PLAN INTEGRAL Y TRATAMIENTO DE RIESGOS EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Teveandina S.A.S.– Canal Trece

Revisiones y control de cambios

Titulo	**Plan Integral de tratamiento de riesgos en seguridad y privacidad de la información Teveandina Ltda. Canal Trece**
Autores	Wilmar López – Andrés Beltran
Tema	Plan Integral de riesgos para la gestión de activos de información y el tratamiento de riesgos en seguridad y privacidad sobre estos.
Fecha de Elaboración	Julio 2018
Formato	PDF
Versión	1.0
Palabras Relacionadas	Seguridad de la información, privacidad de la información, tratamiento de riesgos, vulnerabilidades, controles, activos de información

Control de Cambios			
Fecha	**Autores**	**Versión**	**Cambio**
Abril 2024	Camilo Beltrán – Wilmar López	2.0	Este documento Contempla V1.2 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 una actualización de contenido bajo cumplimiento con la normatividad vigente.

TABLA DE CONTENIDO

TABLA DE ILUSTRACIÓN

ÍNDICE DE TABLAS

1. INTRODUCCIÓN

Este plan sobre la gestión integral del riesgo se basa en la protección de datos, minimizando vulnerabilidades frente a diversas amenazas provocadas por la falta de gestión, control e implementación de estrategias que permitan contrarrestar estos fenómenos, tal y como se define en el marco de referencia que dirige MINTIC. como base aplicaremos la norma ISO27001:2023 y estándares que nos ayudan a reducir el riesgo mediante la adopción de mejores prácticas durante la ejecución de procesos se han convertido en un actor importante en la industria, por lo que su implementación en los últimos años se ha convertido en una necesidad para las organizaciones que quieren TI para administrar adecuadamente su información y obtener beneficios al reducir al mínimo la vulnerabilidad de la información.

2. TABLA CRITERIOS PARA DEFINIR EL NIVEL DE PROBABILIDAD

	Frecuencia de la Actividad	**Probabilidad**
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

Tabla 1:Criterios de Clasificación

3. PRESENTACIÓN

La gestión de riesgos en seguridad y privacidad de la información hace referencia a la reducción de pérdidas y protección sobre la información, con el fin de conocer las debilidades que son susceptibles a ser identificadas sobre servicios, sistemas y herramientas tecnológicas.

El siguiente plan se elabora para dar a conocer la forma como serán tratados los aspectos sobre el tratamiento de riesgos en seguridad y privacidad de la información en la Entidad, conforme a lo establecido en estándares como ISO 27002, ISO 31000, así como metodologías, buenas prácticas y guías suministradas por MINTIC como parte del cumplimiento de la política de gobierno digital.

4. 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).

5. OBJETIVO

Definir y orientar las actividades concernientes para el tratamiento de los riesgos en seguridad y privacidad de la información para TEVEANDINA S.A.S. – CANAL TRECE. Gestionar los riesgos de seguridad de la información con base en criterios de seguridad (confidencialidad, integridad, acceso) que buscan la integración el plan de tratamiento de riesgos

6. ALCANCE

El siguiente plan será definido e implementado por funcionarios, contratistas y practicantes de acuerdo con lo designado por la alta gerencia en las instalaciones de la Entidad, de acuerdo con los recursos asignados para tal efecto, el nivel de aplicabilidad incluye actores internos y externos que interactúen con la información producida y gestionada por el Canal.

7. MARCO REFERENCIAL

7.1 POLITICA DE ADMINISTRACIÓN DE RIESGOS

TEVEANDINA S.A.S. – CANAL TRECE a través del plan integral y tratamiento de riesgos en seguridad y privacidad de la información, se compromete a fomentar una cultura de gestión del riesgo que refuerce las acciones preventivas, de monitoreo y seguimiento, con el fin de minimizar los riesgos asociados a las actividades de la entidad. Estas acciones están vinculadas a su responsabilidad de diseñar, adoptar, implementar y promover políticas, planes, programas, iniciativas y proyectos en el ámbito de las Tecnologías de la Información y las Comunicaciones (TIC). Para ello, se emplean mecanismos, sistemas y controles que permitan identificar, de manera integral, aspectos relacionados con la estrategia, la gestión, la transparencia, la ética, la seguridad y privacidad de la información, la seguridad digital, la continuidad operativa, que puedan afectar el cumplimiento de los objetivos institucionales, la utilización eficiente de los recursos y la atención de los grupos de interés.

