



# CIBERSEGURIDAD EN COSTA RICA

Roberto Lemaître Picado

# **25 AÑOS DE LA PRIMERA CONEXIÓN A LA INTERNET EN COSTA RICA**

**26 DE ENERO 2018**

Finalmente, el 26 de Enero de 1993 se interconecta una docena de nodos ubicados en la Unidad de Redes, Centro de Informática, Escuela de Geología y Escuela de Física de la Universidad de Costa Rica con la Internet, utilizando el Punto de Presencia (PoP) de NSF en Homestead y un enrutador CISCO IGS en préstamo por la Universidad de Wisconsin.

**25 años de la Primera Conexión a la  
Internet en Costa Rica**

# ÍNDICE CIBER CRIME

## Estado de la Ciberseguridad Costa Rica

- El Índice Mundial de Ciberseguridad (IMC) es una medida del nivel de desarrollo de la ciberseguridad de cada Estado nación. El IMC pretende servir de acicate para que los países intensifiquen sus esfuerzos en materia de ciberseguridad. La meta final consiste en contribuir al fomento de una cultura mundial de ciberseguridad, así como a su integración como elemento fundamental de las tecnologías de la información y la comunicación.



Country	GCI Score	Legal	Technical	Organizational	Capacity Building	Cooperation
United States	0.91	1	0.96	0.92	1	0.73
Canada	0.81	0.94	0.93	0.71	0.82	0.70
Mexico	0.66	0.91	0.89	0.48	0.68	0.34

The top three ranked countries in the Americas region are the members of the North American Free Trade Association (NAFTA).

**The United States of America** has the highest scores for the legal and capacity building pillars. One notable aspect of both capacity building and cooperation in the country is the initiatives to coordinate cybersecurity among all states. To that end, the National Governor's Association established the Resource Center for State Cybersecurity, which offers best practices, tools and guidelines<sup>3</sup>.



**Canada** ranks second in the region with its highest score in the legal pillar. The country's Personal Information Protection and Electronic Documents Act (PIPEDA) features several sections relating to cybersecurity<sup>4</sup>. It requires organizations to notify privacy authorities in the event of privacy breaches that could cause significant damage





AMERICAS Region	Score	Global Rank
Jamaica	0.339	85
Costa Rica	0.336	86
Paraguay	0.326	87
Barbados	0.273	95
Guyana	0.269	98
El Salvador	0.208	108
Saint Vincent and the Grenadines	0.189	114
Belize	0.182	116
Antigua and Barbuda	0.179	117
Dominican Republic	0.162	122
Suriname	0.155	132
Nicaragua	0.146	125
Bahamas	0.137	129
Bolivia	0.122	134



Organization of  
American States  
More rights for more people



# Ciberseguridad

¿Estamos preparados  
en América Latina y el Caribe?

---

Informe Ciberseguridad 2016

# OTDER CYBER CRIME

## Educación



### Disponibilidad nacional de la educación y formación cibernéticas

Educación



Formación



### Desarrollo nacional de la educación de seguridad cibernética

### Desarrollo nacional de la educación de seguridad cibernética



### Formación e iniciativas educativas públicas y privadas

### Capacitación de empleados en seguridad cibernética



### Gobernanza corporativa, conocimiento y normas

### Comprensión de la seguridad cibernética por parte de empresas privadas y estatales



# OTDERS CYBER CRIME

## Política y estrategia



**Estrategia nacional de seguridad cibernética oficial o documentada**



## Defensa cibernética



**Desarrollo de la estrategia**

**Organización**

**Contenido**

**Estrategia**

**Organización**

**Coordinación**

# Estado de la Ciberseguridad Costa Rica

Marcos legales	
<b>Marcos jurídicos de seguridad cibernetica</b>	
Para la seguridad de las TIC	
Privacidad, protección de datos y otros derechos humanos	
Derecho sustantivo de delincuencia cibernetica	
Derecho procesal de delincuencia cibernetica	
Investigación jurídica	
Cumplimiento de la ley	
La fiscalía	
Tribunales	
Divulgación responsable de la información	
Divulgación responsable de la información	



