Fraude Corporativo e Informático en Colombia

Audire

Pontificia Universidad Javeriana

Bogotá D.C.

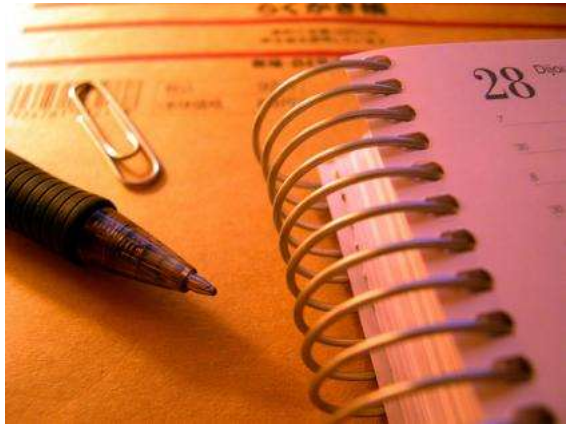
Septiembre de 2013

Ivan Dario Marrugo Jimenez

Abogado

Twitter: @imarrugoj

TEMATICA



1. Contextualización
2. El Fraude corporativo y los delitos informáticos
3. Sistemas de gestión de seguridad de la Información.
4. El caso especial de Protección de datos.
5. Aspectos penales.

Contextualización.

- La Association of Certified Fraud Examiners (ACFE), mayor organización mundial de lucha contra el fraude, estima que las empresas pierden alrededor del 5% de sus ingresos por año debido a este delito.
- Según el ACFE el tipo de fraude más común es la apropiación de activos de la empresa (90% de los casos), mientras que el fraude basado en el falseamiento de informes financieros sólo es el 5% del total.

Contextualización.

- Definición: El fraude corporativo puede definirse como la positiva intención de beneficiarse ilegítimamente, al no hacer algo que se está llamado a hacer, dado la posición que se ocupa.

Tipos mas comunes:

- **Malversación de activos:** Corresponde a la apropiación o mal uso de bienes propiedad de la empresa en beneficio de terceros; aquí se encuentra el clásico robo de mercadería o bienes menores y apropiación de dinero. Dentro de esta categoría hay algunos fraudes menos conocidos, como pago a proveedores ficticios o reembolsos múltiples.
- **Corrupción y soborno:** Consistente en beneficiar ilegítimamente a alguien a cambio de algún tipo de compensación. Es en el ámbito de los contratos a largo plazo donde este fenómeno cobra especial relevancia; la ilustración de esto corresponde a un comprador que elije a un proveedor a cambio de una compensación.
- **Manipulación de Estados Financieros**, que consiste en sub o sobre representar valores, en función de los objetivos que se espere obtener, por ejemplo, si se sobrecontabilizan costos se baja la base imponible y se tributa menos.

Definición clásica; el triangulo del fraude

- Desarrollado por el criminalista Donal Cressey, describe **tres condiciones que comúnmente aparecen cuando se comete este delito**. Los autores del ilícito experimentan cierto incentivo o presión que los lleva a cometer el acto deshonesto. Debe existir una oportunidad para cometerlo y los defraudadores generalmente son capaces de racionalizar o justificar sus acciones.

Algunos puntos interesantes…

- La evidencia indica que la mayoría de los fraudes corporativos se detectan por casualidad ¿La razón? No se actúa proactivamente, porque el problema se percibe como muy lejano.
- En general, los grandes fraudes son muy publicitados y ampliamente comentados, hay no obstante, situaciones poco llamativas, generalmente relacionadas con dolos menores, pero con efectos potencialmente mayores, por cuanto junto al efecto económico directo que causan, afectan las relaciones laborales y destruyen la productividad.
- La ACFE sostiene que la inexistencia de controles adecuados y la falta de mecanismos para constatar la correcta implementación de los mismos, son factores que posibilitan que el fraude permanezca oculto y el daño se acreciente.

Las cifras en colombia no nos ubican muy bien

- Subcampeones en fraude. Por detrás de China y delante de Brasil.
- El 94% de los negocios colombianos sufrió algún fraude en el último año, en comparación con el 88% global.
- El 21% está en la categoría considerada como fraudes electrónicos, que incluyen hurto de información y ciberataques especialmente a sitios Web y el fraude a la infraestructura de las empresas.
- Un factor de alarma: Los exempleados de las organizaciones. El 42% de las encuestadas dijo que había sufrido fraudes a manos de antiguos empleados.
- *Algunas de las estrategias que Kroll recomienda para evitar mejorar la seguridad general e informática, están: la implantación de sistemas de gestión de riesgos, el entrenamiento del personal, definición de los controles financieros y el desarrollo de herramientas de seguridad informática.*

