

## La necesidad de protección de la información y de los datos: Una batalla contra la tecnología.

*Andrés Alfonso Cárdenas Rojas*

### **Resumen**

El avance de la tecnología ha sido devastador en los últimos tiempos, lo que permite al usuario realizar transacciones con sólo un clic o enviar y recibir información en tiempo real. Sin embargo, estos avances han traído con ello una consecuencia que cada día es más difícil de luchar: la delincuencia informática. Esto ha generado una lucha diaria en la protección de la información tecnológica lo cual afecta la evolución de los mismos usuarios

**Palabras clave.** Información, Seguridad Informática, Delitos informáticos, Protección de datos, Crímenes informáticos

### **Abstract**

The advancement of technology has been devastating in recent times, which allows the user to make transactions just a click or send and receive information in real time. However, such advances have brought the couple a consequence that every day is more difficult to fight: computer crime. This has generated a daily struggle in protecting information on pain of the same evolution technology to bring the user end to misfortune

**Keywords.** Information, Security, Cybercrime, Data Protection, Computer Crimes

Desde hace ya varias décadas la tecnología viene avanzando a pasos agigantados, siendo cada vez mayores las oportunidades de desarrollo de las ciencias de la información, entendidas como ese binomio “almacenamiento de datos y comunicación”.

No obstante, así como se presenta ese avance de la tecnología informática, o para efectos prácticos: Tecnologías de la Información y Comunicación - TIC , se han generado diversos mecanismos, a partir de ella, para tratar de vulnerar aquellos sistemas informáticos aparentemente infalibles, por lo que en los tiempos de hoy no

resulta extraño el encontrarse con términos como el phishing o el adware, sumado también a un sin número de modalidades de captación ilegal de la información sensible a través de cualquiera de los medios informáticos actualmente utilizados por los usuarios.

Dado lo anterior, se ha generado la necesidad de buscar, cualquiera que sea la manera, la seguridad en la información, y por sobre todo, la protección de los datos, para poder evitar fraudes basados en estos tipos de modalidades, mediante la creación de softwares especializados, pero sobre todo, con blindaje legal en la materia.

## **I. Protección de datos personales a partir de la ley 1273 de 2009.**

Si bien es cierto, hasta mucho antes del año 2009 no era fácil encontrar herramientas de tipo legal que permitieran de una u otra manera la protección de la información. No obstante, debido al enorme crecimiento de los fraudes informáticos y sobre todo a la necesidad de su penalización, surgió la Ley 1273 de 2009 la cual adicionó al Código Penal un título denominado “De la protección de la información y de los datos”, con el fin de permitir la preservación integral los sistemas, y que a su vez de una u otra manera se permitiera la utilización de las tecnologías de la información y la comunicación – TIC, evitando así su vulneración.

Para ese entonces, fueron nueve los nuevos delitos introducidos en la legislación colombiana, con los que de forma general se pretendía prevenir a la sociedad para evitar la comisión de estas conductas, con penas de prisión que oscilaban entre los cuatro (4) y los diez (10) años.

De igual manera, tales delitos han sido divididos en dos grupos, conforme a lo que se pretende proteger, que para este caso aplica por un lado a los atentados contra “la protección de la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos”. Por otro lado “la protección contra los atentados informáticos y otras infracciones”.

### ***1. La protección de la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos.***

Dentro del primer grupo se encuentran aquellos delitos tipificados como el acceso abusivo a un sistema informático, la obstaculización ilegítima de sistema informático o red de telecomunicación, la interceptación de datos informáticos, el daño informático, el uso de software malicioso, la violación de datos personales y la suplantación de sitios web para capturar datos personales.

Aquí se hace evidente una necesidad de protección de la privacidad de la información y las consecuencias de uso no autorizado, como lo es el caso del PHISHING, entendido este como el fraude a través de la WEB, desde donde se logra la obtención de datos confidenciales de las personas (o comúnmente llamados usuarios) para acceder a sus cuentas bancarias y vaciar las mismas; la modalidad, entre otras, se traduce en el envío de correos electrónicos que se presumen confiables, pero que finalmente resultan ser fraudulentos, donde se le solicita al usuario el acceso mediante un clic, en otros casos se solicita el reinicio del sistema y por sobre todo la asignación de una nueva clave de seguridad, momento en el cual los datos son captados por quien está al otro lado de la red.

