telecafé

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

www.telecafe.gov.co
@canaltelecafe
@telecafetv

Código: TEI-PRO-24
Fecha: 1 de septiembre de 2025
Versión: 01
Sistema Integrado de Gestión

Sociedad de Televisión de Caldas, Risaralda y Quindío Telecafe Ltda.

1. Introducción

En el contexto actual, marcado por la transformación digital y la constante evolución del sector audiovisual, la información se ha consolidado como uno de los activos más estratégicos para Telecafé Ltda. El manejo responsable de los contenidos de transmisión, así como de los datos personales de nuestra audiencia y colaboradores, resulta esencial para garantizar el cumplimiento de nuestra misión de servicio público y preservar la confianza ciudadana.

Con este propósito, se ha diseñado el Plan de Seguridad y Privacidad de la Información (PSPI), el cual establece los lineamientos, políticas y procedimientos orientados a proteger la confidencialidad, integridad y disponibilidad de los activos informáticos de la organización. Este instrumento no solo responde a una necesidad operativa, sino también a un mandato legal enmarcado en la Ley 1581 de 2012, la Ley 527 de 1999 y las directrices del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

El PSPI constituye una herramienta fundamental para garantizar la continuidad del servicio, dar cumplimiento a la normativa vigente, mitigar riesgos legales y técnicos, y promover una cultura institucional basada en la transparencia y la responsabilidad en el manejo de la información.

2. Disposiciones Generales

2.1 Objetivo General

Definir un marco estratégico y operativo que oriente la implementación de políticas, estrategias, controles y responsabilidades encaminadas a preservar de forma continua la seguridad, confidencialidad, integridad y disponibilidad de la información en Telecafé Ltda. Este propósito abarca la protección de los contenidos audiovisuales, los datos personales, los sistemas críticos y la infraestructura tecnológica de la entidad, garantizando el cumplimiento del marco legal colombiano y la adopción de referentes internacionales en buenas prácticas. En última instancia, se busca anticipar y reducir los riesgos asociados a pérdida, alteración, accesos no autorizados o interrupciones en los servicios, fortaleciendo así la continuidad operativa y la confianza de la ciudadanía.

2.2 Objetivos específicos

- Fortalecer la gestión y el gobierno de la seguridad de la información, mediante la formalización de políticas, normas y procedimientos claros, la asignación de

roles y responsabilidades en todos los niveles de la organización, y el desarrollo de programas de capacitación que promuevan una cultura institucional de protección y uso responsable de los activos de información.

- Implementar controles técnicos, medidas de protección y planes de respuesta, asegurando la protección integral de la infraestructura tecnológica, los sistemas de información, los contenidos audiovisuales y los datos personales frente a accesos no autorizados, incidentes de seguridad o interrupciones, garantizando la continuidad del negocio y la prestación ininterrumpida de los servicios públicos.

- Gestionar riesgos y asegurar el cumplimiento normativo, aplicando metodologías de identificación y tratamiento de riesgos, manteniendo actualizado el normograma institucional, cumpliendo con las disposiciones legales y regulatorias vigentes, y avanzando en el cierre de brechas del Modelo de Seguridad y Privacidad de la Información (MSPI), con el fin de proteger la reputación y minimizar contingencias legales para Telecafé Ltda.

3. Marco Normativo

El Plan de Seguridad y Privacidad de la Información (PSPI) de Telecafé Ltda. se formula en atención al marco legal y regulatorio vigente en Colombia, complementado con referentes internacionales de buenas prácticas en la materia. Este marco no solo representa una obligación formal, sino que también constituye la base para garantizar la protección de los activos de información, salvaguardar la privacidad de los titulares de datos y asegurar la continuidad de las operaciones del canal.

La adopción de este plan parte del reconocimiento de la información como un recurso estratégico que demanda medidas específicas para preservar su confidencialidad, integridad y disponibilidad, en armonía con los instrumentos normativos aplicables.

TIPO DE NORMA	IDENTIFICACIÓN	SÍNTESIS DEL DOCUMENTO
Constitución	1991	Establece que la Constitución es la norma de mayor jerarquía en el ordenamiento jurídico colombiano. Ninguna ley, decreto o regulación puede contradecir sus principios, incluyendo aquellos relacionados con tecnologías de la información y protección de datos.
Ley	1581 de 2012	Regula la protección de datos personales, fijando lineamientos para su tratamiento, con el fin de garantizar la privacidad y seguridad de la información de titulares.

