# PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION PSPI

## TELEVISION REGIONAL DEL ORIENTE LTDA
## CANAL TRO

**CONTENIDO**

## INTRODUCCIÓN

Toda organización, independientemente de su tamaño y naturaleza, debe comprender los riesgos que plantea la variedad actual de amenazas a la privacidad y la seguridad de la información, que, cuando se materialicen, no solo generarán costos financieros o sanciones legales; esto afecta no solo su imagen y reputación, sino también la continuidad del negocio. Lo anterior, combinado con un entorno de tecnología de seguridad y administración cada vez más complejo, significa que la seguridad de la información se está convirtiendo cada vez más parte de los objetivos y planes estratégicos de una organización. Por lo tanto, las autoridades de una organización responsables de proteger y asegurar sus recursos, infraestructura e información deben adoptar, implementar y mejorar las medidas de seguridad para prevenir y/o detectar riesgos que puedan comprometer la disponibilidad. Administrar la integridad y confidencialidad de los activos de información de una empresa, ya sea corporativa o personal, pública o privada.

En la medida que las organizaciones tengan una visión general de los riesgos que pueden afectar la seguridad y privacidad de la información, podrán establecer controles y medidas efectivas, viables y transversales con el propósito de salvaguardar la disponibilidad, integridad y confidencialidad tanto de la información del negocio como los datos de carácter personal de sus empleados, usuarios y partes interesadas. Es indispensable que las organizaciones realicen una adecuada identificación, clasificación, valoración, gestión y tratamiento de los riegos que pueden afectar su seguridad, con el propósito de implementar medidas y controles efectivos que les permitan estar preparados ante situaciones adversas que puedan comprometer tanto la seguridad física y lógica de sus instalaciones, personas, recursos y sistemas, como la seguridad de su información.

Para el Canal TRO es fundamental garantizar y proteger la seguridad y protección de la información y los datos personales de toda la comunidad institucional, entendiendo que la protección de su información es esencial para avalar una adecuada gestión financiera, administrativa y operativa y, por lo tanto, se requiere la implementación de un marco regulatorio de seguridad de la información que incluya políticas, responsabilidades y obligaciones para la seguridad y privacidad de la información.

Este documento incluye el plan de seguridad y privacidad de la información para el Canal TRO, que tendrá como referencia el modelo de seguridad y privacidad de la estrategia de gestión en línea y la norma ISO 27001, los cuales suministran un marco metodológico basado en buenas prácticas para la implantación de un modelo de gestión de la seguridad

y privacidad de la información en todo tipo de organizaciones, que permita su gestión efectiva y asegure su continuidad y adecuado desarrollo.

## 1. JUSTIFICACIÓN

Para Canal TRO es importante la protección de la información, con el fin de crear una cultura diseñada para minimizar y eliminar el riesgo de los activos informáticos y sistemas de información. El Plan de Seguridad y Privacidad de la Información (PSPI) está basado en un enfoque de planificación de la gestión de riesgos y tomar decisiones sobre el impacto del mismo donde se debe implementar estrategias que permitan el diagnóstico, evaluación, ejecución y luego el desarrollo de la gestión de eventos que afectan la continuidad de la información y las contramedidas para reducir la probabilidad de la ocurrencia.

## 2. OBJETIVOS

## 3. ALCANCE

Esto se aplica a todos los niveles del Canal TRO y todos sus empleados, contratistas, operadores y todas las personas o terceros cuya información se comparte, utiliza, recopila, procesa, intercambia o se accede en el desempeño de sus funciones y como entidad de control. Asimismo, este plan se aplica a toda la información generada, procesada o utilizada por el Canal TRO, independientemente de su medio, formato, imágenes o ubicación.

## 4. ALINEACIÓN NORMA ISO 27001:2013 VS CICLO DE OPERACION

Desde la Gerencia y Gestión Técnica y Emisión, entienden la importancia de una adecuada gestión
información, implementar sistemas de gestión con el propósito de mejorar y mitigar la seguridad de la información creando marcos de confianza en la práctica, esto se hace de acuerdo con la ley y la misión y visión del Canal TRO.

La protección de la información del Canal está diseñada para minimizar su impacto, identificando sistemática los activos riesgosos para mantener el nivel de exposición para que las respuestas sean integradas, confidencialidad y accesibilidad a las necesidades de la comunidad institucional.

