POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

1. Objeto

La presente Política de Seguridad de la Información tiene como finalidad establecer los lineamientos generales que permitan garantizar la **confidencialidad, integridad y disponibilidad** de los servicios de comunicaciones y de la información gestionada, procesada o almacenada por **COVINET INGENIERÍA SAS**, en cumplimiento de los estándares internacionales ISO/IEC 27000 y de la normativa establecida por la Comisión de Regulación de Comunicaciones (CRC).

2. Alcance

El Sistema de Gestión de Seguridad de la Información (SGSI) será aplicado a todos los procesos, servicios y sistemas de información de **COVINET INGENIERÍA SAS**, incluyendo:

- Infraestructura de red (OLT, switches, routers, servidores, firewall).
- Servicios prestados a clientes (Internet fijo).
- Información de clientes, proveedores, empleados y datos críticos de operación.
- Procedimientos internos de gestión, monitoreo y reporte de incidentes de seguridad.

3. Objetivos

COVINET INGENIERIA SAS identifica los aspectos relevantes para garantizar su:

1. **Confidencialidad:** La información será accesible únicamente por personal autorizado.
2. **Integridad:** La información y los sistemas se mantendrán íntegros, sin alteraciones indebidas.
3. **Disponibilidad:** Los servicios y la información estarán disponibles de forma oportuna para los usuarios y autoridades competentes.
4. Establecer un proceso de mejora continua en ciberseguridad.

4. Gestión de Riesgos

- Se identifican, evalúan y tratan los riesgos relacionados con la seguridad de la información, teniendo en cuenta amenazas internas, externas y vulnerabilidades tecnológicas.
- Se aplicarán controles de seguridad siguiendo las directrices de la norma ISO/IEC 27001: políticas, procedimientos, controles físicos, lógicos y administrativos.

5. Incidentes de Seguridad de la Información

5.1. Verificación de la identificación del incidente

COVINET INGENIERIA SAS ha establecido un procedimiento formal de monitoreo, detección y registro de incidentes, cuyo propósito es garantizar la protección de la red, los datos de los clientes y la continuidad del servicio.

Para verificar que los incidentes están siendo identificados, la empresa ha dispuesto los siguientes mecanismos:

- Sistema de monitoreo (PRTG): Alertar automáticas de anomalías de trafico
- Revisión de logs de seguridad (Firewall Mikrotik): Registro y alertas de ataques con sus respectivos bloqueos.
- Reportes internos del personal técnico y usuarios: Los empleados y clientes pueden reportar eventos sospechosos.

5.2. Proceso de identificación de incidentes

El procedimiento definido consta de las siguientes etapas:

- Detección: El evento es identificado mediante el sistema de monitoreo, alertas automáticas o reporte humano.
- Clasificación inicial: Se evalúa si corresponde a un incidente de seguridad de la información según la topología definida.
    - Denegación del servicio
    - Acceso no autorizado
    - Malware
    - Abuso

    - Recopilación de información
- Registro inmediato: Todo incidente debe registrase en el sistema de gestión de ticket e incidencias.

