Agencia Nacional de Infraestructura

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL

G.I.T DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS TELECOMUNICACIONES

Control de Versiones

Fecha	Versión	Descripción	Autor
31/01/2020	1.0	Creación del Plan	Guillermo Cadena Constratista del GIT de Tecnologías de la Información y las Telecomunicaciones
26/04/2021	2.0	Revisión y Actualización Estructura y contenido del documento	Guillermo Cadena Constratista del GIT de Tecnologías de la Información y las Telecomunicaciones
30/01/2022	3.0	Actualización del documento para formular el plan para la vigencia 2022.	Oscar Ramirez Cárdenas Constratista del GIT de Tecnologías de la Información y las Telecomunicaciones
30/01/2023	4.0	Generación de versión preliminar del plan para la vigencia 2023	Oscar Ramirez Cárdenas Constratista del GIT de Tecnologías de la Información y las Telecomunicaciones

CONTENIDO

1. OBJETIVO 4
2. CONTEXTO 4
3. ALCANCE 4
4. ROLES Y RESPONSABILIDADES. 5
5. ACCIONES PARA EL TRATAMIENTO DE LOS RIESGOS. 5
6. DESCRIPCIÓN DE PROYECTOS. 6
7. HOJA DE RUTA 8
7. MATRIZ DE RELACIONAMIENTO DE RIESGOS VS ACTIVIDADES PARA TRATAMIENTO 9
8. APROBACIÓN 9

1. OBJETIVO

Establecer las actividades, tiempos y recursos involucrados que permitirán llevar a cabo la gestión de los riegos de seguridad de la información, identificados en la entidad.

2. CONTEXTO

La gestión de los riesgos de seguridad de la información es el conjunto de actividades que atiende la necesidad de evitar o reducir pérdidas potenciales y brindan protección a la información, una vez que el proceso de análisis de riesgos ha permitido identificar las causas, debilidades e impacto que afectan los activos de información.

Hace parte del análisis de riesgo la identificación de activos de información, las vulnerabilidades y amenazas a las que se encuentran expuestas así como su probabilidad de ocurrencia y el impacto de las mismas; lo anterior con el fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo.

Es muy importante que las organizaciones cuenten con un plan de tratamiento de riesgos para minimizar impactos en la entidad o afectar el cumplimiento de los objetivos, por lo anterior, se ha visto la necesidad de establecer y ejecutar este plan periódicamente aplicado a la Agencia Nacional de Infraestructura. Previo a este ejercicio, se ha establecido la situación actual de la agencia y la identificación de los activos con sus respectivas amenazas, reflejado en la matriz de riesgos de seguridad, para continuar con la formulación de las medias de protección necesarias estructuradas en este plan.

Los riesgos por desastres naturales, riesgos inherentes relacionados con procesos no adecuados en el tratamiento de la misma información, desconocimiento de normas y políticas de seguridad y el no cumplimiento de estas, suelen ser los temas más frecuentes y de mayor impacto presentes en las entidades. Una organización sin un plan de gestión de riesgos está expuesta a perder su información.

Son requisitos para la ejecución del presente plan:

- Compromiso de la alta gerencia de la ANI.
- Priorizar las actividades del plan, frente a actividades operativas y periódicas del día-día.
- Fortalecer los conocimientos y sensibilización sobre la gestión de riesgos.

3. ALCANCE

El plan de tratamiento de riesgos abarca los riesgos que afectan a los activos de información tanto físicos como digitales, por lo que en su ejecución pueden estar involucrados recursos de otras vicepresidencias o gerencias, este plan hace parte del plan de seguridad y privacidad de la información, en el cual se identifica como PS-04.

La ANI procede a la publicación de la versión preliminar de este documento, en cumplimiento de las normas establecidas y lo actualizará en caso de ser necesario, para alinearlo a los planes del sector y de la entidad, razón por la cual este documento está sujeto a cambios.