Según con nuestro objetivo general, el Modelo de Seguridad y Privacidad de la Información de la Estrategia de Gobierno en Línea contiene el **ciclo de operación** que contempla cinco fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos informáticos.


Fuente: http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html

| FASES | DESCRIPCION |
|---|---|
| **Diagnóstico** | Permite identificar el estado actual de la entidad con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información |
| **Planificación (Planear)** | En esta fase se establecen los objetivos a alcanzar y las actividades del proceso susceptibles de mejora, así como los indicadores de medición para controlar y cuantificar los objetivos. |
| **Implementación (Hacer)** | En esta fase se ejecuta el plan establecido que consiste en implementar las acciones para lograr mejoras planteadas. |
| **Evaluación de desempeño (Verificar)** | Una vez implantada la mejora, se establece un periodo de prueba para verificar el correcto funcionamiento de las acciones implementadas. |
| **Mejora Continua (Actuar)** | Se analizan los resultados de las acciones implementadas y si estas no se cumplen los objetivos definidos se analizan las causas de las desviaciones y se generan los respectivos planes de acciones. |

Aunque ISO 27001:2013 no especifica un modelo de mejora continua (PHVA) como requisito para establecer un sistema de gestión de seguridad de la información operativa, esta versión de la nueva arquitectura puede adaptarse a un ciclo de mejora continua o de operación, de la siguiente manera:


Fuente:[http://www.welivesecurity.com/la-es/2013/10/09/publicada-iso-270002013-cambios-en-la- norma-para-gestionar-la-seguridad-de-la-informacion/](http://www.welivesecurity.com/la-es/2013/10/09/publicada-iso-270002013-cambios-en-la- norma-para-gestionar-la-seguridad-de-la-informacion/)

La siguiente tabla muestra la relación entre las diferentes fases del ciclo de operación del modelo de seguridad y privacidad de la información (diagnóstico, planificación,

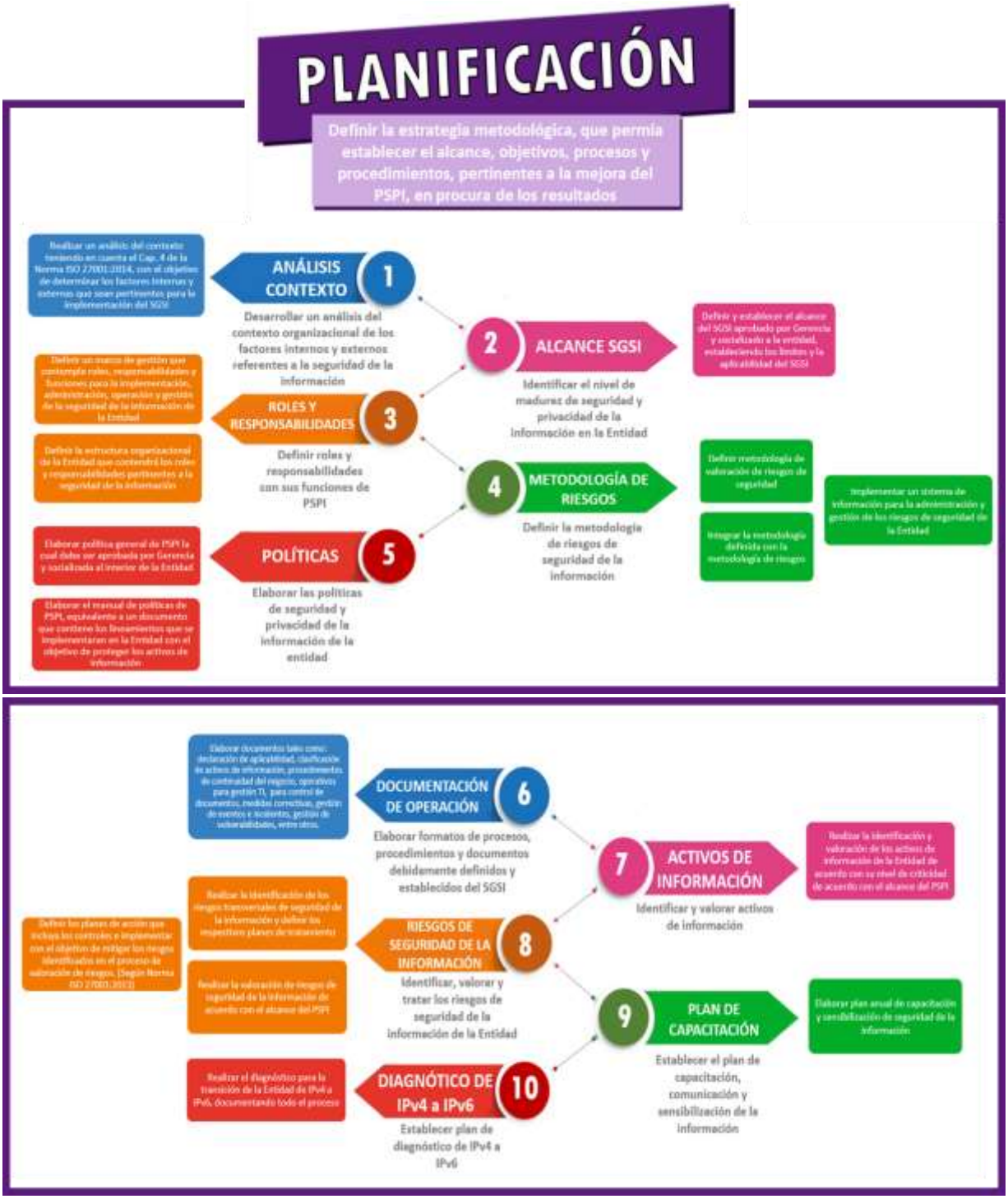
implementación, evaluación y mejora continua) y el número de estructuras y capítulos de la norma ISO 27001:2013:

| FASES ISO 27001:2013 | | DESCRIPCION |
|---|---|---|
| **DIAGNÓSTICO**<br>**Cap. 4: Contexto de la organización** | | Determinar la necesidad de analizar los problemas externos e internos y el contexto de la organización para satisfacer las necesidades y expectativas de las partes interesadas. |
| **PLANEACIÓN** | **Cap. 5: Liderazgo** | Determinar los deberes, responsabilidades y roles en el sistema de gestión de seguridad de la información. |
| | **Cap. 6: Planificación** | Identificar los requisitos para evaluar y abordar los riesgos de seguridad, y definir los objetivos de seguridad de la información apropiados y los planes específicos para lograr esos objetivos. |
| | **Cap. 7: Soporte** | La organización debe proporcionar los recursos necesarios para la creación, implementación y mejora continua del sistema de gestión de seguridad de la información. |
| **IMPLEMENTACIÓN**<br>**Cap. 8: Operación** | | Especifica que la organización debe planificar, implementar y controlar los procesos necesarios para lograr sus objetivos y requisitos de seguridad y para llevar a cabo la evaluación y el tratamiento de los riesgos de seguridad de la información. |
| **EVALAUCIÓN DE DESEMPEÑO**<br>**Cap. 9 Evaluación de desempeño** | | Establecer requisitos para la evaluación periódica del desempeño de la seguridad de la información y la eficacia del sistema de gestión de la seguridad de la información. |
| **MEJORA**<br>**Cap. 10 Mejora** | | Se establece para el proceso de mejora del SGSI, que a partir de las no-conformidades que ocurran, las organizaciones deben establecer las acciones más efectivas para solucionarlas y evaluar la necesidad de acciones para eliminar las causas de la no conformidad con el objetivo de que no se repitan |

Fuente: NTC-ISO-IEC 27001:2013, Pág. 1-12

## 5. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El plan de seguridad y privacidad de la información (PSPI) determina los objetivos a cumplir para salvaguardar la información en sus pilares de confidencialidad, integridad y disponibilidad del Canal TRO. A continuación, se encuentran las metas y actividades en cada una de las fases, anteriormente mencionadas.


