EMPRESA DE SERVICIOS PÚBLICOS DOMICILIARIOS RED VITAL S.A. E.S.P.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

PAIPA S.A. E.S.P. Red Vital

PAIPA
ENERO DE 2026

Km 1 Vía Francisco Montaña / Código Postal 150444
Números de Contacto: +(57) 320 8587785 – 320 8585284
Correo electrónico: redvital@redvitalpaipa.com / sistemas@redvitalpaipa.com
Página Web: www.redvitalpaipasaesp.com

icontec ISO 9001 SC-2001068

TABLA DE CONTENIDO

Pag.

1. INTRODUCCIÓN **03**
2. GENERALIDADES **04**
   - 2.1 MISIÓN **05**
   - 2.2 VISIÓN **05**
3. ESTRUCTURA ORGÁNICA **06**
4. MARCO NORMATIVO **07**
5. OBJETIVOS **09**
   - 5.1 OBJETIVOS GENERAL **09**
   - 5.2 OBJETIVOS ESPECÍFICOS **09**
6. ALCANCE **10**
7. DEFINICIONES / TERMINOLOGIA **11**
8. POLÍTICA DE GOBIERNO DIGITAL **14**
9. POLÍTICA DE SEGURIDAD DIGITAL **15**
10. PROCESO DE IMPLEMENTACIÓN DEL SGSI **16**
11. PROCESO DE CLASIFICACIÓN DEL NIVEL DE MADUREZ **17**
    - 11.1 NIVELES DE MADUREZ DE SEGURIDAD Y PRIVACIDAD DE INFORMACIÓN **18**
12. REQUISITOS MÍNIMOS PARA LA IMPLEMENTACIÓN DEL SGSI **19**

1 INTRODUCCIÓN

La Empresa de Servicios Públicos Domiciliarios Red Vital Paipa S.A. E.S.P., mediante el Acuerdo No. 003 de 2022, derogó los Acuerdos Nos. 004 de 2017 y 002 de 2019, ajustando su Estructura Orgánica, definiendo las funciones de sus dependencias y estableciendo disposiciones institucionales para fortalecer la gestión de sus procesos.

En este marco, la entidad cuenta con una Planta Organizada de Personal reestructurada con base en las necesidades corporativas, optimizando la organización del talento humano y garantizando eficiencia operativa, con un impacto presupuestal controlado frente a la modalidad anterior de Contratos de Prestación de Servicios.

Red Vital Paipa S.A. E.S.P. maneja información crítica para la prestación de servicios públicos domiciliarios, incluyendo datos de clientes, proveedores, procesos administrativos, financieros y operativos, así como información operativa de infraestructura tecnológica y de control de servicios. La protección de esta información es estratégica, dado su valor para la continuidad del servicio y la confianza de la comunidad.

En consecuencia, la entidad ha definido este Plan de Seguridad y Privacidad de la Información, encaminado a garantizar la confidencialidad, integridad y disponibilidad de los datos, así como el cumplimiento de la normativa vigente, incluyendo la Ley 1581 de 2012 sobre protección de datos personales, y estándares internacionales de seguridad de la información como ISO/IEC 27001:2013

Este plan busca establecer un marco estructurado de políticas, controles, procedimientos y responsabilidades, asegurando que la gestión de la información esté alineada con los procesos institucionales, apoye la prestación eficiente de los servicios públicos y promueva la confianza de los ciudadanos en la entidad.

2 GENERALIDADES

Red Vital Paipa S.A. E.S.P. es una empresa de servicios públicos domiciliarios de carácter oficial, constituida como sociedad anónima de orden municipal, sometida al régimen jurídico de las empresas de servicios públicos domiciliarios, con autonomía administrativa, patrimonial y presupuestal.

Instaurada mediante el Acuerdo Municipal No. 019 del 5 de septiembre de 2008, la entidad tiene como propósito garantizar la prestación eficiente y continua de los servicios de acueducto, alcantarillado y aseo, así como sus actividades complementarias, favoreciendo al mejoramiento de la calidad de vida de la comunidad del municipio de Paipa y al desarrollo de un ambiente sano y sostenible.