Ley	1273 de 2009	Modifica el Código Penal e introduce el bien jurídico de la "protección de la información y de los datos". Tipifica delitos como acceso abusivo a sistemas, hurto informático y violación de datos personales.
Ley	2294 de 2023	Ley del Plan Nacional de Desarrollo 2022–2026, que incluye lineamientos de política pública en tecnología, conectividad y seguridad digital.
Ley	1266 de 2008	Conocida como Ley de Habeas Data Financiero. Establece el marco regulatorio para el tratamiento de información financiera, crediticia y comercial, garantizando la protección de derechos de los titulares.
Ley	1915 de 2018	Reforma y actualiza la normativa de derechos de autor, con especial énfasis en el entorno digital y la gestión de activos intangibles relacionados con TI.
Ley	1712 de 2014	Ley de Transparencia y del Derecho de Acceso a la Información Pública. Obliga a garantizar la publicidad y accesibilidad de la información en poder de entidades públicas.
Ley	1978 de 2019	Ley de Modernización del sector TIC, que actualiza la Ley 1341 de 2009, ampliando competencias regulatorias y fortaleciendo la política pública en conectividad y servicios digitales.
Ley	527 de 1999	Reconoce la validez jurídica de mensajes de datos y documentos electrónicos, equiparándolos con sus equivalentes físicos en transacciones comerciales y legales.
Decreto	612 de 2018	Regula aspectos de la Política de Gobierno Digital, incluyendo seguridad de la información, interoperabilidad y gestión de riesgos en entidades públicas.
Decreto	2106 de 2019	Establece disposiciones para la transformación digital en el sector público y define lineamientos de simplificación de trámites y servicios digitales.
Decreto	2609 de 2012	Define directrices para la gestión documental y de archivos electrónicos, con impacto en seguridad de la información y tratamiento de datos.
Decreto	338 de 2022	Establece lineamientos generales de gobernanza de seguridad digital, gestión de riesgos y respuesta a incidentes cibernéticos en el país.
Decreto	1078 de 2015	Decreto Único Reglamentario del Sector TIC, que compila y actualiza la normativa aplicable a telecomunicaciones, servicios postales y tecnologías de la información.
Norma	NTC ISO 27001 de 2022	Norma internacional adoptada en Colombia, que establece requisitos para un sistema de gestión de seguridad de la información (SGSI).

Resolución	1519 de 2020	Define estándares de publicación de información en portales de entidades públicas, garantizando accesibilidad y usabilidad en el marco de Gobierno Digital.
CONPES	3995 de 2020	Política Nacional de Confianza y Seguridad Digital, orientada a fortalecer capacidades en ciberseguridad, impulsar marcos técnicos y fomentar confianza en el entorno digital.

4. Alcance

El Plan de Seguridad y Privacidad de la Información (PSPI) de Telecafé Ltda. se concibe como un instrumento integral y de cumplimiento obligatorio para toda la organización. Su propósito es establecer un marco claro que garantice la protección de la información en todas sus formas y contextos, reconociendo que este activo es esencial para la continuidad de la operación, la confianza del público y el cumplimiento normativo.

El alcance de este plan se desarrolla en los siguientes niveles:

4.1 Cobertura de Personas:

El plan aplica a todas las personas que interactúen con los activos de información de Telecafé Ltda., sin importar el tipo de vinculación o relación contractual, entre ellos:

- Funcionarios: directivos, empleados de planta y personal temporal.
- Contratistas: personas naturales o jurídicas que presten servicios a la entidad.
- Terceros: proveedores, consultores, aliados estratégicos y demás actores externos con acceso a la información.
- Pasantes y aprendices: vinculados en procesos de formación académica o práctica laboral.

4.2 Cobertura de Activos de Información:

El PSPI protege todos los activos de información generados, procesados, almacenados o transmitidos en Telecafé Ltda., en formato físico o digital. Estos incluyen:

- Contenidos Audiovisuales: archivos de video y audio en bruto y editados, masters, bancos de imágenes, guiones, material de preproducción y postproducción.
- Datos Personales: información que identifique o pueda identificar a personas naturales, conforme a lo dispuesto en la Ley 1581 de 2012.
- Información Administrativa y Financiera: Documentación de recursos humanos, nómina, contratos, facturas, estados financieros, presupuestos y correspondencia oficial.

- Sistemas de Información y Tecnología: hardware, software, servidores, redes, estaciones de trabajo, aplicaciones y bases de datos.
- Procesos Críticos de Transmisión: sistemas de broadcast, playout, enlaces de microondas, satélite y plataformas de streaming..
- Plataformas Digitales: Portales web oficiales, aplicaciones móviles y redes sociales institucionales.

4.3 Procesos y áreas incluidas

El plan es de carácter transversal y se aplica a todos los procesos y dependencias de Telecafé Ltda., incluyendo las áreas de dirección general, producción y contenidos, comunicaciones digitales, innovación tecnológica, asuntos jurídicos, ingeniería, administración y finanzas, gestión del talento humano, mercadeo, archivo físico y digital, entre otras.

