PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN

PESI

Teveandina s.a.s. – Canal Trece

Revisiones y control de cambios

Titulo	**Plan Estratégico de Seguridad de la Información - PESI, TEVEANDINA S.A.S– CANAL TRECE**
Autores	Gonzalo Joya, Wilmar López
Tema	Plan Estratégico de Seguridad de la información - PESI
Fecha de Elaboración	Noviembre 2023
Formato	PDF
Versión	1.0
Palabras Relacionadas	Evaluación de riesgos, Análisis de impacto, Políticas de seguridad, Cumplimiento normativo, Confidencialidad, Integridad de la información, Amenazas cibernéticas, Malware y ransomware, Concienciación de seguridad, Formación de empleados, Recuperación ante desastres, Plan de contingencia.

Control de Cambios			
Fecha	**Autores**	**Versión**	**Cambio**
Noviembre 2023	Wilmar López Gonzalo Joya	1.0	Versión Inicial
Octubre 2024	Camilo Beltrán – Wilmar López	2.0	Este documento Contempla 2 Versiones con fecha Mayo 2023, se realizó actualización de formato y de codificación, adicionalmente se actualizó el contenido en cumplimiento de la normatividad vigente
Enero 2025	Camilo Beltrán – Wilmar López	2.1	incluye actualización de contenido bajo cumplimiento con la normatividad vigente.

TABLA DE CONTENIDO

TABLA DE ILUSTRACIÓN

CONTENIDO DE TABLAS

1. INTRODUCCIÓN

La información actualmente se identifica como uno de los activos valiosos en la conducción y consecución de los objetivos definidos en un Plan Estratégico. Es necesario establecer un marco en el cual se proteja la información y se asegure de manera adecuada independientemente del medio en la que ésta sea frecuentada, almacenada, procesada, manejada o transportada. Adicional, a medida en que los sistemas de información se constituyen en un apoyo de los procesos de la entidad, se requiere contar con estrategias de alto nivel que permitan el control y administración asertiva de la información.

La metodología CID (Confidencialidad, Integridad y Disponibilidad) nos ayudara a la identificación y valoración de los activos de información, y con una herramienta definida por la entidad su evaluación y tratamiento del riesgo; siendo éste el último, el medio más consecuente de tratar, gestionar y minimizar, considerando el impacto para la entidad y las partes interesadas.

El Modelo de Seguridad y Privacidad de la Información (MSPI), como una de estas herramientas, define una metodología de autodiagnóstico eficaz y coherente frente a la estrategia de la entidad, desarrollando controles adoptados para el tratamiento de los riesgos, los cuales están en continuo seguimiento y medición, a través de indicadores que aseguren la eficacia de estos.

En apoyado a lo expuesto, los programas de auditoría y revisión enriquecen y fortalecen la identificación de oportunidades de mejora las cuales proyectan el progreso continuo del Modelo. En atención a lo anterior, Teveandina Canal Trece, implementa el Modelo de Seguridad y Privacidad de la Información - MSPI de la Estrategia de Gobierno Digital, a través del Decreto 1008 de 2018 para el sector de tecnologías de la información y comunicaciones y el Decreto 2573 de 2014 el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea.

TEVEANDINA CANAL TRECE, trazo como normativas: la NTC/ISO 27001:2022 la cual establece los requisitos para la implementación del SGSI, la NTC/ISO 31000:2011 que proporciona el esquema para la gestión de riesgos y las mejores prácticas, tales como GTC/ISO 27002:2022, ISO 27005:2008 buscando mejorar el desempeño y la capacidad para prestar un servicio que responda a las necesidades y expectativas.

A su par, el Plan Estratégico de Tecnologías de la Información y Comunicaciones (PETI), documento que expresa las finalidades en la implementación de iniciativas y acciones que impulsen, fomenten, promuevan, protegen y apoyen el uso de las Tecnologías de la Información y las Comunicaciones TICS, como contributivo al logro de los Objetivos y Lineamientos Estratégicos enmarcados en el Plan Estratégico Institucional (PETI), lo citado y descrito en este documento está organizado completamente con el PETI.

