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

INFORME INTEGRADO DE SEGURIDAD DE LA INFORMACIÓN

CAFENET COMUNICACIONES S.A.
Versión 1.0 – Junio 2025

CAFENET COMUNICACIONES S.A., como empresa prestadora de servicios de telecomunicaciones en Colombia, ha desarrollado e implementado políticas, procedimientos y controles que garantizan la protección de la información y la continuidad del servicio, en cumplimiento de la **Resolución CRC 5050 de 2016**, el **Decreto 1078 de 2015**, la **Ley 1581 de 2012** y estándares internacionales como **ISO/IEC 27001**.

Este informe consolida las acciones institucionales en materia de **Seguridad de la Información, Neutralidad en la Red, Gestión de Riesgos Cibernéticos, Incidentes de Seguridad** y **Medidas Internas de Protección**, y documenta su cumplimiento y aplicación efectiva.

1. Política de Seguridad de la Información

1.1 Objetivo

Establecer los lineamientos que aseguren la **confidencialidad, integridad y disponibilidad** de la información corporativa y de los servicios tecnológicos ofrecidos.

1.2 Alcance

Aplica a todo el personal interno y externo que interactúe con la infraestructura, los sistemas y la información de la empresa. Incluye:

- Redes, plataformas, software y datos institucionales.
- Usuarios, proveedores, contratistas y terceros autorizados.

1.3 Principios Rectores

- **Confidencialidad**: Solo usuarios autorizados pueden acceder a la información.
- **Integridad**: La información no debe ser alterada sin control.
- **Disponibilidad**: El acceso oportuno a la información debe estar garantizado.

1.4 Compromisos del SGSI

- Implementar un **SGSI basado en ISO/IEC 27001**.
- Identificar y tratar riesgos de seguridad.
- Utilizar herramientas como **antivirus, firewalls, cifrado**, respaldo de datos, etc.
- Establecer procesos efectivos para la **gestión de incidentes**.
- **Capacitar al personal** de forma continua.

2. Gestión de Incidentes de Seguridad

CAFENET COMUNICACIONES S.A. cuenta con un procedimiento interno de identificación, registro, análisis, clasificación y resolución de incidentes. Este proceso incluye:

2.1. Diligenciamiento de **formato de incidente de seguridad de la información** para el registro y almacenamiento de los incidentes de seguridad de la información

Fecha del Incidente	Servicio afectado	Número de usuarios afectados	Duración	Categoría del incidente	Nivel de severidad del incidente

Fecha del incidente: En este campo deberá indicarse la fecha de inicio del incidente.

Servicio afectado: En este campo deberá indicarse el o los servicios afectados por el incidente de indisponibilidad:

a) Internet Fijo.
b) Internet Móvil.
c) Telefonía fija.
d) Telefonía Móvil

Número de usuarios externos afectados: En este campo, para telefonía fija e Internet fijo, debe indicarse el número de suscriptores afectados.

Para Internet y telefonía móvil, deberá indicarse el número potencial de usuarios afectados de acuerdo con el uso normal de la infraestructura afectada.

Duración: En este campo debe indicarse el tiempo en horas de duración del incidente de seguridad de la información

Categoría del incidente: En este campo debe indicarse la categoría del incidente de seguridad de la información, el operador debe indicar una de las siguientes categorías de causas raíz:

a) Denegación de servicio: Denegación de servicio (DoS) y Denegación de servicio distribuida (DDoS) son una categoría amplia de incidentes con características en común. Estos incidentes causan que un sistema, servicio o red no opere a su capacidad prevista, usualmente causando la denegación completa del acceso a los usuarios legítimos.

b) Acceso no autorizado: esta categoría de incidentes consiste en intentos no autorizados para acceder o hacer un mal uso de un sistema, servicio o red.

c) Malware: esta categoría identifica un programa o parte de un programa insertado en otro con la intención de modificar su comportamiento original, generalmente para realizar actividades maliciosas como robo de información, robo de identidad, destrucción de información y recursos, denegación de servicio, correo no deseado, etc.

d) Abuso: esta categoría de incidentes identifica la violación de las políticas de seguridad del sistema de información de una organización

No son ataques en el sentido estricto de la palabra, pero a menudo se informan como incidentes y requieren ser gestionados.