4.4. Exclusiones:

Queda excluida la información personal de empleados o terceros que sea utilizada fuera de los entornos laborales y sistemas de Telecafé Ltda., siempre que no tenga relación con el objeto y funciones de la entidad. No obstante, su tratamiento deberá ajustarse a las políticas de confidencialidad y uso aceptable definidas por la organización.

En conjunto, este alcance asegura que la seguridad de la información se entienda como una responsabilidad compartida y alineada con la misión, la estructura y los procesos estratégicos de Telecafé Ltda.

5. Gobernanza y Responsables:

La adecuada ejecución del Plan de Seguridad y Privacidad de la Información (PSPI) de Telecafé Ltda. depende de contar con una estructura de gobernanza sólida y bien definida. Esta estructura establece de manera precisa los roles, funciones y mecanismos de control que permitirán implementar, mantener y mejorar de forma permanente las prácticas de seguridad de la información.

El modelo de gobernanza busca garantizar que la gestión de la seguridad no recaiga en un solo actor, sino que se convierta en un compromiso transversal que involucre a todas las áreas y niveles jerárquicos de la organización. De este modo, se asegura que cada colaborador, desde la alta dirección hasta los equipos operativos, entienda su papel dentro del marco de protección de la información y contribuya activamente a la preservación de los principios de confidencialidad, integridad y disponibilidad.

Adicionalmente, esta estructura se articula con los lineamientos estratégicos de Telecafé Ltda., de manera que las decisiones y acciones en materia de seguridad estén alineadas con la misión

institucional, los objetivos de servicio público y el marco regulatorio vigente. Así, la gobernanza del PSPI no solo funciona como un sistema de control interno, sino como un componente esencial para fortalecer la confianza de la ciudadanía y garantizar la sostenibilidad de la operación en el entorno digital y audiovisual.

5.1 Comité de Seguridad De la Información

La responsabilidad máxima sobre la protección de la información dentro de Telecafé Ltda. se concentra en el Comité de Seguridad de la Información, órgano colegiado de carácter directivo que tiene como misión orientar, supervisar y respaldar la ejecución del Plan de Seguridad y Privacidad de la Información (PSPI). Este comité actúa como la instancia más alta de decisión en la materia, asegurando que las políticas y medidas adoptadas estén alineadas con la estrategia institucional y con el marco regulatorio vigente.

5.2 Integrantes:

MIEMBRO	ROL
Gerencia / Alta Dirección:	Ejerce la presidencia del comité, liderando el proceso de toma de decisiones estratégicas. Es responsable de validar las políticas y planes, aprobar la asignación de recursos y, en última instancia, rendir cuentas ante organismos de control y demás partes interesadas.
Líder de TI:	Funge como secretario técnico del comité. Su papel central consiste en coordinar la ejecución operativa del plan, garantizar que las iniciativas de seguridad se traduzcan en acciones concretas y mantener informada a la alta dirección sobre el estado de la seguridad, riesgos identificados y propuestas de mejora.
Coordinadores de Áreas Críticas:	Son los representantes de las dependencias que manejan información crítica, quienes actúan como custodios secundarios de los activos más sensibles. Su labor consiste en aplicar los lineamientos de seguridad en la práctica cotidiana de sus procesos y asegurar que cada procedimiento interno respete los principios de confidencialidad, integridad y disponibilidad.
Talento Humano:	Encargada de gestionar el acceso y la protección de la información personal de empleados, contratistas, aprendices y candidatos. Su gestión garantiza el cumplimiento de la Ley 1581 de 2012 y demás disposiciones relacionadas con la protección de datos personales.
Administrativa y Financiera:	Custodio de la información contable, presupuestal y contractual que respalda la sostenibilidad económica de la entidad. Asegura la protección y disponibilidad de los datos que sirven de soporte para la planeación y toma de decisiones estratégicas.
Producción y Contenidos:	Responsable de la integridad y disponibilidad de los contenidos audiovisuales, guiones, materiales en desarrollo y archivos maestros. Su rol es esencial para preservar la calidad y seguridad de los productos comunicativos y garantizar su transmisión y distribución sin riesgos de pérdida o alteración.

Jurídica:	Brinda acompañamiento permanente al comité, interpretando el marco legal aplicable, orientando las decisiones hacia el cumplimiento normativo y diseñando mecanismos que reduzcan la exposición a riesgos legales relacionados con el uso y manejo de la información.
Tecnología e Innovación:	Administra la infraestructura tecnológica de la organización, asegurando que los servidores, redes, plataformas digitales y sistemas críticos estén debidamente protegidos. Implementa controles técnicos y coordina las acciones necesarias para apoyar a todas las áreas en la protección de sus activos de información.

En conjunto, este comité se constituye como el pilar institucional que articula esfuerzos, define prioridades y garantiza que la seguridad de la información no sea un proceso aislado, sino una práctica transversal y sostenida en toda la organización.

