Instituto de Movilidad de Pereira

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2025

Versión 1

Subdirección de Sistemas de Información y Telemática

Instituto de Movilidad de Pereira

Pereira, enero de 2025

Carrera 14 No. 17 - 60 Locales 4 - 5 y 6 Centro Comercial APEX
PBX: (606) 329 4920 - PEREIRA, RISARALDA
contactenos@movilidadpereira.gov.co
www.movilidadpereira.gov.co

CONTENIDO

1.INTRODUCCIÓN

Propósito: Garantizar la seguridad, confidencialidad, integridad y disponibilidad de la información gestionada por el Instituto de Movilidad Pereira.

Alcance: Este plan abarca toda la información administrada por el Instituto, tanto en formato físico como digital, incluyendo sistemas, procesos y usuarios internos y externos.

Marco normativo: Este plan se fundamenta en las normativas aplicables, tales como:

Ley 1581 de 2012 (Protección de Datos Personales)

Decreto 1377 de 2013

ISO 27001 (Gestión de Seguridad de la Información)

Políticas internas y otros lineamientos legales nacionales e internacionales.

2.OBJETIVOS DEL PLAN

Proteger los activos de información del Instituto contra accesos no autorizados, alteraciones indebidas y pérdidas.

Cumplir con las normativas legales y regulaciones locales relacionadas con la seguridad y privacidad de la información.

Definir responsabilidades claras para todos los involucrados en la gestión de la información.

Promover una cultura organizacional de seguridad y privacidad de la información.

---

3. POLÍTICAS DE SEGURIDAD Y PRIVACIDAD

Confidencialidad: Asegurar que solo el personal autorizado acceda a la información sensible.

Integridad: Garantizar que los datos permanezcan completos y no sean alterados de manera indebida.

Disponibilidad: Mantener los sistemas y datos accesibles para los usuarios autorizados en el momento requerido.

Cumplimiento: Adherirse a todas las leyes, normativas y estándares relevantes.

---

4. CLASIFICACIÓN DE LA INFORMACIÓN

Información pública: Datos que pueden ser divulgados libremente (ejemplo: horarios de atención, servicios disponibles).

Información restringida: Datos operativos internos del Instituto (ejemplo: reportes internos, planes operativos).

Información confidencial: Información personal y sensible de ciudadanos, empleados y terceros (ejemplo: datos personales, sanciones, procesos judiciales).

---

5. GESTIÓN DE RIESGOS

Identificación de riesgos:

Análisis de amenazas internas y externas.

Evaluación de vulnerabilidades en los sistemas tecnológicos y procesos.

Análisis de impacto:

Determinar las consecuencias potenciales de incidentes de seguridad.

Planes de mitigación:

Implementar controles de seguridad para reducir los riesgos.

Actualizar y reforzar sistemas tecnológicos.

---

6. Roles y Responsabilidades

Responsable de Seguridad de la Información:

Liderar la implementación del plan.

Realizar auditorías y coordinar la capacitación del personal.

Usuarios del sistema:

Cumplir con las políticas establecidas y reportar cualquier incidente de seguridad.

Proveedores externos:

Garantizar que los servicios proporcionados cumplan con los estándares de seguridad establecidos.

7. Medidas de Seguridad

Seguridad física:

Control de acceso a las instalaciones (tarjetas de acceso, registros de visitantes).

Monitoreo mediante cámaras de vigilancia.

Seguridad lógica:

Implementación de contraseñas seguras.

Uso de cifrado para proteger datos sensibles.

Instalación y actualización de firewalls y sistemas antivirus.

Capacitación del personal:

Entrenamientos periódicos en temas de seguridad y privacidad de la información.

---

8. Gestión de Incidentes de Seguridad

Detección y notificación:

Implementar herramientas de monitoreo para identificar incidentes.

Establecer un canal claro para reportar eventos de seguridad.

Respuesta:

Acciones inmediatas para contener y mitigar el impacto del incidente.

Recuperación:

Restaurar los sistemas afectados y analizar el incidente para evitar futuras ocurrencias.

---

9. Auditorías y Evaluaciones

Realizar auditorías internas y externas periódicas para verificar el cumplimiento del plan.

Actualizar el plan regularmente para adaptarse a cambios tecnológicos, normativos y organizacionales.

---

10. Anexos

Glosario de términos: Definiciones de conceptos clave relacionados con seguridad y privacidad.

Formatos:

- Registro de incidentes de seguridad.
- Declaraciones de confidencialidad para el personal.
- Lista de referencias legales y normativas aplicables: Normas y estándares utilizados como base para este plan.