Prevención en delitos informáticos

Sandra Johanna Arévalo Fonseca

Fundación Universitaria
SAN MATEO
Editorial

Prevención en delitos informáticos

Prevención en delitos informáticos

Sandra Johanna Arévalo Fonseca

Fundación Universitaria SAN MATEO
Editorial

SOCIO-JURÍDICA SAN MATEO

Prevención en delitos informáticos

Primera edición, 2022
ISBN 978-958-53142-7-6 (digital)

Preparación editorial
Editorial Universitaria San Mateo
Raúl Cera Ochoa, coordinador de publicaciones
Paula Cabezas García, correctora de estilo
Joan Sebastian Yañez, diseño y diagramación

Transversal 17 No 25-25
editorial@sanmateo.edu.co
PBX: 330 99 99, ext. 403
https://www.sanmateo.edu.co/editorial.html

Bogotá, D.C., Colombia, 2022

La Editorial de la Fundación Universitaria San Mateo se encuentra indexada en la Red Iberoamericana de Innovación y Conocimiento Científico (REDIB).

Catalogación en la publicación – Biblioteca Nacional de Colombia

Arévalo Fonseca, Sandra Johanna
Prevención en delitos informáticos / Sandra Johanna Arévalo Fonseca. -- 1a ed. – Bogotá: Fundación Universitaria San Mateo, 2022.
p. 30

Archivo en formato digital.

ISBN 978-958-53142-7-6 (digital)

1. Delitos informáticos - Prevención - Colombia 2. Delitos informáticos - Aspectos jurídicos - Colombia I. Título

CDD: 364.16809861 ed. 23 CO-BoBN– a1089970

Esta guía ha pasado por procedimientos editoriales que garantizan su normalización bibliográfica y su disponibilidad propuestos por el Ministerio de Ciencia,Tecnología e Innovación - MinCiencias

Contenido

Presentación

Desde la década de 1960 el mundo cambió de manera singular con la aparición del internet. Dicho acontecimiento revolucionó a la sociedad, entregando información de manera ágil y pronta; se convirtió en una herramienta tecnológica de colaboración, integración e información de uso continuo en todo tipo de actividades como formativas, laborales, sociales, recreativas, escolares, de convivencia y demás. Sin embargo, a su vez ha sido la entrada para que algunos individuos puedan realizar actividades fraudulentas con la ayuda de nuestros datos.

En Colombia, uno de los mayores compromisos es la actualización de la legislación, de acuerdo con el nacimiento de nuevas formas de criminalidad como el internet, el cual hoy es uno de los mayores mecanismos utilizados para la vulneración de derechos.

En el año 2009 nace la Ley 1273 (anexo), referente a los delitos informáticos, instaurando un nuevo bien jurídico denominado "protección de la información y de los datos", adicionándose al Código Penal Colombiano en el título VII Bis. Esta creación ha permitido garantizar la realización de actividades tendientes a la protección del sistema en el uso de datos por medio de herramientas tecnológicas. Asimismo, evita el atentado contra los pilares de la seguridad de la información como su confidencialidad, integridad y disponibilidad.

Durante el año 2019, el Informe de tendencias del Ciberdelito en Colombia 2019-2020 evidencia que se cometieron 15.948 delitos de esta índole, en los cuales se perdieron más de 5.000 millones de pesos y hay 33.000 sitios web vulnerables en la comisión de delitos. También entrega un reporte de las denuncias instauradas donde Bogotá se encuentra con 5.308 casos en investigación, seguido de Cali (1.190), Medellín (1.186), Barranquilla (693) y Bucaramanga (397).

La cantidad de vulneraciones se ha incrementado de tal manera que en 2015 existieron 7.523 denuncias, en 2016 se registraron 11.225, en 2017 llegó a 15.840, en 2018 a 22524 y 2019 terminó con 15.948. Lo anterior evidencia que las Tecnologías de la Información y la Comunicación (TIC) hoy son un punto de transgresión de los derechos cuando se realizan malas prácticas o el sentido común falla.

De esta manera, la presente cartilla constituye una herramienta que aporta en la prevención de conductas que generan o colaboran en la realización de acciones ilegales más comunes a través del internet; mediante el cual personas inescrupulosas destruyen, modifican, violentan o causan algún tipo de daño a personas o entidades en particular.

