telecafé
Expresión de lo nuestro

POLÍTICA DE TI

www.telecafe.gov.co
@canaltelecafe

Código: TEI-PRO-15
FECHA: 8 de noviembre de 2024
Versión: 01
SISTEMA INTEGRADO DE GESTIÓN

telecafé

Contenido

1.INTRODUCCIÓN

En un entorno audiovisual en constante evolución, la tecnología se ha convertido en el motor que impulsa la innovación y el crecimiento de Telecafé Ltda. Esta Política de Tecnología de la Información (TI) establece las pautas para la gestión eficaz y eficiente de nuestros recursos tecnológicos, con el objetivo de maximizar su potencial y asegurar la continuidad de nuestras operaciones. Desde la producción de contenido hasta la distribución digital, la dependencia TI desempeña un papel fundamental en cada uno de nuestros procesos, es por eso que esta política busca garantizar que sea un aliado estratégico para el logro de los objetivos organizacionales.

2.VISIÓN GENERAL

Telecafé Ltda. se posicionará como líder en la transformación digital del sector audiovisual en Colombia, utilizando la tecnología para innovar constantemente y ofrecer una mejor experiencia para el usuario. A través de esta política, se busca fomentar una cultura de innovación y colaboración, donde la tecnología sea un habilitador clave para el crecimiento y el desarrollo de la organización.

3.OBJETIVO GENERAL

El objetivo de la política TI de Telecafé Ltda., es transformar a la organización en un referente capaz de ofrecer experiencias únicas a sus usuarios, optimizar sus operaciones y contribuir al desarrollo de la región, adoptando medidas de eficiencia energética y de seguridad informática para preservar la confidencialidad, integridad y disponibilidad de la información. Lo anterior incluye proteger la información de los clientes, empleados y socios comerciales de la entidad, así como los equipos y servicios tecnológicos utilizados en sus operaciones.

3.1 Objetivos específicos

I. Establecer procedimientos claros y efectivos para la clasificación y manejo de la información.
1. Desarrollar un sistema de clasificación de información que defina niveles de sensibilidad y protocolos específicos para cada proceso.
2. Implementar un registro de acceso y modificación de la información sensible, asegurando trazabilidad.
3. Crear un manual de procedimientos para el manejo de información clasificada y su divulgación controlada.

II. Implementar medidas de seguridad adecuadas para controlar el acceso a la información.
1. Establecer un sistema de autenticación para el acceso a información crítica.
2. Definir roles y permisos de acceso basados en la necesidad de información para el desempeño de funciones laborales.

3. Realizar auditorías periódicas de accesos para detectar y corregir posibles brechas de seguridad.

III. Optimizar la Infraestructura de TI mediante equipos energéticamente eficientes.
1. Realizar, mantener y actualizar un inventario de servidores y equipos de red para identificar oportunidades de consolidación.
2. Implementar virtualización de servidores para reducir la cantidad de hardware físico y consumo energético.
3. Monitorear y reportar el consumo energético de la infraestructura de TI mensualmente para evaluar mejoras.
4. Implementar la inclusión de certificaciones de eficiencia energética en la adquisición o alquiler de equipos:
a) Realizar estudios previos y/o descripción de las necesidades antes de la cotización de servicios y equipos.
b) Incluir la certificación Energy Star como un requisito indispensable en las cotizaciones.
c) Evaluar proveedores para asegurar que ofrezcan equipos con certificación de eficiencia energética

IV. Configurar dispositivos de TI para operar en modos de bajo consumo.
1. Establecer configuraciones predeterminadas de bajo consumo para todos los dispositivos de TI.
2. Implementar un programa de apagado automático que se active fuera del horario laboral.
3. Informar a los empleados sobre las configuraciones de ahorro de energía y su importancia.

V. Establecer un ciclo de renovación de hardware.
1. Definir criterios claros para la obsolescencia tecnológica y eficiencia energética en la selección de nuevos equipos.
2. Desarrollar un calendario de renovación para asegurar la actualización regular de hardware.

VI. Proporcionar capacitación regular a empleados sobre seguridad de la información.
1. Desarrollar un plan de capacitación anual que incluya módulos sobre seguridad de la información.
2.Crear materiales de capacitación accesibles para el personal sobre mejores prácticas.
3. Realizar evaluaciones post-capacitación para medir el entendimiento y aplicación de los temas tratados.

VII. Lanzar campañas internas para fomentar el ahorro de energía y el uso seguro de sistemas.
1. Diseñar y ejecutar campañas de concienciación sobre prácticas de ahorro energético y seguridad informática.

2. Monitorear y reportar los resultados de las campañas para evaluar su efectividad.
3. Establecer incentivos para equipos o departamentos que demuestren mejoras en el ahorro energético y seguridad.

VIII. Fomentar el uso de videoconferencias y herramientas de colaboración.
1. Utilizar plataformas para realizar videoconferencias, chats internos y herramientas colaborativas en la empresa.
2. Promover políticas de uso de herramientas digitales en lugar de reuniones presenciales.
3. Evaluar el impacto en costos y emisiones de carbono del uso de estas herramientas anualmente.

IX. Promover la impresión a doble cara y la reducción del consumo de papel.
1. Implementar políticas de impresión sostenible que incluyan impresión a doble cara y restricciones de color.
2. Fomentar la digitalización de documentos y el uso de sistemas de gestión documental.
3. Monitorear y reportar el consumo de papel mensualmente para identificar oportunidades de reducción.

X. Realizar capacitaciones sobre buenas prácticas en herramientas de Google Workspace.
1. Desarrollar un programa de capacitación específico para el uso eficiente de Google Workspace.
2. Evaluar el uso de herramientas post-capacitación para medir la eficiencia y adopción.

XI. Asegurar que los sistemas críticos tengan planes de contingencia.
1. Desarrollar un plan de contingencia y recuperación ante desastres para todos los sistemas críticos.
2. Realizar simulacros anuales para evaluar la efectividad de los planes de contingencia.
3. Actualizar los planes de contingencia en función de las lecciones aprendidas de los simulacros y auditorías.

XII. Establecer procedimientos de respuesta ante incidentes de seguridad.
1. Desarrollar un manual de procedimientos de respuesta que incluya todos los pasos desde la identificación hasta la recuperación.
2. Realizar simulacros de respuesta a incidentes para preparar al personal.
3. Revisar y actualizar los procedimientos anualmente basándose en los incidentes ocurridos y las mejores prácticas.

XIII. Realizar auditorías y revisiones periódicas de políticas de TI.
1. Establecer un calendario de auditorías para revisar políticas y procedimientos de seguridad de la información.
2. Definir métricas de efectividad que se usarán durante las auditorías.
3. Implementar un proceso de mejora continua basado en los hallazgos de las auditorías.

XIV. Asegurar el cumplimiento de normativas legales y regulaciones.
1. Realizar un análisis de las normativas aplicables y cómo afectan las políticas de TI de Telecafé Ltda.
2. Desarrollar un programa de capacitación sobre cumplimiento normativo para empleados.
3. Implementar un marco normativo para garantizar que las políticas de TI se mantengan alineadas con las regulaciones cambiantes y sus actualizaciones.

4. ALCANCE DE LAS POLÍTICAS

La política de TI de Telecafé Ltda. se aplica a todo el canal y a todas las partes interesadas, abarcando los activos de información y procesos de negocio. Incluye a todos los empleados, contratistas y pasantes que utilicen recursos informáticos, así como dispositivos electrónicos y redes internas o externas. Su objetivo es proteger la información confidencial y los activos tecnológicos en todos los niveles de la organización, garantizando una cobertura integral para la seguridad de la información.

5. MARCO LEGAL Y NORMATIVO

El marco legal y normativo de la política de TI de Telecafé Ltda. se establece para garantizar que todas las operaciones tecnológicas y de información se realicen en cumplimiento con las leyes y regulaciones aplicables. Este marco incluye normativas sobre protección de datos, derechos de autor, seguridad de la información y uso de tecnologías de la información. Al alinearse con estos requisitos legales, Telecafé Ltda. no solo protege su información y activos tecnológicos, sino que también fomenta la confianza entre sus empleados, colaboradores y la audiencia. Este enfoque proactivo es fundamental para mitigar riesgos legales y garantizar la sostenibilidad y la responsabilidad social de la organización en el entorno digital actual.

5.1 Leyes y Normativas que aplican a la dependencia TI de la entidad.

A continuación, se plantean las normas actuales que influyen sobre esta política:

a) LEY 23 DE 1982 sobre Derechos de Autor. Congreso de la República. Disponible en Línea http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=3431 [Recuperado en enero de 2017]

b) CONSTITUCIÓN POLÍTICA DE COLOMBIA 1991; Artículo 15. “Todas las
a. personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. Disponible en Línea: http://www.constitucioncolombia.com/titulo-2/capitulo- 1/articulo-15 [Recuperado en enero de 2017]

c) LEY 527 DE 1999; por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. Disponible en Línea: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276 [Recuperado en enero de 2017]

d) LEY 1266 DE 2008, por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. Disponible en Línea: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34488 [Recuperado en enero de 2017].

e)LEY 1273 DE 2009, Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Disponible en Línea:http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492 [Recuperado en enero de 2017]

f)LEY ESTATUTARIA 1581 DE 2012, Por la cual se dictan disposiciones generales para la protección de datos personales. Congreso de la República. Disponible en Línea: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981. [Recuperado en enero de 2017]

g)DECRETO 2609 DE 2012. Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado".Disponible en Línea: http://www.mintic.gov.co/portal/604/articles3528_documento.pdf [Recuperado en enero de 2017]

h) DECRETO 2693 DE 2012 Estrategia de Gobierno en Línea. Ministerio de Tecnologías de la Información y las comunicaciones. Disponible en Línea: http://www.mintic.gov.co/portal/604/articles-3586_documento.pdf [Recuperado en enero de 2017].

La dependencia TI debe implementar un normograma que permita el análisis y actualización de las normas, donde se evidencie el grado de cumplimiento, el nivel de aplicación y los planes de cumplimiento de las normas dentro de la entidad, salvaguardando así a la entidad de cualquier incumplimiento a la normativa por desconocimiento de las leyes.

6. GLOSARIO

Acceso no autorizado: Entrada o uso de sistemas, datos o recursos sin el debido permiso.

Acceso no autorizado: Entrada o uso de sistemas, datos o recursos sin el debido permiso.

