



EXPRESO CARTAGO LTDA USO Y MANEJO DE RECURSOS INFORMÁTICOS

Código P-GD-03

Edición: 01

Fecha Edición 05/009/2011

Página 1 de 11

1. OBJETIVO

Indicar a los empleados de la organización el procedimiento a seguir en el manejo y uso de todos los elementos relacionados con equipos de informática y correo electrónico, para el desarrollo de actividades o cargos asignados y de sus funciones a realizar dentro de la organización.

2. ALCANCE

Se aplica para todo el personal de la organización que utilice los equipos de informática y correo electrónico

3. REFERENCIA

[La Ley 1273 de 2009 \(Medio Magnético\)](#)

4. DEFINICIONES

ARCHIVO ADJUNTO:

Es un archivo que se transmite junto a un mensaje de correo electrónico.

BUZÓN DE CORREO:

Área para almacenar los mensajes de correo electrónico provenientes de un servidor.

CORREO ELECTRÓNICO:

Es un servicio de red que permite a usuarios enviar y recibir mensajes mediante sistemas de comunicación electrónica.

DOMINIO:

Es un nombre base que agrupa a un conjunto de equipos o dispositivos, que permite proporcionar nombres de equipo más fácil de recordar que una dirección numérica de Internet.

FREEWARE:

Tipo de software de computadora que se distribuye sin coste y por tiempo ilimitado, siendo una variante gratuita del shareware, en el que la meta es lograr que un usuario pague, usualmente después de un tiempo de prueba ("trial") limitado y con la finalidad de habilitar toda la funcionalidad. A veces se incluye el código fuente, pero no es lo usual.

HARDWARE:

Cualquier componente físico tecnológico, que trabaja o interactúa de algún modo con la computadora. No sólo incluye elementos internos como el disco duro, CD-ROM, disquetera, sino que también hace referencia al cableado, circuitos, gabinete, etc. E incluso hace referencia a elementos externos como la impresora, el mouse, el teclado, el monitor y demás periféricos.



EXPRESO CARTAGO LTDA USO Y MANEJO DE RECURSOS INFORMÁTICOS

Código P-GD-03

Edición: 01

Fecha Edición 05/009/2011

Página 2 de 11

INTERNET:

Es una red mundial con millones de servidores conectados. Estos pueden intercambiar información y establecer distintos servicios tales como visitar páginas de portales, correo electrónico, charlar por medio del teclado en los salones creados para este servicio, entre otros.

INTRANET:

Red propia de una organización, diseñada y desarrollada siguiendo los protocolos propios de Internet, en particular el protocolo TCP/IP. Puede tratarse de una red aislada, es decir no contactada a Internet.

SHAREWARE:

Modalidad de distribución de software, tanto como juegos como programas utilitarios, para que el usuario pueda evaluar de forma gratuita el producto, por un tiempo especificado, aunque también las limitaciones pueden estar en algunas de las formas de uso o las capacidades finales.

SOFTWARE:

Conjunto de programas, instrucciones y reglas informáticas que permiten ejecutar distintas tareas en una computadora.

USUARIO:

Persona, oficina, organización o grupo de personas a quien la organización asigna una cuenta de trabajo en el domino.

5. PROCESO

A continuación se plantean una serie de recomendaciones que pretende garantizar su correcta utilización, disponibilidad y nivel de servicio de los recursos informáticos de la organización.

4.1 Equipos de Informática

- El equipo solo puede ser usado para fines de la organización y para apoyo de las actividades del trabajo del usuario.
- El computador debe tener los programas con su licencia de funcionamiento y los iconos o accesos directos solo de los programas que sean necesarios para el cumplimiento de las funciones al cargo asignado.
- La instalación de software, freeware, shareware como Yahoo! Messenger, MSM, etc., el usuario debe solicitar la autorización del personal calificado para hacerlo y que esto será solamente utilizado en beneficio de la actividad organizacional
- No es permitido la instalación software o programas que provengan del exterior Internet o medios físicos como disquete, USB o CD-ROM.
- Todo tipo de archivos, programas, freeware, shareware, sin su respectiva autorización de su uso, serán eliminados de su PC o equipo de Informática.