# Estado de la Ciberseguridad Costa Rica

## Cultura y sociedad



### Mentalidad de seguridad cibernetica

En el gobierno



En el sector privado



En la sociedad



### Conciencia de seguridad cibernetica

Sensibilización



### Confianza en el uso de Internet

En los servicios en línea



En el gobierno electrónico



En el comercio electrónico



### Privacidad en línea

Normas de privacidad

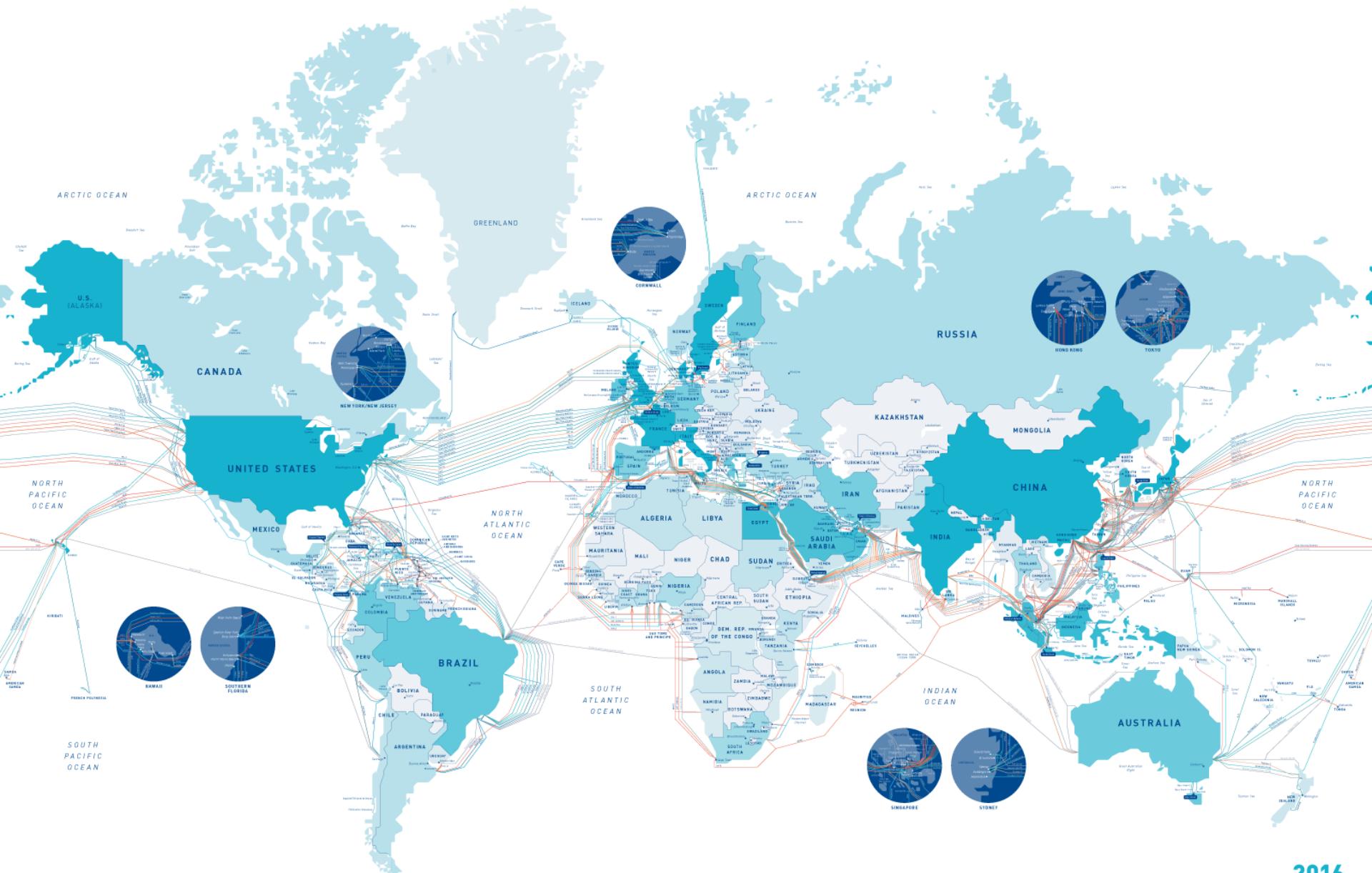


Privacidad del empleado



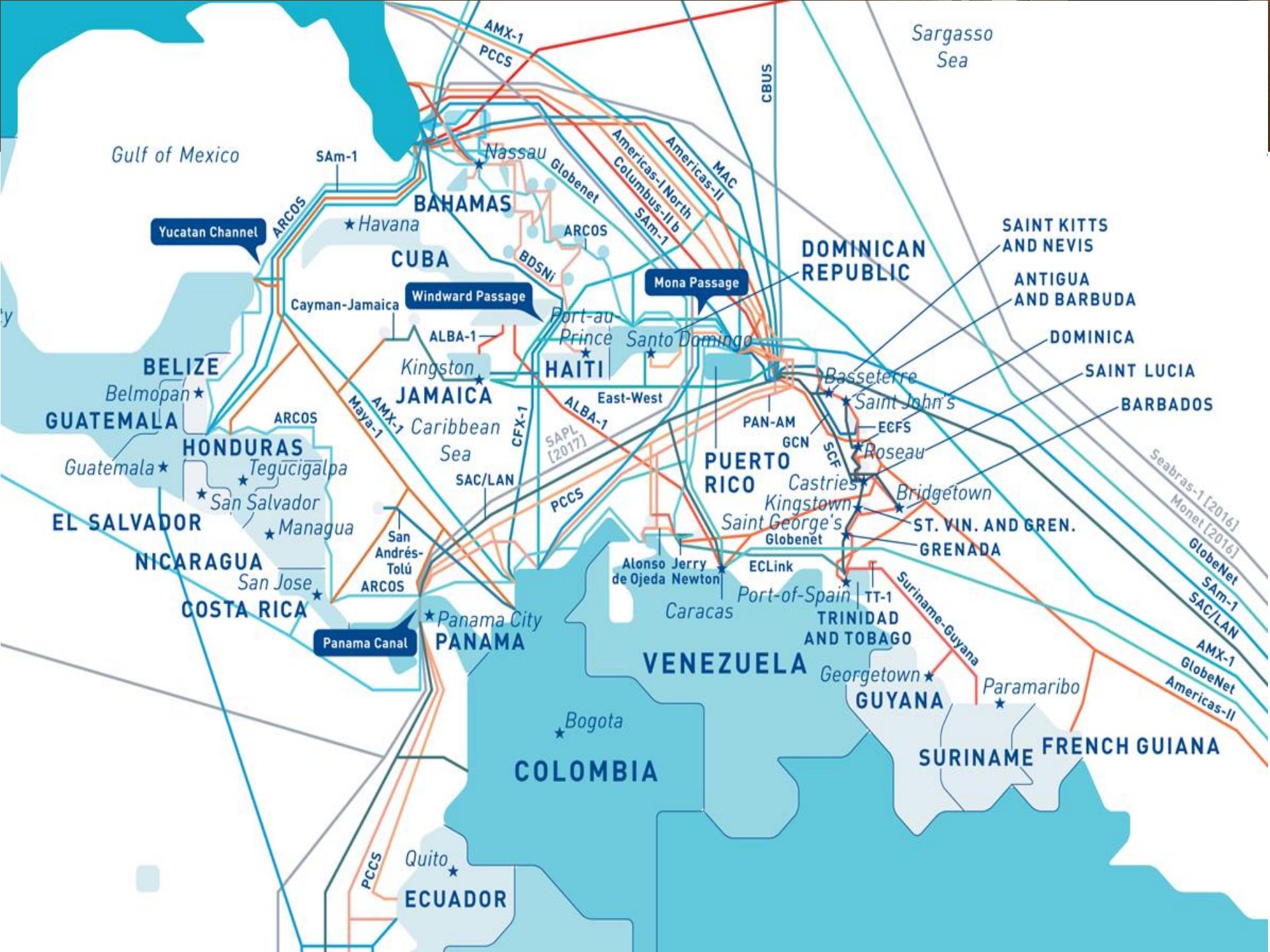
# La Guerra Silenciosa



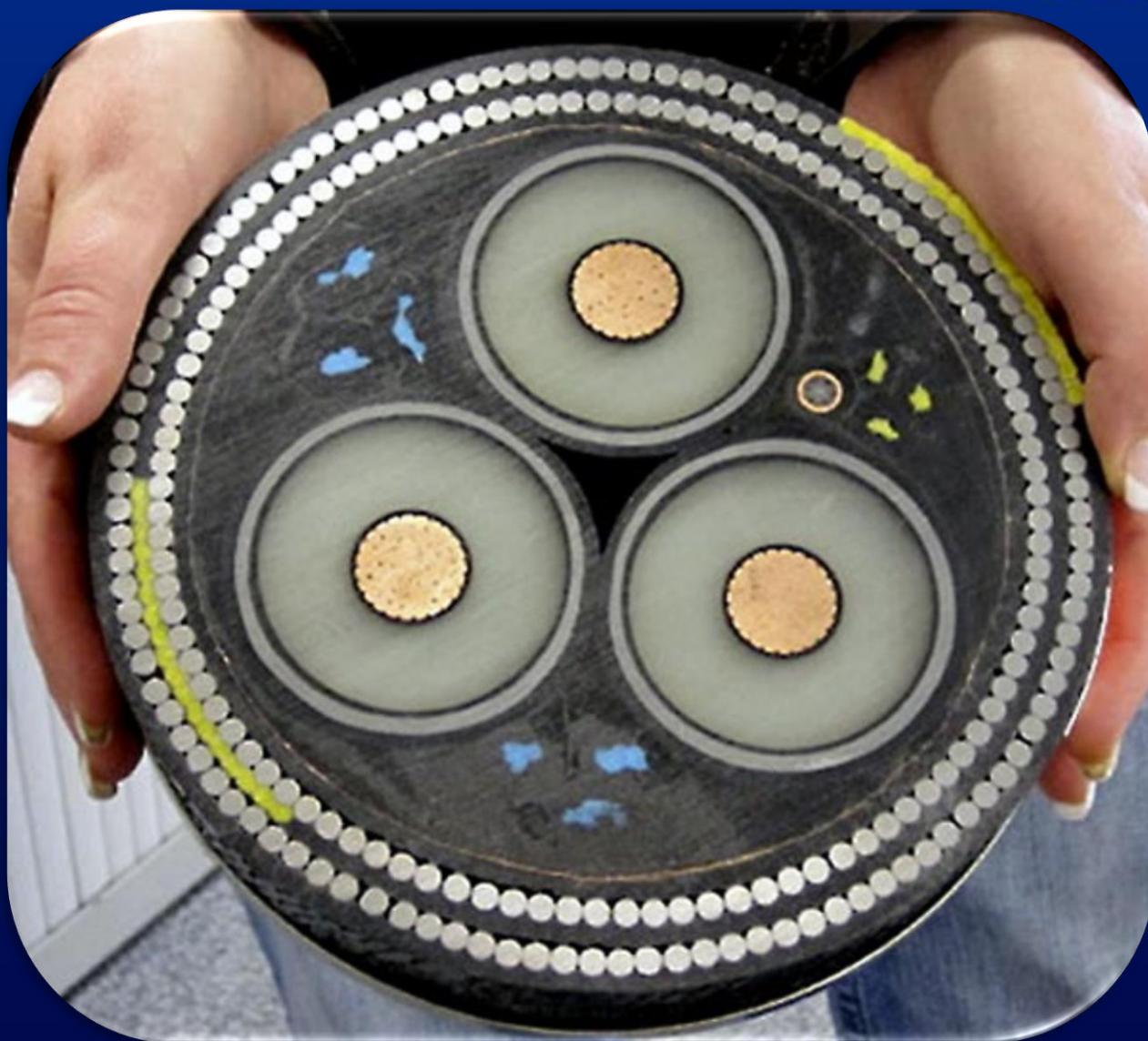


2016  
SUBMARINE CABLE MAP

WWW.TELEGEOGRAPHY.COM  
WWW.SUBMARINECABLEMAP.COM



**CYBER CRIME**



# ESTADÍSTICAS DEL SECTOR DE TELECOMUNICACIONES

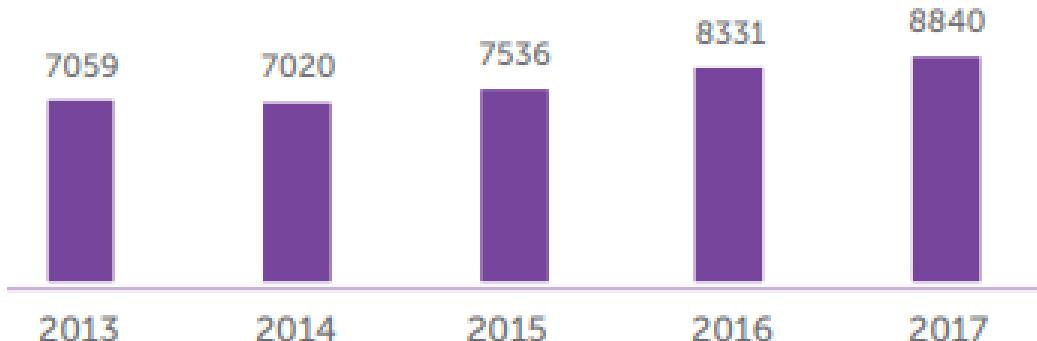
## COSTA RICA 2017



Gráfico N° 41

## Costa Rica. Suscripciones al servicio de telefonía móvil, 2013 -2017 (Cifras anuales en miles)

Las suscripciones crecieron un **6 %** con respecto al 2016.