Para cumplir con su objeto social, Red Vital Paipa S.A. E.S.P. ha desarrollado una infraestructura tecnológica integrada por sistemas de información, aplicaciones, bases de datos y equipos de soporte, que permiten gestionar los procesos administrativos, operativos y de atención a los usuarios. Estos activos de información son estratégicos y críticos para la continuidad de los servicios, la eficiencia operativa y la confianza de la comunidad.

En este contexto, la entidad reconoce que la protección de la información es fundamental, y por ello adopta políticas y procedimientos que buscan garantizar la confidencialidad, integridad y disponibilidad de los datos, cumpliendo con la normativa vigente en materia de protección de datos personales y estándares internacionales de seguridad de la información. Esta visión asegura que la gestión de la información esté alineada con los procesos institucionales y fortalezca la prestación de servicios públicos confiables y seguros.

2.1 MISIÓN

Somos una Empresa creada para contribuir al desarrollo de un ambiente más sano y al mejoramiento sustancial de la calidad de vida de los habitantes a través de la óptima prestación de los servicios públicos domiciliarios de Acueducto, Alcantarillado y Aseo.

2.2 VISIÓN

Consolidar en el mediano plazo a RED VITAL PAIPA S.A. E.S.P., como una Empresa eficiente en la prestación de los servicios públicos domiciliarios de Acueducto, Alcantarillado y Aseo, satisfaciendo las necesidades de nuestros usuarios, generando confianza y reconocimiento, para asegurar la calidad de vida de nuestras futuras generaciones.

