telecafé

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y **PRIVACIDAD DE LA INFORMACIÓN**

www.telecafe.gov.co
@canaltelecafe
@telecafetv

Código: TEI-PRO-23
Fecha: 25 de agosto de 2025
Versión: 01
Sistema Integrado de Gestión

telecafé

CONTENIDO

1. Introducción

El presente Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de Telecafé tiene como propósito establecer un marco claro y estructurado que oriente la gestión de los riesgos relacionados con la seguridad de la información, la protección de los datos personales y la continuidad de los servicios misionales de la entidad. Este plan se fundamenta en un enfoque preventivo y proactivo, orientado a anticipar, identificar, valorar y mitigar las amenazas que puedan comprometer la operación tecnológica y administrativa, minimizando así los impactos sobre la organización y sus grupos de interés.

En Telecafé, la gestión de riesgos no se concibe como una acción aislada, sino como un componente estratégico y transversal que se articula con la planeación institucional, los procesos operativos y el cumplimiento normativo. Este enfoque integral permite al canal responder de manera oportuna y eficiente frente a los desafíos del entorno digital y garantizar la confianza de la ciudadanía y las partes interesadas.

El tratamiento de riesgos en materia de seguridad y privacidad de la información es fundamental para:

- Asegurar el cumplimiento de la misión institucional: preservando la prestación continua del servicio público de televisión y las actividades complementarias que fortalecen la identidad y el desarrollo regional.
- Mantener la estabilidad operativa y tecnológica: protegiendo la infraestructura crítica, los activos digitales, los sistemas de información y los datos sensibles que respaldan la gestión administrativa y técnica.
- Fomentar la confianza y la transparencia: transmitiendo seguridad a la ciudadanía, proveedores, aliados estratégicos, entes de control y colaboradores, mediante una administración responsable, ética y eficiente de los riesgos.
- Dar cumplimiento a la normativa vigente: atendiendo lo dispuesto por el marco legal colombiano en materia de seguridad digital, protección de datos personales, gestión de la información y estándares internacionales aplicables.

De esta manera, Telecafé reafirma su compromiso con la protección de la información y la resiliencia institucional, asegurando que cada acción de gestión tecnológica y administrativa esté respaldada por políticas, controles y prácticas

sólidas que garanticen la continuidad, la confianza y la excelencia en la prestación del servicio público.

2. Definiciones

- Activos de Información: Son todos aquellos recursos físicos y digitales que almacenan, procesan o transmiten datos de valor para Telecafé Ltda., tales como sistemas, aplicaciones, bases de datos, servidores, equipos de cómputo, documentos y la información contenida en ellos. Su adecuada protección es esencial para la continuidad de las operaciones de la entidad.
- Análisis de Riesgos: Proceso mediante el cual se relacionan amenazas y vulnerabilidades con el fin de identificar y dimensionar los riesgos, permitiendo definir los controles más apropiados para su tratamiento.
- Confidencialidad: Principio de la seguridad de la información que garantiza que los datos únicamente sean accesibles a personas o entidades debidamente autorizadas.
- Continuidad de la Operación: Capacidad de Telecafé para asegurar la prestación ininterrumpida del servicio público de televisión y demás procesos relacionados, incluso frente a incidentes de seguridad, fallas técnicas o situaciones externas de contingencia. Su gestión se soporta en el Plan de Continuidad del Negocio.
- Controles de Seguridad: Conjunto de medidas de carácter preventivo, correctivo y de detección implementadas para reducir la probabilidad de ocurrencia de un riesgo o mitigar sus efectos. Estos controles se fundamentan en prácticas reconocidas y estándares internacionales.
- Cultura de Seguridad: Conjunto de valores, prácticas y comportamientos que promueven en la organización la importancia de la seguridad y privacidad de la información, fortalecidos mediante procesos de sensibilización, capacitación y comunicación constante.
- Disponibilidad: Propiedad de la seguridad de la información que asegura que los activos críticos se encuentren accesibles y en correcto funcionamiento en el momento en que sean requeridos.
- Integridad: Característica que garantiza que la información se mantiene exacta, completa y libre de modificaciones no autorizadas.
- Matriz de Riesgos y Controles TI: Instrumento estratégico diseñado para identificar, evaluar, clasificar y dar tratamiento a los riesgos relacionados con los activos de información. Incluye el inventario de activos, la definición de

amenazas y vulnerabilidades, la valoración de riesgos y la selección de los controles pertinentes.