En conclusión, los lineamientos y proyectos para el desarrollo, optimización e implementación efectiva de los Sistemas de Información, así como las iniciativas que permitirán una adecuada gestión de la Infraestructura tanto de Hardware como de Software, basados en el SGSI y en las mejores prácticas de Gestión del Modelo de Seguridad de la información MSPI, favoreciendo no solo con el logro de los objetivos institucionales, sino en la generación de confianza en el uso de los mecanismos tecnológicos

2. OBJETIVO

Establecer estrategias de Seguridad de la información, delineadas con el PESI, liderada por el oficial de seguridad de la información /CISO, y supervisado por el comité de seguridad de la información y el líder del área de Tecnologías de Información – TI y, a partir de la vigencia 2024-2026 que garantice la obligación de preservar el CID (Confidencialidad, Integridad y la disponibilidad) sobre los activos de información.

3. ALCANCE

- Informar sobre las estrategias del SGSI (sistema de seguridad de la información)
- Emplear y aprovechar de manera eficiente el recurso TI, profesional, Físico y Financiero, con el fin de garantizar la continuidad de la presentación del servicio
- Establecer e implementar a propiedad, el MSPI (modelo de seguridad de la información) el cual tenga el objetivo de proteger los sistemas de información de Teveandina Canal Trece, en acceso a uso, divulgación, interrupción o destrucción no autorizada.
- Incentivar y afianzar de manera eficiente el recurso TI, profesional, Físico y Financiero, con el fin de garantizar la continuidad de la presentación del servicio

4. NORMATIVIDAD O DOCUMENTOS

CONSTITUCIÓN POLÍTICA DE COLOMBIA 1991; Artículo 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.

LEY 1266 DE 2008: por la cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia.

LEY 1474 DE 2011: Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.

LEY ESTATUTARIA 1581 DE 2012: Por la cual se dictan disposiciones generales para la protección de datos personales.

LEY 1712 DE 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

LEY 23 DE 1982: Sobre Derechos de Autor.

LEY 527 DE 1999: por medio de 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. comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

LEY 1273 DE 2009: 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 tecnologías de la información y las comunicaciones, entre otras disposiciones.

DECRETO 1008 DEL 2018: Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

DECRETO 612 DE 2018: Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.

DECRETO 4632 DE 2011: Por medio del cual se reglamenta parcialmente la Ley 1474 de 2011, en lo que se refiere a la Comisión Nacional para la Moralización y la Comisión Nacional Ciudadana para la Lucha contra la Corrupción y se dictan otras disposiciones.

DECRETO 2609 DE 2012: Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.

DECRETO 2573 DE 2014: Estrategia de Gobierno en Línea.

DECRETO 1377 DE 2013: Por el cual se reglamenta parcialmente la Ley 1581 de 2012.

CONPES 3854 de 2016. Política Nacional de Seguridad digital.

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

NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC Colombiana 27001:2013. 2013-12-11: Tecnologías de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.

5. GLOSARIO

Acceso a la Información Pública. Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados (Ley 1712 de 2014, art 4)

Archivo. Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia (Ley 594 de 2000, art 3).

Amenazas. Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización (ISO/IEC 27000).
Análisis de Riesgo. Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo (ISO/IEC 27000).

Auditoría. Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).

Ciberseguridad. Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética (CONPES 3701).

Ciberespacio. Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

Control. Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Declaración de aplicabilidad. Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información –SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001 (ISO/IEC 27000).

Gestión de incidentes de seguridad de la información. Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información (ISO/IEC 27000).

Información Pública Clasificada. Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014 (Ley 1712 de 2014, art 6).

Información Pública Reservada. Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014 (Ley 1712 de 2014, art 6)

Plan de continuidad del negocio. Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro (ISO/IEC 27000).

