Dirección de Recursos Humanos

Política Interna de Trabajo

Política para la prevención de delitos informáticos

RH-PO-013

Versión	2012-12-20

Historia de Versiones

Fecha	Autor	Cambios	Secciones modificadas
2012-10-15	Bedese Asesores	Original	Todas
2012-11-15	Tatiana Lizano y Cristina Hernández	Revisión y adaptación	Todas
2012-11-16	Bedese Asesores	Revisión legal	Todas
2012-12-20	Tatiana Lizano	Revisión y adaptación final	Todas
2013-01-10	Tatiana Lizano	Modificaciones	1,4, y Artículos 2,6 ,8 y 9

CONTENIDOS

1 Introducción

1.1 Propósito

Regular en materia de cumplimiento con la Ley de Delitos Informáticos que introdujo reformas al código Penal de Costa Rica. Brindar información y reglas para asegurar que la empresa y sus colaboradores conocen y cumplen con la normativa vigente.

1.2 Audiencia

Este documento es para uso de todo el personal de la empresa, sus filiales o subsidiarias. Su acatamiento es obligatorio para todos sus colaboradores sin distinción de su puesto, función o forma de contratación, en el desempeño de sus funciones.

1.3 Alcance

Lo definido en este documento es aplicable a todas las áreas funcionales de la empresa, proyectos y sus colaboradores.

1.4 Terminología

Término	Definición
Herramientas informáticas de la empresa	Los siguientes componentes: Redes inalámbricas (WLAN), redes de área local (LAN), redes privadas virtuales (VPN), servidores de correo (mail servers), servidores web (web servers), servidores de aplicaciones (Application servers), computadoras host, servidores de archivos (file servers), servidores de fax y máquinas de fax, servidores de comunicaciones (communications servers), estaciones de trabajo (workstations), laptops, software, y redes de cómputo internas y externas (incluyendo redes de intercambio electrónico de datos, Internet, grupos de noticias, servicios comerciales en línea, sistemas de tableros de mensajes -bulletin board systems-, y sistemas de correo electrónico), dispositivos móviles que son accesados utilizando directa o indirectamente la tecnología de telecomunicaciones facilitada por la empresa, sus filiales o subsidiarias.
Herramientas de monitoreo	Websense y administradores de ancho de banda.
Usuario	Cualquier trabajador de la empresa, sus filiales o subsidiarias que utilice el recurso informático de la empresa, sin distinción de su puesto, función o forma de contratación, dentro o fuera de las instalaciones físicas de la empresa.
Password	Cualquier conjunto de caracteres brindado por la empresa o creado por el usuario para el acceso seguro al recurso informático o tecnológico de la empresa.

Red Social	Cualquier página electrónica a partir de la cual haya un intercambio de información entre usuarios, o en la cual sea posible interactuar con otras personas bajo el intercambio de información, la mera exposición de datos de cualquier índole, almacenamiento, modificación de los mismos.
Tipos penales	Cualquier delito que esté contenido dentro de la Ley de Delitos Informáticos que reformó el Código Penal.
Recurso tecnológico o informático	Todas las herramientas informáticas de la empresa a disposición del usuario o trabajador para el ejercicio de la funciones para las que fue contratado(a).
Categorías no permitidas	Categorías o servicios que la empresa ha designado como no accesibles desde su red o bajo el uso de sus recursos informáticos. Estas categorías o servicios están detallados en el documento de políticas empresariales.
Visitante	Cualquier tercero ajeno a la empresa que se encuentre de paso por las instalaciones de la empresa, sus filiales o subsidiarias.

1.5 Abreviaciones

Abreviación	Definición
RH	Departamento de Recursos Humanos
IT	Departamento de Tecnologías de Información

2 Política Interna de Trabajo para la prevención de delitos informáticos

2.1 Objetivo General

La presente Política interna de trabajo tiene como objetivo el establecer los lineamientos necesarios para la prevención de aquellas acciones que, con base a la Ley de Delitos Informáticos que introdujo reformas al Código Penal vigente en el país, son catalogadas como delitos. En este sentido, la empresa divulgará por medios idóneos dichas conductas y advertirá sobre las consecuencias tanto en el ámbito laboral, como en el penal, para aquellos trabajadores que incumplan la normativa citada.

