PLAN DE TRATAMIENTO DE RIESGOS

DIRECCIÓN DE ORDENAMIENTO SOCIAL DE LA PROPIEDAD RURAL

SUBDIRECCIÓN DE SISTEMAS DE INFORMACIÓN DE TIERRAS

TABLA DE CONTENIDO

1. INTRODUCCIÓN

La cultura de la seguridad de la información en el Agencia Nacional de Tierras - ANT, hace que le conjunto de colaboradores, así como de proveedores de la Entidad, reconozcan su integración e importancia en los diferentes procesos que desarrolla la Agencia, a su vez, actúen con pleno conocimiento y conciencia sobre el manejo de la información, comprendan el grado de responsabilidad y los riesgos que conlleva el uso y la transformación de la misma en las diferentes etapas en su ciclo de vida.

Como parte de la preparación y prevención ante posibles riesgos de seguridad de la información que permita la protección de los recursos, la ANT elabora el plan de tratamiento de riesgos, que no es otras cosa que, trazar una hoja de ruta que permite orientar las acciones a los colaboradores de la Entidad frente a los posibles incidentes de seguridad; esta estrategia busca que la ANT identifique, analice, de tratamiento y evalúe los riesgos de seguridad con el fin de mitigar los efectos o impactos negativos sobre la operación del negocio, mejorar la prestación de servicios, además de, cumplir con las normas y leyes que establece el estado colombiano.

2. DEFINICIONES

- Activo: En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, Hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital. (DAFP 2020).

- Amenaza: es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo). (MinTIC 2021).

- Causa: todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo. (DAFP 2020).

- Control o Medida: acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una entidad. (MinTIC 2021).

- Impacto: son las consecuencias que genera un riesgo una vez se materialice. (MinTIC 2021).

- Probabilidad: se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad

inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año. (DAFP 2020).

- Riesgo de Seguridad de la Información: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

- Vulnerabilidad: es una falencia o debilidad activo o de un control que puede estar presente en la tecnología, las personas o en las políticas y procedimientos que puede ser explotada por una o más amenazas.

3. OBJETIVOS

Objetivo General:

Implementar la gestión de riesgos de seguridad digital basado en la definición metodológica del Modelo de Gestión de Riesgos de Seguridad Digital para, entre otros aspectos, asegurar la confidencialidad, integridad y disponibilidad de los activos de información de la ANT e incrementar la confianza de las múltiples partes interesadas en el uso del entorno digital.

Objetivos Específicos:

- Asegurar razonablemente, en forma consistente y sistemática que los riesgos de seguridad digital de la Agencia sean identificados, evaluados, tratados, monitoreados y comunicados.

- Diseñar e implementar indicadores considerando los eventos de riesgo, para generar oportunamente las alertas necesarias en la toma de decisiones.

- Implementar una herramienta para gestionar los Riesgos de Seguridad Digital y de ciberseguridad en la Agencia Nacional de Tierras.

- Generar mecanismos para que la ANT pueda establecer los elementos para identificar, analizar, valorar y tratar los riesgos, amenazas y vulnerabilidades de su entorno digital.

- Mitigar y prevenir los riesgos de seguridad de la información identificados mediante la implementación de controles que permita la protección de los recursos de TI.

- Tratar de manera integral los riesgos de seguridad de la Información.
- Cumplir con los requisitos legales y normativos colombianos sobre la seguridad digital.
- Fomentar una cultura institucional enfocada a la seguridad de la información y la seguridad digital.
- Fortalecer las buenas prácticas en seguridad de la información con forme lo establece la norma ISO 27001.

4. ALCANCE

Este Plan de Tratamiento de Riesgos de la ANT proyecta desarrollar las actividades en el período comprendido de septiembre de 2022 a agosto de 2023, sólo aplicable a los activos de TI de la ANT.
El Plan de Tratamiento de Riesgo gestionará los riesgos que se encuentren en los niveles Moderado, Grave y Crítico acorde con los lineamientos definidos por la ANT, los riesgos que se encuentren en el nivel Bajo no serán tratados.