Fuente: SUTEL, Dirección General de Mercados.

Gráfico N° 42

## Costa Rica. Suscripciones al servicio telefónico móvil por cada 100 habitantes, 2013-2017 (Cifras anuales en porcentajes)

La penetración de telefonía móvil alcanzada en el 2017 es la más alta en su historia:

**179 %**

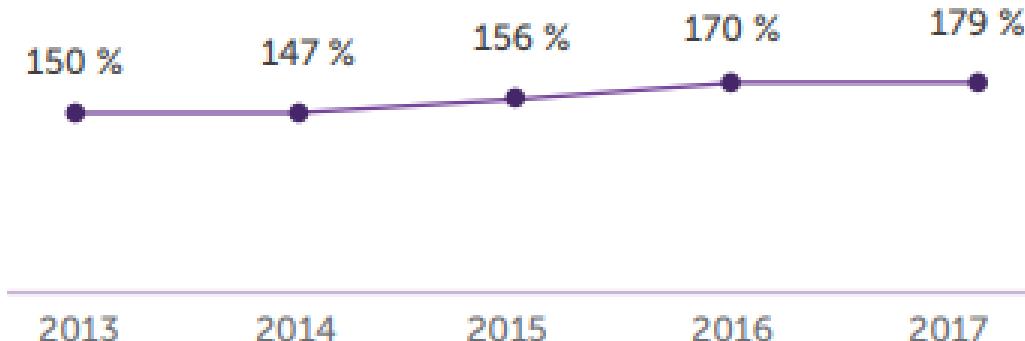
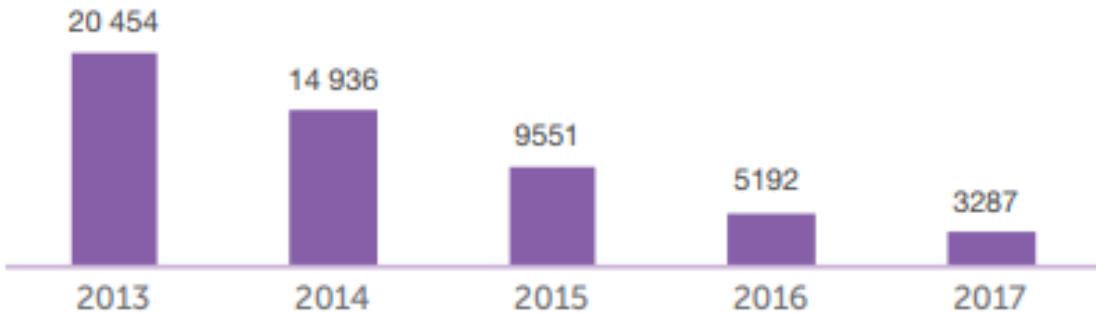


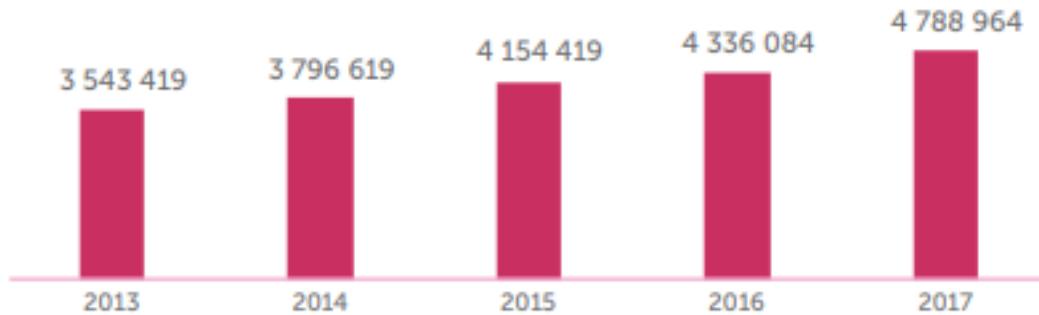
Gráfico N° 53  
Costa Rica. Tráfico total SMS, 2013-2017  
(Cifras anuales en millones de mensajes)

El número de SMS del  
2017 es solo el  
**16 %**  
de la cantidad registrada  
en el 2013.



Fuente: SUTEL, Dirección General de Mercados.

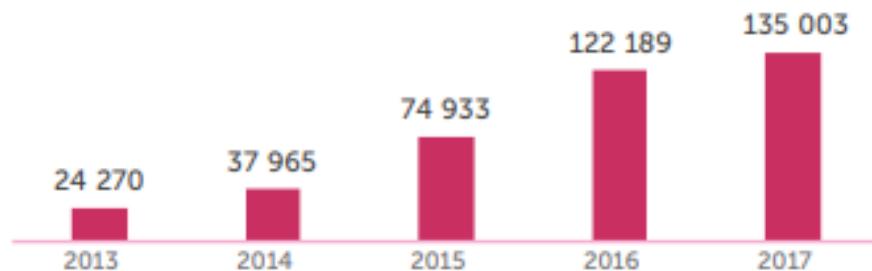
**Gráfico N° 65**  
**Costa Rica. Suscripciones, acceso a Internet en la red móvil, 2013-2017**  
(Cifras anuales)



Las suscripciones  
aumentaron un  
**10,4 %**  
del 2016 al 2017.

Fuente: SUTEL, Dirección General de Mercados.

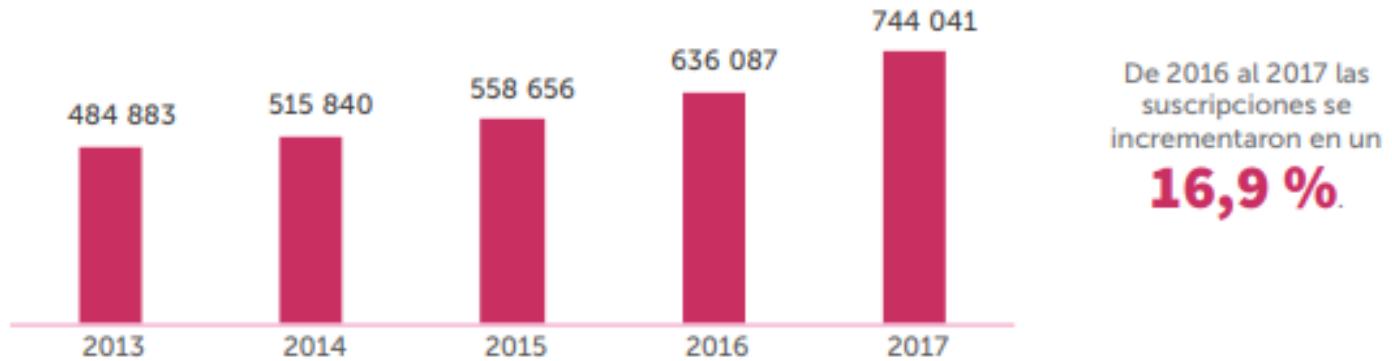
**Gráfico N° 71**  
**Costa Rica. Tráfico de datos, acceso a Internet en la red móvil, 2013-2017**  
(Cifras anuales en TB)



De 2016 a 2017 el tráfico de datos incrementó en un  
**10,4 %.**

Fuente: SUTEL, Dirección General de Mercados.

**Gráfico N° 79**  
**Costa Rica. Suscripciones, acceso a Internet fijo, por año, 2013-2017**  
(Cifras anuales)



Fuente: SUTEL, Dirección General de Mercados.



¿Qué está pasando en este 2018?

## Malware oculto en tráfico cifrado

Los ciber-delincuentes utilizan técnicas de cifrado como método para evitar su detección ocultando la actividad command-and-control. El malware detectado utilizando comunicaciones de red cifradas entre noviembre de 2016 y octubre de 2017 (12 meses) se ha multiplicado por más de tres pasando del 19% al 70%.

A yellow crime scene tape with the word "CRIME" printed on it in large, bold, black capital letters. The tape is diagonally positioned across the left side of the slide. In the background, there is a blue area with binary code (0s and 1s) visible.