PAIPA S.A. E.S.P. Red Vital

3 ESTRUCTURA ORGÁNICA

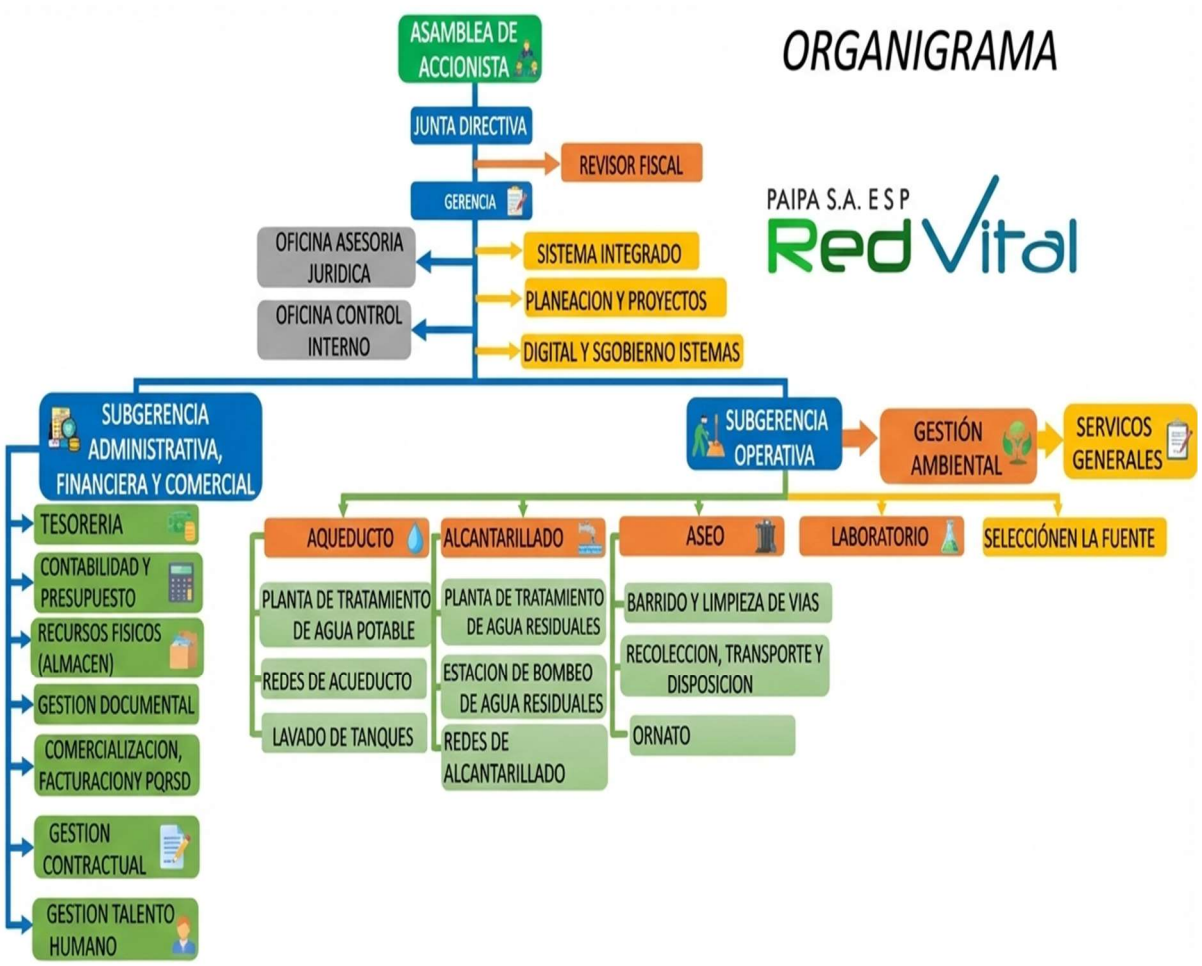


Tabla No. 1

4 MARCO NORMATIVO

Ley 527 de 1999	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
Ley 1266 de 2008	Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
Ley 1273 de 2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
Ley 1581 de 2012	Se expide el Régimen General de Protección de Datos Personales, el cual tiene por objeto: desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el Artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el Artículo 20 de la misma.

Decreto 886 de 2014	Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos.
Ley 1712 de 2014	Por medio del cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional.", fue revisado mediante la sentencia C-274 de 2013, de acuerdo con lo establecido en los artículos 153 y 241-8 de la Constitución Política.
Decreto 103 de 2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.

PAIPA S.A. E.S.P. Red Vital

5 OBJETIVOS

5.1 OBJETIVO GENERAL

Proyectar, orientar y desplegar acciones institucionales para la ejecución de medidas de control y protección de los datos y activos de información de la Entidad, alineadas con la normatividad vigente y orientadas a garantizar la privacidad, integridad y disponibilidad de la información.

5.2 OBJETIVOS ESPECÍFICOS

- Implementar controles de acceso y protección de los activos de información, asegurando la reserva, integridad y disponibilidad de los datos manejados por RED VITAL S.A. E.S.P.
- Establecer procedimientos, documentos y compromisos que permitan la gestión segura de la información y el desempeño de las políticas de seguridad definidas por la organización.
- Fortalecer la cultura organizacional en seguridad y privacidad de la información, promoviendo la concientización, buenas prácticas y el compromiso de todos los funcionarios, contratistas y terceros que operan información de la empresa.
- Implementar mecanismos de monitoreo, auditoría y mejora continua, que permitan identificar riesgos, evaluar la efectividad de los controles y asegurar la mejora permanente del sistema de gestión de seguridad de la información.

6 ALCANCE

El presente Plan de Seguridad y Privacidad de la Información establece los lineamientos, procedimientos y controles necesarios para garantizar la protección de los activos de información de RED VITAL S.A. E.S.P. El plan busca fortalecer la seguridad, confidencialidad, integridad y disponibilidad de la información, asegurando que todos los procesos de la empresa se desarrollen con altos estándares de seguridad y cumpliendo la normativa vigente.

El plan se enmarca en la NTC ISO/IEC 27001:2013 y demás disposiciones legales aplicables en materia de protección de datos personales y seguridad de la información, y contempla la implementación, seguimiento y mejora continua de un Sistema de Gestión de Seguridad de la Información (SGSI) adaptado a la realidad de la entidad.

7 DEFINICIONES / TERMINOLOGIA

Activo. Recurso de información o elemento relacionado con su tratamiento que tiene valor para la organización y requiere protección frente a riesgos.

Activo crítico de información. Activo cuya pérdida, alteración o indisponibilidad puede generar impactos significativos en la operación, el cumplimiento normativo o la prestación del servicio.