Pornografía infantil

La pornografía infantil es uno de los delitos de mayor crecimiento a nivel mundial debido a la creación y fortalecimiento de redes internacionales, así como al uso de las diferentes herramientas tecnológicas. Esto ha permitido el acceso, creación, producción y comercialización de material de pornografía; donde en su mayoría las víctimas directas de este flagelo son los Niños, Niñas y Adolescentes (NNA).

Según el Convenio del Consejo de Europa para la Protección de los Niños contra la Explotación y el Abuso Sexual (AÑO), la pornografía infantil es:

> La representación visual de un menor que mantiene una conducta sexualmente explícita, una persona real que parezca ser menor de edad que participa en actos sexualmente explícitos, o imágenes realistas de un menor no existente que mantiene una conducta sexualmente explícita.

Hoy en día es imposible determinar la cantidad de sitios de internet que son parte de este delito. Este flagelo no es de un país en particular, sino mundial. Aquí las víctimas se encuentran en un país, sus productores en otro y sus clientes alrededor del mundo.

Se debe tener en cuenta que la Corte Suprema de Justicia de Colombia aprobó la revisión de las redes sociales de NNA con el fin de evitar el riesgo de los menores y no hay configuración de la violación del derecho a la Intimidad.

¿Cómo prevenirlo?

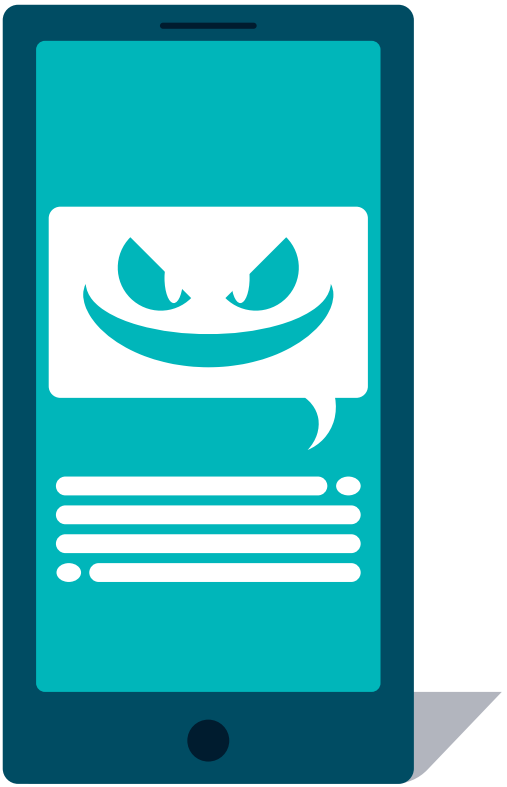
1. Tener comunicación directa con los menores sobre los riesgos en el manejo de las herramientas tecnológicas.
2. Mantener una disciplina y normas claras con los menores de edad frente al uso del internet.
3. No se deben tomar fotos o videos de NNA sin ropa para mantenerlas en dispositivos electrónicos que puedan ser hackeados.
4. No subir fotos de NNA a ninguna red social con el uniforme del colegio (en caso de pornografía, secuestro o trata de personas).
5. No remitir fotos o videos de NNA sin ropa (o con poca) a familiares, amigos o cualquier persona.
6. No compartir fotos o videos de NNA utilizados para este delito.
7. Instalar en los dispositivos tecnológicos controles parentales para mantener un control de la información (Google Safe Search, Avira Social Shield, K9 Web Protection, Protectio, Segukids, entre otros).
8. En algunos casos bloquear las cámaras de los dispositivos.
9. Saber los contactos con los cuales chatean los menores.

Ciberacoso o *cyberbullying*

Es el acoso psicológico que afecta a cualquier persona en el ámbito escolar, laboral u otro, mediante el uso de medios digitales, teniendo en cuenta que es realizado entre iguales. Esta situación puede generarse entre personas de la misma edad, género o contexto, mediante insultos, ofensas, humillaciones, degradaciones, infamias, provocaciones, vejaciones o cualquier hostigamiento que menosprecie al individuo.