Plan de tratamiento de riesgos. Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma (ISO/IEC 27000).

Riesgo. Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Seguridad de la información. Preservación de la confidencialidad, integridad, y disponibilidad de la información (ISO/IEC 27000).

Sistema de Gestión de Seguridad de la Información SGSI. Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua (ISO/IEC 27000).

6. ESTRUCTURA ORGANIZACIONAL

- Gerencia
- Revisoría Fiscal - Control Interno
- Dirección Jurídica y Administrativa
- Gestión de Contenidos
- Gestión de Tecnologias Convergentes
- Comunicaciones
- Planeación Estratégica
- Gestión de Programación
- Producción
- Gestión Financiera
- Gestión de Mercadeo y Finanzas

7. ESQUEMATIZACIÓN DEL MODELO DE SEGURIDAD DE LA INFORMACIÓN

Según lo establecido en el título 9 del Decreto Único Reglamentario 1078 de 2015 del sector de Tecnologías de la información y las Comunicaciones; Teveandina Canal Trece ha estado elaborado y en la avance permanentemente del Modelo de Seguridad y Privacidad de la Información (antes, durante y después) del presente plan, bajo el respaldo y estrategia de Gobierno Digital con el fin de preservar la integridad, confidencialidad, disponibilidad, No repudio y privacidad de la información mediante la oportuna y adecuada gestión del riesgo, la aplicación de la normatividad vigente y la implementación de mejores prácticas relacionadas con seguridad de la información.

La entidad enfoca el Modelo de Seguridad y Privacidad de la Información, basado en el ciclo de mejoramiento continuo PHVA (Planear, hacer, actuar y verificar), el cual asegura y garantiza que este modelo esté expuesto a revisiones continuas cuando existe un cambio importante en la infraestructura o se requiera mejorar su efectividad dependiendo de las mediciones de parámetros claves de su operación.

Por ende, se proyecta los componentes definidos en cada ciclo o fase:

Ilustración 1: Ciclo del PHVA y Compontes de Cada Fase

8. GRUPOS DE INTERÉS

TEVEANDINA CANAL TRECE, en ejercicio a sus facultades como ente público, reconoce los grupos de interés, como el árbol fundamental para el manejo y aceptación de las buenas prácticas en seguridad de la información. Estas pueden verse directa o indirectamente influenciados, bajo las mejoras continuas del SGSI. Por consiguiente, la tabla define el interés general y su expectativa bajo el manejo responsable de estas.

GRUPOS DE INTERÉS	DESCRIPCIÓN	EXPECTATIVAS FRENTE A SEGURIDAD DE LA INFORMACIÓN
Personal Directo	Funcionarios de planta.	Los grupos de interés esperan que Teveandina Canal Trece, genere un manejo responsable de la información, en el desarrollo a su objeto, el cual contempla suministro, gestión, proceso, almacenamiento, y transferencia para el desarrollo de las actividades contractuales. Adicionalmente los grupos de interés a través de la implementación y mejora continua del Modelo de Seguridad y Privacidad de la Información, la entidad asegurará la integridad, disponibilidad y confidencialidad de la información, y el cumplimiento estricto de los requisitos legales, contractuales, regulatorios y normativos que acobija el gobierno la línea.
Contratistas	Proveedores y terceros autorizados	
Entidades Publicas	Entidades del gremio, y organismos nacionales	
Entidades Privadas	Entidades interesadas bajo las normativas y pautas del sector publico	

Tabla 1 Grupo de interés de Teveandina Canal Trece

9. ESTRATEGIA UTILIZADA

La estrategia para el desarrollo del PESI se presenta a continuación:

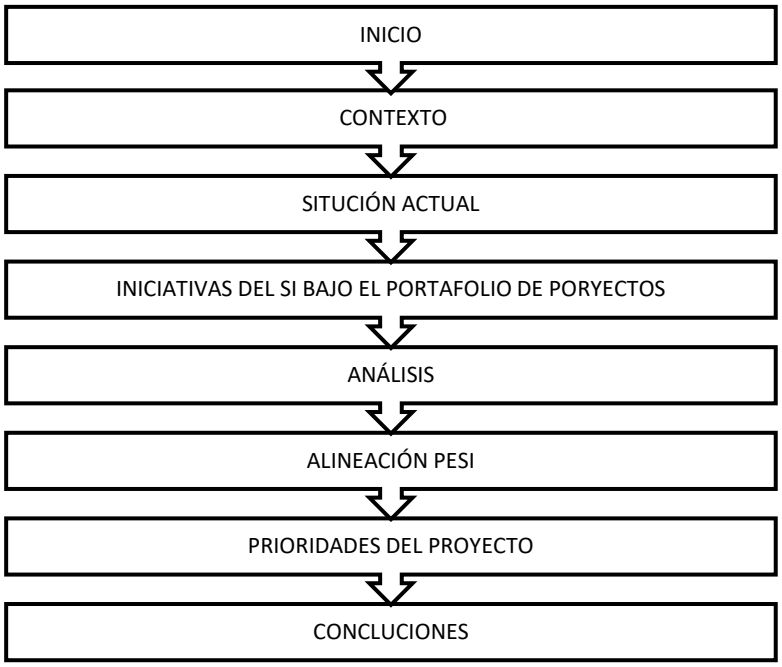

Tabla 2: Estrategia a Implementar

10. PESI-CONTEXTO

El PESI como contexto busca desarrollar una respuesta a los desafíos y riesgos asociados con la seguridad de la información tales como acceso no autorizado, robo de datos, malware, los ataques cibernéticos y las brechas de seguridad. Además, establecer un marco estratégico para favorecer los activos digitales, y el aseguramiento de la confidencialidad, integridad y disponibilidad de la información.

El contexto del PESI para Teveandina Canal Trece abarca los siguientes aspectos:

1. Tecnología y sistemas informáticos: El PESI se centra en los sistemas, redes y aplicaciones utilizadas por la organización. Esto incluye tanto los sistemas internos como los sistemas externos, como la nube y los proveedores de servicios. El contexto tecnológico evoluciona rápidamente y requiere que el PESI esté actualizado para hacer frente a las nuevas amenazas y desafíos

2. Cumplimiento normativo y regulaciones: Regulaciones y normativas específicas relacionadas con la seguridad de la información, como se cita en la normativa y documentos del literal 4 del presente documento, ya que el PESI debe tener en cuenta estos requisitos legales y asegurarse de que Teveandina Canal Trece cumpla con ellos.

3. Amenazas y riesgos: El contexto de seguridad informática incluye la identificación y evaluación de las amenazas y riesgos específicos en los planes, documentos, procedimientos encargados por el oficial de seguridad y el área TI. Amparando las amenazas internas, como el error humano o el acceso no autorizado de empleados, y en amenazas externas como los ataques cibernéticos.

4. Cultura organizacional y concienciación: La seguridad informática implica crear una cultura organizacional de seguridad y concientización a los empleados sobre las mejores prácticas de seguridad. El PESI considera la educación y el acompañamiento formativo en seguridad como el pilar más precisó para todo el personal de Teveandina Canal Trece.

5. Gestión de incidentes: El PESI bajo el portafolio de proyectos, establece un marco para la gestión de incidentes de seguridad, que incluye la detección, la respuesta y la recuperación de incidentes de seguridad. Esto implica tener procedimientos claros y una coordinación efectiva para minimizar los impactos de los incidentes y restaurar la operación normal lo antes posible.

11. DESCRIPCIÓN DEL SGSI EN TEVEANDINA CANAL TRECE

Durante los próximos dos años, se trabajará en el fortalecimiento del Sistema de Seguridad de la Información de Teveandina Canal Trece. Este proceso estará basado en el Autodiagnóstico del MSPI y en las mejores prácticas del Modelo NTC-ISO 27001:2022, que servirán como pilares fundamentales para la mejora continua y el control efectivo de la seguridad de la información.