Amenaza. Causa potencial de un incidente no deseado que puede explotar una vulnerabilidad y afectar la seguridad de la información.

Análisis de riesgos. Proceso sistemático para comprender la naturaleza del riesgo y determinar su nivel, considerando la probabilidad de ocurrencia y el impacto.

Autenticación. Proceso mediante el cual se verifica la identidad de un usuario, sistema o entidad.

Autenticidad. Propiedad que garantiza que una entidad es quien dice ser y que la información es genuina.

Clasificación de la información. Proceso mediante el cual la información se categoriza según su nivel de sensibilidad, criticidad y requisitos de protección.

Confidencialidad. Propiedad de la información de no ser divulgada a personas, entidades o procesos no autorizados.

Control. Políticas, procedimientos, prácticas y estructuras organizacionales implementadas para reducir los riesgos de seguridad de la información a un nivel aceptable.

Copia de seguridad (Backup). Proceso de duplicación de la información con el fin de garantizar su recuperación ante incidentes.

Custodio del activo de información. Persona, cargo o área responsable de administrar y aplicar los controles definidos para un activo de información.

Dato personal. Cualquier información vinculada o que pueda asociarse a una persona natural identificada o identificable.

Datos personales sensibles. Datos que afectan la intimidad del titular o cuyo uso debido puede generar discriminación, conforme a la Ley 1581 de 2012.

Dato público. Testimonio calificado como tal por la Constitución o la ley, cuyo acceso no está restringido.

Dato privado. Dato que por su naturaleza íntima o reservada solo es relevante para su titular.

Dato semiprivado. Dato que no es íntimo ni público y cuyo conocimiento puede interesar a un grupo determinado de personas.

Disponibilidad. Propiedad de la información de estar accesible y utilizable cuando sea requerida por usuarios autorizados.

Evento de seguridad de la información. Suceso identificado en un sistema, servicio o red que puede ser relevante para la seguridad de la información.

Gestión de riesgos. Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, incluyendo evaluación y tratamiento.

Habeas Data. Derecho del titular a conocer, actualizar, rectificar y suprimir la información personal que repose en bases de datos.

Impacto. Consecuencia o efecto que puede generar un incidente de seguridad sobre la organización, ya sea operativo, legal, financiero o reputacional.

Incidente de seguridad de la información. Evento inesperado o no deseado que compromete la confidencialidad, integridad o disponibilidad de la información.

Información. Conjunto de datos procesados y organizados que tienen significado y valor para la toma de decisiones.

Integridad. Propiedad de salvaguardar la exactitud, completitud y consistencia de la información.

Inventario de activos de información. Relación documentada de los activos dentro del alcance del SGSI que requieren protección.

No repudio. Servicio de seguridad que impide que una entidad niegue la autoría o recepción de una acción o información.

Parte interesada. Persona u organización que puede afectar o verse afectada por las decisiones o actividades de la organización.

Plan de continuidad del negocio. Conjunto de estrategias y procedimientos orientados a garantizar la continuidad de los procesos críticos ante eventos disruptivos.

Plan de tratamiento de riesgos. Documento que define las acciones para mitigar, aceptar, transferir o evitar los riesgos identificados.

Propietario del activo de información. Persona o área responsable de definir el uso, controles y nivel de protección del activo de información.

Responsable del tratamiento. Persona natural o jurídica que decide sobre la base de datos y el tratamiento de los datos personales.

Riesgo. Posibilidad de que una amenaza explote una vulnerabilidad y genere un impacto negativo sobre un activo de información.

Seguridad de la información. Preservación de la confidencialidad, integridad y disponibilidad de la información.

Sistema de Gestión de Seguridad de la Información (SGSI). Conjunto de políticas, procesos, procedimientos, roles y recursos destinados a gestionar y proteger la información, bajo un enfoque de mejora continua.

Titular de la información. Persona natural a quien se refieren los datos personales objeto de tratamiento.

Trazabilidad. Capacidad de identificar y reconstruir el historial de acciones realizadas sobre la información.

Tratamiento de datos personales. Cualquier operación realizada sobre datos personales, como recolección, almacenamiento, uso, circulación o supresión.

Vulnerabilidad. Debilidad de un activo o control que puede ser explotada por una amenaza.

