e-boletín legal de Derecho Penal Informático
Boletín Legal sobre Cibercrimen
PERÚ

CYBERCRIMEN
Año I, N°. 4
Diciembre , 2012

En esta oportunidad nuestro boletín se encuentra destinado al delito de Acceso Ilícito o Intrusismo Informático, contemplado en el Artículo 207-A del Código Penal y ubicado dentro Titulo V – Delitos Contra el Patrimonio, desde su incorporación el año 2000 mediante la Ley N° 27309, no se ha explicado el porqué de su ubicación junto a los tipos penales que protegen el bien jurídico Patrimonio, cuando en realidad esta clase de figuras delictivas se encuentran orientadas a la *protección de la información y datos,* entendidos para algunos como un nuevo bien jurídico; o para prevenir cualquier atentado contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, de las redes y de los datos; bien jurídico que no encuentra tutela en nuestra legislación.

En ese orden de ideas, haremos mención a la Ley N° 27309 que incorporó al Código Penal en el año 2000 el delito de Acceso Informático, asimismo haremos mención al Convenio sobre la Cibercriminalidad o Convenio de Budapest, que en el Artículo 2° da un tratamiento a este tipo penal; además del punto de vista del legislador respecto al tratamiento legal de esta figura a la fecha. Normatividad que nos permitirá orientarnos en el tema.

Y para culminar le presentaremos las noticias del mes asociadas a la Cibercriminalidad, así como los eventos y/o cursos, que se encuentran próximos a realizar.

Esperando, como siempre, que la información que la información proporcionada le resulte útil y de su agrado.

Fabiola Villanueva Del Busto
División de Cybercrimen
IRIARTE & ASOCIADOS

SUMILLA

TEMA PRINCIPAL:

- EL INTRUSISMO INFORMÁTICO EN EL PERU, 12 AÑOS DESDE SU INCORPORACIÓN AL CÓDIGO PENAL.

SELECCIÓN DE NORMAS:

- LEY N° 27309 – LEY QUE INCORPORA LOS DELITOS INFORMÁTICOS AL CÓDIGO PENAL
- CONVENIO SOBRE LA CIBERCRIMINALIDAD DEL CONCEJO DE EUROPA O CONVENIO SOBRE CIBERCRIMINALIDAD DE BUDAPEST.
- DICTAMEN DE LA COMISIÓN DE JUSTICIA Y DERECHOS HUMANOS RECAÍDO EN LOS PROYECTOS DE LEY 034/2011-CR, 037/2011-CR Y 1136/2011-CR CON UN TEXTO SUSTITUTORIO POR EL QUE SE PROPONE LA LEY DE LOS DELITOS INFORMÁTICOS

SECCIÓN DE NOTICIAS:

- "CRECEN ROBOS ON LINE: 500 ATAQUES DIARIOS"
- "FACEBOOK AYUDO AL FBI A DESBARATAR BANDA DE CIBERCRIMEN"
- "HACKER DE CHRISTINA AGUILERA Y SCARLETT JOHANSSON IRA A 10 AÑOS DE PRISIÓN"
- "LA UE DESTINA 400 MILLNES A LA LUCHA CONTRA EL CIBERCRIMEN"
- "PERÚ ¿EL PARAÍSO DEL CIBERCRIMEN? SEPA POR QUÉ
- "EN NAVIDAD REDOBLE SU SEGURIDAD INFORMÁTICA"

SECCIÓN DE EVENTOS:

- JORNADA SOLIDARIA DE SEGURIDAD DE LA INFORMACIÓN.
- TERCER CURSO VIRTUAL DE INFORMÁTICA FORENSE ASPECTOS PRÁCTICOS Y METODOLOGICOS.

e-boletín legal de Derecho Penal Informático
Boletín Legal sobre Cibercrimen
PERÚ

CYBERCRIMEN
Año I, N°. 4
Diciembre , 2012

EL INTRUSISMO INFORMÁTICO EN EL PERÚ, 12 AÑOS DESPUÉS DE SU INCORPORACIÓN.

