



**UNIDAD DE BÚSQUEDA**  
DE PERSONAS DADAS POR DESAPARECIDAS

---

# **PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN**

---

## **PESI 2022-2024**

FEBRERO DE 2022

## Contenido

1. Objetivo .....	2
2. Alcance .....	2
3. Normatividad.....	2
4. Desarrollo .....	5
4.1. Estado Actual.....	5
4.2. Estrategia de Seguridad Digital .....	8
4.2.1. Liderazgo de seguridad de la información .....	8
4.2.2. Gestión de Activos y Riesgos de Seguridad de la Información.....	9
4.2.3. Implementación de Controles de Seguridad de la Información .....	9
4.2.4. Gestión de Incidentes de Seguridad de la Información .....	10
4.2.5. Gestión de Cultura de Seguridad de la Información .....	10
5. Portafolio de Actividades .....	11
6. Alineación con el Plan estratégico de Tecnologías de la información -PETI .....	13
7. APROBACIÓN.....	14

## 1. Objetivo

Definir la ruta de trabajo enmarcada en el Sistema de Seguridad de la Información de la UBPD con el fin de posicionar al Sistema en un nivel de madurez aceptable, propendiendo por la preservación de la confidencialidad, integridad, disponibilidad y privacidad de la información de la entidad, dando cumplimiento a la política de seguridad de la información, aplicando las buenas prácticas referenciadas en la ISO/IEC 27001 en su última versión y en normativa legal vigente, a partir de la implementación de las estrategias de seguridad digital definidas en este documento para las vigencias 2022 - 2024.

## 2. Alcance

El presente plan comprende la descripción de las actividades a realizar para la implementación del Sistema de Seguridad de la Información, es aplicable a todos los procesos de la Unidad de Búsqueda de Personas dadas por Desaparecidas, equipos territoriales, proveedores y terceros. Al igual que comparte el alcance definido dentro de la Política de Seguridad de la Información.

## 3. Normatividad

Norma	Descripción
Ley 23 de 1982	Sobre derechos de autor
Ley 734 de 2002	Por la cual se expide el Código Disciplinario único, Artículo 34 literal 4 y 5 Artículo 35 literal 21
Ley 1474 de 2002	Por el cual se promulga el “Tratado de la OMPI, Organización Mundial de la Propiedad Intelectual, sobre Derechos de Autor (WCT)”, adoptado en Ginebra, el veinte (20) de diciembre de mil novecientos noventa y seis (1996)
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 (...)
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.

Norma	Descripción
Ley 1341 de 2009	Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones – TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.
Directiva Presidencial 9 de 2010	Establece la obligación que tienen las Entidades públicas de ajustar anualmente sus planes sectoriales e institucionales
Documento Conpes 3701 de 2011	Con el fin de abordar las incertidumbres, los riesgos, las amenazas, las vulnerabilidades y los incidentes digitales, en el 2011, el Gobierno Nacional expide los Lineamientos de Política para Ciberseguridad y Ciberdefensa.
Ley 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
Decreto 2609 de 2012	Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
Decreto 2693 de 2012	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones.
Decreto 1377 de 2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
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 2573 de 2014	Decreto mediante el cual se dan los tiempos de implementación de la Estrategia de Gobierno en Línea y donde se establece que el modelo de seguridad y privacidad de la información pertenece al componente de Elementos Transversales.
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 – modificado por el decreto 1008 de 2018
CONPES 3854 de 2016	Política Nacional de Seguridad de Seguridad Digital
Decreto 415 de 2016	Por el cual se adiciona el Decreto único Reglamentario del Sector de la Función Pública, Decreto Número 1083 de 2015, en lo relacionado con la definición de los lineamientos para el