8. POLÍTICA DE GOBIERNO DIGITAL

RED VITAL S.A. E.S.P. reconoce la información como un activo estratégico y fundamental para el cumplimiento de su misión, la prestación continua y confiable de los servicios públicos domiciliarios y el cumplimiento de sus obligaciones legales y contractuales.

En este sentido, se compromete a establecer, conservar y mejorar continuamente el Sistema de Gestión de Seguridad de la Información (SGSI), certificando la confidencialidad, integridad y disponibilidad de la información, así como la protección de los datos personales tratados por la entidad.

La presente Política de Gobierno de Seguridad y Privacidad de la Información define los principios, lineamientos y responsabilidades que orientan la toma de decisiones, la gestión de riesgos y la implementación de controles de seguridad de la información en toda la organización.

RED VITAL S.A. E.S.P. se compromete a:

- Integrar la seguridad y privacidad de la información en los procesos misionales, estratégicos y de apoyo de la entidad, como parte de su guía de gobierno corporativo.

- Gestionar los riesgos de seguridad de la información, mediante la caracterización, análisis, estimación y tratamiento pertinente de los riesgos que puedan afectar los activos de información.

- Asegurar la protección de los datos personales, acogiendo medidas técnicas, administrativas y organizacionales que prevengan el acceso no autorizado, la pérdida, variación o uso indebido de la información.

- Generar una cultura organizacional orientada a la seguridad y privacidad de la información, mediante procesos de sensibilización y aprendizaje dirigidos a

funcionarios, contratistas y terceros.

- Inspeccionar y evaluar periódicamente la eficacia del SGSI, estableciendo mecanismos de seguimiento y mejora continua.

9 POLÍTICA DE SEGURIDAD DIGITAL

RED VITAL S.A. E.S.P. adopta la Seguridad Digital como un mecanismo estratégico de su modelo de Gobierno Digital, encaminado a fortalecer la confianza en el uso de las Tecnologías de la Información y las Comunicaciones (TIC), garantizando la continuidad de los servicios públicos domiciliarios y proteger los activos digitales de la entidad.

La entidad establece un camino de gestión del riesgo digital, mediante la identificación, análisis, evaluación y tratamiento de los riesgos que puedan afectar la confidencialidad, integridad, disponibilidad y trazabilidad de la información, así como la permanencia de sus plataformas tecnológicas y procesos digitales.

Para tal fin, se realizan medidas técnicas, administrativas y organizacionales que permitan advertir, detectar, responder y recuperarse frente a sucesos de seguridad digital, incluyendo accesos no autorizados, pérdida o variación de la información, fallas tecnológicas o uso inapropiado de los recursos digitales.

De igual manera, RED VITAL S.A. E.S.P. fomenta una cultura de seguridad digital, promoviendo la responsabilidad, el uso apropiado de la tecnología y la adopción de buenas prácticas por parte de funcionarios, contratistas y terceros.

La presente política es de obligatorio cumplimiento y se articula con la Política de Gobierno Digital, el Sistema de Gestión de Seguridad de la Información (SGSI), el Plan de Seguridad y Privacidad de la Información y la normativa vigente, incluyendo los lineamientos del Ministerio TIC.

10. PROCESO DE IMPLEMENTACIÓN DEL SGSI

FASE 1. PLANIFICAR

- Identificar y priorizar riesgos estratégicos y operativos
- Viabilidad de la Entidad para el diseño del Plan de Seguridad y Privacidad de la Información
- Identificación de la normatividad
- Definir alcance y objetivos del SGSI
- Establecer política de seguridad y principios de protección de activos
- Analizar de los riesgos obtenidos de la Entidad
- Diseño del Plan de Seguimiento y Control
- Diseño del Plan de Tratamiento del Riesgo

FASE 2. IMPLEMENTAR

- Ejecutar el Plan de Tratamiento de Riesgos
- Establecer controles técnicos, administrativos y físicos
- Capacitación y concientización del personal y terceros
- Procedimiento para el Seguimiento y Control del SGSI
- Diseño de la Política de la Seguridad de la información
- Gestión de los recursos humanos/técnicos/financieros
- Integración con el MIPG y procedimientos institucionales