En ese sentido, la víctima de este flagelo tiene por lo general autoestima baja, inseguridad, vergüenza y mantiene en silencio estos hechos. Incluso puede llegar al punto de acabar con su propia vida debido al peso psicológico del acoso.

Por lo general, este delito es la consecución del acoso (o bullying) y debe evidenciarse que no es de contexto sexual, puesto que generaría otro tipo de delito.



¿Cómo se evidencia en ciberacoso o ciberbullying en la red?

1. Creación de perfiles falsos para insultar, ofender, humillar, degradar, profesar infamias o provocar a cualquier persona.
2. Dar a conocer rumores en chats, videojuegos, redes sociales, que degraden a una persona.
3. Robar contraseñas o hackear el correo electrónico de la víctima para confesar algún tipo de práctica o rutina verdadera (o falsa), así como el acoso generalizado a otros.
4. Remitir mensajes de amenaza mediante chats o redes sociales.
5. Realizar y reproducir en la red imágenes reales o editadas que permitan perjudicar a la víctima.

¿Cómo prevenirlo?

1. Tener comunicación directa con los NNA sobre el trato que obtienen de sus compañeros, profesores, vecinos y cualquier persona que tenga contacto con ellos mediante el uso de la tecnología.
2. Tener en cuenta el cambio de hábitos, actitud e incluso apatía de las personas a nuestro alrededor.
3. No compartir fotos, videos o rumores de cualquier individuo que dañe su integridad.
4. No ingresar a correos electrónicos personales en cualquier dispositivo electrónico.

Engaño pederasta o *grooming*

El *grooming* (en español, engaño pederasta) es el ciberacoso sexual de un adulto a un NNA mediante las herramientas tecnológicas. Por lo general, existe un perfil falso en las redes sociales, chats, videos, juegos o cualquier herramienta que le permita el intercambio de información y un acercamiento con el menor que se quiere asediar.

Para la realización de este delito, la primera parte es la solicitud del adulto al menor de una foto o video con contenido sexual para luego intimidar. De esta manera logra la remisión de más fotos o videos o inclusive llevar a cabo una reunión entre ambos. En caso de la negativa del menor, el adulto publica la foto o el video inicial.

El acoso sexual de NNA, junto con la pedofilia, no surgen con el internet. Sin embargo, mediante el uso de las herramientas tecnológicas la problemática se ha vuelto frecuente y con un desenvolvimiento más trágico.

¿Cómo prevenirlo?

1. Tener comunicación directa con los NNA sobre su cuerpo y la no realización de fotos o videos para ser remitidos a ningún chat.
2. No permitir que los menores chateen o jueguen con la cámara activa.
3. No utilizar el nombre completo como usuario en los juegos en línea.
4. Configurar y mantener la privacidad y seguridad de las cuentas y dispositivos.
5. Mantener las contraseñas de todas las cuentas y dispositivos. Actualizarlas permanentemente y alejarlas de cualquier cambio por parte de los menores.

Suplantación de identidad o *phising*

Este tipo de delito es el engaño para conseguir la revelación de información personal mediante el uso de correos electrónicos que pretenden ser legales y con el uso de nombres afines. Sin embargo, el fin es robar información confidencial de los usuarios que reciben las solicitudes.

Los ciberdelincuentes remiten correos de forma masiva para capturar la mayor cantidad de víctimas posible y que, como respuesta, le sean remitidos a enlaces preparados anteriormente para introducir datos personales por los usuarios como tarjetas de crédito, seguridad social, cuentas bancarias, entre otros.

¿Cómo prevenirlo?

No responder enlaces de correos electrónicos no solicitados.

1. No abrir adjuntos de direcciones de correos electrónicos no conocidos o consultados.
2. No proporcionar información confidencial como claves o cualquier información privada a través de correo electrónico, chats o teléfono.
3. Mantener actualizado el sistema operativo, antivirus y demás licencias.
4. Si es necesario, al introducir datos o claves confidenciales se debe observar que las páginas sean sitios web seguros. Una de las maneras es que tengan "https://", al inicio de la dirección electrónica y el otro que el navegador muestre el icono de un candado cerrado.
5. Revisar periódicamente los extractos bancarios para determinar algún tipo de irregularidad.