Fraudes informáticos

La Seguridad de la Información en un Mundo inseguro

- La información es un activo con valor estratégico para las empresas y por ello ésta debe ser protegida eficientemente.
- Las políticas de seguridad de la información buscan proteger a las empresas de un amplio espectro de amenazas; Su objetivo es garantizar la continuidad de los sistemas de información, minimizar los riesgos y asegurar el eficiente cumplimiento de las metas empresariales.
- Es importante que los principios de la política institucional hagan parte de la cultura organizacional.
- Para esto, se debe asegurar un compromiso real de los directivos de la compañía en las labores de difusión y consolidación de las políticas de seguridad.

La Seguridad de la Información en un Mundo inseguro

… entonces porque es importante para ti?

- ✓ Porque tu negocio se sostiene con la información que manejas.
- ✓ Porque todo de una u otra forma gira alrededor de la información. (Gerenciamiento)
- ✓ Seamos honestos… cuantos cuentan con un Documento de Políticas de Seguridad de la Información? O cuantos han identificados sus activos críticos?

Modelo optimo

- ✓ Cultura de seguridad.
- ✓ Gestión conjunta (Es responsabilidad de todos).

Modelo negativo

- ✓ Aquí eso no pasa…
- ✓ Nosotros no somos importantes (No atractivos para los ataques).
- ✓ Si no me pasa… no actúo.

Muchos lo ven como un problema de costos…
pero la Inseguridad tiene un costo MAYOR!

Ok! Y por donde comenzamos?

Elabore un inventario de activos de información.

Con ello usted podrá:

- ✓ Identificar información.
- ✓ Clasificarla (Documentos, datos, BD, archivos)
- ✓ Valorarla
- ✓ Gestionarla

A la par usted podrá conocer e identificar otros activos como:

- ✓ Humanos.
- ✓ Físicos.
- ✓ De servicios.

Pensar en los riesgos!

Considere el principal componente:

Las Amenazas!!!

Una Amenaza es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema, en el caso de la Seguridad Informática, los Elementos de Información.

Y luego vienen las Vulnerabilidades…

Vulnerabilidad: “ una debilidad que facilita la materialización de una amenaza”

Ejemplos:

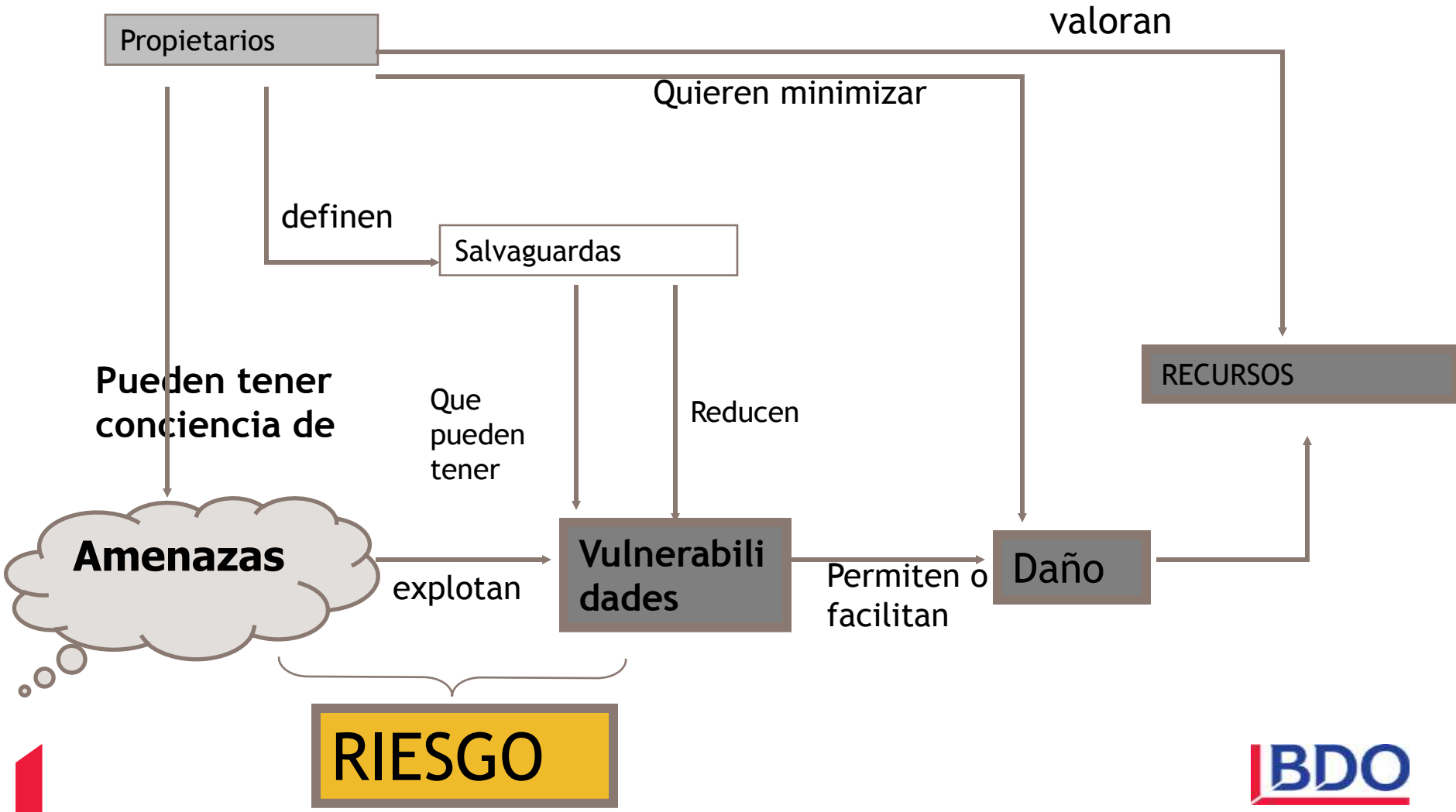
- ✓ Inexistencia de procedimientos de trabajo
- ✓ Concentración de funciones en una sola persona
- ✓ Infraestructura insuficiente

