Contenido

1. INTRODUCCIÓN

El crecimiento en el uso masivo de las Tecnologías de la Información y las Comunicaciones (TIC) en Colombia, se ha reflejado en la masificación de las redes de telecomunicaciones que son base para cualquier actividad socioeconómica y a su vez, el incremento en la oferta de servicios disponibles en línea evidencian un aumento significativo en la participación digital de los ciudadanos. Lo que a su vez se traduce en una economía digital con cada vez más participantes en el país.

En consecuencia, de lo anterior, el ascenso en la participación digital de los ciudadanos trae consigo nuevas y más sofisticadas formas para atentar contra su seguridad. Esta situación debe ser atendida, brindando la protección en el ciberespacio para detectar estas amenazas, y de esta forma Reducir la probabilidad de que sean efectivas, fortaleciendo las capacidades de los posibles afectados para identificar y gestionar el riesgo.

En el presente documento, se toma como enfoque la política Nacional de seguridad digital correspondiente al adoptado en el CONPES 3854 en donde se enmarcan los lineamientos para el diseño de este marco institucional e incluye las dimensiones del modelo integrado de planeación y gestión-MIPG para que proporcionen un instrumento que oriente las acciones dentro del entorno digital y la forma de implementarse en el “CANAL TRO LTDA” en cuanto a seguridad y defensa digital.

2. JUSTIFICACIÓN

TELEVISIÓN REGIONAL DEL ORIENTE LIMITADA “CANAL TRO LTDA” define su política de Seguridad Digital atendiendo los lineamientos establecidos que permiten llevar a cabo la transformación digital a fin de mantener interacción con los grupos de interés, y una gestión de riesgos de Seguridad digital apropiada.

Como resultado, se deben adoptar estrategias que permitan responder a las necesidades que surgen en el entorno digital, que ayude a la automatización de los procesos, identificar las vulnerabilidades, detectar las amenazas y reducir los riesgos y poder garantizar la protección y la calidad de la información, de esta manera adoptar medidas que permitan transformar los servicios, haciendo un uso adecuado de las herramientas del entorno digital.

3. OBJETIVO DE LA POLÍTICA

Fortalecer la capacidad de TELEVISIÓN REGIONAL DEL ORIENTE LIMITADA “CANAL TRO LTDA” para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital, contrarrestar el incremento de las amenazas informáticas que afecten significativamente, y afrontar retos en aspectos de seguridad cibernética.

3.1 OBJETIVOS ESPECIFICOS

- Establecer un marco institucional “CANAL TRO LTDA” para la seguridad digital.
- Adecuar estrategias de gestión del riesgo de seguridad digital en todos los procesos de “DE CANAL TRO LTDA”.
- Fortalecer el esquema de identificación, prevención y gestión de incidentes digitales, con la participación activa de todos los procesos de “CANAL TRO LTDA”
- Promover en los diferentes niveles de “CANAL TRO LTDA” la formación comportamientos responsables en el entorno digital.
- Generar confianza en todos los procesos de “CANAL TRO LTDA” en el uso del entorno digital.
- Socializar y concientizar las tipologías de delitos cibernéticos, cibercrímenes y fenómenos en el entorno digital a todo el personal de “CANAL TRO LTDA”.

4. ALCANCE

El presente documento aplica a todos los procesos de “CANAL TRO LTDA”, descritos en el mapa de procesos.

5. DEFINICIONES

Ciberamenaza o amenaza cibernética: aparición de una situación potencial o actual que pudiera convertirse en un ciberataque.

Ciberataque o ataque cibernético: acción criminal organizada o premeditada de uno o más agentes que usan los servicios o aplicaciones del ciberespacio o son el objetivo de la misma o donde el ciberespacio es fuente o herramienta de comisión de un crimen.

Ciberespacio: entorno complejo resultante de la interacción de personas, software y servicios en Internet a través de dispositivos tecnológicos conectados a dicha red, el cual no existe en ninguna forma física.

Ciberiesgo o riesgo cibernético: posibles resultados negativos derivados de fallas en la seguridad de los sistemas tecnológicos o asociados a ataques cibernéticos.

Ciberseguridad: Es el desarrollo de capacidades empresariales para defender y anticipar las amenazas cibernéticas con el fin de proteger y asegurar los datos.

Entorno digital: Ambiente, tanto físico como virtual sobre el cual se soporta la economía digital. Siendo esta última la economía basada en tecnologías, cuyo desarrollo y despliegue se produce en un ecosistema caracterizado por la creciente y acelerada convergencia entre diversas tecnologías, que se concreta en redes de comunicación, equipos de hardware, servicios de procesamiento y tecnologías web.

Incidente digital: evento intencionado o no intencionado que puede cambiar el curso esperado de una actividad en el entorno digital y que genera impactos sobre los objetivos.