El objetivo principal es garantizar la protección de los activos de información, alineándose con los estándares internacionales y adaptando las acciones a las necesidades específicas de la organización. La implementación de este sistema permitirá mejorar los procesos y reducir riesgos, promoviendo una cultura de seguridad en toda la entidad.

Para asegurar el éxito de este proceso, se reforzarán los controles asociados a los riesgos identificados. Esto incluirá la creación de nuevas políticas de seguridad y ajustando las actuales, planes de seguimiento, y procedimientos específicos que guiarán todas las acciones a tomar. La implementación adecuada de estos controles contribuirá a mitigar vulnerabilidades y fortalecerá la resiliencia del sistema.

Además, se contará con auditores tanto internos como externos que realizarán evaluaciones periódicas, asegurando que las acciones implementadas estén alineadas con las mejores prácticas y con la normatividad vigente. Todo este conjunto de medidas busca reflejar una proyección positiva hacia los resultados que la entidad aspira alcanzar, mejorando su competitividad y garantizando la seguridad de la información a largo plazo.

12. PORYECCIÓN PESI.

Como proyección se espera un cumplimiento de los controles establecidos. Este resultado marca un inicio positivo en el proceso de fortalecimiento de los sistemas de seguridad de la información, reflejando el compromiso de la organización por alinearse con los estándares y mejores prácticas recomendadas en el sector.

Con miras al futuro, se proyecta que para el año 2026 se logre un cumplimiento total, lo que representará un avance significativo en la consolidación de un sistema de seguridad más robusto. Este incremento en el cumplimiento no solo garantizará una mayor protección de los activos de información, sino que también optimizará la eficiencia en la gestión de la seguridad, alineándose completamente con las mejores prácticas internacionales y la normatividad vigente.

13. PORTAFOLIO DE PROYECTOS SEGURIDAD DE LA INFORMACIÓN

El portafolio de proyectos define una estrategia clara del PESI, donde agrupa las iniciativas para encaminar cada propósito. La siguiente tabla muestra esos proyectos que pueden ejecutarse a corto y a largo plazo, según la prioridad específica.

N° del Proyecto	Nombre del Proyecto	Iniciativa	Descripción de Iniciativas
P.0	RNBD	I.01	Revisar las cláusulas de protección de datos para personal interno y externo.
		I.02	Realizar la capacitación interna acerca del RNBD
P.1	EVALUACIÓN DE RIESGOS	I.03	Actualizar la identificación y evaluación de los controles
		I.04	Elaborar el Informe con la evaluación y medición de la efectividad de la implementación de los controles definidos en el plan de tratamiento de riesgos.
		I.05	Construir el Inventario de datos de contacto de los responsables definidos.
		I.06	Construir el procedimiento de inventario y clasificación de la Información e infraestructura crítica.
P.2	RECUPERACIÓN Y DESASTRES	I.07	Actualizar el centro de crisis
		I.08	Construir los escenarios en operación normal DRP o EDRP
		I.09	Definir el set de pruebas a ejecutar la evaluación del DRP o EDRP
		I.10	Definición de los servicios de Comunicaciones de respaldo
		I.11	Revisar que las hojas de vida de los componentes que están en operación se encuentren actualizados
		I.12	Actualizar la lista de contactos para activación del DRP o EDRP y el retorno operacional
		I.13	Construir el procedimiento del DRP o EDRP
P.3	CAPACITACIÓN	I.14	Aplicar el diagnostico a través de encuesta para conocer el estado de conocimientos y percepción de en temas de seguridad de la información
		I.15	Elegir el temario de capacitaciones
		I.16	Priorizar los temas de capacitación
		I.17	Elaborar el programa de capacitación
		I.18	Presentar el plan de capacitación
		I.19	Ejecutar el programa de capacitación
		I.20	Evaluar el plan de capacitación
		I.21	Presentar el informe con el resultado de la ejecución del plan de capacitaciones a los lideres de proceso
		I.22	Formulación de las acciones de mejora y propuesta de nuevas temáticas
P.4	CONTINGENCIA	I.23	Identificar los procesos críticos