Esta modalidad pretende entonces ser contrarrestada a través de mensajes informativos, conforme a los cuales las entidades bancarias no estilan efectuar este tipo de procedimientos a través de internet, para evitar en grado sumo la propagación de esta metodología de robo de información. Existen actualmente campañas desarrolladas por entidades financieras en las cuales se dan a conocer varios de estos “modus Operandi”, sin embargo, siguen existiendo usuarios incautos que terminan cayendo en estas trampas, facilitando la información extremadamente confidencial a aquellos delincuentes de la red.

## ***2. La protección contra atentados informáticos y otras infracciones.***

Dentro del segundo grupo de delitos se encuentra el hurto a través de medios informáticos y semejantes y la transferencia no consentida de activos.

El caso de PHISING también podría enmarcarse dentro de este delito, sin embargo, existe una diferencia, la cual radica en que lo relacionado en el primer grupo de delitos va atado a la obtención ilegal de la información y, para este segundo grupo de delitos, es el uso de la misma para lograr el hurto de dinero.

Es así como podría decirse que este segundo grupo protege entonces los patrimonios económicos, que se podrían llegar a ver afectados a partir del uso de la tecnología, en cualquiera de sus presentaciones y/o manifestaciones, como medio para lograr desfalcos millonarios. Pero en todo caso entendiendo que continúa siendo originado debido a la necesidad de una auténtica protección de la información en una batalla contra la tecnología misma, dado que a partir de ella se han generado hoy en día las diversas formas de fraude y, sobre todo, lo que hoy es conocido como “delitos informáticos”.

“El concepto de delito informático alcanza entonces cualquier conducta que se hubiera cometido en conexión directa o indirecta con un proceso electrónico de datos y cobija tanto las conductas que son realizadas por medio de la computadora (o cualquier aparato que permita una conexión a la red - Internet), como aquellas cuyo objeto material tenga característica informática”<sup>1</sup>.

## II. La lucha contra la criminalidad informática.

Hoy por hoy resulta preocupante la dificultad que se presenta al momento de emprender una lucha contra la criminalidad informática debido a los factores que terminan por caracterizarla: “Se caracteriza la denominada delincuencia informática por la dificultad para su persecución en relación con la delincuencia tradicional o clásica, en razón de la rapidez de su comisión, la distancia que puede haber entre el lugar de la realización de la acción ilícita y el de la producción del resultado, la dificultad para descubrir a los autores y la facilidad para borrar las huellas, por la posibilidad de alterar programas y datos sin dejar rastro, y la facilidad para asegurar su impunidad, pues la complejidad técnica de la materia reduce su conocimiento a un círculo limitado de expertos”<sup>2</sup>.

Así las cosas, son entonces varias las clasificaciones que sobre criminalidad informática se han hecho, independientemente de la fuente que se tome, sin embargo, se hará referencia a una muy acertada:

“ 1. Manipulaciones del INPUT, que consideran en la obtención de un resultado falso del proceso de datos a través de la introducción en el mismo de datos falsos, bien de manera directa o mediante la utilización de una persona interpuesta.

2. Afectaciones del correcto PROCESAMIENTO del sistema electrónico, que pueden cumplirse a través de dos formas:

a) Mediante la introducción de un programa falso, bien al ser cambiado por el correcto previamente existente, o a través de la instalación inicial del falso.

b) Mediante una falsa o errónea entrada hecha desde la consola del sistema informático.

3. Alteración de los datos una vez terminado el procesamiento de los mismos, mediante la modificación del propio resultado: manipulación del OUTPUT.