Gestión del Riesgo

Matriz de Riesgo

Evaluación: Impacto.
Probabilidad de ocurrencia
Asignación: Cualitativa y Cuantitativa

Viéndolo gráficamente…



Amenazas

Password cracking

Escalamiento de privilegios

Fraudes informáticos

Puertos vulnerables abiertos

Exploits

Man in the middle

Servicios de log inexistentes o que no son chequeados

Backups inexistentes

Denegación de servicio

Destrucción de equipamiento

Últimos parches no instalados

Instalaciones default

Desactualización

Keylogging

Port scanning

Hacking de Centrales Telefónicas

Y más Amenazas!!

Violación de contraseñas

Intercepción y modificación y violación de e-mails

Captura de PC desde el exterior

Incumplimiento de leyes y regulaciones

empleados deshonestos

Mails anónimos con agresiones

Programas “bomba, troyanos”

Destrucción de soportes documentales

Acceso clandestino a redes

Robo o extravío de notebooks, palms

Propiedad de la información

Acceso indebido a documentos impresos

Robo de información

Indisponibilidad de información clave

Falsificación de información para terceros

Agujeros de seguridad de redes conectadas

Tabla 9 TIPOS DE FALLAS DE SEGURIDAD	2009	2010	2011	2012
Ninguno	8.10%	4.44%	-	11.66%
Manipulación de aplicaciones de software	22.20%	4.40%	5.48%	15.55%
Instalación de software no autorizado	60.70%	18.65%	**17.28%**	**50.55%**
Accesos no autorizados al web	30.90%	9.43%	9.87%	24.16%
Fraude	10.80%	2.49%	4.93%	12.77%
Virus/Caballos de troya	**70.90%**	**20.70%**	16.87%	**43.88%**
Robo de datos	9.90%	2.06%	3.15%	7.50%
Caballos de troya	33.00%	7.04%	-	
Monitoreo no autorizado del tráfico	11.40%	2.60%	3.42%	8.88%
Negación del servicio	15.00%	4.33%	5.48%	11.94%
Pérdida de integridad	25.80%	8.77%	6.57%	12.77%
Pérdida/fuga de información crítica	19.50%	5.47%	-	10.55%
Suplantación de identidad	13.50%	1.84%	3.15%	9.72%
Phishing	16.80%	4.55%	9.32%	22.77%
Pharming	3.00%	0.54%	1.37%	4.16%
Robo de elementos críticos de hardware	-	-	7.54%	20.00%
Acciones de ingeniería social			4.52%	11.94%
Otras (Espionaje)	-	1.30%	0.96%	3.05%
Ataque de aplicaciones web				18.05%

Sistemas de Gestión de Seguridad de la Información

Beneficios de implementar políticas de seguridad de la información

- Consolidación de la seguridad como tema estratégico.
- Planeamiento y manejo de la seguridad más efectivos.
- Mayor seguridad en el ambiente informático y mejor reacción ante incidentes.
- Minimización de los riesgos inherentes a la seguridad de la información.
- Cuantificación de los posibles daños por ataques a la seguridad de la información.

Beneficios de implementar políticas de seguridad de la información

- Orden en el trabajo bajo un marco normativo que evita la duplicación de tareas y facilita el intercambio de información.
- Concientización global sobre la importancia de la seguridad de la información.
- Mejora de la imagen.
- Aumento de la confianza de terceros.
- Mayor control de la información proporcionada a terceros.
- Auditorías de seguridad más precisas y confiables.

Paradigmas en materia de seguridad de la información

1. La seguridad informática no afecta mi actividad.
2. La seguridad es una incumbencia del área informática
3. La información que manejamos no es objeto de ataques
4. Mi red es segura porque se encuentra protegida de ataques externos
5. Tenemos seguridad pues en la última auditoría no tuvimos observaciones críticas.

6. Tenemos un control absoluto de los incidentes de seguridad que ocurren en nuestra red.
7. El tiempo invertido en documentación debe ser descontado de las tareas habituales del personal destinado a la elaboración de la política.
8. Los recursos valiosos deberán ser apartados de la “línea de fuego”
9. Posibles conflictos políticos, comerciales o de relaciones humanas..
10. No disponemos de personal especializado.

Organización de las políticas de seguridad de la información

- Garantizar que la seguridad sea parte del proceso de planificación de la información.
- Evaluar y coordinar la implementación de controles específicos para nuevos sistemas o servicios.
- Coordinar el proceso de administración de la continuidad de la operatoria de los sistemas de tratamiento de la información frente a interrupciones imprevistas.

Responsabilidad

Comité de Seguridad de la Información

- Seguridad del Personal
- Seguridad Física y Ambiental.
- Seguridad en las Comunicaciones y las Operaciones
- Control de Accesos
- Seguridad en el Desarrollo y Mantenimiento de Sistemas
- Planificación de la Continuidad Operativa
- Control de acceso
- Seguridad de desarrollos

Departamento Legal

- Cumplimiento
- Sanciones

Clasificación y Control de Activos

- **Activos de información:** bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad, información archivada, etc.
- **Recursos de software:** software de aplicaciones, sistemas operativos, herramientas de desarrollo, utilitarios, etc.
- **Activos físicos:** equipamiento informático (CPU, monitores, notebooks, módems), equipos de comunicaciones (routers, máquinas de fax, contestadores automáticos), medios magnéticos (cintas, discos), otros equipos técnicos (relacionados con el suministro eléctrico, unidades de aire acondicionado), mobiliario, lugares de emplazamiento, etc.
- **Servicios:** servicios informáticos y de comunicaciones, utilitarios generales (calefacción, iluminación, energía eléctrica, etc.).

En un sentido practico…

- La seguridad de la información se caracteriza como la preservación de:
  - su **confidencialidad**, asegurando que sólo quienes estén autorizados pueden acceder a la información;
  - su **integridad**, asegurando que la información y sus métodos de proceso son exactos y completos.
  - su **disponibilidad**, asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran.

La ley de Protección de Datos Personales
Ley 1581 de 2012

Protección de Datos Personales

"Es el amparo debido a los ciudadanos contra la posible utilización de sus datos personales por terceros, en forma no autorizada, para confeccionar una información que, identificable con él, afecte su entorno personal, social o profesional, en los límites de su intimidad, o

como la protección de los derechos fundamentales y libertades de los ciudadanos contra una singular forma de agresión: el almacenamiento de datos personales y su posterior cesión."

Art. 15 Constitución Política: Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.

En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.

La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley.

Para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley.