5. MARCO DE REFERENCIA

5.1 Política de administración del riesgo

La política de administración del riesgo (DEST-Politica-001 ADMINISTRACIÓN DEL RIESGO) tiene como finalidad establecer los lineamientos para la Administración de Riesgos en la Agencia Nacional de Tierras, a partir de los cuales se definirán los procedimientos y mecanismos de verificación y evaluación encaminados a la búsqueda de la eficiencia, eficacia y transparencia de los procesos.

5.2 Procedimiento de administración de riesgos de gestión

El procedimiento de administración de riesgos de gestión (DEST-P-001 ADMINISTRACION DE RIESGOS DE GESTION), permite determinar los fundamentos y las tareas para facilitar la evaluación y el tratamiento de los Riesgos de Gestión que pueden afectar el logro de los objetivos de procesos y planes establecidos por la Dirección General para el cumplimiento de las funciones asignadas a la Agencia Nacional de Tierras.

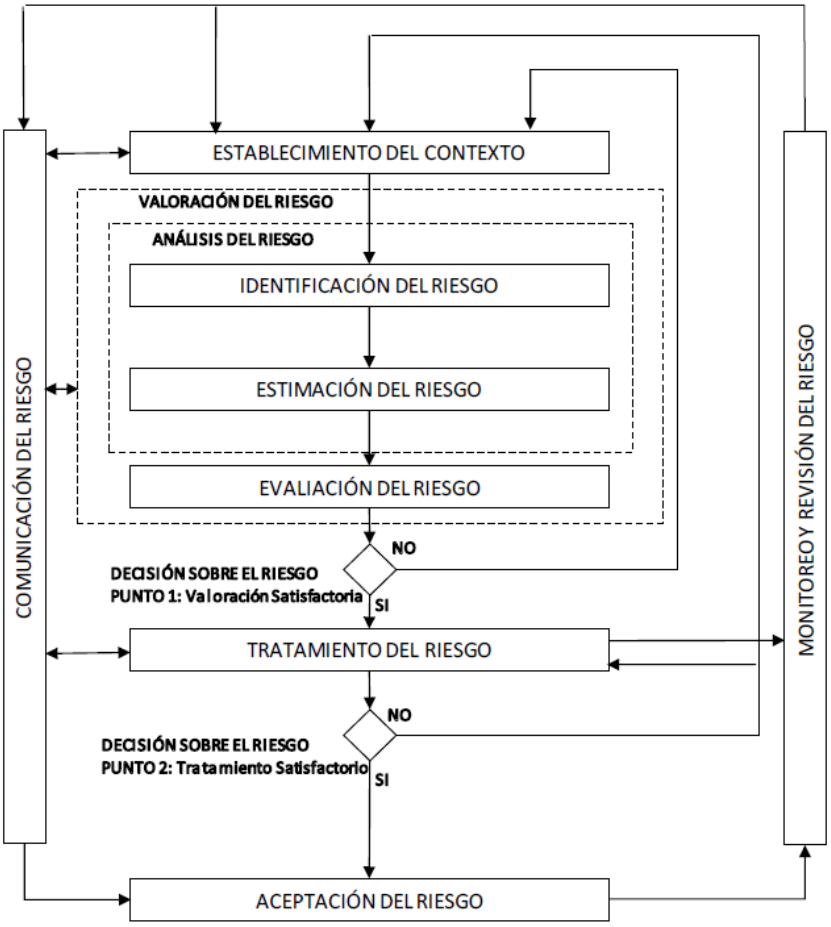
5.3 Política de seguridad de la información

Esta política propone implementar el Sistema de Seguridad de la Información – SGSI, gestionar adecuadamente los riesgos de seguridad, el cumplimiento de las obligaciones legales y contractuales vigentes y aplicables, y la mejora continua del SGSI, además de, satisfacer las necesidades y expectativas de sus partes interesadas en materia de seguridad de la información.