Gestión de riesgos de seguridad digital: Es el conjunto de actividades coordinadas dentro de una organización o entre organizaciones, para abordar el riesgo de seguridad digital, mientras se maximizan oportunidades. Es una parte integral de la toma de decisiones y de un marco de trabajo integral para gestionar el riesgo de las actividades económicas y sociales. Se basa en un conjunto flexible y sistemático de procesos cíclicos lo más transparente y lo más explícito posible. Este conjunto de procesos ayuda a asegurar que las medidas de gestión de riesgos de seguridad digital (medidas de seguridad) sean apropiadas para el riesgo y los objetivos económicos y sociales.

Lineamientos: Directriz o disposición establecida por MinTIC, que debe ser implementada por las entidades públicas para el desarrollo de la Política de Gobierno Digital y se desarrolla a través de estándares, guías, recomendaciones o buenas prácticas.

Estándar: Es el conjunto de características y requisitos que se toman como referencia o modelo y son de uso repetitivo y uniforme. Un estándar se construye a través de consenso reflejando la experiencia y las mejores prácticas en un área en particular, implican uniformidad, normalización y es de obligatorio cumplimiento.

Resiliencia: es la capacidad de un material, mecanismo o sistema para recuperar su estado inicial cuando ha cesado la perturbación a la que había estado sometido

Riesgo: Es el efecto de incertidumbres sobre objetivos y puede resultar de eventos en donde las amenazas cibernéticas se combinan con vulnerabilidades generando consecuencias económicas.

Riesgo de seguridad digital: Es la expresión usada para describir una categoría de riesgo relacionado con el desarrollo de cualquier actividad en el entorno digital. Este riesgo puede resultar de la combinación de amenazas y vulnerabilidades en el ambiente digital. Debilita el logro de objetivos económicos y sociales, incluye aspectos relacionados con el ambiente físico y digital, las personas involucradas en las actividades y los procesos organizacionales que las soportan.

Seguridad de la información: Este habilitador busca que las entidades públicas incorporen la seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información con el fin de preservar la confidencialidad, integridad, disponibilidad, y privacidad de la información, así como la protección de los datos personales que tratan las entidades públicas en cumplimiento de la normatividad de protección de datos personales.

Servicios ciudadanos digitales: busca que todas las entidades públicas implementen lo dispuesto en el Decreto 1413 de 2017 (incorporado en el título 17, parte 2, libro 2 del Decreto 1078 de 2015), que establece los lineamientos para la prestación de los servicios

ciudadanos digitales y para permitir el acceso a la administración pública a través de medios electrónicos.

En dicho Decreto los servicios digitales se clasifican en servicios básicos: autenticación biométrica, autenticación con cédula digital, autenticación electrónica, carpeta ciudadana e interoperabilidad, los cuales son de obligatorio uso y adopción; y servicios especiales, que son adicionales a los servicios básicos, como el desarrollo de aplicaciones o soluciones informáticas para la prestación de los servicios ciudadanos digitales básicos.

6. PROPÓSITO DE LA POLÍTICA

Los propósitos de la política son los siguientes:

Asegurar que se tomen las acciones adecuadas para evitar o disminuir la ocurrencia de riesgos cibernéticos e incidentes digitales, y de este modo retroalimentar y fortalecer su identificación.

y la gestión de dichos riesgos cibernéticos e incidentes digitales amplié la capacidad de "CANAL TRO LTDA" en seguridad digital,

y, con estos insumos, forjar un ambiente digital seguro que promueva la prosperidad económica y social,

que, genere confianza a los ciudadanos e impulse el desarrollo de todos procesos de "CANAL TRO LTDA",

Fortaleciendo la reputación y garantizando el cumplimiento de los objetivos de "CANAL TRO LTDA" de manera organizada, segura y transparente.

7. RESPONSABILIDAD SOBRE LA POLÍTICA

Es responsabilidad de Gestión Técnica, implementar y garantizar que los tres (3) pilares fundamentales de la seguridad de la información: confidencialidad, integridad y disponibilidad se gestionen y se controlen para la mitigación del riesgo. Del mismo modo mantener el contacto con las autoridades y grupos de interés con el fin de apoyar cualquier inquietud o incidencia que se tenga en seguridad a digital.

Es responsabilidad de Planeación, proporcionar los recursos, metodologías y estrategias para el desarrollo de la política de Seguridad Digital, de la misma forma proporcionar definir los roles y responsabilidades en seguridad digital, con el fin de garantizar la separación de deberes.

En cuanto a la gestión de proyectos debe tener en cuenta la incorporación de la seguridad digital y la definición de controles para los proyectos que realice TELEVISIÓN REGIONAL DEL ORIENTE LIMITADA "CANAL TRO LTDA.