# ¿Qué está pasando en este 2018?

## Ransomware basado en red

En 2017 proliferaron los gusanos de ransomware basados en red. Esto elimina la necesidad del elemento humano y facilita la auto-propagación. Además, estos ciber-ataques a menudo se “disfrazan” de ransomware cuando el objetivo principal es la destrucción de los sistemas, servicios y datos (ejemplo: Nyetya), con la posibilidad incluso de ‘destruir’ Internet.



¿Qué está pasando en este 2018?

## Botnets IoT y DDoS

Los botnets IoT (redes zombie de dispositivos IoT) están creciendo tanto en tamaño como en alcance y potencia. Se utilizan para lanzar ataques de denegación de servicio (DDoS) que además aprovechan la capa de aplicaciones. No obstante, sólo el 13% de las organizaciones (cifra global) ven los botnets IoT como una amenaza inminente, y siguen añadiendo dispositivos IoT a sus redes en volumen y sin seguridad IoT.

# TENDENCIAS EN CIBERSEGURIDAD 2018: EL COSTO DE NUESTRO MUNDO CONECTADO



ENJOY SAFER TECHNOLOGY™



# Tendencias 2018

- La revolución del ransomware
- Aumentan los ataques a infraestructuras críticas
- Ataques a la democracia: ¿puede haber procesos electorales seguros?
- La policía y la investigación contra el malware se unen en la lucha
- La información personal en la nueva era de la tecnología y la legislación

## ¿A dónde crees que dirigirán sus ataques los cibercriminales?

Cree muy posible que haya un nuevo Wannacry

75%

71% de los encuestados cree que los cibercriminales seguirán apuntando a las grandes empresas que manejan datos sensibles

Más del **60%** de los encuestados dijo que se protegerá mejor



## ¿A qué se debieron los incidentes del último año?



**2017**



**50%** culpa a las empresas

**21%** culpa al desconocimiento del usuario

## ¿Deberían las empresas invertir en otros controles de seguridad?



**21,7%**  
Perímetros  
de red



Casi el **50%** cree que  
se debería capacitar  
a los colaboradores



**18,3%**  
Cifrado

La clave está en entender el desafío

# MULTIPLES DISPOSITIVOS



La clave está en entender el desafío

# MULTIPLES DISPOSITIVOS



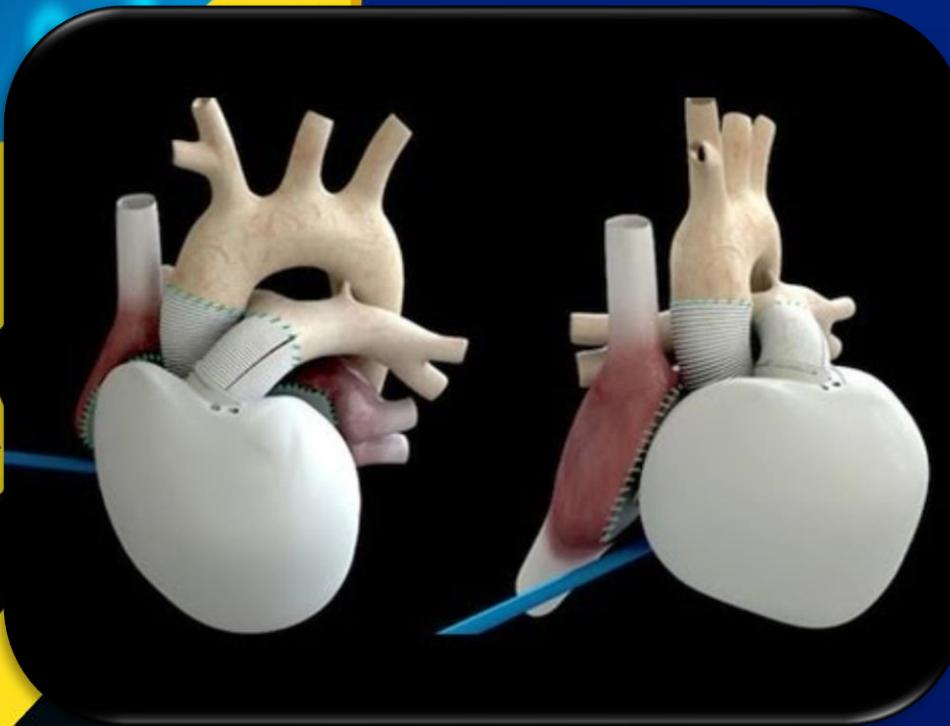
**Analistas aseguran que  
hackers usaban un  
refrigerador para enviar spam**

17 ENERO 2014

(CC) Rich Ande

La clave está en entender el desafío

## MULTIPLES DISPOSITIVOS



French company Carmat developed an artificial heart.

It was first implanted in December 2013.

It has Wireless capabilities

La clave está en entender el desafío

# MULTIPLES DISPOSITIVOS

El lado criminal de la tecnología: Europol advierte sobre la cercanía del primer ciberaSESINATO

11.10.2014



A+ A-

El [organismo europeo indica que](#) "a medida que haya más objetos conectados y nuevos tipos de infraestructura crítica, podemos esperar más ataques tanto contra las infraestructuras ya existentes como en las emergentes, incluyendo nuevas formas de chantaje o extorsión y ataques físicos con posibilidad de muerte". El desarrollo de dispositivos inteligentes y la evolución del Internet de las cosas, con un mayor número de objetos y viviendas conectados a la red, aumenta el número de amenazas.

**La evolución del Internet de las cosas aumenta el número de amenazas.**

La agencia estadounidense del medicamento (FDA) reconoció públicamente la vulnerabilidad de dispositivos como bombas de insulina, desfibriladores, ventiladores mecánicos o monitores, cuyos sistemas informáticos podrían ser víctima de virus y otro tipo de 'malware'.