5.4 Guía de gestión de riegos

Se adopta la Guía 7 de Gestión de Riesgos versión 3 de MinTIC, esta guía permite a las entidades gestionar los riesgos de Seguridad de la información basado en los criterios de seguridad (Confidencialidad, Integridad, Disponibilidad) buscando la integración con la Metodología de riesgos del DAFP.
Permite vincular la identificación y análisis de Riesgos de la Entidad hacia los temas de la Seguridad de la Información.

Proceso para la administración de riesgo de seguridad de la información



Fuente: NTC-ISO IEC/27005

5.5 Guía para la administración de riesgos - DAFP

La guía para la administración del riesgo armoniza el Modelo Estándar de Control Interno (MECI) y la Norma Técnica de Calidad NTCGP1000:2009, facilita a las entidades el ejercicio
de la administración del riesgo. Cabe anotar que el ICONTEC a través de la norma NTC-ISO 31000 actualizó la norma NTC5254.

6. METODOLOGÍA

El Plan de Tratamiento de Riesgos define las actividades a desarrollar en la ANT, con el fin de gestionar los riesgos sobre los activos de información identificados, se adopta la metodología conforme las recomendaciones de la Guía de Gestión de Riesgos de

Seguridad y Privacidad de la Información de MinTIC versión 2016.

Para viabilizar la ejecución del Plan de Tratamiento de Riesgos, estratégicamente se plantea el desarrollo por fases, cada una de las fases cubre uno o varios activos de TI (información, sistemas de información, bases de datos, infraestructura y servicios de TI) de acuerdo a su nivel de complejidad y criticidad para la Agencia.

FASE 1: Sistema de Información de Tierras – SIT (Subsistemas: SIDRA, Galería de reportes, Gestión FNA, etc.,) y Orfeo.
FASE 2: Barrido Predial Masivo – BPM, BD Procesos Agrarios y SIG Formalización.
FASE 3: FISO, RESO, SART, Bodega de datos (Sharepoint), SINERGIA y otros sistemas de información críticos.

Plan de tratamiento de riesgos de seguridad Digital		
	Actividad	**Responsable**
Planeación		
1	Elaboración Plan de Trabajo	SSIT
2	Revisión, ajustes y aprobación Plan de Trabajo	SSIT
Ejecución		
3	Identificación nuevos activos de información (contrastar activos de inf. Publicados Vs. los identificados como infraestructura crítica)	SSIT
4	Actualización Matriz de Activos de Información con su respectiva valoración	SSIT
5	Mesas de trabajo para revisión la matriz actualizada con los líderes de TI (AE, BPM, BD RESO, Aplicaciones, EIST)	SSIT
6	Elaborar acta de aprobación de la Matriz de Activos de Información actualizada, gestionar firmas del acta	SSIT, EIST
7	Gestionar aprobación ante el Comité institucional de Gestión y Desempeño	SSIT
8	Gestionar publicación de Matriz de Activos de información actualizada 2022 en la página web de la ANT.	SSIT
	FASE 1 - SIT y Orfeo	
9	Identificación de los riesgos sobre los nuevos activos de información (puntos de riesgo, impacto, factores, clasificación del riesgo. (Mesas de trabajo con usuarios del área misional, EIST, responsable aplicación, responsable de la información)	SSIT, EIST, otros
10	Valoración o Tratamiento de los riesgos de seguridad digital: Análisis, evaluación, estrategia de mitigación, herramientas de gestión, monitoreo y revisión. (Mesas de trabajo con usuarios del área misional, EIST, responsable aplicación, responsable de la información)	SSIT, EIST
11	Elaboración de controles asociados (Anexo A ISO/IEC 27001:2013)	SSIT