El objetivo principal de esta política es establecer las pautas necesarias para gestionar adecuadamente los riesgos asociados a la seguridad y privacidad de la información, la seguridad digital y la continuidad de los servicios (en cuanto a riesgos de interrupción) dentro de TEVEANDINA S.A.S. – CANAL TRECE. El fin es evitar que estos riesgos se materialicen, siguiendo las directrices de la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas del DAFP. Esto facilitará la toma de decisiones oportunas y minimizará los impactos negativos dentro de la entidad, garantizando así la continuidad de la gestión institucional y el cumplimiento de los compromisos con los grupos de interés.

La gestión de riesgos recae en la primera línea de defensa, es decir, en los líderes o responsables de cada proceso junto con sus respectivos equipos de trabajo, quienes

deben aplicar medidas para mitigar los diversos riesgos. Las respuestas a los riesgos se clasifican en las siguientes categorías (*literal 12 Enfoque de Planificación y mitigación*).

La gestión de riesgos en Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad Operativa de los servicios (riesgos de interrupción) permite a TEVEANDINA S.A.S. – CANAL TRECE., evaluar y manejar los riesgos que podrían impactar el cumplimiento de los objetivos de sus procesos. Esto facilita una toma de decisiones más informada y contribuye a prevenir la materialización de esos riesgos. El enfoque de este plan se centra en identificar, analizar y abordar las amenazas y vulnerabilidades que afectan los activos de información de la entidad, considerando su criticidad y la necesidad de protección. Las diferentes etapas del proceso de gestión de riesgos están alineadas con los objetivos, estrategias y políticas corporativas, lo que permite a la Alta Dirección en asesoría con el comité de seguridad, definir un nivel de riesgo que pueda ser aceptado o asumido.

8. ACTIVIDADES

- **Diagnóstico**: Permite conocer el estado actual de la Entidad y grado de madurez en el tratamiento de riesgos en seguridad de la información sobre todos los activos que tengan relación con este. Su resultado determina las acciones posteriores para la implementación del plan.

- **Activos de Información**: Debe ser documentado un inventario sobre los activos de información presentes en los procesos de la Entidad, como insumo se utiliza el mapa de procesos, inventario de sistemas de información, catálogo de servicios tecnológicos y demás que permitan visualizar flujos de información dentro de la Entidad.

- **Vulnerabilidades y amenazas**: Con base en la actividad anterior, sobre los activos de información deben ser evidenciadas sus principales vulnerabilidades y amenazas sobre variables relacionadas con su protección a nivel interno y externo, documentadas en una matriz.

- **Metodología para la evaluación de riesgos**: Debe ser definida una metodología para el tratamiento de riesgos en seguridad de la información tomando como referencia estándares como ISO 27002, ISO 31000 la metodología para el tratamiento de riesgos MAGERIT, metodología para el tratamiento de riesgos de DAFP, entre otras.

- **Evaluación de riesgos:** Se establece una ponderación de los riesgos de acuerdo con su nivel de impacto e incidencia dentro de la Entidad y se evalúa sobre los activos de información, tomando como base la matriz de vulnerabilidades y amenazas con el fin de materializarlos y ponderarlos como riesgos que afecten el logro de los objetivos estratégicos del Canal. La matriz de riesgos lleva al establecimiento de controles.

- **Diseño de Controles:** Se diseñan e implementan controles de acuerdo con los riesgos definidos en la fase anterior con el fin de ser mitigados a partir del uso de recursos humanos, tecnológicos o físicos.

- **Políticas específicas en seguridad de la información**: Como parte de la aplicación del MSPI, la Entidad debe documentar políticas de seguridad de la información como una forma de establecer las condiciones generales que permitirán a través de controles, mitigar riesgos sobre los activos relacionados.

- **Plan de capacitación y comunicaciones:** La Entidad define en conjunto con los actores pertinentes el plan de sensibilización, comunicación y capacitación, sobre la gestión de riesgos en seguridad y privacidad de la información. De igual forma deben ser definidas las condiciones para el proceso de mejora continua sobre la implementación del plan.