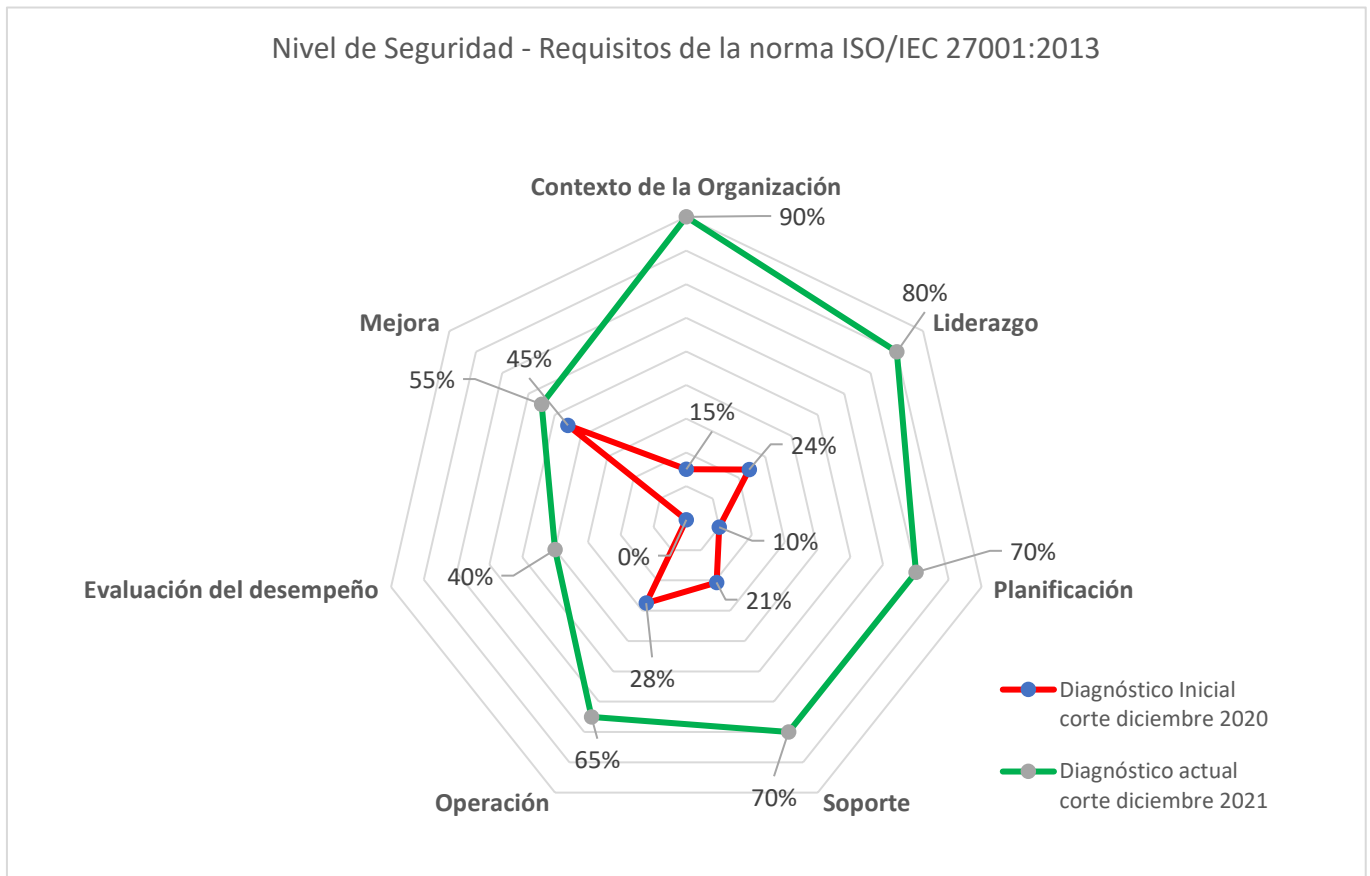
Norma	Descripción
	fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones.
Decreto 1499 de 2017	Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
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
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.
Directiva Presidencial 02 de 2019	Simplificación de la interacción digital entre los ciudadanos y el estado.
Documento CONPES 3975 de 2019	Documento CONPES que formula una política nacional para la transformación digital e inteligencia artificial.
Ley 1978 de 2019	Por la cual se moderniza el sector de las tecnologías de la información y las comunicaciones - TIC, se distribuyen competencias, se crea un regulador único y se dictan otras disposiciones.
CONPES 3995 DE 2020	Política Nacional de Confianza y Seguridad Digital
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
Ley 2018 de 2021	"Ley de internet como servicio público esencial y universal o por medio de la cual se modifica la ley 1341 de 2009 y se dictan otras disposiciones"
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
Resolución 746 de 2022	Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución No. 500 de 2021.
Decreto 338 de 2022	Por el cual se adiciona el Título 21 a la Parte 2 del libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de

Norma	Descripción
	la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanzas de Seguridad Digital y se dictan otras disposiciones
Directiva presidencial 2 de 2022	Reiteración de la política pública en materia de seguridad digital