		I.24	Actualizar las consideraciones especiales para el funcionamiento de la infraestructura
		I.25	Presentar una propuesta de implementación de failover cluster en los servidores de producción incluyendo Emisión, Catalogación y postproducción.
		I.26	Revisar la estrategia y procedimientos de backup definida por el área de TI y Emisión
		I.27	Revisar que se encuentre actualizado procedimiento de actualizaciones en sistemas de información de producción
		I.28	Construir los escenarios de pruebas tanto de operación como de retorno operacional
		I.29	Definición del centro de crisis para plan de contingencia
		I.30	Definición de recursos para operar en modo de contingencia
		I.31	Construir el procedimiento de contingencias.
P.5	CIBERSEGURIDAD	I.32	Diseñar e implementar buenas prácticas en ciberseguridad para el refuerzo de la seguridad de la red.
		I.33	Construir procedimiento para la actualización trimestral de parches de seguridad infraestructura y pc de postproducción
		I.34	Revisar la Activación de controles contra el malware
		I.35	Realizar la revisión anual de los niveles de privilegio de los usuarios a los diferentes Sistemas
		I.36	Construir procedimiento de atención a incidentes en ciberseguridad
		I.37	Actualizar procedimiento para trabajo en casa, Coworking y teletrabajo, aplicando buenas prácticas consignadas en estándares
		I.38	Construir una propuesta para ejecución de un análisis de vulnerabilidades y pruebas de ETHICAL HACKING
P.6	ARQUITECTURA TI	I.39	autodiagnóstico de arquitectura de seguridad de la información
		I.40	Planeación de implementación de arquitectura de seguridad de la información
		I.41	Formular las acciones de mejora sobre la arquitectura de seguridad de la información

Tabla 3: Portafolio de Proyectos SI

14. INFORME DE RESULTADOS

14.1 PRIORIZACIÓN DEL PORTAFOLIO DE PROYECTOS

Definidas las iniciativas con sus respectivos proyectos, y basándonos en las Proyecciones del autodiagnóstico del modelo de seguridad y privacidad de la información (MSPI). Es ineludible priorizar los proyectos que se deben desarrollar en el corto, mediano y largo plazo. Se tiene en cuenta para ello y a nivel gobierno, el modelo de seguridad de información con su nueva vigencia, la gestión de riesgos de seguridad, y la gestión de incidentes de seguridad de la información indicados por MINTIC. Para ello se describen las siguientes categorías de prioridad que permiten evaluar y determinar una orden sistemática para el desarrollo del (PESI):

PRIORIDAD	DESCRIPCIÓN
0	Ciberseguridad: Elaboración de medidas para proteger los sistemas informáticos, redes, dispositivos, datos de amenazas y ataques cibernéticos. Apoyados con un conjunto de técnicas, herramientas y políticas diseñadas para salvaguardar la confidencialidad, integridad y disponibilidad de la información en entornos digitales.
1	Contingencia: Centralizar la planificación y preparación para hacer frente a incidentes de seguridad, así como en la recuperación después de que ocurra un incidente, priorizando actividades clave en el contexto de la contingencia de seguridad de la información.
2	Recuperación y Desastre: Planificar e implementar medidas para restaurar la operatividad de los sistemas y la infraestructura tecnológica después de un evento catastrófico, bajo actividades clave en el contexto de la recuperación y los desastres en seguridad de la información. Estas actividades de recuperación y desastres en seguridad de la información son esenciales para minimizar los tiempos de inactividad, mitigar los impactos y garantizar la continuidad del negocio en caso de un evento adverso.
3	Evaluación de riesgo: Continuar con la identificación y evaluación de los posibles riesgos y amenazas que pueden afectar la confidencialidad, integridad y disponibilidad de los activos de información. La evaluación del riesgo en seguridad de la información será un proceso continuo y dinámico que permitirá comprender y abordar las amenazas y vulnerabilidades. Al llevar a cabo estas actividades, se podrán tomar decisiones, informar y establecer medidas de seguridad más efectivas y proteger los activos de información.
4	Capacitación: Teveandina Canal Trece, tiene como fundamento estratégico, promover la concientización y el conocimiento de las mejores prácticas de seguridad entre los empleados, contratista y terceros. Para ello se fortalecerá el desarrollo de capacitaciones, sesiones de capacitación interactivas, simuladores de phishing, acompañamiento continuo a todas las áreas, y la promoción cultural organizacional.
5	Arquitectura TI: Reforzar y continuar el diseño e implementación de la actual infraestructura de seguridad, la cual garantice la protección adecuada de los activos de información, manteniendo la infraestructura tecnológica robusta, segura, con los controles adecuados, las mejores prácticas de seguridad, y la protección eficazmente de activos de información mitigando los riesgos de seguridad

