TABLA DE CONTENIDO

OBJETIVO 2

ALCANCE 2

ÁREA RESPONSABLE 2

CONTENIDO 2

1. METODOLOGÍA 2
2. CICLO DE OPERACIÓN 3
3. SITUACIÓN ACTUAL 4
4. IMPLEMENTACIÓN 7

4.1. HOJA DE RUTA 7

4.2. CRONOGRAMA 12

NORMATIVIDAD 14

CONTROL DE CAMBIOS 15

OBJETIVO	ALCANCE	ÁREA RESPONSABLE
Incorporar buenas prácticas en seguridad y privacidad de la información en la entidad, conducentes a preservar su confidencialidad, integridad y disponibilidad.	Aplicable a la identificación de la situación actual y la adopción del modelo de seguridad y privacidad de la Información – MSPI en los diferentes procesos y áreas de la Empresa de Servicios Públicos de Santander S.A. E.S.P. – ESANT S.A. E.S.P., de acuerdo con lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC.	Dirección de Planeación

CONTENIDO

1. METODOLOGÍA

La metodología de implementación del modelo de seguridad y privacidad de la información – MSPI en la ESANT S.A. E.S.P., está basado en el ciclo PHVA (Planificar- Hacer-Verificar-Actuar).

Figura 1. Ciclo PHVA del MSPI

- **Planificar:** En esta fase se busca identificar el estado actual de la entidad en lo referente a los requisitos del modelo de seguridad y privacidad de la información - MSPI y realizar la planeación del tiempo, recursos y presupuesto de las actividades que va a desarrollar relacionadas con el mismo.
- **Hacer**: En esta fase se ejecuta el plan establecido, desarrollando las acciones necesarias para lograr las mejoras planteadas en la fase de planificación.
- **Verificar**: En esta fase se hace seguimiento, medición, y análisis de los resultados, verificando que estén acorde con las metas establecidas y a toda la planeación inicial. Se debe hacer una actualización del autodiagnóstico, donde sus resultados serán incluidos como un insumo para la fase de mejoramiento continuo.
- **Actuar**: En esta fase se ejecutan las acciones para el mejoramiento del desempeño de los procesos, se corrigen las desviaciones, se estandarizan los cambios, se realiza la formación y capacitación requerida y se define como monitorearlo.

2. CICLO DE OPERACIÓN

La seguridad y privacidad de la información, como elemento de la política de gobierno digital, busca preservar la confidencialidad, integridad y disponibilidad de los activos de información de las entidades, garantizando su buen uso y la privacidad de los datos, a través del modelo de seguridad y privacidad de la información – MSPI, el cual se basa en un ciclo de operación de cinco (5) fases:

- Diagnóstico
- Planificación
- Implementación
- Evaluación de desempeño
- Mejora continua

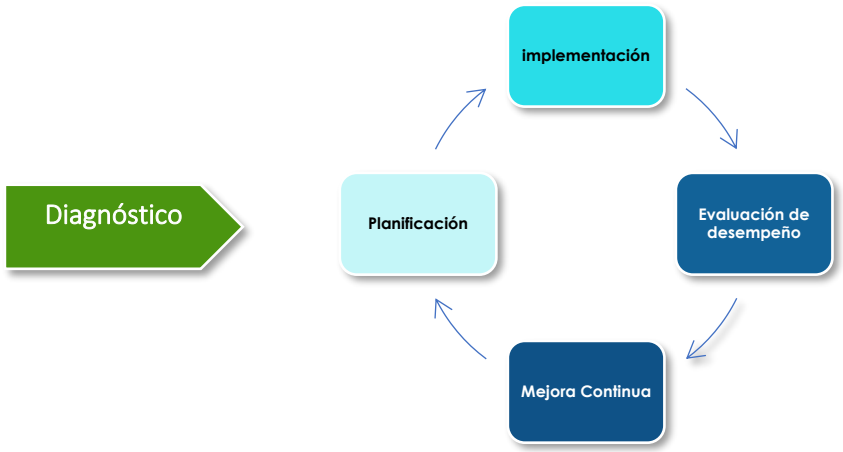

Figura 2. Fases del ciclo de operación del MSPI

3. SITUACIÓN ACTUAL

Durante el año 2023 se realizó un diagnóstico en temas de seguridad y privacidad de la información de la ESANT S.A. E.S.P. frente a los requerimientos del modelo de seguridad y privacidad de la información – MSPI, emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC, utilizando la herramienta de autoevaluación proporcionada por el MINTIC, donde se obtuvieron los siguientes resultados para cada dominio:

DOMINIO	PUNTAJE OBTENIDO	META
ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	65	100
POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	60	100
GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	59	100
SEGURIDAD DE LAS OPERACIONES	54	100
CONTROL DE ACCESO	50	100
SEGURIDAD DE LAS COMUNICACIONES	50	100
RELACIONES CON LOS PROVEEDORES	50	100
GESTIÓN DE ACTIVOS	47	100
SEGURIDAD FÍSICA Y DEL ENTORNO	46	100
ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	40	100
ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	31	100
SEGURIDAD DE LOS RECURSOS HUMANOS	30	100
CRIPTOGRAFÍA	0	100

Cada uno de los dominios evaluados, tiene un valor máximo alcanzable de 100 puntos; una vez realizado el diagnóstico, se encontró que el dominio con menor puntaje obtenido fue el relacionado con criptografía, con una calificación de cero (0) puntos. Mientras que el de mayor valor alcanzado hace referencia a adquisición, desarrollo y mantenimiento de sistemas, donde se obtuvo una calificación de 65 puntos.

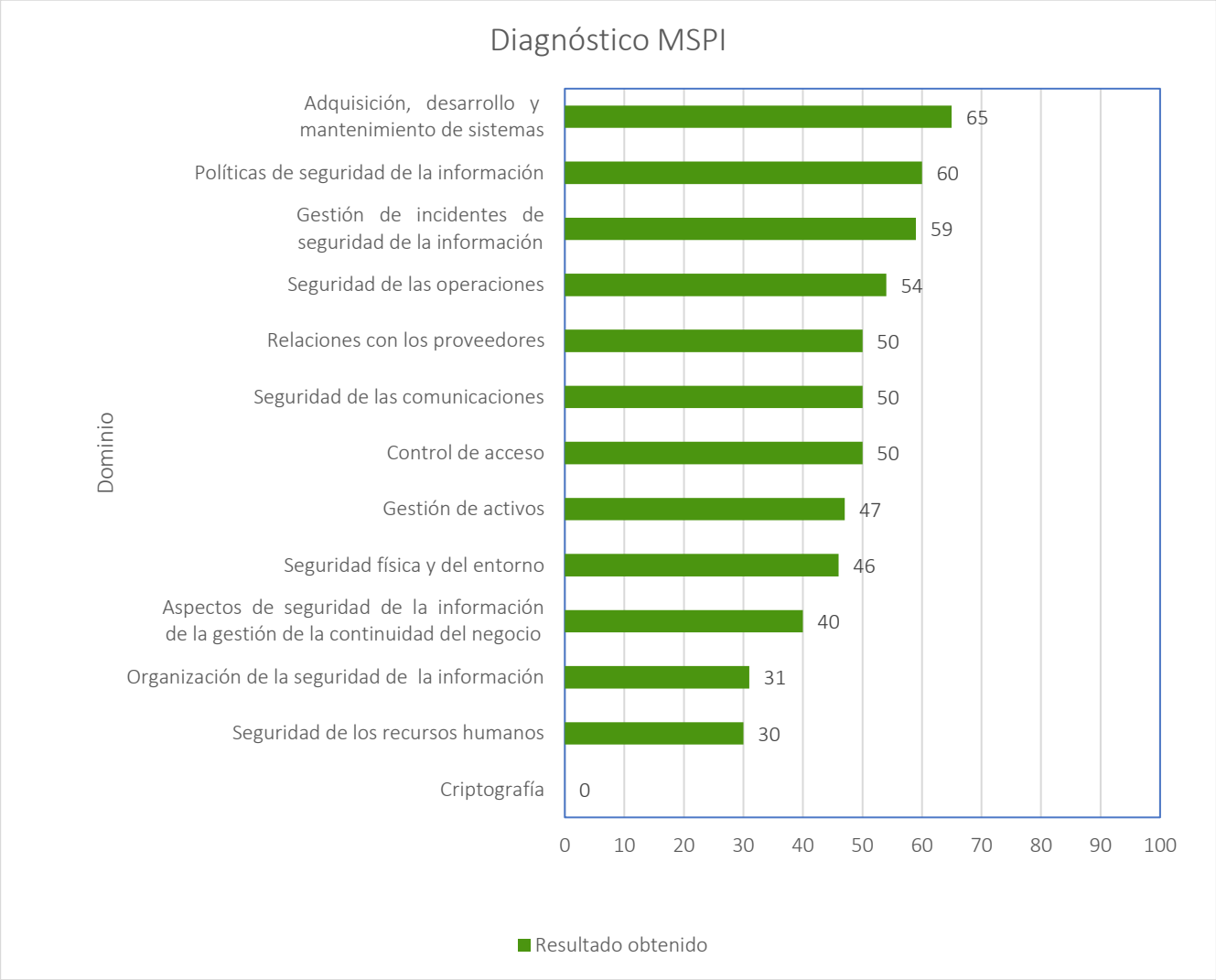

Figura 3. Resultados del diagnóstico del MSPI de la ESANT S.A. E.S.P.

La herramienta también permite identificar el nivel de madurez en el que se encuentran el modelo de seguridad y privacidad de la información – MSPI de la entidad, midiendo la brecha entre el nivel actual y el nivel optimizado. A continuación, se muestra el esquema que determina los niveles de madurez del MSPI y establece los criterios de valoración a través de los cuales se determina el estado actual de la seguridad de la información en la entidad.

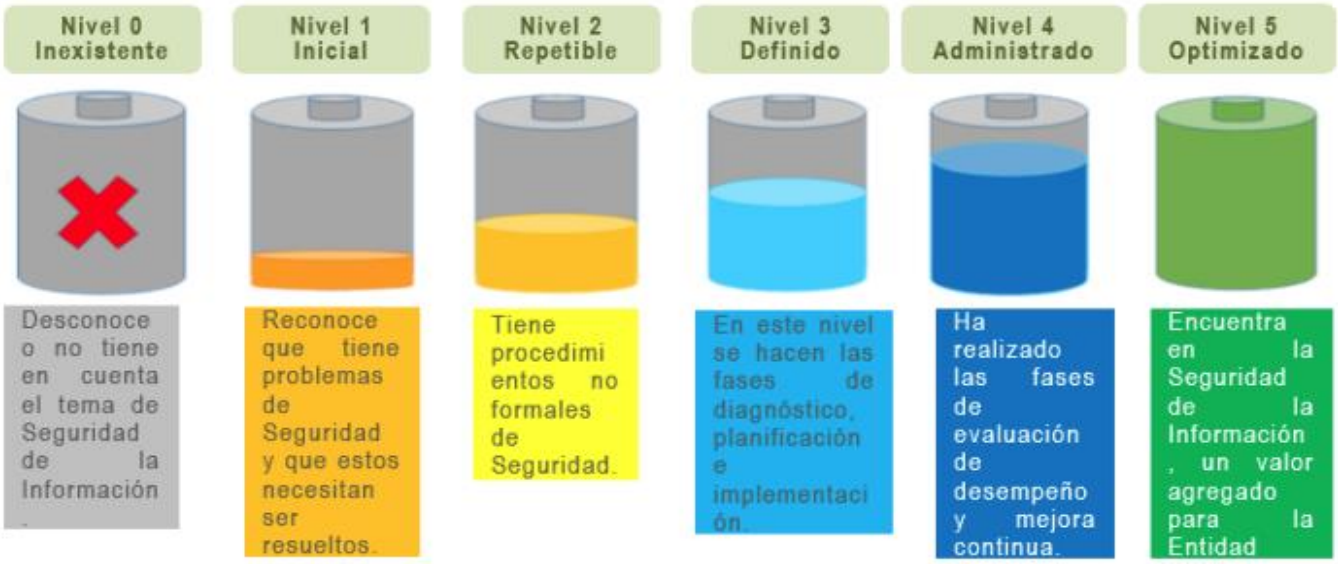

Figura 4. Criterios de valoración del nivel de madurez del MSPI

Mediante el uso de la herramienta, se obtuvieron los siguientes resultados por dominio, respecto al nivel de madurez de la entidad:

DOMINIO	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
CRIPTOGRAFÍA	INEXISTENTE
ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	INICIAL
SEGURIDAD DE LOS RECURSOS HUMANOS	INICIAL
ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	INICIAL
SEGURIDAD FÍSICA Y DEL ENTORNO	REPETIBLE
SEGURIDAD DE LAS OPERACIONES	REPETIBLE
SEGURIDAD DE LAS COMUNICACIONES	REPETIBLE
GESTIÓN DE ACTIVOS	REPETIBLE
CONTROL DE ACCESO	REPETIBLE
RELACIONES CON LOS PROVEEDORES	REPETIBLE
GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	REPETIBLE
POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	EFECTIVO
ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	EFECTIVO
CUMPLIMIENTO	EFECTIVO

El dominio de criptografía es el único que se encuentra en nivel inexistente. Los dominios: organización de la seguridad de la información, seguridad de los recursos humanos y aspectos de seguridad de la información de la gestión de la continuidad del negocio en un nivel inicial. En el nivel repetible se tienen los dominios: seguridad física y del entorno, seguridad de las operaciones, seguridad de las comunicaciones, gestión de activos, control de acceso, relaciones con los proveedores y gestión de incidentes de seguridad de la información; mientras que en el nivel efectivo se encuentran en los dominios: políticas de seguridad de la información, adquisición, desarrollo y mantenimiento de sistemas y cumplimiento.

Estas son las conclusiones del análisis de los resultados del diagnóstico, donde a nivel general, la ESANT S.A. E.S.P. se encuentra en el nivel 2 (repetible):

- Los procesos y los controles siguen un patrón regular.
- Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas.
- No hay formación ni comunicación formal sobre los procedimientos y estándares.
- Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores.
- Tiene procedimientos no formales de seguridad.

Hay que resaltar que, existen metas que, para ser alcanzadas, requieren de una inversión financiera por parte de la entidad. Razón por la cual, en la hoja de ruta del presente plan se considera el aspecto económico.

4. IMPLEMENTACIÓN

4.1. HOJA DE RUTA

Para la implementación del modelo de privacidad y seguridad de la información – MSPI de la Empresa de Servicios Públicos de Santander S.A. E.S.P. - ESANT S.A. E.S.P. para el periodo 2024 – 2027, se propone la siguiente hoja de ruta que se compone de catorce (14) ítems correspondientes a los dominios de seguridad establecidos por el MINTIC, a saber:

Ítem	Dominio	Acciones	Área(s) Involucrada(s)	Responsable(s)
1	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Elaborar el Manual de Políticas de seguridad y privacidad de la información de la entidad cumpliendo con los lineamientos del MINTIC.	Planeación	Dirección de Planeación
		Aprobar el Manual de políticas de seguridad y privacidad de la información de la entidad en Comité Institucional de Gestión y Desempeño.	Gerencia - Planeación	Gerencia General
		Divulgar las políticas de seguridad y privacidad de la información de la entidad.	Administrativa y Financiera - Planeación	Dirección de Planeación
		Implementar las políticas de seguridad y privacidad de la información a nivel de directorio activo de la entidad.	Planeación	Dirección de Planeación
		Formalizar y aplicar formato de registro de indisponibilidad de servicios tecnológicos.	Planeación	Dirección de Planeación
		Configurar consola antivirus con políticas de seguridad y privacidad de la información de la entidad.	Planeación	Dirección de Planeación
2	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	Implementar el Plan de Tratamiento de riesgos de seguridad y privacidad de la información (PL-TEC-GSI-001) vigente.	Planeación	Dirección de Planeación
		Integrar la seguridad de la información al ciclo de proyectos de cada área de la entidad.	Todas	Dirección de Planeación
		Establecer medidas de control para la salida de equipos móviles (tabletas, celulares, etc.) propiedad de la entidad.	Administrativa y Financiera – Planeación	Dirección Administrativa y Financiera
		Establecer las políticas para el teletrabajo en la entidad.	Administrativa y Financiera – Planeación	Dirección Administrativa y Financiera
3	SEGURIDAD DE LOS RECURSOS HUMANOS	Realizar jornadas de capacitación en temas de seguridad y privacidad de la información.	Administrativa y Financiera – Planeación	Dirección de Planeación
		Promocionar y realizar campañas de concientización en temáticas de seguridad y privacidad de la información a través de medios internos de comunicación.	Planeación	Dirección de Planeación
		Actualizar y/o incluir en el proceso disciplinario toda aquella conducta del personal que atente contra la seguridad y privacidad de la información de la entidad.	Planeación – Administrativa y	Dirección Administrativa y Financiera