Activo TI: Es cualquier elemento tangible o intangible relacionado con la tecnología de la información que una organización posee y utiliza para llevar a cabo sus operaciones.

Área y personal de TI: grupo de personas dentro de la entidad encargados del diseño, implementación y establecimientos de las políticas de seguridad de la información, así como la administración, mantenimiento, y todo lo relacionados con las TIC.

Ataque cibernético: intento de penetración de un sistema informático por parte de un usuario no deseado ni autorizado a accederlo, por lo general con intenciones insanas y perjudiciales.

Autenticación: Proceso para confirmar la identidad de un usuario, dispositivo o entidad antes de permitirle el acceso a recursos del sistema.

Autenticación: Proceso para confirmar la identidad de un usuario, dispositivo o entidad antes de permitirle el acceso a recursos del sistema.

Autorización: Determinación de los permisos o niveles de acceso otorgados a un usuario dentro de un sistema.

Autorización: Determinación de los permisos o niveles de acceso otorgados a un usuario dentro de un sistema.
Backup (Copia de seguridad): Creación de duplicados de datos para su preservación y recuperación en caso de pérdida o daño.

Backup (Copia de seguridad): Creación de duplicados de datos para su preservación y recuperación en caso de pérdida o daño.

Brecha de seguridad: deficiencia de algún recurso informático o telemático que pone en riesgo los servicios de información o expone la información en sí misma, sea o no protegida por reserva legal.

Bug: Error en la codificación de un programa que provoca inconvenientes diversos al usuario. En la actualidad se realiza un control de calidad exhaustivo de las aplicaciones mediante beta-testers que prueban el programa durante meses en todas las situaciones imaginables, con el objetivo de detectar la presencia de bugs. Debido a la complejidad de las aplicaciones actuales, es casi imposible depurar totalmente un programa, que suele incluir siempre algún bug, que puede producir un efecto indeseado en determinadas ocasiones.

Ciberseguridad: Prácticas y tecnologías destinadas a proteger sistemas, redes y datos de ataques digitales.

Ciberseguridad: Prácticas y tecnologías destinadas a proteger sistemas, redes y datos de ataques digitales.

Clave: contraseña, clave o password es una forma de autentificación que utiliza información secreta para controlar el acceso hacia algún recurso. La contraseña debe mantenerse en secreto ante aquellos a quien no se le permite el acceso. A aquellos que desean acceder a la información se les solicita una clave; si conocen o no conocen la contraseña, se concede o se niega el acceso a la información según sea el caso. En ocasiones clave y contraseña se usan indistintamente. (Asimismo llamado PIN - Personal Identificación Number).

Confidencialidad: Garantía de que la información solo esté disponible para personas con autorización.

Confidencialidad: Garantía de que la información solo esté disponible para personas con autorización.

Control de acceso: Medidas para asegurar que el acceso a recursos de información se ajuste a las políticas establecidas.

Control de acceso: Medidas para asegurar que el acceso a recursos de información se ajuste a las políticas establecidas.

Criptografía: Uso de técnicas para proteger la información mediante la transformación de datos en un formato que solo pueden leer personas autorizadas.

Criptografía: Uso de técnicas para proteger la información mediante la transformación de datos en un formato que solo pueden leer personas autorizadas.

Disponibilidad de la información: La disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. A groso modo, la disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran.

Disponibilidad: Asegurar que la información y los recursos estén accesibles y utilizables por usuarios autorizados cuando se necesiten.

Disponibilidad: Asegurar que la información y los recursos estén accesibles y utilizables por usuarios autorizados cuando se necesiten.

Dominio: El sistema de nombres de dominio (DNS) es un sistema para asignar nombres a equipos y servicios de red que se organiza en una jerarquía de dominios. DNS proporciona un espacio de nombres jerárquico, lo que garantiza que cada nombre de host será único en una red de área local o extensa.

Evaluación de riesgos: Identificación, análisis y evaluación de riesgos potenciales para la información y los sistemas de información.

Evaluación de riesgos: Identificación, análisis y evaluación de riesgos potenciales para la información y los sistemas de información.

Firewall (Cortafuegos): Sistema de seguridad de red que monitorea y controla el tráfico de entrada y salida basado en reglas de seguridad preestablecidas.

Firewall (Cortafuegos): Sistema de seguridad de red que monitorea y controla el tráfico de entrada y salida basado en reglas de seguridad preestablecidas.

Hardware: Conjunto de los componentes que integran la parte material de una computadora.

Información: Puede existir en muchas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, presentada en imágenes, o expuesta en una conversación. Cualquiera sea la forma que adquiere la información, o los medios por los cuales se distribuye o almacena, siempre debe ser protegida en forma adecuada.

Integridad: Garantizar que la información no ha sido modificada de manera no autorizada y se mantiene completa y precisa.

Integridad: Garantizar que la información no ha sido modificada de manera no autorizada y se mantiene completa y precisa.

Internet: Red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación.

Log: Archivo que registra movimientos y actividades de un determinado programa (log file). En un servidor web, se encarga de guardar todos los requerimientos (“requests”) y servicios entregados desde él, por lo que es la base del software de estadísticas de visitas.
Malware (Software malicioso): Programas diseñados para infiltrarse o dañar sistemas de información sin el consentimiento del usuario.

Malware (Software malicioso): Programas diseñados para infiltrarse o dañar sistemas de información sin el consentimiento del usuario.

Malware: El malware es la descripción general de un programa informático que tiene efectos no deseados o maliciosos. Incluye virus, gusanos, troyanos y puertas traseras. El malware a menudo utiliza herramientas de comunicación populares, como el correo electrónico y la mensajería instantánea, y medios magnéticos extraíbles, como dispositivos USB, para difundirse. También se propaga a través de descargas inadvertidas y ataques a las vulnerabilidades de seguridad en el software. La mayoría del malware peligroso actualmente busca robar información personal que pueda ser utilizada por los atacantes para cometer fechorías.

No repudio: este mecanismo genera registros especiales con alcances de "prueba judicial" acerca de que el contenido del mensaje de datos es la manifestación de la voluntad del firmante y que se atiene a las consecuencias de su decisión.

Phishing: Técnica de engaño para obtener información confidencial, como nombres de usuario, contraseñas y datos de tarjetas de crédito, haciéndose pasar por una entidad confiable.

Phishing: Técnica de engaño para obtener información confidencial, como nombres de usuario, contraseñas y datos de tarjetas de crédito, haciéndose pasar por una entidad confiable.

Política de seguridad: Conjunto de normas y directrices destinadas a proteger la información y los sistemas de una organización.

Política de seguridad: Conjunto de normas y directrices destinadas a proteger la información y los sistemas de una organización.

Política: son instrucciones a manera de mandato que indican la intención de la alta gerencia respecto a la operación de la organización.

Protección de datos: Medidas y procesos para salvaguardar la información contra pérdida, robo o daño.

Protección de datos: Medidas y procesos para salvaguardar la información contra pérdida, robo o daño.

Recuperación ante desastres: Estrategias y procedimientos para restaurar sistemas, datos y operaciones críticas tras una interrupción significativa.

Recuperación ante desastres: Estrategias y procedimientos para restaurar sistemas, datos y operaciones críticas tras una interrupción significativa.

Recurso Informático: Elementos informáticos (base de datos, sistemas operacionales, redes, sistemas de información y comunicaciones) que facilitan servicios informáticos, y que operan en los computadores del Canal.

Redundancia: Implementación de componentes adicionales para asegurar la continuidad operativa en caso de fallos del sistema principal.

Seguridad de la información: Prácticas y tecnologías para proteger la información contra acceso no autorizado, alteración, destrucción o divulgación.

Seguridad de la información: Prácticas y tecnologías para proteger la información contra acceso no autorizado, alteración, destrucción o divulgación.

Servicio: Es el conjunto de acciones o actividades de carácter misional diseñadas para incrementar la satisfacción del usuario, dándole valor agregado a las funciones de la entidad.

Software: Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora.

TI: Tecnologías de la información.

Usuarios Terceros: Todas aquellas personas naturales o jurídicas, que no son funcionarios del Canal, pero que por las actividades que realizan en el Canal, deban tener acceso a Recursos Informáticos.

Vulnerabilidad: Debilidad en un sistema que puede ser explotada para causar daño o acceso no autorizad.

Vulnerabilidad: Debilidad en un sistema que puede ser explotada para causar daño o acceso no autorizado.

Warez: se refiere principalmente al material bajo copyright distribuido con infracción al derecho de autor.

7. DESARROLLO DE LA POLÍTICA

Se presentan los lineamientos adoptados por la entidad para el uso, administración y gestión de los sistemas de información enmarcados en los siguientes ítems que serán desarrollados a continuación:

7.1 Cláusula de confidencialidad.

El colaborador que desarrolla las funciones en la dependencia TI se compromete a guardar absoluta y estricta confidencialidad respecto de toda la información a la que tenga acceso durante el desarrollo de sus funciones, incluyendo: información técnica, comercial, financiera, estratégica, de clientes, proveedores y demás que considerada confidencial por Telecafé Ltda. dentro de las políticas de la entidad.
Este compromiso de confidencialidad se encuentra respaldado por las disposiciones legales colombianas, en particular la Ley 1581 de 2012 (Protección de Datos Personales), el Código de Comercio (Secretos empresariales), y la Constitución Política de Colombia (Derecho al honor y a la buena reputación).

a) Obligaciones del colaborador:
1. Mantener la confidencialidad: El colaborador deberá mantener la confidencialidad de toda la información a la que tenga acceso, incluso después de finalizada la relación laboral.
2. No divulgar: El trabajador no podrá divulgar, revelar o compartir la información confidencial con terceros, bajo ninguna circunstancia.
3. Uso adecuado de la información: El colaborador solo podrá utilizar la información confidencial para el desempeño de sus funciones y en beneficio de Telecafé Ltda.
4. Proteger la información: El colaborador deberá tomar todas las medidas necesarias para proteger la confidencialidad de la información, evitando su pérdida, daño o acceso no autorizado.

b) Consecuencias del incumplimiento:
El incumplimiento de esta cláusula de confidencialidad dará lugar a las acciones legales pertinentes, incluyendo, una indemnización por los daños y perjuicios causados a Telecafé Ltda., así como a las sanciones penales a que haya lugar conforme a la legislación colombiana.

c) Resolución de conflictos:
Cualquier controversia que surja en relación con el cumplimiento de esta cláusula será sometida a un proceso de conciliación previa. En caso de no llegar a un acuerdo, las partes se someten a la jurisdicción de los jueces y tribunales competentes.