Por lo tanto, se establece la siguiente política para la prevención de delitos informáticos de Grupo Avantica Inc., sus filiales o subsidiarias, en adelante denominada la empresa, regulación que se regirá por las siguientes condiciones:

2.2 Normas de Acatamiento General

Artículo 1: **Política General**. A partir de las reformas introducidas al Código Penal, mediante la llamada “Ley de Delitos Informáticos”, la empresa se ve en el deber de regular a nivel interno, todas aquellas posibles áreas que, a partir del giro comercial de la misma, la afectan de manera directa o indirecta. De ahí que se entiende que la presente política cubre aspectos relacionados a:

1. Uso de herramientas informáticas.
2. Protección de información confidencial.
3. El uso de las redes sociales y cualquier otro medio de entretenimiento o comunicación social informático.
4. Uso de datos personales de clientes y/o trabajadores de la misma.
5. Uso de páginas de internet y cualquier otra acción que la empresa determine siempre dentro del marco de la legislación laboral y la ley de delitos informáticos

2.3 Monitoreo y Control

Artículo 2: **Control de uso.** La empresa se reserva el derecho de implementar los programas necesarios para supervisar y monitorear la operación y uso de los recursos y herramientas informáticas suministradas a los colaboradores.

La supervisión de dichas actividades pueden incluir, sin ser esta lista taxativa: fiscalización de la actividad de los usuarios de su recurso informático en Internet, incluyendo los sitios visitados, los grupos de noticias utilizados, actividad en salas de chat autorizadas, materiales descargados y/o cargados

de/a la web, así como el envío y recepción de correos electrónicos, y supervisar el tiempo total utilizado en actividades relacionadas a Internet.

Esta política aplica igualmente para los trabajadores que realicen teletrabajo, viajes de negocios de la compañía y / o que utilicen remotamente la red de la empresa y en todo momento mientras estén utilizando los recursos tecnológicos de la empresa.

No solo se incluye dispositivos de la empresa, sino todo dispositivo que se conecte a las redes de la empresa.

En lo pertinente y en cuanto la empresa lo considere necesario, ésta podrá comunicar a las Autoridades Judiciales sobre cualquier sospecha en cuanto al mal uso de recursos informáticos de parte de los trabajadores de la misma.

Artículo 3: **Uso de recursos informáticos**. El recurso informático de la empresa puesto a disposición de sus colaboradores en calidad de usuarios, deberá ser utilizado solamente en el desarrollo de sus responsabilidades de trabajo y para el beneficio de la compañía. En tal sentido el usuario del recurso tecnológico de la empresa sólo podrá utilizarlo para actividades relacionadas al giro de la empresa y en ningún caso para actividades personales o privadas.

En el caso de que por un uso contrario a la política o a la Ley, de los recursos informáticos de la empresa, el trabajador cometa algún delito, se entenderá que éste responderá por los daños y perjuicios ocasionados a la empresa y / o a terceros, sin menoscabo de la responsabilidad penal que se le pueda acreditar al mismo.

Artículo 4: **Propiedad de recursos informáticos**. La empresa es propietaria de los recursos informáticos descritos en la presente política, así como de cualquier otra herramienta facilitada a los colaboradores para el mejor desempeño de sus labores. Asimismo, toda la información contenida en estos recursos y herramientas es considerada propiedad de la empresa. Los registros de los correos electrónicos, que surjan a través de la herramienta que se proporcione con ese fin, son considerados propiedad de la empresa.

En virtud de lo anterior, los colaboradores deberán dar un uso profesional al recurso tecnológico de la empresa.

Se espera un comportamiento decoroso y dentro de la ley por parte del usuario de los recursos de la empresa o recursos personales en su jornada laboral.