- Mitigación: Estrategia de gestión de riesgos que consiste en implementar medidas de seguridad orientadas a disminuir la probabilidad de ocurrencia o a reducir el impacto que podría generar un evento de riesgo.
- Modelo de Seguridad y Privacidad de la Información (MSPI): Conjunto de lineamientos definidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) de Colombia, adoptados por Telecafé como marco de referencia para la gestión de la seguridad y privacidad de la información.
- Normograma de Tecnologías de la Información (TI): Herramienta de consulta y seguimiento que consolida, organiza y analiza la normativa nacional e internacional aplicable a la gestión de TI. Constituye un insumo clave dentro del plan de riesgos, al permitir la trazabilidad y cumplimiento normativo.
- PHVA (Planificar – Hacer – Verificar – Actuar): Metodología de mejora continua utilizada por Telecafé para evaluar y perfeccionar de manera cíclica la efectividad de los controles de seguridad frente a nuevas amenazas o cambios en el entorno tecnológico y organizacional.
- Plan de Tratamiento de Riesgos: Documento estratégico orientado a la gestión de riesgos en materia de seguridad de la información, protección de datos personales y continuidad operativa. Su enfoque preventivo busca minimizar el impacto de potenciales incidentes que puedan comprometer la gestión institucional.
- Riesgo: Posibilidad de que una amenaza aproveche una vulnerabilidad y genere un impacto adverso sobre los activos de información o la operación de Telecafé. Los riesgos son objeto de monitoreo, revisión y tratamiento continuo.
- Seguridad y Privacidad de la Información: Disciplina que abarca la protección de la información contra accesos no autorizados, usos indebidos, divulgación no controlada, interrupción de procesos o destrucción. Incluye también la gestión responsable de los datos personales.
- Telecafé Ltda.: Sociedad regional de televisión que presta servicios públicos en los departamentos de Caldas, Risaralda y Quindío, bajo los principios de responsabilidad social, transparencia y compromiso con la ciudadanía.

3. Disposiciones Generales

3.1 Objetivo General

Establecer un marco integral de gestión para el tratamiento de riesgos asociados a la seguridad y privacidad de la información en Telecafé Ltda., con el fin de resguardar los activos de información, asegurar la continuidad de los procesos misionales y de apoyo, y garantizar el cumplimiento de la normativa colombiana vigente, en concordancia con los

lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) definido por el MinTIC.

3.2 Objetivos específicos

- Garantizar el cumplimiento normativo y la confianza digital, mediante la alineación del tratamiento de riesgos de seguridad y privacidad de la información con las disposiciones legales vigentes, la protección de datos personales y la transparencia en el acceso a la información pública.
- Proteger y asegurar la continuidad de los activos de información críticos, garantizando su confidencialidad, integridad y disponibilidad, a través de medidas preventivas, correctivas y de recuperación que permitan la operación ininterrumpida del servicio público de televisión.
- Fortalecer la cultura organizacional en seguridad y privacidad de la información, promoviendo la sensibilización, la capacitación permanente y la apropiación de buenas prácticas por parte de directivos, colaboradores y contratistas, de manera que la gestión de riesgos se convierta en un proceso transversal y sostenible dentro de Telecafé Ltda.

4. Alcance

El presente Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información aplica a todos los procesos, dependencias y áreas de Telecafé Ltda., abarcando tanto la gestión administrativa como la operativa y tecnológica de la entidad. Su alcance comprende los activos de información, la infraestructura tecnológica, las plataformas digitales, los sistemas de información y las redes de comunicaciones utilizadas para el desarrollo de la misión institucional y la prestación del servicio público de televisión.