12	Identificación de necesidades para desarrollar herramienta para gestionar los Riesgos de Seguridad Digital Dashborad con Power BI) Tablero de control	SSIT
	FASE 2 - BPM, BD Procesos Agrarios y SIG Formalización	
13	Identificación de los riesgos sobre los nuevos activos de información (puntos de riesgo, impacto, factores, clasificación del riesgo)	SSIT, EIST
14	Valoración o Tratamiento de los riesgos de seguridad digital: Análisis, evaluación, estrategia de mitigación, herramientas de gestión, monitoreo y revisión.	SSIT, EIST
15	Elaboración de controles asociados (Anexo A ISO/IEC 27001:2013)	SSIT
16	Desarrollar herramienta para gestionar los Riesgos de Seguridad Digital Dashborad con Power BI) Tablero de control- Identificación de necesidades.	SSIT
	FASE 3 - FISO, RESO, SART, Bodega Datos (Sharepoint), Sinergia y otros SI	
17	Identificación de los riesgos sobre los nuevos activos de información (puntos de riesgo, impacto, factores, clasificación del riesgo)	SSIT, EIST
18	Valoración o Tratamiento de los riesgos de seguridad digital: Análisis, evaluación, estrategia de mitigación, herramientas de gestión, monitoreo y revisión.	SSIT, EIST
19	Elaboración de controles asociados (Anexo A ISO/IEC 27001:2013)	SSIT
20	Mapa de riesgos	SSIT
21	Elaboración de memorando y aprobación del mapa de riesgos	SSIT
22	Capacitaciones (6) sobre seguridad digital y ciberseguridad	SSIT
23	Actualizar la documentación sobre seguridad de la información	SSIT
24	Medición (verificar efectividad de los controles de seguridad) Diseñar e implementar indicadores considerando eventos de riesgos	SSIT
25	Elaboración Informe de medición controles de seguridad	SSIT
26	Implementar una herramienta para gestionar los Riesgos de Seguridad Digital Dashborad con Power BI) Tablero de control basado en los indicadores.	SSIT
27	Cargue de la información en el repositorio de AE	SSIT

Los controles seleccionados serán cruzados con los estándares ISO 27001:2013 y su anexo A, que permite determinar las vulnerabilidades.

6.1 Desarrollo metodológico

6.1.1 Contexto del Plan de Tratamiento de Riesgos

La Agencia Nacional de Tierras – ANT pone especial atención a su Arquitectura de TI, al

modelo de gobierno de TI integrada a su estructura organizacional, a los roles y responsabilidades; contempla además, los procesos internos de gestión institucionales, y con respecto a la seguridad de la información implementa las políticas, lineamientos, gestión y planes; tiene en cuenta las capacidades de sus recursos humanos e infraestructura, los sistemas de información, la información, los flujos de información, los servicios de TI, las expectativas y necesidades de las partes interesadas internas y la cultura organizacional.

La Agencia identifica su entorno a nivel nacional y del exterior, estudia los factores sociales, culturales, políticos, legales, regulatorios, financieros, tecnológicos, económicos, tendencias tecnológicas, necesidades y expectativas de las partes externas interesadas, para lograr un entendimiento de su posición nacionalmente y sectorialmente en materia de seguridad digital.

6.1.2 Identificación de los activos de información

Para registrar los activos de información de la ANT, se realizará cuidadosamente el contraste y análisis entre el inventario de activos de información de la ANT del año 2021 frente a cada uno de los actuales componentes que conforman los dominios de Información, Sistemas de Información, Servicios Tecnológicos y Seguridad, cuyo resultado permitirá identificar nuevos activos de información y gestionar la actualización de los activos de información de la ANT.

