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 2025

TABLA DE CONTENIDO

1 INTRODUCCIÓN 3

2 GENERALIDADES 4

2.1 MISIÓN 4

2.2 VISIÓN 4

3 ESTRUCTURA ORGÁNICA 5

4 MARCO NORMATIVO 5

5 OBJETIVOS 7

5.1 OBJETIVO GENERAL 7

5.2 OBJETIVOS ESPECÍFICOS 7

6 ALCANCE 7

7 DEFINICIONES / TERMINOLOGÍA 8

8 PROCESO DE IMPLEMENTACIÓN DEL SGSI 12

8.1 FASE 1. PLANEACIÓN 12

8.2 FASE 2. HACER 12

8.3 FASE 3. VERIFICAR 12

8.4 FASE 3. ACTUAR 12

9 PROCESO DE CLASIFICACIÓN DEL NIVEL DE MADUREZ 13

9.1 NIVELES DE MADUREZ DE SEGURIDAD Y PRIVACIDAD DE INFORMACIÓN 13

10 REQUISITOS MINIMOS PARA LA IMPLEMENTACIÓN DEL SGSI 13

1 INTRODUCCIÓN

La Empresa de Servicios Públicos Domiciliarios Red Vital Paipa S.A. E.S.P., mediante Acuerdo No. 003 de 2022, por medio del cual se deroga el Acuerdo No. 004 de 2017 y Acuerdo No. 002 de 2019 y se ajusta la Estructura Orgánica de Red Vital Paipa S.A. E.S.P., se definen funciones a sus dependencias y se dictan otras disposiciones. La Entidad cuenta con una Planta Estructural de Personal, cuya Reestructuración ha sido implementada en base a las necesidades institucionales que se han estado financiado a través de Contratos de Prestación de Servicios, que implica la formalización de la planta y presupuestalmente un aumento más reducido de los costos de personal.

Con el fin de garantizar el manejo eficaz de la información con la cual trabaja la Empresa de Servicios Públicos Domiciliarios Red Vital Paipa S.A. E.S.P., se tendrá una infraestructura tecnológica por medio de los equipos, aplicaciones informáticas y demás medios con los cuales interactúan diariamente los funcionarios y usuarios en general, se hace necesario identificar y gestionar las actividades que se relacionan con la Seguridad de la Información.

Para la Empresa de Servicios Públicos Domiciliarios Red Vital Paipa S.A. E.S.P., resalta la integración de un Estándar de Seguridad de Información con su respectiva actualización, que contribuirá en mantener un sistema coherente con los procesos de la entidad en beneficio de la comunidad.

2 GENERALIDADES

RED VITAL PAIPA S.A. E.S.P. es una empresa de servicios públicos oficial, constituida como sociedad anónima, de carácter comercial de orden municipal, sometida al régimen jurídico de las empresas de Servicios Públicos Domiciliarios.

La sociedad tiene autonomía administrativa, patrimonial y presupuestal. 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.

La empresa es una sociedad por acciones con capital público, creada mediante acuerdo Municipal Número 019 del 05 de septiembre de 2008, fundada el 10 de septiembre del año 2008, con deberes y derechos que la hacen responsable del bienestar de vida de la población de Paipa. Dedicada a la prestación de servicios públicos domiciliarios de acueducto, alcantarillado, aseo y sus actividades complementarias.