5.2 Roles y Responsabilidades Específicas

En concordancia con la matriz de roles definida y la política institucional TEI-PRO-15, se establecen las funciones y compromisos de cada nivel de la organización en relación con la seguridad y privacidad de la información. Estas responsabilidades buscan garantizar la correcta aplicación del Plan y fortalecer la cultura de protección de los activos informacionales.

ROL	RESPONSABILIDADES CLAVE SEGÚN POLÍTICA INTERNA
Alta Dirección / Gerencia	• Revisar, aprobar y respaldar el Plan de Seguridad y Privacidad de la Información (PSPI) junto con las políticas asociadas. • Asignar los recursos financieros, tecnológicos y humanos necesarios para asegurar su implementación. • Fijar la importancia estratégica de la seguridad de la información dentro de la entidad, transmitiendo un mensaje de compromiso y ejemplo hacia toda la organización.
Líder de Tecnología e Innovación Dependencia TI	• Administrar y mantener los controles técnicos de seguridad, incluyendo accesos, firewalls, copias de respaldo y cifrado de datos. • Coordinar la gestión de incidentes de seguridad desde su detección hasta su resolución. • Realizar evaluaciones periódicas, revisiones y auditorías sobre los sistemas tecnológicos. • Promover programas de sensibilización y capacitación para fortalecer las buenas prácticas entre los usuarios. • Proteger los activos de información custodiados en la infraestructura tecnológica. • Clasificar los datos según su nivel de criticidad y gestionar de manera integral los recursos de TI. • Velar por el cumplimiento del marco normativo vigente en materia de seguridad digital y protección de datos.

Líderes de Proceso / Coordinadores de Área	• Asegurar la implementación del PSPI en las actividades y procesos de sus respectivas dependencias. • Ejercer el rol de “propietarios secundarios” de la información que se genera y administra en su área. • Clasificar y controlar el acceso a los datos bajo su custodia, aplicando el principio de necesidad. • Supervisar y autorizar los permisos de acceso de acuerdo con la naturaleza del cargo o la función. • Informar oportunamente cualquier anomalía, incidente o desviación detectada a la Dependencia de TI.
Todos los Usuarios (Empleados, Contratistas, Pasantes)	• Utilizar responsablemente la información a la que acceden, respetando los niveles de clasificación establecidos. • Proteger sus credenciales de autenticación, como usuarios y contraseñas, evitando su uso indebido o compartido. • Cumplir con las políticas de uso aceptable sobre recursos tecnológicos, incluyendo correo electrónico, internet, software y hardware. • Reportar de inmediato cualquier evento sospechoso, incidente de seguridad o uso inadecuado de los sistemas al jefe inmediato y al área de TI. • Desconectar los equipos y apagar los dispositivos al terminar la jornada laboral, contribuyendo con las políticas de ahorro energético y seguridad informática.

5.3 Mecanismos de comunicación

Con el propósito de garantizar un flujo de información eficiente, oportuno y transparente en materia de seguridad de la información, se han dispuesto los siguientes mecanismos:

- Dependencia de Tecnología e Innovación (TI): Será la encargada de presentar de forma periódica informes detallados al Comité de Seguridad, en los que se incluya el estado de avance del Plan, los indicadores de cumplimiento, así como el registro y análisis de los incidentes de seguridad ocurridos. Estos reportes permitirán tomar decisiones basadas en evidencias y priorizar acciones de mejora.
- Usuarios y líderes de área: Tendrán la responsabilidad de informar a la Dependencia TI cualquier evento, anomalía o inquietud relacionada con la protección de la información. Para tal fin, se han dispuesto canales formales de comunicación que garantizan trazabilidad, atención oportuna y confidencialidad en el manejo de los reportes.
- Comité de Seguridad de la Información: Este organismo colegiado transmitirá a toda la organización las decisiones estratégicas adoptadas, así como las actualizaciones de políticas, lineamientos y medidas correctivas o preventivas. Su rol será asegurar que cada miembro de Telecafé Ltda. conozca y aplique las directrices emitidas.

Esta dinámica de comunicación fortalece el modelo de gobernanza, al integrar la supervisión de la alta dirección, la ejecución técnica especializada y la participación activa de todos los niveles de la

entidad. De esta manera, la seguridad de la información se gestiona de forma transversal, compartida y alineada con los objetivos institucionales.

6. Políticas para el Plan de Seguridad y Privacidad de la Información (PSPI) - Telecafé Ltda.

El establecimiento de políticas claras constituye la base para la gestión integral de la seguridad de la información en Telecafé Ltda. Estas directrices actúan como marco de referencia para orientar las decisiones, las prácticas y los comportamientos esperados en toda la organización, garantizando la protección de los activos críticos y el cumplimiento normativo vigente. El conjunto de políticas definidas en este Plan busca no solo mitigar riesgos tecnológicos y organizacionales, sino también consolidar una cultura de seguridad que trascienda los procesos y se convierta en un principio transversal para todos los colaboradores, contratistas y terceros vinculados al canal.