7.2 Acceso a la información

Los funcionarios públicos, contratistas y pasantes del Canal, personal temporal y otras personas relacionadas con terceras partes, deben tener acceso a la información necesaria para el desarrollo de sus actividades. En el caso de personas ajenas a la institución, el Coordinador Administrativo y Financiero o el Coordinador de Área responsable de generar la información, debe autorizar el acceso de acuerdo con el trabajo realizado por estas personas con previa justificación.

a. Una vez que el trabajador deja de prestar servicios al Canal, se le retirarán de manera inmediata todas las autorizaciones para utilizar los sistemas de información de la empresa.

b. Cuando se presenten eventos que pongan en riesgo la integridad, veracidad y consistencia de la información, la dependencia de TI deberá documentar y realizar las acciones que conlleven a su solución.

7.3 Responsabilidades frente a la seguridad de la información.

La apropiación de todos los actores en el proceso de cuidado de los activos de información, es lo que permite que se fortalezca el concepto dentro de la organización a fin de que se genere una estructura y conceptualización de la importancia de la participación activa de cada agente para cumplir con dicho

propósito. Es por ello que se describen las responsabilidades de cada grupo de la siguiente forma:

7.3.1 Responsabilidades de la dependencia TI frente a la gestión de la información

La dependencia TI de Telecafé Ltda. es el responsable principal de la gestión integral de la información del canal, con autoridad para supervisar, proteger y controlar todos los aspectos relacionados con la recolección, almacenamiento, procesamiento, distribución y eliminación de la información, asegurando su seguridad, disponibilidad, integridad y confidencialidad.

a. Custodia y Protección de la Información
1) La dependencia TI es responsable de garantizar la custodia de todos los datos almacenados en los sistemas tecnológicos de Telecafé Ltda.
2) Implementar mecanismos de control que aseguren la protección contra pérdidas, accesos no autorizados, manipulación indebida o cualquier tipo de riesgo que comprometa la integridad de la información

b. Clasificación de la Información
1) La dependencia TI debe clasificar la información según su nivel de sensibilidad y criticidad (pública, interna, confidencial y crítica).
2) Asegurar que la información más crítica esté sujeta a los niveles más altos de seguridad, control de acceso y monitoreo constante.

c. Control de Acceso
1) La dependencia TI es el único responsable de asignar y gestionar los permisos de acceso a la información, asegurándose de que solo el personal autorizado pueda acceder a ciertos niveles de datos.
2) Implementar sistemas de autenticación robustos para validar la identidad de los usuarios que accedan a la información crítica.

d. Seguridad de la Información
1) La dependencia TI es responsable de implementar políticas y tecnologías que garanticen la protección contra amenazas cibernéticas y la prevención de accesos no autorizados, virus, malware y otras vulnerabilidades.
2) Asegurar que se realicen evaluaciones de seguridad periódicas y pruebas de penetración para identificar y corregir fallos en los sistemas.

e. Respaldo y Recuperación de Datos
1) Implementar un plan de respaldo regular de la información, asegurando que todos los datos relevantes estén protegidos y puedan ser recuperados en caso de incidentes o desastres.
2) Diseñar un plan de recuperación ante desastres (DRP) que incluya la restauración de la infraestructura y datos críticos en el menor tiempo posible.

f. Supervisión y Auditoría
1) La dependencia TI debe realizar auditorías internas periódicas para garantizar el cumplimiento de los estándares de seguridad de la información y detectar cualquier posible fallo o incumplimiento.
2) Se establecerán procedimientos para la revisión continua del uso, acceso y tratamiento de la información por parte de todo el personal de la organización.

7.3.1.2 Delegación de Responsabilidades
Aunque la dependencia TI es el propietario principal de la información, puede delegar algunas responsabilidades específicas en otros departamentos, siempre bajo su supervisión y control, garantizando que el manejo de la información esté alineado con las políticas generales de seguridad de la organización.

7.3.1.3 Cumplimiento de Normativas
La dependencia TI debe garantizar que el manejo de la información cumpla con las regulaciones locales e internacionales aplicables, como la Ley de Protección de Datos Personales de Colombia (Ley 1581 de 2012) y los estándares aplicables en la industria de medios y telecomunicaciones, para ello deberá manejar un marco normativo donde especifique la aplicabilidad de cada norma y garantice el cumplimiento de estas a la entidad.

7.3.1.4 Capacidad de Decisión y Control
Como propietario principal de la información, La dependencia TI tendrá la última palabra en cuanto a las decisiones sobre el tratamiento, almacenamiento, procesamiento y disposición final de la información. Además, deberá velar porque todas las áreas de Telecafé Ltda. cumplan con las políticas establecidas para el manejo seguro de la información.
Esta estructura pone a la dependencia TI en el centro del control de la información, asegurando su papel clave en la protección y gestión de los datos críticos de la empresa.

7.3.2 Áreas funcionales como propietarios secundarios:
a) Contenido audiovisual: Los jefes de cada área o sección mantendrán la responsabilidad del contenido en sí, pero la dependencia TI será responsable de su almacenamiento, gestión, protección y distribución de la información.
b) Datos personales: Recursos Humanos mantendrá los datos personales de los empleados, pero la dependencia TI garantizará su seguridad y privacidad.
c) Información financiera: El área de Administrativa y Financiera mantendrá los registros financieros y alimentará el sistema contable independiente INTEGRASOFT, donde se almacenarán y protegerán los datos. Por su parte la dependencia TI será responsable de auditar la base de datos de INTEGRASOFT, la protección y el mantenimiento de la infraestructura de Telecafé Ltda. que enlaza el software contable.

7.3.3 Información digitalizada
Los coordinadores y jefes de cada área, dependencia o sección de la entidad Telecafé Ltda., deberán cargar la información digitalizada a la nube de Google Drive, para ser protegida, almacenada y administrada por la dependencia TI.

7.3.4 Responsabilidades de los empleados, contratistas y practicantes

a. Utilizar la información necesaria para llevar a cabo las funciones que le fueron asignadas, de acuerdo con los permisos establecidos o aprobados en el Manual de Funciones.

b. Manejar la Información del canal y rendir cuentas por el uso y protección de tal información, mientras que este bajo su custodia. Esta puede ser física o electrónica e igualmente almacenada en cualquier medio.

c. Proteger la información a la cual tengan acceso, para evitar su pérdida, alteración, destrucción o uso indebido.

d. Evitar la divulgación no autorizada o el uso indebido de la información.

e. Cumplir con todos los controles establecidos por los propietarios de la información y los custodios de la misma.

f. Informar a sus superiores sobre la violación de estas políticas o si conocen de alguna falta a alguna de ellas.

g. Proteger los datos almacenados en los equipos de cómputo y sistemas de información a su disposición de la destrucción o alteración intencional o no justificada y de la divulgación no autorizada.

h. Reportar los Incidentes de seguridad, eventos sospechosos y el mal uso de los recursos que involucren a la dependencia TI.

i. Proteger los equipos de cómputo, de comunicaciones y demás dispositivos tecnológicos designados para el desarrollo de sus funciones. No está permitido el ingreso y la conexión de equipos de cómputo y de comunicaciones ajenos al canal a la red Institucional, ni el uso de dispositivos de acceso externo a Internet o de difusión de señales de red que no hayan sido previamente autorizados por la dependencia TI. En el caso en que se realice bajo alguna circunstancia y con autorización expresa, la conexión de equipos de terceros, estos estarán sujetos a verificación por parte del personal de la dependencia TI asegurando el cumplimiento de las políticas de seguridad de la información.

j. Usar únicamente software autorizados que hayan sido adquiridos legalmente por el canal. No está permitido la instalación ni uso de software diferentes a los Institucionales sin el consentimiento de sus superiores y visto bueno del personal de la dependencia TI.

k. Aceptar y reconocer que en cualquier momento y sin previo aviso, el área directiva, auditores y entidades gubernamentales amparadas en leyes, pueden solicitar una inspección de la información a su cargo sin importar su ubicación o medio de almacenamiento. Esto incluye todos los datos y archivos de los correos electrónicos institucionales, sitios web institucionales y redes sociales propiedad del canal, al igual que las unidades de red institucionales.

l. Apagar los equipos de cómputo, cuando no se usen por más de 1 hora, con el fin de reducir el consumo energético de la entidad y cumplir con las políticas de eficiencia energética de la entidad. Al finalizar el día, cada usuario deberá desconectar los equipos de la red eléctrica, garantizando la protección de los mismos y evitando consumos eléctricos innecesarios.

m. Telecafé Ltda. no es responsable por la pérdida de información, desfalco o daño que pueda tener un usuario al brindar información personal como identificación de usuarios, claves, números de cuentas o números de tarjetas débito/crédito dentro de la institución.

n. Divulgar, aplicar y cumplir con la presente Política.

7.4 Instalación y uso de software

La adquisición, instalación, control y uso correcto del software es responsabilidad directa de la dependencia TI, y por ende se generan los controles que permitan hacer la gestión óptima de dichos recursos, los cuales son verificados de forma anual por auditores externos, generando el informe de derechos de autor y licenciamiento para la Entidad. Es responsabilidad de cada usuario el velar por usar únicamente las aplicaciones licenciadas acordes con sus funcionalidades y que el uso inadecuado de las mismas corresponde una violación a lo establecido dentro de esta política.

7.5 Control mediante servidor de dominio

Este servidor tiene a cargo el manejo de la herramienta Active Directory, la cual contiene la base de datos distribuida de la información de los recursos de la red. A continuación, se presentan algunas de las características principales del servidor en la red:

a. Administración simplificada de usuarios y recursos de red.
b. Sistemas de autenticación y autorización flexibles y seguros.
c. Consolidación de directorios.
d. Infraestructura y aplicaciones habilitadas para el uso de directorios.
e. Administración de los equipos empresariales para evitar personalizaciones en los activos de la entidad.
f. Restricciones de programas no autorizados o licenciados para la entidad.
g. Restricción para la instalación de software ilegal.
h. Políticas de acceso en red.

