MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

MSPI

DIAGNOSTICENTRO DE RISARALDA

Diciembre de 2025

1. Objetivo del Modelo

Establecer el **Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI)** del Centro de Diagnóstico Automotor de Risaralda EICE (en adelante "el Diagnosticentro"), con el fin de **proteger la confidencialidad, integridad y disponibilidad** de la información que administra, incluyendo:

- Información misional de RTM y Estación de Servicio.
- Datos personales de usuarios, funcionarios, proveedores y terceros.
- Información financiera, contractual, técnica y administrativa.

El modelo se basa en el **Modelo de Seguridad y Privacidad de la Información – MSPI del MinTIC** y en el ciclo PHVA (Planear, Hacer, Verificar y Actuar).

---

2. Alcance

El MSPI del Diagnosticentro aplica a:

- **Procesos misionales**:
    - Revisión Técnico–Mecánica y de emisiones contaminantes.
    - Operación de la Estación de Servicio (24 horas).
- **Procesos de apoyo y estratégicos**:
    - Talento humano, contratación, financiera–contable, sistemas de información, atención al ciudadano, transparencia, control interno.

Incluye toda la información en **soporte físico y digital**, sistemas de información, infraestructura tecnológica, personal propio y contratistas que traten información de la entidad.

---

3. Marco normativo de referencia

Entre otras, el modelo se soporta en:

- Constitución Política (arts. 15, 209 y 269).
- Ley 1581 de 2012 y decretos reglamentarios (protección de datos personales).
- Ley 1712 de 2014 y Decreto 103 de 2015 (transparencia y acceso a la información).

- Ley 594 de 2000 y Decreto 2609 de 2012 (gestión documental).
- Decreto 1078 de 2015 y Decreto 767 de 2022 (Política de Gobierno Digital y Seguridad Digital).
- Resolución 500 de 2021 MinTIC (estrategia de seguridad digital y adopción del MSPI).
- Norma ISO/IEC 27001:2022 como referencia de buenas prácticas.

---

4. Principios

El MSPI del Diagnosticentro se rige por los siguientes principios:

1. **Confidencialidad**: la información solo es accesible a personas autorizadas.
2. **Integridad**: la información es exacta, completa y no ha sido manipulada indebidamente.
3. **Disponibilidad**: la información y los servicios críticos (RTM y Estación de Servicio) están disponibles cuando se requieren.
4. **Legalidad y finalidad** en el tratamiento de datos personales.
5. **Necesidad y minimización de datos**: se recolecta solo la información estrictamente necesaria.
6. **Responsabilidad demostrada**: el Diagnosticentro debe poder demostrar el cumplimiento de sus obligaciones en seguridad y privacidad.

---

5. Gobernanza, roles y responsabilidades

5.1 Comité Institucional de Gestión y Desempeño

Se le asignan, mediante acto administrativo, las funciones de **dirección y seguimiento del MSPI**, incluyendo:

- Aprobar la **Política de Seguridad y Privacidad de la Información**.
- Asignar recursos (presupuesto, personal y tiempo).
- Revisar al menos dos veces al año los avances del MSPI.

5.2 Responsable de Seguridad y Privacidad de la Información

La Gerencia designará (por resolución) un **Responsable de Seguridad y Privacidad de la Información**, con las funciones de:

- Coordinar la implementación del MSPI.
- Liderar la identificación de activos y riesgos.
- Gestionar incidentes de seguridad de la información.
- Coordinar capacitaciones y campañas de sensibilización.

5.3 Propietarios de activos de información

Cada líder de proceso (RTM, estación de servicio, talento humano, contabilidad, etc.) será **propietario de los activos de información** de su proceso y deberá:

- Identificar y clasificar sus activos de información.
- Identificar y gestionar riesgos asociados a esos activos.

---

6. Gestión de Activos y Riesgos

6.1 Inventario y clasificación de activos

El Diagnosticentro mantendrá un **Inventario de Activos de Información** (como el que ya construimos), donde se identifiquen al menos:

- Nombre del activo.
- Descripción.
- Proceso al que pertenece.
- Responsable.
- Soporte (físico/digital).
- Clasificación (público, reservado, confidencial).

