SNR	**PROCESO: PLANES INSTITUCIONALES** **PROCEDIMIENTO: FORMULACIÓN PLANES INSTITUCIONALES** **FORMATO: ANÁLISIS DEL CONTEXTO**	Código	MP - DNEEP - PO - 01 - PR - 01 - FR - 02
		Versión	1
		Fecha	31/03/2022

PROCESO	**Gestionar el sistema de Seguridad de la información**
Objetivo [Descripción]	**Implementar, sostener y mejorar el sistema de gestión de seguridad de la información**
Conector	**mediante**
Alcance [Descripción]	**políticas, normas, metodologías y procedimientos**
Conector	**para**
Fuga Clave [Descripción]	**gestionar los riesgos de confidencialidad, integridad y privacidad de la información**

Objetivo	**Implementar, sostener y mejorar el sistema de gestión de seguridad de la información mediante políticas, normas, metodologías y procedimientos para gestionar los riesgos de confidencialidad, integridad y privacidad de la información**

CONTEXTO DE LA GESTIÓN DEL PROCESO

Análisis DOFA

Entorno Interno - Debilidades	
1	No se cuenta con un sistema de gestión de seguridad y privacidad de la información implementado, alineado con MIPG, MSPI y fortalecido a nivel institucional
2	No se han asignado formalmente roles y responsabilidades asociados al SGSI.
3	Falta de conocimiento y conciencia sobre seguridad de la información(capacitación)
4	Falta de procedimientos documentados y normalizados para el Sistema de Gestión de Seguridad de la información
5	Aplicaciones e Infraestructura misionales con componentes con altos niveles de obsolescencia
6	No existen aplicaciones y herramientas especializadas en la gestión de la seguridad de la información
7	Falta de una arquitectura tecnológica de referencia (mediante el uso de buenas prácticas ITIL, TOGAF, COBIT) para la gestión de la infraestructura y servicios de tecnología

Entorno Interno - Fortalezas	
1	Compromiso de la Alta Dirección de la SNR en la implementación del SGSI
2	Existe proyecto en ejecución para implementar el SGSI con un plan de trabajo para la vigencia 2022 y enfocado en los procesos misionales de registro
3	La SNR cuenta con metodologías para la construcción y formulacion de documentos para el Sistema de seguridad y privacidad de la información
4	Los documentos de implementación del SGSI en la SNR están alineados con los marcos metodológicos de DAFP y MINTIC
5	
6	
7	

Entorno externo - Amenazas	
1	Proliferación de prácticas de intrusión , secuestro, robo y alteración de activos de información
2	Cambios continuos en la regulación y marcos normativos nacionales
3	Existen diferencias entre marcos conceptuales normativos y los de buenas prácticas estándar (ej.: el concepto de activos de información combina agentes de riesgo que pueden afectar la información. Este es el caso de Guía 5 MSPI Mintic y la Gestión de riesgos DAFP versión 5)
4	
5	
6	
7	

Entorno externo - Oportunidades	
1	Alianzas con Entidades Externas: MINTIC (analisis de vulnerabilidades), Minjusticia (celulas de seguridad de la información), DAFP (soporte en sistemas de gestión)
2	Existen en el mercado herramientas tecnológicas que facilitarian la implementación del Sistema de gestión de Seguridad de la información de la Entidad actualizadas con marcos normativos
3	Oferta de productos y servicios del mercado que facilitan la actualización tecnológica para mejorar la seguridad de la información
4	La implementación del MIPG y el SGSI contribuyen a la mejora de la gestión y desempeño institucional
5	
6	
7	

