EMPRESA DE SERVICIOS PUBLICOS DE LEBRIJA E.S.P.

PLAN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

VIGENCIA 2024

DR. EDUARDO VASQUEZ ZORRO
GERENTE

Lebrija, Diciembre 2022

1. INTRODUCCION

El Plan de Seguridad y Privacidad de la Información de la Empresa de servicios públicos de Lebrija ESP, está compuesto por la Confidencialidad, integridad, disponibilidad de la información, mediante de identificación, diagnóstico y nivel de riesgo de los activos de información de la Empresa.
Este documento elaboró la recopilación de los lineamientos dados por el Ministerio de las tecnologías de la Información y las comunicaciones, de acuerdo al modelo de PHVA, que consiste en diagnosticar, planear, hacer e implementar el Plan de Seguridad y Privacidad de la Información.
Para esto se tiene en cuenta el tamaño y estructura de la Empresa de servicios públicos de Lebrija ESP, sus objetivos, sus procesos misionales, con el fin de identificar la situación actual, las necesidades que tiene la Empresa y el Nivel de Riesgo a que se encuentra Expuesta.

2. OBJETIVOS

Identificar actividades orientadas a fortalecer el aseguramiento de los servicios de TI y la información de la Empresa de servicios públicos de Lebrija ESP, para preservar la confidencialidad, integridad y disponibilidad de los datos, según el Plan de Seguridad de la información de la Estrategia de Gobierno Digital, del Ministerio de las Tecnologías de la Información y las comunicaciones.

3. ALCANCE

Con la implementación del Plan de Seguridad y privacidad de la formación, busca establecer elementos fundamentales de seguimiento y control, para fomentar una Cultura de Seguridad y privacidad de la información en sus funcionarios, contratistas y/o terceros contratados por operadores.
El plan esta formulado para que se ejecute durante la Vigencia 2024, 2025 2026 y 2027, tiempo necesario para lograr la adopción del Plan de Seguridad y Privacidad de la Información MSPI y garantizar su continuidad.

4. MARCO LEGAL

El Estado colombiano cuenta con normatividad vigente que obliga el adecuado tratamiento de la información manejada por la Empresa en términos de confidencialidad, integridad y disponibilidad. Entre otras se citan:
• Ley 1273 de 2009, Por el cual de modifica el código penal, se crea un nuevo bien jurídico tutelado-denominado "de la protección de la información y los datos", y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

• Conpes 3701 de 2011: "Lineamientos de política para Cibersiguridad y Ciberdefensa" "...Este documento busca generar lineamientos de política en ciberseguridad y ciberdefensa orientados a desarrollar una estrategia nacional que contraste el incremento de las amenazas informáticas que afecten significativamente al país....". Ley 1437 de 2011, Capítulo IV, "utilización de medios electrónicos en el procedimiento administrativo" ."Los procedimientos y trámites administrativos podrán realizarse a través de medios electrónicos. Para garantizar la igualdad de acceso a la administración, la autoridad deberá asegurar mecanismos suficientes y adecuados de acceso gratuito a los medios electrónicos, o permitir el uso alternativo de otros procedimientos."
• Ley 1581 de 2012, g) Principio de seguridad: "La información sujeta a Tratamiento por el responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento."
• Ley 1581 de 2012, Artículo 17, ítem d: "Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento" Decreto 1413 de 2017, artículo 2.2.17.2.1.1 "Descripción de los servicios ciudadanos digitales, 1.5 servicio de interoperabilidad: Cualquier desarrollo en el marco de los servicios ciudadanos digitales especiales deberá hacer uso de o estar soportado en los servicios ciudadanos digitales básicos cuando lo requieran."
• Decreto 1008 de 2018, Por el cual se establecen los lineamientos generales de Gobierno Digital y se subroga el capítulo I del título 9 de la parte 2 del libro 2 del decreto 1078 de 2015, Decreto Único reglamentario del Sector de las Tecnología de la Información y las Comunicaciones.
• Decreto 612 de 2018, artículo 1. "Integración de planes institucionales y estratégico. Las Empresaes del Estado, de acuerdo con el ámbito de aplicación del Plan Integrado de Planeación y Gestión, al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011, deberán integrar los planes institucionales y estratégicos que se relacionan a continuación y publicarlo, en su respectiva página web."