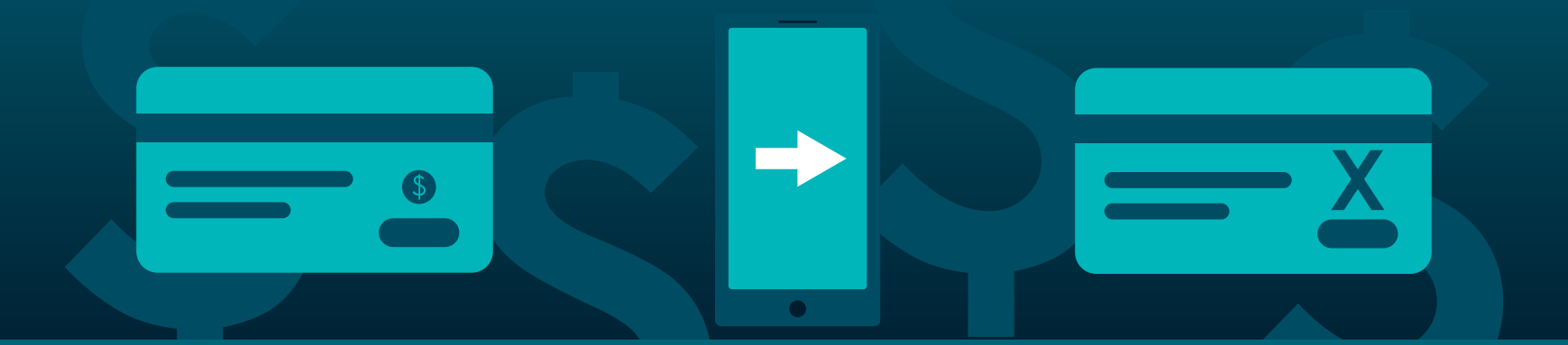
Sexteo o *sexting*

Debido al incremento de dispositivos electrónicos y uso por parte de la sociedad, se efectúa el envío de imágenes de índole sexual por medio de chats de mensajería instantánea, redes sociales, correos electrónicos o cualquier otra herramienta que permita la comunicación. No obstante, se debe dejar en claro que es una práctica libre y totalmente voluntaria.

Aunque esta actividad no es de uso exclusivo de jóvenes, sí son los más vulnerados por este tipo de información, convirtiéndose en un delito cuando deja de ser una práctica entre dos o más personas de manera voluntaria y se vuelve un contenido de amplia circulación sin el consentimiento de la persona a la cual pertenece la imagen.

¿Cómo prevenirlo?

1. En caso de remitir este tipo de fotografías o videos, tener en cuenta que la persona que la recibe sea de entera confianza.
2. Las personas que remiten y reciben este tipo de fotografías deben ser mayores de edad.
3. Los dispositivos para esta práctica deben ser confidenciales y con disponibilidad privada.



Fraude o *skimming*

Es el robo de información de las tarjetas débito o de crédito por medio de transacciones, donde el objetivo es clonar o reproducir este medio. Los sitios que utilizan los delincuentes para poder clonar las tarjetas de crédito mediante el uso de dispositivos electrónicos son:

- Restaurantes.
- Hoteles.
- Bares.
- Cajeros automáticos.
- Cualquier sitio que permita el uso de estos.

¿Cómo prevenirlo?

1. Revisar el cajero automático para evidenciar posibles fraudes.
2. Mantener a la vista las tarjetas débito o crédito al realizar compras o pagos.
3. No recibir ayuda de nadie durante las transacciones.
4. Las claves deben estar ocultas mientras sean digitadas.
5. En el momento del cambio de tarjeta se debe borrar la información en la antigua por medio de un imán sobre la cinta magnética y, por último, su destrucción total.
6. En caso de anomalía, comunicar de inmediato al banco.
7. Sistema anti-skimming: este sistema codifica la información de la banda magnética.

¿Qué hacer en caso de ser víctima o enterarme de la realización de los presentes delitos informáticos?

