PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2025

TABLA DE CONTENIDO

1. INTRODUCCIÓN

El Modelo de Seguridad y Privacidad de la Información (MSPI) se estructura en torno a las fases de diagnóstico, planeación, implementación, verificación y acción, y se lleva a cabo mediante el Sistema de Gestión de Seguridad de la Información (SGSI). Las actividades clave de cada fase son las siguientes:

- **Diagnóstico y Planificación**: Evaluación inicial del estado del MSPI, identificación de brechas existentes, elaboración de planes de implementación, actualización de la documentación, actividades de sensibilización y capacitación, clasificación de los activos de información y gestión de riesgos en seguridad digital.
- **Implementación**: Ejecución de los planes definidos, incluyendo tratamiento de riesgos, capacitación y controles.
- **Verificación**: Verificaciones internas y externas, así como revisiones del sistema.
- **Actuar**: Monitoreo, revisión y mejora continua del SGSI.

El plan se centra en las actividades de la AGENCIA para implementar este modelo.

La AGENCIA LOGÍSTICA tiene como prioridad avanzar en la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI). Para lograr este objetivo, se apoyará en la asignación de recursos humanos que permitan capacitar y fortalecer las capacidades técnicas y operativas, alineándose con los estándares del sector. Este documento actualiza las disposiciones estratégicas y operativas, con el fin de consolidar estos avances y avanzar en la madurez del MSPI.

2. DEFINICIONES

- **MSPI:** Modelo de Seguridad y Privacidad de la Información.
- **MGRSI:** Modelo Nacional de Gestión de Riesgos de Seguridad Digital.
- **MGRSD:** Modelo Nacional de Gestión de Riesgos de Seguridad Digital.
- **SGSI:** Sistema de Gestión de Seguridad de la Información.
- **Confidencialidad:** propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.
- **Disponibilidad:** propiedad de la información de ser accesible, utilizable y recuperable a demanda por una entidad.
- **Estándar:** Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. En este documento se habla de las Norma Técnica Colombiana ISO27001:2022 e ISO31000:2019.
- **Gestión de riesgos:** Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos.
- **Incidente de seguridad de la información:** Resultado de intentos intencionales o accidentales de romper las medidas de seguridad de la

información impactando en la confidencialidad, integridad o disponibilidad de la información.

- **Integridad:** propiedad de la información de ser completa, exacta e inalterada exactitud y completitud.
- **Información:** Es un conjunto organizado de datos, que constituyen un mensaje sobre un determinado ente o fenómeno. Indicación o evento llevado al conocimiento de una persona o de un grupo. Es posible crearla, mantenerla, conservarla y trasmitirla.

3. NORMATIVIDAD

El Plan de Seguridad y Privacidad de la Información se rige por la normativa vigente en Colombia, que establece los marcos legales y reglamentarios relacionados con la protección de la información y la gestión de riesgos. Entre las principales disposiciones se encuentran la Ley 1581 de 2012, que regula la protección de datos personales, y la Ley 1266 de 2008, que establece las condiciones para la gestión de la información financiera. Además, se deben cumplir las directrices establecidas por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), así como los estándares internacionales, como la ISO/IEC 27001, que define los requisitos para establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). La aplicación de estas normativas garantiza la protección adecuada de la información, la confidencialidad, la integridad y la disponibilidad de los datos en toda la Entidad.

4. OBJETIVOS

OBJETIVO GENERAL

Elaborar el Plan de Tratamiento de Riesgos de la Agencia Logística con el fin de establecer una guía estratégica que permita mitigar los riesgos, fortaleciendo así la confidencialidad, integridad y disponibilidad de la información en los activos críticos de la AGENCIA.