2.4 Regulaciones para el uso del recurso informático, las redes sociales y los medios de comunicación virtual

Artículo 5: **Correo electrónico.** El correo electrónico asignado a cada trabajador, es exclusivamente para uso laboral, con el fin de optimizar los servicios prestados por los colaboradores, por lo que está absolutamente

prohibido utilizar esta herramienta para usos personales u otros que pongan en peligro la imagen de la empresa o la integridad de la información de ésta o de sus clientes y proveedores.

El colaborador no deberá utilizar la cuenta de correo otorgada por la empresa para aspectos personales, de ahí que no deberá enviar desde esa dirección correos de esa índole. Igualmente, cualquier correo que no responda a las funciones desempeñadas dentro de la organización deberá ser borrado por el colaborador de forma inmediata.

Artículo 6: **Internet.** Internet es una herramienta necesaria para la prestación de servicios ofrecidos por la empresa, por lo que su utilización es principalmente para las actividades propias del giro normal de la empresa. Por lo tanto, la empresa no permite la utilización de redes sociales para el uso personal utilizando los recursos de la empresa.

En el caso de que un colaborador utilice herramientas informáticas de su propiedad, utilizando una red que no es fiscalizable por la empresa, la responsabilidad penal y / o civil en que incurra dicho colaborador será única para él.

Artículo 7: **Redes Sociales** y medios de entretenimiento análogos. Si por razones de trabajo se debe dar acceso a una red social, su uso deberá apegarse única y exclusivamente a las exigencias del servicio prestado al cliente, de ahí que el colaborador no podrá aprovechar tal acceso para efectos ajenos a los intereses de la empresa o de su puesto.

Artículo 8: **Claves.** La asignación y uso de usuarios y claves (“passwords”) que se le adjudiquen a los colaboradores en los respectivos sistemas y que contribuyan con el desempeño diario, son de uso estrictamente personal, por lo que su utilización y conservación será responsabilidad directa de cada colaborador.

No se permite a los colaboradores hacer del conocimiento de terceros o de compañeros de labores, independientemente de la posición de éstos dentro de la estructura jerárquica de la empresa, los usuarios y claves personales que les son asignados.

No obstante, los passwords que son asignados o creados como parte de los proyectos ya sea para desarrollo o pruebas, se deben administrar de acuerdo a las necesidades de cada proyecto y en común acuerdo con el cliente en los casos que así lo requiera.

Artículo 9: **Reglas de uso de recursos tecnológicos**. Los colaboradores que sean usuarios del recurso tecnológico de la empresa están sujetos a los siguientes términos de uso, las cuales son de cumplimiento obligatorio y podrán variar previa comunicación por escrito de la empresa:

- El usuario no debe instalar software sin la debida autorización. Este debe ser de uso libre o cumplir con todas las licencias de software y derechos de autor y con toda la legislación internacional sobre propiedad intelectual y actividades en línea. El usuario no está autorizado para realizar copias del software instalado en el recurso tecnológico de la empresa.
- El usuario no debe involucrarse de ninguna forma, ni promover actividades fraudulentas, ilegales, de corrupción, sexualmente explícitas o implícitas, obscenas, intimidantes, difamatorias, u otras inapropiadas a través del uso del recurso informático u otras herramientas propiedad de la empresa. El usuario que reciba este tipo de material o conozca del incumplimiento de esta política por parte de otro usuario, debe comunicarlo por escrito inmediatamente a su superior, al Departamento de Recursos Humanos o bien al Director de la organización.
- Ningún usuario está autorizado para involucrarse en ningún tipo de foros de discusión de temas fuera del ámbito laboral utilizando el recurso informático de la empresa. El recurso informático de la empresa no puede ser usado para la transmisión o almacenamiento de programas destructivos, solicitudes, material de índole político u otro tipo de uso no autorizado.
- El contenido de todas las comunicaciones autorizadas debe ser apropiado y conciso. El usuario tendrá el mismo cuidado al enviar correos electrónicos o cualquier otro tipo de comunicación electrónica. Todos los archivos que sean creados utilizando el recurso informático de la empresa podrán ser revisados por otros usuarios. El contenido de todos los equipos de la empresa puede ser revisado por otros usuarios de la misma empresa y en este sentido, el usuario actual que tenga asignado el equipo no podrá objetar dicha revisión ni las modificaciones que de dicha revisión sea necesario efectuar en el equipo. Estas revisiones siempre deberán ser realizadas en presencia del titular.
- El usuario está impedido para firmar, enviar, recibir, distribuir o revelar, información confidencial propiedad de la empresa a personas no autorizadas para tales efectos y con fines distintos a los estrictamente laborales. El incumplimiento de esta obligación facultará a la empresa a tomar acciones a nivel civil y penal.
- Ningún usuario está autorizado para instalar software de ningún tipo en el recurso informático de la empresa. Sólo está autorizado el uso del software instalado por el encargado de informática de la empresa. En la eventualidad que el usuario necesite software adicional no provisto por la empresa, el usuario deberá hacer una solicitud vía correo electrónico o mediante la herramienta de manejo de solicitudes que le provea la compañía con copia a su jefe inmediato para la aprobación respectiva. Dicha solicitud deberá incluir el propósito para ese software y la función que cumplirá a través del uso del mismo. No se permite encriptar información almacenada en los equipos de la compañía, sea esta de cualquier índole, sin antes contar con la autorización explícita de la empresa