1. Denuncia virtual: el Centro Cibernético Policial virtual (CPP) permite realizar denuncias que ingresan a ser evaluadas y valoradas por la Fiscalía General de la Nación a través de la página www.ccp.gov.co
2. Te Protejo: es un reporte anónimo de situaciones de pornografía Infantil. Se puede descargar la aplicación o ingresar a la página web www.teprotejo.org
3. Protectio: aplicación de la Policía Nacional para la protección de situaciones de pornografía Infantil.
4. Informar a padres o docentes en casos requeridos.
5. Informar al banco de manera inmediata en caso de uso de tarjetas de crédito o transacciones fraudulentas.

Entidades de detección de delitos informáticos

Centro cibernético policial

Es un Centro de Atención Inmediata (CAI) virtual donde se pueden realizar denuncias desde internet, incluidas denuncias de delitos cibernéticos.

Figura 1. Entorno web del CCP

Fuente: captura de pantalla.

Comando conjunto cibernético

Unidad militar creada en 2012 con el fin de planear, coordinar, integrar y sincronizar las dependencias y unidades para las operaciones cibernéticas en el territorio colombiano.

Figura 2. Entorno Sistema Nacional de Denuncia Virtual

Fuente: captura de pantalla.

Referencias

Banco Interamericano de Desarrollo [BID] y Organización de los Estados Americanos [OEA]. (2016). *Ciberseguridad ¿Estamos preparados en América Latina y el Caribe? Informe Ciberseguridad 2016*. BID y OEA.

Beltramone, G., Herrera, R. y Zabale, E. (1998). *Nociones básicas sobre los delitos informáticos* [Ponencia]. X Congreso Latinoamericano y II Iberoamericano de Derecho Penal y Criminología, Santiago, Chile.

Cámara Colombiana de Informática y Telecomunicaciones [CCIT] y Fedesarrollo. (2014). *Coyuntura TIC. Avances y retos de la defensa digital en Colombia*. CCIT y Fedesarrollo. https://www.ccit.org.co/wp-content/uploads/avances-y-retos.pdf

Cano, J. (2007). Inseguridad Informática y Computación Anti-forense: Dos conceptos emergentes de la seguridad de la Información. *Information System Control Journal, 4*.

Colprensa. (2015, 26 de febrero). *Un millón de personas han sido afectadas por el cibercrimen en Colombia*. La República. http://www.larepublica.co/un-mill%C3%B3n-de-personas-han-sidoafectadas-por-el-cibercrimen-en-colombia_224986

Consejo de Europa. (2017). *Convenio del Consejo de Europa para la Protección de los Niños contra la Explotación y el Abuso Sexual.* https://www.humanium.org/es/convenio-del-consejo-de-europa-para-la-proteccion-de-los-ninos-contra-la-explotacion-y-el-abuso-sexual/

De la Cuesta, J. (Dir.) y De la Mata, N. (Coord.). (2010). *Derecho penal informático.* Civitas.

Díaz, A. (2012). *Derecho Informático: elementos de la Informática Jurídica.* Leyer.

Líbano Manzur, C. (2000). Los Delitos de Hacking en sus diversas manifestaciones. *Revista Informática Jurídica Inteligente,* (21). https://vlex.es/vid/delitos-hacking-diversas-manifestaciones-107511

Martínez Escobar, C. (2001). *El delito informático "la información y la comunicación en la esfera penal conforme con el nuevo código penal"*. Editorial Tecnos S.A.

Ministerio de Tecnologías de Información y Comunicaciones [MinTIC]. (2021, 13 de julio). *¡La iniciativa en TIC confío + regresa recargada!* https://www.enticconfio.gov.co/video/la-iniciativa-En-TIC-conf%C3%ADo-regresa-recargada

Palazzi, P. (2000). *Delitos informáticos*. Ad-Hoc.

Palomá, L. (2012). *Delitos Informáticos (en el ciberespacio) doctrina y análisis de casos reales*. Ediciones Jurídicas Andrés Morales.

Patiño, A. (2007). *Bandidos y hackers*. Editorial Universidad de Antioquia.

Policía Nacional de Colombia. (2019). Informe de Tendencias del Cibercrimen en Colombia. 2019-2020. https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

Posada, R. (2013). El delito de sistema abusivo a sistema informático: a propósito del art. 269A del CP de 2000. *Revista de Derecho, Comunicaciones y nuevas tecnologías,* (9).

Rayón, M. y Gómez, J. (2014). Cibercrimen: particularidades en su investigación y juzgamiento. *Anuario jurídico y económico escurialense,* 47, 209-234.