7.5.1 GPO (Grupos de Trabajo)

Los grupos de trabajo en el Directorio Activo (AD) en la entidad Telecafé Ltda., son una colección de objetos de Active Directory, típicamente usuarios y equipos, que comparten características o requisitos comunes. Estos grupos se crean para organizar a los empleados, asignar permisos y recursos de manera eficiente, y simplificar la administración de las cuentas y los sistemas, estos grupos se encuentran configurados de acuerdo con los aplicativos que posee la entidad. Estos grupos de trabajo se caracterizan por tener atributos en común como permisos de acceso a las carpetas y se diferencian de acuerdo con las exigencias del aplicativo. En general se realiza la actualización y configuración por el personal encargado de la dependencia TI, de las aplicaciones, wallpapers y scripts de configuración.
El control de los grupos de trabajo se establece mediante esta política, además, deben realizarse revisiones periódicas mediante inspección de manera semestral dentro de los mantenimientos preventivos de todos los equipos y sistemas a fin de evidenciar que no existan instalaciones indeseadas y se debe verificar el control sobre este aspecto.

7.6 Configuración de nuevos usuarios en la entidad

Para los usuarios nuevos del canal Telecafé Ltda. o los usuarios que ocupen un nuevo cargo en la entidad, se deberán asignar equipos y no se permitirá el ingreso de equipos personales. Los equipos asignados, deberán ser configurados por el encargado de la dependencia TI, garantizando el buen funcionamiento y asegurando el entorno virtual para los usuarios finales.

Las siguientes son las configuraciones específicas que deben realizarse:
a. Crear los usuarios nuevos en el servidor de dominio.
b. Definir el área a la cual es parte el usuario, con esto se determinan las restricciones de software y hardware de este nuevo usuario.
c. Enlazar el equipo al servidor de dominio.
d. Configurar su nueva dirección de red de acuerdo al área en la cual trabaja.
e. Configurar las políticas de navegación y acceso de aplicaciones de acuerdo al perfil de usuario.

Para usuarios externos y dispositivos personales que deban ingresar a la entidad y al recurso de Internet de la entidad, deben realizar la solicitud mediante correo electrónico al encargado de la dependencia TI para matricular su dirección MAC en el servidor DHCP, con el fin de otorgar y restringir sus servicios, adicional el personal técnico de la dependencia, deberá realizar una inspección del equipo garantizando el cumplimiento de la ley colombiana 23 1982 “Sobre derechos de autor del 28 de enero –, donde se garantice que dentro de la entidad no se usarán Software Ilegales, ya que se podría incurrir en delitos en virtud del artículo 271 del Código Penal colombiano, castigado con pena privativa de la libertad y multa.

7.7 Configuración de retiro de usuarios

Los usuarios del canal que se encuentran registrados en las bases de datos de la entidad, tienen acceso a información interna y catalogada como privada. Al retiro de un usuario, se debe gestionar la información de las bases de datos con el fin de eliminar el acceso a esta información privada, además de esto permitir el flujo de información de los nuevos usuarios.

Para el retiro de los usuarios se deben realizar los siguientes procedimientos en la dependencia TI:

a. Realizar notificaciones mediante correo electrónico desde la dependencia de Talento Humano del usuario que debe ser desvinculado de la entidad.
b. Cambiar la contraseña de la cuenta de usuario de correo electrónico.
c. Realizar copia de seguridad del equipo y del correo electrónico institucional.
d. Eliminar equipos matriculados en el servidor DHCP.
e. Realizar mantenimiento preventivo del equipo para reasignarlo a un nuevo usuario.
f. Deshabilitar al usuario del servidor de dominio.

7.8 Mantener en operación las aplicaciones corporativas

Con el fin de garantizar la integridad y el correcto funcionamiento de los sistemas y servidores de Telecafé Ltda., se ha implementado un proceso de revisión diaria para evaluar el estado general de los servidores.

Procedimiento
1. El personal de la dependencia TI, debe realizar una verificación diaria del estado de los servidores, switches, racks, señales de transmisión y conexiones de red, evaluando su rendimiento, disponibilidad y cualquier incidente o anomalía detectada.
2. Los resultados de esta revisión son registrados en la Bitácora de Registro Centro de Datos, un documento administrado exclusivamente por el equipo de TI, donde se consignan detalles como:
a. Fecha y hora de ingreso.
a. Fecha y hora de salida.
b. Estado general del centro de datos.
c. Problemas o incidencias detectadas.
d. Acciones correctivas tomadas.
e. Nombre del funcionario TI.

Responsabilidad
La dependencia TI es la responsable de llevar a cabo esta revisión y mantener actualizada la bitácora, asegurando que cualquier incidente sea gestionado de manera oportuna para prevenir afectaciones al funcionamiento de los sistemas.

Alcance
Este proceso de monitoreo se aplicará a todos los equipos que operen dentro de la infraestructura del centro de datos de la entidad.

7.8.1 Soporte y Mantenimiento de Aplicativos de la entidad

La dependencia de TI, debe monitorear las actividades de soporte y mantenimiento, prestadas por entidades contratistas que se encargan de los aplicativos.

Las aplicaciones corporativas son las siguientes:

a) Sistema Admiarchi: Para el cual existe un contrato de soporte y mantenimiento con la empresa Admiarchi, se tiene un contrato de actualización y mantenimiento anual. Este contrato obliga al personal Admiarchi a acudir en los momentos de emergencia dado el caso en que se comprometan problemas directamente relacionados con los cambios de versiones o inconvenientes de funcionalidad del aplicativo. Para este efecto el personal de la dependencia TI será el contacto y apoyo a la labor de mantenimiento de la funcionalidad del aplicativo, registrando en informes, las eventualidades y mantenimientos realizados.
b) Aplicativo Antivirus: Cada computador tiene instalado un sistema de Antivirus actualizado, el cual permite que se haga un control de amenazas y escaneo del equipo frente a diferentes vulnerabilidades y malware, es compromiso del usuario notificar a la dependencia TI, cualquier eventualidad que presente el antivirus.
• La dependencia de TI debe velar por que la actualización de las bases de firmas de virus se haga de forma permanente y apoyará labores en la administración, implementación de políticas y verificación las actualizaciones y el correcto funcionamiento de dichas herramientas.
• Es obligación del contratista brindar soporte, capacitar y realizar informes de administración del antivirus a la dependencia TI.
c) Aplicativo de Edición y Graficación: Los equipos de trabajo Work Station de la entidad y equipos autorizados, albergan un software de edición de pago Suit de Adobe, es responsabilidad de la empresa contratista proporcionar soporte relacionado con las licencias, la consola administrativa y los paquetes de Adobe, cuando se requiera. La dependencia de TI debe actuar como enlace entre los contratistas y los usuarios, brindando apoyo en las labores de mantenimiento y garantizando la funcionalidad del software Adobe, además, es obligación de la dependencia TI, exigir al contratista informes detallados sobre las anomalías y mantenimientos realizados al aplicativo, garantizando una documentación histórica de los hechos para posibles reclamos y/o soluciones a futuros fallos.

7.9 Uso y manipulación de equipos de cómputo

Cada usuario cuenta con un equipo de cómputo para el desarrollo de sus funciones. El diseño, adquisición e implementación de estos equipos es responsabilidad de la dependencia TI, pero es deber de los usuarios garantizar su buen funcionamiento, entendiendo que un uso adecuado asegura la continuidad de los servicios. Para mantener el correcto funcionamiento de los equipos, se establece la ejecución de mantenimientos preventivos de manera semestral, cuatrimestral, bimensual y mantenimientos correctivos cuando lo requiera.

a) Uso Adecuado: El equipo de cómputo asignado es una herramienta de trabajo y su uso se limitará a las actividades laborales. Queda prohibido el uso de los equipos para fines personales, como juegos, descargas de archivos no autorizados o acceso a sitios web no relacionados con el trabajo.
b) Mantenimiento: La dependencia TI realizará mantenimientos preventivos a los equipos de cómputo según el cronograma y necesidades de la entidad. Los usuarios deberán reportar cualquier falla o mal funcionamiento a través del sistema propuesto por la dependencia TI.
c) Seguridad Física: Los equipos de cómputo deben permanecer en las áreas de trabajo asignadas. Al finalizar la jornada laboral, los usuarios deberán apagar y desconectar los equipos de cómputo para evitar daños y reducir el consumo energético, para extraer el equipo de la entidad, se deberá comunicar a la dependencia TI el retiro del equipo para ser inspeccionado al ingreso nuevamente. Los equipos de cómputo ajenos al canal, no podrán ser usados dentro de la institución sin el debido análisis y bajo el seguimiento por parte de la dependencia TI.
d) Concientización: La dependencia de TI realizará capacitaciones periódicas a los usuarios para que conozcan y cumplan con esta política.
e) Actualización: La política deberá ser revisada y actualizada periódicamente para adaptarse a los cambios tecnológicos y a las nuevas amenazas.
Al incluir esta sección en la política de seguridad, Telecafé Ltda. estará dando un paso importante para proteger sus activos informáticos y garantizar la continuidad de sus operaciones.

7.10 Gestión de la información y copias de seguridad

Con el propósito de mantener la integridad de los activos de información, la dependencia de TI, asignará responsabilidades a cada actor de la organización respecto a la protección de dichos activos. Para garantizar la continuidad y operatividad del servicio, se establecerá un procedimiento de copias de seguridad. Este procedimiento tiene como objetivo realizar copias de las bases de datos y archivos más relevantes de la entidad, definidos según cada caso de usuario.
Se realizará una copia diaria en el sistema de almacenamiento principal, lo que permite restaurar la información con un mínimo de pérdida en caso de fallas o catástrofes que afecten el funcionamiento de los equipos. Para los servidores, se efectúa una copia completa de la imagen del sistema de manera quincenal en un disco duro de recuperación, asegurando la restauración del sistema en caso de fallos críticos.
a) Pruebas de restauración: Se realizarán pruebas de restauración completas de los sistemas críticos al menos una vez trimestralmente. Los resultados de estas pruebas serán documentados y archivados.
b) Desastres naturales: La entidad debe almacenar respaldos en un sitio remoto para protegerlos en caso de desastres naturales.
c) Cifrado: Implementar el cifrado de los respaldos para proteger la confidencialidad de los datos.

7.10.1 Clasificación de la Información

1. Objetivo
La dependencia de TI de la entidad, debe establecer un sistema de clasificación de la información que permita identificar los distintos niveles de sensibilidad, confidencialidad y criticidad de la información en Telecafé Ltda., asegurando su protección, uso adecuado y control.