Priorización de enfoque

			Oportunidad						
			1	**2**	**3**	**4**	**5**	**6**	**7**
0			**Alianzas con Entidades Externas: MINTIC (analisis de vulnerabilidades), Minjusticia (celulas de seguridad de la información), DAFP (soporte en sistemas de gestión)**	**Existen en el mercado herramientas tecnológicas que facilitarian la implementación del Sistema de gestión de Seguridad de la información de la Entidad actualizadas con marcos normativos**	**Oferta de productos y servicios del mercado que facilitan la actualización tecnológica para mejorar la seguridad de la información**	**La implementación del MIPG y el SGSI contribuyen a la mejora de la gestión y desempeño institucional**	**0**	**0**	**0**
Fortaleza	1	**Compromiso de la Alta Dirección de la SNR en la implementación del SGSI**	2	5	3	5			
	2	**Existe proyecto en ejecución para implementar el SGSI con un plan de trabajo para la vigencia 2022 y enfocado en los procesos misionales de registro**	5	5	1	5			
	3	**La SNR cuenta con metodologías para la construcción y formulacion de documentos para el Sistema de seguridad y privacidad de la información**	3	5	1	5			
	4	**Los documentos de implementación del SGSI en la SNR están alineados con los marcos metodológicos de DAFP y MINTIC**	5	5	1	5			
	5	0							
	6	0							
	7	0							
		Total Perfil	**61**						

	Amenaza						
1	**2**	**3**	**4**	**5**	**6**	**7**
Proliferación de prácticas de intrusión , secuestro, robo y alteración de activos de información	**Cambios continuos en la regulación y marcos normativos nacionales**	**Existen diferencias entre marcos conceptuales normativos y los de buenas prácticas estándar (ej.: el concepto de activos de información combina agentes de riesgo que pueden afectar la información. Este es el caso de Guía 5 MSPI Mintic y la Gestión de riesgos DAFP versión 5)**	**0**	**0**	**0**	**0**
5	5	1				
5	3	1				
1	5	5				
3	5	5				
	44					

Debilidad	1	No se cuenta con un sistema de gestión de seguridad y privacidad de la información implementado, alineado con MIPG, MSPI y fortalecido a nivel institucional	2	3	5	2				5	3	5				
	2	No se han asignado formalmente roles y responsabilidades asociados al SGSI.	1	1	1	2				5	5	3				
	3	Falta de conocimiento y conciencia sobre seguridad de la información(capacitación)	2	1	1	2				5	3	1				
	4	Falta de procedimientos documentados y normalizados para el Sistema de Gestión de Seguridad de la información	2	1	1	2				5	5	1				
	5	Aplicaciones e infraestructura misionales con componentes con altos niveles de obsolescencia	1	1	5	1				5	3	1				
	6	No existen aplicaciones y herramientas especializadas en la gestión de la seguridad de la información	1	5	5	2				3	5	3				
	7	Falta de una arquitectura tecnológica de referencia (mediante el uso de buenas prácticas ITIL, TOGAF, COBIT) para la gestión de la infraestructura y servicios de tecnología	1	5	5	2				5	5	1				
		Total Perfil	63							77						