CRIME

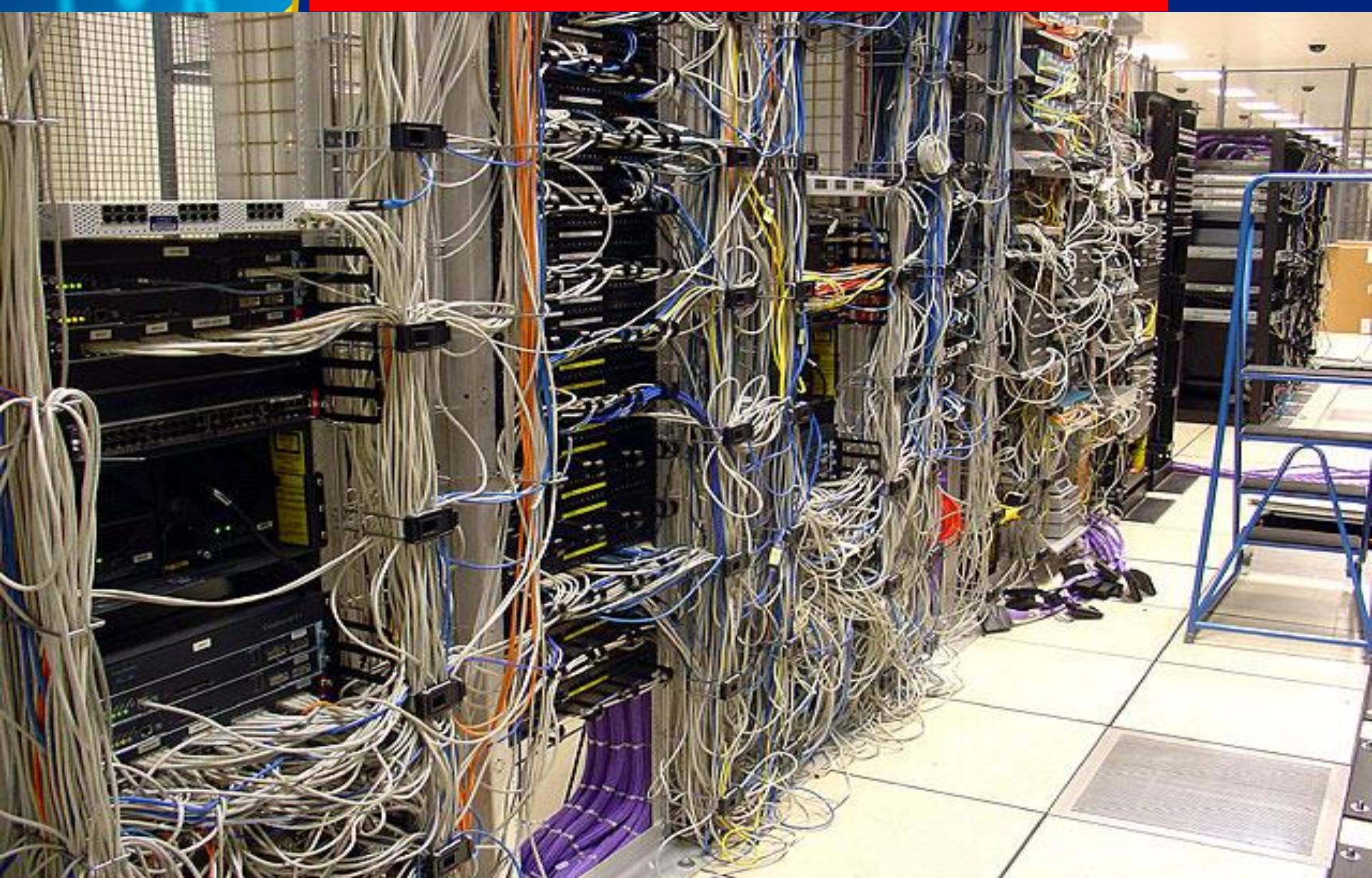


# La clave está en entender el desafío **EL LUGAR DEL DELITO**



La clave está en entender el desafío

# EL LUGAR DEL DELITO



# EL CIBERCRIMEN

SI EL CIBERCRIMEN FUERA UNA  
INDUSTRIA LEGÍTIMA, SERÍA LA  
SEGUNDA MÁS GRANDE  
DETRÁS DE APPLE

**450 mil millones** de dólares  
al año



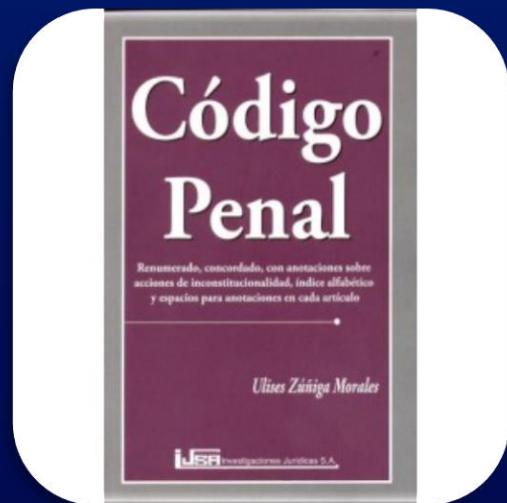
# Marco Normativo



CRIME

OTDER CYBER CRIME

# Código Penal de Costa Rica Reúne el Marco Punitivo del Estado costarricense



# **CYBER CRIME**

## **Artículo 167 bis.- Seducción o encuentros con menores por medios electrónicos.**

Será reprimido con prisión de **uno a tres años** a quien, por cualquier medio, establezca comunicaciones de contenido sexual o erótico, ya sea que incluyan o no imágenes, videos, textos o audios, con una **persona menor de quince años o incapaz**.

# **CYBER CRIME**

## **Artículo 167 bis.- Seducción o encuentros con menores por medios electrónicos.**

La **misma pena** se impondrá a quien **suplantando la identidad de un tercero o mediante el uso de una identidad falsa**, por cualquier medio, procure establecer comunicaciones de contenido sexual o erótico, ya sea que se incluyan o no imágenes, videos, textos o audios, con una persona menor de edad o incapaz.

# **CYBER CRIME**

## **Artículo 167 bis.- Seducción o encuentros con menores por medios electrónicos.**

La pena será de **dos a cuatro años**, en las conductas descritas en los dos párrafos anteriores, **cuando el actor procure un encuentro personal** en algún lugar físico con una persona menor de edad incapaz.

# Allanaron casa de sospechoso de seducir menor a través de Facebook para luego violarla

- Hecho se dio el jueves anterior, en Curridabat

20 DE ABRIL DE 2015

3:59 PM

ANGIE GUERRERO

Escriba al periodista

## Compartir

 Recomendar 1384

 Twittear

 Correo

 Imprimir

Agentes del Organismo de Investigación Judicial (OIJ) decomisaron equipos electrónicos y el celular de un hombre de apellido Brenes, de 42 años, sospechoso de seducir menores a través de redes sociales.

través de redes sociales y de violación en perjuicio de una



Imagen de la detención de un hombre de apellido Brenes, de 42 años, sospechoso de seducir jóvenes por medio de redes sociales. Cortesía OIJ.

## Temas

# **CYBER CRIME**

## **Artículo 196.- Violación de correspondencia o comunicaciones**

Será reprimido con pena de prisión de **uno a tres años** a quien, con peligro o daño para la **intimidad o privacidad** de otro, y sin su autorización, se **apodere, acceda, modifique, altere, suprima, intervenga, intercepte, abra, entregue, venda, remita o desvíe** de su destino documentación o comunicaciones dirigidas a otra persona.

# **OTROS CRIMES Y CYBER CRIME**

## **Artículo 196.- Violación de correspondencia o comunicaciones**

La misma sanción indicada en el párrafo anterior se impondrá a quien, con peligro o daño para la intimidad de otro, **utilice o difunda el contenido de comunicaciones o documentos privados que carezcan de interés público.**

La misma pena se impondrá a quien promueva, **incite, instigue, prometa o pague un beneficio patrimonial a un tercero** para que ejecute las conductas descritas en los dos párrafos anteriores.

# OT DE DÍA A CRIMEN CYBER CRIME

## Artículo 196.- Violación de correspondencia o comunicaciones

La pena será de **dos a cuatro años** de prisión si las conductas descritas en el primer párrafo de este artículo son realizadas por:

- a) Las personas encargadas de la recolección, entrega o salvaguarda de los documentos o comunicaciones.

# ARTÍCULO 196 CYBER CRIME

## Artículo 196.- Violación de correspondencia o comunicaciones

La pena será de **dos a cuatro años** de prisión si las conductas descritas en el primer párrafo de este artículo son realizadas por:

- b) Las personas encargadas de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tengan acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.

[Imprimir](#)[Enviar](#)

# Marido condenado por robar mensajes a esposa para divorcio

POR HULDA MIRANDA P. / hulda.miranda@nacion.com - Actualizado el 3 de marzo de 2015 a: 12:00 a.m.

- Hombre reenvió conversaciones del celular de cónyuge y les tomó fotos
- Jueza también lo castigó a pagar ¢5 millones a mujer y a amigo de ella

## MAS SOBRE ESTE TEMA

### NOTICIA

Publicar mensajes privados puede castigarse con cárcel

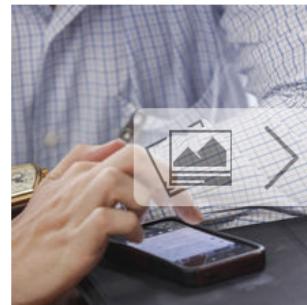
## ETIQUETAS

[MENSAJES](#)[PRIVADOS](#)[CÁRCEL](#)[JUAN GABRIEL GUZMÁN](#)[DELITOS](#)

SUSCRÍBASE A EDICIÓN VESPERTINA  
Y reciba actualizaciones diarias

 Correo electrónico ENVIAR Acepto condiciones[VER OTROS BOLETINES](#)

Con la intención de recabar prueba sobre una supuesta infidelidad, en medio de un proceso de divorcio, un empleado bancario robó mensajes de texto del celular de su esposa.



El esposo obtuvo un beneficio para no ir a la cárcel. | ARCHIVO.  Ampliar

La pareja finalmente se separó por mutuo acuerdo, pero luego el exesposo fue demandado por el delito de violación a las comunicaciones y condenado a seis meses de cárcel. Se le concedió un beneficio de ejecución condicional y quedó libre.

No obstante, también se le ordenó pagar ¢2,5 millones a su excompañera y la misma cantidad a un amigo de ella, quien había enviado los mensajes de texto.

La sentencia la dictó el Tribunal Penal de Cartago, el 8 de setiembre del año pasado.

El caso de este matrimonio pone en evidencia un riesgo que algunos desconocen: adueñarse de comunicaciones privadas o publicarlas, puede ser castigado, incluso con prisión.