El plan contempla la identificación, evaluación, tratamiento y monitoreo de los riesgos relacionados con la seguridad y privacidad de la información, incluyendo

aspectos como: la protección de datos personales, la continuidad de la operación, la gestión de incidentes, la seguridad física y lógica de los activos tecnológicos, y la prevención de accesos no autorizados.

De igual forma, el alcance se extiende a los colaboradores, contratistas, proveedores y terceros que, de manera directa o indirecta, tengan acceso o administren información de la entidad, quienes deberán cumplir con las políticas, lineamientos y controles definidos en este plan.

En consecuencia, el Plan de Tratamiento de Riesgos constituye un marco integral y transversal que orienta la implementación de medidas preventivas y correctivas, con el fin

de minimizar las amenazas, garantizar la confidencialidad, integridad y disponibilidad de la información, y asegurar la continuidad y confiabilidad de los servicios ofrecidos por Telecafé Ltda.

5. Marco Normativo

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de Telecafé Ltda. se sustenta en un marco normativo robusto que garantiza que la gestión institucional se encuentre en estricto cumplimiento de las disposiciones legales, regulatorias y técnicas vigentes en Colombia. Este marco orienta la formulación de políticas, la adopción de medidas de seguridad, la implementación de controles y el fortalecimiento de la confianza frente a ciudadanos, usuarios, aliados estratégicos y entes de control.

Con el fin de asegurar la aplicación sistemática y permanente de las disposiciones, Telecafé ha diseñado y mantiene actualizado un Normograma de Tecnologías de la Información (TI). Esta

Herramienta consolida, organiza y monitorea todas las normativas aplicables a la entidad, tanto en el ámbito nacional como internacional, permitiendo alinear las operaciones con los estándares más exigentes en materia de seguridad digital, protección de datos personales y transparencia en la gestión pública.

El marco normativo que orienta este plan está conformado por las siguientes disposiciones legales, decretos y estándares técnicos de mayor relevancia:

TIPO DE NORMA	NÚMERO / REFERENCIA	DESCRIPCIÓN / ALCANCE
Ley	1581 de 2012	Establece el marco general para la protección de datos personales en Colombia, regulando su tratamiento y definiendo los principios que garantizan la privacidad y seguridad de la información.
Ley	1273 de 2009	Modifica el Código Penal e incorpora como bien jurídico la “protección de la información y de los datos”, tipificando delitos como acceso abusivo a sistemas informáticos, violación de datos personales y hurto por medios informáticos.
Ley	2294 de 2023	Plan Nacional de Desarrollo 2022-2026, que incluye lineamientos para la transformación digital, la

