PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

TELEVISION REGIONAL DEL ORIENTE LTDA
CANAL TRO

CONTENIDO

INTRODUCCION 3
1. JUSTIFICACION 4
2. OBJETIVOS 4
2.1 Objetivos específicos 5
3. ALCANCE 5
4. NORMATIVIDAD 6
5. RESPONSABILIDADES 7
6. DEFINICIONES 7
7. DESARROLLO DEL PLAN 9
7.1 Identificación y valoración de riesgos de seguridad de la información 12
7.2 Administración de riesgos y el diseño de controles 12
7.3 Controles 13
8. SEGUIMIENTO Y REVISIÓN 13
9. CONTROL DE CAMBIOS 14

INTRODUCCIÓN

En la actualidad, las empresas están inmersas en la revolución digital, donde la información y los datos tienen un papel clave en los procesos productivos. Por eso, es fundamental identificar, proteger y gestionar adecuadamente esta información, cumpliendo con las obligaciones comerciales y contractuales, como los acuerdos de confidencialidad y otras normativas.

El plan de tratamiento de riesgos de Seguridad y Privacidad de la información, Seguridad Digital en el CANAL TRO, se basa en una orientación estratégica que requiere el desarrollo de una cultura de carácter preventivo y correctivo en la entidad, de manera que, al comprender el concepto de riesgo, así como el contexto, a través de este instrumento se planean las acciones que reduzcan la afectación a la entidad en caso de materialización de estos, adicional se busca desarrollar estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos con mayor objetividad, dando a conocer aquellas situaciones que pueden comprometer el cumplimiento de los objetivos trazados en el mundo del Entorno Digital.

El Canal TRO cumple con la normativa colombiana vigente, incluyendo el CONPES 3854 de 2016, el Modelo de Seguridad y Privacidad del MINTIC, y el Decreto 1008 de 14 de junio de 2018, adoptando las mejores prácticas y lineamientos del estándar ISO 27001:2013. Además, se alinea con ISO 31000:2018 y la guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital, emitida por el Departamento Administrativo de la Funciona Pública.

La seguridad de la información empresarial tiene como objetivo proteger los activos y datos frente a diversas amenazas que puedan afectar los principios fundamentales de privacidad, integridad y disponibilidad. Esto permite gestionar y reducir los riesgos e impactos a los que está expuesta la organización, maximizando el retorno de las inversiones y aprovechando las oportunidades del negocio. El Canal TRO define, a través del Manual de Políticas de Seguridad Digital, las conductas y responsabilidades.

1. Política de uso de correo electrónico
2. Política de escritorio y pantalla limpia
3. Política de respaldo y restauración de la información
4. Política de uso de internet
5. Política de reporte de incidentes de sistemas de información

6. Política de administración de contraseñas
7. Política de protección contra código malicioso
8. Política de acceso físico al Data Center
9. Política de mantenimiento de sistemas de información
10. Política de confidencialidad de la información
11. Política de gestión de calves de acceso a los sistemas de información
12. Política de uso de los activos de información
13. Política de uso de dispositivos de almacenamiento y transferencia de información

En virtud de lo expuesto, se define el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, dando continuidad a los procesos de mejora continua a partir de la identificación de riesgos inherentes asociados con la integridad, confidencialidad y disponibilidad de la información.

1. JUSTIFICACIÓN

El propósito de este documento es establecer una cultura de mitigar los riesgos que enfrentan diariamente los activos y los sistemas de información del CANAL TRO. Con base en el enfoque de planificación de la gestión de riesgos, se debe crear estrategias que permitan su identificación, diagnóstico, tratamiento y evaluación, con el fin de facilitar la implementación y desarrollo planes o contramedidas en los activos y sistemas de información para mitigar o eliminar la probabilidad de su ocurrencia o materialización.