OBJETIVOS ESPECÍFICOS

- Realizar el contexto de los riesgos de seguridad de la información en articulación con la política establecida por la AGENCIA LOGÍSTICA DE GESTIÓN INMOBILIARIA Y DE SERVICIOS DE CUNDINAMARCA.
- Articular la gestión de riesgos y el plan de tratamiento con la Oficina de Planeación.
- Sensibilizar a los servidores públicos y contratistas de la Agencia acerca de la Gestión de Riesgos de Seguridad de la Información.

5. ALCANCE

El plan es aplicable a todo el personal de planta, contratistas y terceros, según corresponda. Su alcance abarca las actividades de planificación, diagnóstico, diseño, implementación, verificación y acciones vinculadas al MSPI y al SGSI, así como la planificación, ejecución, monitoreo, revisión y mejora de todas las etapas del MGRSI

El plan es aplicable a todo el personal de planta, contratistas y terceros, según corresponda. Su alcance incluye las actividades de planificación, diagnóstico, diseño, implementación, verificación y acciones relacionadas con el MSPI y el SGSI, así como la planificación, ejecución, monitoreo, revisión y mejora de todas las etapas del MGRSI.

La Política y el Plan de Seguridad y Privacidad de la Información, junto con el Tratamiento de Riesgos, abarcan todas las áreas y procesos de la Agencia, lo que resalta la importancia de su implementación, aplicación, seguimiento y las autorizaciones asociadas. Estas políticas se integran como herramientas de gestión esenciales y deben ser cumplidas de manera obligatoria por todos los funcionarios. Para garantizar su efectividad, es necesario que los funcionarios, contratistas y terceros involucrados en la gestión y administración de la información firmen el Compromiso de Confidencialidad, establecido por la AGENCIA LOGÍSTICA DE GESTIÓN INMOBILIARIA Y SERVICIOS DE CUNDINAMARCA (formato 01)

El Plan de Seguridad y Privacidad de la Información de la AGENCIA se fundamenta en el Modelo Nacional de Gestión de Riesgos de Seguridad Digital (MGRSI) y el Modelo de Seguridad y Privacidad de la Información (MSPI), ambos desarrollados por el Ministerio de las TIC como entidad reguladora en esta materia. Estos modelos están interrelacionados.

6. LINEAMIENTOS DE IMPLEMENTACIÓN

Con el objetivo de proteger la información de la Agencia Logística en todos sus aspectos, asegurando la seguridad de los datos y el cumplimiento de las normativas legales, se ha decidido implementar un Plan de Seguridad y Privacidad de la Información. Este plan busca prevenir pérdidas, robos, accesos no autorizados y duplicaciones de datos. Asimismo, promueve una política integral de seguridad para la información física y digital, adaptada a las características de los usuarios internos y externos.

La seguridad de la información implica preservar las siguientes propiedades fundamentales:

- **Confidencialidad**: Garantizar que la información solo sea accesible para las personas autorizadas.
- **Integridad**: Proteger la precisión y completitud de la información, así como los métodos utilizados para procesarla.
- **Disponibilidad**: Asegurar que los usuarios autorizados puedan acceder a la información y a los recursos relacionados siempre que lo necesiten.

Además, se consideran los siguientes conceptos adicionales:

- **Auditabilidad**: Todos los eventos de un sistema deben registrarse para facilitar su control y seguimiento posterior.
- **Protección contra duplicación**: Garantizar que una transacción solo se ejecute una vez, salvo que se especifique lo contrario, evitando que se grabe y reproduzca con el fin de generar múltiples solicitudes fraudulentas.
- **No repudio**: Impedir que las partes involucradas en el envío o recepción de información puedan negar su participación ante terceros.

- **Legalidad**: Cumplir con las leyes, normativas y disposiciones aplicables al organismo.
- **Confiabilidad de la información**: Asegurar que la información generada sea adecuada para respaldar decisiones y ejecutar las funciones y misiones de la Agencia Logística.