## PUBLICIDAD



## ÚLTIMAS NOTICIAS

03:31 P.M. Tráiler de Star Wars: impresiones de un fanático

03:25 P.M. Ministro de Ambiente señala a Gobiernos de Arias y Chinchilla por problemas con refinadora china

03:17 P.M. El Arsenal se mantiene vivo en la Champions con triunfo sobre el Bayern Múnich

03:15 P.M. Pequeña mosca asiática siembra el

 MÁS

# OTIENDA CRIMINAL CYBER CRIME

## Artículo 196 bis.- Violación de datos personales

Será sancionado con pena de prisión de **uno a tres años** quien en beneficio propio o de un tercero, con peligro o daño para la **intimidad o privacidad** y sin la autorización del titular de los datos, **se apodere, modifique, interfiera, acceda, copie, transmita, publique, difunda, recopile, inutilice, intercepte, retenga, venda, compre, desvíe** para un fin distinto para el que fueron recolectados o dé un tratamiento no autorizado a las imágenes o datos de una persona física o jurídica almacenados en sistemas o redes informáticas o telemáticas, o en contenedores electrónicos, ópticos o magnéticos.

# OTI DEDICATED TO CYBER CRIME

## Artículo 196 bis.- Violación de datos personales

La pena será de **dos a cuatro años** de prisión cuando las conductas descritas en esta norma:

- a) Sean realizadas por personas encargadas de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tengan acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.
- b) La información vulnerada corresponda a un menor de edad o incapaz.
- c) Las conductas afecten datos que revelen la ideología, la religión, las creencias, la salud, el origen racial, la preferencia o la vida sexual de una persona.

# OT DE DÍA A CRIMEN CYBER CRIME

## Artículo 196 bis.- Violación de datos personales

**No constituye delito** la publicación, difusión o transmisión de información de interés público, documentos públicos, datos contenidos en registros públicos o bases de datos públicos de acceso irrestricto cuando se haya tenido acceso de conformidad con los procedimientos y limitaciones de ley.

Tampoco constituye delito la recopilación, copia y uso por parte de las entidades financieras supervisadas por la Sugef de la información y datos contenidos en bases de datos de origen legítimo de conformidad con los procedimientos y limitaciones de ley."

# Marcela Negrini asegura que fotos que se filtraron fueron robadas del celular de su exnovio

13 DE ABRIL DE 2015

1:44 PM

YASLIN CABEZAS

Escriba al periodista

## Compartir

 Me gusta

172

 Twittear

 Correo

 Imprimir



Imagen tomada del Facebook de Marcela Negrini

La modelo Marcela Negrini aseguró por medio de su perfil de Facebook que las fotografías que se filtraron durante este fin de semana –en donde se observa semidesnudas– fueron robadas del celular de su exnovio.

La mujer, oriunda de Orotina, reconoce que sí es ella la que sale en las imágenes y que no se trata de un montaje, pero que no sabía que se las habían tomado.

# OTIDED K CRIME CYBER CRIME

## Artículo 214.- Extorsión

Será reprimido con pena de prisión de **cuatro a ocho años** al que para procurar un lucro obligue a otro, con intimidación o con amenazas graves, a tomar una disposición patrimonial perjudicial para sí mismo o para un tercero.

La pena será de **cinco a diez años** de prisión cuando la conducta se realice valiéndose de **cualquier manipulación informática, telemática, electrónica o tecnológica.**"



# Aumentan denuncias por extorsión sexual vía Internet

ENERO 31, 2017 10:49 AM | JOHEL SOLANO 



El **Organismo de Investigación Judicial (OIJ)** registró un total de **80 casos de extorsión sexual** a través de internet en el último año.

Según explicó Erick Lewis, director de la Unidad de Delitos Informáticos del OIJ, los delincuentes son bandas extranjeras que **por medio de redes sociales convencen a hombres de mantener "sexo virtual"**.

"Son perfiles de Facebook con una creación muy corta. No hay amigos en común y sin tener ningún tipo de relación empiezan

a interactuar y luego pasan a utilizar sistemas de video llamadas como Skype donde son grabados", señaló Lewis.

# OT DE DÍA CRIMEN CYBER CRIME

## Artículo 217 bis.- Estafa informática

Se impondrá prisión de **tres a seis años** a quien, en perjuicio de una **persona física o jurídica**, manipule o influya en el **ingreso**, en el **procesamiento** o en el **resultado** de los datos de un sistema automatizado de información, ya sea mediante el **uso de datos falsos o incompletos**, el **uso indebido de datos, programación**, valiéndose de **alguna operación informática o artificio tecnológico**, o bien, por cualquier otra acción que incida en el procesamiento de los datos del sistema o que dé como resultado **información falsa, incompleta o fraudulenta**, con la cual procure u obtenga un beneficio patrimonial o indebido para sí o para otro.

# **CYBER CRIME**

## **Artículo 217 bis.- Estafa informática**

La pena será de **cinco a diez años** de prisión, si las conductas son cometidas contra **sistemas de información públicos, sistemas de información bancarios y de entidades financieras**, o cuando el **autor es un empleado encargado de administrar o dar soporte al sistema o red informática o telemática**, o bien, **que en razón de sus funciones tenga acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos**.

# Cae banda de estudiantes de Informática por estafas con tarjetas de crédito en Liberia

Los sospechosos tienen 19 años; ninguno cuenta con antecedentes criminales

Cuatro estudiantes que se dedicaban a comprar en tiendas y ventas de comidas con tarjetas de terceros cayeron este miércoles en manos del Organismo de Investigación Judicial (OIJ).

Según la Policía Judicial, se trata de jóvenes de 19 años que estudiaron Informática en diferentes universidades tanto públicas como privadas.

Los sospechosos son de apellidos Castillo, Chaves Lira y Rugama. En apariencia los cuatro son vecinos de Upala y estudian en la misma universidad para poder estudiar. Ninguno cuenta con antecedentes criminales.

Según la pesquisa, los muchachos obtenían información de las tarjetas de crédito de los clientes y con esos datos hacían compras en Internet. En este momento ya fueron detenidos y acusados por estafa informática con un perjuicio que ronda ¢1.500 millones.



Los allanamientos fueron realizados en los barrios Los Cedros, IMAS y La Guardia, además de otro en el distrito de Cañas Dulces. Foto: Cortesía OIJ.

# **CYBER CRIME**

## **Artículo 229 ter.- Sabotaje informático**

Se impondrá pena de prisión de **tres a seis años** al que, en provecho propio o de un tercero, **destruya, altere, entorpezca o inutilice la información contenida en una base de datos**, o bien, impida, altere, obstaculice o modifique sin autorización el funcionamiento de un sistema de tratamiento de información, sus partes o componentes físicos o lógicos, o un sistema informático.

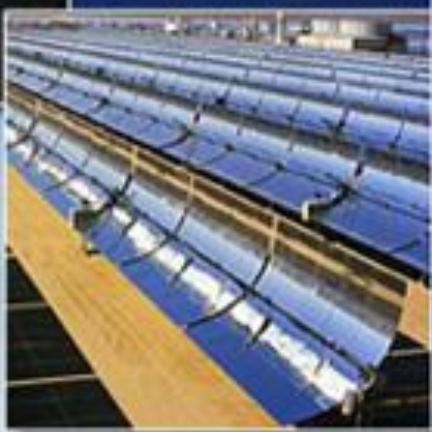
# **OTROS CRIMENES CYBER CRIME**

La pena será de **cuatro a ocho años** de prisión cuando:

- a) **Peligro colectivo** o daño social.
- b) La conducta se realice por parte de un empleado **encargado de administrar** o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus **funciones tenga acceso a dicho sistema o red**, o a los contenedores electrónicos, ópticos o magnéticos.

# OTDERS CYBER CRIME

- c) El sistema informático sea de **carácter público** o la información esté contenida en bases de datos públicas.
- d) Sin estar facultado, emplee medios tecnológicos que impidan a personas autorizadas el acceso lícito de los sistemas o redes de telecomunicaciones.



# **OTROS CRIMENES Y CYBER CRIME**

## **Artículo 230.- Suplantación de identidad**

Será sancionado con pena de prisión de uno a tres años **quien suplante la identidad de una persona física, jurídica o de una marca comercial en cualquiera red social, sitio de Internet, medio electrónico o tecnológico de información.**

# Aumentan denuncias por suplantación de identidad en Costa Rica

- A agosto del 2013 se superó el corte final del año anterior

29 DE SEPTIEMBRE DE 2013

12:02 AM

DANIELA GARCÍA

 Escriba al periodista

## Compartir



Hasta agosto de este año, se presentaron todo el 2013.

aumentan consistencia año. Incluso, en el determinó que las interuestas en el 20

22 DE FEBRERO DE 2015

12:04 AM

YASLIN CABEZAS

Escriba al periodista

## Compartir



## Temas

- OIJ dice que para minimizar problema, operadoras deben pedir copia de cédula, huella dactilar o en su defecto entregar las líneas solo en las agencias
- Telefonía Claro dice que para ellos no es suplantación de identidad



Imagen ilustrativa. (AP Photo/Sang Tan, File)

Lamentablemente la suplantación de identidad con líneas prepago se sigue presentando en el país, el Organismo de Investigación Judicial (OIJ) sigue recibiendo

denuncias de personas afectadas. Sin embargo, la mayoría de investigaciones no llegan a nada porque no se logra dar con los responsables.