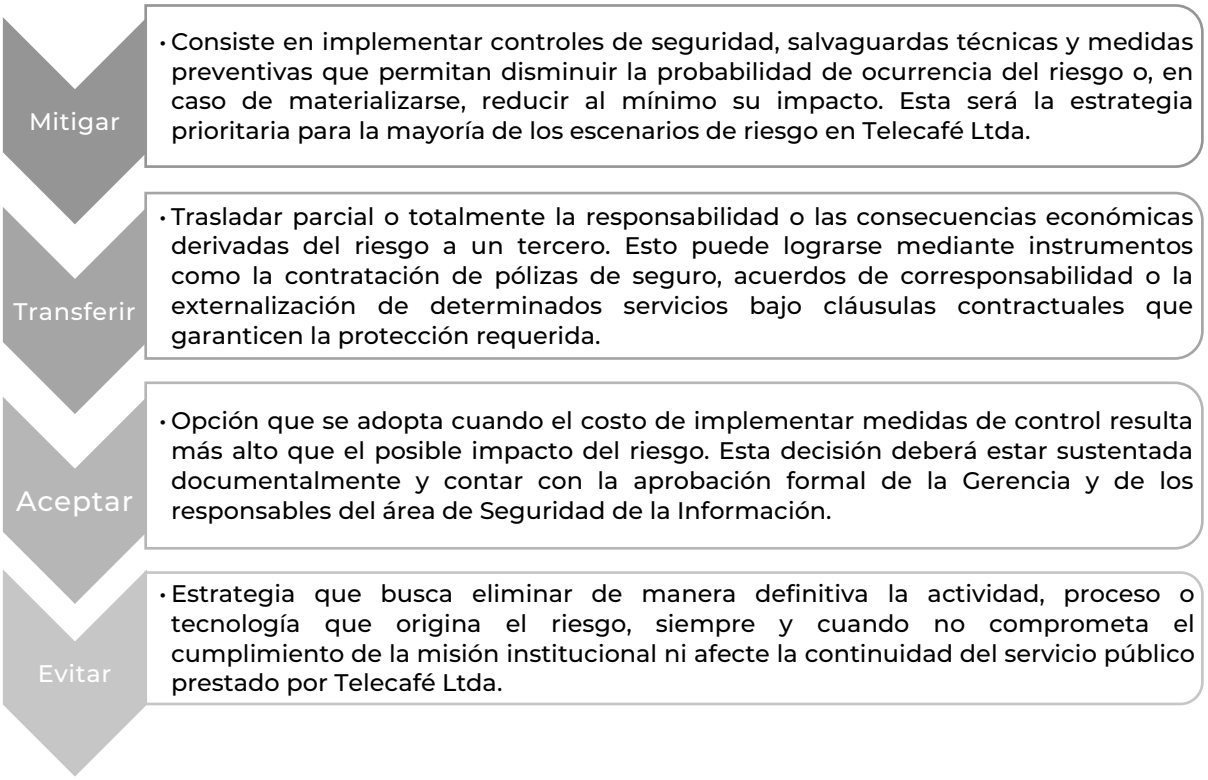
		seguridad de la información y el fortalecimiento de la conectividad como política pública.
Ley	1712 de 2014	Conocida como la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional, establece la obligación de garantizar que la información pública sea accesible, veraz y disponible para la ciudadanía.
Ley	1978 de 2019	Por medio de la cual la Ley 1978 de 2019, también conocida como la Ley de Modernización del Sector de las Tecnologías de la Información y las Comunicaciones (TIC), es fundamental ya que toma puntos claves tales como modernización y regulación (Esta ley busco modernizar la ley 1341 de 2009 modificando ciertos puntos debido a los avances tecnológicos)
Ley	527 de 1999	Regula el comercio electrónico en Colombia y otorga plena validez jurídica a los documentos, firmas y transacciones electrónicas, equiparándolos a sus equivalentes físicos.
Decreto	2106 de 2019	Impulsa la transformación digital del Estado, simplificando trámites y promoviendo el uso de tecnologías seguras y confiables.
Decreto	2609 de 2012	Reglamenta la gestión de documentos electrónicos de archivo, vinculando directamente la seguridad de la información y el tratamiento de datos en entornos digitales
Decreto	1078 de 2015 (DUR)	Decreto Único Reglamentario del sector TIC, que compila y unifica la normatividad vigente en materia de tecnologías de la información y comunicaciones.
Decreto	338 de 2022	Fortalece la gobernanza de la seguridad digital en Colombia, estableciendo lineamientos para la gestión de riesgos, respuesta a incidentes y protección de infraestructuras críticas
Decreto	2609 de 2012	Este decreto reglamenta el Título V de la Ley 594 de 2000 (Ley General de Archivos) y parcialmente los artículos 58 y 59 de la Ley 1437 de 2011, estableciendo los lineamientos para la gestión documental en entidades públicas. Define los principios, procesos y componentes esenciales del Programa de Gestión Documental (PGD), incluidos los documentos electrónicos. Asimismo, exige que cada entidad cuente