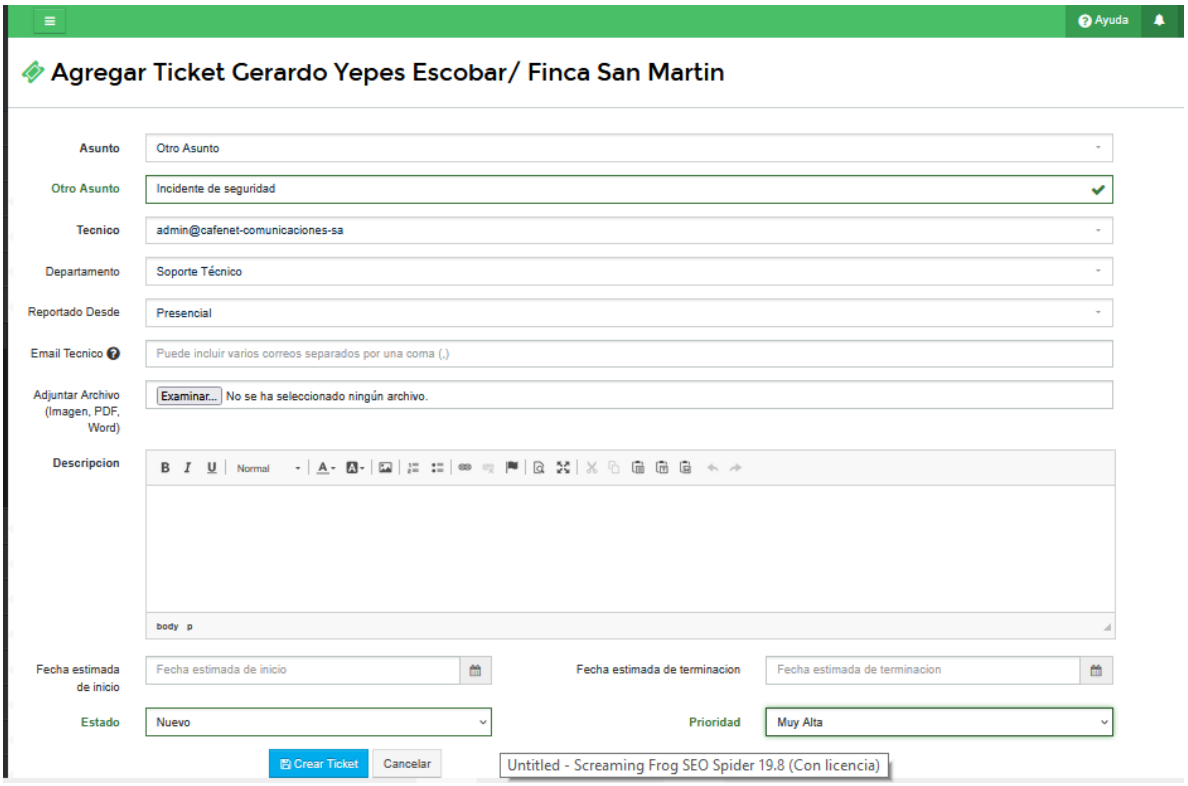
e) Recopilación de información de sistema: esta categoría de incidentes incluye las actividades asociadas con la identificación de objetivos potenciales y el análisis de los servicios que se ejecutan en esos objetivos (ej. probing, ping, scanning).

Nivel de severidad de incidente: En este campo, debe indicarse el nivel de severidad del incidente de seguridad de la información, teniendo en cuenta la importancia del sistema de información involucrado, las potenciales pérdidas de negocio y el posible impacto social, según lo dispuesto en el Anexo 5.8 de la presente resolución:

a) Muy Serio (Clase IV)
b) Serio (Clase III)
c) Menos serio (Clase II)
d) Pequeño (Clase I)

2.2. Registro de Incidente, una vez se dé la atención y tratamiento, es guardado en el CRM, que en nuestro caso es la aplicación WISPHUB, creado como un ticket para el usuario afectado y adjuntando en PDF el formato del incidente, para esto se utilizan herramientas digitales internas con trazabilidad, almacenamiento por mínimo un (1) año y capacidad de exportación para fines de auditoría y reporte regulatorio.

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



3. Reporte a COLCERT

Todo incidente clasificado como **Clase III o IV** es reportado a **COLCERT Colombia**, conforme a la Resolución CRC 5569 de 2018, incluyendo **Formato reporte Incidente COLCERT Cafenet.docx**

Información técnica del evento

- Responsable de la gestión
- Evidencia técnica (logs, capturas)
- Tiempo de resolución