# **CYBER CRIME**

## **Artículo 232.- Instalación o propagación de programas informáticos maliciosos**

Será sancionado con prisión de **uno a seis años** quien sin autorización, y por cualquier medio, **instale programas informáticos maliciosos en un sistema o red informática o telemática**, o en los contenedores electrónicos, ópticos o magnéticos.

# **CYBER CRIME**

La misma pena se impondrá en los siguientes casos:

- a) A quien induzca a error a una persona para que instale un programa informático malicioso en un sistema o red informática o telemática, o en los conten edores electrónicos, ópticos o magnéticos, sin la debida autorización.

# **CYBER CRIME**

La misma pena se impondrá en los siguientes casos:

**b)** A quien, sin autorización, instale programas o aplicaciones informáticas dañinas en sitios de Internet legítimos, con el fin de convertirlos en medios idóneos para propagar programas informáticos maliciosos , conocidos como sitios de Internet atacantes.

# OTROS CRIMENES CYBER CRIME

La misma pena se impondrá en los siguientes casos:

- c) A quien, para propagar programas informáticos maliciosos, invite a otras personas a descargar archivos o a visitar sitios de Internet que permitan la instalación de programas informáticos maliciosos.
  
- d) A quien distribuya programas informáticos diseñados para la creación de programas informáticos maliciosos.

# **OTROS CRIMENES CYBER CRIME**

La misma pena se impondrá en los siguientes casos:

- e) A quien ofrezca, contrate o brinde servicios de de negación de servicios, envío de comunicaciones masivas no solicitadas, o propagación de programas informáticos maliciosos.

# OTROS CRIMENES Y CYBER CRIME

La pena será de **tres a nueve años** de prisión cuando el programa informático malicioso:

- i) Afecte a una entidad bancaria, financiera, cooperativa de ahorro y crédito, asociación solidarista o ente estatal.
- ii) Afecte el funcionamiento de servicios públicos.

# OTI DEDICATED TO CYBER CRIME

La pena será de tres a nueve años de prisión cuando el programa informático malicioso:

- iii) Obtenga el control a distancia de un sistema o de una red informática para formar parte de una red de ordenadores zombi.
- iv) Esté diseñado para realizar acciones dirigidas a procurar un beneficio patrimonial para sí o para un tercero.

# **CYBER CRIME**

La pena será de tres a nueve años de prisión cuando el programa informático malicioso:

- v) Afecte sistemas informáticos de la salud y la afectación de estos pueda poner en peligro la salud o vida de las personas.
- vi) Tenga la capacidad de reproducirse sin la necesidad de intervención adicional por parte del usuario legítimo del sistema informático.

SEGÚN OIJ ERA ESTUDIANTE DE LA UNA

# Estudiante de informática buscado por el FBI se dedicaba a propagar programas maliciosos

- Operaba de manera individual en una red internacional
- Investigarán evidencia para determinar si empresas nacionales o internacionales fueron afectadas

14 DE JULIO DE 2015

11:08 AM

JOSELYNE UGARTE

Escriba al periodista

## Compartir

 Recomendar

4

 Twittear

 Correo

 Imprimir

## Temas

SUCESOS



Imagen ilustrativa. OIJ.

Esta mañana el Organismo de Investigación Judicial (OIJ), realizó la detención de un joven de apellidos Rivera Sánchez de 24 años de edad, quien era buscado por la Oficina Federal de Investigaciones de los Estados Unidos (FBI, por sus siglas en inglés), como sospechoso de instalación o propagación de programas maliciosos.

Unidos (FBI, por sus siglas en inglés), como sospechoso de instalación o propagación de programas maliciosos.

# OT DE DÍA CRIMEN CYBER CRIME

## Artículo 233.- Suplantación de páginas electrónicas

Se impondrá pena de prisión de **uno a tres años** a quien, en perjuicio de un tercero, **suplante sitios legítimos de la red de Internet**.

La pena será de **tres a seis años** de prisión cuando, como consecuencia de la suplantación del sitio legítimo de Internet y mediante engaño o haciendo incurrir en error, **capture información confidencial de una persona física o jurídica para beneficio propio o de un tercero**.

# Banco de Costa Rica advierte de correo fraudulento

14 DE AGOSTO DE 2013

10:08 AM

MARÍA SIU

Escriba al periodista

## Compartir

Recomendar 1

Twittear

Correo

Imprimir

## Temas

NACIONALES

El Banco de Costa Rica (BCR) advierte a la población que delincuentes aprovechan de la cercanía de la celebración del día de la madre, y están haciendo circular un correo electrónico que redirige a los clientes a un sitio fraudulento ("phishing") en donde luego de digitar el nombre de usuario y clave de [bancobcr.com](http://bancobcr.com), les solicita la dirección de correo electrónico en donde reciben notificaciones de la entidad; todo esto con la intención evidente de poder prematricular la cuentas para luego cometer el fraude.



El BCR alertó de posibles correos fraudulentos

# **ARTÍCULO 234.- CYBER CRIME**

## **Artículo 234.- Facilitación del delito informático**

Se impondrá pena de prisión de **uno a cuatro años** a quien facilite los medios para la consecución de un delito efectuado mediante un sistema o red informática o telemática, o los contenedores electrónicos, ópticos o magnéticos.

# Banda sospechosa de cometer millonario fraude informático a juicio

29 DE AGOSTO DE 2012

10:38 AM

AGENCIA/REDACCIÓN

Escriba al periodista

## Compartir

 Recomendar

0

 Twittear

 Correo

 Imprimir



Imagen con fines ilustrativos. CRH

Una supuesta banda que habría cometido una serie de delitos informáticos entre el 2007 y el 2008 irá a juicio en octubre. Los sospechosos habrían afectado a clientes bancarios

del país con más de 110 millones de colones.

Las transacciones bancarias las realizaban desde diversos café internet, para impedir que la direcciones IP de las computadoras fueran localizados por las autoridades. Los recursos eran transferidos a cuentas personales de los llamados "frenteadores", a quienes se reclutaba y les pagaba un monto por prestar dicha cuenta y retirar el dinero, el mismo día de la transferencia, para entregar los montos a los "cabecillas" de la organización. Según las investigaciones, estas personas que prestaban sus cuentas, tenían conocimiento del ilícito.

# OT DEP CYBER CRIME

## Artículo 295.- Espionaje.

Será reprimido con prisión de uno a seis años a quien procure u obtenga indebidamente secretos de Estado debidamente decretados relativos a la seguridad interna o externa de la nación, la defensa de la soberanía nacional y las relaciones exteriores de Costa Rica.

# **CYBER CRIME**

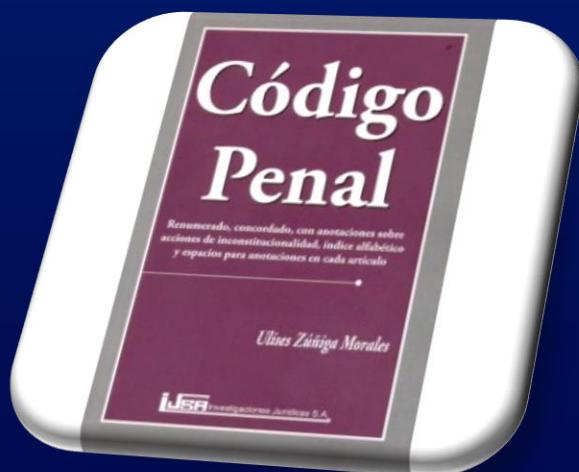
## **Artículo 295.- Espionaje.**

La pena será de dos a ocho años de prisión cuando la conducta se realice mediante manipulación informática, programas informáticos maliciosos o por el uso de tecnologías de la información y la comunicación.

# CÓDIGO PENAL CYBER CRIME

## Código Penal de Costa Rica Ley 9177

**REFORMA DE LOS ARTÍCULOS 173, 173 BIS Y 174 Y ADICIÓN  
DE UN ARTÍCULO 174 BIS AL CÓDIGO PENAL, LEY N.º 4573,  
Y REFORMA DEL INCISO 3) Y DEL PÁRRAFO FINAL  
DEL ARTÍCULO 61 DE LA LEY N.º 8764, LEY  
GENERAL DE MIGRACIÓN Y EXTRANJERÍA**



# **OTROS CRIMENES Y CYBER CRIME**

## **Artículo 173.- Fabricación, producción o reproducción de pornografía**

Será sancionado con **pena de prisión de cuatro a ocho años**, quien **fabrique, produzca o reproduzca**, por cualquier medio, material pornográfico infantil.

