Política de Seguridad de la Información

Versión Pública

1. Objetivos y Principios

La política busca proteger tres pilares fundamentales:

- **Confidencialidad:** Acceso solo a personal autorizado.
- **Integridad:** Información exacta y completa.
- **Disponibilidad:** Acceso garantizado cuando se requiera.

2. Alcance

Es aplicable a **todas las personas** que interactúen con la infraestructura o información de la organización: empleados, colaboradores externos y proveedores.

3. Responsabilidades

- **Dirección:** Compromiso con la cultura de seguridad, asignación de recursos y definición de roles.
- **Responsable de Seguridad:** Supervisar el cumplimiento, actualizar políticas, gestionar incidentes (punto de contacto) y coordinar capacitaciones.
- **Empleados:** Obligación de cumplir la política y reportar incidentes de inmediato.

4. Lineamientos de Desarrollo (Compromisos)

- **Gestión de Riesgos e Incidentes:** Evaluación sistemática de riesgos y alineación con las pautas del **CERTuy** para incidentes.
- **Continuidad y Resiliencia:** Implementación de planes para mantener servicios críticos ante fallos.
- **Clasificación y Uso Legal:** La información se clasifica por criticidad y se procesa solo para fines organizacionales legítimos.
- **Proveedores:** Deben adoptar los mismos principios de seguridad de la organización.
- **Cultura y Capacitación:** Programas permanentes de sensibilización y formación ética en seguridad.

5. Control y Sanciones

- La política se mantiene vigente mediante revisiones de la dirección y auditorías internas.
- **Consecuencias:** El incumplimiento conlleva medidas disciplinarias según el reglamento interno y la ley.