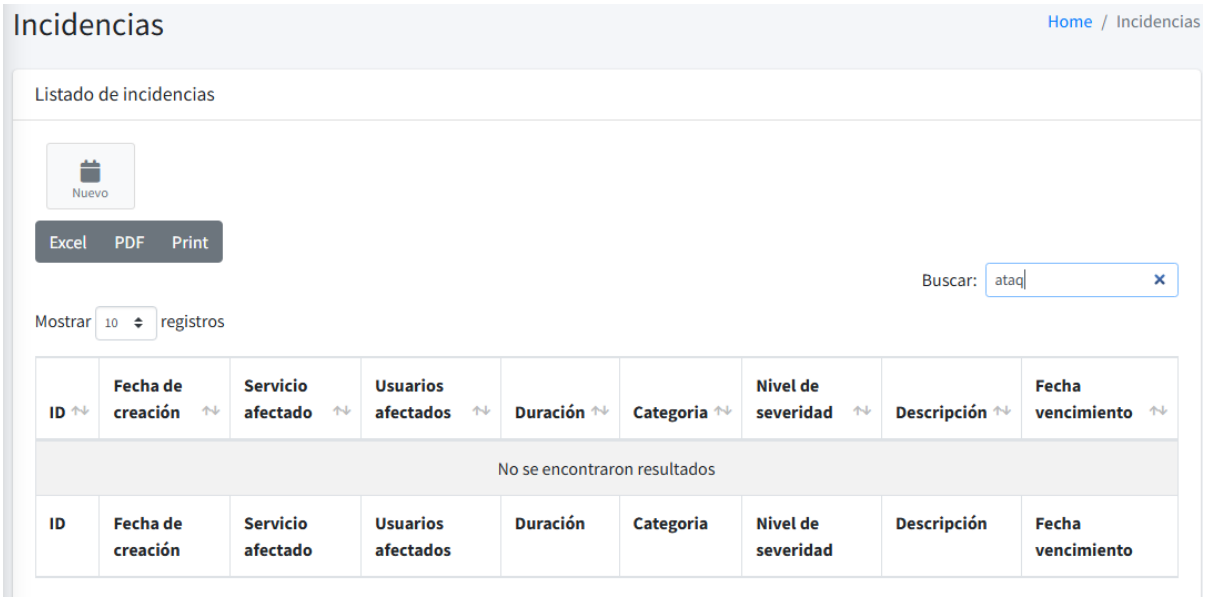
5.3. Sistema de gestión de ticket e incidencias

Los incidentes se registran en el sistema de gestión la cual permite:

- Registro centralizado de todos los eventos
- Tener un control de cada caso y su respectivo estado
- Conservación mínima de 1 año, conforme a los requisitos de la CRC

5.4. Información mínima registrada será:

- Fecha del incidente.
- Servicio afectado.
- Número de usuarios afectados.
- Duración del incidente (horas).
- Categoría del incidente
- Nivel de seguridad del incidente
    - Clase IV: Muy serio.
    - Clase III: Serio.
    - Clase II: Menos serio.
    - Clase I: Pequeño.



5.5. Reporte de Incidentes

Después de la contención, erradicación o recuperación, se enviará un reporte oficial a colCERT o la entidad que haga sus veces. El reporte incluirá: fecha, servicio afectado, usuarios afectados, duración, categoría del incidente, nivel de severidad, descripción del incidente y acciones de mitigación.

Fecha	Servicio afectado	Usuarios afectados	Duración	Categoría	Nivel de severidad	descripción	Acciones de mitigación

- **Plazos de reporte:**
  - Hasta 3 meses posteriores a la detección del incidente (para todos los incidentes).
  - Dentro de 24 horas hábiles siguientes a la detección, cuando el incidente sea clasificado como Clase III (Serio) o Clase IV (Muy serio)**.**

6. Responsabilidades

- **Gerencia de COVINET INGENIERÍA SAS:** Aprobar y garantizar los recursos para el SGSI.
- **Área de Seguridad de la Información / NOC:** Implementar controles, monitorear y gestionar incidentes.
- **Empleados:** Cumplir con las políticas establecidas y reportar cualquier incidente.
- **Proveedores:** Adoptar controles de seguridad acordes a los lineamientos contractuales y normativos.

7. Formación y Concientización

COVINET INGENIERÍA SAS desarrollará programas de capacitación periódica para todos los colaboradores, con el fin de garantizar la comprensión y correcta aplicación de las políticas de seguridad de la información.

8. Vigencia y Actualización

La presente Política entra en vigencia a partir de su aprobación por la Gerencia General de **COVINET INGENIERÍA SAS** y deberá ser revisada anualmente o cuando se presenten cambios regulatorios, tecnológicos o de riesgos que lo ameriten.