- Todo el material instalado con autorización en el recurso informático de la empresa o descargado de Internet con autorización o provisto por otra fuente, deberá ser primero revisado con el fin de evitar el ingreso de virus informáticos o cualquier otro tipo de material dañino al recurso informático de la empresa. Cualquiera de los anteriores deberá ser reportado al departamento de informática de la empresa, quien deberá cerciorarse de revisar dicho material adecuadamente. La introducción de dicho material dentro del recurso informático de la empresa no estará autorizado hasta que se lleve a cabo exitosamente el examen anteriormente descrito.
- Los usuarios no deben enviar correos tipo “spam” o no solicitados a ninguna persona física o jurídica. De la misma forma, los usuarios no están facultados para utilizar el recurso informático de la empresa para el envío de correo basura o “spam”, así como tampoco están facultados para el envío o participación en “cadenas de correos”. Si algún usuario tiene necesidad de envío de este tipo de correos se revisará previamente con Recursos Humanos de la subsidiaria correspondiente para su análisis y aprobación.
- Todas las comunicaciones vía correo electrónico deberán incluir una leyenda identificando ese material como confidencial y protegido por la legislación costarricense.
- El usuario debe tomar todas las previsiones del caso con el fin de proteger cualquier password asignado para su uso personal. Los passwords deberían ser memorizados y no guardados en los recursos informáticos de la empresa, impresos o guardados en forma escrita en cualquier otro tipo de copia física. Los usuarios están impedidos para acceder el recurso informático de la empresa utilizando passwords asignados a otros usuarios.
- El usuario solamente deberá exportar a Internet o transmitir por correo electrónico o cualquier otro medio el material propiedad de la empresa, incluyendo tecnología de encriptación u otra tecnología restringida de la empresa, para fines estrictamente laborales.
- Salvo autorización escrita previa, el usuario únicamente podrá hacer uso de la clave personal y el nombre de usuario que le sea debidamente asignado por la empresa.
- Los usuarios únicamente podrán acceder, revisar o verificar información que haya sido dirigida de manera explícita a éstos por el titular de la misma o bien por la persona designada por el titular. No será permitido utilizar ninguna información personal, imagen o cualquier recurso de una persona sin su autorización. Esto incluye subir a redes sociales, medios de entretenimiento, páginas de la organización, blogs, o cualquier portal o herramienta de acceso público o privado.

Artículo 10: La revisión y uso del correo electrónico personal es permitido dentro de la empresa siempre y cuando éste sea revisado vía web y de forma razonable y responsable por parte de los trabajadores. Todas las disposiciones señaladas en la presente política respecto a la descarga, carga, envío,

recepción y disposición en general de la información serán de aplicación para cuando los trabajadores hagan uso de su correo electrónico personal.