El Derecho Penal al ser considerado como el medio de control social más efectivo con que cuenta el Estado para mantener la vida en comunidad, debe responder siempre a los cambios que esta atraviesa, regulando de esta manera aquellas conductas contrarias a ley que pongan en peligro la coexistencia en sociedad,; es pues que partiendo de esta línea base, instrumentos internacionales como el Convenio sobre la Cibercriminalidad o Convenio de Budapest, conscientes de los cambios de las tecnologías y preocupados por el riesgos de las redes informáticas y la información electrónica sean utilizadas para cometer delitos, en caminan sus esfuerzos a proteger a la sociedad frente a la ciberdelincuencia, adoptando para ello una legislación adecuada y fomentando la cooperación internacional, es así pues que el Convenio en su Artículo 2° tipifica el *Acceso Ilícito,* definiéndola de la siguiente manera:

"…El acceso deliberado e ilegítimo al a totalidad o a una parte de un sistema informático. Cualquier Parte podrá exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos o contra intención delictiva, o en relación con un sistema informático que esté conectado a otro sistema".

Por nuestra parte, en el Perú el 17 de julio del año 2000 mediante la Ley N° 27309 se incorporaron los Delitos informáticos al Código Penal, ubicándolos dentro del Título V del Libro Segundo – Delitos Contra el Patrimonio, aun cuando, como lo señala el propio Convenio de Budapest esta clase de delitos se encuentran orientados a la protección de bienes jurídicos como *la información o protección de datos informáticos, o en su defectos la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, de las redes y de los datos.* En ese orden de ideas, autores como Luis Miguel Reyna Alfaro señalan que si bien el Patrimonio resulta ser el valor genéricamente tutelado, el interés social resguardado de manera específica es *"la información contendida en los sistemas de tratamiento automatizados de datos",* siendo esto así para innegable que se otorga, señala el antes mencionado autor, a la "información" un valor económico, con lo que la regulación de lege lata guardaría cercana relación con la concepción del suscrito sobre el valor social digno de tutela, sin embargo – precisa una vez más - existen saltantes diferencias en la ubicación del bien jurídico penal, lo que tiene a su vez importantes consecuencias prácticas.[1]

[1] REYNA ALFARO, Luis. *Los Delitos Informáticos Aspectos Criminológicos Dogmáticos y de Política Criminal.* Edición Enero 2002. Lima. Jurista Editores. 2002. Pág. 257.

Es mediante la Ley N° 27309, que nuestro Código Penal en el Artículo 207°- A, contempla la figura del Acceso Ilícito o Intrusismo Informático, el cual es definido como:

"El que utiliza o ingresa indebidamente a una base de datos, sistema o red de computadoras o cualquier parte de la misma, para diseñar, ejecutar o alterar un esquema u otro similar, o para interferir, interceptar, acceder o copiar información en tránsito o contenida en una base de datos, será reprimido con pena privativa de libertad no mayor de dos años o con prestación de servicios comunitarios de cincuentidós a ciento cuatro jornadas.

Si el agente actuó con el fin de obtener un beneficio económico, será reprimido con pena privativa de libertad no mayor de tres años o con prestación de servicios comunitarios no menor de ciento cuatro jornadas".

El **Intrusismos Informático o Hacking**, entendido como la conducta de arrogarse ilegalmente el derecho o la jurisdicción de ingresar en un sistema informático o red de comunicaciones electrónica de datos, con la consecuente transgresión de las seguridades por el webmaster o prestados por al webhosting, con el fin de proteger los servicios de transmisión, almacenamiento y procesamiento de datos que ofrece frente a posibles abusos de terceros.[2]En cambio para nuestra legislación es aquella conducta típica que consiste en la utilización o ingreso ilícito a una base de datos, sistema o red de computadoras. En ese orden de ideas debemos indicar que para la configuración del delito no basta que se utilice o ingresa a una base de datos, red o sistemas de computadoras, es necesario que esta conducta esté orientada a diseñar, ejecutar o alterar un esquema u otro similar, a efectos de interferir, interceptar, acceder o copiar información en tránsito o contenida en una base de datos. De la definición antes brindada nos pone en advertencia, que para nuestra legislación no es necesario que el tipo penal se comenta infringiendo una medida de seguridad.

Ahora bien, desde el año 2000 en que se incorporó el tipo penal de Intrusismo en el Perú a la fecha, solo contamos con un intento de modificación y perfeccionamiento de este tipo penal, el ya mencionado Dictamen De La Comisión De Justicia Y Derechos Humanos Recaído En Los Proyectos De Ley 034/2011-Cr, 037/2011-Cr Y 1136/2011-Cr Con Un Texto Sustitutorio Por El Que Se Propone La Ley De Los Delitos Informáticos, el cual en su Artículo 2° define al Intrusismo de la siguiente manera:

" Será reprimido con pena privativa de libertad no menor de uno ni mayor de tres años o con prestación de servicios comunitarios no menos de ciento cuatro jornadas, el que si estar autorizado:

[2] CANO MARTÍNEZ, Jeimy. *El Peritaje Informático y la Evidencia Digital en Colombia.* Primera Edición. Bogotá. Ediciones Uniandes. 2010. Pág. 241.