2. Alcance
Esta clasificación aplica a todos los tipos de información generada, procesada, almacenada o transmitida por Telecafé Ltda., ya sea en formato físico o digital, incluyendo datos audiovisuales, documentos internos, bases de datos y cualquier otra información relevante para la organización.

3. Criterios de Clasificación
La información se clasificará según su sensibilidad y necesidad de protección en función de los riesgos que implicaría su acceso no autorizado, alteración o pérdida. Los criterios básicos para la clasificación incluyen:
•Confidencialidad: Grado de restricción en el acceso a la información.
•Impacto: Consecuencias en caso de divulgación o alteración no autorizada.
•Valor: Importancia estratégica para la organización.

4. Categorías de Clasificación
Se debe clasificar la información en las siguientes categorías:
a) Información Pública: La información debe ser compartida con el público general y no representa riesgos para la organización en caso de divulgación. Incluye comunicados de prensa, información institucional disponible en la página web y publicaciones en redes sociales.
b) Información Interna: Información que solo puede ser compartida dentro de la entidad Telecafé Ltda. y cuyo acceso externo no está permitido sin autorización previa. Si bien no es altamente sensible, su uso incorrecto podría afectar la operación diaria.
c) Información Confidencial: Información cuya divulgación no autorizada podría tener un impacto negativo significativo en las operaciones, reputación o cumplimiento normativo de Telecafé Ltda. Incluye planes estratégicos, acuerdos comerciales, información financiera y datos sobre la programación audiovisual no publicados.
d) Información Restringida: Información altamente sensible y crítica para la operación y continuidad de Telecafé Ltda. Su acceso debe estar limitado a personal autorizado, y su divulgación no autorizada podría causar daños severos a la organización, incluyen datos personales de empleados, acuerdos de confidencialidad, y contenido audiovisual exclusivo antes de su emisión.

5. Responsabilidades ante la clasificación de la información
•Dependencia TI: Responsable de implementar las medidas técnicas y organizativas necesarias para proteger la información según su clasificación.
•Propietarios de la Información: Es responsable de determinar el nivel de clasificación de la información que maneja y asegurar su correcta protección.

•Usuarios: Deben manejar la información conforme a su clasificación, asegurando que se utilicen los medios apropiados para su almacenamiento, procesamiento y transmisión.

6.Manejo y Protección de la Información
•Información Pública: Puede ser difundida sin restricciones.
•Información Interna: Debe ser compartida únicamente con empleados y colaboradores autorizados, utilizando los medios internos de comunicación aprobados.
•Información Confidencial: Debe estar protegida mediante controles de acceso, cifrado y almacenamiento seguro. Solo personal autorizado debe tener acceso.
•Información Restringida: Requiere las máximas medidas de seguridad, incluyendo cifrado avanzado, autenticación multifactor, y control estricto de acceso físico y digital.

7.Revisión y Actualización
La clasificación de la información debe revisarse periódicamente por la dependencia TI y los coordinadores de área para asegurar que refleje adecuadamente la sensibilidad y criticidad de los datos en función de los cambios en las operaciones de Telecafé Ltda. o en el entorno regulatorio.

7.11 Almacenamiento de copias

Para disminuir el riesgo de pérdida de las copias y hacerlas de fácil acceso en caso de urgencia, se deben almacenar de la siguiente manera:

a) Las copias de seguridad se deberán realizar automáticamente por el programador de tareas de Windows a través de un Script y se guardarán en el servidor NAS, en una hora específica durante la jornada laboral.
b) La dependencia de Archivo Central deberá entregar a la dependencia TI los Discos Duros HDD durante los primeros 3 días de cada mes.
c) La dependencia TI, es responsable de extraer las copias de seguridad de los servidores (NAS, Directrion Activo y NAS de DATA Compartida) de la entidad de forma mensual en los Discos Duros HDD, para ser entregadas a la dependencia Archivo Central.
d) La dependencia Archivo Central Realizará la entrega de los Discos Duros HDD a la empresa contratista de almacenamiento externo de la información.
e) La empresa contratista, almacenará la información extraída en un sitio externo a la entidad en un periodo de tiempo, no mayor a 30 días. Esta empresa deberá cumplir con las especificaciones de la Ley 594 de 2000, por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones; el acuerdo 008 del Archivo General de la Nación, por el cual se establecen las especificaciones técnicas y los requisitos para la prestación de los servicios de depósito, custodia, organización, reprografía y conservación de documentos de archivo y demás procesos de la función archivística en desarrollo de los artículos 13° y 14° y sus parágrafos 1° y 3° de la Ley 594 de 2000; y el acuerdo 049 del Archivo General de la Nación, por el cual se desarrolla el artículo del Capítulo 7 “Conservación de

Documentos” del Reglamento General de Archivos sobre “condiciones de edificios y locales destinados a archivos”; donde se definen los requisitos para la adecuada conservación de soportes documentales en instalaciones dedicadas a archivo.

7.12 Internet, control de navegación y correo electrónico

a) Los equipos de comunicaciones, como routers, módems, switches y servidores, deben estar ubicados en el Centro de Datos del canal.
b) Este Centro de Datos debe contar con un sistema de acceso biométrico por huella.
c) La zona debe de estar clasificada como un área de acceso restringido, permitiendo el ingreso únicamente al personal técnico autorizado por la dependencia de TI.

7.12.1 Acceso a Internet

La postura para los servicios de navegación describe la filosofía fundamental de la seguridad en la entidad es "Todo lo que no esté explícitamente permitido está prohibido".

Dicho lo anterior, se establece que en la Entidad debe asegurarse además de la seguridad e integridad de los activos de información, el control de navegación y recursos de Internet como política generalizada, la cual debe ser cumplida por cada usuario dentro de su caracterización en la organización. Es así, como se establece mediante el dispositivo de seguridad perimetral de red principal, los controles de acceso, navegación y aplicaciones.
1.Objetivos
a) Protección de recursos: La dependencia TI debe asegurar que los recursos de Internet sean utilizados de manera eficiente y segura, en línea con las funciones de cada cargo.
b) Seguridad de la información: La dependencia TI debe garantizar la integridad y confidencialidad de la información de la entidad.
c) Cumplimiento normativo: La dependencia TI deberá Cumplir y velar por el cumplimiento de las normativas y regulaciones aplicables al uso de recursos públicos referente a la navegación WEB.
2. Alcance
a) Servicios cubiertos: Los servicios que tendrán cobertura por estas políticas serán, correo electrónico, navegación web, acceso a aplicaciones en la nube y aplicaciones de videojuegos.
b) Usuarios: Los usuarios relacionados en esta política son empleados, contratistas y personal invitado a la entidad
c) Dispositivos: computadoras de escritorio, portátiles, dispositivos móviles, dispositivos de transmisión y tablets

7.12.1.1 Principio de Seguridad

a) Permiso explícito: Se establece el principio de "todo lo que no esté explícitamente permitido está prohibido".
b) Justificación: Implica que cualquier acción, acceso o uso de un sistema o recurso no debe ser considerado autorizado a menos que exista una regla específica que lo permita. La dependencia de Ti administrará usuarios finales el servicio de acceso a Internet.
Las presentes normas son aplicables y extens ivas a los servicios de navegación y firewall proporcionados al interior de Telecafé Ltda. (LAN y WAN).

7.12.1.2 Controles de Acceso

• Dispositivo de seguridad perimetral: El firewall FortiGate de la entidad, es el encargado en el control del tráfico de Internet, que verifica el ingreso y salida de paquetes.
• Configuraciones de acceso: La dependencia de TI está encargada de administrar la segmentación de red, por medio de la tecnología de Vlans para el acceso de las áreas, este acceso es diferente para cada área de la entidad.
1. Aplicaciones permitidas y bloqueadas:
a) Permitidas:
• Aplicaciones gubernamentales
• Aplicaciones educativas
• Redes sociales
• Aplicaciones de acceso remoto licenciado
• Aplicaciones de audio y video
• Aplicaciones de ALFABET

b) Bloqueadas:
• Contenido para adultos
• Páginas web que no cuentan con certificación SSL
• Páginas de compras
• VPN no autorizadas
• Sitios PROXY no autorizados

7.12.2 Tratamiento de Datos

Con el fin de garantizar la seguridad de las instalaciones y de las personas, Telecafé Ltda. ha implementado un sistema de circuito cerrado de televisión y un sistema de control de acceso biométrico. Las imágenes grabadas y los datos biométricos serán utilizados exclusivamente para fines de seguridad y control de acceso. El acceso a esta información estará restringido a personal autorizado. Los empleados tienen derecho a conocer la información que se ha recolectado sobre ellos y a solicitar la rectificación de datos erróneos. Al incorporar estas medidas en la política de TI, Telecafé Ltda. no solo estará protegiendo sus activos, sino que también estará demostrando su compromiso con la seguridad y la privacidad de sus empleados.

7.12.3 Uso Prohibido

1) Actividades prohibidas
a) Descargar archivos ilegales.
b) Visitar sitios web inapropiados.
c) Realizar actividades personales que no estén relacionadas con el trabajo.
d) Realizar conexiones a internet en equipos ajenos a la entidad sin supervisión de la dependencia TI.
Consecuencias: El no cumplimiento de estas políticas, amerita un llamado de atención y/o plan de mejoramiento.

7.12.4 Monitoreo y Auditoría

• Monitoreo del tráfico: Este se realiza a través del personal de la dependencia TI y del Firewall, a través del LOG de eventos, donde se monitorea el consumo de banda ancha, perdida de paquetes, SLA, conectividad y disponibilidad de canales con la comunicación en las sedes.
• Educación de los usuarios: La dependencia de TI deberá realizar capacitaciones periódicas a los usuarios para concientizarlos sobre la importancia de seguir esta política y las buenas prácticas de seguridad en Internet.
• Actualización de la política: La política debe revisarse y actualizarse periódicamente para reflejar los cambios en la tecnología y las amenazas de seguridad en el acceso a internet.

7.12.5 Acceso a sistema de correo electrónico

7.12.5.1 Gestión del Servicio de Correo

• Responsable: La dependencia TI es la encargada de la administración, configuración y mantenimiento del sistema de correo electrónico de la entidad.
• Solicitudes: La de pendencia de TI gestiona las solicitudes para nuevas cuentas de correo, cambios de contraseña y recuperación de información, que realiza la empresa contratista que administra el servicio de Google Worckspace.
• Entrega de cuentas: La dependencia TI, genera la creación de correos electrónicos y las credenciales de acceso a los usuarios sugeridos por los coordinadores de área.

