PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

2026

Agencia Logística de Gestión Inmobiliaria y Servicios de Cundinamarca
Sede Administrativa Calle 26 #51-53. Torre Beneficencia Piso 3.
Bogotá, D.C.
/CundiGob @CundinamarcaGob
www.cundinamarca.gov.co

Tabla de contenido

Agencia Logística de Gestión Inmobiliaria y Servicios de Cundinamarca
Sede Administrativa Calle 26 #51-53. Torre Beneficencia Piso 3.
Bogotá, D.C.
/CundiGob @CundinamarcaGob
www.cundinamarca.gov.co

Introducción

La Agencia Logística de Gestión Inmobiliaria y Servicios de Cundinamarca gestiona información crítica para el cumplimiento de sus funciones misionales, estratégicas y de apoyo, por lo cual resulta indispensable adoptar un enfoque sistemático para la gestión de los riesgos de seguridad de la información.

El presente Plan de Tratamiento de Riesgos de Seguridad de la Información se constituye como una herramienta operativa que permite identificar, analizar y tratar los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información institucional, en coherencia con los requisitos normativos y del Modelo Integrado de Planeación y Gestión – MIPG.

Este instrumento articula:

- La Guía de Administración Integral de Riesgos del DAFP (versión 7).
- Los resultados del Índice de Desempeño Institucional – IDI 2024 (FURAG), dimensión Seguridad Digital.
- Los lineamientos de la Política Nacional de Seguridad Digital – CONPES 3995 de 2020.
- Los controles y buenas prácticas de los estándares ISO/IEC 27001:2022 y NIST Cybersecurity Framework (CSF).

Con ello, la Agencia fortalece su capacidad de prevención, detección, respuesta y recuperación frente a incidentes de seguridad digital, incrementando su nivel de madurez institucional y reduciendo el impacto operativo, legal, financiero y reputacional derivado de eventos de ciberseguridad.

Importancia de la Gestión de Riesgos de Seguridad de la Información

La gestión de riesgos de seguridad de la información es un elemento estratégico

para la Agencia, en la medida en que:

- Garantiza la continuidad de los servicios institucionales.
- Protege los activos de información frente a amenazas internas y externas.

- Reduce la probabilidad e impacto de incidentes cibernéticos, como ataques de ransomware.
- Fortalece la confianza de las partes interesadas de la Agencia y de los entes de control.
- Aporta al cumplimiento normativo y al mejoramiento del índice de Desempeño Institucional IDI – FURAG.

La implementación efectiva de esta matriz permite una toma de decisiones informada, priorizando los riesgos críticos y orientando los recursos hacia controles que generen mayor valor público.

2.1 Marco de referencia:

- Plan de Seguridad y Privacidad de la Información de la Agencia
- Guía de Administración Integral de Riesgos – DAFP, Versión 7
- Resultados IDI 2024 – FURAG (Dimensión Seguridad Digital)
- CONPES 3995 de 2020 – Política Nacional de Seguridad Digital

Objetivo

Ejecutar el tratamiento de los riesgos de seguridad de la información identificados en la Agencia Logística de Gestión Inmobiliaria y Servicios de Cundinamarca, mediante la aplicación de controles técnicos, administrativos y operativos, alineados con la Guía de Administración Integral de Riesgos del DAFP (v.7) y las recomendaciones derivadas del IDI 2024 – FURAG, con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información.

Alcance

Este plan aplica a todos los procesos misionales, estratégicos, de apoyo y de evaluación, así como a los activos de información, sistemas de información, infraestructura tecnológica, usuarios internos y terceros que interactúan con la información de la entidad.

Metodología para el Tratamiento del Riesgo

De conformidad con la Guía DAFP v.7, el tratamiento de riesgos se define a partir de:

- Riesgos identificados en el Mapa de Riesgos de Seguridad de la Información.
- Nivel de riesgo residual (Alto, Medio o Bajo).
- Opciones de tratamiento: Mitigar, Evitar, Transferir o Aceptar.
- Definición de controles, responsables, recursos y plazos.

Este plan prioriza los riesgos Altos y Medios, especialmente aquellos relacionados con ciberseguridad, continuidad del servicio y pérdida de información, conforme a los resultados del IDI 2024.

Estrategia General de Tratamiento

La Agencia adoptará una estrategia de mitigación enfocada en:

- Fortalecimiento del gobierno de la seguridad digital.
- Protección de la información mediante respaldos seguros.
- Gestión adecuada de incidentes cibernéticos.
- Continuidad y recuperación ante desastres.
- Gestión de vulnerabilidades y actualizaciones.

Plan de Tratamiento de Riesgos (Seguridad Digital)

Designación de un responsable de Seguridad Digital

- **Riesgo asociado:** Falta de gobernanza y control en seguridad de la información.
- **Tratamiento:** Mitigar.
- **Acción:** Designar formalmente un área o responsable de Seguridad Digital, con funciones claras en gestión de riesgos, incidentes, continuidad y cumplimiento normativo.
- **Responsable:** Dirección / Oficina TIC.
- **Resultado esperado:** Gobernanza clara y fortalecida en seguridad digital.

