POLITICA GENERAL DE SEGURIDAD DE LA INFORMACION

Teveandina Ltda. – Canal Trece

Revisiones y control de cambios

Titulo	**Política general de seguridad de la información. Teveandina Ltda. Canal Trece**
Autores	Alejandro Daza – Cristian Ostos - Gonzalo Joya Santana
Tema	Política general diseñada de acuerdo con lineamientos, estándares, guías en seguridad y privacidad de la información
Fecha de Elaboración	Julio 2018
Formato	PDF
Versión	1.0
Palabras Relacionadas	Seguridad de la información, riesgo, control, vulnerabilidad, seguridad informática, políticas

Control de Cambios			
Fecha	**Autores**	**Versión**	**Cambio**
Julio 2018	Alejandro Daza Cristian Ostos Gonzalo Joya	1.0	Versión Inicial para revisión

INTRODUCCION

La Información es el activo más importante para la entidad, de tal manera que optará por tomar las medidas necesarias para su **protección y conservación.** Teveandina Ltda. desde la alta dirección dispuso un equipo interdisciplinario con el fin de adaptar el modelo de seguridad de la información (MSPI) basándose en estándares internacionales, buenas prácticas, guías, metodologías, entre otros, los cuales permitan asegurar el cumplimiento de los objetivos estratégicos de la Entidad.

OBJETIVO GENERAL

Mantener un ambiente seguro alineando a los objetivos estratégicos del Canal, de tal manera que permita proteger los activos de información a través de su uso responsable, con base en la gestión y mitigación de riesgos, con la finalidad de mantener la **DISPONIBILIDAD, INTEGRIDAD y CONFIDENCIALIDAD** de la información sobre la continuidad de los procesos en la entidad.

Esta política debe ser revisada de acuerdo con cambios en los procesos, estructura orgánica y objetivos estratégicos durante cada vigencia.

OBJETIVOS ESPECIFICOS

- Proteger los activos de la información de Teveandina LTDA.
- Identificar e implementar las tecnologías de información y las comunicaciones (TIC´s) necesarias para fortalecer la seguridad de la información.
- Concientizar a los funcionarios, contratistas y practicantes de la Entidad sobre el uso adecuado de los activos de información puestos a su disposición para la realización de las funciones y actividades diarias, garantizando la confidencialidad, la privacidad y la integridad de la información

ALCANCE

La Política de Seguridad de la Información aplica a todos los colaboradores del **CANAL REGIONAL DE TELEVISON TEVEANDINA LTDA.,** con la finalidad de que tengan acceso a un activo de información o través de los documentos en los entornos analógicos o digitales, equipos de cómputo, infraestructura tecnológica, servicios tecnológicos y canales de comunicación de la Entidad.

DEFINICIONES

- **Activo:** Cualquier cosa que tiene valor para la organización.
- **Confidencialidad:** Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
- **Disponibilidad:** Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.
- **Estándar:** Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Los estándares son diseñados para promover la implementación de las políticas de alto nivel de la entidad antes de crear nuevas políticas.
- **Integridad:** Propiedad de salvaguardar la exactitud y estado completo de los activos.
- **Política:** Declaración de alto nivel que describe la posición de la entidad sobre un tema específico.
- **Riesgo:** Efecto de la incertidumbre en un resultado esperado.
- **Seguridad de la Información:** Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad (Accountability), no repudio y fiabilidad.
- **Sistemas de Información:** Sistema organizado para la recopilación, organización, almacenamiento y comunicación de información. Más específicamente, es el estudio de redes complementarias que las personas y las organizaciones usan para recopilar, filtrar, procesar, crear y distribuir datos.
- **TIC (Tecnologías de la Información y la Comunicación):** Son todos aquellos recursos, herramientas y programas que se utilizan para procesar, administrar y compartir la información mediante diversos soportes tecnológicos

MARCO LEGAL Y NORMATIVO

- Constitución Política de Colombia 1991. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data. Artículo 20. Libertad de Información.
- Código Penal Colombiano - Decreto 599 de 2000
- Ley 906 de 2004, Código de Procedimiento Penal.
- Ley 87 de 1993, por la cual se dictan Normas para el ejercicio de control interno en las entidades y organismos del Estado, y demás normas que la modifiquen.

