PROYECTA

PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

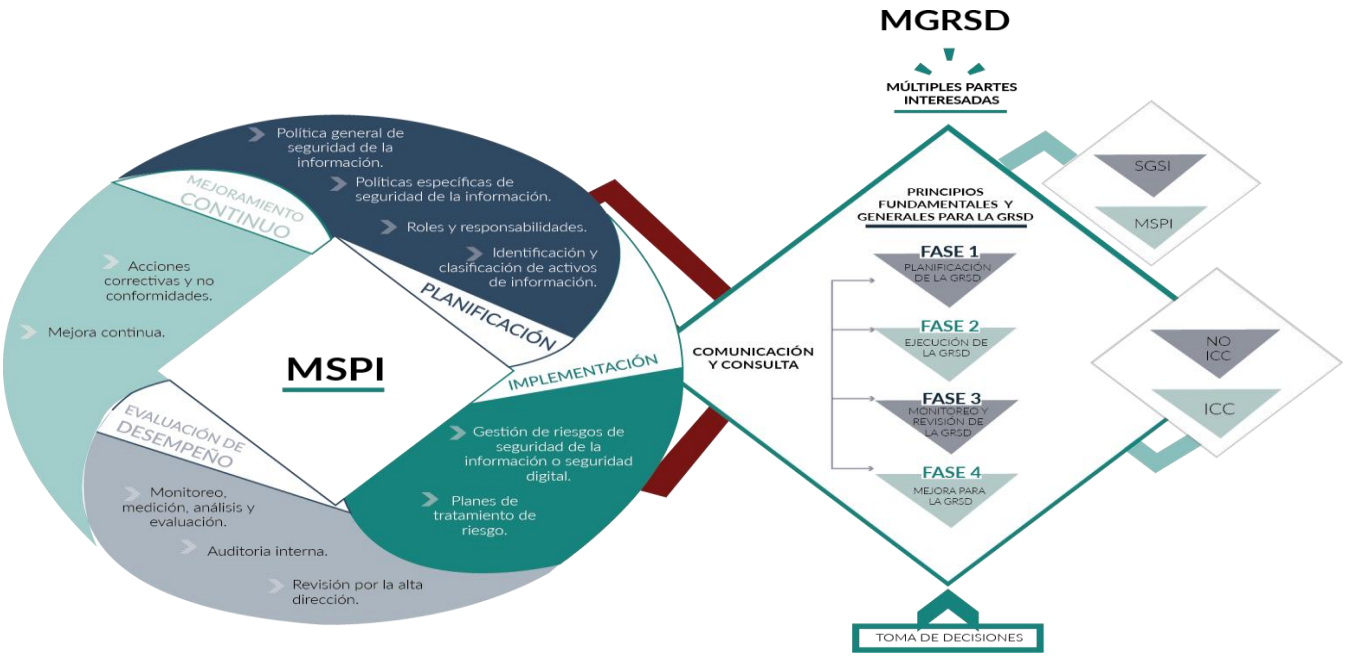
VIGENCIA 2025

TABLA DE CONTENIDO

1.ALCANCE

El Plan de Seguridad y Privacidad de la Información se basa en el Modelo Nacional de Gestión de Riesgos de Seguridad Digital (MGRSI) y el Modelo de Seguridad y Privacidad de la Información (MSPI), ambos del Ministerio de las TIC como órgano regulador en la materia.

El Plan Estratégico de Seguridad de la Información al buscar la mejora continua, en el componente de Gestión de Seguridad de la Información y la estrategia de seguridad digital de la Empresa Para el Desarrollo Territorial Proyecta, donde se indica que el componente de seguridad aplica a todos los procesos de la Entidad incluidos en el Modelo de Operación por procesos.



Interacción entre el MSPI y el MGRSD.

El Modelo de Seguridad y Privacidad de la Información (MSPI) se compone de las fases de diagnóstico, planeación, implementación, verificación y actuar, y a través de la implementación del Sistema de Gestión de Seguridad de la Información (en adelante SGSI) se cumple con lo requerido y exigido en los lineamientos y directrices emitidas por MinTIC.