EXPRESO CARTAGO LTDA USO Y MANEJO DE RECURSOS INFORMÁTICOS

Código P-GD-03

Edición: 01

Fecha Edición 05/009/2011

Página 3 de 11

- La revisión de los equipos PC o de informática, se hará en forma periódica, para verificar su buen funcionamiento y que los programas instalados sean los que solo la Organización necesita para realizar las funciones asignadas, (como mínimo cada tres meses)
- La configuración, revisión de cualquier componente de hardware o software del PC o equipo de informática, labores de mantenimiento preventivo, etc. sólo puede ser realizada por el proveedor autorizado por la Gerencia General
- Todo equipo debe tener la protección en la parte eléctrica con un estabilizador, regulador, o UPS. Sin esto no podrá hacer la utilización del PC o equipo de Informática.
- La instalación o descarga de archivos de música en cualquier tipo de formato está prohibida; estos, así como aquellos archivos que no tengan relación alguna con el trabajo que realiza en la Organización, si estos no están autorizados, serán eliminados PC o equipo de Informática
- Se prohíbe a los empleados de la organización, el ingreso y salida de información por medio de disquetes, unidad de U.S.B. y/o CD-ROM.
- El sitio de trabajo de su PC o equipo de Informática debe tener los estándares de soporte, comodidad tanto para el PC o equipo de Informática, como para el usuario, así como su aseo general del sitio o ubicación del mismo.
- El tomar líquidos, comer cualquier tipo de alimentos en el puesto de trabajo del PC o equipo de Informática está totalmente prohibido.

4.2 Correo Electrónico

4.2.1. Normas por parte de los usuarios

4.2.1.1 Volumen

Cada empleado que use el servicio de correo electrónico incide directamente en el rendimiento de la red de datos de la Organización, la cual tiene una capacidad limitada y la carga excesiva sobre esta red puede causar interrupciones y demoras en la transmisión de datos críticos y prioritarios para el negocio.

Algunas recomendaciones sobre la forma de reducir el volumen del correo generado, son las siguientes:

- Los mensajes deberían enviarse únicamente a esas personas que realmente necesiten recibir la información.
- Evite reenviar mensajes que contienen cadenas, avisos de un nuevo y peligroso virus, desacreditar marcas y productos, ya que ellos sólo buscan alimentar las listas de correo del sitio que los originan y en algunos casos simplemente, congestionar el tráfico en algunos tramos de la red.
- Evite el envío de material pornográfico y pida a sus contactos que se abstengan de enviárselo.
- En los últimos años, la infraestructura de mensajería electrónica se ha beneficiado de mejoras en cuanto al rendimiento y confiabilidad. Sin embargo, la demanda en el uso del correo también se ha incrementado. Se requiere que los usuarios aseguren que el volumen del correo electrónico no exceda la capacidad de nuestro sistema.



EXPRESO CARTAGO LTDA USO Y MANEJO DE RECURSOS INFORMÁTICOS

Código P-GD-03

Edición: 01

Fecha Edición 05/009/2011

Página 4 de 11

- Hay varias cosas que se esperan de nuestros usuarios. Ante todo, esperamos la buena administración de los buzones de correo.
- Desarrolle el hábito de borrar los mensajes viejos e innecesarios periódicamente.
- Configure su programa de correo para que elimine los mensajes definitivamente cada vez que decida salir del programa. Recuerde que los mensajes que se borran van a residir a la carpeta de “mensajes eliminados”.
- Minimice el hábito de adjuntar archivos a los mensajes que podrían ser enviados usando texto plano dentro del cuerpo del mensaje.

4.2.1.2 Abuso

La mensajería electrónica, es suministrada únicamente para propósitos de negocio. La Organización reconoce que algún correo personal será inevitable, sin embargo, tal correspondencia debería permanecer la menor cantidad de tiempo almacenada y su envío y recepción también deberían ser mínimos. La solicitud y/o distribución de material que no esté relacionado con el negocio, particularmente aquel del que se obtiene un beneficio personal, está estrictamente prohibido.


El abuso del correo electrónico es un problema serio y es considerado de la misma forma que el abuso de equipos e información de propiedad de la organización. El correo electrónico no esta exento de las consideraciones sociales, éticas y legales que nos convierten en ciudadanos responsables.

Los empleados de la Organización, deben asegurarse de no usar el correo electrónico para:

- Representarse ellos mismos como otras personas.
- Transmitir o almacenar material que podría ser considerado inapropiado, ofensivo o irrespetuoso a los demás.
- Transmitir o almacenar videos, imágenes y/o texto considerado pornográfico.
- Transmitir o almacenar mensajes obscenos o amenazantes.
- Originar o retransmitir las cartas conocidas como “cadenas”.
- Acosar, hostigar o asediar a otros empleados.
- Proveer información acerca de lista de los empleados de la Organización a terceros.
- Participar en actividades que interfieren con su trabajo o el trabajo de otros empleados.
- Interferir con la operación del sistema de mensajería de la Organización.
- Violar cualquier ley o derechos de cualquier persona.
- Instar, apoyar o promover la afiliación con un partido político o persona.
- Generar mensajes para beneficio personal.

Los empleados no deberían presentar puntos de vista o ideas como representantes de la organización, a menos que lo estén haciendo como parte de la función que desempeñan dentro de la organización. Los usuarios necesitan recordar que ellos son siempre identificables cuando expresen puntos de vista personales deberán siempre hacer claridad de cuando se están representando a ellos mismos o lo hacen en nombre de la organización.

Los empleados no deben nunca deliberadamente generar mensajes que dañen, inhabiliten o interrumpan parcial o totalmente el servicio de mensajería electrónica de la organización.

	<p align="center">EXPRESO CARTAGO LTDA USO Y MANEJO DE RECURSOS INFORMÁTICOS</p>		
Código P-GD-03	Edición: 01	Fecha Edición 05/009/2011	Página 5 de 11

4.1.2.3 Seguridad

La Organización ha delegado en sus empleados la libertad para generar y recibir mensajes sin excesiva vigilancia por tal razón es conveniente tener en cuenta las siguientes consideraciones:

- La organización depende de sus colaboradores para el tratamiento adecuado de información o asuntos delicados y el impacto que pudiera generar su distribución. Los mensajes que contiene en ese tipo de información recibida por socios de negocios, competidores, y/o el público en general, pueden causar daños serios a la organización. La discreción debe ser usada cuando se establezcan comunicaciones con empleados que no pertenecen a la Organización.
- En particular, la información “privada” y “confidencial” nunca debe ser transmitida fuera de la organización pues de ninguna manera garantiza la privacidad de la mensajería electrónica.
- El siguiente extracto resume la política de la organización respecto a la privacidad de los mensajes electrónicos. “Todo correo electrónico, conferencia de datos, y correo de voz almacenado sobre un equipo de la organización es considerado de propiedad de LA ORGANIZACIÓN. Por lo tanto, los funcionarios asignados para tal fin, pueden periódicamente chequear el contenido de los mensajes almacenados en tales equipos ya sea porque se requiere corregir problemas de la red o simplemente para establecer el uso apropiado de los mensajes recibidos o generados. Usted no puede esperar privacidad personal de los mensajes enviados, recibidos o almacenados en esos equipos”.
- Las cuentas de mensajería electrónica están normalmente protegidas por una contraseña, la cual reduce el riesgo de acceso por parte de los intrusos. Esta protección, sin embargo, no confiere ninguna característica especial a los mensajes almacenados en equipos de propiedad de la Organización y por tanto serán susceptibles de ser controlados por la organización.

Para este control de seguridad EL Representante ante la Gerencia del Sistema de Gestión en Control y Seguridad, tendrá en sobre cerrado las claves de cada uno de los equipos que la organización tiene.

4.2.2 Normas por parte de la organización

- Se asignará una cuenta por usuario.
- La cuenta se dará de baja en el momento que el personal deje de pertenecer a la organización.
- La organización se reserva el derecho de enviar al usuario la información que considere necesaria por el correo electrónico, como un medio de comunicación organizacional
- La vigencia y espacio de las cuentas será definido por la Gerencia General y/o la Dirección Comercial de acuerdo a los recursos disponibles, con base en las necesidades del usuario.



EXPRESO CARTAGO LTDA USO Y MANEJO DE RECURSOS INFORMÁTICOS

Código P-GD-03

Edición: 01

Fecha Edición 05/009/2011

Página 6 de 11

4.3 Internet e Intranet

4.3.1 Internet

Desde el equipo asignado a cada usuario será posible hacer uso de la red de Internet, únicamente para fines de interés laboral y no personal.

4.3.2 Intranet

La utilización de freeware, shareware como Yahoo! Messenger, MSM, etc esta autorizada por la organización para servicio de intranet ó herramienta de comunicación en beneficio de la actividad organización, manejado dentro del horario laboral en las instalaciones de la organización.

El cambio de red o suspensión de esta será autorizado por la Gerencia General.