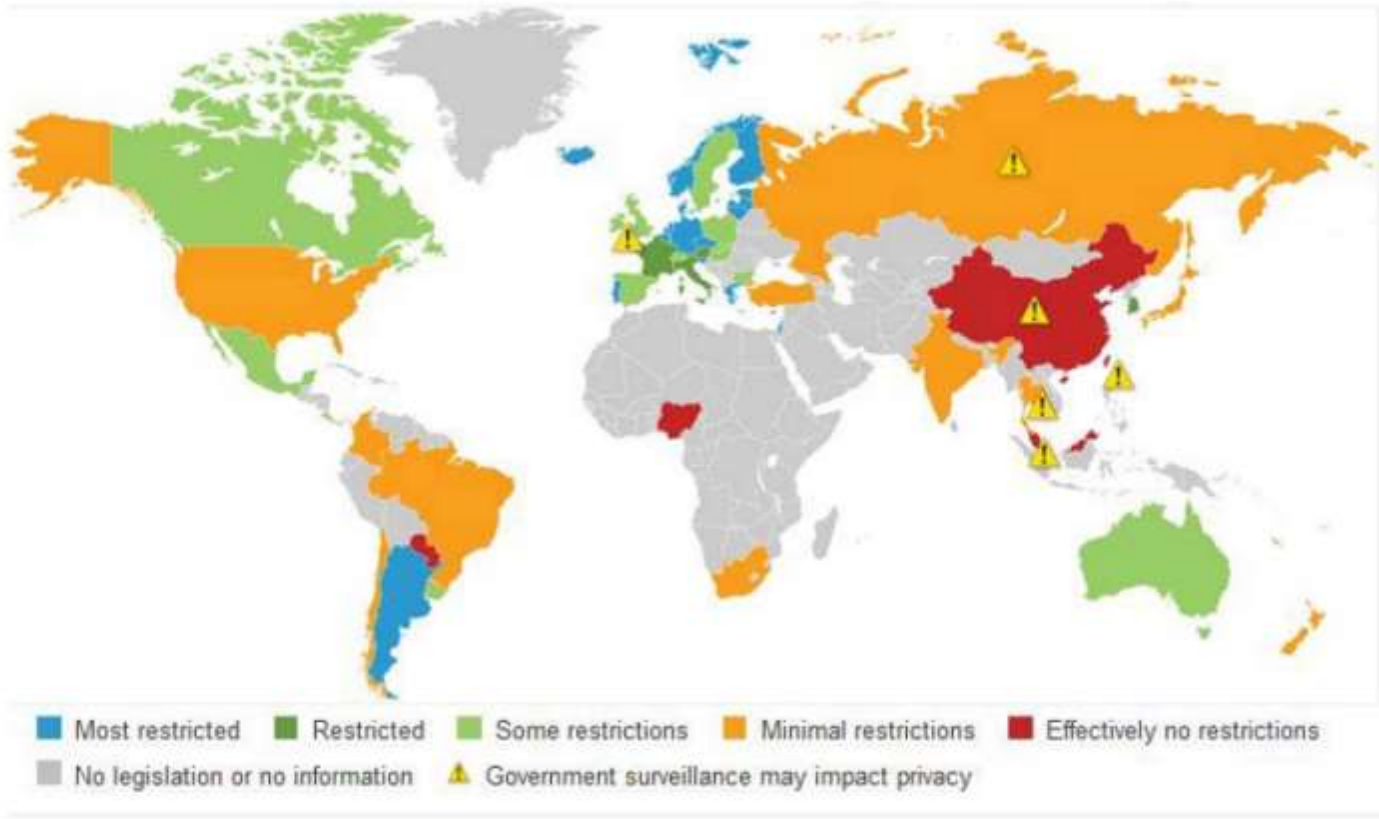
El concepto de Privacidad

- Los datos personales son una clase de información.
- Hoy sin dudas representan el principal activo de cualquier organización.
- *El nuevo Petróleo de la Internet y la nueva moneda del mundo digital*.
- Los Sistemas de Información se han vuelto el nuevo mercado.

Características de los nuevos Sistemas de Información

- Se nutren automáticamente de datos personales.
- Recolectan y procesan grandes cantidades de información en poco tiempo y sin que te enteres.
- Son inseguros.
- Traspasan cualquier frontera física.

Sistemas normativos en el mundo



Fuente: Forrester's Global Data Protection and Privacy Heatmap
http://heatmap.forrestertools.com

Principales aspectos del sistema colombiano

- Es un sistema Mixto: Coexisten 2 normas. (Colisión normativa)
- Declarada constitucional por la Corte mediante sentencia c-748 de 2011
- Sistema de principios.
- Aplicable a cualquier dato contenido en una BD que sea susceptible de tratamiento.

Excepciones

- BD o archivos de ámbito netamente personal. (Manejo interno)
- BD para Defensa nacional.
- BD e información periodística.
- Datos regulados por Ley 1266 de 2008.
- Datos regulados por Ley 79 de 2003.

La norma trae definiciones

Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas determinadas o determinable
(dato público, dato semi-privado, dato privado y dato privado sensible)
- **Responsable del tratamiento**: Persona natural o jurídica, pública o
privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de los datos.
- **Encargado del tratamiento**: Persona natural o jurídica, pública o
privada, que por sí misma o en asocio con otros, realicé el tratamiento de datos personales por cuenta del responsable del tratamiento.
- **Titular**: Persona natural cuyos datos personales sean objeto de
tratamiento.
- **Tratamiento**: Cualquier operación o conjunto de operaciones sobre
datos personales, tales como la recolección, almacenamiento, uso,
circulación o supresión.