4. Combinación de varias de las modalidades anteriores, denominada forma mixta”<sup>3</sup>.

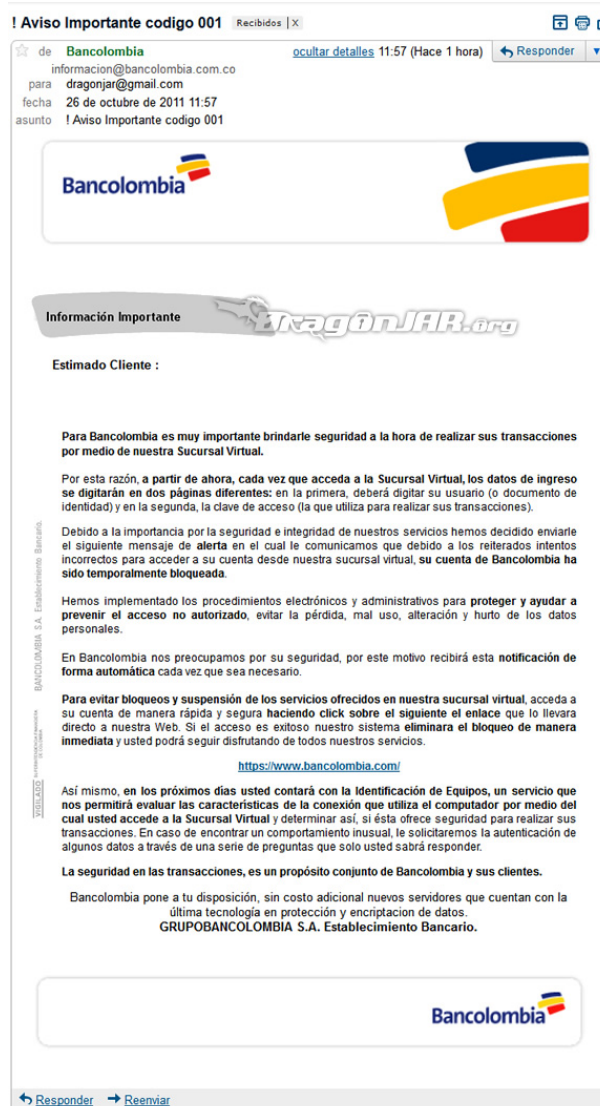
Dado lo anterior, se podría afirmar sin temor a una equivocación, que cada vez son más las modalidades que se encuentran acerca de los delitos informáticos, por lo que pareciera que la sociedad estaría encaminada a tratar de contrarrestar estas modalidades y por sobre todo sus efectos, mediante campañas que busquen promover la precaución a la hora de proporcionar información confidencial (datos personales) a través de la red, puesto que pese a que existan en la actualidad múltiples sistemas de protección, el primer riesgo siempre estará en el dueño de la información. Quien finalmente terminaría siendo el directo responsable de su protección. Si el usuario final no protege su información personal, deberá tenerlo por seguro, que ninguna otra persona podría hacerlo en su lugar.

### III. Referencias

- ◆ SUAREZ SÁNCHEZ, Alberto. La estafa informática. Ed. Ibáñez. 2009.
- ◆ [http://www.delitosinformaticos.info/delitos\\_informaticos/glosario.html](http://www.delitosinformaticos.info/delitos_informaticos/glosario.html).
- ◆ <http://www.dragonjar.org/wp-content/uploads/2011/10/Phishing-Bancolombia-1.jpg>
- ◆ <https://estamosencontacto.files.wordpress.com/2009/07/davivienda2.png>

### IV. Apéndice

#### Apéndice A: Ejemplo de PHISING entidad bancaria BANCOLOMBIA



**! Aviso Importante codigo 001** Recibidos | X

de **Bancolombia** [informacion@bancolombia.com.co](mailto:informacion@bancolombia.com.co) [ocultar detalles](#) 11:57 (Hace 1 hora) [Responder](#)

para [dragonjar@gmail.com](mailto:dragonjar@gmail.com)

fecha 26 de octubre de 2011 11:57

asunto ! Aviso Importante codigo 001

**Bancolombia**

**Información Importante** [DragonJAR.org](http://DragonJAR.org)

Estimado Cliente :

Para Bancolombia es muy importante brindarle seguridad a la hora de realizar sus transacciones por medio de nuestra Sucursal Virtual.

Por esta razón, a partir de ahora, cada vez que acceda a la Sucursal Virtual, los datos de ingreso se digitarán en dos páginas diferentes: en la primera, deberá digitar su usuario (o documento de identidad) y en la segunda, la clave de acceso (la que utiliza para realizar sus transacciones).