Se debe involucrar activamente a todas las partes interesadas, y asegurar una responsabilidad compartida entre las mismas para la aplicación de la política.

7. NORMATIVIDAD

Constitución Política de Colombia	Artículos 11, 12, 13, 14, 17, 21, 22, 24, 29, 44, entre otros. Por ejemplo, Art. 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.
Ley 527 de 1999 (Comercio Electrónico)	Por medio de la cual se define y se reglamenta el acceso y uso de los mensajes de datos, el comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. Se tratan conceptos como: mensaje de datos (artículos 2º y 5º), el principio de equivalencia funcional (artículos 6º, 8º, 7º, 28º, 12º y 13º), la autenticación electrónica (artículo 17º), la firma electrónica simple (artículo 7º), la firma digital (artículo 28º), y la firma electrónica certificada (artículo 30º, modificado por el artículo 161 del Decreto Ley 019 de 2012).
Ley 594 de 2000 (Ley General de Archivos)	Habilita el uso de nuevas tecnologías de manera general, es posible establecer que para satisfacer los requerimientos establecidos en esta norma sea viable usar firmas electrónicas simples, certificadas y firmas digitales.
Ley 599 de 2000 (Código Penal)	Por la cual se expide el código penal colombiano.
Ley 600 de 2000 (Código de Procedimiento Penal)	Por la cual se expide el código de procedimiento penal.
Ley 679 de 2001 (Pornografía y explotación sexual con menores)	Esta Ley contempla en el artículo 4, un sistema de autorregulación, en virtud del cual el Gobierno nacional, por intermedio del Ministerio de Comunicaciones hoy Ministerio de Tecnologías de la Información y las Comunicaciones, promoverá e incentivará la adopción de sistemas de autorregulación y códigos de conducta eficaces en el manejo y el aprovechamiento de redes globales de información, estos códigos se elaboraran con la participación de organismos representativos de los proveedores y usuarios de servicios de redes globales de información.

Ley 906 de 2004 (Código de Procedimiento Penal)	Por la cual se expide el código de procedimiento penal (corregida de conformidad con el Decreto 2770 de 2004)
Ley 962 de 2005 (racionalización detrámites y procedimientos)	Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funcionespúblicas o prestan servicios públicos. Prevé el incentivo del usode medios tecnológicos integrados para disminuir los tiempos y costos de realización de los trámites por parte de losadministrados.
Ley 1032 de 2006 (derechos de autor y conexos)	Por la cual se modifican los artículos 257, 271, 272 y 306 del código penal (artículo 271. violación a los derechos patrimoniales de autor y derechos conexos).
Ley 1150 de 2007 (medidas para la eficiencia y la transparencia)	Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con recursos públicos. Específicamente, se establece la posibilidad de que laadministración pública expida actos administrativos y documentos y haga notificaciones por medios electrónicos paralo cual prevé el desarrollo del Sistema Electrónico para la Contratación Pública (SECOP).
Circular Externa SFC 052 de 2007	Por la cual la Superintendencia Financiera de Colombia incrementa los estándares de seguridad y calidad para el manejode la información a través de medios y canales de distribución de productos y servicios que ofrecen a sus clientes y usuarios las entidades vigiladas por esta Entidad.
Ley 1266 de 2008 (Habeas Data)	Contempla las disposiciones generales en relación al derecho de habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
Ley 1273 de 2009 (Delitos Cibernéticos)	Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado denominado “De la protección de lainformación y de los datos y se preservan integralmente los sistemas que utilicen las TIC.

9. IMPLEMENTACIÓN DE LA POLITICA.

Con el fin de articular las iniciativas, metodologías y estrategias de “CANAL TRO LTDA” para la implementación de la política de seguridad digital, a continuación, se presentan el plan de acción que permitan afianzar la seguridad de la información en el ciberespacio:

9.1 Plan de seguridad de la información:

Deben realizar la revisión de políticas de Seguridad Digital que se describen a continuación y establecer el mecanismo que permitan verificar el cumplimiento de las siguientes políticas:

a) Política De Uso de correo electrónico
b) Política De Escritorio y Pantalla Limpia
c) Política De Respaldo y Restauración de la Información
d) Política De Uso de Internet
e) Política de Reporte de Incidentes de Sistemas de Información
f) Política de Administración de Contraseñas
g) Política de Protección contra código malicioso
h) Política de acceso físico al Data Center
i) Política de Mantenimiento de Sistema de Información
j) Política de Confidencialidad de la Información
k) Política de Gestión de Claves de Accesos a los Sistemas de Información
l) Política de Uso de los Activos de Información
m) Política de Uso de dispositivos de almacenamiento y transferencia de información.