9. RECURSOS

Humanos	* Profesional en gestión de riesgos del Grupo Interno de Trabajo. * Líderes de área y gestores de procesos. * Responsable de la seguridad informática en la Oficina de TI. * Especialista en respuesta ante emergencias cibernéticas en Colombia (COLCERT). * Profesional en Seguridad y Privacidad de la Información en la Dirección de Gobierno Digital.
Técnicos	Guía para la gestión del riesgo y diseño de controles en entidades públicas. Enfocada en riesgos de gestión, corrupción y seguridad digital, según el DAFP Herramienta para la gestión de riesgos: Matriz de Riesgos SGSI.
Lógicos	Gestión de recursos para la socialización, transferencia de conocimientos y seguimiento de la gestión de riesgos.
Financieros	Recursos para la adquisición de conocimientos, personal técnico y el desarrollo de auditorías en el sistema de Seguridad y Privacidad de la Información. Con un coste definido mediante el análisis y requisitos del proyecto

10. ETAPAS DE GESTIÓN DEL RIESGO

EL presente plan integra etapas generales para la gestión del riesgo a partir de las cuales se soportan cada una de las actividades que permiten a TEVEANDINA S.A.S. – CANAL TRECE tener una administración de riesgos acorde con las necesidades de la entidad.

Lo más importante para conseguir un adecuado avance en todo el proceso de administración del riesgo es el "Compromiso de las alta y media dirección" puesto que al igual que como se menciona en la estructura del plan, tener el verdadero compromiso de TEVEANDINA S.A.S. – CANAL TRECE, garantizando en gran medida el éxito de cualquier proceso emprendido, puesto que se necesita su aprobación y concurso en el momento de cualquier toma de decisiones, así mismo como se menciona en el MSPI la necesidad de tener aprobación de la dirección en cada etapa es necesaria.

Así mismo en concordancia con lo estipulado en el presente plan, "debe designar el mecanismo que conforme todos los niveles de riesgo y apalanque todo el proceso de diseño e implementación que aquí se indica. Adicionalmente tomar la medida que estipula el MSPI el cual acoge y busca lograr una gestión integral del riesgo estandarizada.

En segundo lugar se encuentra la "Conformación de un grupo de controles y objetivos con apoyo de un grupo interdisciplinario", la idea es una integralidad en el tratamiento de los riesgos para poder tener una visión completa sobre TEVEANDINA S.A.S. – CANAL TRECE,y en la cual se pueda tener el aporte de diferentes áreas analizando un mismo proceso, es esencial y ayuda a encaminar correctamente el MSPI, es por esta razón que se deben incluir los riesgos de seguridad en el momento que se hace el análisis, o para el modelo de Gestión de Calidad.

Finalmente se encuentra el "Aprendizaje en la metodología", este punto es un poco más profundo, porque es claro que el equipo interdisciplinario debe capacitarse para poder analizar ahora los riesgos de seguridad, sin embargo, dicho equipo debe estar integrado por alguno de los integrantes del MSPI, para tener un contexto Organizacional en todos los aspectos del desarrollo.

11. ENFOQUE GENERAL PARA EL RIESGO DE SEGURIDAD DE LA INFORMACIÓN

Como se argumenta en el plan de riesgo de seguridad de la información, consta de una definición y enfoque de tipo organizacional, para la valoración del riesgo y su tratamiento

