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

CYBERCRIMEN
Año II, N°. 5
Enero , 2013

En este, nuestro primer boletín del año, nos hemos orientado hacia el tipo penal de Daño informático de Acceso Ilícito contemplado en el Artículo 207-B 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 por qué 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 Daño Informático, mencionaremos, una vez más, al Convenio sobre la Cibercriminalidad o Convenio de Budapest, que en el Artículo 4° - Ataques a la Integridad de los datos y Artículo 5° - Ataques a la integridad del sistema; 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.

Finalmente, les presentaremos las noticias del mes asociadas a la Cibercriminalidad, así como los eventos cursos, que se encuentran próximos a realizar.

A la espera de que la información proporcionada le resulte útil, oportuna y agradable.

Fabiola Villanueva Del Busto
División de Cybercrimen
Iriarte & Asociados

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

CYBERCRIMEN
Año II, N°. 5
Enero , 2013

SUMILLA

TEMA PRINCIPAL:

- EL DELITO DE DAÑO INFORMÁTICO EN EL CÓDIGO PENAL PERUANO.

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:

- "EL CIBERCRIMEN SE CENTRA EN LAS EMPRESAS CON PRESENCIA EN INTERNET"
- "LA CE CREA UN CENTRO ESPECÍFICO PARA LUCHAR CONTRA EL CIBERCRIMEN"
- "FILIPINAS. PROTESTA CONTRA LEY DE PREVENCIÓN DEL CIBERCRIMEN"
- "EL VIRUS DE GRINGASHO"

SECCIÓN DE EVENTOS:

- SEMINARIO: VIRUS INFORMATICOS
- CURSO DE COMPUTO FORENSE (CNCF)
- CURSO FULL DAY DE HACKING LIBRE

EL DELITO DE DAÑO INFORMÁTICO EN EL CÓDIGO PENAL PERUANO

El delito de Daño o Sabotaje informático fue incorporado al Código Penal 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, dando a entender que el bien jurídico a proteger sería el patrimonio, sin embargo, instrumentos internacionales como Convenio de Budapest, da a entender que 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",* [1]de lo cual se colige que a la "información" se le ha asignado un valor económico. El delito de Daño Informático, suele ser uno de los comportamientos más frecuentes y más graves en el ámbito informático, desprendiéndose de diversos estudios que su incidencia en la empresa, en particular en la pequeña y mediana, es muy elevada, generando elevadas pérdidas económicas[2]. Sin embargo, la sanción a este tipo de delitos, así como su investigación es escasa, por no decir nula. Así tenemos que según el anuario estadístico del Ministerio Público correspondiente al año 2011, solo se registran 243 casos de delitos informáticos.

Es pues, que mediante la Ley N° 27309, que nuestro Código Penal en el Artículo 207°- B, contempla la figura de Daño o Sabotaje Informático, que es definida como:

"El que utiliza, ingresa o interfiere indebidamente una base de datos, sistema, red o programa de computadoras o cualquier parte de la misma con el fin de ***alterarlos, dañarlos o destruirlos****, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años y con setenta a noventa días multa"*

Del párrafo anterior se desprende que el objeto material del delito son las bases de datos, sistemas, red o programas de computador o cualquier parte de la misma, con lo cual se diferencia del tipo penal de Daños descrito en el Artículo 205° del Código Penal. Si bien es cierto el legislador no ha definido que se entiende por datos o sistemas informáticos, el Convenio de Budapest en el Artículo 1, los define de la siguiente manera:

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

[2] FARALDO CABANA, Patricia. *Las Nuevas Tecnologías en los Delitos contra el Patrimonio y el Orden Socioeconómico.* Primera Edición. Valencia. Tirant lo Blanch.2009. Pág. 138.

a. *"por "**sistema informático**" se entenderá todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa";*

b. *"por "**datos informáticos**" se entenderá toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función."*

De la redacción del Artículo 207-B del Código Penal se advierte que nos encontramos ante un tipo penal de resultado, y de carácter doloso, pues se requiere la conciencia y voluntad del agente de causar daño. En ese sentido, para su consumación se requiere **alterar, dañar o destruir,** indebidamente, una base de datos, sistema, red o programa de computadoras.

En cuanto al Convenio de Budapest, debemos indicar que el tipo penal de Daño o Sabotaje informático se encuentra contemplado en los siguientes artículos:

"Artículo 4 – Ataques a la integridad de los datos

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos informáticos.