Principios

Ley 1581 de 2012	Ley 1266 de 2008
Veracidad o calidad	Veracidad o calidad
Finalidad	Finalidad
Acceso y circulación restringida	Circulación restringida
Seguridad	Seguridad
Confidencialidad	Confidencialidad
Transparencia	**Temporalidad**
Legalidad	**Interpretación integral de derechos constitucionales**
Libertad	

Aspectos claves de los Principios

- Libertad: El tratamiento solo puede efectuarse con el consentimiento previo y expreso del titular; no se pueden obtener o divulgar sin previa autorización.
- Finalidad: Propósito explicito, legitimo y predeterminado.
- Acceso y circulación restringida: Protección y transferencia.
- Veracidad: La información sujeta a tratamiento debe ser veraz, completa y exacta.
- Seguridad: Medidas técnicas, humanas y administrativas.
- Confidencialidad: Reserva información.

Contenido de la norma

CATEGORIAS ESPECIALES DE DATOS

- Datos sensibles

Aquellos que afectan la intimidad de la personas o cuyo uso indebido puede generar discriminación. (Origen racial o étnico, orientación política, convicciones filosóficas o religiosas, pertenencia a sindicatos u organizaciones sociales o de derechos humanos, datos de salud, vida sexual y biométricos).

Se prohíbe el tratamiento de datos sensibles salvo las excepciones del artículo 6 de la ley.

CATEGORIAS ESPECIALES DE DATOS

-Datos personales de menores
Se proscribe el tratamiento de datos personales de menores de edad salvo aquellos datos que sean de naturaleza pública.

La Corte Constitucional precisó que tal prohibición debe interpretarse en el sentido de que los datos personales de los menores de 18 años, pueden ser tratados, siempre y cuando el fin que se persiga con dicho tratamiento responda al interés superior de los menores y se asegure el respeto de sus derechos prevalentes.

Sujetos

- Responsable del Tratamiento.

PN o PJ que decide sobre los datos contenidos en una BD.

- Encargado del Tratamiento.

PN o PJ que realiza el tratamiento de datos personales por cuenta del Responsable.

Derecho de los titulares

- CARS. Conocer, Actualizar, Rectificar y Suprimir.
- Solicitar prueba de su autorizacion.
- Ser informado por el responsable o encargado del uso de sus datos.
- Presentar quejas a la SIC.
- Revocar su autorización.

Deberes de los responsables

- Informar al titular: Que tratamiento le darán a los datos.
- El carácter facultativo de la respuesta a las preguntas cuando sean datos sensibles y de menores.
- Derechos del titular.
- Identificación, dirección física y electrónica y teléfono del responsable.
- Conservar la información en condiciones de Seguridad.
- Actualizar la Información.
- Rectificar la información.
- Exigir al encargado condiciones de seguridad.
- Tramitar consultas.
- Adoptar un manual interno de politicas y procedimientos.

Autoridad y funciones

Delegatura de Protección de Datos Personales.

- Velar por el cumplimiento de las normas y leyes vigentes y proponer nuevas disposiciones.
- Disponer el bloqueo temporal de los datos cuando, de la solicitud y de las pruebas aportadas por el Titular, se identifique un riesgo cierto de vulneración de sus derechos fundamentales, y dicho bloqueo sea necesario para protegerlos mientras se adopta una decisión definitiva.
- Proferir las declaraciones de conformidad sobre las transferencias internacionales de datos.
- Decidir los recursos de reposición y las solicitudes de revocatoria directa que se interpongan contra los actos que expida, así como los de apelación que se interpongan contra los actos expedidos por la Dirección a su cargo.

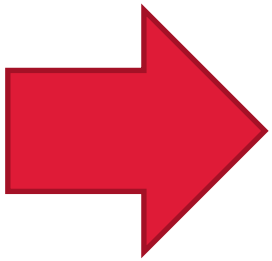
El objeto de protección.

El derecho constitucional que tienen todas las personas a :

Conocer

Actualizar

Rectificar



Las informaciones que se hayan recogido sobre ellas en bases de datos o archivos

Derecho a la Información: ART. 20. Se garantiza a toda persona la libertad de (…) informar y recibir información veraz e imparcial (…)

¿Qué tipo de base de datos o archivos los cobija esta ley?