#### 4. Desarrollo

##### 4.1. Estado Actual

De acuerdo con el instrumento “Formato Diagnóstico de Seguridad” con corte a diciembre de 2021, el avance general del ciclo PHVA del sistema de Seguridad de la Información es del 76%, tal como se muestra a continuación:



Calificación de los numerales 4 a 10 de la norma ISO 27001:2013			
Numerales	Numeral Evaluado	Calificación	
		Diagnóstico Inicial corte diciembre 2020	Diagnóstico actual corte diciembre 2021
4	Contexto de la Organización	15%	95%
5	Liderazgo	24%	93%
6	Planificación	10%	62%
7	Soporte	21%	94%
8	Operación	28%	70%
9	Evaluación del desempeño	0%	55%
10	Mejora	45%	60%
<b>Nivel de Seguridad</b>		<b>20%</b>	<b>76%</b>

De acuerdo con lo anterior, el nivel de madurez del Sistema de Seguridad de la información de la vigencia 2020 a la vigencia 2021, incrementó en un 56% en lo que se refiere a los numerales de la norma ISO/IEC 27001 sin embargo, al revisar los avances en la implementación de los controles definidos en cada uno de los dominios es necesario realizar énfasis en los numerales cuya calificación es igual o menor al 70%, por lo cual se deben establecer acciones que apoyen la implementación de los controles y lo lleven a un nivel de madurez superior, estos dominios son:

- Planificación
- Operación
- Evaluación de desempeño
- Mejora

Para los demás dominios se deben implementar acciones de monitoreo y mantenimiento para mantenerlos en un nivel de mejoramiento continuo.

En cuanto al componente de Planificación, en lo que respecta a la implementación de los controles del Anexo A de la norma ISO/IEC 27001 el cual posee 114 controles, el avance con corte a diciembre de 2021 es el siguiente:

Promedio de la calificación de las preguntas a los dominios del Anexo A de la norma ISO 27001:2013 y demás estándares					
Anexo	Dominio Evaluado	Calificación			
		Diagnostico Inicial	31-may-21	31-dic-21	Proyectado
A.5	Políticas de seguridad	10%	90%	90%	80%
A.6	Organización de seguridad de la información	34%	46%	68%	80%
A.7	Seguridad de los Recursos Humanos	69%	78%	88%	90%
A.8	Gestión de los Activos	37%	55%	64%	85%
A.9	Control de Acceso	58%	48%	67%	65%
A.10	Criptografía	5%	45%	80%	50%
A.11	Seguridad Física y del Entorno	59%	61%	62%	70%
A.12	Seguridad de las Operaciones	61%	62%	69%	70%
A.13	Seguridad de las Comunicaciones	47%	46%	66%	50%
A.14	Adquisición, desarrollo y mantenimiento de SI	37%	51%	64%	55%
A.15	Relaciones con los Proveedores	56%	55%	73%	65%
A.16	Gestión de Incidentes de Seguridad de la Información	59%	60%	77%	80%
A.17	Gestión de Continuidad del Negocio	11%	10%	41%	60%
A.18	Cumplimiento	48%	48%	49%	70%
	<b>Nivel de Seguridad</b>	<b>42%</b>	<b>54%</b>	<b>68%</b>	<b>69%</b>



Al realizar la revisión de los avances en la implementación de los controles definidos por la Norma ISO 27001:2013, Anexo A, en cada uno de los dominios, se puede concluir que:

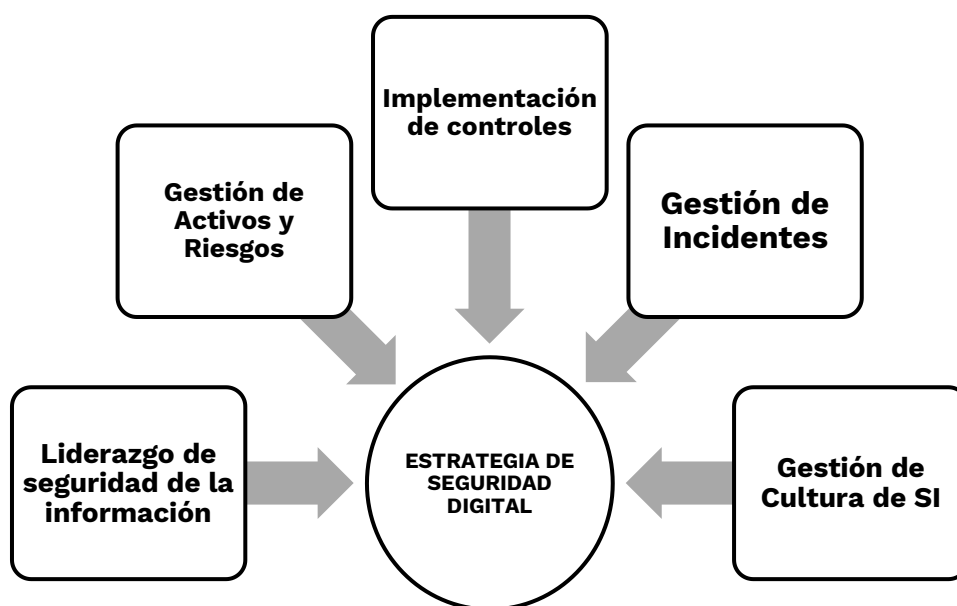
- Los dominios que se encuentra en el nivel bajo inferior al 60%, son: Gestión de continuidad del negocio, y Cumplimiento, para lo cual se deben establecer las acciones que apoyen la implementación de los controles y lo lleven a un nivel de madurez superior.
- Los dominios que se encuentran en el nivel medio, es decir entre 61% y 80% requieren la implementación de acciones de automatización de los controles y herramientas que permitan realizar el monitoreo permanente del control.

- Los dominios que están en nivel alto, superior al 81%, deben implementar acciones de monitoreo y mantenimiento para mantenerlos en un nivel de mejoramiento continuo.
- La calificación general de la implementación de los controles es del 68%, el cual está por debajo de la calificación proyectada.

Por lo anterior es necesario que el portafolio de proyectos de seguridad de la información incluya un proyecto que permita el fortalecimiento y mejoramiento del sistema de gestión de seguridad de la información.

## 4.2. Estrategia de Seguridad Digital

Para elevar el nivel de madurez del Sistema de Seguridad de la Información en la Unidad de Búsqueda de Personas dadas por Desaparecidas en adelante UBPD, se definieron las siguientes estrategias que permitirán establecer en su conjunto la estrategia general de seguridad digital:



### 4.2.1. Liderazgo de seguridad de la información

El mapa de ruta establecido para la implementación del Sistema de Seguridad de la Información de la UBPD, se encuentra detallado en el documento “Plan de Implementación de Seguridad de la Información vigencia 2022”, el cual es aprobado por los miembros del comité de Seguridad de la Información de la entidad y presentado por el Oficial de Seguridad de la Información de la UBPD, en este plan se encuentra la modificación y

aprobación de la política general y demás lineamientos que se definen buscando proteger la confidencialidad, integridad y disponibilidad de la información teniendo como pilar fundamental el compromiso de la alta dirección y de los líderes de las diferentes dependencias y/o procesos de la Entidad a través del establecimiento de los roles y responsabilidades en seguridad de la información

#### **4.2.2. Gestión de Activos y Riesgos de Seguridad de la Información**

Los activos de información de una organización son considerados el segundo recurso más importante después del talento humano, razón por la cual es necesario su correcta clasificación, valoración y protección.

Por lo anterior y de acuerdo con lo gestionado en activos de información en la UBPD, tomando como base el producto del ejercicio realizado el año anterior, se debe realizar un análisis de las matrices de activos de información existentes con el fin de establecer, con los responsables e involucrados de cada proceso, el inventario real de los activos de información, su clasificación y valoración. Así mismo, dar a conocer a todas las personas, especialmente al dueño del activo el valor real de realizar la gestión de activos de información.

De igual forma, la gestión de riesgos de seguridad de la información juega un papel clave en las organizaciones, dado que a través de dicha gestión se pueden aplicar los controles necesarios y de esta manera mitigar el impacto que pueda ocasionar la materialización de un riesgo de seguridad de la información.

Aunque se tiene implementada una metodología de riesgos de gestión, se debe realizar una revisión de la metodología actual que posee la UBPD y actualizar esta, aplicando la guía de riesgos del Departamento de la Función Pública – DAPF en su última versión, esto con el fin de iniciar la identificación de riesgos de seguridad de la información, aplicando la metodología e instrumentos diseñados a partir de la documentación antes mencionada, dado que las matrices de riesgos actuales poseen inconsistencias las cuales no permiten mantener la gestión de riesgos de seguridad de la información en un nivel de madurez aceptable.