Matriz Dofa

MATRIZ DOFA	OPORTUNIDADES							AMENAZAS						
	Alianzas con Entidades Externas: MINTIC (analisis de vulnerabilidades), MinJusticia (cebllas de seguridad de la información), DAFP (soporte en sistemas de gestión)	Existen en el mercado herramientas tecnológicas que facilitarian la implementación del Sistema de gestión de Seguridad de la Información de la Entidad actualizadas con marcos normativos	Oferta de productos y servicios del mercado que facilitan la actualización tecnológica para mejorar la seguridad de la información	La implementación del MIPG y el SGSI contribuyen a la mejora de la gestión y desempeño institucional	0	0	0	Proliferación de prácticas de intrusión , secuestro, robo y alteración de activos de información	Cambios continuos en la regulación y marcos normativos nacionales	Existen diferencias entre marcos conceptuales normativos y los de buenas prácticas estándar (ej.: el concepto de activos de información combina agentes de riesgo que pueden afectar la información. Este es el caso de Guia 5 MSPI Mintic y la Gestión de riesgos DAFP versión 5)	0	0	0	0
FORTALEZAS	Estrategias FO							Estrategias FA						
1 Compromiso de la Alta Dirección de la SNR en la implementación del SGSI	F1.01 Integrar a la Alta Dirección en la gestión de alianzas de alto valor en seguridad de la información para la SNR F1.04 Mantener en alto el compromiso y la participación activa del Comité de Gestión y Desempeño Institucional durante la implementación del SGSI mediante informes mensuales de avance							A1.1 Implementación de los procedimientos de gestión de activos de información y tratamiento de riesgos, gestión de vulnerabilidades y gestión de incidentes de seguridad de la información (plan de implementación 2022) A1.2 Despliegue del plan de comunicaciones y capacitación del SGSI 2022 A2.1 Asignar formalmente en la OTI el rol de identificación y reporte de cambios normativos que afecten o incidan el SGSI						
2 Existe proyecto en ejecución para implementar el SGSI con un plan de trabajo para la vigencia 2022 y enfocado en los procesos misionales de registro	F2.01 Coordinar y formalizar la alianza con Csirt Gobierno en la identificación de vulnerabilidades técnicas de los sistemas de información misionales de la SNR F2.02 Ejecutar el proceso de selección y contratación de plataforma de gestión del SGSI F2.03 Implementar el procedimiento de gestión de vulnerabilidades técnicas F2.04 Ejecutar el plan de trabajo propuesto del SGSI para 2022													
3 La SNR cuenta con metodologías para la construcción y formulacion de documentos para el Sistema de seguridad y privacidad de la información	F3yF4.02 Asegurar el cumplimiento de los procedimientos SGSI diseñados para la SNR con la plataforma de soporte para el SGSI a ser adquirida													
4 Los documentos de implementación del SGSI en la SNR están alineados con los marcos metodológicos do DAFP y MINTIC														
5 0														
6 0														
7 0														
DEBILIDADES	Estrategias DO							Estrategias DA						
1 No se cuenta con un sistema de gestión de seguridad y privacidad de la información implementado, alineado con MIPG, MSPI y fortalecido a nivel institucional	D1.1. Efetuar analisis de priorización de brechas en el autodiagnóstico. D1.01 Conocer en profundidad los temas que ofrecen las entidades y que ayudarían a una mejor implementación del SGSI teniendo en cuenta la brecha identificada en el autodiagnóstico. Formalizar las alianzas y materializar los beneficios en la implementación SGSI en la SNR.							A1.1 Implementación de los procedimientos de gestión de activos de información y tratamiento de riesgos, gestión de vulnerabilidades y gestión de incidentes de seguridad de la información (plan de implementación 2022) A1.2 Despliegue del plan de comunicaciones y capacitación del SGSI 2022 D2.A1.1 Definición de roles y responsabilidades de seguridad de la información D2.A1.2 Asignación formal de los roles y responsabilidades de seguridad de la información a funcionarios y contratistas A2.1 Asignar formalmente en la OTI el rol de identificación y reporte de cambios normativos que afecten o incidan el SGSI Nota: D7 La OTI adelanta ejercicio de arquitectura empresarial para aproximar una arquitectura de referencia en los sistemas misionales de instrumentos públicos que facilitará la identificación los requerimientos de seguridad de información						
2 No se han asignado formalmente roles y responsabilidades asociados al SGSI.	D1.02 Adelantar contratación de plataforma de implementación ISolución , análisis de brechas para implementación e implementar.													
3 Falta de conocimiento y conciencia sobre seguridad de la información(capacitación)	D1.03.1. Implementar el procedimiento de Analisis de vulnerabilidades técnicas. D1.03.2. Formalizar el equipo de Gestión de incidentes/vulnerabilidades de seguridad de la información. D1.03.3. Priorizar iniciativas de actualización tecnológica, destinar recursos y adquirir tecnologia.													
4 Falta de procedimientos documentados y normalizados para el Sistema de Gestión de Seguridad de la información	D2.1. Formalizar roles y responabilidades de Seguridad de la Información de acuerdo con los avances de la implementación del SGSI.													
5 Aplicaciones e infraestructura misionales con componentes con altos niveles de obsolescencia	D3.1. Implementar el plan de capacitación y comunicaciones asociado a la implementación del SGSI. D3.01. Buscar y aprovechar el apoyo en temas de capacitación en seguridad de la información con entidades en Alianzas estratégicas.													
6 No existen aplicaciones y herramientas especializadas en la gestión de la seguridad de la información	D4.1. Implementar el plan de trabajo vigencia 2022 del SGSI enfocado en procedimientos de Gestión de Activos de Información y tratamiento de riesgos, Gestión de vulnerabilidades técnicas y Gestión de incidentes de seguridad de la información. D5. * Incluido en D1.03. D6. * Incluido en D1.02.													
7 Falta de una arquitectura tecnológica de referencia (mediante el uso de buenas prácticas ITIL, TOGAF, COBIT) para la gestión de la infraestructura y servicios de tecnología	D7. Incluido en D1.03.													