Debido a la importancia por la seguridad e integridad de nuestros servicios hemos decidido enviarle el siguiente mensaje de alerta en el cual le comunicamos que debido a los reiterados intentos incorrectos para acceder a su cuenta desde nuestra sucursal virtual, su cuenta de Bancolombia ha sido temporalmente bloqueada.

Hemos implementado los procedimientos electrónicos y administrativos para proteger y ayudar a prevenir el acceso no autorizado, evitar la pérdida, mal uso, alteración y hurto de los datos personales.

En Bancolombia nos preocupamos por su seguridad, por este motivo recibirá esta notificación de forma automática cada vez que sea necesario.

Para evitar bloqueos y suspensión de los servicios ofrecidos en nuestra sucursal virtual, acceda a su cuenta de manera rápida y segura haciendo click sobre el siguiente el enlace que lo llevara directo a nuestra Web. Si el acceso es exitoso nuestro sistema eliminara el bloqueo de manera inmediata y usted podrá seguir disfrutando de todos nuestros servicios.

<https://www.bancolombia.com/>

Así mismo, en los próximos días usted contará con la Identificación de Equipos, un servicio que nos permitirá evaluar las características de la conexión que utiliza el computador por medio del cual usted accede a la Sucursal Virtual y determinar así, si ésta ofrece seguridad para realizar sus transacciones. En caso de encontrar un comportamiento inusual, le solicitaremos la autenticación de algunos datos a través de una serie de preguntas que solo usted sabrá responder.

La seguridad en las transacciones, es un propósito conjunto de Bancolombia y sus clientes.

Bancolombia pone a tu disposición, sin costo adicional nuevos servidores que cuentan con la última tecnología en protección y encriptación de datos.

GRUPOBANCOLOMBIA S.A. Establecimiento Bancario.

**Bancolombia**

[Responder](#) [Reenviar](#)

## Apéndice B: Ejemplo de PHISING entidad bancaria DAVIVIENDA



Viernes 03 Julio 2009

ESTIMADO CLIENTE DE BANCO DAVIVIENDA COLOMBIA


nuevo

Como parte de nuestras medidas de seguridad, examinamos periódicamente la actividad del sistema de **Banco Davivienda**. Durante una reciente investigación, hemos observado un problema en su cuenta.


Se recomienda restaurar el acceso su cuenta para administrar completamente los servicios contratados, para ello simplemente siga las instrucciones del enlace inferior auto-generado por el sistema para que para usted reactive su cuenta.

Número de identificación de caso: **BDVivienda-CO 110-494-963**

Por su seguridad, hemos limitado el acceso a su cuenta hasta que se lleven a cabo nuevas medidas adicionales, A lo cual solo podrá consultar el estado de su cuenta pero estará inutilizable. Le pedimos disculpas por cualquier inconveniente que esto pueda producir.

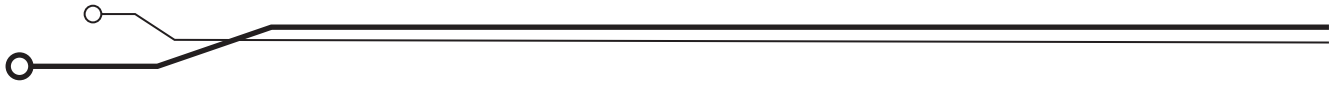
 Para resolver este problema puede entrar a su cuenta desde el siguiente enlace autogenerado para el problema de su caso. Con esto podrá reactivar su cuenta y seguir utilizando completamente los servicios contratados.

Accesar

 **Click para Restaurar el Acceso a su Cuenta**

## V. Notas al pie

- 1 SUAREZ SÁNCHEZ, Alberto. *La estafa informática*. Ed. Ibáñez. 2009. Página 39.
- 2 SUAREZ SÁNCHEZ, Alberto. *La estafa informática*. Ed. Ibáñez. 2009. Página 34.
- 3 SUAREZ SÁNCHEZ, Alberto. *La estafa informática*. Ed. Ibáñez. 2009. Página 63.





# #GSHtag

REVISTA ESPECIALIZADA EN INGENIERIA

EDICION ESPECIAL 4 & 5