6.1 Política de Alcance y Aplicabilidad del PSPI

- Objetivo: Delimitar el campo de acción, los activos prioritarios y el contexto en el que se implementa el Plan de Seguridad y Privacidad de la Información (PSPI) de Telecafé Ltda., de manera que su ejecución sea clara, coherente y dirigida hacia las áreas críticas de la organización.

- Alcance: El PSPI aplica a todos los procesos, información, sistemas, personas (empleados, contratistas, terceros) y las sedes físicas de Telecafé Ltda. que intervienen en la creación, procesamiento, almacenamiento o transmisión de información institucional, incluyendo contenidos audiovisuales, datos personales, información financiera y sistemas de transmisión.

- Exclusiones: Quedan excluidos los sistemas personales no autorizados y la información manejada fuera de los canales y sistemas corporativos aprobados.

- Responsable: La Alta Dirección, con el apoyo de la Dependencia TI, es responsable de aprobar y revisar periódicamente este alcance.

6.2 Política de Gestión de la Información Documentada

- Objetivo: Garantizar que todos los documentos relacionados con el Sistema de Gestión de Seguridad de la Información (SGSI), incluyendo políticas, manuales, procedimientos y registros, se mantengan actualizados, disponibles y protegidos contra accesos no autorizados.
- Disponibilidad: La documentación estará centralizada en repositorios controlados y accesible únicamente a las personas con autorización, garantizando su consulta en el momento que sea requerida.
- Protección: Cada documento será clasificado según su nivel de sensibilidad y se implementarán controles para regular su acceso, modificación y distribución. Los registros relacionados con seguridad serán protegidos frente a alteraciones o pérdidas.

- Responsable: La Dependencia de Tecnología e Innovación (TI) velará por la seguridad técnica y la disponibilidad de los repositorios, mientras que los líderes de proceso deberán garantizar la exactitud y actualización de la documentación bajo su custodia.

6.3 Política de Administración de Riesgos en Seguridad de la Información

- Objetivo: Implementar un proceso formal y continuo para identificar, analizar, evaluar y mitigar los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información de Telecafé Ltda.
- Metodología: Se adoptará el estándar ISO/IEC 27001:2022 como marco para valorar riesgos inherentes y residuales.
- Tratamiento: Los riesgos se gestionarán mediante controles adecuados que permitan reducir, transferir, evitar o aceptar su impacto, de acuerdo con los niveles de tolerancia definidos por la Alta Dirección.
- Revisión: El proceso de gestión de riesgos será evaluado anualmente o cada vez que existan cambios relevantes en el entorno tecnológico u operativo.

- Responsable: La Dependencia TI liderará el proceso con el apoyo de los dueños de la información y procesos. La Alta Dirección tendrá la función de aprobar la aceptación de riesgos residuales.

6.4 Política de Concientización y Formación en Seguridad

- Objetivo: Asegurar que cada empleado, contratista y tercero reciba capacitación constante en materia de seguridad de la información, ajustada a sus responsabilidades, reduciendo así el riesgo derivado del factor humano.

- Plan de Capacitación: Se diseñará e implementará un programa anual que cubra temas como phishing, protección de datos personales, uso responsable de los recursos tecnológicos y cumplimiento de políticas internas.
- Periodicidad: La inducción incluirá formación inicial obligatoria para todo nuevo integrante de la organización, además de campañas de actualización al menos dos veces al año.
- Evaluación: Se aplicarán encuestas y simulacros (incluyendo pruebas de phishing) para medir la efectividad del plan.
- Responsable: El diseño y ejecución estará a cargo de la Dependencia TI en coordinación con Talento Humano.

6.5 Política de Auditoría Interna

- Objetivo: Comprobar la efectividad de los controles establecidos, asegurar el cumplimiento de las políticas y detectar oportunidades de mejora continua.

- Plan de Auditoría: Se elaborará un plan anual de auditorías que cubra procesos críticos, con base en los resultados de la gestión de riesgos.
- Independencia: Los auditores no podrán revisar procesos en los que participen directamente. Podrán ser personal interno capacitado o auditores externos.

- Informes y Seguimiento: Los hallazgos deberán quedar documentados en informes formales, incluyendo las acciones correctivas, cuyo cumplimiento será verificado hasta su cierre.
- Responsable: La Alta Dirección aprobará el plan anual, garantizando cobertura y frecuencia adecuadas.