FASE 3. MONITOREAR

- Ejecutar el Plan de Tratamiento de Riesgos
- Establecer controles técnicos, administrativos y físicos
- Capacitación y concientización del personal y terceros
- Procedimiento para el Seguimiento y Control del SGSI
- Diseño de la Política de la Seguridad de la información
- Gestión de los recursos humanos/técnicos/financieros
- Integración con el MIPG y procedimientos institucionales

FASE 4. MEJORA CONTINUA

- Actualizar procedimientos y controles según resultados
- Optimizar la gestión de riesgos y políticas
- Incorporar lecciones aprendidas y mejores prácticas
- Fortalecer cultura de seguridad y concientización

11. PROCESO DE CLASIFICACIÓN DEL NIVEL DE MADUREZ

La Empresa de Servicios Públicos Domiciliarios Red Vital Paipa S.A. E.S.P. instaura un modelo de clasificación del nivel de madurez del Sistema de Gestión de Seguridad de la Información (SGSI), como unidad para evaluar de manera organizada el grado de implementación, operación y mejora de la seguridad de la información en la entidad.

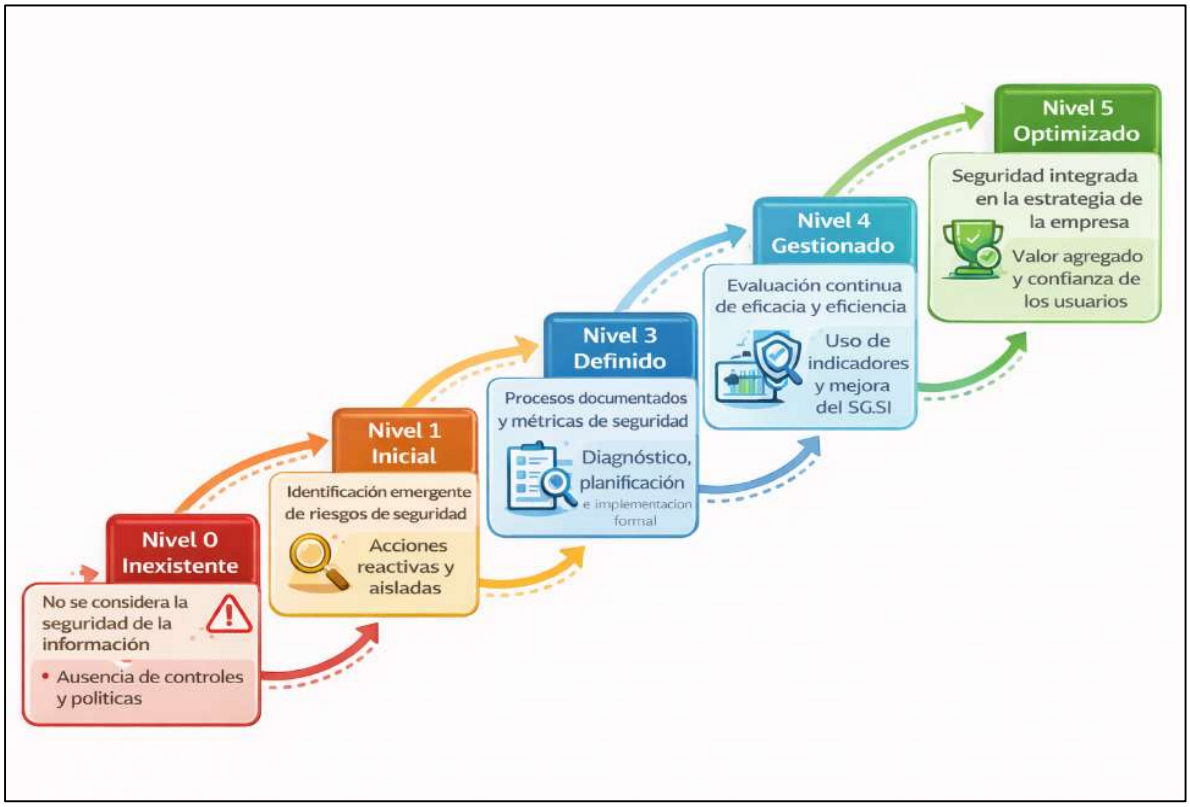
Este modelo permite identificar el estado actual del SGSI, examinar avances alcanzados y determinar brechas frente a las buenas prácticas definidas en la NTC/ISO 27001:2013, sirviendo como pieza clave para la toma de decisiones, la priorización de acciones y el fortalecimiento continuo de la seguridad de la información.