Separación de equipos de respaldo

- **Riesgo asociado:** Compromiso simultáneo de información productiva y respaldos (Ransomware).
- **Tratamiento:** Mitigar.

- **Acción:** Separar los equipos destinados a copias de respaldo del software, imágenes de sistemas y de la red principal de servidores y computadores.
- **Responsable:** Dirección Administrativa y Financiera a través del profesional de gestión tecnológica.
- **Resultado esperado:** Reducción del impacto de ataques cibernéticos.

Almacenamiento aislado de copias de respaldo

- **Riesgo asociado:** Pérdida total de información por accesos no autorizados o ataques.
- **Tratamiento:** Mitigar.
- **Acción:** Almacenar las copias de respaldo en un entorno aislado, en un segmento de red independiente al de servidores y estaciones de trabajo.
- **Responsable:** Oficina TIC.
- **Resultado esperado:** Mayor resiliencia y protección de la información.

Pruebas periódicas de respaldos

- **Riesgo asociado:** Indisponibilidad de información crítica en caso de incidente.
- **Tratamiento:** Mitigar.
- **Acción:** Realizar pruebas programadas de restauración de respaldos de los aplicativos misionales, estratégicos, de soporte y mejora, coordinadas con los responsables de proceso.
- **Responsable:** Oficina TIC / Líderes de proceso.
- **Resultado esperado:** Disponibilidad y confiabilidad de la información.

Implementación del Plan de Recuperación de Desastres (DRP)

- **Riesgo asociado:** Interrupción prolongada de los servicios institucionales.
- **Tratamiento:** Mitigar.
- **Acción:** Definir, documentar e implementar un Plan de Recuperación de Desastres (DRP) que cubra todos los procesos y sistemas críticos de la entidad.
- **Responsable:** Oficina TIC / Comité Institucional de Gestión y Desempeño.
- **Resultado esperado:** Continuidad operativa ante eventos críticos.

Pruebas de recuperación de sistemas críticos

- **Riesgo asociado:** Fallas en la recuperación efectiva de los sistemas de información.
- **Tratamiento:** Mitigar.
- **Acción:** Realizar pruebas periódicas de recuperación de los sistemas de información críticos, documentando resultados y planes de mejora.
- **Responsable:** Oficina TIC.
- **Resultado esperado:** Validación de la efectividad del DRP.

Gestión de incidentes de seguridad digital

- **Riesgo asociado:** Respuesta inadecuada a incidentes cibernéticos.
- **Tratamiento:** Mitigar.
- **Acción:** Establecer, documentar e implementar un procedimiento para la gestión de incidentes de seguridad digital, incluyendo la notificación a CSIRT Gobierno y COLCERT.
- **Responsable:** Oficina TIC / Responsable de Seguridad Digital.
- **Resultado esperado:** Respuesta oportuna y coordinada ante incidentes.

Retest de vulnerabilidades y parches de seguridad

- **Riesgo asociado:** Explotación de vulnerabilidades técnicas.
- **Tratamiento:** Mitigar.
- **Acción:** Realizar retest periódicos para verificar la mitigación de vulnerabilidades y la correcta aplicación de actualizaciones y parches de seguridad.
- **Responsable:** Oficina TIC.
- **Resultado esperado:** Reducción del riesgo de intrusiones y ataques.

Seguimiento y Monitoreo

El seguimiento del Plan de Tratamiento se realizará mediante:

- Indicadores de seguridad digital (IDI – FURAG).
- Reportes periódicos al Comité Institucional de Gestión y Desempeño.
- Actualización anual del mapa de riesgos de seguridad de la información.

Presupuesto Asignado para el Tratamiento de Riesgos de Seguridad de la Información

Definición y Gestión del Presupuesto

La Agencia Logística de Gestión Inmobiliaria y Servicios de Cundinamarca asigna y ejecuta los recursos necesarios para el tratamiento de los riesgos de seguridad de la información a través del proceso de Gestión Tecnológica, en concordancia con el Plan de Seguridad y Privacidad de la Información, el Plan Estratégico de Tecnologías de la Información (PETI) y el Modelo Integrado de Planeación y Gestión – MIPG.

El presupuesto destinado a la seguridad de la información se gestiona bajo la responsabilidad del profesional encargado del proceso de Gestión Tecnológica, quien actúa como articulador técnico y administrativo para la planeación, ejecución, seguimiento y control de las inversiones requeridas para mitigar los riesgos identificados en la Agencia.

Agencia Logística de Gestión Inmobiliaria y Servicios de Cundinamarca
Sede Administrativa Calle 26 #51-53. Torre Beneficencia Piso 3.
Bogotá, D.C.
/CundiGob @CundinamarcaGob
www.cundinamarca.gov.co