		con un Sistema de Gestión Documental y publique su PGD en el sitio web institucional
Decreto	338 de 2022	Este decreto adiciona el Título 21 a la Parte 2 del Libro 2 del Decreto Único Reglamentario 1078 de 2015, estableciendo los lineamientos generales para robustecer la gobernanza de la seguridad digital en Colombia. Además, crea un modelo institucional y sus instancias, promueve la protección de infraestructuras críticas e incorpora la gestión de riesgos y respuesta coordinada ante incidentes cibernéticos. Formaliza, asimismo, la ciudad de los Equipos de Respuesta a Incidentes Cibernéticos (CERTs)
Decreto	1078 de 2015	Este decreto es el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones (TIC). Reúne y sistematiza la normativa vigente del sector, facilitando su consulta y aplicación normativa por parte de entidades públicas y actores del sector TIC
Resolución	1519 de 2020	Define los estándares de publicación de información en línea, estableciendo criterios de accesibilidad, usabilidad y disponibilidad en los portales web del Estado.
COMPES	3995 de 2020	Política Nacional de Confianza y Seguridad Digital, orientada a fortalecer la ciberseguridad, la gestión de riesgos y la resiliencia digital del país.
Norma Técnica	NTC ISO/IEC 27001:2013 (y actualización 2022)	Estándar internacional para la gestión de seguridad de la información, que establece los requisitos para implementar, mantener y mejorar un sistema de gestión de seguridad basado en riesgos.
Norma	NTC ISO 27001	Por medio del cual la NTC ISO 27001 cumple como función principal el servir como un marco de referencia técnico y de gestión para la ciberseguridad.

6. Metodología

El tratamiento de los riesgos de seguridad y privacidad de la información en Telecafé Ltda. se llevará a cabo bajo un enfoque integral, fundamentado en las mejores prácticas internacionales definidas por la norma ISO/IEC 27001 y en armonía con los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) establecido por el MinTIC.

Cada riesgo identificado en los procesos de gestión será analizado y tratado a través de una de las siguientes estrategias:



7. Plan de Acción y Controles a Implementar

El Plan de Acción y Controles a Implementar, como parte fundamental del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de Telecafé Ltda., constituye la ruta estratégica para gestionar de manera efectiva los riesgos que puedan afectar los activos de información de la entidad.

Este plan se sustenta en el análisis detallado desarrollado a través de la Matriz de Riesgos y Controles de TI, instrumento que permite identificar, evaluar y priorizar amenazas y vulnerabilidades con un enfoque sistemático. Dicha herramienta proporciona una visión integral de los riesgos inherentes a los procesos tecnológicos y organizacionales,

utilizando escalas cuantitativas y mapas de calor que facilitan la toma de decisiones basadas en criterios objetivos.

El propósito central es definir las bases para la mitigación de riesgos mediante la aplicación de controles preventivos, correctivos y detectivos, alineados con estándares internacionales y con las mejores prácticas en seguridad de la información. La dependencia de Tecnologías de la Información (TI) lidera la ejecución de estas acciones, garantizando la confidencialidad, integridad y disponibilidad de los activos críticos de Telecafé Ltda.

Con este enfoque proactivo, la organización no solo fortalece su postura de seguridad, sino que fomenta una cultura organizacional de gestión del riesgo, orientada a la protección continua de la información y al aseguramiento de la prestación del servicio público de televisión.

La Matriz de Riesgos y Controles constituye un documento de gobernanza que integra:

- Inventario de activos de información.
- Identificación de amenazas y vulnerabilidades.
- Evaluación cuantitativa del riesgo.
- Selección de controles apropiados.

De esta manera, facilita la priorización de acciones, la asignación de recursos y la planeación de estrategias de mitigación coherentes con los objetivos institucionales.

8. Plan de Acción Específico para el Área de TI

A continuación, se presentan las actividades principales que guían la gestión de riesgos de seguridad y privacidad de la información:

ACTIVIDAD	DESCRIPCION
Identificación y clasificación de activos de la información	Elaborar un inventario exhaustivo de sistemas, bases de datos, aplicaciones, equipos (servidores, estaciones de trabajo, dispositivos móviles), así como documentos físicos y digitales. A cada activo se le asignará un valor según su relevancia y el impacto que generaría su pérdida, alteración o divulgación.
Identificaciones de amenazas y vulnerabilidades	Analizar los activos para determinar los riesgos a los que están expuestos: ataques cibernéticos (malware, phishing), errores humanos (configuración incorrecta, accesos indebidos), fallos técnicos (daños de hardware,