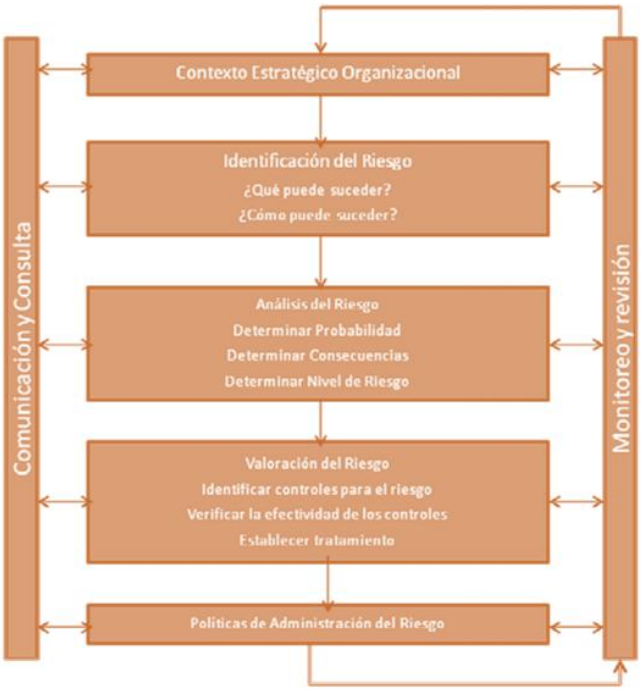

Ilustración 1 Citado de la Cartilla de Administración de Riesgos

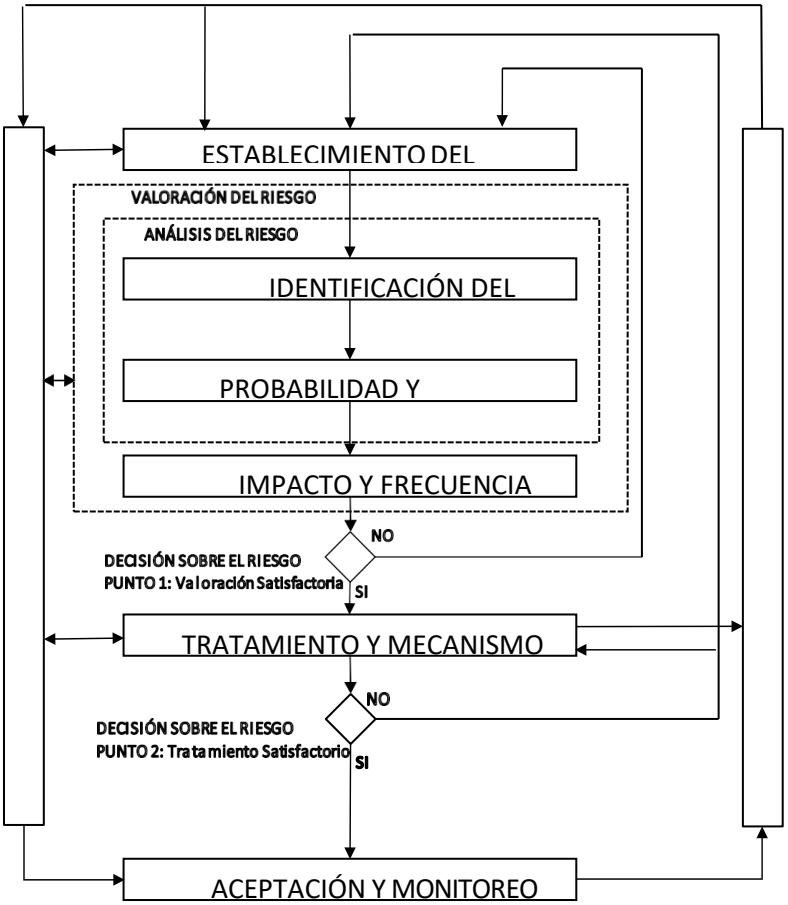

Ilustración 2: Proceso de Administración del Riesgos

La ilustración 2, nos entrega el proceso de gestión del riesgo en la seguridad de la información como un mapa de flujo, donde se nos muestra un iterativo para las actividades de valoración del riesgo y/o el tratamiento de este. Un enfoque transversal para realizar la valoración del riesgo puede ser incremental a profundidad y a detalle de la valoración en cada iteración.

En contexto se establece como primera medida, luego se realiza la valoración del riesgo y si esta suministra información suficiente para determinar de manera eficaz las acciones que se necesitan para modificar los riesgos a un nivel aceptable entonces la labor está terminada y sigue el tratamiento del riesgo. Si la información no es suficiente, se llevará a cabo otra iteración de la valoración del riego con un contexto revisado.

La eficacia del tratamiento de tratamiento del riesgo depende de los resultados de la valoración del riesgo. El tratamiento del riesgo en esta situación puede resultar inmediatamente en un riesgo residual inaceptable, y puede ser necesaria una mayor iteración de la evaluación del riesgo con cambios en los parámetros contextuales

Las actividades de aceptación de riesgos deben asegurar que los riesgos residuales sean claramente aceptados por los directores TEVEANDINA S.A.S. – CANAL TRECE. Esto es especialmente importante si las pruebas no se realizan o se retrasan, por ejemplo, por motivos de costes.

ETAPAS DEL MSPI	PROCESO DE GESTION DEL RIESGO EN LA SEGURIDADDE LA INFORMACION
Planear	Establecer Contexto Valoración del Riesgo
	Planificación del Tratamiento del Riesgo Aceptación del Riesgo
Implementar	Implementación del Plan de Tratamiento de Riesgo
Gestionar	Monitoreo y Revisión Continuo de los Riesgos
Mejora Continua	Mantener y Mejorar el Proceso de Gestión del Riesgo en la
	Seguridad de la Información.