7.12.5.2 Uso Adecuado del Correo Electrónico

• Propósito: comunicación corporativa interna y externa.
• Restricciones: La dependencia de TI plantea las siguientes actividades prohibidas como:
a) Envío de correo no solicitado (spam).
b) Uso del correo electrónico para fines personales no relacionados con el trabajo.
c) Divulgación de información confidencial.
d) Depuración de información que comprometa a la entidad.

7.12.5.3 Seguridad del Correo Electrónico

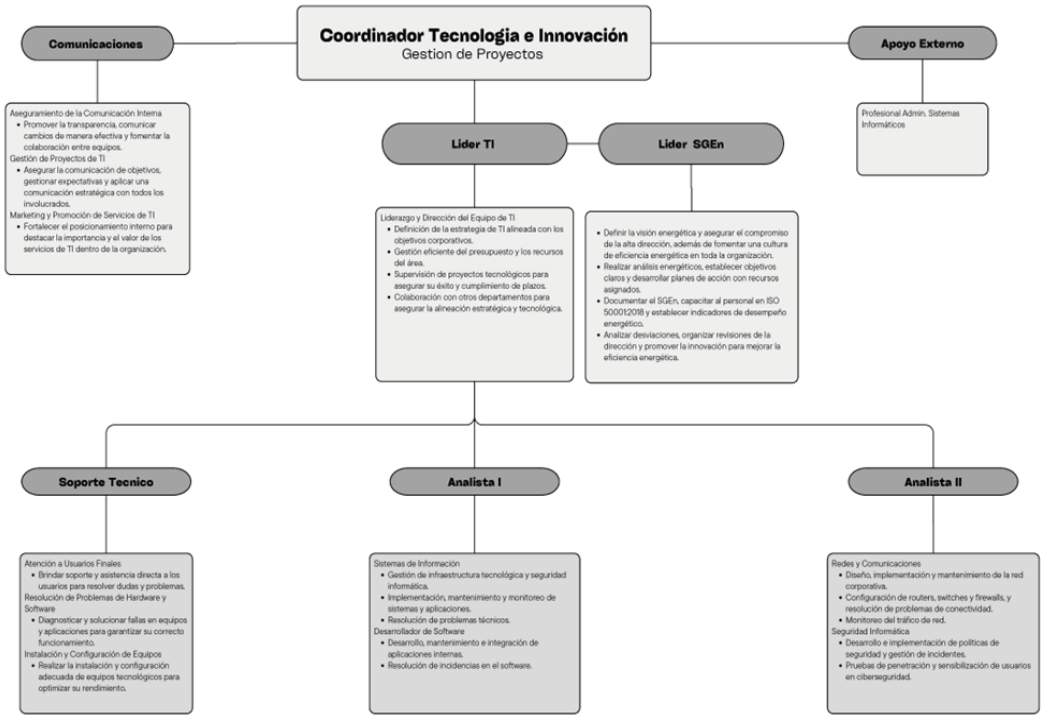
• Contraseñas: La dependencia de TI, exige a los usuarios usar contraseñas seguras, donde se incluyan caracteres especiales, letras mayúsculas y minúsculas, números. Se programarán cambios de contraseñas cada 30 días.
• Phishing: La dependencia TI, debe capacitar al personal contra riesgos del phishing y cómo identificar correos electrónicos fraudulentos, es obligación de los usuarios notificar cualquier anomalía en los correos a la dependencia TI.
• Archivos adjuntos: Se debe capacitar al personal contra riesgos de abrir archivos adjuntos o links de descargas y/o ejecutables de remitentes desconocidos, es obligación de los usuarios notificar cualquier anomalía en los correos a la dependencia TI.

7.12.5.4 Página web

La responsabilidad del manejo del contenido de la página web está a cargo del área digital alineada con la estrategia de comunicaciones web establecida por la entidad.
La dependencia TI frente a la página WEB de la entidad, deberá brindar:
a) Asistencia técnica para el funcionamiento de la plataforma web.
b) Elevar solicitudes de soporte al desarrollador y proveedor de hosting.
c) Asegurar la integridad y la disponibilidad de la plataforma web.

8. MATRIZ ROLES Y RESPONSABILIDADES

Telecafé Ltda. se compromete a velar por la seguridad de todos los activos bajo su responsabilidad, adoptando las medidas necesarias para garantizar el cumplimiento de las normativas y leyes aplicables a los sistemas de Tecnologías e Innovación. Tanto la entidad como sus filiales deberán designar una figura responsable para definir, implementar y monitorizar las medidas de ciberseguridad y seguridad de la información. Esta figura, establecida desde un entorno de gobierno y gestión independiente de cualquier área organizativa, reportará al órgano de gobierno o, en su defecto, a la comisión de auditoría. Entre sus responsabilidades estarán la aplicación de principios de segregación de funciones y el contacto con autoridades y grupos de interés en materia de seguridad de la información.



9. GESTIÓN Y CLASIFICACIÓN DE ACTIVOS DE TI

1. Objetivo
Establecer un marco para identificar, clasificar, proteger y controlar todos los activos de TI de Telecafé Ltda. Se deben definir los criterios para evaluar la criticidad y sensibilidad de cada activo, así como las medidas de seguridad necesarias para garantizar su protección. Además, se deben establecer procesos para el inventario, seguimiento y mantenimiento de los activos, con el objetivo de asegurar la continuidad operativa, proteger la información confidencial y optimizar la inversión en tecnología.

2. Alcance
Esta política aplica a todos los activos de TI de Telecafé Ltda. que son utilizados en el desarrollo de las actividades, incluyendo hardware, software, datos, redes, sistemas y cualquier otro recurso que soporte los servicios de TI.

9.1 Definición de Activos

Se considera activo de TI cualquier recurso que tenga valor para la organización y que esté relacionado con la infraestructura tecnológica. Estos incluyen:

• Hardware: Equipos de cómputo, servidores, dispositivos de red, impresoras, escáner y teléfonos IP.
• Software: Sistemas operativos, aplicaciones comerciales, desarrollos internos y licencias.
• Datos: Información digital y en papel, bases de datos, archivos multimedia y cualquier información crítica.
• Infraestructura de red: Enrutadores, switches, Firewall, cables, puntos de acceso y demás componentes de conectividad.
• Activos intangibles: Licencias de software y contratos de servicio.

9.2 Clasificación de Activos

La clasificación de los activos se debe basar en su criticidad y valor para las operaciones de Telecafé Ltda., esto garantiza que los recursos sean gestionados de manera eficiente y prioritaria, dependiendo de su impacto en el funcionamiento de la organización.
Las categorías recomendadas son las siguientes:

• Críticos: Activos esenciales para la operación del canal, cuya indisponibilidad afectaría gravemente la prestación de servicios como: servidores, sistemas de producción audiovisual, Firewall y componentes de conectividad.
• Importantes: Activos que, aunque no interrumpen completamente las operaciones, sí afectan significativamente la productividad si fallan: estaciones de trabajo para edición, emisión, Suiches de RED, Software de edición y aplicativos de correo electrónico.
• Menor prioridad: Activos cuyo impacto en la operación es bajo en caso de falla: dispositivos periféricos, impresoras, escáner, discos duros externos, teléfonos y memorias USB.

9.3 Responsabilidades frente a la Clasificación y Gestión de activos

a) Dependencia de TI: Es responsable de la gestión integral de los activos de TI, desde su adquisición, instalación, configuración y mantenimiento.
b) Propietarios de los Activos: Áreas o personas designadas como responsables del uso y protección de activos específicos. Deben asegurar que los activos se utilicen conforme a las políticas de seguridad y operativas establecidas.
c) Usuarios finales: Son responsables de usar los activos de manera adecuada y conforme a los lineamientos establecidos por la dependencia de TI, según las normativas establecidas en la política, reportando cualquier anomalía o falla.

9.4 Registro y Control de Activos

a) Inventario: Todos los activos de la dependencia TI deben estar debidamente inventariados, con información actualizada sobre el tipo de activo, ubicación, propietario, estado y características relevantes como número de serie, licencias, fechas de adquisición, modelo y nomenclatura interinstitucional de activo. Los inventarios de activos, se deben actualizar semestralmente por la dependencia TI

b) Etiquetado: Todos los activos deben estar correctamente etiquetados para su fácil identificación y rastreo, bajo la coordinación de la dependencia de bienes y servicios bajo el acompañamiento de la dependencia TI.
c) Ciclo de vida: Cada activo debe gestionarse durante todo su ciclo de vida, adquisición, uso, mantenimiento y baja. El ciclo de vida de los activos, dependerá del criterio técnico y obsolescencia prevista por la dependencia TI, con el aval del comité de bienes y servicios de la entidad.

9.5 Mantenimiento y Actualización de Activos

a) Mantenimiento preventivo y correctivo: La dependencia TI debe establecer un plan de mantenimiento para garantizar el funcionamiento continuo de los activos.
b) Actualización tecnológica: La dependencia TI debe evaluar periódicamente las necesidades de actualización o renovación de los activos, considerando factores como obsolescencia, soporte de proveedores y nuevas tecnologías emergentes.

9.6 Seguridad de los Activos

a) Protección de datos: Los activos que almacenan o procesan datos críticos deben contar con medidas de seguridad apropiadas como encriptación, Backup y acceso controlado.
b) Control de acceso: La dependencia TI debe implementar controles de acceso físico y lógico para restringir el uso de activos al personal autorizado.
c) Política de Backup: La dependencia de TI deben respaldar los datos y activos esenciales periódicamente, según el plan de continuidad y recuperarse en caso de fallas.

9.7 Disposición Final de Activos

Cuando un activo llegue al final de su vida útil o sea reemplazado, La dependencia TI, debe iniciar un proceso formal para su disposición:
• Borrado seguro de datos: Garantizar que todos los datos almacenados en el activo se eliminen de manera segura y conforme a las normativas de protección de la información estipuladas dentro de las políticas TI.
• Disposición responsable: Cumplir con la normativa ambiental para la correcta disposición de equipos electrónicos, en concordancia con las políticas de responsabilidad ambiental de la entidad, gestionando los respectivos certificados de disposición final.