9.2 Levantamiento de activos: Deben hacer la revisión de los activos de información en cada uno de los procesos y establecer los mecanismos para la aprobación u mantenimiento de las buenas prácticas de los activos

9.3 Matriz de riesgos de información: En la matriz de Riesgos **se** Establecen las fuentes o factores de riesgo, los eventos o riesgos, sus causas y sus consecuencias, donde permita establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el fin de estimar la zona de riesgo inicial (RIESGO INHERENTE).

Una vez realizado este análisis se deben definir las medidas de control que permitan reducir la probabilidad de ocurrencia y/o los impactos ocasionados por los riesgos inherentes detectados, y definir el mecanismo para la aprobación de los riesgos de seguridad digital identificados.

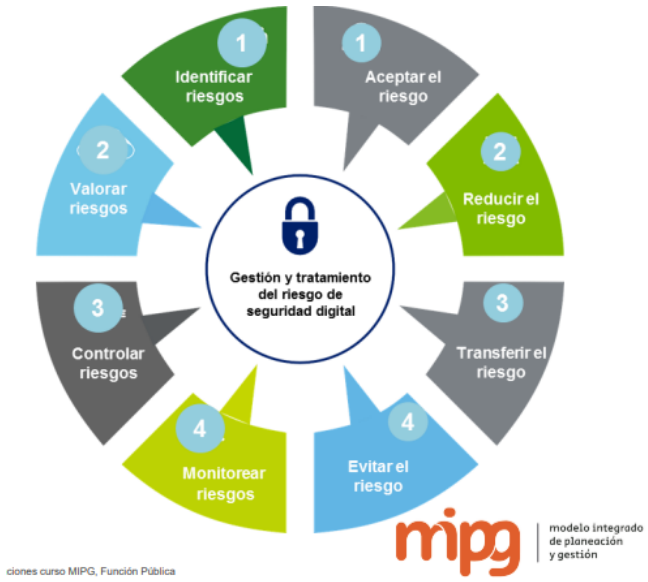

Figura 1. Tomado de MIPG

9.4 Tratamiento del riesgo: Se realiza el seguimiento sobre la evolución en cada uno de los riesgos y Adoptar medidas para el tratamiento del riesgo.

9.5 Diseño y definición de Controles: Se realiza el diseño, definición y actualización de Controles que permitan abordar los riesgos y Adoptar medidas para el tratamiento del riesgo, a través del plan de Seguridad y Privacidad de la información cómo estrategia de mitigación de riesgo.

9.6 Seguimiento a los Riesgos: Se debe definir una periodicidad para el seguimiento de riesgos y actualización de estos.

9.7 Concientización: Capacitar a los agentes que se encuentren involucrados en todos los procesos de “CANAL TRO LTDA”, con el fin de promover el uso del entorno digital de manera responsable y fortalecer las capacidades de los responsables de salvaguardar la información en el entorno digital que permita una interacción confiable entre todas las partes interesadas en el uso del entorno digital.

9.8 Marco en Ciberseguridad: Se inicia una construcción de un marco adecuado en relación con temas de ciberseguridad para gestionar la seguridad digital de “CANAL TRO LTDA”. Teniendo en cuenta los lineamientos jurídicos sobre los delitos cibernéticos, cibercrímenes y otros fenómenos en el entorno digital.

9.9 Indicadores y métricas. En esta categoría se definen indicadores asociados a los objetivos de seguridad digital de "CANAL TRO LTDA" con el fin de verificar su cumplimiento y alineación.

9.10. Medición y Mejora

El plan de mejoramiento continuo debe estar alineado con la gestión del riesgo de seguridad Digital, como resultado de este, "Canal TRO LTDA" requiere establecer acciones de control y prevención del riesgo en caso de tener no conformidades.
Ejecutar medidas y acciones encaminadas a minimizar sus causas evitando así la materialización de las debilidades que se encontraron y tratamiento correctivo para los riesgos que tengan probabilidad alta de materializaron.

Así mismo, con el fin de cumplir con los requisitos del Mejoramiento Continuo en "Canal TRO LTDA", se debe llevar el respectivo documento del Plan de Mejoramiento Continuo que contenga los procesos de tratamiento realizados con las no conformidades, acciones de mejora y de posible impacto de estas.

Se debe contar con una estrategia de comunicación que permita llegar a la claridad del tema a todas las partes interesadas e involucradas con las acciones realizadas.

10. Seguimiento y Periodicidad

El seguimiento se hace de acuerdo con las acciones establecidas en los planes propuestos, estos seguimientos pueden ser permanentes, semestrales, anuales, etc., en relación con lo estipulado en la planeación estratégica

11.Aprobación

Los cambios, revisiones y aprobación de esta política se establecen a través del Comité y queda registrado en Acta.

12. Control de Cambios

Versión	Descripción del Cambio	Fecha
01	Versión inicial del procedimiento	Noviembre 2 de 2021

Elaboró	Aprobó
Gestión Técnica	Comité de Gestión y desempeño Institucional