4. ROLES Y RESPONSABILIDADES.

Los siguientes roles participan en la ejecución del presente plan:

- **Coordinador del G.I.T de Tecnologías de la Información y las Telecomunicaciones**. Primer nivel de aprobación del plan asigna los recursos internos y coordina los recursos externos al G.I.T, realiza seguimiento, da las directrices y aplicación de ajustes para la ejecución de las actividades. Punto de enlace con la primera línea de defensa y con el comité institucional de Gestión y Desempeño.
- **Contratista de Seguridad de la Información**. Ejecución de algunas de las actividades del plan, coordinación y monitoreo de la ejecución de actividades a cargo de otros participantes de éste.
- **Líder del proceso.** Es el rol responsable del activo de información y sobre quien recae la responsabilidad de la gestión del riesgo, en consecuencia, para efectos del contenido del presente documento, es el encargado de asegurar el cumplimiento de las directrices y lineamientos que se definan para la seguridad de la información.
- **Colaboradores de la ANI:** Responsables de cumplir las directrices y lineamientos que se definan para la seguridad de la información.

5. ACCIONES PARA EL TRATAMIENTO DE LOS RIESGOS.

Los riesgos asociados a la seguridad de la información identificados actualmente en la entidad se armonizan con los riesgos incorporados en otros instrumentos de gestión como: la matriz de riesgos de procesos de la entidad la matriz de riesgos de procesos de la entidad y la matriz de riesgos de corrupción.

Los riesgos de seguridad de la información son:

- R.1 Revelar información reservada y clasificada para beneficio propio o de un tercero
- R.2 Ocultar a la ciudadanía la información considerada pública.
- R.3 Destrucción de información con fines ilícitos
- R.4 Fuga de información.
- R.5 Ataque Informático sobre la plataforma Tecnológica.
- R.6 Inadecuada gestión de requerimientos.
- R.7 Inadecuado tratamiento de datos personales.
- R.8 Cambios o modificaciones no autorizados a la plataforma tecnológica

Las actividades o proyectos que conforman este plan son los siguientes:

1. Continuar la sensibilización y socialización en seguridad de la información.
2. Actualizar componentes de software (aplicación de parches).
3. Realizar ethical hacking y assessment de seguridad y gestionar las vulnerabilidades identificadas.
4. Revisión y actualización de riesgos de seguridad de la información.

6. DESCRIPCIÓN DE PROYECTOS.

A continuación, se detallan algunos de los elementos que hacen parte de los proyectos y actividades formuladas:

1. CONTINUAR LA SENSIBILIZACIÓN Y SOCIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN.	
Proceso / Comentarios	Capacitación.
Descripción y productos:	Contempla el siguiente alcance: • Realización de pruebas de ingeniería social dirigida a usuarios finales (ataques simulados y controlados). • Mensajes de sensibilización y prevención dirigidos a todo el personal. incorporando los siguientes elementos: Video, e-card y test de evaluación.
Periodo de ejecución	Abril – Junio del 2023
Riesgos Mitigados:	R.1 Revelar información reservada y clasificada para beneficio propio o de un tercero. R.2 Ocultar a la ciudadanía la información considerada pública. R.3 Destrucción de información con fines ilícitos R.4 Fuga de información. R.5 Ataque Informático sobre la plataforma Tecnológica. R.6 Inadecuada gestión de requerimientos R.7 Inadecuado tratamiento de datos personales.
Controles Asociados:	A.7.2.2 Toma de conciencia, educación y formación en seguridad
Recursos Requeridos:	Integrantes del equipo de Infraestructura y Seguridad de TI y equipo de comunicaciones de la entidad.

2. ACTUALIZAR COMPONENTES DE SOFTWARE (APLICACIÓN DE PARCHES).	
Proceso/Comentarios:	Administración y gestión de la plataforma tecnológica.
Descripción y productos:	Consiste en la actualización del software con las actualizaciones que permanentemente generan los fabricantes y que la actividad se realice de manera proactiva, el plan tiene como alcance lo siguiente: • Servidores • PC
Periodo de ejecución:	Actualización de servidores: Semestralmente o cuando las condiciones lo requieran. Actualización de PC: Permanente.