Ilustración 3: Etapas de la gestión del Riesgo

Las etapas son comprendidas y ejecutadas por el PHBA, contemplando las buenas prácticas para una gestión del riesgo, y de la forma más indicada de abordarlas. Ya que se desprende de las fases del proceso MPSI.

12. ENFOQUES DE PLANIFICACIÓN Y MITIGACIÓN

TEVEANDINA S.A.S. – CANAL TRECE define los enfoques principales para tratar el riesgo.

12.1 PROBABILIDAD Y EVALUACIÓN DE RIESGOS:

Desarrollar criterios de probabilidad y evaluación del riesgo para determinar el riesgo de seguridad de la información de la organización, teniendo en cuenta los siguientes aspectos:

- El valor estratégico del proceso de información para el sujeto.
- Importancia de la información Activos involucrados en el proceso
- Requisitos legales y reglamentarios y obligaciones contractuales
- Importancia del acceso, confidencialidad e integridad de la información para las operaciones y la empresa.
- Expectativas y percepciones de los grupos de interés e impacto negativo en el nombre y la reputación de la empresa.
- De manera similar, los criterios de evaluación del impacto del riesgo se pueden utilizar para determinar las prioridades para la gestión del riesgo.

12.2 IMPACTO Y FRECUENCIA DE RIESGOS:

Se determina desarrollar criterios de impacto y frecuencia del riesgo y especificarlos en términos de la magnitud de los daños o costos a la entidad causados por un evento de seguridad de la información, teniendo en cuenta los siguientes aspectos:

- Nivel grado de clasificación de los activos de información del proceso
- Información brechas de seguridad (por ejemplo, pérdida de confidencialidad, integridad y disponibilidad)
- Operaciones alteradas
- Pérdida de valor comercial y financiero
- Modificaciones de planes y plazos
- Daño a la reputación
- Incumplimiento de requisitos legales.

12.3 ACEPTACIÓN DEL RIESGO

El plan contempla mejorar los criterios específicos con respecto a la aceptación de riesgos los riesgos. los cuales dependerán de la mejora continua de políticas, metas, objetivos de la organización y de las partes interesadas

TEVEANDINA S.A.S. – CANAL TRECE adaptara los niveles de aceptación del riesgo. Durante el desarrollo, se deberían considerar los siguientes aspectos:

• Los criterios de aceptación del riesgo pueden incluir umbrales múltiples, con una meta de nivel de riesgo deseable, pero con disposiciones para que la alta dirección acepte los riesgos por encima de este nivel, en circunstancias definidas

• Los criterios de aceptación del riesgo se pueden expresar como la relación entre el beneficio estimado (u otros beneficios del negocio) y el riesgo estimado

• Los diferentes criterios de aceptación del riesgo pueden aplicar a diferentes clases de riesgos, por ejemplo, los riesgos que podrían resultar en incumplimiento con reglamentos o leyes podrían no ser aceptados, aunque se puede permitir la aceptación de riesgos altos si esto se especifica como un requisito contractual

• 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.

Los criterios de aceptación del riesgo pueden diferir de acuerdo con la expectativa de duración que se tenga del riesgo y se podrían considerar los siguientes elementos:

- Criterios del negocio
- Aspectos legales y reglamentarios
- Operaciones
- Tecnología
- Finanzas
- Factores sociales y humanitarios

12.4 EVITACIÓN DEL RIESGO

Se define primero la identificación de los riesgos asumidos y aceptados, seguidamente generación de doctrinas para evitarlos. Las acciones tomadas en esta estrategia incluyen la planificación de riesgos para obtener un dibujo claro del mejor curso de acción para evitar consecuencias y desaprobaciones.

- **Programación de riesgos:** identifique los problemas clave que pueden afectar el progreso del proyecto. Los plazos de entrega de servicios o bienes pueden verse afectados si el cronograma corre el riesgo de ser demasiado optimista. Las estrategias de evitación se pueden usar para crear cronogramas más flexibles para respaldar las fases de planificación, prueba y cambio potencial, reduciendo el riesgo de cambios potenciales.

- **Riesgo de costo:** los equipos pueden determinar el costo esperado de un proyecto y contabilizar todos los demás costos posibles como costos esperados. Todos los gastos se pueden incluir en el presupuesto inicial para evitar gastos excesivos.