    - Ejecución: Las auditorías estarán a cargo de la Dependencia TI, siempre que el personal auditor posea certificaciones en ISO/IEC 27001:2022 o experiencia equivalente; de lo contrario, se recurrirá a un auditor externo acreditado.
    - Auditoría Independiente: La Revisoría Fiscal revisará anualmente el área de TI en el marco de su función de control sobre los estados financieros, incluyendo la verificación de controles de seguridad de la información.
    - Acciones Correctivas: Los líderes de área deberán implementar las medidas necesarias para subsanar los hallazgos en los plazos establecidos.

6.6 Política de Respuesta ante Incidentes de Seguridad.

- Objetivo: Definir un esquema de actuación frente a incidentes de seguridad para contenerlos, erradicarlos y recuperar los servicios en el menor tiempo posible.

- Clasificación y Reporte: Todo incidente deberá ser reportado de inmediato a la Dependencia TI, la cual los clasificará según niveles de criticidad (bajo, medio, alto, crítico).
- Contención y Erradicación: TI será responsable de contener el incidente y eliminar sus causas.
- Lecciones Aprendidas: Cada incidente grave será objeto de análisis para implementar controles preventivos.
- Simulacros: Al menos una vez al año se realizarán ejercicios prácticos de respuesta para validar el plan.
- Responsables: La Alta Dirección asignará los recursos para su ejecución; la Dependencia TI gestionará el plan y cada empleado será responsable de reportar incidentes oportunamente.

6.7 Política de Continuidad del Negocio y Recuperación ante Desastres.

Objetivo: Asegurar la disponibilidad y rápida recuperación de los sistemas críticos y procesos esenciales en caso de interrupciones.

- Planes de Continuidad: Se implementarán planes específicos para continuidad operativa y recuperación ante desastres.
- Pruebas: Los planes deberán validarse mediante simulacros al menos una vez al año.
- Responsables: La Alta Dirección aprobará la estrategia general, la Dependencia TI se encargará de los planes técnicos y los líderes de proceso de los planes operativos.

6.8 Política de Indicadores y Medición del Desempeño

Objetivo: Evaluar de manera objetiva la eficacia del SGSI y el grado de cumplimiento de las políticas mediante indicadores cuantitativos.

- Indicadores: Se establecerán métricas como número y tiempo de respuesta a incidentes, cumplimiento de capacitaciones, resultados de auditorías y porcentaje de riesgos gestionados.
- Reportes: Se elaborarán informes trimestrales para la Alta Dirección, que servirán de base para la toma de decisiones estratégicas.
- Responsable: La Dependencia TI recopilará la información, calculará los indicadores y emitirá los reportes.

6.9 Política de Desarrollo Seguro y Administración de Activos.

Objetivo: Garantizar que todo el ciclo de vida de los sistemas de información, desde su diseño hasta su operación, contemple criterios de seguridad.

- Seguridad desde el Diseño: Todo proyecto de TI deberá incorporar medidas de seguridad desde la fase inicial.
- Entornos de Prueba: Los datos productivos no podrán utilizarse en pruebas; en caso de ser indispensable, deberán anonimizarse previamente.
- Gestión de Vulnerabilidades: Se adoptará un proceso sistemático para identificar, evaluar y remediar vulnerabilidades técnicas conforme al plan de riesgos de Telecafé Ltda.
- Responsable: La Dependencia TI establecerá los lineamientos técnicos y supervisará su cumplimiento.

6.10 Política de Compromiso de la Alta Dirección.

Objetivo: Formalizar el liderazgo de la Alta Dirección en la implementación, seguimiento y mejora continua del PSPI.

- Aprobación Formal: La Alta Dirección aprobará y firmará el PSPI y sus políticas asociadas.
- Revisión: El plan será evaluado en sesiones semestrales de revisión de desempeño.
- Asignación de Recursos: La gerencia garantizará los recursos financieros, humanos y tecnológicos necesarios.
- Promoción: La Alta Dirección fomentará una cultura de seguridad en toda la organización.

7. Monitoreo, Revisión y Mejora Continua

El PSPI contará con un esquema permanente de seguimiento que permita medir su efectividad, identificar áreas de mejora y adaptarse a los cambios normativos, tecnológicos y operativos.

- Objetivo: Establecer un sistema estructurado de monitoreo y revisión que garantice la actualización y pertinencia del PSPI frente a nuevos riesgos y cambios del entorno.

7.1 Actividades de Monitoreo y Seguimiento.

El éxito y sostenibilidad del Plan de Seguridad y Privacidad de la Información (PSPI) de Telecafé Ltda. dependen no solo de su diseño e implementación inicial, sino también de la capacidad de la organización para mantenerlo actualizado, evaluar su efectividad y ajustarlo frente a los cambios

internos y externos. En este sentido, el monitoreo y seguimiento constituyen pilares fundamentales para garantizar la mejora continua del sistema, permitiendo identificar de manera temprana desviaciones, incidentes o riesgos que puedan comprometer la seguridad de la información y la continuidad de las operaciones.