Ahora bien, para la identificación de activos de información, la entidad debe:

- Realizar un inventario de los activos de información por cada proceso
- Identificar el dueño del riesgo sobre el activo y el responsable del activo de información
- Clasificar los activos de información
- Determinar el nivel de importancia del activo
- Identificar la Infraestructura Crítica Cibernética (ICC)
- Identificar activos de TI/TO asociados a la Infraestructura Crítica Cibernética (ICC)
- Clasificar la información

De forma complementaria, la entidad debe identificar el dueño del riesgo sobre el activo y responsable o dueño del activo de información:

- Dueño del riesgo o custodio sobre el activo: persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo. Ej. Técnico en operaciones.
- Responsable o dueño del activo de información: cargo de la persona responsable del activo. Ej. jefe de operaciones.

Una vez identificados los activos de información, estos se deben clasificar, esto es, determinar la clasificación de acuerdo con el tipo de activo de información; a continuación, se relacionan algunos tipos de activos:

Personas

Aquellos roles que, por su conocimiento, experiencia y criticidad para el proceso, son considerados activos de información, por ejemplo: personal con experiencia y capacitado para realizar una tarea específica en la ejecución de las actividades.

Documentos información

Datos e información almacenada o procesada física o lógicamente, tales como: contratos, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, registros contables, estados financieros, archivos ofimáticos, documentos y registros del Sistema Integrado de Gestión, entre otros.

Software

Activo informático lógico como aplicaciones, programas, herramientas ofimáticas o sistemas lógicos para la ejecución de las actividades.

Hardware

Equipos de cómputo y de comunicaciones físicos y virtuales, como servidores, impresoras, routers, switches, modems, biométricos que por su criticidad son considerados activos de información.

Servicios

Prestación de un servicio por parte de una compañía para el apoyo de las actividades de los procesos, tales como: internet, páginas web, intranet, interoperabilidad, etc.

Intangibles

Se consideran intangibles aquellos activos inmateriales que otorgan a la entidad una ventaja competitiva relevante, uno de ellos es la imagen corporativa y el good will, entre otros.

Datos/bases de datos

Conjunto de datos y registros lógicos ingresados en las aplicaciones o servidores que a su vez quedan almacenados en un repositorio de datos centralizado. Puede considerarse base de datos, la información alojada en las aplicaciones de contabilidad y nomina, entre otras.

Componentes de red

Medios necesarios para realizar la conexión de los elementos de hardware y software en una red, por ejemplo, el backbone, el cableado estructurado y tarjetas de red, entre otros.

Instalaciones

Espacio o área asignada para alojar y salvaguardar los activos de información, considerados como activos críticos para la empresa.

Dentro de esta identificación de los Activos de Información, cabe mencionar que es muy importante establecer si existe Infraestructura Crítica Cibernética, aquí la entidad debe

determinar si los procesos en los cuales identificó los activos de información son servicios esenciales y si estos hacen parte de la Infraestructura Crítica Cibernética.

6.1.3 Identificación del riesgo

6.1.3.1 Identificación del riesgo inherente de seguridad digital

Los riesgos se deben identificar basados en las amenazas y vulnerabilidades asociadas al activo de información sobre el cual se está haciendo la identificación. En este caso, hay referencias que permiten vislumbrar la claridad que hay que tener para esta definición, en este caso son de gran ayuda los anexos de la NTC ISO27005:2011.

No obstante, la identificación de riesgos también puede ser realizada a través de diferentes metodologías:

- **Lluvia de ideas**: Mediante esta opción se busca animar a los participantes a que indiquen qué situaciones adversas o incidentes de seguridad asociadas al manejo de la información digital y los activos de información se pueden presentar, experiencias conocidas de los participantes en la entidad o en el sector. Las jornadas deben tener un orden de sesión, un líder y personas que ayuden con el registro de las memorias.
- **Juicio de expertos**: A través de este esquema se reúnen las personas con mayor experiencia y conocimiento sobre la materia de análisis e indican cuáles aspectos negativos o riesgos de seguridad digital se pueden presentar. Para emplear esta técnica, se requiere disponer de una agenda con un orden de temas, establecer reglas claras y contar con la participación de un orientador o moderador, así como personas que tomen notas de los principales conceptos expuestos. Al finalizar, se retoman los principales riesgos identificados y se procede a hacer una valoración.
- **Análisis de escenarios**: En este esquema también se busca que un grupo de personas asociadas al proceso determinen situaciones potenciales que pueden llegar a presentarse: caídas de energía que afectan la disponibilidad de servicios, el acceso no autorizado a áreas de cómputo, pérdida de control de una unidad operada remotamente; y con base en estas posibilidades, se determina qué impacto puede provocar sobre la operación.
- **Otras técnicas** que pueden ser empleadas son: entrevistas estructuradas, encuestas, listas de chequeo.