1. *Acceda a un sistema informático o se mantenga en él.*
2. *Interfiera, impida u obstaculice el acceso a un sistema informática o sus datos, o a una red de telecomunicaciones.*
3. *Intercepte datos informáticos o de usuario en su origen, destino o en el interior de un sistema informático o las señales electromagnéticas que provienen de un sistema informático que los transporte."*

Como se advierte, no esta intención de regularizar este tipo de conductas no dista mucho de lo ya regulado en el Artículo 207°-A del Código Penal, en ese sentido consideramos que una vez más y a efectos de combatir con mejores armas la cibercriminalidad, se tome en cuenta el modelo o el espíritu de lo ya regulado por el Convenio de Budapest para el Intrusismo.

Consideraciones Finales:

A efectos de combatir la ciberdelincuencia, el Perú día a día se ven en la necesidad de adherirse a Convenios como el de Budapest, tipo de normatividad internacional que permite evitar la sensación de inseguridad que atraviesan los ciudadanos cuando se encuentran frente a conductas delictivas como la del Acceso Informático o Intrusismo Informático; o en su defecto actualizar la normatividad vigente, acogiendo como fuente o principio los valores que recoge el convenio antes mencionado, respetuoso de los Derechos Fundamentales y acorde a las tendencias de un Derecho Penal Garantista.

SELECCIÓN DE NORMAS

- **17 de Julio de 2000**

LEY N° 27309 – LEY QUE INCORPORA LOS DELITOS INFORMÁTICOS AL CÓDIGO PENAL.
Conforme al Artículo Único de la ley se modificó el Título V del Libro Segundo del Código Penal, incorporándose el Artículo el Capítulo "X" – Delitos Informáticos, siendo el Artículo 207°-A - *Interferencia, Acceso o copia ilícita contenida en base de datos*.

- **23 de Noviembre de 2001**

(Entra en Vigor el 1 de Julio de 2004)

CONVENIO SOBRE LA CIBERCRIMINALIDAD DEL CONCEJO DE EUROPA O CONVENIO SOBRE CIBERCRIMINALIDAD DE BUDAPEST

El siguiente instrumento internacional, con la finalidad de combatir la cibercriminalidad, regula en su Artículo 2, define al delito de Acceso Informático, como aquella conducta de acceder deliberadamente e ilegítimamente a la totalidad o a una parte de un sistema informático, asimismo indica que el delito se puede cometer infringiendo medidas de seguridad, con la intención de obtener datos informáticos o con otra intención delictiva, o en relación con un sistema informático que esté conectado a otro sistema informático.

- **20 de Julio de 2012**

DICTAMEN DE LA COMISIÓN DE JUSTICIA Y DERECHOS HUMANOS RECAÍDO EN LOS PROYECTOS DE LEY 034/2011-CR, 037/2011-CR Y 1136/2011-CR CON UN TEXTO SUSTITUTORIO POR EL QUE SE PROPONE LA LEY DE LOS DELITOS INFORMÁTICOS.

Siempre aclarando que se trata de un Dictamen y no de una norma, solo que a efectos de tener encuentra el punto de vista del legislador sobre materia de Cibercriminalidad, hemos considerado pertinente ubicarlo en esta sección de nuestro boletín, en ese orden de ideas debemos precisar que el Artículo 2° del Dictamen contempla la figura penal del Intrusismo informático.

NOTICIAS

"CRECEN ROBOS ON LINE: 500 ATAQUES DIARIOS"
28 DE NOVIEMBRE

Si piensa hacer compras o transacciones bancarias por Internet en esta Navidad, tenga mucho cuidado. Los 'ciberdelincuentes' están al acecho: al día se cometen 500 ataques 'online' en el Perú, según la empresa Kunak Consulting.

"La delincuencia común se ha trasladado al ciberespacio y se ha vuelto más sofisticada en nuestro país y, en vísperas de las fiestas de fin de año, aumentan los ataques digitales para robar datos, sobornar o generar fraude financiero. Las extorsiones bajo la amenaza de la divulgación de

fotografías íntimas también se incrementan", advirtió a Perú21 Stanley Velando, director de la referida compañía.