Ítem	Dominio	Acciones	Área(s) Involucrada(s)	Responsable(s)
			Financiera – Jurídica - Gerencia	
		Revisar las implicaciones del Manual de Políticas de seguridad y privacidad de la información de la entidad en la gestión del talento humano.	Planeación – Administrativa y Financiera	Dirección de Planeación – Dirección Administrativa y Financiera
4	GESTIÓN DE ACTIVOS	Actualizar el inventario de activos de información cuando se generen novedades, tanto en el Inventario de activos de información (FR-TEC-GSI-001); como en el Inventario físico de propiedad, planta y equipo (FR-GAD-PAI-002).	Planeación	Dirección de Planeación
		Actualizar hojas de vida de equipos de cómputo cuando se generen novedades.	Planeación	Dirección de Planeación
		Actualizar el Instructivo asignación e inhabilitación de recursos tecnológicos (IN-TEC-GSI-001).	Administrativa y financiera – Planeación	Dirección de Planeación
		Actualizar Procedimiento de baja de bienes.	Administrativa y financiera – Planeación	Dirección Administrativa y Financiera
5	CONTROL DE ACCESO	Elaborar política de control de acceso.	Planeación	Dirección de Planeación
		Actualizar la matriz de roles y recursos tecnológicos cuando se requiera.	Planeación	Dirección de Planeación
6	CRIPTOGRAFÍA	Determinar los procesos internos que pueden requerir el uso de criptografía.	Todas	Dirección de Planeación
7	SEGURIDAD FÍSICA Y DEL ENTORNO	Evaluar las condiciones mínimas de seguridad física y ambientales de los cuartos de comunicaciones de la ESANT S.A. E.S.P.	Planeación	Dirección de Planeación
		Presentar informe de evaluación de las condiciones mínimas de seguridad física y ambientales de los cuartos de comunicaciones de la ESANT S.A. E.S.P.	Planeación	Dirección de Planeación
		Definir lineamientos para el uso y mantenimiento de centros de cableado y sus formatos asociados.	Planeación	Dirección de Planeación

Ítem	Dominio	Acciones	Área(s) Involucrada(s)	Responsable(s)
		Establecer normas de uso de equipos fuera de las instalaciones de la ESANT S.A. E.S.P.	Planeación - Administrativa y Financiera – Jurídica - Gerencia	Dirección de Planeación
		Definir los cargos y/o roles que pueden autorizar la salida de la entidad de activos informáticos.	Gerencia – Administrativa y Financiera – Planeación	Gerencia General
		Promover el uso del carné institucional en las diferentes sedes y en los eventos en los que participe personal de la entidad.	Administrativa y Financiera – Planeación	Dirección Administrativa y Financiera
		Mejorar el proceso de registro de visitantes a las instalaciones de la entidad, revisando el Instructivo de Control de ingreso de personal a las instalaciones (IN-GTH-SST-001).	Administrativa y Financiera – Planeación	Dirección Administrativa y Financiera
8	SEGURIDAD DE LAS OPERACIONES	Mantener actualizados los registros de las copias de seguridad de aplicativos.	Planeación	Dirección de Planeación
		Elaborar Plan continuidad del negocio.	Todas	Dirección de Planeación
		Elaborar y divulgar la política de uso de software no autorizado.	Planeación	Dirección de Planeación
		Mantener actualizado el inventario de software de equipos de cómputo.	Planeación	Dirección de Planeación
		Actualizar matrices de roles sistema de información SIGED.	Planeación	Dirección de Planeación
		Actualizar/crear matrices de roles sistema de información GD.	Planeación	Dirección de Planeación
9	SEGURIDAD DE LAS COMUNICACIONES	Actualizar firmware de switches administrables.	Planeación	Dirección de Planeación
		Actualizar el firmware del firewall de la entidad.	Planeación	Dirección de Planeación
		Actualizar firmware de los Access Point – AP.	Planeación	Dirección de Planeación
		Crear política de uso de correo electrónico.	Planeación	Dirección de Planeación
		Implementar correo certificado para comunicaciones emitidas a través del SIGED.	Planeación	Dirección de Planeación
10		Implementar políticas de seguridad de la información a nivel de directorio activo de la entidad.	Planeación	Dirección de Planeación