6.1.4 Valoración del riesgo de seguridad

A través de mesas de trabajo con las áreas responsables de los procesos y la mesa técnica de TI, se analiza el contexto, se identifican los riesgos y se realiza el análisis de

la probabilidad e impacto como valoración preliminar para identificar el nivel del riesgo inherente, asociando sus vulnerabilidades e identificando los controles para mitigarlas.

A estos controles se le identifican las variables a evaluar para el adecuado diseño de controles como son: responsable, periodicidad, propósito, cómo se realiza la actividad de control, observaciones o desviaciones y la evidencia de la ejecución del control. Adicionalmente se evalúa que cada control se ejecute de manera consistente, de tal forma que pueda mitigar el riesgo. Esta valoración se realiza de acuerdo con las tablas y metodología establecida y mencionada en la Guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP.

Para llevar a cabo la valoración del riesgo inherente de todos los activos incluidos los de ICC, deben identificarse previamente los siguientes aspectos:

- Probabilidad de ocurrencia
- Impacto asociado a las variables de confidencialidad, integridad, disponibilidad, social, económico y ambiental.

Una vez definidos los riesgos, las amenazas y las vulnerabilidades se calcula la probabilidad de ocurrencia y el impacto para cada uno de los riesgos y se toma como base los criterios definidos en la fase de planificación. Para el caso del impacto, se definen cinco niveles asignados (insignificante, menor, moderado, mayor y catastrófico) para seis variables a saber: confidencialidad, integridad, disponibilidad, social, económico y ambiental. Es importante estimar que la calificación del impacto que pueda generar o establecer el riesgo analizado, como fue mencionado anteriormente, no necesariamente aplica a todas las seis variables. Por lo tanto, se deben considerar solamente aquellas que realmente sirvan para el análisis. El impacto total puede ser la combinación de los valores aplicados en un promedio. El resultado del riesgo inherente está determinado por la relación entre la probabilidad y el impacto.

De esta manera, se busca establecer cuál es el nivel de riesgo sin considerar la existencia de ningún control, así se logra obtener el nivel de riesgo inherente. Por ejemplo: Se identifica un riesgo de acceso no autorizado a una base de datos, la cual es un activo muy importante para la Agencia.

Probabilidad: según registros, esta situación es posible. Por lo tanto, de acuerdo con los criterios de probabilidad definidos tiene una valoración de tres.

Impacto: según el análisis de la información realizada por el experto de la entidad, se determinan los siguientes valores: - Impacto social (1- insignificante) - Económico (3 - moderado) - Confidencialidad (2 - menor) - Integridad (2 - menor).

El resultado obtenido a través de la valoración del riesgo es denominado también tratamiento del riesgo, ya que se "involucra la selección de una o más opciones para modificar los riesgos y la implementación de tales acciones. (DAFP, 2020).

6.1.4.1 Definición de Matriz de Probabilidad e Impacto

La matriz de probabilidad e impacto, llamada también matriz de riesgos, es una herramienta de gestión que permite identificar, de manera rápida y visual, las posibilidades de que ocurra un evento en la entidad, para tomar las medidas preventivas. Las ANT adopta un sistema estándar de calificación para promover el entendimiento común de lo que cada riesgo significa el cual aplica según sus necesidades particulares.