Para una interpretación adecuada del presente plan, se definen los siguientes términos:

- **Información**: Toda representación o comunicación de conocimiento en forma de datos, ya sea textual, numérica, gráfica, cartográfica, narrativa o audiovisual, en cualquier soporte, como papel, medios magnéticos, pantallas de computadoras, entre otros.
- **Sistema de Información**: Un conjunto organizado de recursos destinados a recopilar, procesar, mantener, transmitir y difundir información, mediante procedimientos manuales o automatizados.
- **Tecnología de la Información**: Hardware y software operados por la AGENCIA o un tercero para procesar información en su nombre, independientemente de la tecnología utilizada, como computación de datos o telecomunicaciones.

La Agencia, establecerá las directrices para la implementación del Modelo de Seguridad y Privacidad de la Información, el Modelo de Gestión de Riesgos de Seguridad y Privacidad de la Información, y el Sistema de Gestión de Seguridad de la Información, siguiendo los lineamientos definidos en la política de seguridad de la información.

El profesional designado por la gerencia de la AGENCIA, o a quien ella encargue, deberá coordinar los esfuerzos, recursos, metodologías y estrategias necesarios para garantizar la implementación y sostenibilidad de los modelos y sistemas de gestión de seguridad.

La gerencia designará un representante para el Sistema de Gestión de Seguridad de la Información y un responsable de la seguridad de la información de la entidad. En ausencia de una designación explícita, el líder del equipo de trabajo de tecnologías de la información asumirá ambas responsabilidades, apoyándose en expertos técnicos para la implementación, operación, mantenimiento, supervisión y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI).

COMUNICACIÓN

El contenido del documento de la política, el Plan de Seguridad y Privacidad de la Información y Tratamiento de Riesgos, junto con el Compromiso de Confidencialidad de la Información será socializado con todos los funcionarios de la AGENCIA LOGÍSTICA DE GESTIÓN INMOBILIARIA Y DE SERVICIOS DE CUNDINAMARCA. De igual forma, se informará a contratistas y terceros según sea necesario, con el objetivo de realizar ajustes y brindar la retroalimentación necesaria para asegurar el cumplimiento efectivo del plan.

Todos los funcionarios, contratistas y terceros de la AGENCIA deben estar al tanto de la existencia de la política, las políticas de seguridad, y el compromiso de

confidencialidad, así como de su carácter obligatorio. El documento físico estará bajo la custodia del Sistema de Gestión para su consulta cuando sea necesario el cual puede ser solicitado en cualquier momento en el sitio www.agenciacundinamarca.gov.co

7. MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI)

El Modelo de Seguridad y Privacidad de la Información (MSPI), desarrollado por el Ministerio de las TIC, establece un ciclo operativo compuesto por cinco (5) fases que facilitan a las entidades gestionar de manera efectiva la seguridad y privacidad de sus activos de información.

El MSPI define metas, indicadores, documentación e instrumentos que deben implementarse siguiendo los lineamientos y guías proporcionados por el Ministerio, basados en las mejores prácticas del sector.

Este modelo promueve la protección de la confidencialidad, integridad y disponibilidad de la información y los datos, a través de un proceso adecuado de gestión de riesgos y operación del Sistema de Gestión de Seguridad de la Información, generando confianza y seguridad para todas las partes interesadas.

8. MODELO NACIONAL DE GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL (MGRSD)

El propósito de este modelo es fortalecer la conciencia ciudadana y las capacidades del Gobierno, así como de las empresas en general, para identificar, analizar, evaluar y gestionar los riesgos asociados a la seguridad digital.

Además, dicho modelo incluye guías específicas para la gestión de riesgos de seguridad digital, adaptadas según el tipo de sector: Gobierno nacional, entidades territoriales y sector público; sector privado y mixto; sector de la fuerza pública y ciudadanía en general.