La política adoptada sobre el uso de correo electrónico será de igual aplicación para otros recursos de la intranet y el Internet.

4.4 Backup

El objetivo del backup es proteger los datos y aplicaciones de software contra todo tipo de fallas que puedan ocurrir y posibilitar la recuperación de fallas en el menor tiempo posible y sin la pérdida de datos.

Los archivos que deben tener copias de respaldo son:

1. Backup de los documentos y correos de cada equipo en el dominio
2. Backup del Sistema de Contabilidad
3. Backup del Sistema de Gestión en Control y Seguridad
4. Backup de los sistemas operativos

El Backup se realiza diariamente en forma magnética y la copia se almacena fuera de la organización

El Backups para los numerales 2,3 y4 se realizará diariamente con una (1) copia que se guarda en el servidor de archivos y la 2 copia, el administrador de sistemas la guardada fuera de la organización en un disco USB o se la entregan al gerente para que sea guardada fuera de las instalaciones.

4.5 Claves

Los equipos de cómputo tienen una clave para su ingreso. Su cambio se realizará cada tres (3) meses y está a cargo del operador de sistemas, estas claves de acceso al equipo son conocidas



EXPRESO CARTAGO LTDA USO Y MANEJO DE RECURSOS INFORMÁTICOS

Código P-GD-03

Edición: 01

Fecha Edición 05/009/2011

Página 7 de 11

para el administrador para un control sobre los equipos, el administrador es el único que puede cambiar las claves.

4.6 Responsabilidades

Los usuarios son responsables de cumplir los puntos señalados en este documento para el mejor manejo de los recursos informáticos.

La Gerencia General es responsable de la correcta utilización de los equipos de cómputo, del servidor de correo, de la cuenta de correo, del Internet y del software con los que cuenta la organización

4.7 Privacidad y confidencialidad de la información

La organización no realizará monitoreo o inspecciones de un buzón de correo electrónico sin el consentimiento del usuario, salvo en los casos detallados a continuación:

- Algún requerimiento legal.
- Sospecha de violación de la política interna de la organización o de leyes locales, nacionales e internacionales.
- Circunstancias de emergencia, donde no actuar pudiera repercutir gravemente en el servicio general a los clientes y proveedores de la organización.

4.8 Acciones Disciplinarias


Cuando se determine que hubo una violación a lo establecido en este procedimiento, se aplicaran las medidas correctivas y disciplinarias necesarias de acuerdo con la gravedad de la infracción, tomando como base el reglamento interno de la organización.

En caso que el usuario no sea empleado regular de la organización, el Gerente o la persona que éste designe recibirán el asesoramiento pertinente para determinar la acción a seguir.

SEGURIDAD EN LA RED

La Ley 1273 de 2009 creó nuevos tipos penales relacionados con delitos informáticos y la protección de la información y de los datos con penas de prisión de hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes.

El 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273 “Por medio del 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”.

	<p align="center">EXPRESO CARTAGO LTDA USO Y MANEJO DE RECURSOS INFORMÁTICOS</p>		
Código P-GD-03	Edición: 01	Fecha Edición 05/009/2011	Página 8 de 11

Dicha ley tipificó como delitos una serie de conductas relacionadas con el manejo de datos personales, por lo que es de gran importancia que las empresas se blinden jurídicamente para evitar incurrir en alguno de estos tipos penales.

No hay que olvidar que los avances tecnológicos y el empleo de los mismos para apropiarse ilícitamente del patrimonio de terceros a través de clonación de tarjetas bancarias, vulneración y alteración de los sistemas de cómputo para recibir servicios y transferencias electrónicas de fondos mediante manipulación de programas y afectación de los cajeros automáticos, entre otras, son conductas cada vez más usuales en todas partes del mundo. Según la Revista Cara y Sello, durante el 2007 en Colombia las empresas perdieron más de 6.6 billones de pesos a raíz de delitos informáticos.

De ahí la importancia de esta ley, que adiciona al Código Penal colombiano el Título VII BIS denominado "De la Protección de la información y de los datos" que divide en dos capítulos, a saber: "De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos" y "De los atentados informáticos y otras infracciones".

El capítulo primero adiciona el siguiente articulado (subrayado fuera del texto):

Artículo 269A: 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.

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 1000 salarios mínimos legales mensuales vigentes.



EXPRESO CARTAGO LTDA
USO Y MANEJO DE RECURSOS INFORMÁTICOS

Código P-GD-03

Edición: 01

Fecha Edición 05/009/2011

Página 9 de 11

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 1000 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.