	interrupciones de energía) y contingencias externas (desastres naturales). Se documentarán vulnerabilidades como contraseñas débiles, falta de actualización de software o deficiencias en los procesos internos.
Análisis y clasificación de riesgos	Definir el umbral de riesgo aceptable para la organización. Aquellos riesgos que superen este umbral deberán contar con un plan de tratamiento documentado.
Evaluación y aceptación de los riesgos	Diseñar e implementar estrategias específicas de gestión: mitigar, transferir, aceptar o evitar, según corresponda a cada caso.
Plan de tratamiento de riesgos	Se define un plan de que como tratar el riesgo encontrado según lo estructurado tal como: mitigar, trasferir, aceptar y evitar.
Monitoreo	Establecer un proceso periódico de seguimiento y actualización de la Matriz de Riesgos, garantizando su vigencia y la efectividad de los controles implementados.

Los riesgos identificados se clasifican globalmente en la Matriz de Riesgos y Controles, documento complementario a este plan, donde se detallan los controles de seguridad diseñados para reducir su probabilidad y mitigar sus efectos en los siguientes términos:

1. Gobernanza y Gestión de la Seguridad

- Carencia de políticas institucionales formalmente establecidas en materia de seguridad de la información.
- Definición ambigua o inexistente de roles y responsabilidades en la gestión de seguridad.
- Procesos insuficientes para la clasificación y categorización adecuada de la información según su nivel de criticidad y sensibilidad.

2. Seguridad de los Activos de Información

- Posibilidad de accesos no autorizados a sistemas, aplicaciones o recursos tecnológicos.
- Uso inadecuado de credenciales de acceso, incluyendo contraseñas débiles, reutilizadas o compartidas.
- Equipos de cómputo sin mecanismos de protección adecuados frente a incidentes internos o externos.

- Riesgo de pérdida o corrupción de información derivada de fallos técnicos, errores humanos o ataques cibernéticos.

3. Privacidad y Protección de Datos Personales (Ley 1581 de 2012)

- Tratamiento de datos personales sin el consentimiento expreso de los titulares o sin cumplir requisitos normativos.
- Exposición o filtración de información personal contenida en bases de datos institucionales.
- Escaso conocimiento y capacitación del personal en relación con las obligaciones legales y buenas prácticas sobre el manejo de datos personales.

4. Seguridad en las Comunicaciones y Operaciones

- Presencia de vulnerabilidades en servidores, aplicaciones web y otros servicios expuestos.
- Deficiencias en los mecanismos de registro, seguimiento y monitoreo de eventos relevantes de seguridad.

9. Controles Aplicados

La adecuada gestión y tratamiento de los riesgos de seguridad y privacidad de la información en Telecafé Ltda. requiere la implementación de controles específicos alineados con las mejores prácticas internacionales. En este sentido, se han seleccionado y adoptado una serie de medidas contempladas en el Anexo A de la norma ISO/IEC 27001:2022, las cuales se orientan a fortalecer la protección de los activos de información, garantizar el cumplimiento normativo y preservar la continuidad operativa de la entidad.

Estos controles constituyen la base para una estrategia de mitigación integral, ya que permiten reducir la probabilidad de materialización de incidentes, minimizar su impacto y establecer un marco de gobernanza que asegure la trazabilidad y la efectividad de las acciones implementadas. Cada actividad definida busca responder a riesgos identificados en el análisis institucional, abarcando dimensiones como la gestión de accesos, la protección de registros, la seguridad física, el cifrado de datos y el cumplimiento de políticas internas y normativas legales.

De esta manera, los controles aplicados no solo representan un componente técnico, sino también un instrumento de gestión estratégica que consolida el compromiso de Telecafé

Ltda. con la seguridad de la información, la confianza digital y la prestación ininterrumpida de sus servicios.A.6.8 Evaluación y decisión sobre eventos de la seguridad de la información.

A.8.23.	Filtrado WEB
A. 5.33	Protección de registros
A. 5.36	Cumplimiento con políticas, reglas y estándares para la seguridad de la información.
A.5.32	Derechos de propiedad intelectual.
A8.24	Cifrado de la información.
A.5.9	Inventario de información y otros activos asociados.
A.8.24	Uso de criptografía.
A.5.15	Control de acceso.
A.5.16	Gestión de identidades.
A.5.17	Autenticación de información de acceso.
A.7.2	Seguridad física de instalaciones.
A.5.1	Políticas para la seguridad de la información.
A.8.19	Seguridad de redes.
A.5.1	Políticas para la seguridad de la información.