El marco conceptual del modelo establece las fases descritas y detalladas a continuación:

- **Planificación de la GRSD:** En esta etapa se definen los contextos y variables necesarias para el análisis y evaluación de riesgos, así como otros aspectos que se desarrollarán en las fases posteriores. Se realizan entrevistas con los responsables de cada área para identificar posibles riesgos.
- **Ejecución de la GRSD:** Esta fase implica llevar a cabo actividades relacionadas con el análisis y evaluación de riesgos de seguridad digital. Se identifican los riesgos inherentes y residuales, y se define su tratamiento dentro del marco de la seguridad de la información, especialmente en las Infraestructuras Críticas de la Información (ICC). Además, los riesgos son socializados con los responsables, y su aceptación es gestionada por los líderes del proceso.

- **Monitoreo y Revisión de la GRSD:** Consiste en evaluar de manera continua para garantizar que la gestión de riesgos de seguridad digital se realice conforme a los lineamientos establecidos. Incluye la generación de reportes y el seguimiento de los planes de tratamiento derivados de su aplicación. Los responsables de la revisión de riesgos de la entidad llevan a cabo el monitoreo correspondiente.
- **Mejora de la GRSD:** Esta fase busca implementar mecanismos que incrementen la madurez de la gestión de riesgos de seguridad digital en la entidad. La mejora continua se logra progresivamente mediante el cumplimiento de los objetivos establecidos. Se desarrollan y aplican modelos de evaluación de riesgos menos subjetivos, basados en metodologías matemáticas, para medir con mayor precisión el impacto de los riesgos en los activos de información y las ICC identificadas.

9. ACTIVOS DE SEGURIDAD DE INFORMACION

El plan y los lineamientos para la gestión del riesgo de la AGENCIA LOGÍSTICA incorporan un enfoque integral que atraviesa todas las áreas de gestión de la entidad, abarcando los activos de información, las políticas operativas y la cultura organizacional. Asimismo, contemplan los aspectos legales y normativos relacionados con la gestión de riesgos en seguridad digital.

GESTIÓN DE ACTIVOS DE INFORMACIÓN

- Difundir la guía de activos de información entre los responsables.
- Capacitar al personal en el uso de la plataforma de administración y control de activos de información institucional.
- Crear un inventario de activos relacionados con la seguridad y privacidad de la información, clasificado por criterios de disponibilidad, integridad y confidencialidad. Este inventario deberá ser aprobado por el Comité de Seguridad de la Información, implementado y actualizado de manera continua como parte de un proceso de mejora.
- Identificar y registrar nuevos activos de información en cada área o dependencia.
- Revisar los instrumentos relacionados con los activos de información, realizando ajustes necesarios y proporcionando retroalimentación a las áreas correspondientes.
- Actualizar los instrumentos de gestión de activos de información, incluyendo modificaciones como cambios físicos en la ubicación de los activos.

GUÍA PARA LA IDENTIFICACIÓN, CLASIFICACIÓN Y CONTROL DE ACTIVOS DE INFORMACIÓN.

Por parte de la AGENCIA LOGÍSTICA DE GESTIÓN INMOBILIARIA Y SERVICIOS DE CUNDINAMARCA se llevará a cabo la supervisión de cada proceso, asegurándose de que el inventario de los activos de información procesados y generados por la Agencia sea aprobado. Este inventario

deberá incluir la clasificación, valoración, ubicación y control de acceso a la información. Las áreas de Gestión de TIyC y Gestión Documental serán responsables de proporcionar las herramientas necesarias para la administración del inventario en cada área, garantizando la disponibilidad, integridad y confidencialidad de los datos.

Por su parte, el facilitador del proceso de Gestión de Recursos Físicos, con el apoyo del técnico operativo de sistemas, tendrá la responsabilidad de mantener un inventario completo y actualizado de los recursos de hardware y software de la Agencia.