Estas actividades están orientadas a evaluar, de manera sistemática y periódica, tanto el desempeño del PSPI como la eficacia de los controles implementados, el cumplimiento normativo y la adaptación frente a nuevas condiciones del entorno tecnológico, legal y organizacional. Con ello, se busca no solo mitigar riesgos, sino también fortalecer la cultura de seguridad en toda la entidad y asegurar que las decisiones estratégicas de la Alta Dirección se fundamenten en información confiable y oportuna.

El proceso de monitoreo abarca la revisión de indicadores clave de desempeño, la verificación continua de la efectividad de controles técnicos y administrativos, así como el análisis de cambios regulatorios, tecnológicos y operativos que impacten directamente la gestión de seguridad de la información. De esta forma, el seguimiento se convierte en un ejercicio integral que involucra a las distintas áreas de la organización bajo la coordinación de la Dependencia de TI, con el apoyo de los líderes de proceso, el área jurídica y la Alta Dirección.

Qué se monitorea	Cómo se monitorea	Frecuencia	Responsable
Indicadores de Desempeño (KPIs)	Reportes de avance, dashboards, sistema de gestión de incidentes.	Mensual / Trimestral	Dependencia TI
Cumplimiento del plan de acción.			
Número y tipo de incidentes de seguridad.			
% de riesgos tratados.			
-- Resultados de capacitaciones.			
Efectividad de Controles	Auditorías automáticas, revisiones de logs, encuestas de cumplimiento.	Continuo / Trimestral	Dependencia TI / Líderes de área
Estado de los controles técnicos (firewalls, antivirus, backups).			

Cumplimiento de políticas por parte del personal.			
Cambios en el Entorno	Revisión de fuentes externas, análisis de impacto ante cambios.	Semestral	Jurídica / TI / Alta Dirección
Nuevas leyes o regulaciones.			
Nuevas tecnologías implementadas.			
-- Cambios en procesos operativos.			

7.2 Revisiones Formales del PSPI

Para garantizar que el Plan de Seguridad y Privacidad de la Información (PSPI) de Telecafé Ltda. se mantenga vigente, pertinente y alineado con las necesidades estratégicas de la organización, resulta indispensable establecer un mecanismo de revisiones formales y periódicas. Estas revisiones no solo permiten evaluar de manera integral la efectividad del plan, sino también identificar oportunidades de mejora, anticipar riesgos emergentes y asegurar la disponibilidad de los recursos necesarios para su sostenibilidad.

El proceso de revisión formal constituye una herramienta de control y retroalimentación, mediante la cual la Alta Dirección, junto con los responsables técnicos y operativos, analiza el desempeño del PSPI desde diferentes perspectivas: cumplimiento de auditorías, gestión de incidentes, avance de indicadores, cambios en el entorno regulatorio y tecnológico, así como la adecuación del alcance y los objetivos del plan.

De igual manera, se realizan revisiones específicas sobre la gestión de riesgos, orientadas a verificar la identificación de nuevas amenazas, la eficacia de los controles aplicados y la actualización del nivel de tolerancia al riesgo definido por la organización. De esta forma, las revisiones formales garantizan que el PSPI no sea un documento estático, sino un instrumento dinámico en permanente evolución, capaz de responder con agilidad a los retos del entorno digital y normativo.

Tipo de Revisión	Participantes	Frecuencia	Temas a Revisar
Revisión por la Dirección	Alta Dirección, Líder de TI, Coordinadores de áreas críticas.	Anual (o cuando sea necesario)	- Resultados de auditorías. - Estado de incidentes de seguridad.

			- Desempeño de los indicadores.
			- Adecuación del alcance del PSPI.
			- Cambios en el contexto de la organización.
			- Recursos necesarios para el PSPI.
Revisión de Riesgos	Dependencia TI, Líderes de proceso.	Anual (o ante cambios significativos)	- Nuevos riesgos identificados.
			- Efectividad del plan de tratamiento de riesgos.
			- Actualización del apetito de riesgo.

7.3 Mecanismos de Mejora Continua

El fortalecimiento del Plan de Seguridad y Privacidad de la Información (PSPI) de Telecafé Ltda. requiere que este no sea concebido como un esquema estático, sino como un sistema dinámico capaz de adaptarse a los cambios tecnológicos, regulatorios y organizacionales. Para lograrlo, se adopta un enfoque de mejora continua, el cual permite revisar, ajustar y perfeccionar de manera sistemática los procesos, controles y políticas que conforman el plan, garantizando su vigencia y efectividad en el tiempo.

Este proceso se desarrolla bajo la metodología del ciclo PHVA (Planificar – Hacer – Verificar – Actuar), reconocida internacionalmente como una herramienta de gestión para la excelencia operativa. A través de este ciclo, se asegura que las lecciones aprendidas de auditorías, incidentes de seguridad, revisiones directivas y retroalimentación del personal sean convertidas en acciones concretas de mejora, con responsables y plazos definidos.