9.8 Cumplimiento y Auditoría

Se deben realizar auditorías periódicas para asegurar el cumplimiento de esta política, revisando el estado de los activos, su correcta gestión y la actualización del inventario. Cualquier desviación o incumplimiento deberá ser reportado y corregido de manera oportuna.

9.9 Revisión y Actualización

Esta política debe ser revisada y actualizada anualmente o cuando se produzcan cambios significativos en la infraestructura tecnológica de Telecafé Ltda.

10 PROYECTOS DE TI

Dentro de la política de TI de Telecafé Ltda., los proyectos desempeñan un papel crucial para asegurar la mejora continua de la infraestructura tecnológica, el cumplimiento de las normativas y la innovación en los procesos. Estos proyectos deberán permitir a la organización, mantener la competitividad, optimizar recursos y ofrecer servicios de calidad.

1.Objetivo

La dependencia TI debe definir directrices claras para la planificación, gestión, implementación y evaluación de los proyectos dentro de Telecafé Ltda., alineando cada proyecto con los objetivos estratégicos de la organización y asegurando la optimización de los recursos tecnológicos.

2.Alcance

Esta sección de la política aplica a todos los proyectos relacionados con la infraestructura tecnológica, software, seguridad de la información, comunicaciones y sistemas de gestión de Telecafé Ltda. Incluye desde la adquisición de nuevos sistemas hasta la mejora y actualización de los sistemas existentes.

10.1 Tipos de Proyectos de TI

Los proyectos de TI en Telecafé Ltda. Se clasifican en las siguientes categorías:

a) Proyectos de Infraestructura:

• Mejoras o actualizaciones de hardware, servidores, redes y centro de datos.

• Optimización de la infraestructura física y virtual para soportar los servicios del canal.

b) Proyectos de Seguridad de la Información:

• Implementación de sistemas de ciberseguridad, control de acceso, autenticación y cifrado de datos.

• Actualización de protocolos y sistemas de respaldo de información (backup) para garantizar la continuidad del crecimiento de la organización.

c) Proyectos de Transformación Digital:

• Migración hacia soluciones en la nube.

• Automatización de procesos mediante herramientas de inteligencia artificial (IA) o machine learning (ML).

• Creación de plataformas de contenido multimedia en línea para adaptarse a nuevas demandas de usuarios digitales.

d) Proyectos de Cumplimiento Normativo:

• Implementación de soluciones para asegurar el cumplimiento de normativas locales e internacionales, como la Ley de Protección de Datos Personales en Colombia y estándares como RETIE, RETILAP y NTC2050.

• Evaluación y ajustes necesarios para cumplir con regulaciones audiovisuales y de telecomunicaciones.

10.2 Revisión y Actualización de la Política de Proyectos de TI

Debido a la naturaleza dinámica de la tecnología, esta política de proyectos debe ser revisada y actualizada periódicamente para adaptarse a los avances tecnológicos y a las necesidades estratégicas de Telecafé Ltda. Esto debe hacerse al menos una vez al año o cuando se identifiquen cambios significativos en el entorno tecnológico o regulatorio.

Es responsabilidad de la dependencia de TI vigilar que las herramientas tecnológicas disponibles sean acordes a las necesidades establecidas, entendiendo que deben asegurarse los recursos necesarios para el desarrollo del plan estratégico de la entidad, entendiendo que la tecnología es un agente dinamizador de los procesos, por lo cual, es necesario mantener la infraestructura actualizada entendiendo los efectos de la obsolescencia, y a su vez mantenernos a la vanguardia tecnológica de modo que la garantice la competitividad frente a las exigencias del mundo actual.
De esta forma, se establece por política:
a) La dependencia Ti debe realizar análisis de ingeniería, diseño e implementación de proyectos que garanticen la actualización tecnológica, que disminuyan costos de producción, que garantice ahorro energético y seguridad informática frente a las necesidades de la entidad.

11 CUMPLIMIENTO DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

a) Es responsabilidad y compromiso de cada área de la estructura organizacional del canal, la divulgación del Manual de Políticas de Seguridad de la información, así como su cumplimiento y verificación, debido a cada contexto.
b) Todos los clientes del canal o proveedores que se encuentren en el nivel de servicios TIC deben estar autorizados por la dependencia TI para el uso de los recursos TIC, quienes deben vigilar el uso adecuado de la información y de toda la plataforma tecnológica.
c) Es responsabilidad de la dependencia TI capacitar al personal de la entidad sobre los riesgos y amenazas que pueden afectar la información, así como concientizar a los usuarios sobre el manejo adecuado de la misma, dado que es un recurso de gran importancia.
d) La dependencia TI debe fomentar la apropiación y el empoderamiento de los usuarios para aplicar las políticas de seguridad informática, con el fin de evitar vulnerabilidades que puedan impactar negativamente a la entidad.
e) La dirección de Telecafé Ltda., debe definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza.

f) Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.
g) La dependencia TI protegerá la información creada, procesada, transmitida o resguardada con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
h) Telecafé Ltda. controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
i) La dependencia TI garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
j)Telecafé Ltda. garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas por medio de la dependencia TI.

El incumplimiento de las políticas de Seguridad y Privacidad de la Información no solo puede tener consecuencias legales según la normativa vigente, tanto a nivel de la entidad como del Gobierno Nacional y Territorial, sino que también afecta el funcionamiento general de la organización. Es fundamental que todas las áreas adopten y cumplan las políticas y lineamientos establecidos en el documento para garantizar la continuidad del negocio, la correcta operación de la plataforma tecnológica y la optimización en el manejo de los recursos de TI. La alineación con estas políticas asegura que se eviten sanciones legales y se mantenga la eficiencia operativa.

11.1 Sanciones Disciplinarias con Respecto a la Seguridad de la Información de la Entidad.

En Telecafé Ltda., se establece un riguroso sistema de sanciones disciplinarias como parte integral de nuestra política de seguridad de la información. Estas medidas se aplican en casos de violación de las políticas establecidas, con el fin de garantizar la integridad y confidencialidad de los datos de la organización. Las sanciones disciplinarias se adaptan a la gravedad de la infracción y se aplican de manera justa y consistente. Entre las medidas disciplinarias se incluyen:

a) Amonestación verbal: En situaciones donde se haya cometido una infracción menor o como primera medida correctiva, se proporcionará una amonestación verbal al empleado afectado, para recordarle la importancia del cumplimiento de las políticas de seguridad de la información.
b) Amonestación escrita: En caso de que se repita la infracción o esta sea de mayor gravedad, se emitirá una amonestación por escrito, dejando constancia formal de la violación y las posibles consecuencias futuras.
c) Suspensión temporal: Para infracciones graves que pongan en riesgo la seguridad de la información de Telecafé Ltda., se aplicará una suspensión temporal del empleo como medida disciplinaria, con el fin de investigar adecuadamente el incidente y tomar las medidas necesarias.

d) Terminación del contrato: En casos extremos, donde se compruebe una violación significativa de las políticas de seguridad de la información o una falta de cumplimiento reiterada, se procederá con la terminación del empleo del individuo involucrado, con el objetivo de proteger los intereses y la reputación de Telecafé Ltda.

12. POLÍTICAS DEL SGEN EN TELECAFÉ LTDA.

Es objetivo principal es alinear las políticas de TI con los objetivos del SGEn, promoviendo el uso eficiente de la energía en todos los equipos y sistemas informáticos, reduciendo el consumo energético y minimizando el impacto ambiental.

a) Alcance:
Esta política se aplica a todos los equipos informáticos, servidores, redes, centros de datos y software utilizados por Telecafé Ltda.

b) Principios:
1. Eficiencia energética: Promover la adquisición y el uso de equipos informáticos con bajo consumo energético.
2. Gestión de la energía: Implementar medidas de gestión de la energía en los sistemas informáticos, como la programación de apagados automáticos y la optimización de la configuración de los equipos.
3. Concientización: Fomentar una cultura de eficiencia energética entre los empleados a través de capacitaciones y campañas de sensibilización.
4. Medición y seguimiento: Establecer indicadores clave de desempeño para medir el consumo energético de los sistemas informáticos y realizar un seguimiento continuo de los resultados.

12.1 Políticas Energéticas Específicas.

a) Adquisición de equipos:
1. Priorizar la adquisición de equipos con certificación energética.
2. Evaluar el consumo energético de los equipos durante el proceso de selección.
3. Establecer criterios de eficiencia energética en los pliegos de condiciones de las compras.

b) Gestión de la energía en los equipos:
1. Configurar los equipos para que entren en modo de bajo consumo o suspensión cuando no estén en uso.
2. Desactivar las pantallas y los discos duros cuando no sean necesarios.
3. Utilizar software de gestión de energía para optimizar el consumo de los equipos.
4. Implementar políticas de apagado de equipos al finalizar la jornada laboral.

c)Virtualización:
1. Promover la virtualización de servidores para consolidar equipos y reducir el consumo energético.
2. Optimizar la configuración de los entornos virtuales para minimizar el consumo de recursos.

d)Enfriamiento:
1. Utilizar sistemas de enfriamiento eficientes para los centros de datos y MCR.
2. Optimizar el flujo de aire y la temperatura de los equipos para reducir el consumo energético.

e) Almacenamiento de datos:
1. Implementar políticas de almacenamiento de datos para eliminar archivos innecesarios y liberar espacio en los discos duros.
2. Utilizar tecnologías de almacenamiento en la nube para reducir la necesidad de servidores físicos.

f) Capacitación:
1. Implementar programas de capacitación para los empleados sobre el uso eficiente de la energía en los equipos informáticos.
2. Promover la participación de los empleados en iniciativas de ahorro energético.

12.2 Medición y seguimiento:

a) Establecer indicadores: Definir indicadores clave de desempeño para medir el consumo energético de los sistemas informáticos, como el consumo por equipo, por área o por proyecto.
b) Monitoreo continuo: Utilizar herramientas de monitoreo para recopilar datos sobre el consumo energético y generar reportes periódicos de los equipos de la dependencia TI.
c) Análisis de datos: Analizar los datos recopilados para identificar oportunidades de mejora y tomar medidas correctivas.

12.3 Revisión y Mejora:

a) Revisión periódica: Revisar esta política con una periodicidad anual para asegurar su alineación con los objetivos del SGEn y las nuevas tecnologías que influyen en la dependencia TI de la entidad.
b) Mejora continua: Implementar un proceso de mejora continua para identificar y aplicar nuevas medidas de eficiencia energética en el entorno TI.