2. OBJETIVOS

Establecer un marco de acción para el tratamiento de los riesgos de seguridad y privacidad de la información, aplicable a todos los activos, en especial a las tecnologías de la información que respaldan la prestación de servicios digitales de la Entidad. Este marco se basará en un enfoque de seguridad informática frente a diversas amenazas, definiendo acciones específicas para mitigar los riesgos.

1.1 Objetivos específicos

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información - PTRSPI da cumplimiento al objetivo general a través de los siguientes objetivos específicos:

3. ALCANCE

El Plan de Tratamiento de Riesgos aquí propuesto, establece los lineamientos de gestión de riesgos de Seguridad de la información del CANAL TRO adaptando la norma ISO 27001 contribuyendo a las buenas prácticas para gestión de la seguridad de la información, que ayuden a prevenir, controlar y mitigar las amenazas y los posibles ataques que afectan el logro de los objetivos, planes y estrategias en todos los procesos de la entidad.

La gestión de la seguridad representa un reto en cuanto a la implementación para las organizaciones, las cuales deben entender las implicaciones y el nivel de esfuerzo requerido, para lo cual se debe planificar muy bien y para llegar a tener una estrategia de implementación exitosa.

El plan debe ser aplicable para todas las funciones y procesos administrativos y de control, y debe ser ejecutado por todos los contratistas, administrativos, proveedores, socios comerciales y terceros que trabajen o presten servicios en el canal según las directrices de Gestión Técnica y Emisión.

4. NORMATIVIDAD

Norma	Descripción
Ley 527 de 1999	Define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, se establecen las entidades de certificación y se dictan otras disposiciones.
Ley 1712 de 2014	Crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
Decreto 1581 de 2012	Dicta disposiciones generales para la protección de datos personales.
Ley 1341 de 2009	Definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones TIC, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.
Decreto 1377 de 2013	Reglamenta parcialmente la Ley 1581 de 2012.
Decreto 2573 de 2014	Establece los lineamientos generales de la Estrategia de Gobierno en Línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
Decreto 1753 de 2015	Por la cual se expide el Plan Nacional de Desarrollo 2014 – 2018 “Todos por un nuevo país”.
Decreto 1978 de 2015	Marco de referencia de arquitectura empresarial para la gestión de TI. (Artículo 2.2.5.1.2.2)
Decreto 1078 de 2015	Por medio del cual se expide el Decreto único reglamentario del sector de función pública.
Decreto 415 de 2016	Por el cual se adiciona el Decreto único reglamentario del sector de la función pública, Decreto 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones.
CONPES 3854 - 2016	“Política Nacional de Seguridad Digital”, se consideró que era necesario cambiar el enfoque tradicional e incluir la gestión de riesgo como uno de los elementos más importantes para abordar la temática.
Decreto 1008 de 2018	Por el cual establece el Objeto. El presente capítulo establece lineamientos generales de la Política de Gobierno Digital para Colombia, antes estrategia de Gobierno en Línea, la cual desde ahora debe ser entendida como: el uso y aprovechamiento de las

	tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos e innovadores, que generen valor público en un entorno de confianza digital.
CONPES 3995 DE 2020	Política Nacional de Confianza y Seguridad Digital. De esta manera, el objeto es establecer medidas para ampliar la confianza digital y mejorar la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital. Para alcanzar este objetivo: 1., se fortalecerán las capacidades en seguridad digital de los ciudadanos, del sector público y privado del país; 2. se actualizará el marco de gobernanza en materia de seguridad digital para aumentar su grado de desarrollo y finalmente, se analizará la adopción de modelos, estándares y marcos de trabajo materia de seguridad digital, con énfasis en nuevas tecnologías.
Decreto 767 de 2022	El presente capítulo establece los lineamientos generales de la Política de Gobierno Digital, entendida como el uso y aprovechamiento de las Tecnologías de la Información y las Comunicaciones, con el objetivo de impactar positivamente la calidad de vida de los ciudadanos y, en general, los habitantes del territorio nacional y la competitividad del país, promoviendo la generación de valor público a través de la transformación digital del Estado.