10. Monitoreo, Revisión y Mejora Continua

La gestión de riesgos en seguridad y privacidad de la información dentro de Telecafé Ltda. se concibe como un proceso dinámico y en permanente evolución, que demanda supervisión constante para asegurar su efectividad y vigencia frente a los cambios del entorno. Con este propósito, la organización ha establecido un ciclo de Monitoreo, Revisión y Mejora Continua, orientado a evaluar de manera sistemática el desempeño de los controles aplicados y a ajustar el plan de tratamiento frente a nuevas necesidades, amenazas u oportunidades.

El eje de este ciclo es el Cronograma de Actividades de TI, herramienta que convierte los objetivos estratégicos en tareas concretas, programadas y con responsables definidos. Dicho cronograma establece plazos específicos para cada actividad de la dependencia de Tecnologías de la Información, garantizando orden, trazabilidad y cumplimiento oportuno.

Mediante la aplicación disciplinada de este mecanismo, Telecafé Ltda. asegura la ejecución periódica de revisiones de controles, auditorías técnicas, actualizaciones de seguridad y procesos de capacitación al personal. Este enfoque preventivo no solo facilita

la verificación del cumplimiento de las políticas internas, sino que también permite detectar posibles brechas, medir la eficacia de los mecanismos implementados y retroalimentar el proceso de mejora continua. De este modo, la gestión de la Seguridad y Privacidad de la Información se consolida y se adapta a los retos emergentes del entorno digital.

Las actividades de seguimiento se estructuran de la siguiente manera:

- Seguimiento bimensual: Liderado por el director de TI, con reuniones periódicas para revisar el avance de las acciones establecidas.
- Revisión semestral: Análisis integral del plan y del estado de los riesgos, con la participación de la Gerencia en la revisión por la dirección.
- Reporte anual a la Revisoría Fiscal: Consolidación de resultados y generación de un informe de gestión de riesgos presentado en el marco de la auditoría anual.
- El principio rector de este proceso será el ciclo Planificar–Hacer–Verificar–Actuar (PHVA), garantizando que los controles se mantengan vigentes, efectivos y en continua adaptación frente a nuevas amenazas.

Finalmente, como complemento esencial, se incorpora el Plan de Continuidad del Negocio, documento estratégico que define los lineamientos y procedimientos para respaldar y reforzar las acciones de monitoreo, revisión y mejora continua.

11. Anexos

Como soporte al presente Plan de Gestión y Tratamiento de Riesgos de Seguridad y Privacidad de la Información de Telecafé Ltda., se incluyen los siguientes documentos:

- Normograma de Tecnologías de la Información (TI): Compendio actualizado de la normatividad nacional e internacional aplicable al sector, que orienta el cumplimiento regulatorio y fortalece la gobernanza en materia de seguridad de la información.
- Matriz de Riesgos y Controles TI: Instrumento estratégico que integra el inventario de activos, amenazas, vulnerabilidades, riesgos identificados y controles implementados, facilitando la toma de decisiones y la priorización de acciones.
- Plan de Continuidad del Negocio TI: Documento que establece las directrices, procedimientos y responsabilidades necesarias para garantizar la operación continua de los servicios críticos ante incidentes de seguridad, fallas tecnológicas o contingencias externas.

12. Disposiciones Finales

Este plan constituye una guía de referencia obligatoria para la gestión de la seguridad y privacidad de la información en Telecafé Ltda. Su aplicación es responsabilidad de todas las áreas involucradas en la administración y uso de activos de información, bajo la coordinación de la dependencia de Tecnologías de la Información.

Las disposiciones aquí contenidas estarán sujetas a procesos de actualización y mejora continua, en función de cambios normativos, tecnológicos o de riesgos emergentes. Cualquier modificación deberá ser documentada y aprobada formalmente por la Gerencia, garantizando su alineación con el Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC y con las mejores prácticas internacionales.