Existen diferentes técnicas de estafa, aunque la más común es el 'phishing'. Este ocurre cuando la víctima es inducida –mediante correos electrónicos– a abrir falsos sitios web de entidades bancarias.

Así, los hampones obtienen datos de los usuarios que les permiten transferir dinero o hacer compras 'online'. "Esta modalidad se ha extendido no solamente a los bancos, sino también a los comercios 'online' y a los sitios de inversiones", indicó Velando.

Además, se refirió al 'pharming', que es una versión más sofisticada de fraude 'online'.

Lo increíble es que el 5% de peruanos que reciben este tipo de mails lo abren. "La proporción parece poca si no se tiene en cuenta que el hacker lanza el anzuelo a millones de direcciones", manifestó.

En el 'pharming', los maleantes instalan en la PC de su víctima un programa que altera las direcciones de Internet. Así, la llevan a otra página para robarle sus datos. También están los 'key logers', que son instalados en las cabinas de Internet.

Fuente: Perú 21
http://peru21.pe/impresa/crecen-robos-online-500-ataques-diarios-2105452

"FACEBOOK AYUDO AL FBI A DESBARATAR BANDA DE CIBERCRIMEN"
12 DE DICIEMBRE

En San Francisco. Investigadores liderados por el FBI y ayudados por Facebook, **desarticularon una organización internacional que infectó 11 millones de computadoras en todo el mundo, causando más de US$850 millones en pérdidas,** en una de las principales operaciones contra delitos cibernéticos de la historia.

El FBI, trabajando de forma conjunta con la mayor red social del mundo y varios organismos internacionales, detuvieron a diez personas a las que se les acusa haber infectado las máquinas con el software malicioso "Yahos", para luego robar números de tarjetas de crédito y otro tipo de información personal.

Sus "sistemas de seguridad fueron capaces de detectar las cuentas afectadas y proporcionar herramientas para eliminar estas amenazas", dijo el FBI.

El FBI dijo que los detenidos provienen de Bosnia Herzegovina, Croacia, Macedonia, Nueva Zelanda, Perú, Reino Unido y Estados Unidos, y que ejecutó numerosas órdenes de búsqueda y llevó a cabo una serie de entrevistas.

Es difícil conseguir datos concretos, pero expertos dicen que los delitos cibernéticos están aumentando en todo el mundo ya que el uso de computadores y teléfonos móviles se ha vuelto más frecuente y más transacciones financieras se realizan a través de internet.

Los profesionales de la seguridad cibernética y las empresas especializadas tienen cada vez más dificultades para detectar y detener estos ataques.

Fuente: Tecno América Economía
http://tecno.americaeconomia.com/noticias/facebook-ayudo-al-fbi-desbaratar-banda-de-cibercrimen

"HACKER DE CHRISTINA AGUILERA Y SCARLETT JOHANSSON IRA A 10 AÑOS DE PRISIÓN"
17 DE DICIEMBRE

En los Ángeles, un juez federal sentenció a **10 años de prisión a un pirata cibernético** que entró ilegalmente a las cuentas personales en Internet de Scarlett Johansson, Christina Aguilera, Mila Kunis y otras celebridades.

El juez federal de distrito S. James Otero en Los Ángeles dictó la sentencia contra Christopher Chaney después de que el tribunal escuchara el testimonio de una conmovida Johansson en una declaración grabada en video.

El mayor escándalo del caso fueron las fotos que la actriz se tomó estando desnuda y que fueron publicadas en Internet. Las fotos estaban destinadas a Ryan Reynolds, su entonces esposo.
Chaney, de 35 años, originario de Jacksonville, Florida, se declaró culpable de cargos que incluyeron espionaje y acceso sin autorización a una computadora.
Chaney también dañó moralmente a dos mujeres que conocía. Envió fotografías de una ex compañera de trabajo al padre de ella, en la que la mujer aparecía desnuda.

Fuente: El Comercio

http://elcomercio.pe/espectaculos/1511141/noticia-hacker-christina-aguilera-scarlett-johansson-ira-10-anos-prision

"LA UE DESTINA 400 MILLNES A LA LUCHA CONTRA EL CIBERCRIMEN"
17 DE DICIEMBRE

La UE incrementa el presupuesto destinado a ciberseguridad un 14% hasta el año 2020. Para el período comprendido entre 2007 y 2013 el presupuesto asignado es de 350 millones de euros, cifra que tan sólo se ha visto incrementada en 50 millones para el periodo 2013-2020. Serán 400 millones a repartir entre diversos proyectos y organismos dedicados a combatir el crimen cibernético.