PLANIFICACIÓN
Definir la estrategia metodológica, que permia establecer el alcance, objetivos, procesos y procedimientos, pertinentes a la mejora del PSPI, en procura de los resultados
Realizar un análisis del contexto teniendo en cuenta el Cap. 4 de la Norma ISO 27001:2014, con el objetivo de determinar los factores internos y externos que sean pertinentes para la implementación del SGSI
ANÁLISIS CONTEXTO
1
Desarrollar un análisis del contexto organizacional de los factores internos y externos referentes a la seguridad de la información
2
ALCANCE SGSI
Identificar el nivel de madurez de seguridad y privacidad de la información en la Entidad
Definir y establecer el alcance del SGSI aprobado por Gerencia y socializado a la entidad, estableciendo los límites y la aplicabilidad del SGSI
Definir un marco de gestión que contemple roles, responsabilidades y funciones para la implementación, administración, operación y gestión de la seguridad de la información de la Entidad
ROLES Y RESPONSABILIDADES
3
Definir roles y responsabilidades con sus funciones de PSPI
Definir la estructura organizacional de la Entidad que contendrá los roles y responsabilidades pertinentes a la seguridad de la información
4
METODOLOGÍA DE RIESGOS
Definir la metodología de riesgos de seguridad de la información
Definir metodología de valoración de riesgos de seguridad
Integrar la metodología definida con la metodología de riesgos
Implementar un sistema de información para la administración y gestión de los riesgos de seguridad de la Entidad
Elaborar política general de PSPI la cual debe ser aprobada por Gerencia y socializada al interior de la Entidad
POLÍTICAS
5
Elaborar las políticas de seguridad y privacidad de la información de la entidad
Elaborar el manual de políticas de PSPI, equivalente a un documento que contiene los lineamientos que se implementaran en la Entidad con el objetivo de proteger los activos de información
Elaborar documentos tales como: declaración de aplicabilidad, clasificación de activos de información, procedimientos de continuidad del negocio, operativos para gestión TI, para control de documentos, medidas correctivas, gestión de eventos e incidentes, gestión de vulnerabilidades, entre otros.
DOCUMENTACIÓN DE OPERACIÓN
6
Elaborar formatos de procesos, procedimientos y documentos debidamente definidos y establecidos del SGSI
7
ACTIVOS DE INFORMACIÓN
Identificar y valorar activos de información
Realizar la identificación y valoración de los activos de información de la Entidad de acuerdo con su nivel de criticidad de acuerdo con el alcance del PSPI
Realizar la identificación de los riesgos transversales de seguridad de la información y definir los respectivos planes de tratamiento
Definir los planes de acción que incluya los controles a implementar con el objetivo de mitigar los riesgos identificados en el proceso de valoración de riesgos. (Según Norma ISO 27001:2013)
RIESGOS DE SEGURIDAD DE LA INFORMACIÓN
8
Identificar, valorar y tratar los riesgos de seguridad de la información de la Entidad
Realizar la valoración de riesgos de seguridad de la información de acuerdo con el alcance del PSPI
9
PLAN DE CAPACITACIÓN
Establecer el plan de capacitación, comunicación y sensibilización de la información
Elaborar plan anual de capacitación y sensibilización de seguridad de la información
Realizar el diagnóstico para la transición de la Entidad de IPv4 a IPv6, documentando todo el proceso
DIAGNÓTICO DE IPv4 a IPv6
10
Establecer plan de diagnóstico de IPv4 a IPv6


IMPLEMENTACIÓN
Llevar acabo la implementación de la fase de planificación del SGSI teniendo en cuenta para esto los aspectos más relevantes del SGSI
1. PLAN DE IMPLEMENTACIÓN
Establecer el plan de implementación de seguridad de la información el cual debe ser revisado y aprobado por Gerencia y Área Técnica
2. PLAN DE TRATAMIENTO DE RIESGOS
Ejecutar el plan de tratamiento de los riesgos transversales de seguridad de la información identificados en la fase de planificación
3. PLAN DE TRANSICIÓN IPv4 A IPv6
Ejecutar dal plan y estrategia de transición de IPv4 a IPv6 y elaborar informe de implementación
4. INDICADORES DE GESTIÓN DE SEGURIDAD
Definir los indicadores para medir la gestión de seguridad y establecer los mecanismos para su medición y verificar la eficacia y efectividad de los controles implementados para mitigar los riesgos
5. PROCEDIMIENTO DE EVENTOS DE SEGURIDAD
Implementar el procedimiento y los mecanismos para la gestión de los eventos e incidentes de seguridad de la información
6. PROCEDIMIENTO DE VULNERABILIDADES
Implementar el procedimiento y los mecanismos para la gestión de vulnerabilidades de seguridad de la información
7. PLAN DE CAPACITACIÓN
Ejecutar el plan anual de capacitación y sensibilización de seguridad de la información
8. PRUEBAS DE VULNERABILIDADES
Ejecutar el plan anual de pruebas vulnerabilidades e intrusión con el objetivo de identificar el nivel de protección de los activos de información
9. PRUEBAS DE ETICA HACKING
Implementar pruebas anuales de Ética Hacking orientadas a poder determinar los niveles de riesgo y exposición de la organización ante atacantes interno o externo que puedan comprometer activos críticos
10. PRUEBAS DE INGENIERIA SOCIAL
Ejecutar pruebas anuales de ingeniería social orientadas a verificar protocolos internos de seguridad y el nivel de concientización de los funcionarios, el conocimiento y cumplimiento de las políticas