Pautas Técnicas a Considerar

A. **Categorización de Activos de Información:**

El inventario de activos de información no se limita a componentes de hardware o software, como se mencionó anteriormente. Es fundamental clasificar los activos según las siguientes tipologías:

- **Físico:** Equipos tangibles como servidores, computadores y dispositivos.
- **Información Electrónica:** Datos almacenados en medios digitales.
- **Información Física:** Documentos impresos y archivos en papel.
- **Infraestructura Medio:** Redes, sistemas de energía, entre otros.
- **Removible:** Dispositivos portátiles como USB y discos externos.
- **Persona:** Recursos humanos asociados al manejo de la información.
- **Servicio:** Servicios contratados relacionados con la gestión de información.
- **Software:** Aplicaciones y sistemas utilizados.
- **Tercero:** Proveedores y entidades externas involucradas.

La categorización facilita la identificación preliminar de los riesgos asociados a cada activo.

B. **Clasificación y Manejo de la Información:**

Los usuarios deben cumplir con los lineamientos establecidos para la clasificación de la información, los cuales regulan el acceso, divulgación, almacenamiento, copia, transmisión, etiquetado y eliminación de los datos, tanto digitales como físicos.

C. **Periodos de Almacenamiento y Disposición Final:**

La información física y digital de la entidad debe ser almacenada por los periodos definidos en las tablas de retención documental, en función de los requerimientos legales o misionales. Una vez cumplido este plazo, la información deberá recibir el tratamiento adecuado conforme a la disposición final establecida.

D. **Control de Documentos en Equipos de Oficina:**

Al realizar tareas como impresión, escaneo, copias o envío de correos electrónicos, los usuarios deben:

- Verificar las áreas cercanas a impresoras, escáneres y fotocopiadoras para asegurar que no queden documentos desatendidos.
- Recoger inmediatamente documentos confidenciales para evitar divulgaciones no autorizadas o malintencionadas.

E. **Seguridad en los Puestos de Trabajo:**

Tanto funcionarios como personal externo deben garantizar que, al ausentarse de sus puestos, los escritorios estén libres de documentos y medios de almacenamiento. Estos elementos deben contar con medidas de seguridad apropiadas según su nivel de clasificación.

F. **Protección de Documentos Físicos:**

La información contenida en documentos físicos debe resguardarse mediante controles de acceso físico y condiciones de almacenamiento que aseguren su protección y conservación adecuada.

10. POLÍTICA Y LINEAMIENTOS DE GESTIÓN DEL RIESGO EN LA AGENCIA LOGÍSTICA DE GESTIÓN INMOBILIARIA Y DE SERVICIOS DE CUNDINAMARCA

La política y los lineamientos para la gestión del riesgo de la AGENCIA LOGÍSTICA incorporan un enfoque integral que atraviesa todas las áreas de gestión de la entidad, abarcando los activos de información, las políticas operativas y la cultura organizacional. Asimismo, contemplan los aspectos legales y normativos relacionados con la gestión de riesgos en seguridad digital.

Este documento establece políticas alineadas con los objetivos institucionales y la misión de la Agencia, diseñadas para proporcionar directrices que garanticen la protección y salvaguarda de la información gestionada por la Entidad. En este contexto, funcionarios, contratistas y terceros desempeñan un papel crucial en su conservación.

La Agencia, consciente de la necesidad de implementar controles que aseguren la confidencialidad, integridad y disponibilidad de la información utilizada en sus procesos y procedimientos, adopta políticas de seguridad destinadas a mitigar los riesgos que puedan comprometer o vulnerar dicha información, asegurando así la continuidad de los servicios ofrecidos.