5. RESPONSABILIDADES

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

Proceso de Gestión Técnica y Emisión es el responsable de emitir las normas, manuales, guías y la metodología de implementación del Plan de tratamiento de riesgos.

Los procesos de Planeación y Control Interno, es responsable del control y evaluación del tratamiento de riesgos de seguridad y privacidad de la información, como también proporcionar los recursos y estrategias para el desarrollo del plan realizando seguimiento y verificación de la implementación.

6. DEFINICIONES

Acceso a la Información: Conjunto de técnicas para buscar, categorizar, modificar y acceder a la información que se encuentra en un sistema de bases de datos, archivos en red.

Acción correctiva: Conjunto de técnicas para buscar, categorizar, modificar y acceder a la información que se encuentra en un sistema de bases de datos, archivos en red.

Acción correctiva: Medida orientada a eliminar la causa de cualquier amenaza, evento, riesgo o vulnerabilidad asociada a la seguridad de la información.

Acción preventiva: Medida orienta a prevenir cualquier amenaza, evento, riesgo o vulnerabilidad asociada a la seguridad de la información.

Activo de información: Datos o información que tienen un valor para una Entidad.

Amenaza: Circunstancia, suceso o persona con el potencial para dañar un sistema mediante la destrucción, divulgación, modificación de datos o negación de servicios.

Análisis de riesgo: Método cualitativo o cuantitativo para la evaluación del impacto de riesgo en la toma de decisiones.

Aplicaciones: Es todo software que se utiliza para la gestión o manejo de la información.

Autenticación: Proceso que tiene por objetivo asegurar la identificación de una persona en cualquiera de los sistemas de información de la entidad.

Autorización: Consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales.

BackUp: Parámetros que determinan que equipo o información debe incluirse en una copia de respaldo dentro de la entidad.

Confidencialidad: Mantener la información oculta a individuos, entidades o proceso no autorizados.

Control: Procedimiento, procesos, políticas que permitan mantener el riesgo de la seguridad de la información por debajo del riesgo presente.

Denegación de servicio: Es una acción iniciada por un ataque a un sistema objetivo, que provoca la denegación a los usuarios legítimos forzando su cierre o conllevando a una inoperatividad.

Disponibilidad: Mantener la información accesible a quien la necesita en el momento que la necesite.

Dispositivo: Es un ordenador que se puede utilizar para acceder a los servicios de red, computador.

Evento: Suceso identificado en un sistema, estado que deja al descubierto una brecha de seguridad.

Ingeniería social: Método utilizado para engañar a los usuarios informáticos, para que realicen una acción que normalmente producirá consecuencias negativas, como la divulgación de información.

Integridad: Prevenir la modificación no autorizada de la información.

Política: Medidas necesarias para garantizar la seguridad de las tecnologías de la información.

Riesgo: Posibilidad de que ocurra un contra tiempo o alerta.

Seguridad de la información: Según ISO 27002 es la preservación de la confidencialidad, integridad y disponibilidad de la información.

Seguridad informática: Encargada de diseñar las normas, procedimientos, métodos y técnicas destinadas a conseguir un sistema de gestión de seguridad de la información seguro y confiable.

Seguridad física: Limites mínimos que se den cumplir en cuanto a los perímetros de seguridad, de forma que se puedan establecer controles.

Seguridad lógica: Integrar mecanismos y procedimientos que permitan monitorear el acceso a los activos de la información.

SGSI: Sistema de Gestión de Seguridad de la Información. Es un mecanismo que permite preservar la confidencialidad, integridad y disponibilidad de la información.

Usuario: Cualquier personal que haga uso de los servicios de red proporcionados por la entidad tales como equipos de cómputos, sistemas de información y redes.

Virus: Es un tipo de software o aplicación que tiene como objetivo alterar el normal funcionamiento de los equipos tecnológicos, sin permiso o conocimiento de los usuarios.

Vulnerabilidad: Condición de un sistema que lo hace susceptible a una amenaza.

