POLÍTICA SEGURIDAD DIGITAL

TELEVISIÓN REGIONAL DEL ORIENTE LTDA.
CANAL TRO

FLORIDABLANCA
2023

CONTENIDO

INTRODUCCIÓN

El avance tecnológico y el uso masivo de las tecnologías de la información y las comunicaciones (TIC) han permitido optimizar las actividades ejecutadas por las entidades colombianas ya sean de carácter público, privado o de cualquier índole. Este avance ha incrementado el uso de las TIC, particularmente en la prestación de servicios esenciales a la nación.

Así mismo, los cambios provocados por la evolución continua de la tecnología, y en general de las redes informáticas, han inclinado a algunas entidades y ciudadanos a utilizarlas como medios para incrementar su productividad, para ser más competitivos en los negocios, para satisfacer necesidades propias y para generar valor. Por otra parte, en otros escenarios se ha incrementado el uso de la tecnología con fines delictivos o para generar amenazas informáticas; este propósito busca afectar otras infraestructuras tecnológicas, sistemas de información financieros, personas e, incluso, llegar a impactar la economía de toda una nación. Es por esta razón, que los estados han incrementado su preocupación por los riesgos a los que puedan estar expuestas las instituciones (entidades, organizaciones, empresas y la misma ciudadanía) y han decidido incluir en sus planes estratégicos modelos de ciberseguridad y ciberdefensa encaminados básicamente a fortalecer la seguridad de su nación y, por ende, de todos los que la componen.

En Colombia, gracias a las estrategias desarrolladas por el MinTIC, durante el primer trimestre de 2017, se cuenta con una cifra de veintiocho millones de conexiones a internet de banda ancha, lo que evidencia un aumento considerable en la economía digital del país. Así mismo, conscientes de que la seguridad digital es fundamental para el desarrollo del país, en los últimos años se ha puesto a la vanguardia la lucha contra las amenazas en el ámbito digital con estrategias tales como: la creación de lineamientos como la Política para Ciberseguridad y Ciberdefensa (CONPES 3701 y 3854), un modelo de seguridad y privacidad de la información (MSPI) y misiones de asistencia técnica internacional. Igualmente, el apoyo de diferentes organizaciones para la prevención y gestión de incidentes (MinTIC, Grupo de Respuestas a Emergencias Cibernéticas de Colombia ColCERT, Equipo de respuesta a incidentes de seguridad informática CSIRT, -Centro Cibernético Policial de la Policía Nacional), los mecanismos de investigación (fiscalía general de la Nación, Centro Cibernético Policial) y de judicialización (rama judicial). Con el conjunto de estas organizaciones se busca aumentar la capacidad de defensa ante las amenazas presentes en el medio digital.

De igual forma, el Gobierno colombiano ha facilitado la creación de políticas como el CONPES 3854 de 2016 para la protección del entorno digital y cibernético; en él se involucran a todos los ciudadanos y sectores económicos para fortalecer la prosperidad económica, social y ambiental del país. Es aquí donde aquellas infraestructuras críticas de la nación toman un valor preponderante y se hace necesario ser más especializados en esta identificación, al punto de determinar cuáles de ellas se pueden considerar infraestructuras críticas cibernéticas (ICC), que,

al estar inmersas en un ambiente altamente digital, presentan mayor exposición a riesgos que pueden afectar a la nación a nivel social, ambiental y por supuesto, económico.

1. JUSTIFICACION

El CANAL TRO identifica la información como un componente indispensable en la consecución y conducción de los objetivos definidos por la estrategia de la Entidad, por esta razón es necesario establecer un modelo que asegura que la información es protegida de una manera adecuada para su manejo, procesamiento, almacenamiento y recolección.

Esta política describe normas de seguridad digital definidas por el CANAL TRO. Para la elaboración del mismo, se toman como base las leyes y demás regulaciones aplicables, las políticas incluidas en este manual son parte integral del sistema de gestión de seguridad digital del MINTIC y son la base para la implantación de los controles, procedimientos y estándares.
La seguridad digital es una prioridad para el CANAL TRO y por tanto el cumplimiento de estas políticas es responsabilidad de todos sus colaboradores. A lo largo del documento al emplear el término seguridad digital se agrupan los conceptos de seguridad de la información, seguridad informática, ciberseguridad y la protección de los datos personales.

2. OBJETIVO

Establecer los lineamientos definidos por la Alta Dirección y Gestión Técnica y Emisión del CANAL TRO para la seguridad de la información, teniendo en cuenta el Modelo de Seguridad y Privacidad de la Información, las políticas de Seguridad Digital y Gobierno Digital y demás requisitos de ley y las necesidades de las partes interesadas.

3. ALCANCE

La política de seguridad digital cubre todos los procedimientos que tiene la Entidad y se gestionan a nivel del mapa de procesos en búsqueda de una adecuada protección y calidad de la información.

4. 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.
- **Confidencialidad:** Propiedad de la información que la hace no disponible o que no sea divulgada a individuos, entidades o procesos no autorizados.
- **Controles:** Medida que permite reducir o mitigar un riesgo.
- **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.
- **Integridad:** Propiedad de la información que busca preservar su exactitud y completitud.
- Disponibilidad: Propiedad de la información de ser accesible y utilizable a demanda por una parte interesada.
- **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.
- **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.

- **Sistema de Gestión de Seguridad de la Información:** Es el conjunto de manuales, procedimientos, controles y técnicas utilizadas para controlar y salvaguardar todos los activos que se manejan dentro de una entidad.

5. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

El CANAL TRO, entendiendo la importancia de sus activos de información para el cumplimiento de su misión institucional, se guiará con el Modelo de Seguridad y Privacidad de la Información (MSPI) buscando proteger la confidencialidad, integridad y disponibilidad de los activos de información y además establecer un marco de confianza en el ejercicio de su misión con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes aplicables.
El CANAL TRO en su propósito de dar cumplimiento con la política de seguridad y privacidad de la información, establece los siguientes objetivos:

- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes del CANAL TRO.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Minimizar el riesgo de todos los procesos de la entidad.
- Mejorar continuamente el sistema de gestión de seguridad de la información.
- Implementar los controles tecnológicos necesarios para la protección de los activos de la entidad y para la reducción de los riesgos.

6. COMPROMISO DE LA ALTA DIRECCIÓN

La Alta Dirección del CANAL TRO se compromete coordinar, hacer seguimiento y verificación de la estabilidad y mejora de la Política, garantizando los recursos suficientes (tecnológicos y talento humano calificado), así mismo incluirá dentro de las decisiones estratégicas y la seguridad de la información.

7. APLICABILIDAD

La presente política, sus objetivos, además de los manuales, procedimientos o documentos derivados o complementarios aplican a toda la entidad, servidores públicos, contratistas y terceros de CANAL TRO. El incumplimiento a la Política de Seguridad y Privacidad de la Información o de sus lineamientos derivados, traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad.

8. 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 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 de trámites 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 funciones públicas o prestan servicios públicos. Prevé el incentivo del uso de medios tecnológicos integrados para disminuir los tiempos y costos de realización de los trámites por parte de los administrados.

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 la administración pública expida actos administrativos y documentos y haga notificaciones por medios electrónicos para lo 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 manejo de 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 la información y de los datos y se preservan integralmente los sistemas que utilicen las TIC.

9. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (ROLES Y RESPONSABILIDADES)

CANAL TRO, define los roles y responsabilidades para la implementación del MSPI y el cumplimiento de los lineamientos de seguridad descritos en esta política y los demás documentos derivados (Manuales, Procedimientos, Formatos etc.):

ROL/INSTANCIA/ DEPENDENCIA	RESPONSABILIDADES (Definir los deberes respecto a la SEGURIDAD DE LA INFORMACIÓN)
Alta Dirección	● Proporcionar los recursos necesarios para la implementación y mantenimiento del sistema de gestión de seguridad de la información (Recursos económicos, formación y recursos tecnológicos).
Comité de Gestión y Desempeño	● Aprobar los recursos correspondientes para la implementación y el mantenimiento del sistema de gestión de seguridad de la información.
Grupo TIC	● Implementar los controles de tipo tecnológico que ayuden a mitigar los riesgos de seguridad de la información.

ROL/INSTANCIA/ DEPENDENCIA	RESPONSABILIDADES (Definir los deberes respecto a la SEGURIDAD DE LA INFORMACIÓN)
Talento Humano	● Asegurar que los empleados y contratistas tomen conciencia de sus responsabilidades en seguridad de la información y las cumplan, además de dar aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos.
Control Interno	● Incluir la seguridad de la información, dentro de los planes de auditoría institucionales. ● Apoyar en situaciones de posibles violaciones a las políticas de seguridad de la información.
Comunicaciones	● Apoyar en las labores de comunicación y sensibilización en seguridad de la información, para difundir la información en todos los niveles de la entidad.
Líderes de los procesos	● Implementar las políticas y procedimientos de seguridad de la información que se definan como parte del SGSI (Por ejemplo: gestión de activos, gestión de riesgos, entre otros).
Todos los funcionarios y contratistas	● Apoyar a los líderes de proceso en el desarrollo de tareas como gestión de activos y gestión de riesgos. ● Cumplir a cabalidad con las políticas y procedimientos de seguridad de la información definidos y aprobados.

10. SANCIONES

a. Cualquier violación a las políticas de seguridad de la información de CANAL TRO debe ser sancionada de acuerdo con el Reglamento Interno de Trabajo, a las normas, leyes y estatutos de la ley colombiana, así como la normativa atinente y supletoria, y apoyados en las leyes regulatorias de delitos informáticos de Colombia.
b. Las sanciones podrán variar dependiendo de la gravedad y consecuencias generadas de la falta cometida o de la intencionalidad de la misma.

11. SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN

CANAL TRO indica que realizará revisiones periódicas al SGSI. Dichas revisiones estarán enfocadas en los siguientes aspectos:

- Revisión de avance del Modelo de Seguridad y Privacidad de la Información del Ministerio TIC.

- Revisión de avance de la Política de Seguridad Digital de acuerdo con lo solicitado por FURAG o la herramienta definida para tal fin.

12. APROBACIÓN Y REVISIONES A LA POLÍTICA

Esta política será efectiva desde su aprobación por la (Alta Dirección/Instancia). La aprobación, revisión y cambios de esta política se establecen a través del Comité de Gestión y Desempeño Institucional y queda registrado en Acta.

13. CONTROL DE CAMBIOS

Versión	Descripción del Cambio	Fecha
01	Versión inicial del procedimiento	Noviembre 2 de 2021
02	Se realiza la modificación de todo el procedimiento desde el contenido hasta la aprobación Con el fin de fortalecer la evolución, logros y oportunidades de mejora de la Política de Seguridad Digital y así como una propuesta de actualización bajo los lineamientos del MINTIC,	Agosto 22 de 2023

Elaboró	Aprobó
Gestión Técnica	Comité de Gestión y desempeño Institucional