Regulaciones especiales para el personal de IT
El personal del departamento de tecnologías de información (IT) realiza las tareas de monitoreo del uso de los recursos tecnológicos de la empresa. Por tanto se les brinda a los funcionarios de dicho departamento la potestad de realizar las siguientes tareas:

1. Monitoreo del ancho de banda y los sitios accedidos por los trabajadores.
2. Monitoreo de los equipos para asegurar el uso adecuado de los recursos tecnológicos.
3. Ante una sospecha de uso indebido del correo de la empresa, del correo personal, de las redes sociales o cualquier medio de entretenimiento, de los archivos electrónicos, o cualquier material tecnológico de o en la organización se realizará una auditoría in-situ del usuario en sospecha.

Cualquier incumplimiento de esta política o de lo definido en la ley de delitos informáticos detectado por el personal designado de IT o alertado por cualquier colaborador es causal de todas las consecuencias laborales, civiles y penales que permita la ley.

2.5 De los delitos que prevé la presente política

Artículo 11: Delitos tipificados por la ley. Para todos los efectos, y de conformidad con la reforma sufrida por el Código Penal, serán considerados como delitos informáticos, las siguientes conductas:

- “Corrupción”: quien mantenga o promueva la corrupción de una persona menor de edad o incapaz, con fines eróticos, pornográficos u obscenos, en exhibiciones o espectáculos públicos o privados, aunque la persona menor de edad o incapaz lo consienta. Lo anterior será extensivo a quien realice tal acción utilizando las redes sociales o cualquier otro medio informático o telemático, u otro medio de comunicación, busca encuentros de carácter sexual para sí, para otro o para grupos, con una persona menor de edad o incapaz, utiliza a estas personas para promover la corrupción o las obliga a realizar actos sexuales perversos, prematuros o excesivos, aunque la víctima consienta participar en ellos o verlos ejecutar.”

- “Violación de correspondencia o comunicaciones”: aquel quien con peligro o daño para la intimidad o privacidad de un tercero, y sin su autorización, se apodere, accede, modifique, altere, suprima, intervenga, intercepte, utilice, abra, difunda o desvíe de su destino documentos o comunicaciones dirigidos a otra persona. Podrán incluirse como responsables de este delito a:

- Las personas encargadas de la recolección, entrega o salvaguarda de los documentos comunicaciones.
- Las personas encargadas de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tengan acceso a dicho sistema o red, a los contenedores electrónicos, ópticos o magnéticos.

- "Violación de datos personales": aquel quien en beneficio propio o de un tercero, con peligro o daño para la intimidad o privacidad y sin la autorización del titular de los datos, se apodere, modifique, interfiera, acceda, copie, transmita, publique, difunda, recopile, inutilice, intercepte, retenga, venda, compre, desvíe para un fin distinto para el que fueron recolectados o dé un tratamiento no autorizado a las imágenes o datos de una persona física o jurídica almacenados en sistemas o redes informáticas o telemáticas, o en contenedores electrónicos, ópticos o magnéticos. Podrán incluirse como responsables de este delito a las personas encargadas de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tengan acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.

- "Extorsión": aquel quien procura un lucro y obligue a otro, con intimidación o con amenazas graves, a tomar una disposición patrimonial perjudicial para sí mismo o para un tercero valiéndose de cualquier manipulación informática, telemática, electrónica o tecnológica."

- "Estafa informática": aquel quien manipule o influya en el ingreso, en el procesamiento o en el resultado de los datos de un sistema automatizado de información, ya sea mediante el uso de datos falsos o incompletos, el uso indebido de datos, programación, valiéndose de alguna operación informática o artificio tecnológico, o bien, por cualquier otra acción que incida en el procesamiento de los datos del sistema o que dé como resultado información falsa, incompleta o fraudulenta, con la cual procure u obtenga un beneficio patrimonial o indebido para sí o para otro.

  La anterior conducta también se considerara como tal cuando es cometida contra sistemas de información públicos, sistemas de información bancarios y de entidades financieras, o cuando el autor es un empleado encargado de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tenga acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.