5. PLAN DE SEGURIDAD DE LA INFORMACIÓN

EMPULEBRIJA ESP, dando cumplimiento a los estándares de Seguridad y Privacidad de la información, adopta el Plan de Seguridad y Privacidad de la Información (MSPI), el cual se encuentra alineado con el Plan propuesto por el ministerio de tecnologías de la información y las comunicaciones MINTIC.
El Plan de Seguridad y Privacidad para estar acorde con las buenas prácticas de seguridad será actualizado periódicamente; reuniendo los cambios técnicos de la norma 27001 del 2013, legislación de la Ley de Protección de Datos Personales,

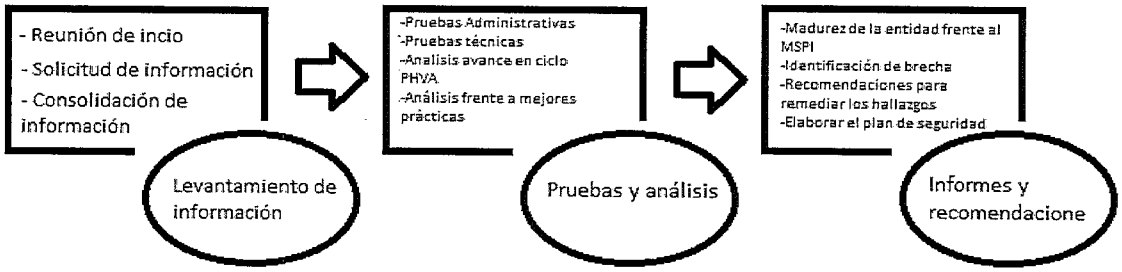
Transparencia y Acceso a la Información Pública, entre otras, las cuales se deben tener en cuenta para la gestión de la información.
A nivel metodológico es importante tener presente que el (MSPI) cuenta con las siguientes guías:

- Guía 1 - Metodología de pruebas de efectividad
- Guía 2 - Política General MSPI v1
- Guía 3 - Procedimiento de Seguridad de la Información
- Guía 4 - Roles y responsabilidades
- Guía 5 - Gestión Clasificación de Activos
- Guía 6 - Gestión Documental
- Guía 7 - Gestión de Riesgos
- Guía 8 - Controles de Seguridad de la Información
- Guía 9 - Indicadores Gestión de Seguridad de la Información
- Guía 10 - Continuidad de Negocio
- Guía 11 - Análisis de Impacto de Negocio
- Guía 12 - Seguridad en la Nube
- Guía 13 - Evidencia Digital
- Guía 14 - Plan de comunicación, sensibilización, capacitación
- Guía 15 – Auditoria
- Guía 16 - Evaluación de Desempeño
- Guía 17 - Mejora continúa
- Guía 18 - Lineamientos terminales de áreas financieras de Empresaes públicas
- Guía 19 - Aseguramiento de protocolo IPv4_IPv6
- Guía 20 - Transición IPv4_IPv6
- Guía 21 - Gestión de Incidentes
- Plan de Seguridad y Privacidad

