ELEMENTOS DE SEGURIDAD EN INTERNET

CABLENET ENTERTAINMENT S.A.S.

CAPÍTULO I

DISPOSICIONES GENERALES

Artículo 1. Contexto general

La red mundial Internet y sus elementos asociados constituyen mecanismos ágiles que proveen una amplia gama de posibilidades de comunicación, interacción y entretenimiento, tales como servicios multimedia, foros, chats, correo electrónico, comunidades virtuales y bibliotecas digitales, los cuales pueden ser accedidos por todo tipo de público.

No obstante, dichos elementos deben contar con mecanismos que permitan proteger y reducir los riesgos de seguridad inherentes a la información alojada, distribuida y potencializada a través del servicio de Internet.

Artículo 2. Compromiso institucional

Cablenet Entertainment S.A.S., en su calidad de proveedor del servicio de conectividad, está convencida de que las relaciones con sus clientes deben fortalecerse mediante una comunicación asertiva, sana y orientada a proporcionar herramientas y recomendaciones prácticas que permitan la adecuada protección de los equipos de cómputo y de los servicios asociados a Internet.

En virtud de lo anterior, la Empresa pone a disposición de sus clientes y de la comunidad en general conceptos teórico-prácticos destinados a prevenir o reducir los riesgos a los que se encuentran expuestos los usuarios al interactuar con Internet y sus elementos asociados.

CAPÍTULO II

CONCEPTOS GENERALES DE SEGURIDAD

Artículo 3. Principios de la seguridad de la información

Para efectos del presente documento, se adoptan los siguientes principios:

3.1 **Confidencialidad:** Garantiza que la información solo sea conocida por personas debidamente autorizadas.

3.2 **Integridad:** Asegura que la información no haya sido alterada, eliminada, copiada o modificada de manera no autorizada, ya sea durante su transmisión o en su almacenamiento.

3.3 **Disponibilidad:** Permite que la información pueda ser recuperada o consultada en el momento en que sea requerida.

3.4 **Seguridad de la información:** Conjunto de acciones orientadas a establecer directrices que aseguren la confidencialidad, integridad y disponibilidad de la información, así como la continuidad de las operaciones ante eventos que puedan interrumpirlas.

3.5 **Activo:** Recursos que poseen valor para la Empresa, ya sean tangibles (servidores, equipos de cómputo, equipos de comunicación) o intangibles (información, políticas, normas y procedimientos).

3.6 **Vulnerabilidad:** Exposición a fallos o debilidades de seguridad detectadas en un sistema o aplicación.

3.7 **Amenaza:** Evento o situación con potencial de causar daño a un sistema de información.

3.8 **Riesgo:** Hecho potencial que, de materializarse, puede afectar negativamente la seguridad, los costos, los procesos o los proyectos de la organización.

3.9 **Correo electrónico:** Servicio de red que permite el envío y recepción de mensajes de datos, incluyendo textos, imágenes, videos, audios y programas, mediante sistemas de comunicación electrónica.

CAPÍTULO III

ELEMENTOS DE PROTECCIÓN

Artículo 4. Mecanismos de protección tecnológica

Para la mitigación de riesgos de seguridad, se identifican los siguientes elementos de protección:

4.1 **Firewall:** Elemento de seguridad que permite filtrar paquetes de entrada y salida en redes conectadas a Internet o Intranet, mediante reglas que controlan direcciones URL, puertos y protocolos.

4.2 **Antivirus:** Programa destinado a detectar, controlar y eliminar virus informáticos y códigos maliciosos, tales como troyanos, spyware, rootkits, adware y backdoors.

4.3 **Antispam:** Herramienta orientada a detectar y bloquear correos electrónicos no solicitados.

4.4 **Criptografía:** Técnica de cifrado y descifrado de información que permite que los mensajes solo sean legibles por los destinatarios autorizados.

CAPÍTULO IV

AMENAZAS TÉCNICAS DE SEGURIDAD

Artículo 5. Tipologías de amenazas

Se consideran amenazas técnicas de seguridad, entre otras, las siguientes:

5.1 **Spam:** Envío masivo o no solicitado de correos electrónicos con contenido publicitario, pornográfico, engañoso o no requerido por el destinatario.

5.2 **Ingeniería social:** Manipulación de personas para inducirlas a divulgar información o ejecutar acciones que comprometen la seguridad.

5.3 **Código malicioso:** Software, hardware o firmware introducido de forma intencional con fines maliciosos.

5.4 **Hoax:** Mensajes falsos o engañosos distribuidos en cadena que congestionan redes y servidores de correo.

5.5 **Suplantación:** Acción mediante la cual un atacante se hace pasar por un servicio o entidad legítima.

CAPÍTULO V

FRAUDES INFORMÁTICOS

Artículo 6. Phishing y modalidades asociadas

El **phishing** consiste en la duplicación de páginas web legítimas con el fin de engañar a los usuarios y obtener información confidencial. Este tipo de fraude puede presentarse mediante:

a) **Vishing:** Uso de técnicas de phishing a través de servicios de voz sobre IP.
b) **Smishing:** Uso de técnicas de phishing mediante mensajes de texto.

Artículo 7. Riesgos y consecuencias

Una vez los usuarios ingresan sus datos en sitios falsos, dicha información puede ser utilizada para cometer fraudes, suplantaciones de identidad o robos de recursos económicos.

CAPÍTULO VI

RECOMENDACIONES DE PREVENCIÓN

Artículo 8. Medidas de prevención

Para evitar ser víctima de fraudes informáticos, se recomienda:

a) Ingresar siempre a los sitios oficiales desde el navegador y no desde enlaces recibidos por correo.
b) Verificar los certificados digitales de seguridad.
c) No reenviar correos en cadena ni mensajes engañosos.
d) Mantener actualizados los sistemas operativos y navegadores web.
e) Utilizar herramientas de seguridad como antivirus, antispyware y firewall.

CAPÍTULO VII

MECANISMOS DE SEGURIDAD IMPLEMENTADOS

Artículo 9. Controles institucionales

Cablenet Entertainment S.A.S. cuenta con sistemas de autenticación y autorización para controlar el acceso a los servicios de red y a los equipos terminales de los clientes.

La Empresa ha implementado configuraciones de seguridad base en sus equipos de red, así como medidas de control y protección mediante:

a) Firewall perimetral
b) Sistemas antivirus en estaciones de trabajo y servidores
c) Sistemas antispam en servidores de correo
d) Mecanismos de filtrado de URLs

CAPÍTULO VIII

LIMITACIONES DE ACCESO

Artículo 10. Libre navegación

Si bien **Cablenet Entertainment S.A.S.** implementa mecanismos de seguridad y filtrado conforme a la normativa vigente, en especial la Ley 679 de 2001 y sus decretos reglamentarios, en ningún caso restringe la libre navegación y acceso a Internet, salvo lo expresamente establecido por la ley.

En consecuencia, la Empresa da cumplimiento a lo dispuesto por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), garantizando el acceso a Internet conforme al marco legal aplicable.