2. Las Partes podrán reservarse el derecho a exigir que los actos definidos en el párrafo 1 comporten daños graves."

"Artículo 5 – Ataques a la integridad del sistema

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos."

Como se observa de la redacción, tanto el Código Penal Peruano, como el Convenio de Budapest, sancionan la misma conducta, siendo la diferencia que el instrumento internacional sanciona este tipo de conductas a través de dos tipos penales, en tanto el código penal peruano, agrupa ambos comportamientos en un solo tipo penal.

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 3°, segundo párrafo, define al Sabotaje Informático de la siguiente manera:

"(…) El que sin autorización, distribuya, borre, desvanezca, quite, dañe, deteriore, suprima o altere datos informáticos o de usuario, el funcionamiento de un sistema informático o de una red de telecomunicaciones, será reprimido…"

De la redacción del artículo se advierte, que el legislador incluye nuevos verbos rectores y complementa el tipo penal del 207-B del vigente Código Penal, lo que en consecuencia permitiría sancionar nuevas conductas asociadas a la cibercriminalidad.

Consideraciones Finales:

Recalcamos una vez más que, a efectos de combatir la ciberdelincuencia, el Perú se ven en la necesidad de adherirse a Convenios como el de Budapest u otro tipo de normatividad internacional que permite evitar la sensación este tipo de conductas, que en muchos casos, generan en el colectivo una sensación de inseguridad legal; respetando siempre los Derechos Fundamentales.

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°-B - *Alteración, daño y destrucción de base de datos, sistema, red o programa de computadoras*

- **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 presente instrumento internacional, al cual siempre nos referimos a efectos de contar con normas que permitan combatir la cibercriminalidad, regula en sus Artículo 4° y 5° , define al delito de Daño Informático, como ataques a la integridad de los datos y del sistema respectivamente, indicando que se trata de una conducta deliberada e ilegítima que dañe, borre, deteriore o altere datos o sistemas informáticos.

- **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.
Una vez más indicamos que se trata de un Dictamen y no de una norma, solo que a fin de contar la perspectiva del legislador sobre materia de Cibercriminalidad, consideramos pertinente ubicarlo en esta sección de nuestro boletín, en ese orden de ideas debemos precisar que el Artículo 3° del Texto Sustitutorio del Dictamen, contempla la figura penal del Daño informático.

NOTICIAS

"EL CIBERCRIMEN SE CENTRA EN LAS EMPRESAS CON PRESENCIA EN INTERNET"

28 DE DICIEMBRE

Los ciberdelincuentes han enfocado sus amenazas a las empresas y al robo de información confidencial, según el último estudio de Panda sobre las tendencias de los delitos perpetrados en Internet. El informe también ha señalado que la mayoría de las nuevas infecciones provienen de troyanos.

La empresa de seguridad Panda Security ha recogido en su último informe trimestral una infografía con las tendencias más habituales del cibercrimen. Entre los ataques perpetrados entre julio y septiembre de 2012, han destacado el envío de 'spam' a Dropbox a finales del julio, así como el ataque doble a la web de la agencia de noticias Reuters en agosto, en la que los 'hackers' publicaron dos noticias falsas.

Blizzard, Adobe y Kt Corp (KSE: 030200.KS - noticias) también han sufrido ataques de este tipo durante el verano.

El estudio también ha señalado que los troyanos o archivos espía constituyen la mayoría de los archivos maliciosos de nueva creación. Los troyanos han ocupado el 72,58 por ciento de estas nuevas infecciones, seguidos por un 14,4 por ciento de virus y por un 10,53 por ciento de gusanos.

En cuanto a los países más afectados por los diversos tipos de 'malware', afortunadamente España no lidera el top ten de los más amenazados, aunque tampoco se encuentra en el ranking de los más seguros. Los más infectados son principalmente países asiáticos, mientras que los más seguros son europeos.

China ha encabezado la lista negra de los más afectados del trimestre, seguido por Corea del Sur, Turquía, Eslovaquia y Taiwán. En el lado contrario, Irlanda se ha descubierto como el país más seguro, seguido por Noruega, Suecia, Suiza y por el Reino Unido.

FUENTE: YAHOO
http://es.noticias.yahoo.com/cibercrimen-centra-empresas-presencia-internet-090011766.html

“LA CE CREA UN CENTRO ESPECÍFICO PARA LUCHAR CONTRA EL CIBERCRIMEN”

09 DE ENERO

La Comisión Europea (CE) presentó hoy el centro europeo contra el cibercrimen (EC3), a través del cual expertos en seguridad en la red intentarán poner coto a los 1.500 millones de euros que se defraudan cada año a los ciudadanos europeos, principalmente, por las compras por internet.