Tabla 4: Criterios de Priorización de Proyectos

A continuación, se presenta por prioridad los proyectos que se deben desarrollar a partir de la vigencia 2024 y hasta la vigencia 2026, sujeto a cambios.

N° del Proyecto	Nombre del Proyecto	Prioridad (0) AÑO 1	Prioridad (1) AÑO 2
P.0	RNBD	**x**	**x**
P.1	EVALUACIÓN DE RIESGOS	**x**	**x**
P.2	RECUPERACIÓN Y DESASTRES		**x**
P.3	CAPACITACIÓN	**x**	**x**
P.4	CONTINGENCIA		**x**
P.5	CIBERSEGURIDAD	**x**	
P.6	ARQUITECTURA TI		**x**

Tabla 5: Prioridad de Proyectos

15. PLAN ESTRATÉGICO SEGURIDAD DE LA INFORMACIÓN

Nombre del Proyecto	Iniciativa	Descripción de Iniciativas		
RNBD	I.01	Revisar las cláusulas de protección de datos para personal interno y externo.	AÑO 1	AÑO 2
	I.02	Realizar la capacitación interna acerca del RNBD		
EVALUACIÓN DE RIESGOS	I.03	Actualizar la identificación y evaluación de los controles		
	I.04	Elaborar el Informe con la evaluación y medición de la efectividad de la implementación de los controles definidos en el plan de tratamiento de riesgos.		
	I.05	Construir el Inventario de datos de contacto de los responsables definidos.		
	I.06	Construir el procedimiento de inventario y clasificación de la Información e infraestructura crítica.		
CAPACITACIÓN	I.14	Aplicar el diagnostico a través de encuesta para conocer el estado de conocimientos y percepción de en temas de seguridad de la información		
	I.15	Elegir el temario de capacitaciones		
	I.16	Priorizar los temas de capacitación		
	I.17	Elaborar el programa de capacitación		
	I.18	Presentar el plan de capacitación		
	I.19	Ejecutar el programa de capacitación		
	I.20	Evaluar el plan de capacitación		
	I.21	Presentar el informe con el resultado de la ejecución del plan de capacitaciones a los lideres de proceso		