Así mismo, se debe definir el plan de tratamiento de riesgos de seguridad de la información, de los riesgos identificados en cada uno de los procesos, la aceptación por parte de los líderes de proceso a dicho plan y realizar el seguimiento a la implementación de este plan.

#### **4.2.3. Implementación de Controles de Seguridad de la Información**

La norma ISO 27001 en su última versión, tiene contemplado el cumplimiento de siete (7) requisitos para considerar el establecimiento de un Sistema de Gestión de Seguridad de la Información. Teniendo en cuenta la declaración de aplicabilidad diseñada, una vez

identificados los riesgos de seguridad de la información, se debe realizar la implementación de los controles aplicables a la entidad según lo establecido en dicha declaración.

Es importante darle continuidad a las actividades que se establezcan en el marco de la implementación del Sistema de Seguridad de la Información con el fin de alcanzar el nivel de madurez adecuado y mantener la confidencialidad, integridad, disponibilidad y privacidad de la información.

#### **4.2.4. Gestión de Incidentes de Seguridad de la Información**

La Gestión de Incidentes de seguridad de la información, es la que se aplica al comprometerse un activo de información por la materialización de un riesgo identificado o no. Por tal motivo se debe realizar una revisión y si es pertinente una actualización de la documentación de incidentes de seguridad de la información de la UBPD basándose en la norma ISO/IEC 27001 y en la norma ISO 27035 en sus últimas versiones, con el fin de garantizar una administración de incidentes de seguridad de la información en pro de conocerlos y proceder en el tiempo y manera adecuada para no generar impactos negativos a la entidad.

Se recomienda implementar mecanismos de apropiación para que toda la entidad esté en la capacidad de reaccionar de manera adecuada e inmediata ante un evento o un incidente de seguridad de la información.

#### **4.2.5. Gestión de Cultura de Seguridad de la Información**

Si bien el recurso humano se ha catalogado por mucho tiempo como el eslabón más débil de la cadena de seguridad, es importante que esta concepción sea cambiada y que se consideren a las personas como aliados y garantes de la seguridad de la información en las organizaciones, lo cual se consigue con una cultura de seguridad a conciencia apoyada y aplicada por la alta dirección.

Para fortalecer la construcción de la cultura organizacional se debe realizar la revisión y actualización del plan de socialización de seguridad de la información en la UBPD, e implementar las estrategias necesarias para lograr un nivel de apropiación en seguridad de la información adecuada, realizando además la divulgación de las responsabilidades de todo el personal de la entidad en seguridad de la información.

## 5. Portafolio de Actividades

Para cada estrategia específica, la UBPD ha definido las siguientes actividades que tienen por objetivo lograr la implementación y mejoramiento continuo del Sistema de Seguridad de la Información. La medición se realiza con el indicador “Porcentaje de ejecución de los proyectos PETI enmarcados en el fortalecimiento a la infraestructura tecnológica y seguridad de la información.”, que está orientado principalmente a aumentar el nivel de madurez de la implementación y operación del SSI. El avance en ciclo PHVA del sistema debe aumentar en 9 puntos frente al diagnóstico inicial, para lograr un avance del 85%.

Estrategia	Actividades	Productos Esperados
Liderazgo de seguridad de la información	Revisión, actualización y aprobación de Políticas de Seguridad digital y de la Información y resoluciones asociadas	Políticas de Seguridad Formalizadas e Implementadas. Resoluciones aprobadas
	Actualización, implementación de documentación asociada al sistema de seguridad de la información	Documentación Actualizada
Gestión de Activos y Riesgos de Seguridad de la Información	Definición de lineamientos para la Gestión de activos de información	Matriz de activos publicada
	Levantamiento y publicación de Activos de Información	
	Publicación de instrumentos de Registro de activos de información e índice de información Clasificada y Reservada - Ley 1712 de 2014	
	Reporte Datos Personales - Ley 1581 de 2012	
	Definición de lineamientos para la Gestión de Riesgos de Seguridad y Privacidad de la Información	Matriz de riesgos de seguridad digital
Identificación de Riesgos de Seguridad y Privacidad de la Información	Planes de tratamiento de riesgos	