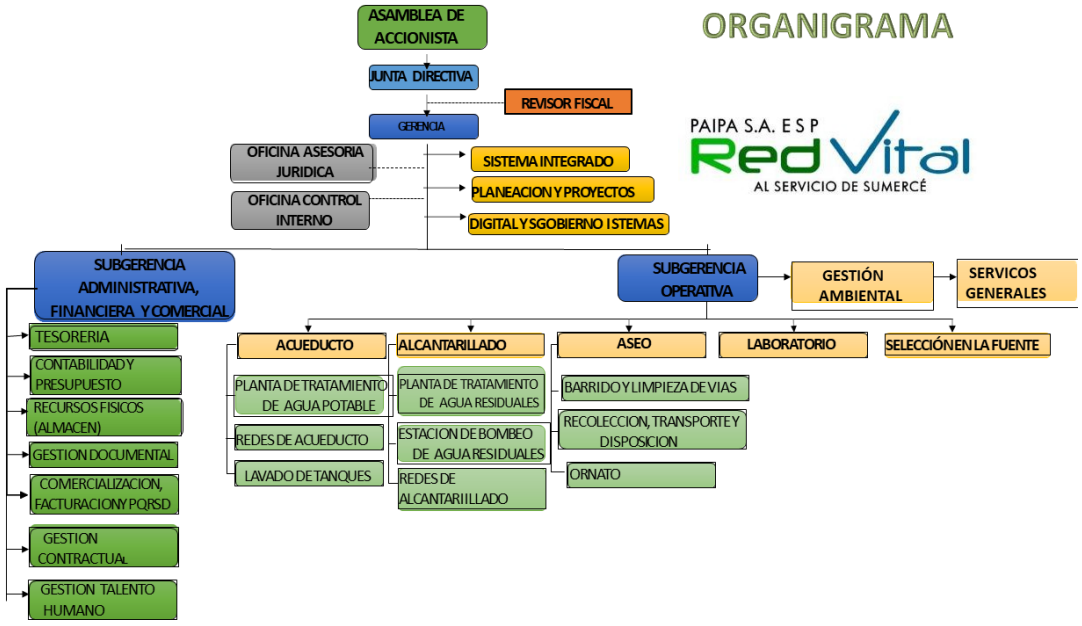
2.1 MISIÓN

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.

3 ESTRUCTURA ORGÁNICA



4 MARCO NORMATIVO

Tabla No. 1

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 1714 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.

5 OBJETIVOS

5.1 OBJETIVO GENERAL

Planear, orientar y desarrollar los planes de acción institucionales de medidas de control y protección al conjunto de datos y activos de información de la Entidad.

5.2 OBJETIVOS ESPECÍFICOS

- Formular el esquema de seguridad de la información de acuerdo a las necesidades del Sistema de Información Empresa de Servicios Públicos Domiciliarios Red Vital Paipa S.A. E.S.P.

- Instaurar medidas de control de acceso a los activos de información Empresa de Servicios Públicos Domiciliarios Red Vital Paipa S.A. E.S.P.

- Establecer las acciones, documentos, procedimientos y responsabilidades frente a la garantía de la seguridad de la información en la Empresa de Servicios Públicos Domiciliarios Red Vital Paipa S.A. E.S.P.

- Dar cumplimiento con los principios de confidencialidad, disponibilidad e integridad de la información, garantizando la protección de los activos de información de Empresa de Servicios Públicos Domiciliarios Red Vital Paipa S.A. E.S.P.

- Promover la cultura de la Seguridad y Privacidad de la Información fortaleciendo las buenas prácticas y la conciencia de los funcionarios, contratistas y terceros.

- Establecer la continuidad del negocio mediante la implementación de planes y controles que sea necesario desarrollar frente a la existencia de incidentes de seguridad de la información.

- Identificar la viabilidad institucional de la Entidad de cubrir las necesidades, en conjunto con la necesidad cuantitativa y cualitativa para la vigencia 2023.

- Implementar el proceso de Reestructuración, que no afecte significativamente la Disponibilidad Presupuestal de la Entidad.

6 ALCANCE

El Plan de Seguridad y Privacidad de la Información busca la implementación del SGSI, para mejorar los niveles de seguridad de la información y la protección de los activos de información de la Entidad, teniendo en cuenta los lineamientos de la NTC 27001:2013 y los demás concordantes hasta su seguimiento y control.

7 DEFINICIONES / TERMINOLOGÍA

Activo. En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma que tenga valor para la organización.

Amenaza. Causa potencial de un incidente no deseado, que pueda provocar daños a un sistema o a la organización.

Amenaza informática. Es la aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado.

Análisis de riesgos. Es el proceso que permite comprender la naturaleza del riesgo y determinar su nivel de riesgo.

Autenticación. Provisión de una garantía de que una característica afirmada por una entidad es correcta.

Autenticidad. Propiedad de que una entidad es lo que afirma ser.

Ciberseguridad. Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética.

Ciberespacio. Ámbito o espacio hipotético o imaginario de quienes se encuentran inmersos en la civilización electrónica, la informática y la cibernética.

Confidencialidad. Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Control. Comprenden las políticas, procedimientos, prácticas y estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.

Custodio de activo de información. Identifica a un individuo, un cargo, proceso o grupo de trabajo designado por la entidad, que tiene la responsabilidad de

administrar y hacer efectivo los controles que el propietario del activo haya definido, con base en los controles de seguridad disponibles en la entidad.