De igual manera, se promueve la verificación periódica de la efectividad de dichas acciones mediante indicadores y evaluaciones objetivas, lo que permite determinar su impacto real y estandarizar las prácticas más exitosas dentro de la organización. Cuando los resultados no cumplen con lo esperado, el ciclo se reinicia, lo que garantiza un proceso de ajuste permanente y de aprendizaje organizacional.

En este sentido, los mecanismos de mejora continua representan una pieza esencial del PSPI, ya que aseguran que Telecafé Ltda. no solo responda de manera reactiva a los riesgos, sino que también

anticipe los cambios y evolucione de manera proactiva frente a los retos que impone la seguridad y privacidad de la información.

7.4 Acciones Correctivas y Preventivas

Con el fin de garantizar la eficacia del Plan de Seguridad y Privacidad de la Información (PSPI) y fortalecer el sistema de gestión, se establece el siguiente marco de actuación:

- Todas las acciones correctivas derivadas de incidentes, no conformidades o hallazgos provenientes de auditorías internas y externas deberán ser registradas formalmente, asignando responsables, plazos y recursos necesarios. Su seguimiento se mantendrá activo hasta comprobar su cierre efectivo mediante evidencias verificables.
- Se promoverá la identificación temprana de acciones preventivas, orientadas a anticipar y mitigar posibles riesgos o desviaciones que puedan comprometer la seguridad de la información. Estas acciones estarán alineadas con la cultura de mejora continua, buscando minimizar la probabilidad de ocurrencia de incidentes y reforzar la resiliencia institucional.

De esta forma, el sistema no solo responde a los problemas existentes, sino que también desarrolla una capacidad proactiva para prevenir contingencias, asegurando la protección integral de los activos de información y la sostenibilidad operativa de Telecafé Ltda.

7.5 Comunicación y Documentación

Para asegurar la transparencia y la efectividad del proceso de mejora continua, se implementarán los siguientes lineamientos:

- Los resultados obtenidos en las revisiones periódicas, el estado de los indicadores de desempeño y los avances en la ejecución de las acciones de mejora serán comunicados de manera oportuna a los actores clave de la organización, incluyendo a la Alta Dirección, líderes de proceso y demás responsables vinculados con la seguridad de la información.
- Todo el ciclo de mejora continua deberá quedar debidamente documentado, incorporando evidencias de las revisiones realizadas, registros de seguimiento y comprobantes de las acciones implementadas. Esta documentación garantizará la trazabilidad del sistema, facilitará la verificación por parte de auditores internos o externos y respaldará la toma de decisiones estratégicas orientadas a la protección de los activos de información.

De esta manera, la comunicación clara y la documentación sistemática se consolidan como herramientas esenciales para mantener la confianza institucional, fomentar la rendición de cuentas y fortalecer la cultura de seguridad en Telecafé Ltda.

8. Disposiciones Finales.

La presente política, lineamientos y directrices establecidas en el Plan de Seguridad y Privacidad de la Información (PSPI) de Telecafé Ltda. constituyen un marco obligatorio de referencia para toda la

organización. Su implementación busca garantizar la protección integral de los activos de información, el cumplimiento del marco normativo vigente y la continuidad de las operaciones institucionales.

En este sentido, se establecen las siguientes disposiciones:

1. Aprobación y Socialización: El contenido del PSPI deberá ser revisado y aprobado formalmente por la Gerencia General, y posteriormente socializado con todos los niveles de la organización, asegurando que cada funcionario, contratista y tercero conozca las responsabilidades derivadas de estas políticas.
2. Incorporación al Sistema de Gestión: Las políticas y procedimientos definidos serán integrados al Sistema de Gestión de la Calidad de Telecafé Ltda., bajo el código correspondiente, con el fin de mantener coherencia con el marco documental institucional.
3. Carácter Obligatorio: El cumplimiento de estas disposiciones es de carácter obligatorio para todas las personas que interactúan con los activos de información de la entidad, sin excepción, quedando sujetas a las sanciones y medidas disciplinarias previstas en la normativa interna y legal aplicable.
4. Auditoría y Seguimiento: El cumplimiento de las políticas será objeto de verificación en auditorías internas y externas, así como en los procesos de control implementados por la organización, asegurando la mejora continua y la efectividad del plan.
5. Actualización: Estas políticas deberán revisarse y actualizarse de manera periódica, o cuando se presenten cambios normativos, tecnológicos u organizacionales que impacten la seguridad y privacidad de la información.

Con estas disposiciones finales, Telecafé Ltda. reafirma su compromiso con la seguridad, la transparencia y la confianza pública, asegurando que la información institucional se gestione con responsabilidad, solidez técnica y respaldo legal.