Ítem	Dominio	Acciones	Área(s) Involucrada(s)	Responsable(s)
	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	Definir los cargos y roles que tendrán uso de firma electrónica.	Planeación - Administrativa y Financiera - Jurídica - Gerencia	Gerencia General
		Definir lineamientos para la solicitud de cambios a los sistemas de información de la entidad (solicitud desarrollo-cambios).	Planeación	Dirección de Planeación
		Definir lineamientos para la solicitud de adquisición de un nuevo sistema de información-software.	Planeación	Dirección de Planeación
		Definir lineamientos para pruebas de aceptación de nuevos sistemas de información, para actualizaciones y nuevas versiones.	Planeación	Dirección de Planeación
11	RELACIONES CON LOS PROVEEDORES	Elaborar la Política de seguridad de la información - Relacionamiento con proveedores.	Planeación	Dirección de Planeación
		Elaborar matriz de proveedores (no solo tecnológicos) en donde se evalué si tienen incidencia alguna con la seguridad y privacidad de la información de la entidad.	Todas	Dirección de Planeación
12	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	Formalizar y aplicar formato de reporte de incidentes TI.	Planeación	Dirección de Planeación
		Elaborar y aplicar formato de requerimientos y eventos TI.	Planeación	Dirección de Planeación
		Elaborar y aplicar Procedimiento de Recepción y atención de requerimientos, incidentes y eventos TIC.	Planeación	Dirección de Planeación
13	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	Elaborar el Plan de continuidad del negocio.	Planeación	Dirección de Planeación
14	CONTROLES	Elaborar Inventario de software instalado.	Planeación	Dirección de Planeación
		Elaborar Políticas de instalación de software.	Planeación	Dirección de Planeación
		Validar y actualizar en caso de que se requiera las Tablas de valoración documental donde se incluyan temas de seguridad y privacidad de la información.	Planeación	Dirección de Planeación
		Actualizar la Política de tratamiento datos personales.	Planeación - Jurídica	Dirección de Planeación

4.2. CRONOGRAMA

A continuación, se muestra el cronograma de actividades propuesto para la implementación del Plan de Seguridad y Privacidad de la Información de la Empresa de Servicios Públicos de Santander S.A. E.S.P. - ESANT S.A. E.S.P. para el periodo 2024 – 2027.

Actividad	2024												2025												2026												2027											
	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
Actualizar el inventario de activos de información cuando se generen novedades.																																															
Actualizar hojas de vida de equipos de cómputo cuando se generen novedades.																																															
Mantener actualizado el formato Control de copias de seguridad de aplicativos.																																															
Actualizar el firmware del firewall de la entidad.																																															
Actualizar firmware switches administrables.																																															
Aplicar el Plan de Tratamiento de riesgos de seguridad y privacidad de la información vigente.																																															
Actualizar la matriz de roles y recursos tecnológicos cuando se requiera.																																															
Promover el uso del carné institucional en las diferentes sedes y en los eventos en los que participe personal de la entidad.																																															
Formalizar procedimiento de recepción y atención de requerimientos, incidentes y eventos tic y sus formatos asociados.																																															
Promocionar y realizar campañas de concientización en temáticas de seguridad y privacidad de la información a través de medios internos de comunicación.																																															
Elaborar e implementar Procedimiento de Recepción y atención de requerimientos, incidentes y eventos TIC.																																															
Elaborar el Manual de Políticas de seguridad y privacidad de la información de la entidad cumpliendo con los lineamientos del MINTIC.																																															
Realizar jornadas de capacitación en temas de seguridad y privacidad de la información.																																															
Evaluar y presentar informe de las condiciones mínimas de seguridad física y ambientales de los cuartos de comunicaciones de la ESANT S.A. E.S.P.																																															
Aprobar el Manual de políticas de seguridad y privacidad de la información de la entidad en Comité Institucional de Gestión y Desempeño.																																															
Divulgar las políticas de seguridad y privacidad de la información de la entidad.																																															