AREA INTERVENCIÓN	ACCIONES	DESCRIPCIONES	RECURSOS	ENE	FEB	MAR	ABR	MAY
SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)	medir el Sistema de Gestión de Seguridad de la Información (SGSI)							
ACTIVOS DE SEGURIDAD DE INFORMACIÓN	Actualizar y modernizar los Instrumentos de Activos de Información							
	Elaborar el inventario de activos de seguridad y privacidad de la información de la entidad por área							
DIAGNÓSTICO DE SEGURIDAD INFORMÁTICA	Revisar y actualizar el Manual de Políticas de Seguridad y Privacidad de la Información							
	Evaluar y verificar las condiciones de los activos de la entidad							
	Analizar la información relacionada con modelo de seguridad y privacidad de la información (MSPI)							
RIESGOS DE SEGURIDAD DIGITAL	Realizar Seguimiento a la implementación de Planes de Tratamiento de Riesgos de Seguridad Digital							
ESTRATEGIA DE SENSIBILIZACIÓN	Sensibilización en Privacidad y Seguridad de la Información							

11. PLAN DE IMPLEMENTACIÓN

Formato 01
Compromiso de Confidencialidad, Integridad, Seguridad de la Información, Conflicto de Interés y Tránsito Documental

Yo, [Nombre completo], identificado(a) con cédula de ciudadanía N° [Número], en mi calidad de [funcionario(a)/Contratista/Otro] de la Agencia Logística y de Gestión Inmobiliaria y Servicios de Cundinamarca, adscrito(a) al área de [Grupo/Dependencia], desempeñando el cargo o actividad de [Cargo/Actividad], declaro que suscribo el presente compromiso bajo los términos establecidos.
Declaraciones Generales:

En el desarrollo de mis funciones, reconozco que tendré acceso a información en diversas formas y medios, relacionada tanto con la Agencia Logística y de Gestión Inmobiliaria y Servicios de Cundinamarca como con otras entidades del Estado Colombiano, incluyendo información de directores, empleados y clientes. Declaro que:

1. Toda información no pública de la Agencia es confidencial, está sujeta a reserva y será utilizada únicamente para fines relacionados con mis responsabilidades laborales.
2. Entiendo que los recursos tecnológicos, como hardware, software, correo electrónico, internet, dispositivos de cómputo, impresoras y telefonía, son propiedad institucional y están destinados exclusivamente a fines laborales, sin generar expectativas de privacidad.
3. Reconozco que el uso de estos recursos está regulado por las políticas institucionales y puede ser objeto de revisión.

Compromiso con la Política de Seguridad y Privacidad de la Información:
Manifiesto haber sido informado sobre la Política de Seguridad y Privacidad de la Información, así como el Manual de Políticas y Seguridad de la Información, disponible en el Sistema Integrado de Gestión (SIG. Me comprometo a:

- Respetar las disposiciones establecidas en estas políticas.
- Promover y apoyar activamente su cumplimiento.

1. Confidencialidad e Integridad de la Información:

a) No divulgar información confidencial interna o externa, por ningún medio, a terceros, salvo autorización expresa.

b) Proteger la información confidencial contra usos indebidos o divulgación no autorizada.

c) Utilizar la información confidencial exclusivamente para el cumplimiento de mis funciones y devolverla cuando finalice mi relación laboral o contractual.

d) Salvaguardar información privilegiada obtenida en el ejercicio de mis responsabilidades.

e) Administrar y gestionar de manera íntegra y coherente la información que corresponda a mis funciones.

f) Garantizar que toda información gestionada sea entregada de manera íntegra y únicamente a las personas autorizadas, utilizando los sistemas designados.

g) Usar los recursos tecnológicos de la entidad exclusivamente para actividades relacionadas con mis funciones.

2. **Tránsito Documental:**

a) No retirar documentos físicos o electrónicos de la entidad sin autorización escrita del superior inmediato.

b) Solicitar las autorizaciones pertinentes para el manejo y retiro de documentos, según las normativas de la entidad.

3. **Seguridad de la Información:**

Cumplir con las políticas de privacidad y seguridad de la información definida en el Sistema Integrado de Gestión (SIG).

Aceptación y Conformidad:

Al suscribir este documento, manifiesto mi conformidad con los términos aquí descritos, comprometiéndome a cumplir las obligaciones establecidas.

Firma: _____

Nombre: _____

Cédula: _____

Cargo: _____

Dependencia: _____

Firma del funcionario/contratista.