7. DESARROLLO DEL PLAN

El CANAL TRO, a través de su Sistema Integrado de Gestión y Gestión Técnica y Emisión, se comprometen a mantener una cultura de la gestión del riesgo asociados con la responsabilidad de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector TIC, regulando los riesgos de los procesos y proyectos actuando continuamente contra la corrupción; mediante mecanismos, sistemas y controles enfocados a la prevención y detección de hechos asociados a este fenómeno y fortaleciendo las medidas de control y la eficiencia a lo largo del ciclo de vida del proyecto para optimizar de manera continua y oportuna la respuesta a los riesgos además de los de seguridad y privacidad de la Información y Seguridad Digital de manera integral con el compromiso de toda la comunidad institucional.

El tratamiento del riesgo para activos de información nos permite desde un punto de vista orientado al negocio y sistémico en su naturaleza, comprender claramente los riesgos a los que puede estar expuesto el CANAL TRO.

A continuación, se presenta la estructura de la metodología de riesgos y actividades que permitirán desarrollar e implementar, lo dispuesto en el presente plan. La metodología está integrada por las siguientes etapas:

a) Establecimiento del contexto

Permite a los responsables y/o lideres de procesos describir el entorno y las situaciones particulares de ésta con los actores del ámbito de su dependencia.

b) Identificación del riesgo

Establecer cuáles son los activos críticos para asociarlos a los procesos correspondientes y de allí generar el listado de procesos críticos. Inventariar los activos de información sensible, revisar los procesos según la clasificación y del modelo de gestión, con este punto se revisa la pertinencia del alcance planteado para el MSPI.

c) Evaluación del riesgo

Los responsables y/o lideres de procesos identifican, analizan y evalúan los riesgos a fin de determinar aquellos que por su impacto y probabilidad de ocurrencia pueden afectar el cumplimiento de las metas y objetivos de la dependencia.

d) Tratamiento del riesgo

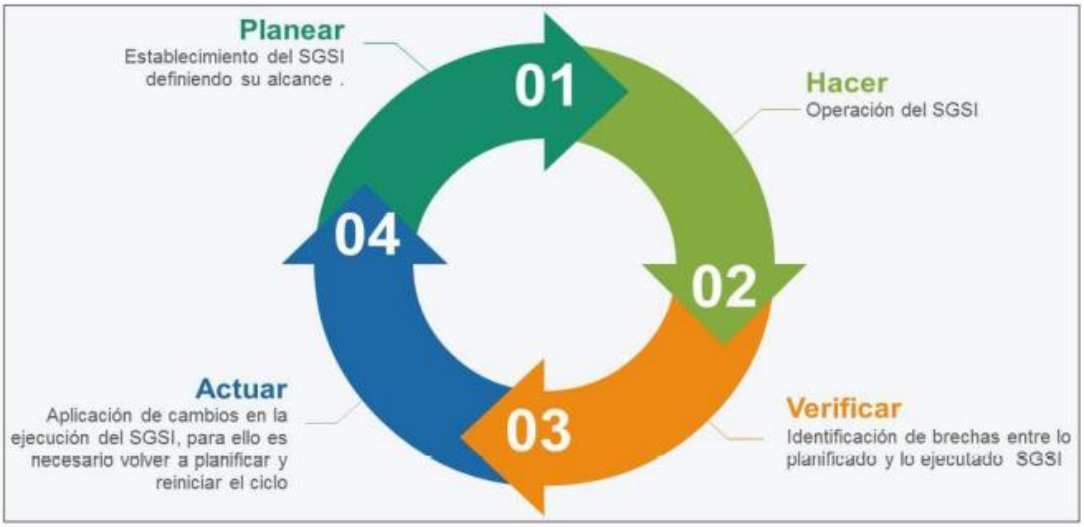
Identificar y analizar los riesgos, de esta forma se busca escoger los controles que permitan disminuir los valores de exposición, daño o perdida del riesgo, y luego se debe hacer un recalculo comparando nuevamente con los criterios establecidos y así buscar un nivel aceptable del riesgo en cada proceso para los temas de Seguridad de la Información.

e) Aceptación del riesgo

Los criterios de aceptación del riesgo pueden incluir requisitos para tratamiento adicional en el futuro, por ejemplo, se puede aceptar un riesgo si existe aprobación y compromiso

para ejecutar acciones que reduzcan dicho riesgo hasta un nivel aceptable en un periodo definido de tiempo.