13 REVISIÓN DE LA POLÍTICA

La revisión periódica de la política de TI es un aspecto crucial para garantizar que esta se mantenga alineada con las necesidades cambiantes de la organización y las tendencias tecnológicas. A continuación, se proponen los procesos que deben implementarse en Telecafé Ltda.

Establecer un Comité de Revisión:
• Composición: El comité deberá incluir representantes de TI, áreas de negocio, legales y un representante de la alta dirección.
• Responsabilidades:
a) Definir la frecuencia de las revisiones.
b) Establecer los criterios para identificar la necesidad de una revisión extraordinaria.
c) Evaluar el cumplimiento de la política actual.
d) Identificar áreas de mejora y nuevas necesidades tecnológicas.
e) Proponer modificaciones a la política.

13.2 Evaluación Anual:

1) Revisión documental: El comité debe analizar la política existente en busca de inconsistencias, ambigüedades o secciones obsoletas.
2) Encuesta a usuarios: La dependencia de TI debe realizar una encuesta a los usuarios para conocer su percepción sobre la política e identificar áreas de mejora.
3) Auditoría de cumplimiento: El comité de revisión evaluará si los procesos y procedimientos de TI se ajustan a la política establecida.
4) Análisis de riesgos: La dependencia de TI debe identificar nuevos riesgos tecnológicos y evaluar cómo la política los aborda.

13.3 Revisión Extraordinaria por la Dependencia TI:

1) Cambios regulatorios: Actualizar la política para cumplir con nuevas leyes o regulaciones.
2) Incidentes de seguridad: Revisar la política después de un incidente de seguridad para identificar debilidades y fortalecer los controles.
3) Nuevos proyectos tecnológicos: Evaluar si la política se adapta a los requisitos de nuevos sistemas o aplicaciones.
4) Cambios organizacionales: Ajustar la política a los cambios en la estructura organizacional o en los procesos de negocio.

13.4 Propuesta de Modificaciones:

1) Elaboración de un documento: El comité de revisión elaborará un documento detallado con las propuestas de modificación, justificando cada cambio.
2) Consenso: Las propuestas serán discutidas y consensuadas entre los miembros del comité.

13.5 Aprobación y Comunicación:

1)Presentación a la gerencia: El comité presentará las propuestas de modificación a la gerencia para su aprobación.
2)Comunicación a los usuarios: Una vez aprobada, la nueva versión de la política será comunicada a todos los empleados a través de los canales adecuados.

13.6 Implementación y Seguimiento:

1) Capacitación: Se brindará capacitación a los empleados sobre los cambios introducidos en la política.
2) Actualización de la documentación: Se actualizarán todos los documentos relacionados con la política, como procedimientos y manuales.
3) Seguimiento continuo: Se realizará un seguimiento continuo para asegurar que la política se cumpla y se ajusten los procesos si es necesario.

La revisión periódica de la política TI es una práctica fundamental para la entidad que garantiza su relevancia y eficacia en un entorno en constante evolución. Para llevar a cabo esta revisión de manera efectiva, se establecen los siguientes procesos:

a. Proceso de revisión: Establecer un proceso detallado que incluye la recopilación de retroalimentación de los empleados, la evaluación de riesgos actuales y la identificación de áreas de mejora en la política de seguridad de la información.

b. Actualización y aprobación: Una vez completada la revisión, se actualiza la política de seguridad de la información según sea necesario y se somete a la aprobación de la alta dirección de Telecafé Ltda. antes de su implementación, asegurando su alineación con los objetivos y las necesidades de la organización.

Se recomienda implementar en la entidad un SGTI, ya que proporciona un marco estructurado para gestionar todos los aspectos de la tecnología de la información dentro de una organización. Al adoptar un SGTI, Telecafé Ltda. puede documentar, comunicar y hacer cumplir la política de TI de manera más efectiva, además, facilita el monitoreo y la medición del cumplimiento de los requisitos de la política y permite gestionar de manera ordenada los cambios en la infraestructura y los procesos de TI.

14 BIBLIOGRAFÍA

[1] DEFINICIÓN DE CLAVE. Wikipedia la enciclopedia libre. En Línea disponible: http://es.wikipedia.org/wiki/Contraseña.
[2] DEFINICIÓN DE DISPONIBILIDAD DE LA INFORMACIÓN. http://www.coreoneit.com/disponibilidad-de-la-informacion/.
[3] DEFINICIÓN DE HARDWARE. Diccionario de la Real Academia Española; Sitio: http://lema.rae.es/drae/.
[4] DEFINICIÓN DE INTERNET. Diccionario de la Real Academia Española; Sitio: http://lema.rae.es/drae/
[5] DEFINICIÓN DE MALWARE. SYMANTEC, Es una de las compañías líder del mundo en seguridad informática;Sitio: http://www.symantec.com/es/mx/theme.jsp?themeid=glosario-de-seguridad
[6] DEFINICIÓN DE SERVICIO. MinTIC (Ruta) Inicio / Atención al público; Sitio: http://www.mintic.gov.co/portal/604/w3-propertyvalue1051.html
[7] DEFINICIÓN DE SERVICIO. MinTIC (Ruta) Inicio / Atención al público; Sitio:

[8] DEFINICIÓN DE SOFTWARE. Diccionario de la Real Academia Española; Sitio: http://lema.rae.es/drae/
15 DEFINICIÓN DE AUTENTICACIÓN: ;Sitio:https://www.microsoft.com/es-co/security/business/security-101/what-is-authentication#:~:text=La%20autenticaci%C3%B3n%20es%20el%20proceso,a%20recursos%20de%20la%20organizaci%C3%B3n

CONTROL DE CAMBIOS				
Descripción del cambio	**Motivo del cambio**	**Responsable**	**Fecha Modificación**	**Nueva Versión**
Se actualiza el numeral 6.4.1. cambiando la entrega de la copia de seguridad de control interno a técnico de gestión documental	La copia de seguridad que se describe en este numeral se entrega al técnico de gestión documental y es éste quien documenta de manera oficial la entrega a la empresa contratada para la custodia	Líder Tecnología e Innovación	2 de junio de 2021	2
Se adiciona la INTRODUCCIÓN y se asigna el punto # 2	Este punto estructura la idea central del documento, siendo la puerta de entrada para asegurar que la política sea comprendida, aceptada y aplicada de manera efectiva, contribuyendo así a la seguridad, eficiencia y cumplimiento de los objetivos de la organización.	Líder Tecnología e Innovación	21 de octubre de 2024	3

telecafé

CONTROL DE CAMBIOS				
Descripción del cambio	**Motivo del cambio**	**Responsable**	**Fecha Modificación**	**Nueva Versión**
Se elimina el punto PROPÓSITO y se reemplaza por el OBJETIVO GENERAL #4	El propósito, no enmarca el objetivo general, dado que no cumple con el fundamento establecido dentro de la entidad por la estructura de la dependencia TI.	Líder Tecnología e Innovación	2 de junio de 2021	2
Se adiciona el punto # 4.1 Objetivos Específicos	Los Objetivos Específicos aseguran que la tecnología sea una herramienta estratégica que contribuya al éxito de la organización. Están definidos de manera clara y concisa, estableciendo una dirección clara para facilitar la toma de decisiones, lo que permite optimizar el uso de los recursos tecnológicos y maximizar el retorno de la inversión.	Líder Tecnología e Innovación	21 de octubre de 2024	3
El alcance de las políticas se estipuló en el punto #5, en la versión anterior este ocupaba el punto #3	La estructura de la política requiere de este orden, ya que garantiza que el personal y el procedimiento puedan entender y llevar a cabo el cumplimiento de la política.	Líder Tecnología e Innovación	21 de octubre de 2024	3

telecafé

CONTROL DE CAMBIOS				
Descripción del cambio	**Motivo del cambio**	**Responsable**	**Fecha Modificación**	**Nueva Versión**
Se modifica el punto #6 MARCO LEGAL Y NORMATIVO	Se proponen cambios en la actualización y aplicación de las normas por medio de un normograma interno, que se enlace con el normograma de la entidad y permita un desglose de las leyes para tener un mejor control sobre estas y su función en la entidad.	Líder Tecnología e Innovación	2 de junio de 2021	2
Se adiciona el punto #7 DESARROLLO DE LA POLÍTICA	Dentro de este punto se establecen: ·Acceso a la información y responsabilidades. ·Instalación y uso de software. ·Manipulación de equipos de cómputo, responsabilidad de los usuarios frente a las herramientas de cómputo. ·Internet, Control de navegación y Correo electrónico. ·Gestión de la información, copias de seguridad. ·Seguridad y privacidad de la información, cambio de contraseñas y acceso a los sistemas. ·Roles y responsabilidades. ·Proyectos de TI. el acceso a la información y responsabilidades.	Líder Tecnología e Innovación	21 de octubre de 2024	3

telecafé

CONTROL DE CAMBIOS				
Descripción del cambio	**Motivo del cambio**	**Responsable**	**Fecha Modificación**	**Nueva Versión**
Se modifica en el punto #8 la MATRIZ ROLES Y RESPONSABILIDADES	Se estructura la Matriz de Roles y Responsabilidades, reforzándola con un organigrama jerárquico donde interviene personal de otras áreas, fortaleciendo el cumplimiento y la aplicación de las políticas de TI dentro de la organización.	Líder Tecnología e Innovación	2 de junio de 2021	2
Se adiciona el punto #9 GESTIÓN Y CLASIFICACIÓN DE ACTIVOS DE TI	Este punto, garantiza la eficiencia, seguridad y rentabilidad de la inversión en tecnología. Con la estrategia de gestión de activos, la organización puede reducir costos, mejorar la seguridad de la información y tomar decisiones más informadas	Líder Tecnología e Innovación	21 de octubre de 2024	3
Se adiciona el punto #10 REVISIÓN DE LA POLÍTICA	Este punto es importante, ya que la revisión de las políticas de TI es una práctica esencial para garantizar que la tecnología sea un activo estratégico y que contribuya al éxito de la organización. Al mantener las políticas actualizadas y alineadas con los objetivos del negocio, se reduce el riesgo, se mejora la eficiencia y se garantiza el cumplimiento normativo.	Líder Tecnología e Innovación	21 de octubre de 2024	3

telecafé

Expresión de lo nuestro

SISTEMA DE GESTIÓN DE CALIDAD 2024

Política de TI.