Al respecto es importante aclarar que la Ley 1266 de 2008 definió el término dato personal como “cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica”. Dicho artículo obliga a las empresas un especial cuidado en el manejo de los datos personales de sus empleados, toda vez que la ley obliga a quien “sustraiga” e “intercepte” dichos datos a pedir autorización al titular de los mismos.

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 1000 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.

Es primordial mencionar que este artículo tipifica lo que comúnmente se denomina “phishing”, modalidad de estafa que usualmente utiliza como medio el correo electrónico pero que cada vez con más frecuencia utilizan otros medios de propagación como por ejemplo la mensajería instantánea o las redes sociales. Según la Unidad de Delitos Informáticos de la Policía Judicial (Dijín) con esta modalidad se robaron más de 3.500 millones de pesos de usuarios del sistema financiero en el 2006[2].

Un punto importante a considerar es que el artículo 269H agrega como circunstancias de agravación punitiva de los tipos penales descritos anteriormente el aumento de la pena de la mitad a las tres cuartas partes si la conducta se cometiere:



EXPRESO CARTAGO LTDA
USO Y MANEJO DE RECURSOS INFORMÁTICOS

Código P-GD-03

Edición: 01

Fecha Edición 05/009/2011

Página 10 de 11

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.

Es de anotar que estos tipos penales obligan tanto a empresas como a personas naturales a prestar especial atención al tratamiento de equipos informáticos así como al tratamiento de los datos personales más teniendo en cuenta la circunstancia de agravación del inciso 3 del artículo 269H que señala “por quien tuviere un vínculo contractual con el poseedor de la información”.

Por lo tanto, se hace necesario tener unas condiciones de contratación, tanto con empleados como con contratistas, claras y precisas para evitar incurrir en la tipificación penal.

Por su parte, el capítulo segundo establece:

Artículo 269I: HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239[3] 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 del Código Penal[4], es decir, penas de prisión de tres (3) a ocho (8) años.

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 1500 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.

Así mismo, la Ley 1273 agrega como circunstancia de mayor punibilidad en el artículo 58 del Código Penal el hecho de realizar las conductas punibles utilizando medios informáticos, electrónicos ó telemáticos.



EXPRESO CARTAGO LTDA
USO Y MANEJO DE RECURSOS INFORMÁTICOS

Código P-GD-03

Edición: 01

Fecha Edición 05/009/2011

Página 11 de 11

Como se puede apreciar, la Ley 1273 es un paso importante en la lucha contra los delitos informáticos en Colombia, por lo que es necesario que se esté preparado legalmente para enfrentar los retos que plantea.

En este sentido y desde un punto de vista empresarial, la nueva ley pone de presente la necesidad para los empleadores de crear mecanismos idóneos para la protección de uno de sus activos más valiosos como lo es la información.

Las empresas deben aprovechar la expedición de esta ley para adecuar sus contratos de trabajo, establecer deberes y sanciones a los trabajadores en los reglamentos internos de trabajo, celebrar acuerdos de confidencialidad con los mismos y crear puestos de trabajo encargados de velar por la seguridad de la información.

Por otra parte, es necesario regular aspectos de las nuevas modalidades laborales tales como el teletrabajo o los trabajos desde la residencia de los trabajadores los cuales exigen un nivel más alto de supervisión al manejo de la información.

Así mismo, resulta conveniente dictar charlas y seminarios al interior de las organizaciones con el fin de que los trabajadores sean conscientes del nuevo rol que les corresponde en el nuevo mundo de la informática.

Lo anterior, teniendo en cuenta los perjuicios patrimoniales a los que se pueden enfrentar los empleadores debido al uso inadecuado de la información por parte de sus trabajadores y demás contratistas.

Pero más allá de ese importante factor, con la promulgación de esta ley se obtiene una herramienta importante para denunciar los hechos delictivos a los que se pueda ver afectado, un cambio importante si se tiene en cuenta que anteriormente las empresas no denunciaban dichos hechos no sólo para evitar daños en su reputación sino por no tener herramientas especiales.

Control de Cambios		
Edición	Descripción de la Modificación	Fecha de Cambio
01	Elaboración Inicial	Sin

Revisó

Aprobó

Katerine Escobar Sánchez
Líder Gestión Documental

Wilson Ernesto Serna Ospina
Gerente General