- "Daño informático": aquel que sin autorización del titular o excediendo la que se le hubiera concedido y en perjuicio de un tercero, suprima, modifique o destruya la información contenida en un sistema o red

informática o telemática, o en contenedores electrónicos, ópticos o magnéticos. Esta conducta será agravada si la información suprimida, modificada, destruida es insustituible o irrecuperable.

- “Espionaje”: aquel quien procure u obtenga indebidamente informaciones secretas políticas o de los cuerpos de policía nacionales, o de seguridad concernientes a los medios de defensa o a las relaciones exteriores de la nación, o afecte la lucha contra el narcotráfico o el crimen organizado. Se considerará como tal la conducta cuando se realice mediante manipulación informática, programas informáticos maliciosos o por el uso de tecnologías de la información y la comunicación.

- “Daño agravado”: Se considerará como tal cuando algún trabajador produzca un daño que recayera sobre redes, sistemas o equipos informáticos, telemáticos o electrónicos, o sus componentes físicos, lógicos o periféricos.

- “Sabotaje informático”: aquel quien en provecho propio o de un tercero, destruya, altere, entorpezca o inutilice la información contenida en una base de datos, o bien, impida, altere, obstaculice o modifique sin autorización el funcionamiento de un sistema de tratamiento de información, sus partes o componentes físicos o lógicos, o un sistema informático.

- “Suplantación de identidad”: aquel quien suplante la identidad de una persona en cualquier red social, sitio de Internet, medio electrónico o tecnológico de información.

- “Espionaje informático”: aquel quien sin autorización del titular o responsable, valiéndose de cualquier manipulación informática o tecnológica, se apodere, transmita, copie, modifique, destruya, utilice, bloquee o recicle información de valor para el tráfico económico de la industria y el comercio.

- “Instalación o propagación de programas informáticos maliciosos”: aquel quien sin autorización, y por cualquier medio, instale programas informáticos maliciosos en un sistema o red informática o telemática, o en los contenedores electrónicos, ópticos o magnéticos. Dicha conducta persistirá cuando:

    - Se induzca a error a una persona para que instale un programa informático malicioso en un sistema o red informática o telemática, o en los contenedores electrónicos, ópticos o magnéticos, sin la debida autorización.
    - Cuando sin autorización alguien, instale programas o aplicaciones informáticas dañinas en sitios de Internet legítimos, con el fin de

convertirlos en medios idóneos para propagar programas informáticos maliciosos, conocidos como sitios de Internet atacantes.
    - A quien, para propagar programas informáticos maliciosos, invite a otras personas a descargar archivos o a visitar sitios de Internet que permitan la instalación de programas informáticos maliciosos.
    - A quien distribuya programas informáticos diseñados para la creación de programas informáticos maliciosos.

- “Suplantación de páginas electrónicas”: aquel quien, en perjuicio de un tercero, suplante sitios legítimos de la red de Internet, así como haga incurrir en error, capture información confidencial de una persona física o jurídica para beneficio propio o de un tercero.

- “Facilitación del delito informático”: aquel quien facilite los medios para la consecución de un delito efectuado mediante un sistema o red informática o telemática, o los contenedores electrónicos, ópticos o magnéticos.

2.6 De las sanciones por incumplimiento

Artículo 12: El incumplimiento de esta política laboral dará lugar a la aplicación de una sanción disciplinaria, según lo dispuesto por la legislación laboral costarricense. Para la aplicación de una sanción, se tomará en cuenta la gravedad de la falta y el perjuicio ocasionado por el incumplimiento del trabajador.

Artículo 13: En caso de estar en presencia de un posible delito informático, además de las sanciones laborales descritas en esta Política Laboral y en el Código de Trabajo, la falta cometida por el trabajador será puesta en conocimiento del Ministerio Público para que realice las investigaciones del caso.

Asimismo, quedan a salvo las consecuencias civiles, en cuanto a la obligación de indemnizar a la empresa por los daños y perjuicios a ella ocasionados como consecuencia de las competencia desleal o violación a esta política laboral.