Riquert, M. (2014). Convenio sobre Cibercriminalidad de Budapest y el MERCOSUR: propuestas de derecho penal material y su armonización con la legislación regional sudamericana. *Revista Derecho Penal, 3*(7).

Riquert, M. (2008). Estado de la Legislación contra la Delincuencia Informática en el Mercosur. *AR: Revista de Derecho Informático,* (116).

Semana. (2015, 28 de septiembre). El cibercrimen es un delito más rentable que el narcotráfico. https://www.semana.com/internacional/articulo/principales-cifras-del-cibercrimen-mundo-colombia/213988/

Silva, J. (2015, 9 de marzo). *Cada segundo 12 personas son víctimas del cibercrimen*. Semana. https://www.semana.com/opinion/columnistas/articulo/perdidas-genera-cibercrimen-mundo/206653/

Téllez, J. (2008). *Derecho informático* (4ª ed.). McGraw-Hill.

Zuluaga, C. (2014, 13 de mayo). *En busca de cura para los delitos informáticos*. El espectador. https://www.elespectador.com/politica/en-busca-de-cura-para-los-delitos-informaticos-article-492170/

Anexo Ley 1273 de 2009

(Enero 5)

Diario Oficial No. 47.223 de 5 de enero de 2009

CONGRESO DE LA REPÚBLICA

Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

EL CONGRESO DE COLOMBIA

DECRETA:

ARTÍCULO 1o. Adicionase el Código Penal con un Título VII BIS denominado "De la Protección de la información y de los datos", del siguiente tenor:

CAPITULO I

De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos

Artículo 269A: *Acceso abusivo a un sistema informático.* <Ver Notas del Editor> El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269B: *Obstaculización ilegítima de sistema informático o red de telecomunicación.* El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

Artículo 269C: *Interceptación de datos informáticos.* El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Artículo 269D: *Daño Informático.* El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269E: *Uso de software malicioso.* El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269F: *Violación de datos personales.* El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue,

modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269G: *Suplantación de sitios web para capturar datos personales.* El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

Artículo 269H: *Circunstancias de agravación punitiva:* Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.

2. Por servidor público en ejercicio de sus funciones.

3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.
5. Obteniendo provecho para sí o para un tercero.
6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
7. Utilizando como instrumento a un tercero de buena fe.
8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

CAPITULO II

De los atentados informáticos y otras infracciones

Artículo 269I: *Hurto por medios informáticos y semejantes.* El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.

Artículo 269J: *Transferencia no consentida de activos.* El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en

perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.

Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.

ARTÍCULO 2o. Adiciónese al artículo 58 del Código Penal con un numeral 17, así:

Artículo 58. *Circunstancias de mayor punibilidad.* Son circunstancias de mayor punibilidad, siempre que no hayan sido previstas de otra manera:

(...)

17. Cuando para la realización de las conductas punibles se utilicen medios informáticos, electrónicos o telemáticos.

ARTÍCULO 3o. Adiciónese al artículo 37 del Código de Procedimiento Penal con un numeral 6, así:

Artículo 37. *De los Jueces Municipales.* Los jueces penales municipales conocen:

(...)

6. De los delitos contenidos en el título VII Bis.

ARTÍCULO 4o. La presente ley rige a partir de su promulgación y deroga todas las disposiciones que le sean contrarias, en especial el texto del artículo 195 del Código Penal.

El Presidente del honorable Senado de la República,
HERNÁN ANDRADE SERRANO.

El Secretario General del honorable Senado de la República,
EMILIO RAMÓN OTERO DAJUD.

El Presidente de la honorable Cámara de Representantes,
GERMÁN VARÓN COTRINO.

El Secretario General de la honorable Cámara de Representantes,
JESÚS ALFONSO RODRÍGUEZ CAMARGO.

REPUBLICA DE COLOMBIA - GOBIERNO NACIONAL
Publíquese y cúmplase.
Dada en Bogotá, D. C., a 5 de enero de 2009.

ÁLVARO URIBE VÉLEZ

El Ministro del Interior y de Justicia,
FABIO VALENCIA COSSIO.

Fundación Universitaria
SAN MATEO
Editorial