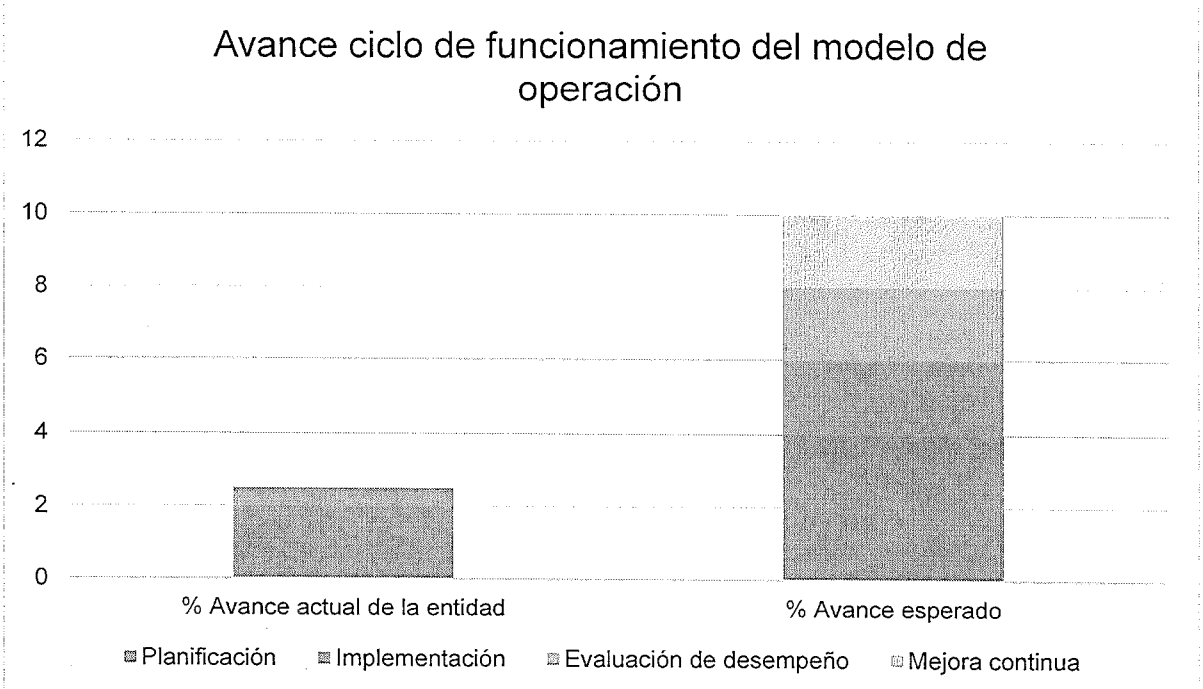
Al desarrollar se estará dando cumplimiento a cada una de las fases del Plan, buscando a su vez comprender cuáles son los resultados a obtener y como desarrollarlos, incluyendo los nuevos lineamientos que permiten la adopción del protocolo IPv6 en el Estado Colombiano.
La implementación del Plan de Seguridad y Privacidad de la Información - MSPI, en la Empresa está determinado por las necesidades objetivas, los requisitos de seguridad, procesos, el tamaño y la estructura de la misma, todo con el objetivo de preservar la confidencialidad, integridad, disponibilidad de los activos de información, garantizando su buen uso y la privacidad de los datos.
Mediante la adopción del Plan de Seguridad y Privacidad por parte de EMPULEBRIJA ESP se busca contribuir al incremento de la transparencia en la Gestión Pública, promoviendo el uso de las mejores prácticas de Seguridad de la Información como base de la aplicación del concepto de Seguridad Digital.

5.1 DESARROLLO DE LA METODOLOGÍA DE AUTODIAGNOSTICO

En la siguiente grafica se muestran las diferentes fases de ejecución de la evaluación:



Grafica 1: Fases de ejecución autodiagnóstico.



En el Instrumento de Evaluación, hoja madurez MSPI, se identificaron cada uno de los requisitos para cumplir los niveles de madurez definidos en el MSPI. Estos requisitos en su mayoría han sido previamente evaluados en las hojas Administrativas, Técnicas y PHVA.

5.2 POLITICA GENERAL DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION.

La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la administración de la Empresa de servicios públicos de Lebrija ESP, con respecto a la protección de los activos de información (los funcionarios, contratistas, terceros. la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la Empresa y apoyan la implementación del Plan de Seguridad y Privacidad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

La Empresa de servicios públicos de Lebrija ESP, para asegurar la dirección estratégica de la Empresa, establece la compatibilidad de la política de seguridad de la información y los objetivos de seguridad de la información, estos últimos correspondientes a:

- Minimizar el riesgo de los procesos misionales de la Empresa.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.¬
- Mantener la confianza de los funcionarios, contratistas y terceros.
- Apoyar la innovación tecnológica.
- Implementar el sistema de gestión de seguridad de la información.
- Proteger los activos de información.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de Empresa de servicios públicos de Lebrija ESP (Santander).
- Garantizar la continuidad del negocio frente a incidentes.

Alcance/Aplicabilidad

Esta política aplica a toda la Empresa, sus funcionarios, contratistas y terceros de la Empresa de servicios públicos de Lebrija ESP y la ciudadanía en general.