Datos abiertos. Son datos primarios o sin procesar puestos a disposición de cualquier ciudadano, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos.

Datos biométricos. Parámetros físicos únicos de cada persona que comprueban su identidad y se evidencian cuando la persona o una parte de ella interacciona con el sistema (huella digital o voz).

Datos personales sensibles. se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

Dato privado. Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.

Dato público. Es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con la presente ley. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas.

Dato semiprivado. Es el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios.

Disco duro. Disco de metal cubierto con una superficie de grabación ferro magnético. Haciendo una analogía con los discos musicales, los lados planos de la placa son la superficie de grabación, el brazo acústico es el brazo de acceso y la púa (aguja) es la cabeza lectora/grabadora. Los discos magnéticos pueden ser grabados, borrados y re-grabados como una cinta de audio.

Disponibilidad. Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

DVD. Disco Versátil (video) Digital. En la actualidad constituye el natural sucesor del CD para la reproducción de sonido e imagen de calidad.

Evento de seguridad de la información. Ocurrencia identificada de estado en un sistema de información, servicio o red que indica una posible brecha de seguridad, falla de un control o una condición no identificada que puede ser relevante para la seguridad de la información.
Gestión de claves. Son controles que realizan mediante la gestión de claves criptográficas.

Gestión de riesgos. Actividades coordinadas para dirigir controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.

Habeas data. Derecho a acceder a la información personal que se encuentre en archivos o bases de datos; implica la posibilidad de ser informado acerca de los datos registrados sobre sí mismo y la facultad de corregirlos.

Impacto. El coste para la empresa de un incidente “de la escala que sea”, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc.

Incidente de seguridad de la información. evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Información. Está constituida por un grupo de datos ya supervisados y ordenados, que sirven para construir un mensaje basado en un cierto fenómeno o ente. La información permite resolver problemas y tomar decisiones, ya que su aprovechamiento racional es la base del conocimiento.

Integridad. Es la propiedad de salvaguardar la exactitud y complejidad de la información.

Inventario de activos. Es lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

No repudio. Servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido).

Parte interesada. Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

Plan de continuidad del negocio. Plan orientado a permitir la continuidad de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro

Plan de tratamiento de riesgos. Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

Proceso. Conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas.

Propietario de activo de información. Identifica a un individuo, un cargo, proceso o grupo de trabajo designado por la entidad, que tiene la responsabilidad de definir los controles, el desarrollo, el mantenimiento, el uso y la seguridad de los activos de información asignados.

Riesgo. Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consideraciones.

Responsable del tratamiento. Persona natural o jurídica. Pública o privada. Que por sí misma o en asocio con otros. Decida sobre la base de datos y/o el Tratamiento de los datos.

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 elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basando en un enfoque de gestión y de mejora a un individuo o entidad**.**

Titular de la información. Es la persona natural o jurídica a quien se refiere la información que reposa en un banco de datos y sujeto del derecho de hábeas data y demás derechos y garantías a que se refiere la presente ley.

Trazabilidad. Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.

Vulnerabilidad. Debilidad de un activo o control que pueda ser explotado por una o más amenazas.

8 PROCESO DE IMPLEMENTACIÓN DEL SGSI

8.1 FASE 1. PLANEACIÓN

- Viabilidad de la Entidad para el diseño del Plan de Seguridad y Privacidad de la Información
- Identificación de la normatividad
- Definición del Alcance del SGSI
- Diseño de la Política de la Seguridad de la Información
- Realizar la Matriz de Riesgo de Seguridad y Privacidad
- Identificación del Inventario de Activos
- Analizar de los riesgos obtenidos de la Entidad
- Diseño del Plan de Seguimiento y Control
- Diseño del Plan de Tratamiento del Riesgo

8.2 FASE 2. HACER

- Implementación del Plan de Tratamiento del Riesgo
- Procedimiento para el Seguimiento y Control del SGSI
- Implementación del Modelo Integrado de Planeación y Gestión MIPG
- Diseño de la Política de la Seguridad de la información
- Diseño de los Indicadores de Medición del SGSI
- Diseño de los Procedimientos para la operación del SGSI
- Gestión de los recursos humanos/técnicos/financieros

8.3 FASE 3. VERIFICAR

- Ejecución de la Operatividad de SGSI
- Implementación de los Procedimientos del SGSI
- Estandarización a través de Instructivos de Seguridad y Privacidad de Información
- Recolección de información de resultados a través de Auditorías Internas en conjunto con el Modelo Integrado de Planeación y Gestión MIPG