- **Riesgos de rendimiento:** lidiar con dinámicas de equipo incómodas con recursos insuficientes o inadecuados para completar las tareas plantea riesgos de rendimiento. Puede experimentar con materiales de calidad y confiar en la gestión interactiva del equipo.

12.5 CONTROL DEL RIESGO

Al reducir el riesgo dentro de un proyecto, los miembros de TEVEANDINA S.A.S. – CANAL TRECE, pueden implementar estrategias de control. Esto incluye evaluar los riesgos identificados y tomar medidas para minimizar o evitar posibles impactos adversos. Concéntrese en las consecuencias y en cómo batallar con ellas, en lugar de evitar o aceptar los riesgos por completo.

- **Planifique la gestión de riesgos:** diversifique las tareas y garantice la flexibilidad de tiempo para completar subtareas y proyectos relacionados. Esto incluye el seguimiento del tiempo dedicado a cada tarea y la asignación de roles apropiados a cada miembro del equipo. Una estrategia de gestión del tiempo es una forma importante de controlar el riesgo del cronograma.

- **Gestione el riesgo de costes:** al identificar posibles problemas de presupuesto del proyecto, TEVEANDINA S.A.S. – CANAL TRECE, puede gestionar el riesgo de costes. Centrarse en la toma de decisiones y la gestión o evaluación de las fuentes de financiación para las vulnerabilidades. La composición del financiamiento es un tema clave aquí, especialmente con respecto a la capacidad de volver a priorizar el gasto y eliminar recursos costosos.

- **Controles de riesgo de desempeño:** esta estrategia se enfoca en cómo se dirige y administra el trabajo del grupo, cómo se administra la calidad del producto y otras medidas para controlar la degradación del riesgo de desempeño.

12.6 TRANSFERENCIA DEL RIESGO

La mitigación de riesgos implica que, aunque los riesgos sean inminentes, se tomen medidas. Esta estrategia funciona transfiriendo el impacto de las consecuencias a la otra parte. La forma más común de transferencia de riesgos seguro, en el que TEVEANDINA S.A.S. – CANAL TRECE, podrá pagar a un tercero la protección de pérdidas futuros impactos.

- **Delegación de programación:** Se utiliza para transferir la responsabilidad de los los miembros de TEVEANDINA S.A.S. – CANAL TRECE, y del equipo apropiado asignado por el canal. Dado que los departamentos individuales, como los equipos de programación, producción y diseño son responsables de sus plazos individuales, el resto del equipo puede concentrarse únicamente en sus tareas.

- **Costo de propiedad:** esto puede incluir la responsabilidad del contador, el equipo de finanzas o el consultor por los problemas que surjan durante la

preparación del presupuesto. Por ejemplo, cuando se discute un presupuesto, son los equipos de finanzas responsables del seguimiento de los costos los que abordan el problema, no todo el equipo del proyecto.

- **Entrega de rendimiento:** los problemas de rendimiento del producto pueden ser causados por los materiales comprados y no solo por los métodos de fabricación. En este caso, la empresa fabricante puede asumir las consecuencias y tomar medidas como un aviso de retirada del producto. Por el contrario, es posible culpar al proveedor responsable de suministrar las materias primas de TEVEANDINA S.A.S. – CANAL TRECE.

12.7 MECANISMO DE MONITOREO

TEVEANDINA S.A.S. – CANAL TRECE, el mecanismo de monitoreo de riesgos Los proyectos y actividades de monitoreo de amenazas y consecuencias involucran la evaluación de cualquier desarrollo que pueda afectar el impacto del riesgo. Evaluar el desempeño de un proyecto o actividad a medida que comienza para permitir una respuesta en tiempo real para mitigar el riesgo y requiere saber cómo cada cambio puede afectar la probabilidad de que ocurra un riesgo potencial.

- **Seguimiento de la programación:** para el cumplimiento de la programación, se establece actividades y actualizaciones cada trimestre del año, semanales con el fin de medir el rendimiento de todas las áreas involucradas, y el tiempo de finalización de la tarea. Esto permite reevaluar el cronograma en tiempo real, y proceder con los cambios necesarios para cumplir con los plazos.

- **Supervisión del rendimiento:** TEVEANDINA S.A.S. – CANAL TRECE debe realizar un seguimiento del rendimiento de los miembros de las aras encargadas monitorizadas, sus recursos y los productos para evaluar, para determinar la mejora continua con el fin de lograr resultados de calidad.

13. ANEXOS