Nivel de cumplimiento

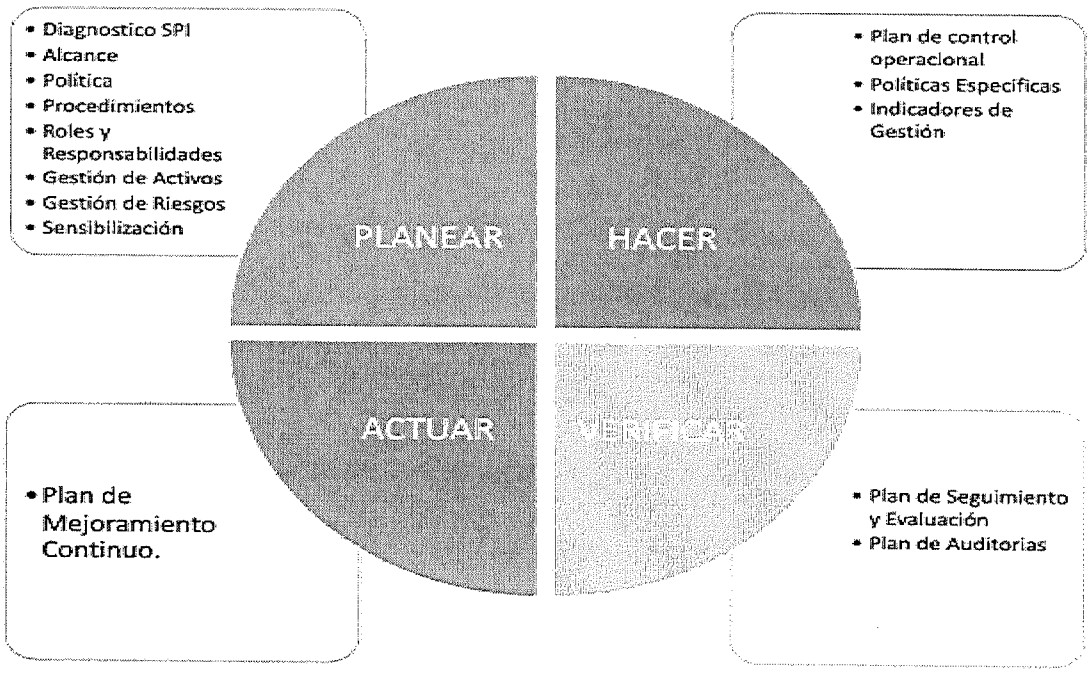
Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento un 100% de la política.
A continuación, se establecen las 12 políticas de seguridad que soportan el MSPI de la Empresa de servicios públicos de Lebrija ESP:

- La Empresa de servicios públicos de Lebrija ESP ha decidido definir, implementar, operar y mejorar de forma continua un Plan de Seguridad y Privacidad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza.
- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.
- La Empresa de servicios públicos de Lebrija ESP protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de los mismos.
- La Empresa de servicios públicos de Lebrija ESP protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- La Empresa de servicios públicos de Lebrija ESP protegerá su información de las amenazas originadas por parte del personal.

- La Empresa de servicios públicos de Lebrija ESP protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- La Empresa de servicios públicos de Lebrija ESP controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- La Empresa de servicios públicos de Lebrija ESP implementará control de acceso a la información, sistemas y recursos de red.
- La Empresa de servicios públicos de Lebrija ESP garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- La Empresa de servicios públicos de Lebrija ESP garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su Plan de seguridad.
- La Empresa de servicios públicos de Lebrija ESP garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- La Empresa de servicios públicos de Lebrija ESP garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

El incumplimiento a la política de Seguridad y Privacidad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa de la Empresa, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

A continuación se detalla la estructura del plan de seguridad de la información:



De esta estructura se realizaron los autodiagnósticos y ya se cuentan con las políticas generales del Plan de seguridad y privacidad de la información.

Se establece el siguiente plan de acción para la vigencia 2024:

5.3 PLAN DE ACCION VIGENCIA 2024 PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION (MSPI)

ITEM	DESCRIPCIÓN	ENTREGABLE	FECHA
Actualización inventario de activos	Identificar nuevos activos de información en cada dependencia	Inventario de activos actualizado	Febrero 28 de 2024
Activos de información	Publicación del Registro Activos de Información en el sitio web de la Empresa.	Link del documento publicado	Febrero 28 de 2024
Gestión de riesgos	Identificación, Análisis y Evaluación de Riesgos - Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Matriz de riesgos	Marzo de 2024
Gestión de riesgos	Publicación matriz de riesgos página web	Matriz de riesgos	Marzo de 2024
Seguridad de la información	Socializar a funcionarios las políticas de seguridad y privacidad de la información	Planilla de asistencia	Febrero y Junio de 2024, o cuando ingrese un funcionario nuevo

El presente plan fue aprobado por el comité institucional de gestión y desempeño según acta de trabajo 001-2024 del día 29 de enero de 2024.

Dr. EDUARDO VASQUEZ ZORRO
Gerente

Apoyo:
Sergio Mauricio Ramírez
Contratista de apoyo de control interno