Dentro del Sistema de Gestión de Seguridad de la Información, se contemplan grandes conjunto de actividades dentro de cada una de las fases como son: Diagnóstico inicial del estado del sistema con el fin de validar la brecha y las acciones que se deben desarrollar para su mitigación, actualización o elaboración de la documentación, sensibilización y capacitación, identificación y clasificación de los activos de información, identificación, valoración y gestión y tratamiento del riesgo de seguridad digital, revisiones del sistema, auditorías internas y externas, implementación de controles técnicos, entre otras. Así mismo el Modelo de Gestión de Riesgos de Seguridad Digital (MGRSD), abarca el monitoreo, revisión

y mejora para las actividades propias de la gestión de riesgos de seguridad digital.

El alcance en el Plan de Seguridad y Privacidad de la Información abarca la planificación, el diagnóstico, planeación, implementación, verificación y actuar del MSPI y SGSI, así como la planificación, la ejecución, el monitoreo, revisión y mejora de todas las fases del MGRSD.

El alcance del plan aplica para todo el personal de planta, contratista y terceros cuando es el caso.

2. OBJETIVOS

Realizar el mejoramiento continuo del componente de gestión de seguridad de la información en la Empresa Para el Desarrollo Territorial Proyecta, con el fin de mitigar los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información digital institucional, a partir de la implementación de las estrategias de seguridad digital definidas en este documento para la vigencia 2025.

2.1OBJETIVOS ESPECÍFICOS

- Fortalecer la cultura de seguridad de la información en la Empresa Para el Desarrollo Territorial Proyecta a través de la ejecución integral del Plan de capacitación, sensibilización y comunicación durante el año.
- Mejorar la protección y gestión de los activos de información de la Empresa Para el Desarrollo Territorial Proyecta mediante la actualización periódica de los activos de información y la declaración de aplicabilidad ISO 27001.
- Evaluar y mitigar riesgos de seguridad de la información mediante la realización de ejercicios de ingeniería social en ambos semestres y la actualización del diagnóstico del Anexo de Seguridad Digital conforme a la resolución 1519 de 2020 y la elaboración del documento autodiagnóstico MSPI 2025.
- Establecer una ruta para la correcta planeación y ejecución de un modelo de seguridad y privacidad de la información en la Entidad.
- Formalizar una estrategia de gestión de riesgos de seguridad digital en todos los procesos de la Entidad.
- Promover el uso de mejores prácticas de seguridad de la información en todo nivel dentro y fuera de la Entidad con todas las partes interesadas.
- Establecer un Sistema de Gestión en Seguridad de la Información en la Entidad, que conlleve a las actividades del ciclo Deming de la en el Planear (P), Hacer (H), Verificar (V) y Actuar (A); de cualquier sistema de Gestión.
- Velar por cumplimiento normativo dado por el Gobierno a través del Ministerio de las TIC, con respecto a la Seguridad y Privacidad de la Información en todas las entidades del Estado del orden Nacional y Territorial

3.DOCUMENTOS DE REFERENCIA

El Plan Estratégico de Seguridad de la Información se basa en los siguientes documentos, normas y lineamientos para su estructura y funcionamiento:

- Decreto 612 de 2018, "Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado", donde se encuentra el presente Plan Estratégico de Seguridad de la Información (PESI) como uno de los requisitos a desarrollar para cumplir con esta normativa.
- Resolución 500 de 2021. "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital".

- Manual de Gobierno Digital – MINTIC.
- Modelo de Seguridad y Privacidad de la Información – MINTIC.
- Normativa relacionada con seguridad de la información incluida en el Normograma institucional.