"Los ciberdelincuentes son inteligentes y rápidos. El EC3 nos ayudará a ser aún más listos y rápidos que ellos para poder contribuir a prevenir y combatir sus delitos", dijo en rueda de prensa la comisaria de Interior, Cecilia Malmstrom, que presentó el centro junto al director jefe del EC3, Troels Oerting.

El EC3, que se inaugurará oficialmente el viernes y estará ubicado en La Haya, dentro de las premisas de Europol, "dará un fuerte impulso a la capacidad de la UE (Unión Europea) para luchar contra la ciberdelincuencia y defender la existencia de una Internet libre, abierta y segura", añadió Malmstrom.

Oerting, que dirigirá un grupo de expertos en seguridad en la red, destacó que "para luchar contra el cibercrimen, que por naturaleza no respeta fronteras, y la gran habilidad de los delincuentes para ocultarse, tenemos que responder de manera flexible y adecuada".

En este sentido, apuntó que el EC3 "está diseñado para aportar sus conocimientos como centro de fusión de la información y de apoyo operativo forense y de investigación, pero también, por su capacidad para movilizar todos los recursos pertinentes en los Estados miembros de la UE".

La actividad del EC3 se centrará en las actividades ilegales que perpetran las bandas de crimen organizado ayudándose de la red, "especialmente en los ataques dirigidos contra las operaciones bancarias y otras actividades financieras en línea", destacó la Comisión en un comunicado.

También estará en el ojo de mira de los expertos luchar contra la pornografía infantil en línea y los delitos contra las infraestructuras informáticas de las administraciones de la UE.

Según el último Eurobarómetro encargado por la CE, los usuarios europeos siguen estando muy preocupados por la seguridad informática y por ello el 89 % de usuarios de internet evita desvelar información personal en la red.

El 12 % ha sido de hecho víctima de fraude en internet.

FUENTE: TERRA

http://noticias.terra.com/internacional/la-ce-crea-un-centro-especifico-para-luchar-contra-el-cibercrimen,70235fd65661c310VgnCLD2000000dc6eb0aRCRD.html

"FILIPINAS. PROTESTA CONTRA LEY DE PREVENCIÓN DEL CIBERCRIMEN"

15 DE ENERO

Blogueros filipinos, con máscaras tapando sus caras, participan en una protesta contra la implementación de la Ley de Prevención del CibercrImen frente al Tribunal Supremo de Manila, en Filipinas. Organizadores defensoras de los derechos humanos, abogados, organizaciones de medios de comunicación, y blogueros marcharon hacia la sede del Tribunal Supremo en protesta por la nueva ley, que consideran puede llevar a la censura y a la supresión de la libertad en Internet.

FUENTE: El Siglo de Durango.
http://www.elsiglodedurango.com.mx/noticia/419037.protesta-contra-ley-de-prevencion-del-cibercr.html

EL VIRUS DE "GRINGASHO"
15 DE ENERO

Delincuentes informáticos pretenden engañar a sus posibles víctimas, con la verdadera historia de amor de "Gringasho Y Jazmin".

Correos electrónicos con el más que sugerente título: "descubren videos sexuales entre Gringasho y Gringasha", vienen siendo enviados por internet.

Un grupo de Hackers vienen envidando correos electrónicos con un supuesto video sexual del joven sicario y su novia, una vez que estos falsos enlaces son abierto, infectan las computadoras con un virus conocido como "Troyano" capaz de robar información clasificada como claves bancarias o clonar páginas web de bancos e instituciones

FUENTE: ATV NOTCIAS.

http://play.tuteve.tv/videogaleria/programa/122416/2013-01-16-15012013

EVENTOS

SEMINARIO: VIRUS INFORMATICOS
Fecha: Domingo 20 de Enero
Lugar: Lima
URL: http://www.computo-forense.blogspot.com/

CURSO DE COMPUTO FORENSE (CNCF)
Fecha: Abril 2013
Lugar: Lima
URL: http://www.npros.com.pe/new/?q=cursos

CURSO FULL DAY DE HACKING LIBRE
Fecha: 27 de Enero de 2013
Lugar: Av. Agust[in de la Rosa Toro 883 San Luis.
URL: http://www.computo-forense.blogspot.com/
Twitter: @sedeforense

CONTACTO

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