Actividad	2024												2025												2026												2027											
	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
Revisar y definir con los involucrados el proceso de implementación de políticas de seguridad y privacidad de la información.																																															
Evaluar las herramientas utilizadas por el equipo de Administración de personal para la verificación de antecedentes de empleados y contratistas.																																															
Revisar con el equipo de Administración de personal las implicaciones del manual de políticas de seguridad y privacidad de la información de la entidad.																																															
Definir los cargos y/o roles que pueden autorizar la salida de la entidad de activos informáticos.																																															
Implementar políticas de seguridad y privacidad de la información con todos sus componentes.																																															
Actualizar la Política de tratamiento datos personales.																																															
Definir los cargos y roles que tendrán uso de firma electrónica.																																															
Actualizar procedimiento de baja de bienes.																																															
Elaborar Inventario de software instalado.																																															
Actualizar matrices de roles sistema de información SIGED.																																															
Validar y actualizar en caso de que se requiera las Tablas de valoración documental donde se incluyan temas de seguridad y privacidad de la información.																																															
Definir lineamientos para el uso y mantenimiento de centros de cableado y sus formatos asociados.																																															
Elaborar plan de continuidad del negocio.																																															
Aprobar plan de continuidad del negocio en Comité Institucional de Gestión y Desempeño.																																															
Publicar el plan de continuidad del negocio.																																															
Implementar el plan de continuidad del negocio.																																															
Actualizar el Instructivo asignación e inhabilitación de recursos tecnológicos.																																															
Mejorar el proceso de registro de visitantes a las instalaciones de la entidad.																																															
Definir lineamientos para aceptación y solicitud de nuevos sistemas de información; y solicitud de cambios, actualizaciones y nuevas versiones a sistemas de información existentes.																																															
Aprobar lineamientos para aceptación y solicitud de nuevos sistemas de información; y solicitud de cambios, actualizaciones y nuevas versiones a sistemas de información existentes.																																															
Elaborar matriz de proveedores.																																															
Actualizar/crear matrices de roles sistema de información GD.																																															
Implementar correo certificado para comunicaciones emitidas a través del SIGED.																																															

NORMATIVIDAD

- **Ley 599 de 2000.** Por la cual se expide el Código Penal.
- **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.** Por la cual se dictan disposiciones generales para la protección de datos personales.
- **Decreto 1377 de 2013**. Por la cual se reglamenta parcialmente la Ley 1581 de 2012.
- **NTC-ISO/IEC Colombiana 27001:2013**: Norma Técnica Colombiana NTC-ISO-IEC 27001.Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de Información.
- **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 de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones.
- **Decreto 103 de 2015.** Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- **Decreto 1078 de 2015.** Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- **Decreto 1081 de 2015.** Por medio del cual se expide el Decreto Único Reglamentario del Sector Presidencia de la República.
- **Decreto 1008 de 2018.** Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
- **Ley 1915 de 2018.** Por la cual se modifica la ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
- **Resolución 1519 de 2020**. Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.
- **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.

CONTROL DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN DEL CAMBIO	
01	12/04/2024	Versión actualizada del Plan de seguridad y privacidad de la información DPL-TIC-PLA-03, con base en nueva estructura documental y codificación.	
ELABORÓ		**REVISÓ**	**APROBÓ**
Nombre: Óscar M. Martínez O. Cargo o rol: Prof. Apoyo TIC		Nombre: Mónica C. Castellanos C. Cargo o rol: Prof. Apoyo Procesos	Nombre: Sergio Andrés Díaz Ardila Cargo o rol: Director de Planeación