- Datos personales registrados en cualquier base de datos que sean susceptibles de tratamiento por entidades públicas y privadas

Categoría especiales de Datos

Datos sensibles

- Afectan la intimidad del titular
- Su uso indebido pueden generar discriminación
- Datos relativos a la salud, vida sexual y datos biométricos

Esta prohibido el tratamiento de datos sensibles, salvo las excepciones que establece la ley

Tratamiento de datos personales de niños, niñas y adolescentes

Queda proscrito el Tratamiento de datos personales de niños, niñas y adolescentes, salvo aquellos datos que sean de naturaleza pública.

La especial protección que se da a los datos personales de niños, niñas y adolescentes, es una proyección razonable que se desprende de su condición de sujetos que gozan de una especial protección constitucional.

El Gobierno Nacional reglamentará la materia, dentro de los seis (6) meses siguientes a la promulgación de esta ley.

Autorización del titular de la información

Siempre, se requerirá la autorización previa e informada del Titular, la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta posterior.

¿Cuándo no es necesario la autorización previa?

- Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial;
- Datos de naturaleza pública;
- Casos de urgencia médica o sanitaria;
- Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos;
- Datos relacionados con el Registro Civil de las Personas.

Quien acceda a los datos personales sin que medie autorización previa deberá en todo caso cumplir con las disposiciones contenidas en la presente ley.

¿Porque medios se suministra la información?

La información solicitada podrá ser suministrada por cualquier medio, incluyendo los electrónicos, según lo requiera el Titular.

Deber de informar al Titular del Dato

Cuando el responsable del Tratamiento solicita al titular del dato la autorización, debe informarle de manera clara y expresa lo siguiente:

a) El Tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo;

b) El carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando estas versen sobre datos sensibles o sobre los datos de las niñas, niños y adolescentes;

c) Los derechos que le asisten como Titular;

d) La identificación, dirección física o electrónica y teléfono del Responsable del Tratamiento.

El Responsable del Tratamiento deberá conservar prueba del cumplimiento de estos requisitos cuando el Titular lo solicite, y entregarle copia de esta.

Personas a quienes se les puede suministrar la información

- La información que reúna las condiciones establecidas en la ley de protección de datos, podrá suministrarse a las siguientes personas:

a. A los Titulares, sus causahabientes o sus representantes legales;

b. A las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial;

c. A los terceros autorizados por el Titular o por la ley.

Procedimientos
Consulta

La consulta será atendida en un término máximo de diez (10) días hábiles contados a partir de la fecha de recibo de la misma. Cuando no fuere posible atender la consulta dentro de dicho término, se informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término.

Procedimientos
Reclamos

- El reclamo se formulará mediante solicitud dirigida al Responsable del Tratamiento o al Encargado del Tratamiento.
- Si el reclamo resulta incompleto, se requerirá al interesado dentro de los cinco (5) días siguientes a la recepción del reclamo para que subsane las fallas.
- Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo.
- En caso de que quien reciba el reclamo no sea competente para resolverlo, dará traslado a quien corresponda en un término máximo de dos (2) días hábiles e informará de la situación al interesado.
- El término máximo para atender el reclamo será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo.

Tener en cuenta el requisito de procedibilidad

Deberes de los Responsables y Encargados del tratamiento

- **Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data**
- Solicitar y conservar, en las condiciones previstas en la presente ley, copia de la respectiva autorización otorgada por el Titular
- Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada
- Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;
- Actualizar la información, comunicando de forma oportuna al Encargado del Tratamiento.

Deberes de los Responsables y Encargados del tratamiento

- Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular;
- **Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y en especial, para la atención de consultas y reclamos;**
- Informar al Encargado del Tratamiento cuando determinada información se encuentra en discusión por parte del Titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo;
- Informar a solicitud del Titular sobre el uso dado a sus datos;
- Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.
- Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

Aspectos penales

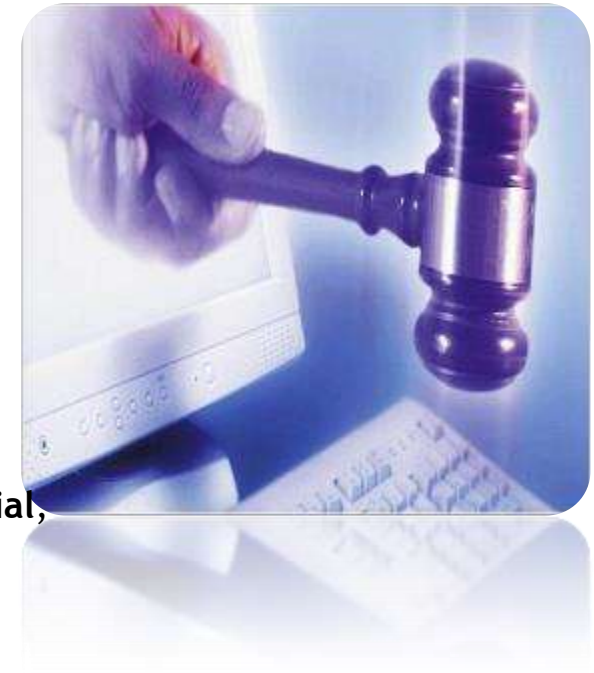
- LEY 1273 DE 2009.