2. ACTUALIZAR COMPONENTES DE SOFTWARE (APLICACIÓN DE PARCHES).	
Riesgos Mitigados:	R.5 Ataque Informático sobre la plataforma Tecnológica. R.8 Cambios o modificaciones no autorizados a la plataforma tecnológica
Controles Asociados:	A.12.6.1 Gestión de las vulnerabilidades técnicas.
Recursos Requeridos:	Integrantes del equipo de Infraestructura y Seguridad de TI.

3. REALIZAR ETHICAL HACKING Y ASSESSMENT DE SEGURIDAD Y GESTIONAR LAS VULNERABILIDADES IDENTIFICADAS.	
Proceso/Comentarios:	Gestión de vulnerabilidades.
Descripción y productos:	Realización de un ejercicio de ethical hacking con alcance a la página web y ANISCOPIO, ORFEO y la gestión de las vulnerabilidades detectadas.
Periodo de ejecución:	Segundo semestre 2023
Riesgos Mitigados:	R.5 Ataque Informático sobre la plataforma Tecnológica. R.8 Cambios o modificaciones no autorizados a la plataforma tecnológica
Controles Asociados:	A.12.6.1 Gestión de las vulnerabilidades técnicas.
Recursos Requeridos:	Integrantes del equipo de Infraestructura y Seguridad de TI. Proveedor externo.

4. REVISIÓN Y ACTUALIZACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN.	
Proceso:	Administración y gestión de Riesgos.
Descripción y productos:	Revisión y alineación de la matriz de riesgos de seguridad a las directrices de la guía de gestión de riesgos del DAFP versión 5. Realización de la identificación, valoración y documentación de los riesgos de seguridad con los gestores de riesgo de las áreas de la entidad e incorporación de los riesgos en la matriz de riesgos de seguridad. (El alcance aquí descrito se manejará como una primera fase de la identificación y gestión los riesgos de seguridad en las áreas).
Periodo de ejecución	Marzo – Agosto de 2023

4. REVISIÓN Y ACTUALIZACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN.	
Riesgos Mitigados:	R.1 Revelar información reservada y clasificada para beneficio propio o de un tercero. R.2 Ocultar a la ciudadanía la información considerada pública. R.3: Destrucción de información con fines ilícitos R.4 Fuga de información. R.5 Ataque Informático sobre la plataforma Tecnológica. R.6 Inadecuada gestión de requerimientos R.7 Inadecuado tratamiento de datos personales.
Controles Asociados:	Este proyecto permite aplicar los requerimientos de la ISO27001, identificados como: Valoración y tratamiento de riesgos de seguridad de la información (ítems 8.2 y 8.3 de la norma)
Recursos Requeridos:	Integrantes del equipo de Infraestructura y Seguridad de TI. Gestores de riesgo de las áreas. Líder de riesgos de planeación.

7. HOJA DE RUTA.

La siguiente tabla presenta en forma gráfica la ejecución de los proyectos en el transcurso del año.

Nombre del Proyecto	2023											
	ene	feb	mar	abr	may	jun	jul	ago	sep	oct	nov	dic
1. Continuar la sensibilización y socialización en seguridad de la información.												
2. Actualizar componentes de software (aplicación de parches).												
3. Realizar ethical hacking y assessment de seguridad y gestionar las vulnerabilidades identificadas.												
4. Revisión y actualización de riesgos de seguridad de la información.												

7. MATRIZ DE RELACIONAMIENTO DE RIESGOS VS ACTIVIDADES PARA TRATAMIENTO

ACTIVIDAD	RIESGOS IDENTIFICADOS							
	R.1	R.2	R.3	R.4	R.5	R.6	R.7	R.8
1. Continuar la sensibilización y socialización en seguridad de la información.	X	X	X	X	X	X	X	
2. Actualizar componentes de software (aplicación de parches).					X			X
3. Realizar ethical hacking y assessment de seguridad y gestionar las vulnerabilidades identificadas.					X			X
4. Revisión y actualización de riesgos de seguridad de la información.	X	X	X	X	X	X	X	

8. APROBACIÓN

9. Nombre	Cargo	Firma
Guillermo Gómez Gómez	Coordinador G.I.T. Tecnologías de la información y las Telecomunicaciones	
Diego Alejandro Morales Silva	Vicepresidente de Planeación Riesgos y Entorno	