4.MARCO NORMATIVO

4.1 MARCO LEGAL

- Ley 23 de 1982 de Propiedad Intelectual - Derechos de Autor
- Ley 1032 de 2006, por el cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales.
- Ley 1266 de 2007, por la cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales.
- Ley 1273 de 2009, "Delitos Informáticos" protección de la información y los datos.
- Ley 1437 de 2011, "Código de procedimiento administrativo y de lo contencioso administrativo".
- Ley 1581 de 2012, "Protección de Datos personales".
- Decreto 2609 de 2012, por la cual se reglamenta la ley 594 de 200 y ley 1437 de 2011.
- Decreto 1377 de 2013, por la cual se reglamenta la ley 1581 de 2012.
- Ley 1712 de 2014, "De transparencia y del derecho de acceso a la información pública nacional"
- Decreto 1078 de 2015, por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Ley 962 de 2005. "Simplificación y Racionalización de Trámite. Atributos de seguridad en la Información electrónica de entidades públicas;"
- Ley 1150 de 2007. "Seguridad de la información electrónica en contratación en línea".
- Ley 1341 de 2009. "Tecnologías de la Información y aplicación de seguridad".
- Decreto 2952 de 2010. "Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008".
- Decreto 886 de 2014. "Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012".
- Decreto 1008 de 2018 "por la cual se establecen los lineamientos generales para la Política de Gobierno Digital…"
- Decreto 1083 de 2015. "Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012".
- CONPES 3701 de 2011 Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- CONPES 3854 de 2016 Política Nacional de Seguridad Digital.
- Resolución 746 de 2022 Modelo de Seguridad y Privacidad de la Información.

4.2 REQUISITOS TÉCNICOS

- Modelo de Seguridad y Privacidad de la Información – MINTIC.
- Modelo Nacional de Gestión de Riesgos de Seguridad Digital – MINTIC.
- Norma Técnica Colombiana NTC/ISO 27001:2013 y 2022 Sistemas de gestión de la seguridad

de la información.
- Norma Técnica Colombiana NTC/ISO 17799 Código de práctica para la gestión de la seguridad.

5. MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION -MSPI

El Modelo de Seguridad y Privacidad de la Información (MSPI) desarrollado por MINTIC, contempla un ciclo de operación que consta de cinco (5) fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información. En la siguiente figura se presenta el ciclo de operación:

Figura 1 – Ciclo de operación del Modelo de Seguridad y Privacidad de la Información
Fuente: MINTIC

El MSPI propone unas metas, resultados e instrumentos que deben ser ejecutados de acuerdo con unos lineamientos y guías que propone el Ministerio de las TIC, basado en las mejores prácticas en la materia. Este modelo conduce a la preservación de la confidencialidad, integridad y disponibilidad de la información, permitiendo asegurar la privacidad de la información y los datos, mediante la aplicación de un adecuado proceso de gestión del riesgo y operación del Sistema de Gestión de Seguridad de la Información brindado confianza a las partes interesadas.

6.POLÍTICA Y LINEAMIENTOS DE GESTIÓN DEL RIESGO

La política y lineamientos de gestión del riesgo en la Empresa Para el Desarrollo Territorial del Quindío Proyecta integran un proceso de gestión del riesgo de manera transversal en toda la gestión de la entidad, en sus activos de información, políticas de operación y en general en la cultura organizacional. Incluye además los planteamientos legales y reglamentarios referidos a la gestión del riesgo de seguridad digital, de acuerdo con el Anexo 4 de la Guía para la administración del riesgo y el diseño de controles en entidades públicas.

7.ACTIVIDADES DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y DEL

PLAN DE TRATAMIENTOS DE RIESGOS

De acuerdo con los modelos anteriormente descritos y la política y lineamientos de gestión del riesgo del Fondo Adaptación, se proponen las siguientes actividades del plan de seguridad y privacidad de la información y de tratamiento del riesgo de seguridad digital.

Actividad	Fecha Inicio
Revisar y actualizar la Política de seguridad y privacidad de la información	Febrero de 2025
Difundir la política de seguridad y privacidad de la información mediante campañas institucionales	Febrero de 2025
Actualizar el autodiagnóstico de MSPI y desarrollar comparativo y difusión de resultados	Febrero-marzo de 2025
Actualizar y consolidar el catálogo de activos de información y socializarlo	Febrero-marzo de 2025
Definir roles y responsabilidades.	Febrero-marzo de 2025
Actualizar los riesgos de seguridad sobre activos de información.	Marzo de 2025
Gestionar la implementación de controles de seguridad.	Marzo de 2025
Definir y gestionar la implementación del plan	Marzo de 2025
Sensibilización y capacitación en seguridad de la información.	Junio de 2025
Actualización de la documentación del SGSI	Junio de 2025
Revisiones por la alta dirección.	Junio de 2025

8.RESPONSABLES

1. Personal de apoyo de Seguridad de la Información.
2. Dependencias responsables de la actualización de los activos de información.
3. Líderes técnicos y funcionales responsables del monitoreo de primera línea de defensa de los riesgos de seguridad de la información.