La gestión del riesgo dentro de la seguridad de la información se puede también enmarcar dentro del ciclo de planear, hacer, verificar y actuar (PHVA) tal como se muestra en la siguiente ilustración (ISO 27001:2013):



7.1 Identificación y valoración de riesgos de seguridad de la información

La identificación y valoración de los riesgos de seguridad de la información está compuesto por los siguientes hitos o actividades:

Actividad	Descripción
Programación y agendamiento de entrevistas	En esta fase se seleccionan los procesos incluidos en el alcance del plan del CANAL TRO y se procede a programar y a agendar a los líderes de las dependencias y grupos internos de trabajo que conforman los procesos, para la identificación de riesgos.
Entrevista con los líderes de proceso del CANAL TRO	Se entrevista a cada líder de proceso, se presenta la metodología y en conjunto se procede a realizar la identificación de los riesgos sobre los activos de información, los cuales se consignan en la Matriz de Riesgos.

Identificación y calificación de riesgos	En el proceso de identificar los riesgos dentro del CANAL TRO, es clave contar con información coherente y actualizada acerca de las actividades que se llevan a cabo en los diferentes procesos, los resultados esperados de las mismas, como orígenes de riesgos, se puede acudir a diversas fuentes de información.
Valoración del riesgo residual	En esta fase se hace una proyección de la eficacia de los controles para calcular el riesgo residual: - Las fuentes de riesgos materiales, las que podemos ver y las fuentes de riesgos que no podemos identificar a simple vista o que existe y se pasan por alto. - Del análisis de contexto extraer las amenazas y debilidades para la identificación de riesgos y las oportunidades de mejora. - Caracterizar los activos y recursos con los que cuenta el CANAL TRO, identificando su naturaleza, importancia y valor. - Los aspectos relacionados con los tiempos.
Mapas de calor donde se ubican los riesgos	Luego se procede a ubicar los riesgos en un mapa de calor para visualizar su comportamiento a medida que se van aplicando los controles.

7.2 Administración de riesgos y el diseño de controles

Una vez ejecutadas las etapas de análisis y valoración de riesgos, y con base en los resultados obtenidos en la determinación real de riesgos, es necesario tomar decisiones aplicando el apetito de riesgos definido por el CANAL TRO.

Si el riesgo se ubica en una zona No Aceptable (Altos y Extremos), cada líder es responsable de los riesgos identificados y con el apoyo de los líderes de Gestión Técnica y Emisión como Planeación deben definir e implementar los controles necesarios para llevar el riesgo a un nivel Aceptable a través del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

A continuación, se define la estrategia de tratamiento, consistente en asumir los riesgos Bajos y Moderados a través del monitoreo, y gestionar los riesgos Altos y Extremos a través de la implementación de controles por parte de los responsables del cada uno de los procesos.

Controles

Para la gestión y tratamiento de los riesgos, como estrategia de mitigación, se definirán actividades asociadas a los siguientes controles de la norma ISO 27001: 2013 Anexo A.