- Ley 734 de 2002, del Congreso de la República de Colombia, Código Disciplinario Único.
- Ley 23 de 1982 de Propiedad Intelectual - Derechos de Autor.
- Ley 594 de 2000 - Ley General de Archivos.
- Ley 80 de 1993, Ley 1150 de 2007 y decretos reglamentarios.
- Ley 527 de 1999, por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.
- Directiva presidencial 02 del año 2000, Presidencia de la República de Colombia, Gobierno en línea.
- Ley 1032 de 2006, por el cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales.
- Ley 1266 de 2007, por la cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales.
- Ley 1273 de 2009, "Delitos Informáticos" protección de la información y los datos.
- Ley 1437 de 2011, "Código de procedimiento administrativo y de lo contencioso administrativo".
- Ley 1581 de 2012, "Protección de Datos Personales".
- Decreto 2609 de 2012, por la cual se reglamenta la ley 594 de 200 y ley 1437 de 2011
- Decreto 1377 de 2013, por la cual se reglamenta la ley 1581 de 2012
- Ley 1712 de 2014, "De transparencia y del derecho de acceso a la información pública nacional"
- Ley 962 de 2005. "Simplificación y Racionalización de Trámite. Atributos de seguridad en la Información electrónica de entidades públicas;"
- Ley 1150 de 2007. "Seguridad de la información electrónica en contratación en línea"
- Ley 1341 de 2009. "Tecnologías de la Información y aplicación de seguridad".
- Decreto 2952 de 2010. "Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008"

- Decreto 886 de 2014. "Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012"

- Decreto 1083 de 2015. "Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012"

- CONPES 3701 de 2011 Lineamientos de Política para Ciberseguridad y Ciberdefensa

- CONPES 3854 de 2016 Política Nacional de Seguridad digital.

REQUISITOS TÉCNICOS

- Norma Técnica Colombiana NTC/ISO 27001:2013 Sistemas de gestión de la seguridad de la información

- Norma Técnica Colombiana NTC/ISO 17799 Código de práctica para la gestión de la seguridad de la información.

- ISO/IEC 27005 Information technology Systems- Security techniques- information security risk management.

- Modelo Estándar de Control Interno MECI 1000 2da versión "Subsistema: Control de Gestión; Componente: Actividades de Control; Elemento: Monitoreo y Revisión e Información"

- Norma Técnica Colombiana NTC - ISO 19011 "Directrices para la Auditoria de los Sistemas de Gestión de la Calidad y/o Ambiental"

RESPONSABILIDADES EN SEGURIDAD DE LA INFORMACIÓN

Asegurar que los funcionarios, contratistas y demás colaboradores de Teveandina LTDA., entiendan sus responsabilidades, funciones y roles, con el fin de reducir y/o mitigar riesgos relacionados con hurto, fraude, filtraciones, uso inadecuado de la información y de las instalaciones.

Crear el Comité de Seguridad de la Información, y asignar el rol de Oficial de seguridad de la información y su equipo de apoyo, junto con los roles, funciones y responsabilidades respectivamente.

El proceso de Gestión TIC debe establecer roles, funciones y responsabilidades de operación y administración de los sistemas de información, los servicios tecnológicos e infraestructura de Teveandina LTDA. a los funcionarios dispuestos para esto. Cada aspecto mencionado deberá estar debidamente documentado y publicado.

Todos los usuarios de los sistemas de información, servicios tecnológicos e infraestructura tecnológica de Teveandina LTDA. tienen la responsabilidad y obligación de cumplir con las políticas, normas, procedimientos y buenas prácticas de seguridad de la información establecidas en las políticas específicas para tal fin.

Los jefes de área y líderes de proceso deben asegurarse que todos los procedimientos de seguridad de la información se realizan correctamente para lograr el cumplimiento de las políticas y estándares de seguridad de la información de Teveandina LTDA.