POLÍTICA DE SEGURIDAD INFORMÁTICA

COMUNICADORES DEL ECUADOR COMUNIDOR S.A.

1. Introducción

La seguridad de la información es un pilar estratégico para **COMUNIDOR S.A.**, empresa especializada en soluciones de radiocomunicación y telecomunicaciones. Esta política establece los principios, lineamientos y responsabilidades para proteger la **confidencialidad**, **integridad** y **disponibilidad** de la información y de los sistemas que la procesan, almacenan o transmiten.

Esta política se alinea con la **Ley Orgánica de Protección de Datos Personales del Ecuador (LOPDP)**, regulaciones de **ARCOTEL**, y estándares internacionales de seguridad de la información (como ISO/IEC 27001).

2. Objetivo

Garantizar la protección de los activos de información de COMUNIDOR frente a amenazas internas o externas, deliberadas o accidentales, que puedan comprometer los servicios prestados, la privacidad de los datos personales o la continuidad operativa.

3. Alcance

Aplica a todos los colaboradores, contratistas, proveedores, técnicos de campo, operadores de red, y cualquier tercero que tenga acceso a los activos informáticos y de red de COMUNIDOR, incluyendo:

- Servidores de datos (facturación, servicios web, sistemas de telecomunicaciones, NAS).
- Infraestructura interconectada en los sitios de COMUNIDOR S.A.
- Antenas de datos, dispositivos de red, consolas de configuración y sistemas SCADA (si aplica).

4. Principios Generales

- **Confidencialidad:** La información solo será accesible para personas autorizadas.
- **Integridad:** La información será completa, exacta y protegida contra modificaciones no autorizadas.

-

- **Disponibilidad:** La información y los sistemas estarán accesibles cuando se necesiten.

  Responsabilidad: Todo acceso, uso o administración de sistemas debe ser rastreable.

- **Prevención y respuesta:** Se implementarán medidas para prevenir incidentes y responder ante ellos.

5. Lineamientos Generales de Seguridad

5.1. Gestión de Activos

- Todos los activos de información deben estar inventariados y categorizados.
- Se asignarán responsables por cada sistema o servicio.

5.2. Control de Accesos

- Se utilizarán mecanismos de autenticación fuerte (contraseñas robustas, MFA).
- El acceso a servidores, routers, radios, y consolas debe ser limitado según el principio de **mínimo privilegio**.
- Cada usuario debe tener credenciales únicas; se prohíbe compartir contraseñas.

5.3. Gestión de Usuarios

- Todos los accesos serán registrados y auditables.
- Se eliminarán cuentas inactivas o de usuarios desvinculados inmediatamente.
- Se aplicará segregación de funciones (administradores vs. usuarios operativos).

5.4. Seguridad en la Red

- Se segmentará la red entre servicios críticos y administrativos.
- Se utilizarán firewalls, VPN seguras y control de tráfico entre sedes.
- Se monitoreará el uso de ancho de banda y se aplicarán medidas ante detección de anomalías.

•

5.5. Seguridad en Sitios Remotos

- El acceso a infraestructura remota (torres, enlaces de microondas) deberá realizarse por personal autorizado.
- Se mantendrán registros de visitas, mantenimientos y cambios de configuración.

  Toda configuración remota debe registrarse en un sistema de control de versiones.

5.6. Respaldo y Recuperación

- Se realizarán respaldos automáticos diarios de servidores críticos.
- Se almacenarán copias fuera del sitio (offsite o en la nube privada).
- Se probará el plan de recuperación ante desastres (DRP) al menos dos veces al año.

5.7. Seguridad Física

- Acceso a centros de datos o racks de comunicación debe estar restringido.
- Se instalarán cámaras de vigilancia, sensores de apertura y sistemas de alarma.
- Todo ingreso deberá registrarse en bitácoras o sistemas de control de acceso.

5.8. Protección contra Malware

- Se instalarán soluciones antivirus y antimalware en todos los equipos de usuario y servidores.
- Se limitará la ejecución de software no autorizado.
- Se bloqueará el uso de dispositivos USB sin autorización previa.

5.9. Gestión de Vulnerabilidades

- Se aplicarán parches y actualizaciones de seguridad en sistemas operativos, software y firmware.
- Se realizarán escaneos de vulnerabilidades periódicos.
- Se mantendrá actualizado un registro de brechas y acciones correctivas.

•

6. Registro y Manejo de Incidentes

Todo incidente de seguridad debe ser reportado al Equipo de Seguridad Informática mediante el correo: **privacidad@comunidor.com**
Los incidentes serán clasificados, investigados y tratados conforme al protocolo de respuesta definido en el Plan de Continuidad de Negocio (BCP).

7. Capacitación y Concienciación

- Todos los empleados y contratistas recibirán formación anual sobre seguridad informática y protección de datos.

  Se realizarán simulacros de phishing y campañas de buenas prácticas digitales.

- El incumplimiento de esta política será sancionado conforme al reglamento interno de trabajo.

8. Evaluación y Auditoría

- Se auditarán periódicamente los sistemas críticos y accesos a datos.
- Se revisará la eficacia de las políticas y controles técnicos cada 12 meses.
- Se mantendrán evidencias de cumplimiento para fines regulatorios y legales.

9. Revisión y Actualización

Esta política será revisada y actualizada cada año o cuando existan cambios tecnológicos, normativos o estructurales relevantes.

Fecha de emisión: 28 de marzo de 2025
Aprobado por: Gerencia General – COMUNIDOR S.A.
Revisión programada: Marzo 2026