Agencia Nacional de Infraestructura

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL

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

Bogotá D.C. 2022

GTEC

Control de Versiones

Fecha	Versión	Descripción
31/01/2020	1.0	Creación del Plan
26/04/2021	2.0	Revisión y Actualización Estructura y contenido del documento
31/01/2022	3.0	Actualización del documento para formular el plan para la vigencia 2022.

CONTENIDO

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-06.

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**. seguimiento y monitoreo de la ejecución de las actividades del plan
- **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. Revisar y ajustar la política y estrategia de respaldos.
2. Analizar, definir y documentar los esquemas de contingencia y recuperación – PS-4
3. Despliegue de Microsoft defender en los dispositivos de usuario final.
4. Generación de documentos y adopción de procesos de monitoreo de seguridad y disponibilidad.
5. Continuar la sensibilización y socialización en seguridad de la información – PS-05.
6. Implementar el instructivo de activos de información.
7. Actualizar componentes de software (aplicación de parches).

8. Realizar ethical hacking y assessment de seguridad y gestionar las vulnerabilidades identificadas.

De acuerdo a los riesgos establecidos, a continuación aparece la ficha de los proyectos y actividades para el tratamiento de éstos:

1. REVISAR Y AJUSTAR LA POLÍTICA Y ESTRATEGIA DE RESPALDOS.	
Descripción y productos:	Esta actividad propende por una revisión integral de la política actualmente aplicada, así como la identificación de los ajustes que se deben realizar en cuanto a frecuencia y periodos de retención de back up, para las principales plataformas. Entregable: Nueva versión del instructivo de Copias de Seguridad TI y ajustes aplicados en la operación.
Periodo de ejecución	Mayo – Julio de 2022
Proceso:	GTEC-I-005 Copias De Seguridad De TI
Riesgos Mitigados:	R.3: Destrucción de información con fines ilícitos R.5 Ataque Informático sobre la plataforma Tecnológica.
Controles Asociados:	A.12.3.1 - Respaldo de información
Recursos Requeridos:	Integrantes del equipo de Infraestructura y Seguridad de TI.

2. ANALIZAR, DEFINIR Y DOCUMENTAR LOS ESQUEMAS DE CONTINGENCIA Y RECUPERACIÓN – PS-4	
Proceso:	Recuperación de servicios de TI ante desastres (DRP)
Descripción y productos:	Esta es un proyecto que hace parte del plan de seguridad (Proyecto: PS-4) su objetivo es identificar y documentar las actividades que permitan en forma proactiva, la recuperación de las plataformas ANISCOPIO y Pagina web cuando se presenten situaciones de contingencia como mecanismo para una rápida recuperación de los servicios. Instructivo de recuperación de servicios ANISCOPIO y Página Web.
Periodo de ejecución	Febrero – mayo de 2022
Riesgos Mitigados:	R.5 Ataque Informático sobre la plataforma Tecnológica. R.8 Cambios o modificaciones no autorizados a la plataforma tecnológica.
Controles Asociados:	A.16.1.1 Responsabilidad y procedimientos A.16.1.5 Respuesta a incidentes de seguridad de la información

2. ANALIZAR, DEFINIR Y DOCUMENTAR LOS ESQUEMAS DE CONTINGENCIA Y RECUPERACIÓN – PS-4	
Recursos Requeridos:	Integrantes del equipo de Infraestructura y Seguridad de TI.

3. DESPLIEGUE DE MICROSOFT DEFENDER EN LOS DISPOSITVOS DE USUARIO FINAL.	
Proceso:	Administración y gestión de la plataforma tecnológica
Descripción y productos:	Esta actividad hace parte del proyecto del plan de seguridad y privacidad identificado como: PS-02 Fortalecer la seguridad de los servicios para usuario final. MS Defender for endpoint desplegado en los 505 dispositivos de usuario final que lo requieren. (Fase I).
Periodo de ejecución	Febrero – Julio de 2022
Riesgos Mitigados:	R.3: Destrucción de información con fines ilícitos R.4 Fuga de información. R.5 Ataque Informático sobre la plataforma Tecnológica.
Controles Asociados:	A.12.2.1 Controles contra códigos maliciosos
Recursos Requeridos:	Integrantes del equipo de Infraestructura y Seguridad de TI.

4. GENERACIÓN DE DOCUMENTOS Y ADOPCIÓN DE PROCESOS DE MONITOREO DE SEGURIDAD Y DISPONIBILIDAD.	
Proceso y Comentarios:	Administración y gestión de la plataforma tecnológica.
Descripción y productos:	Esta es una actividad que hace del proyecto PS-03 Generación de documentos con guías, políticas específicas y adopción de procesos de monitoreo de seguridad y disponibilidad, el objetivo de esta actividad es documentar y adoptar un esquema de operación por parte del personal del servicio de soporte para realizar actividades de monitoreo proactivo que permita detectar oportunamente alertas que puedan afectar el rendimiento y desempeño de la plataforma, la Fase I la componen las siguientes plataformas: ○ Red (networking y conectividad) ○ Seguridad (firewall y antivirus)

4. GENERACIÓN DE DOCUMENTOS Y ADOPCIÓN DE PROCESOS DE MONITOREO DE SEGURIDAD Y DISPONIBILIDAD.	
	○ Recursos de servidores críticos (CPU, memoria y disco)
Periodo de ejecución	Marzo – abril de 2022
Riesgos Mitigados:	R.4 Fuga de información. R.5 Ataque Informático sobre la plataforma Tecnológica. R.8 Cambios o modificaciones no autorizados a la plataforma tecnológica.
Controles Asociados:	A.12.1.1 Procedimientos de operación documentados
Recursos Requeridos:	Integrantes del equipo de Infraestructura y Seguridad de TI.