Tabla 6: Plan Estratégico de SGSI

	I.22	Formulación de las acciones de mejora y propuesta de nuevas temáticas	AÑO 1	
CIBERSEGURIDAD	I.32	Diseñar e implementar buenas prácticas en ciberseguridad para el refuerzo de la seguridad de la red.		
	I.33	Construir procedimiento para la actualización trimestral de parches de seguridad infraestructura y pc de postproducción		
	I.34	Revisar la Activación de controles contra el malware		
	I.35	Realizar la revisión anual de los niveles de privilegio de los usuarios a los diferentes Sistemas		
	I.36	Construir procedimiento de atención a incidentes en ciberseguridad		
	I.37	Actualizar procedimiento para trabajo en casa, Coworking y teletrabajo, aplicando buenas prácticas consignadas en estándares		
	I.38	Construir una propuesta para ejecución de un análisis de vulnerabilidades y pruebas de ETHICAL HACKING		
RECUPERACIÓN Y DESASTRES	I.07	Actualizar el centro de crisis		AÑO 2
	I.08	Construir los escenarios en operación normal DRP o EDRP		
	I.09	Definir el set de pruebas a ejecutar la evaluación del DRP o EDRP		
	I.10	Definición de los servicios de Comunicaciones de respaldo		
	I.11	Revisar que las hojas de vida de los componentes que están en operación se encuentren actualizados		
	I.12	Actualizar la lista de contactos para activación del DRP o EDRP y el retorno operacional		
	I.13	Construir el procedimiento del DRP o EDRP		
CONTINGENCIA	I.23	Identificar los procesos críticos		

	I.24	Actualizar las consideraciones especiales para el funcionamiento de la infraestructura	AÑO 2
	I.25	Presentar una propuesta de implementación de failover cluster en los servidores de producción incluyendo Emisión, Catalogación y postproducción.	
	I.26	Revisar la estrategia y procedimientos de backup definida por el área de TI y Emisión	
	I.27	Revisar que se encuentre actualizado procedimiento de actualizaciones en sistemas de información de producción	
	I.28	Construir los escenarios de pruebas tanto de operación como de retorno operacional	
	I.29	Definición del centro de crisis para plan de contingencia	
	I.30	Definición de recursos para operar en modo de contingencia	
	I.31	Construir el procedimiento de contingencias.	
ARQUITECTURA TI	I.39	autodiagnóstico de arquitectura de seguridad de la información	
	I.40	Planeación de implementación de arquitectura de seguridad de la información	
	I.41	Formular las acciones de mejora sobre la arquitectura de seguridad de la información	

16. CONCLUSIONES

La construcción del Plan Estratégico de Seguridad de la Información (PESI) es un componente fundamental para garantizar la protección de la información sensible y crítica dentro de TEVEANDINA CANAL TRECE. A través de un enfoque sistemático y estructurado buscando identificar y mitigar los riesgos asociados con la seguridad de la información, establecer controles nuevos y adecuados, promoviendo una cultura de seguridad en todos los niveles de Teveandina Canal Trece.

Al desarrollar el PESI, es crucial continuar con el análisis exhaustivo de los activos de información, evaluando las amenazas y vulnerabilidades existentes, y determinar el impacto potencial de una brecha de seguridad. A partir de esta evaluación, se pueden fortalecer los objetivos y metas para la seguridad de la información, así como establecer las nuevas políticas, procedimientos y controles necesarios para alcanzar esos objetivos.

El documento considera la implementación de tecnologías de seguridad adecuadas bajo el portafolio de proyectos, como firewalls, sistemas de detección de intrusiones, cifrado de datos y autenticación de usuarios. Además, la capacitación y concientización a todo el personal sobre las mejores prácticas de seguridad, fomentando una cultura de responsabilidad compartida fuera y dentro de la entidad.

Una vez implementado, el PESI como conjunto, debe ser constantemente evaluado, actualizado y mejorado para adaptarse a los cambios tecnológicos, las nuevas amenazas y los requisitos regulatorios. La seguridad de la información no es un objetivo estático, sino un proceso continuo que requiere atención constante.

En sinopsis, el Plan Estratégico de Seguridad de la Información es esencial para proteger los activos de información valiosos. Al adoptar un enfoque holístico y proactivo para la seguridad de la información. TEVEANDINA CANAL TRECE, está en la capacidad humana, Física y técnica para poder mitigar los riesgos, fortalecer sus defensas y mantener la confianza de los clientes y socios comerciales, diseñado y ejecutado es un componente vital para garantizar la continuidad del negocio y proteger la reputación de la organización en un entorno cada vez más digital y amenazante.