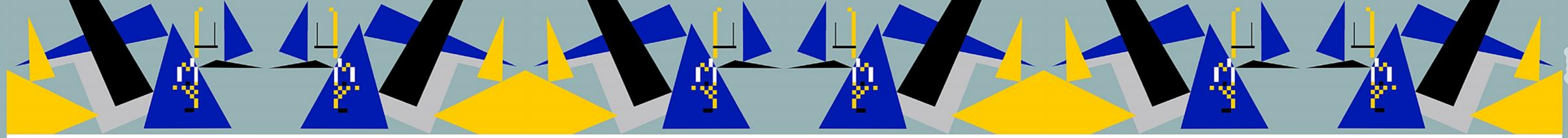

Sin Título

Carlos Gonzales Bogen (1960)

Delitos Informáticos

El marco legal en Venezuela

Reina Camacho / Antonio Machado
reina.camacho@ucv.ve / antonio.machado@ucv.ve

Las facilidades y beneficios que ofrecen las Tecnologías de Información y Comunicaciones (TICs), han causado que la mayoría de las organizaciones, entre ellas las educativas, adopten estas tecnologías, formando parte de la interconexión de redes a nivel mundial, y propiciando la posibilidad de disponer de un medio rápido para intercambiar y compartir recursos de información. Poseer información precisa, oportuna, correcta y poder obtenerla con facilidad, se ha convertido, en la actualidad, en una prioridad tanto para la gran mayoría de las organizaciones como para las personas.

Sin embargo, esta apertura mundial trae consigo riesgos que deben ser asumidos y manejados por las organizaciones. Muchas instituciones son constantemente amenazadas y vulneradas en sus activos de información a través de la tecnología, normalmente con fines lucrativos, lo que puede representar altos costos y pérdidas. Las vulnerabilidades existentes en las tecnologías de información pueden representar problemas graves; por ello, es muy importante comprender y emprender los correctivos necesarios para combatirlos y proteger de posibles ataques informáticos a las organizaciones.

Pero, ¿qué es un delito informático? Según el Centro Nacional de Informática Forense (CENIF), es un crimen genérico o crimen electrónico, que agobia con operaciones ilícitas realizadas por medio de Internet o que tienen como objetivo destruir y dañar computadores, medios electrónicos y redes de Internet.

Actualmente, en Venezuela existe un conjunto de leyes que conforman un marco jurídico en relación a las tecnologías de información. Dentro de ese marco hay dos leyes específicas en materia de seguridad informática: ***Ley de Mensajes de Datos y Firmas Electrónicas*** y la ***Ley Especial contra Delitos Informáticos***. El objeto de esta última radica en la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas o cualquiera de sus componentes, o los cometidos mediante el uso de dichas tecnologías, en los términos previstos en esa ley.

Dicha ley se promulgó en octubre de 2001 en Gaceta oficial N° 37.313, la cual plantea cinco clases de delitos: Contra los sistemas que utilizan Tecnologías de Información; Contra la Propiedad; Contra la privacidad de las personas y de las comunicaciones; Contra niños, niñas o adolescentes; y Contra el orden económico.

Al momento de ocurrir un delito informático, el ente encargado de procesar la denuncia es el Cuerpo de Investigaciones Penales, Científicas y Criminalísticas (CICPC). Existe, además, la alternativa de presentar las denuncias al correo: delitosinformaticos@cicpc.gob.ve

Sanciones

La Leyes tienen diferentes artículos donde contemplan multas y/o sanciones tanto para las personas naturales como jurídicas. Estas oscilan entre:

- Una multa entre diez unidades tributarias (10U.T) o mil unidades tributarias (1.000 U.T).
- De 1 a 10 años de prisión, que podrán ser aumentadas o disminuidas en atención a las circunstancias agravantes o atenuantes existentes.
- La inhabilitación para el ejercicio de funciones, en el ejercicio de la profesión o laborar en instituciones o empresas.

En el ámbito universitario se encuentran muchos riesgos o vulnerabilidades. La UCV no escapa de los ataques y delitos informáticos. Entre los principales tipos que ocurren se encuentran los siguientes: Desfiguración de Portales Web, Código malicioso, Correo Basura (SPAM), entre otros, aunque no se cuenta con estudios estadísticos en esta materia.

El éxito de la seguridad informática radica en concientizar a las personas, para que realicen sus funciones utilizando las mejores prácticas en cuanto a configuración de correo, redes sociales, entre otros, así como estar informados sobre leyes actuales en materia de seguridad tecnológica y las consecuencias en caso de incurrir en delitos informáticos.

Además del marco jurídico nacional, toda organización debe establecer un marco normativo regulatorio dinámico: lineamientos, normas y políticas generales, por ejemplo en la UCV se tienen "Políticas para el uso de la los Recursos Tecnológicos de la UCV", entre las que destacan en materia de seguridad:

- El usuario de la cuenta de correo será responsable de mantener la confidencialidad de su contraseña y la información de la cuenta, así como todas las actividades que ocurran durante la utilización de la misma.
- El usuario de la cuenta deberá notificar a la DTIC de manera inmediata si detecta el uso indebido o no autorizado de su cuenta por terceras personas.
- La cuenta de correo electrónico y la clave asociada asignada por la DTIC es personal, intransferible y por razones de seguridad deberá ser cambiada periódicamente.
- No descargar programas ejecutables con origen desconocido.
- No acceder y/u obtener información de manera no autorizada.
- No transmitir información pornográfica.
- Actualizar periódicamente el antivirus y los parches de seguridad.■

VenCERT

En Noviembre de 2008 se crea el Sistema Nacional de Gestión de Incidentes Telemáticos de la República Bolivariana de Venezuela, cuyo principal objetivo, como CERT (Computer Emergency Response Team) gubernamental es la prevención, detección y gestión de los incidentes generados en los sistemas de información de la Administración Pública Nacional y los Entes Públicos a cargo de la gestión de Infraestructuras Críticas de la Nación.