Política general de seguridad y privacidad de la información

Gestión de riesgos, continuidad y protección de la información.

NOVANET COLOMBIA SAS establece lineamientos para proteger la confidencialidad, integridad y disponibilidad de la información y sus servicios. La empresa debe implementar y mejorar un Sistema de Gestión de Seguridad de la Información acorde con su operación y riesgos, tomando como referencia la familia ISO/IEC 27000 y las obligaciones aplicables.

Esta política no afirma una certificación ISO ni una implementación técnica ya auditada. La evidencia de cumplimiento se conserva en registros y controles de la operación, no en la sola publicación del documento.

1. Alcance y objetivos

Comprende internet fijo, infraestructura bajo control de la empresa, soporte, facturación, atención al usuario y la información administrada en esas actividades. Aplica al personal y terceros con acceso por su función o contrato.

- Identificar activos y riesgos para la continuidad y los derechos de los usuarios.
- Asignar responsables, controles y registros verificables para tratar los riesgos.
- Identificar, conservar y reportar incidentes conforme al régimen aplicable.
- Revisar resultados y corregir las debilidades encontradas.

2. Responsabilidades

Función	Responsabilidad
Representación Legal	Aprobar la política, asignar recursos y responsables, aceptar los riesgos que le correspondan y revisar resultados.
Responsable técnico designado	Inventarios y riesgos técnicos; administración de accesos, cambios y respaldos; incidentes y evidencias.
Atención y administración	Recibir reportes y PQR, proteger datos y coordinar comunicaciones autorizadas.
Personal y contratistas	Usar accesos solo para sus funciones, guardar confidencialidad y reportar eventos, vulnerabilidades o pérdidas.

Las personas responsables y sus suplencias deben constar en el registro interno. Las funciones no presuponen departamentos independientes ni cargos adicionales.

Controles y gestión de riesgos

3. Activos y evaluación de riesgos

Mantener un inventario con responsable, ubicación lógica o física y criticidad. Evaluar amenazas, vulnerabilidades, impacto y probabilidad. Cada tratamiento debe tener responsable, plazo, prioridad y evidencia de ejecución.

4. Accesos e información

Autorizar accesos por función; evitar cuentas compartidas cuando sea viable; retirar permisos al terminar la relación y revisar accesos privilegiados. Usar claves robustas y autenticación adicional compatible. Clasificar la información pública, interna y restringida y limitar su circulación.

5. Red y equipos

Documentar configuración aprobada, controlar cambios y actualizar equipos según riesgo y compatibilidad. Proteger interfaces de administración y aplicar mecanismos de autenticación, control de acceso, confidencialidad e integridad que correspondan al servicio y a la arquitectura UIT-T X.800 para redes fijas.

6. Respaldos y continuidad

Definir información a respaldar, frecuencia, ubicación, responsables y retención según criticidad. Proteger copias y comprobar restauraciones. Definir prioridades de recuperación, contactos de escalamiento y alternativas de operación.

7. Proveedores y trabajo remoto

Establecer obligaciones de confidencialidad y seguridad, controlar accesos temporales y cambios de terceros. Las conexiones remotas deben autorizarse y protegerse. El uso de dispositivos personales requiere condiciones acordadas y proporcionales al riesgo.

8. Privacidad y uso responsable

Tratar datos con finalidad legítima, autorización cuando proceda, seguridad y conservación limitada. Respetar neutralidad y aplicar restricciones exigibles con fundamento, alcance y trazabilidad. Consulte la política de datos y el procedimiento de bloqueo.

> Los usuarios pueden reportar una sospecha por novanetcolombia@gmail.com o por los teléfonos publicados. Nunca deben entregar claves, códigos de recuperación o datos de terceros innecesarios.

Incidentes, revisión y adopción

9. Respuesta a incidentes

Todo evento sospechoso debe registrarse y evaluarse. La respuesta comprende detección, clasificación, contención, recuperación y revisión de causas. Se preserva evidencia, se limita el acceso y se documentan acciones, tiempos y responsables.

Etapa	Registro mínimo
Detección y evaluación	Fecha y hora; servicio y activos afectados; síntomas y fuente del reporte; categoría y severidad.
Contención y recuperación	Responsable, acciones realizadas, cambios autorizados, respaldo utilizado y validación del restablecimiento.
Cierre y mejora	Duración, usuarios afectados, causa, medidas preventivas, comunicaciones y soportes de reporte.

10. Conservación y reportes regulatorios

Conservar por incidente, como mínimo durante un año, fecha de inicio, servicio afectado, número de usuarios externos afectados, duración en horas, categoría y severidad conforme al Anexo 5.8 de la Resolución CRC 5050 de 2016. El registro puede ampliarse con detección, cierre, responsables y soportes.

Se atenderán los reportes a colCERT o quien haga sus veces previstos en el artículo 5.1.2.3: una vez cerrado el incidente y dentro de los tres meses siguientes a su detección; para severidades III o IV, también el reporte inicial dentro de las 24 horas hábiles siguientes a su detección. Se verifica el mecanismo oficial vigente y se guarda constancia de envío. Las obligaciones por afectación de datos personales se evalúan por separado.

11. Revisión y mejora

La empresa revisará la política al menos anualmente y ante cambios o incidentes relevantes. Evaluará riesgos, accesos pendientes, restauraciones e incidentes. Las acciones correctivas tendrán responsable y seguimiento. Cualquier incumplimiento se atenderá mediante los procedimientos legales, contractuales o laborales aplicables, respetando el debido proceso.

12. Aprobación y vigencia

La política entra en aplicación con aprobación del representante legal. El acta o registro interno identificará fecha, versión, responsable técnico y plan inicial de implementación. La versión pública omite configuraciones, inventarios sensibles y credenciales. Se comunicarán los cambios que afecten a los usuarios.

Referencias y consulta

CRC 5050 de 2016 · artículo 5.1.2.3 y Anexo 5.8

Ley 1581 de 2012