Estrategia	Actividades	Productos Esperados
	Tratamiento y monitoreo de Riesgos de Seguridad y Privacidad de la Información	
Implementación de Controles de Seguridad de la Información	Revisión de los numerales y controles de la norma ISO 27001:2013	Procedimiento de áreas seguras. Clasificación de la información. Revisión de los lineamientos de navegación
	Actualización de la documentación relacionada con los procedimientos, guías y formatos de los controles implementados	
	Revisión del Plan de recuperación de desastres, y la Documentación del Análisis de Impacto de la Operación	Análisis de impacto de la operación
	Formulación y gestión de indicadores de SSI	Indicadores Medidos
Gestión de Incidentes de Seguridad de la Información	Definición de lineamientos para la Gestión de incidentes de Seguridad de la Información	Procedimiento de gestión de Incidentes formalizado.
	Gestión de vulnerabilidades	Reporte del resultado de las vulnerabilidades gestionadas
	Atención de incidentes	Reporte de Incidentes gestionados
Gestión de Cultura de Seguridad de la Información	Definición de lineamientos para la Cultura de Seguridad y Privacidad de la Información	Sesiones de socialización desarrolladas
	Publicación y ejecución del Plan de Socialización y Divulgación de Seguridad de la Información	
	Curso de seguridad de la información	

Adicional a las actividades aquí definidas se Implementará por parte de seguridad digital las estrategias definidas en el documento Presentación Hoja de Ruta SD.pptx

## 6. Alineación con el Plan estratégico de Tecnologías de la información - PETI

El PESI se encuentra alineado con el PETI, apoyando los lineamientos y principios de calidad, servicio y mejora continua establecidos. Dentro de esta alineación se han definido los proyectos que se muestran en la siguiente gráfica, dentro de los cuales se encuentran los siguientes para apoyar el plan estratégico de seguridad de la Información:

- PRY-19: Implementación y mejora del Sistema de Seguridad de la Información (SSI) para la UBPD, cuyo objetivo es establecer los lineamientos de alto nivel como las políticas de seguridad de la información y las políticas de seguridad digital, hasta los documentos que permitan su implementación, seguimiento y control, de tal manera que permitan garantizar una mejora continua de la gestión de la seguridad.
- PRY-20: Implementar el plan de recuperación ante desastres DRP (Disaster Recovery Plan) aplicable a los Sistemas de Información críticos de la UPBD
- PRY-25: Adquisición de herramientas especializadas para implementar los controles tecnológicos de Seguridad Digital y Seguridad de la Información de la UBPD, el cual consiste en adquirir y poner en operación las herramientas especializadas que apoyen la implementación de los controles tecnológicos de Seguridad Digital y Seguridad de la Información fortaleciendo la protección de datos sensibles e infraestructura de TI crítica.
- PRY-26: Implementar la estrategia de defensa en profundidad para la UBPD, desarrollando las acciones necesarias que permitan poner en práctica esta estrategia.

Para la vigencia 2023 se tiene proyectado realizar los siguientes proyectos:

- PRY-19: Implementación y mejora del Sistema de Seguridad de la Información (SSI) para la UBPD, cuyo objetivo es establecer los lineamientos de alto nivel como las políticas de seguridad de la información y las políticas de seguridad digital, hasta los documentos que permitan su implementación, seguimiento y control, de tal manera que permitan garantizar una mejora continua de la gestión de la seguridad.
- PRY 20: Implementar el plan de recuperación ante desastres DRP (Disaster Recovery Plan) aplicable a los Sistemas de Información críticos de la UPBD
- PRY-28: Implementar el modelo de servicios SOC (Security Operation Center) o Centro de Operaciones de Seguridad para la UBPD - año 1

Para la vigencia 2024 se tiene proyectado realizar los siguientes proyectos:

- PRY-19 - Implementación y mejora del Sistema de Seguridad de la Información (SSI) para la UBPD.
- PRY-25 Adquisición de herramientas especializadas para implementar los controles tecnológicos de Seguridad Digital y Seguridad de la Información de la UBPD.
- PRY-27 Adquirir e Implementar la herramienta especializada para Gestión de Eventos de Seguridad de la Información o SIEM (Security Information and Event Management) para la UBPD.

## 7. APROBACIÓN

El presente plan ha sido sometido a consideración y conocimiento de la alta dirección, el comité de Seguridad de la Información con el objetivo de ser aprobado y aplicado conforme a lo que aquí se define. Queda aprobado en el acta 001 de 2022 (23/02/2022)

Proyectó: Nancy Mireya Barbosa. Contratista.  
Revisó: Diego Ramírez Pulido. Asesor Unidad Especial 01.  
Aprobó: Diego Ramírez Pulido. Asesor Unidad Especial 01.