Estos 400 millones deben contribuir a financiar durante siete años más de media docena de proyectos, entre ellos **Syssec**, una red europea que trabaja en el desarrollo de vías para predecir amenazas y puntos débiles; **Nessos**, que diseña arquitecturas de servicios seguros; **SecureChange**, que prueba softwares detectando problemas de seguridad; y **Tclouds**, que aspira a construir "nubes" seguras.

Además, el presupuesto debe servir para asegurar los datos. En ello se centra el proyecto **Ecrypt II**, que reúne a 32 institutos de investigación líderes, universidades y compañías para desarrollar herramientas mejoradas para empresas digitales.

Según la Comisión Europea, unos **150.000 virus o** *malware* **rondan por Internet, infectando a más de un millón de personas cada día**. El antivirus **MacAfee** contabiliza 75 millones de piezas de código de *malware* malicioso en sus bases de datos con botnets lanzando spam y llegando a suponer un tercio de los e-mails enviados cada día. **El coste mundial del cibercrimen se estima en más de 750 billones de euros anuales**, en términos de tiempo perdido, recursos, pérdida de oportunidades de negocio...

Son muchos los expertos en seguridad informática que han calificado de pobre este presupuesto. Rik Ferguson, director de Investigación de Seguridad y Comunicación de la empresa **TrendMicro**, ha afirmado que "la industria de seguridad comercial está ya brindando recursos a través de organizaciones sin ánimo de lucro, no obstante, ha llegado el momento de que los gobiernos hagan una inversión acorde con el cada vez mayor riesgo al que se enfrentan procedente del auge del cibercrimen".

Fuente: Dirigentes Digitales
http://www.dirigentesdigital.com/articulo/mercado_eurolatino/210152/destina/400/millones/lucha/cibercrimen/ciberseguridad/cloud/computing/seguridad/virus/malware.html

"PERÚ ¿EL PARAÍSO DEL CIBERCRIMEN? SEPA POR QUÉ"
20 DE DICIEMBRE

Un reciente informe publicado por El Comercio señala que, en el mundo, los delitos informáticos generan pérdidas de US$ 110 billones, de los cuales corresponden al Perú menos de US$ 5 millones. Sin embargo eso no significa que el problema no nos afecte gravemente.

Según Álvaro Thais Rodríguez, asesor de seguridad informática de ASBANC, el Perú se está convirtiendo en un paraíso para los cibercriminales debido a la falta de una adecuada legislación y por eso los cientos de miles de afectados crecen exponencialmente cada año.
En la actualidad, recordó Thais, solo existe en el Congreso una propuesta que fue aprobada a fines de la legislatura pasada en la Comisión de Justicia y quedó lista para el pleno, pero ha sido duramente criticada porque incluía medidas contrarias a los derechos fundamentales, razón por la cual se espera que surjan nuevas propuestas o se optimicen las ya existentes.
"Estamos con una legislación desfasada. Tenemos una ley penal que se remite al año 2000, la cual solo contempla el intrusismo y el sabotaje en formas agravadas. No cubre el fraude informático y este es un grave déficit", advirtió.

En nuestro país, agregó, se necesita seguir la tendencia mundial y suscribir el Convenio de Budapest sobre delitos informáticos. "Nosotros solo tenemos tipificado uno de los nueve delitos que penaliza Budapest", advirtió.

El mes pasado, Erick Iriarte, del estudio Iriarte & Asociados, informó que en el ámbito gubernamental existe una comisión con representantes de varios ministerios que se encargan de trabajar para lograr la suscripción del citado convenio. No obstante, en ASBANC están preocupados porque a lo largo de los últimos años ha habido varios acercamientos, pero no se han visto medidas concretas que permitan su pronta concreción.

Incidencia
De acuerdo con cifras de la fiscalía, en nuestro país se han denunciado en el último año 243 casos. Los expertos en el tema calculan que la incidencia es mayor. Norton considera que en el mundo existen 556 millones de víctimas al año y más de 2,5 millones de afectados por país, en promedio. El Perú, dada la cantidad de pobladores, se calcula que al menos se debe estar cerca del medio millón.