La madurez del SGSI se concibe como un proceso evolutivo, en el cual la organización avanza progresivamente desde prácticas iniciales e informales hacia un proyecto de gestión consolidado, medible y orientado a la mejora continua. Cada nivel de madurez simboliza un grado diferente de control, formalización y efectividad, conforme con el contexto, los riesgos y las capacidades institucionales.

La clasificación del nivel de madurez se efectúa con base en los resultados de la implementación del SGSI, el desempeño de los controles definidos, la gestión de riesgos, el rastreo a incidentes y la evidencia documental disponible, permitiendo a la entidad establecer planes de mejora alineados con sus objetivos estratégicos y con el Modelo Integrado de Planeación y Gestión (MIPG).

11.1 NIVELES DE MADUREZ DE SEGURIDAD Y PRIVACIDAD DE INFORMACIÓN

Modelo del Nivel de Madurez. Fuente: Adaptada de MINTIC [14]



12. REQUISITOS MÍNIMOS PARA LA IMPLEMENTACIÓN DEL SGSI

La ejecución del Sistema de Gestión de Seguridad de la Información (SGSI) se piensa como un proceso evolutivo que avanza progresivamente a través de los niveles definidos en el modelo de madurez de seguridad y privacidad de la información adoptado por la organización. En este sentido, las siguientes condiciones básicas permiten transitar desde estados iniciales hasta niveles de gestión optimizada y generación de valor:

i. Conformación del marco de gestión de la seguridad de la información, mediante la definición de lineamientos, responsabilidades y prácticas mínimas, lo cual establece la base para avanzar desde niveles iniciales hacia procesos definidos y consistentes.

ii. Gestión sistemática de los riesgos de información, como mecanismo habilitador del modelo de madurez, logrando identificar activos críticos, priorizar amenazas y orientar la implementación de controles acordes al nivel de madurez esperado.

iii. Formalización de procesos de planificación, operación y control, que soportan la evolución hacia niveles gestionados del modelo, asegurando la aplicación coherente de las acciones de seguridad y su alineación con los objetivos institucionales y el MIPG.

iv. Administración y control de la información documentada y evidencias, que facilitan la trazabilidad, medición y mejora continua del SGSI, elementos clave para alcanzar los niveles superiores de madurez y optimización.

ELABORÓ	NATURALEZA DEL CAMBIO	VERSIÓN	FECHA DE APROBACIÓN
Andrew Masami Asakura García	Procedimiento inicial	01	31/01/2023
Andrew Masami Asakura García	Cambio de codificación PE-GCOM-PL-01 a PA-GCOM-PL-01 (Procesos estratégico a procesos de apoyo)	02	14/03/2023
Andrew Masami Asakura García	Unificación de los Procesos de Gestión de Sistemas y Comunicaciones	03	15/03/2023
Andrew Masami Asakura García	Unificación de los Procesos de Gestión de Sistemas y Comunicaciones	04	30/01/2024

ELABORÓ	REVISÓ	APROBÓ
Nombre: Byron Duwar Maldonado Sanchez	Nombre: Andrew Masami Asakura García	Nombre: Yeison Rokney Torres Suarez
Cargo: Técnico Administrativo (sistemas)	Cargo: Profesional SIG	Cargo: Gerente General
Firma: Original Firmado	Firma: Original Firmado	Firma: Original Firmado

PAIPA S.A. E.S.P. Red Vital

Km 1 Vía Francisco Montaña / Código Postal 150444
Números de Contacto: +(57) 320 8587785 – 320 8585284
Correo electrónico: redvital@redvitalpaipa.com / sistemas@redvitalpaipa.com
Página Web: www.redvitalpaipasaesp.com