6.2 Gestión de riesgos de seguridad de la información

Se adoptará una **metodología simple de riesgos**, alineada con el MSPI, que incluya:

1. Identificar amenazas y vulnerabilidades que puedan afectar la confidencialidad, integridad, disponibilidad o privacidad de la información (ej.: pérdida de certificados RTM, ataque a la base de datos, fuga de datos personales, indisponibilidad de sistemas).

2. Valorar probabilidad e impacto.
3. Determinar nivel de riesgo (bajo, medio, alto).
4. Definir **planes de tratamiento de riesgos**:
    - Evitar
    - Mitigar (controles)
    - Transferir
    - Aceptar (si está dentro del apetito de riesgo).

El **Plan de Tratamiento de Riesgos** será un documento vivo, revisado al menos una vez al año.

---

7. Controles básicos de Seguridad de la Información

Sin entrar al detalle de todos los controles ISO 27001, el Diagnosticentro adoptará un **mínimo de controles básicos**, agrupados así:

7.1 Controles organizacionales

- Política de Seguridad y Privacidad de la Información aprobada por la Gerencia.
- Políticas de uso aceptable de recursos tecnológicos.
- Cláusulas de confidencialidad para funcionarios y contratistas.
- Procedimientos de gestión de cambios en sistemas.

7.2 Controles físicos

- Control de acceso a áreas críticas (líneas RTM, oficinas con información sensible, cuartos de equipos).
- Protección de documentos físicos (archivo restringido, llave, acceso autorizado).

7.3 Controles tecnológicos

- Usuarios y contraseñas personalizadas para sistemas de información.
- Cambios periódicos de contraseñas y bloqueo automático tras varios intentos fallidos.
- Antivirus y actualizaciones de seguridad.

- Copias de seguridad (backups) de bases de datos de RTM, facturación y demás sistemas.
- Control de acceso remoto (VPN, si aplica) y registro de accesos.

---

8. Privacidad y Protección de Datos Personales

El Diagnosticentro, como **responsable del tratamiento de datos personales**, adoptará al menos:

1. **Política de Tratamiento de Datos Personales**, publicada en la web.
2. Registro de bases de datos personales ante la **Superintendencia de Industria y Comercio**, cuando aplique.
3. Procedimiento para atención de **derechos de los titulares** (consultas, reclamos, actualización o supresión).
4. Mecanismos de protección:
    - Acceso controlado a información personal.
    - Uso de datos anonimizados o agregados cuando se publiquen estadísticas (p.ej. en datos abiertos).
    - Cifrado o seudonimización cuando aplique.

---

9. Gestión de incidentes de Seguridad y Privacidad

Se definirá un **Procedimiento de Gestión de Incidentes**, que contemple:

1. **Detección y reporte**: cualquier funcionario o contratista puede reportar incidentes (pérdida de información, acceso no autorizado, malware, etc.) al Responsable de Seguridad de la Información.
2. **Clasificación y análisis** del incidente.
3. **Contención y recuperación** (por ejemplo, aislar equipos, restaurar backups, cambiar claves).
4. **Notificación** a autoridades (SIC, MinTIC, COLCERT, según el caso) cuando exista afectación relevante de datos personales o infraestructura.
5. Registro y lecciones aprendidas para evitar la recurrencia.

---

10. Capacitación y Cultura de Seguridad

Anualmente, la entidad realizará:

- Jornadas de sensibilización para todo el personal sobre:
    - manejo seguro de la información,
    - protección de datos personales,
    - phishing, ingeniería social,
    - responsabilidades disciplinarias por mal uso de información.
- Inducción en seguridad y privacidad para todo nuevo funcionario o contratista.

---

11. Seguimiento, auditoría y mejora continua

En línea con el MSPI, el Diagnosticentro se compromete a:

1. **Monitorear** el cumplimiento del modelo mediante indicadores básicos, por ejemplo:
    - Número de incidentes reportados y gestionados.
    - Porcentaje de activos inventariados y clasificados.
    - Porcentaje de personal capacitado.
2. Realizar al menos **una auditoría interna anual** del MSPI.
3. El Comité Institucional de Gestión y Desempeño hará una **revisión anual** del MSPI para:
    - Revisar resultados,
    - Aprobar acciones de mejora,
    - Ajustar el alcance, políticas o controles.
4. Documentar **acciones correctivas** cuando se identifiquen no conformidades o incidentes relevantes.