5. CONTINUAR LA SENSIBILIZACIÓN Y SOCIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN – PS-05.	
Proceso / Comentarios	Capacitación.
Descripción y productos:	Este proyecto también hace parte del plan de seguridad. Contempla el siguiente alcance: • Campaña de sensibilización realizada y dirigida a todo el personal incorporando los siguientes elementos: Video, e-card y test de evaluación. • Jornada de capacitación técnica en seguridad para el personal del GIT de Tecnologías de la Información y las Telecomunicaciones.
Periodo de ejecución	Abril – Junio del 2022
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.4 Fuga de información. R.6 Inadecuada gestión de requerimientos R.7 Inadecuado tratamiento de datos personales.
Controles Asociados:	A.12.3.1 - Respaldo de información
Recursos Requeridos:	Integrantes del equipo de Infraestructura y Seguridad de TI.

6. IMPLEMENTAR EL INSTRUCTIVO DE ACTIVOS DE INFORMACIÓN.	
Proceso:	Gestión de activos de información
Descripción y productos:	Su objetivo es formalizar la gestión de activos en la entidad bajo lo establecido en la ley de transparencia y con alcance transversal en la entidad.
Periodo de ejecución	Marzo – Abril del 2022
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.7 Inadecuado tratamiento de datos personales
Controles Asociados:	A.13.2.4 Acuerdos de confidencialidad o de no divulgación A.18.1.4 Privacidad y protección de datos personales A.18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales
Recursos Requeridos:	Integrantes del equipo de Infraestructura y Seguridad de TI.

7. 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: Mensualmente, para PC: Mayo-Julio
Periodo de ejecución:	Actualización de servidores 6 distribuidas desde febrero hasta Julio Actualización de PC: Mayo a Julio de 2022
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.

8. REALIZAR ETHICAL HACKING, VALORACIÓN DE SEGURIDAD Y GESTIÓN DE LAS VULNERABILIDADES IDENTIFICADAS.	
Proceso/Comentarios:	Gestión de vulnerabilidades.

8. REALIZAR ETHICAL HACKING, VALORACIÓN DE SEGURIDAD Y GESTIÓN DE LAS VULNERABILIDADES IDENTIFICADAS.	
Descripción y productos:	Realización de un ejercicio de ethical hacking con alcance a la página web y ANISCOPIO y la gestión de las vulnerabilidades detectadas.
Periodo de ejecución:	Junio de 2022
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.

6. HOJA DE RUTA.

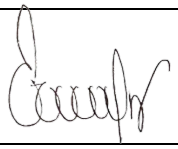
La siguiente tabla muestra la realización de actividades en el tiempo y acorde al alcance establecido.

Nombre del Proyecto	2022											
	ene	feb	mar	abr	may	jun	jul	ago	sep	oct	nov	dic
1. Revisar y ajustar la política y estrategia de respaldos.												
2. Analizar, definir y documentar los esquemas de contingencia y recuperación.												
3. Despliegue de Microsoft defender en los dispositivos de usuario final.												
4. Generación de documentos y adopción de procesos de monitoreo de seguridad y disponibilidad.												
5. Continuar la sensibilización y socialización en seguridad de la información – PS-05.												
6. Implementar instructivo de activos de información.												
7. Actualizar componentes de software (aplicación de parches). Servidores, mensualmente. PC, mayo-Julio												
8. Realizar ethical hacking y assessment de seguridad y gestionar las vulnerabilidades identificadas.												

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. Revisar y ajustar la política y estrategia de respaldos.			X		X			
2. Analizar, definir y documentar los esquemas de contingencia y recuperación.					X			X
3. Despliegue de Microsoft defender en los dispositivos de usuario final.			X	X	X			
4. Generación de documentos y adopción de procesos de monitoreo de seguridad y disponibilidad.				X	X			X
5. Continuar la sensibilización y socialización en seguridad de la información – PS-05.	X	X		X		X	X	
6. Implementar instructivo de activos de información.	X	X					X	
7. Actualizar componentes de software (aplicación de parches). Servidores – mensualmente. PC – PC_ Mayo-Julio					X			X
8. Realizar ethical hacking y assessment de seguridad y gestionar las vulnerabilidades identificadas.					X			X

8. APROBACIÓN

Nombre	Nombre y Cargo	Firma
Elaboró	**Oscar Ramírez Cárdenas** - Contratista G.I.T. Tecnologías de la Información y las Telecomunicaciones	Oscar Ramírez Cárdenas Firmado digitalmente por Oscar Ramírez Cárdenas Fecha: 2022.01.28 20:24:48 -05'00'
Revisó	**Erika Diaz Abella** - Contratista G.I.T. Tecnologías de la Información y las Telecomunicaciones	
Aprobó	**Andrés Francisco Boada** - Coordinador G.I.T. Tecnologías de la Información y las Telecomunicaciones	 Firmado digitalmente por ANDRES FRANCISCO BOADA ICABUCO
	Diego Alejandro Morales Silva Vicepresidente de Planeación Riesgo y Entorno.	Diego Alejandro Morales Silva Firmado digitalmente por Diego Alejandro Morales Silva