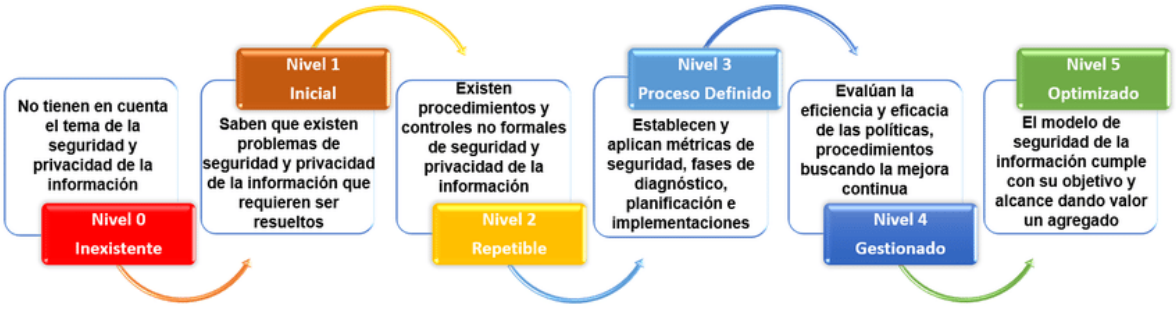
8.4 FASE 3. ACTUAR

- Análisis de resultados obtenidos en la implementación del SGSI
- Autoevaluación del SGSI
- Revisión del Inventario de Activos de Información integrados al SGSI
- Análisis de los incidentes y fallas de seguridad de información obtenidos en la Entidad

9 PROCESO DE CLASIFICACIÓN DEL NIVEL DE MADUREZ

La Empresa de Servicios Públicos Domiciliarios Red Vital Paipa S.A. E.S.P., teniendo en cuenta los resultados de la implementación del Sistema de Gestión de Seguridad de la Información SGSI, determina la clasificación según la NTC 2700:2013. La Gestión de la Seguridad de la Información debe pasar por varios niveles o escalones, cada uno con su coste asociado y contexto de aplicabilidad. Se comienza a perfilar una escala de progresión en lo que ahora conocemos como Sistemas de Gestión de Seguridad de la Información basados en la NTC 27001:2013. Considerando los avances y las preocupaciones actuales, esta escala se compondría de los siguientes niveles:

9.1 NIVELES DE MADUREZ DE SEGURIDAD Y PRIVACIDAD DE INFORMACIÓN



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

10 REQUISITOS MÍNIMOS PARA LA IMPLEMENTACIÓN DEL SGSI

- Política y objetivos del SGSI
- Alcance del SGSI
- Procedimientos, manuales, instructivo que apoyan el SGSI
- Metodología de Análisis de Valoración de Riesgos
- Matriz de Valoración de Riesgos

- Plan de Tratamiento de Riesgos
- Procedimientos documentados que necesita la organización para asegurar la eficacia de la planificación, operación y control de sus procesos de seguridad de la información, bajo la directriz del Modelo Integrado de Planeación y Gestión MIPG
- Control documental de los registros exigidos por esta norma
- Acto administrativo para la declaración de aplicabilidad del SGSI

ELABORÓ	NATURALEZA DEL CAMBIO	VERSIÓN	FECHA DE APROBACIÓN
Andrew Masami Asakura Garcia	Procedimiento inicial	01	31/01/2023
Andrew Masami Asakura Garcia	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 Garcia	Unificación de los Procesos de Gestión de Sistemas y Comunicaciones	03	15/03/2023
Andrew Masami Asakura Garcia	Unificación de los Procesos de Gestión de Sistemas y Comunicaciones	04	30/01/2024
Andrew Masami Asakura Garcia	Inclusión del Logo ICONTEC / MIPG y ajuste de Pie de Página / Ajuste de contenido	05	26/08/2024
Andrew Masami Asakura Garcia	Actualización de contenido	06	24/01/2024

ELABORÓ	REVISÓ	APROBÓ
Nombre: Oscar Iván La Rotta Ojeda	Nombre: Andrew Masami Asakura Garcia	Nombre: Jhon Edison Barón Fonseca
Cargo: Profesional de Gobierno Digital	Cargo: Profesional SIG	Cargo: Jefe Oficina de Control Interno
Firma:	Firma:	Firma: