**Resumen Política de Delitos Informáticos**

• Supervisión de actividades en internet tanto en dispositivos de la empresa como propios (Tales como materiales descargados, envío y recepción de correos electrónicos, tiempo en actividades de internet).

• Recursos de la empresa deben utilizarse para el giro de la empresa.

• En el caso de que se comenta algún delito por medio los recursos informáticos de la empresa queda entendido que el colaborador responderá por los daños y perjuicios a terceros y/o a la empresa.

• Toda la información contenida en los recursos y herramientas de la empresa es considerada propiedad de la empresa.

• Está prohibido el uso del correo DE LA EMPRESA para usos personales.

• SI por razones de trabajo se le da a una persona acceso a una red social, debe usarse exclusivamente para el servicio prestado al cliente.

• Los usuarios y passwords son extrictamente de uso personal.

• Todo material instalado con autorización debe ser revisado con el Departamento de Soporte de la Empresa.

• Los usuarios no deben enviar correos tipo “spam” o no solicitados a usuarios físicos y jurídicos. Si se tiene necesidad de algún envío, se revisará previamente con Recursos Humanos.

• Todo correo debe tener la leyenda de confidencial y protegido por la legislación costarricense.

• No es permitido utilizar ninguna información personal, imagen o cualquier recurso de una persona sin su autorización.

• La revisión del correo personal es permitido, en forma razonable.

• El Departamento de Soporte puede monitorear sitios accedidos o incluso auditorías in-situ, en este último caso con la presencia de un titular.

Definiciones importantes de la política:

• Delito de corrupción: quien mantenga o promueva la corrupción de una persona menor de edad.

• Violación de correspondencia y comunicaciones o datos personales, todo lo que afecte la privacidad de un tercero y sin autorización haga uso de esa información.

• Extorsión: aquel que procure el lucro con intimidación.

• Estafa informática: Obtener un beneficio patrimonial por medio de brindar información falsa.

• Daño informático: Aquel que sin autorización del titular suprime, modifique o destruya información.

• Espionaje: Aquel quien procure u obtenga indebidamente informaciones políticas secretas.

• Daño agravado: cuando algún trabajador produzca un daño que recayera sobre redes, sistemas o equipos.

• Sabotaje informático: quien en provecho propio o de otros, altere o destruya información de un sistema.

• Suplantación de identidad: Aquel que suplante la identidad de una persona en red social o medio electrónico.

• Espionaje informático: Tomar información de valor para el tráfico económico de la industria.

• Instalación o propagación de programas informáticos maliciosos.

• Suplantación de páginas electrónicas: aquel quien en perjuicio de un tercero suplante sitios legítimos en una red de internet.

• Facilitación de delito informático: quien facilite los medios para la consecución de un delito informático.

• El incumplimiento de esta legislación dará lugar a una sanción disciplinaria en la cual se tomará en cuenta la gravedad de la falta

• En el caso de delito informático será puesto en conocimiento del Ministerio Público

• Se da la obligación de indemnizar a la empresa por los daños y perjuicios ocasionados a la empresa en caso de que alguno de las regulaciones se transgreda.

• Este documento no exime al colaborador de la lectura del documento y dad su aceptación por escrito se compromete a cumplir con lo estipulado en la Política de Delitos Informáticos.