Será sancionado con pena de prisión de **tres a seis años**, quien **transporte o ingrese en el país este tipo de material**.

# **CYBER CRIME**

**Artículo 173 bis.- Tenencia de material pornográfico**

Será sancionado con pena de prisión de uno a cuatro años, quien posea material pornográfico infantil.

# **CYBER CRIME**

## **Artículo 174.- Difusión de pornografía**

Quien **entregue, comercie, difunda, distribuya o exhiba** material pornográfico a personas menores de edad o incapaces, será sancionado con pena de prisión de **tres a siete años**.

# **CIBER CRIME**

## **Artículo 174.- Difusión de pornografía**

Se impondrá pena de **cuatro a ocho años**, a quien **exhiba, difunda, distribuya, financie o comercialice**, por cualquier medio y cualquier título, material pornográfico en el que aparezcan personas menores de edad o lo posea para estos fines."

# **CYBER CRIME**

## **Artículo 174 bis.- Pornografía virtual y pseudo pornografía**

Se impondrá pena de prisión **de seis meses a dos años** al que **posea, produzca, venda, distribuya, exhiba o facilite**, por cualquier medio, material pornográfico en el que **no habiendo utilizado personas menores de edad**:

- **Emplee a una persona adulta que simule ser una persona menor de edad realizando actividades sexuales.**

# **CYBER CRIME**

## **Artículo 174 bis.- Pornografía virtual y pseudo pornografía**

**Emplee imagen, caricatura, dibujo o  
representación, de cualquier clase, que  
aparente o simule a una persona menor de  
edad realizando actividades sexuales.**

**CYBER CRIME**

# ¿Qué hacer?



OTDER X CRIME CYBER CRIME

# Cooperación Internacional



**CIBER CRIME**

# Marco Legal Internacional

Convención sobre el Cibercrimen  
conocida como el  
“Convenio de Budapest”



OTDER CYBER CRIME

# MARCO LEGAL NACIONAL



OTDER CYBER CRIME

# CULTURA DIGITAL



OTDER CYBER CRIME

## CULTURA DIGITAL



## Estados Unidos: el tiroteo en una pizzería de Washington DC que se originó por una falsa noticia viral en Facebook

Redacción  
BBC Mundo

6 diciembre 2016

Compartir



AP

Cuando se dio cuenta de que estaba rodeado, el atacante se rindió y entregó sus armas.

# CULTURA DIGITAL

crn<sup>oy</sup>.com  
NOTICIAS 24/7

NACIONALES

DEPORTES

ENTRETENIMIENTO

ECONOMÍA

TECNOLOGÍA

OPIN

NOSOTROS

CONTACTO

ÚLTIMAS

MÁS LEÍDAS

TEMAS

BUEN GUSTO

CR DE AYER

FRASE DEL DÍA

FOTO DEL DÍA

MUNDO > SUCESOS

## Noticia falsa desata la histeria en Perú

DICIEMBRE 2, 2016 2:51 PM | AGENCIA/REDACCIÓN 



(AFP) “¡Alerta! !Tráfico de órganos! ¡Cuiden a sus hijos!”. Una **noticia falsa en Facebook** demostró su poderoso alcance: habitantes de un sector pobre de la periferia de Lima, Perú, salieron enardecidos en busca de los delincuentes, destruyendo todo a su paso.

Según los pobladores, los **presuntos traficantes de órganos** estaban detenidos en la delegación policial del barrio de Huaycán, al este de la capital. Una turba enardecida fue a su caza **la tarde y noche del jueves, volteando autos, lanzando bombas molotov y objetos contundentes**. La policía debió disparar al aire para dispersarlos.

**SUCESOS**

Grupo estima haber arreglado unos 150 aparatos en Upala

## Limonenses donaron tiempo para reparar refrigeradoras dañadas por huracán

ACTUALIZADO EL 30 DE NOVIEMBRE DE 2016 A LAS 01:36 PM

Técnicos en refrigeración se mostraron sorprendidos de que en redes sociales los confundieran con militantes del PLN porque sus carros iban identificados con banderas verdiblancas del equipo Limón F. C.



POR GUSTAVO FALLAS M. [gustavo.fallas@nacion.com](mailto:gustavo.fallas@nacion.com) y POR EILLYN JIMÉNEZ B. [eillyn.jimenez@nacion.com](mailto:eillyn.jimenez@nacion.com)



OTDER CYBER CRIME

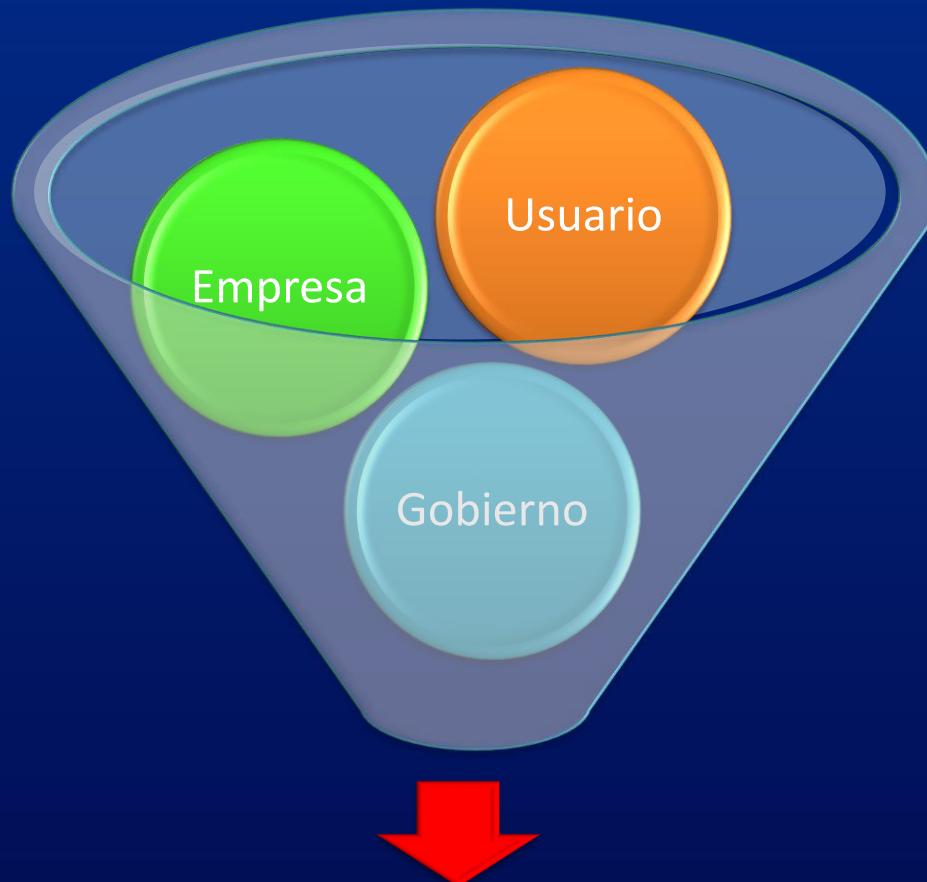
# CULTURA DIGITAL

---



OTDER CYBER CRIME

ENTRE  
TODOS



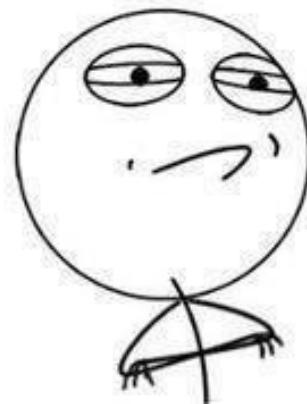
Cibersociedad lo más  
segura posible

# CIBER CRIME CYBER CRIME

La  
**Ciberseguridad**  
un tema de  
**TODOS**

Ayer le cambie el nombre a mi  
wi-fi y le puse:  
“Trata de hackearla”

Hoy día desperté y se llamaba:  
“Challenge Accepted”



# OTROS CRIMENES Y CYBER CRIME

Lic. Ing. Roberto Lemaître Picado  
Abogado-Ingeniero Informático  
Especialista en Delitos Informáticos  
[rolemaître@abogados.or.cr](mailto:rolemaître@abogados.or.cr)  
[roberto.lemaître@ucr.ac.cr](mailto:roberto.lemaître@ucr.ac.cr)



## Noches de Ciberseguridad

Con Roberto Lemaître Picado