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

La Ley 1273 de 2009

DELITOS QUE UTILIZAN LOS SISTEMAS COMO UN MEDIO ATENTA CONTRA BIENES JURÍDICOS TUTELADOS

- **libertad individual**
- **la libertad sexual**
- **la integridad moral**
- **patrimonio económico,**
- **la fe pública,**
- **los derechos de autor,**
- **el orden económico y social,**
- **la seguridad pública**
- **la administración pública.**



NUEVO SISTEMA DE PROTECCIÓN A BIENES JURÍDICOS TUTELABLES LA INFORMACIÓN Y LOS DATOS

sancionando a aquellas personas que:

- *accedan,*
- *obstaculicen,*
- *intercepten,*
- *dañen o usen de manera maliciosa software o tecnología*

ASPECTOS RELACIONADOS CON LA LEY 1273 DE 2009

ARTÍCULO 1 LA LEY 1273 DE 2009

introduce a la Ley 599 de 2000 en el Título VII Bis que se conoce con el nombre

"De la protección de la información y de los datos"

Artículo 269 A Acceso abusivo a un sistema informático. 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 1000 salarios mínimos legales mensuales vigentes".

Hacking, persona versada en el uso de los sistemas, quien mediante de software o manipulación de códigos binarios, tiene la capacidad de ingresar a un sistema de forma no autorizada y que se conoce popularmente como hacker o pirata cibernético

ASPECTOS RELACIONADOS CON LA LEY 1273 DE 2009

artículo 269 B 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"

el individuo, utiliza un medio o sistema tecnológico, para interceptar información o datos, que se encuentran en los sistemas informáticos, sin tener la autorización debida para acceder a estas, este procedimiento puede realizarse desde el lugar de origen o de una zona en donde tenga fácil acceso a un sistema informático

ASPECTOS RELACIONADOS CON LA LEY 1273 DE 2009

Artículo 269 D, 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 1000 salarios mínimos legales mensuales vigentes"

Individuo interfiere en el estado de un elemento que contiene información o bases de datos, el cual cambia, perturba e inclusive elimina, y además extrae información del mismo sin tener la autorización para realizar dicho procedimiento, esto constituye una conducta delictiva en el uso de los medios electrónicos.

ASPECTOS RELACIONADOS CON LA LEY 1273 DE 2009

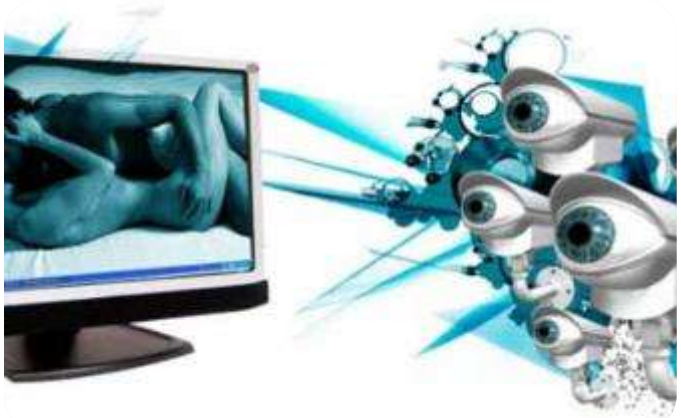
Artículo 269 E Uso De Software Malicioso. "El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes"

software llamado "malware", el cual es empleado hábilmente para diferentes actividades, por medio de las cuales se puede añadir o copiar software y de igual manera extraer programas de los sistemas informáticos. Este procedimiento genera una serie de daños en los medios tecnológicos e informáticos

ASPECTOS RELACIONADOS CON LA LEY 1273 DE 2009

ARTÍCULO 269 F, 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"

Sujeto lleva a cabo una serie de actividades como enviar, tomar y sustraer información privada de un sistema de información de una empresa o cualquier actividad económica, ya sea para emplearlos con fines personales o para beneficiar otras personas, a cambio de una remuneración económica u otra razón.



INQUIETUDES – COMENTARIOS

GRACIAS

Ivan Dario Marrugo Jimenez
Abogado
Twitter: @imarrugoj