Fuente: Terra
http://economia.terra.com.pe/noticias/noticia.aspx?idNoticia=201212202126_TRR_81861232

"EN NAVIDAD REDOBLE SU SEGURIDAD INFORMÁTICA"
22 DE DICIEMBRE

La Navidad es una de las fechas del año más esperadas por los ciberdelincuentes. Ellos se aprovechan de la emoción, el apuro y el descuido de muchos usuarios para beneficiarse a través de estafas, virus y otras artimañas.

En la mira están aquellos que recurrirán a Internet para hacer sus compras de último minuto. "Entre los principales riesgos a los que se exponen los usuarios en estas situaciones son las estafas electrónicas, el robo de datos personales y el "phishing"", señala Raphael Labaca, coordinador de Awareness & Research de ESET Latinoamérica.

La primera recomendación es la protección del dispositivo a usar. "Así sea una computadora de escritorio o un dispositivo móvil, debe tener el sistema operativo actualizado. Además, es necesario que contengan alguna solución de seguridad que proteja al usuario durante su navegación", indican los expertos de ESET.

La otra sugerencia básica es comprar solo en sitios web reconocidos y que cuenten con buena reputación. Asimismo, antes de realizar cualquier transacción, debe revisar cuáles son los sistemas de seguridad con los que cuenta el sitio.

"Durante el tercer trimestre del 2012, hemos encontrado 43,4 millones de sitios web sospechosos, lo que representa un incremento de 20% con respecto al trimestre anterior", indicó en un comunicado la empresa de seguridad McAfee.

"Aunque está muy de moda, el uso de redes Wi Fi (inalámbricas) puede ser un riesgo para intercambiar información sensible, pues el tráfico de la red puede ser interceptado. Se recomienda usar una red privada", recomienda ESET Latinoamérica.

Adicionalmente, debe tener mucho cuidado con los supuestos premios sorpresa que se ofrecen en las ventanas emergentes con publicidad, y con los enlaces o "links" en los correos electrónicos y redes sociales. Este tipo de técnicas solo busca atraer a sus víctimas para robarles su dinero.

NUEVAS MODALIDADES DE LA CIBERDELINCUENCIA
Los nuevos usos que la gente le da a sus aparatos tecnológicos originan que los ciberdelincuentes también renueven su accionar criminal. "Han aparecido mensajes de texto 'phishing', conocidos como 'smishing', y están en aumento. Suplantan la identidad de una persona o institución y, con

engaños, hacen que la víctima ingrese a un enlace que lleva a un sitio malicioso", explican los expertos de McAfee Labs.

De otro lado, ha aparecido el 'scareware', un engaño que busca que el usuario crea que su PC puede estar infectada y lo invita a comprar un antivirus falso. Para ello tiene que entregar sus datos personales y financieros. Generalmente utilizan ventanas emergentes.

Por su parte, el 'ramsonware' acusa a quienes navegan por la red de que visitaron páginas web ilegales, tomando el nombre de la policía y amenazan de bloquear el sistema de la computadora hasta que paguen una multa.

Según los datos que maneja McAfee Labs, el 'ramsonware' ha crecido un 43% en el tercer trimestre del año, mientras que el 'scareware' continúa avanzando y se calcula que crea un millón de víctimas cada día.

Y para prevenir cualquier tipo de ataque a través de las consolas de videojuegos de última generación, que se conectan a Internet, se recomienda a los padres ajustar los controles paternos adecuados para evitar que se comparta información privada y sensible.

Fuente: El Comercio
http://elcomercio.pe/actualidad/1513135/noticia-navidad-redoble-su-seguridad-informatica_1

EVENTOS

JORNADA SOLIDARIA DE SEGURIDAD DE LA INFORMACIÓN
Fecha: Sábado 22 de diciembre
URL: http://www.computo-forense.blogspot.com/

TERCER CURSO VIRTUAL DE INFORMÁTICA FORENSE ASPECTOS PRÁCTICOS Y METODOLOGICOS.
Fecha: Domingo 06 de enero.
URL: http://computo-forense.blogspot.com/2012/11/tercer-curso-virtual-de-informatica.html

IRIARTE & ASOCIADOS
Jr. Miró Quesada 191 - Of. 510. Lima 01 – Perú.
Telefax (+511) 427 0383
http://www.iriartelaw.com
contacto@iriartelaw.com

©2012 Iriarte & Asociados.