EVALUACIÓN DE DESEMPEÑO
Evaluar el desempeño y al eficacia del SGSI, se hace con base a los resultados que arrojan los indicadores de la seguridad de la información de las acciones implementadas.
AUDITORIAS
Ejecutar auditorias internas del modelo de seguridad y de temas normativos y de cumplimiento de seguridad de la información aplicables a la Entidad, con la finalidad de verificar que los objetivos de control, procesos y procedimientos del SGSI cumplan con los requisitos
PLAN DE SEGUIMIENTO
Elaboración del documento con el plan de seguimiento, evaluación y análisis del SGSI revisado y aprobado por el Área Técnica y Gerencia


## 6. CONCEPTOS

**ACTIVO DE INFORMACIÓN:** Aquello que es de alta validez y que contiene información de la empresa que debe ser protegida.
**AMENAZA:** Es la causa potencial de un daño a un activo de información.
**ANÁLISIS DE RIESGO:** Utilización sistemática de la información disponible, para identificar peligros y estimar los riesgos.
**CAUSA:** Razón por la cual el riesgo sucede.
**CICLO DE DEMING**: Modelo mejora continua para la implementación de un sistema de mejora continua.
**CONFIDENCIALIDAD:** Propiedad que determina que la información no esté disponible a personas no autorizadas.
**CONTROLES:** Son aquellos mecanismos utilizados para monitorear y controlar acciones que son consideradas sospechosas y que pueden afectar de alguna manera los activos de información.
**DISPONIBILIDAD:** Propiedad que determina que la información se accesible y utilizable por aquellas personas debidamente autorizadas.

**IMPACTO:** Consecuencias de que la amenaza ocurra. Nivel de afectación en el activo de información que se genera al existir el riesgo.
**INCIDENTE:** Evento no deseado o inesperado, que tiene una probabilidad de amenazar la seguridad de la información.
**INTEGRIDAD:** Propiedad de salvaguardar la exactitud y estado completo de los activos.
**PROBABILIDAD DE OCURRENCIA:** Posibilidad de que se presente una situación o evento específico.
**RESPONSABLE DEL ACTIVO:** Persona responsables del activo de información.
**RIESGO:** Grado de exposición de un activo que permite la materialización de una amenaza.
**RIESGO INHERENTE:** Nivel de incertidumbre propio de cada actividad, sin la ejecución de ningún control.
**RIESGO RESIDUAL:** Nivel de riesgo remanente como resultado de la aplicación de medida de seguridad sobre el activo.
**SEGURIDAD DE LA INFORMACIÓN:** Preservación de la confidencialidad, la integridad y la disponibilidad de la información (ISO 27001:2013).
**SGSI:** Sistema de Gestión de Seguridad de la Información.
**SGSI:** Sistema que permite establecer, implementar, mantener y mejora continuamente la gestión de la seguridad de la información de acuerdo con los requisitos de la norma NTC-ISO-IEC 27001.
**VULNERABILIDAD:** Debilidad de una activo o grupo de activos de información que puede ser aprovechada por una amenaza. La vulnerabilidad se caracteriza por ausencia en controles de seguridad que permite ser explotada.

## 7. CONTROL DE CAMBIOS.

| Versión | Descripción del cambio | Fecha |
|---|---|---|
| 01 | Versión inicial | Enero 25 de 2023 |

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