114 controles de seguridad. Algunos de los riesgos tienen más de un control asociado así:

- A.7.2.2.2 Toma de conciencia, educación y formación en la seguridad de la información
- A.8.2.3 Manejo de activos
- A.9 Control de accesos
- A.11.2.6 Seguridad de equipos y activos fuera de las instalaciones
- A.11.1.3 Seguridad de oficinas, recintos e instalaciones
- A.11.2.4 Mantenimiento de equipos
- A.12.3.1 Copias de respaldo de la información
- A.12.6.1 Gestión de vulnerabilidades técnicas
- A.14.1.3 Protección de transacciones de los servicios de las aplicaciones
- A.17.1.1 Planificación de la continuidad de la seguridad de la información
- A.18.1.4 Privacidad y protección de la información de datos personales
- A.9.2.1 Registro y cancelación de registro de usuarios

8. SEGUIMIENTO Y REVISIÓN

Teniendo en cuenta que los riesgos son dinámicos y pueden cambiar de forma sin ser previsto es necesario definir mecanismos que permitan hacer una supervisión continua que detecte: nuevos activos o modificaciones en el valor de los activos, nuevas amenazas, cambios o aparición de nuevas vulnerabilidades, aumento de las consecuencias o impactos, incidentes de seguridad de la información.

En este sentido se deben establecer instrumentos para realizar la revisión del valor de los activos, impactos, amenazas, vulnerabilidades y probabilidades en busca de posibles cambios, que exijan la valoración iterativa de los riesgos de seguridad de la información. También se deberán definir esquemas de seguimiento y medición al sistema de gestión de riesgos de la seguridad de la información, con el propósito de conocer los estados de cumplimiento de los objetivos de la gestión de los riesgos de seguridad de la información.

Dentro de las actividades que se ejecutan en esta fase, se tienen:

- Analizar los cambios, las tendencias, los éxitos y los fracasos dentro del proceso de gestión de riesgos de seguridad de la información.
- Detectar cambios en el contexto interno o externo, incluyendo los cambios que se puedan presentar en los criterios de riesgos de seguridad de la información.

- Revisar la implementación de los planes de tratamiento de riesgo de seguridad de la información y las prioridades de implementación de estos.
- Identificación de nuevos riesgos de seguridad de la información.
- La revisión de la gestión de riesgos se debe hacer por lo menos una vez al año, el seguimiento a los riesgos debe ser permanente por parte de los líderes de los procesos involucrados

9. HOJA DE RUTA 2025

ACTIVIDADES	ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC
Establecimiento del contexto												
Comité Institucional de Gestión y Desempeño												
Identificación de riesgos de seguridad de la información												
Identificación de Activos de Información de Acuerdo a Inventario												
Identificación de Activos de Información de Acuerdo al SIG												
Identificar Activos Críticos												
Identificar Procesos Críticos												
Relacionar Activos y Procesos Críticos												
Evaluación del Riesgo												
Analizar y Evaluar los Riesgos												
Identificar Riesgos que Afecten el cumplimiento de objetivos y/o metas												
Tratamiento de Riesgos												
Identificación de Riesgos en la Zona de No Aceptables												
Definir e implementar Controles para Riesgo en la Zona no Aceptables												
Estrategia de Monitoreo para Riesgos Bajos y Moderados												

Estrategia de Control de los Riesgos Alto y Extremos												
Controles												
Definir actividades asociadas a los controles seleccionados de la norma ISO 27001: 2013 Anexo A												
Seguimiento												
Identificación de Nuevos Activos												
Identificación de Nuevas Amenazas y Vulnerabilidades												
Identificación de Cambios												
Aumento de Incidentes												
Análisis de Éxito												
Análisis de Fracaso												

10. CONTROL DE CAMBIOS

Versión	Descripción del cambio	Fecha
01	Versión inicial	Enero 25 de 2023
02	Se actualiza el plan según lo propuesto por la auditoría de control interno con el fin de definir en el desarrollo del plan los controles del riesgo. Desde la tabla de contenido hasta el punto 8 de seguimiento y revisión	Octubre 30 de 2023
03	Se Actualiza el plan teniendo en cuenta la inclusión de la hoja de ruta para la vigencia 2024	Enero 30 de 2024
04	Se actualiza el contenido del plan dentro del alcance y la hoja de ruta para la vigencia 2025	Enero 30 de 2025

Elaboró	Aprobó
Líder del proceso de Técnica	Comité de Gestión y desempeño Institucional.