CAFENET COMUNICACIONES S.A.
Teléfono: 315 552 46 19
Carrera 23 No.62-39 Of.1204
Edificio Empresarial Capitalia
cafenetsa@cafenet.com.co
Manizales – Caldas

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN
CAFENET COMUNICACIONES S.A.

Versión 1.0 – 17-06-2025

1. Objetivo

Esta Política tiene como objetivo establecer los lineamientos generales que permitan garantizar la confidencialidad, integridad y disponibilidad de la información y los servicios prestados por **CAFENET COMUNICACIONES S.A**., en cumplimiento con las regulaciones establecidas por la Comisión de Regulación de Comunicaciones (CRC).

2. Alcance

Esta política aplica a:
Todo el personal de **CAFENET COMUNICACIONES S.A.**
Contratistas y proveedores que accedan o gestionen información o recursos tecnológicos de la empresa
Procesos operativos, administrativos y técnicos
Infraestructura de red, software, plataformas digitales y bases de datos

3. Principios de Seguridad de la Información

CAFENET COMUNICACIONES S.A. se compromete a proteger su infraestructura tecnológica y la información que administra, basándose en los siguientes principios:

Confidencialidad: Proteger y garantizar que la información no se divulgará ni se pondrá a disposición de individuos, entidades o procesos no autorizados (Recomendaciones UIT X.805 y X.814).

Integridad: Garantizar la exactitud y la veracidad de los datos, protegiendo los datos contra acciones no autorizadas de modificación, supresión, creación o reactuación, y señalar o informar estas acciones no autorizadas (Recomendaciones X.805 y X.815).

Disponibilidad: Garantizar que las circunstancias de la red no impidan el acceso autorizado a los elementos de red, la información almacenada, los flujos de información, los servicios y las aplicaciones (Recomendación X.805).

Autenticación: Verificación de identidad tanto de usuarios, dispositivos, servicios y aplicaciones. La información utilizada para la identificación, la autenticación y la autorización debe estar protegida (Recomendaciones UIT X.805 y UIT X.811).

Acceso: Prevenir la utilización no autorizada de un recurso. El control de acceso debe garantizar que sólo los usuarios o los dispositivos autorizados puedan acceder a los elementos de red, la información almacenada, los flujos de información, los servicios y aplicaciones (Recomendaciones UIT X.805 y UIT X.812).

Servicio de No repudio: Es aquél que tiene como objeto recolectar, mantener, poner a disposición y validar evidencia irrefutable sobre la identidad de los remitentes y destinatarios de transferencias de datos. (Recomendaciones UIT X.805 y X.813).

4. Responsabilidades

La gerencia general es responsable de aprobar, apoyar y hacer cumplir esta política.

El responsable de seguridad de la información velará por la implementación y monitoreo del SGSI.

Todos los empleados y contratistas deben cumplir las medidas de seguridad establecidas.

5. Compromiso con la seguridad

CAFENET COMUNICACIONES S.A. se compromete a:

Implementar un Sistema de Gestión de Seguridad de la Información (SGSI) basado en principios de la norma ISO/IEC 27001.

Identificar, evaluar y tratar los riesgos que puedan afectar la seguridad de la información.

Mantener controles técnicos y administrativos actualizados: antivirus, firewalls, respaldos, sistemas de autenticación, cifrado, etc.

Gestionar incidentes de seguridad de forma oportuna y eficaz.

Capacitar de forma periódica a su personal en buenas prácticas de seguridad digital.

6. Gestión de incidentes

CAFENET COMUNICACIONES S.A. cuenta con un procedimiento interno de gestión de incidentes de seguridad, que permite detectar, reportar, analizar y solucionar eventos que puedan comprometer la red o la información de los usuarios.

Todos los incidentes son registrados y tratados según su nivel de criticidad.

7. Mejora continua

El Sistema de Gestión de Seguridad de la Información será revisado de forma periódica para asegurar su efectividad, adaptarse a nuevos riesgos tecnológicos y cumplir con los requisitos legales y contractuales vigentes.

CAFENET COMUNICACIONES S.A.
Teléfono: 315 552 46 19
Carrera 23 No.62-39 Of.1204
Edificio Empresarial Capitalia
cafenetsa@cafenet.com.co
Manizales – Caldas

8. Cumplimiento normativo
Esta política está alineada con:
Resolución CRC 5050 de 2016 y artículos complementarios
Ley 1581 de 2012 – Protección de Datos Personales
Ley 1273 de 2009 – Delitos informáticos
Normas internacionales como ISO/IEC 27001

9. Divulgación
Esta política será divulgada a todo el personal y estará disponible en el sitio web oficial de **CAFENET COMUNICACIONES S.A**. para consulta de usuarios, entidades regulatorias y partes interesadas.

Componentes clave de una política de seguridad de la información en Internet

1. **Cumplimiento legal y normativo**
   - Alineación con normativas como GDPR, ISO/IEC 27001, NIST, etc.
   - Revisión periódica de políticas para asegurar el cumplimiento.
2. **Control de acceso**
   - Definición de roles y permisos para acceder a recursos.
   - Uso de contraseñas seguras, autenticación multifactor (MFA) y gestión de identidades.
3. **Protección de datos**
   - Cifrado de información sensible (en tránsito y en reposo).
   - Copias de seguridad regulares.
   - Políticas de retención y eliminación de datos.
4. **Uso aceptable de Internet**
   - Reglas sobre la navegación, descarga de archivos y uso del correo electrónico.
   - Restricciones sobre sitios web no autorizados o peligrosos.
5. **Seguridad de la red**
   - Implementación de firewalls, VPNs y sistemas de detección de intrusiones (IDS).
   - Segmentación de redes para limitar el alcance de ataques.
6. **Gestión de incidentes**
   - Procedimientos para detectar, responder y recuperarse de incidentes de seguridad.
   - Registro y análisis de eventos y vulnerabilidades.
7. **Educación y concienciación**
   - Programas de capacitación para empleados sobre ciberseguridad.
   - Campañas de concientización sobre phishing, ingeniería social, etc.

Ejemplo de política básica de seguridad en Internet para una organización

- Todo el tráfico de red será monitoreado y registrado.
- El uso de Internet debe estar relacionado con funciones laborales.
- Está prohibido instalar software no autorizado.
- La información sensible debe cifrarse antes de ser transmitida por Internet.
- Se deben reportar incidentes de seguridad al equipo de TI en un plazo de 24 horas.

Beneficios de tener una política de seguridad bien definida

- Reducción del riesgo de ciberataques.
- Protección de datos sensibles y propiedad intelectual.
- Mejora de la reputación y confianza de clientes/usuarios.
- Cumplimiento de requisitos legales y normativos.

Aprobado por:
Gerencia General – CAFENET COMUNICACIONES S.A.
Fecha: 17-06-2025