia.co

JIA
JURÍDIA

LOS DESTACADOS EDI DEL PERIODISTAS/BLOGS/ SITIOS

EBLOG.COM.AR

Responsable: Lalo Zanoni
http://www.eblog.com.ar/

MARINCAROLINA.COM

Responsable: Carolina Marin
http://marincarolina.com/blog

ITCONNECT.LAT

Responsable: Marcelo Lozano
http://itconnect.lat

INSECURITYIT

Resposanble: Jeimy Cano
http://insecurityit.blogspot.com.co

LOS DESTACADOS EDI A LA TRAYECTORIA

YARINA AMOROSO - CUBA

Vicepresidenta de la Federación Iberoamericana de Derecho e Informática. Profesora del Centro de Gobierno Electrónico

HORACIO FERNANDEZ DELPECH - ARGENTINA

Vicepresidente de la Federación Iberoamericana de Asociaciones de Derecho Informático (FIADI)

CARLOS DELPIAZZO - URUGUAY

Decano de la Facultad de Derecho de la Universidad Católica del Uruguay.

HORACIO GRANERO - ARGENTINA

Fundador y actual Director de la Carrera de Posgrado de Abogado Especializado en Derecho de la Alta Tecnología (UCA)

EDI - LA REDIBEROAMERICA

LOS DESTACADOS EDI PROYECTOS DE DIFUSIÓN

CHARLAS COLEGIO SUPERIOR - ARGENTINA

Responsables: Analia Martinez, Juan Quaranta - Santa Fe / Argentina

ABOGADO DIGITAL - MÉXICO

Resposable: Joel Gomez Treviño
abogadodigital.tv

OGDI - GUATEMALA

Resposable: José Leonett
Observatorio Guatemalteco de Delictos Informático

TERMINOS Y CONDICIONES - ESPAÑA

Responsable: Jorge Morell Ramos
Sitio dedicado a prestar servicio en materia de terminos y condiciones de uso y otras prestaciones

LOS DESTACADOS EDI
PROYECTOS DE DIFUSIÓN

DATAINN - ESPAÑA

Responsable: Daniel López Carballo - DataInn nace como un laboratorio de innovación en el ámbito de la privacidad y protección de datos

LOS DESTACADOS
EDI APORTES ACADÉMICOS

FABIÁN DESCALZO

Identidades y funciones, el principio de la seguridad y el cumplimiento - Revista EDI N ° 24

FRANCO VERGARA

Los Televisores, tampoco se salvan - Revista EDI N° 23

LOS DESTACADOS EDI APORTES ACADÉMICOS

MARCELO BAUZA

Por su participación en el II ENCUENTRO DE DERECHO INFORMÁTICO - Uruguay

INFO-LAB

Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense (InFo-Lab) es una iniciativa conjunta de la Universidad FASTA

LAURA NAHATBETIAN BRUNET

Participación en el II ENCUENTRO DE DERECHO INFORMÁTICO - Uruguay

PAULINA CASARES SUBIA

"DERECHO A LA PERSONALIDAD Vs PROTECCIÓN DE DATOS PERSONALES" - Revista EDI N° 24

EDI - LA REDIBEROAMERICA

Estamos donde estas vos

ElDerechoInformatico

Centro de Información y Formación

ELDERECHOINFORMATICO.COM

TODA LA INFORMACIÓN EN UN SOLO LUGAR