Se deberá establecer los criterios que se definan en los diferentes niveles para valorar los riesgos de seguridad digital en el marco de:

- La probabilidad y el impacto asociados al riesgo en cuestión
- Las cualidades y las características de los controles que estén asociados a los riesgos de seguridad digital
- El nivel de aceptación o apetito del riesgo de seguridad digital
- Las zonas con su respectiva definición, donde se ubiquen los riesgos inherentes durante el análisis y los riesgos residuales durante su evaluación y posterior tratamiento.

La Agencia deberá definir escalas o niveles de medición de los riesgos de seguridad digital, ya sea de forma autónoma o basada en metodologías adoptadas previamente. Para el caso de este ejercicio particular la ANT, propone la definición de una escala de medición para el impacto, probabilidad y riesgo de seguridad digital de cinco niveles, de acuerdo con lo expuesto por la guía para la administración del riesgo de la función pública.

Con respecto a los criterios de impacto, para este plan se hace con base en lo establecido en el modelo MGRSD, y las variables a considerar, para definir los criterios de impacto, son: integridad (I), disponibilidad (D) confidencialidad (C), social (S), económica (E), ambiental (A), las cuales se exponen en la guía de gestión de riesgos de seguridad digital GRSD, Tabla Criterios de valoración de impacto de acuerdo con la información, página 25.

En este contexto, para la definición de escalas o criterios de probabilidad se recomienda tomar como referencia la metodología de riesgos del Departamento Administrativo de la Función Pública DAFP, y en general las buenas prácticas de riesgos que se sugieren una escala de cinco niveles como se muestra en la siguiente ilustración:

Criterios de Valoración de la Probabilidad de Ocurrencia

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

Fuente: Guía DAFP

Zona de riesgo: las zonas de riesgo que se consideran para esta guía, y según lo dispuesto por el DAFP, en los cinco niveles de impacto y en los cinco niveles de probabilidad (donde veinticinco es el mayor valor), a continuación, se muestra gráficamente las zonas de riesgos propuestas para la ANT:

Zonas de Riesgo

Zona de riesgo	Valor asignado	Acción requerida
Extremo	Mayor o igual a 15 y hasta 25	Requiere acciones inmediatas para evitar la materialización de los riesgos asociados a la seguridad digital
Alto	Mayor o igual a 9 y menor de 15	Requiere acciones rápidas, a corto plazo, por parte de la alta dirección para disminuir los riesgos asociados a la seguridad digital
Moderado	Mayor o igual a 4 y menor de 9	Requiere medidas a mediano plazo y adecuadas, que permitan disminuir los riesgos asociados a la seguridad digital
Bajo	Menor de 3	Requiere monitoreo y seguimiento a través de actividades propias de la entidad y preferiblemente de acciones de detección y prevención

Fuente: Guía GRSD Versión 4. (MinTIC 2018).

De la ilustración anterior, cabe explicar que el valor asignado se refiere a los valores sobre los que se establece la combinación del impacto y la probabilidad de un riesgo identificado. Por ejemplo, si el valor del impacto de un riesgo (analizadas las variables de confidencialidad, integridad, disponibilidad, social, ambiental o económica) es igual a

cuatro y el valor de la probabilidad es dos el nivel de riesgo es igual a ocho, lo que lo ubica en la zona de riesgo moderado.

Sin embargo, estas zonas se pueden visualizar en lo que técnicamente se denomina un mapa de calor, como se determina en el contexto de la gestión de riesgos a nivel general.

Con relación a escala de criterios para la definición del impacto, por tratarse de una entidad pública se hace con base en los impactos económicos y reputacionales como las variables principales. Anteriormente para la administración del riesgo se contemplaban afectaciones a la ejecución presupuestal, pagos por sanciones económicas, indemnizaciones a terceros, sanciones por incumplimientos de tipo legal; así como afectación a la imagen institucional por vulneraciones a la información o por fallas en la prestación del servicio, todos estos temas se agrupan en impacto económico y reputacional a partir del año 2020.

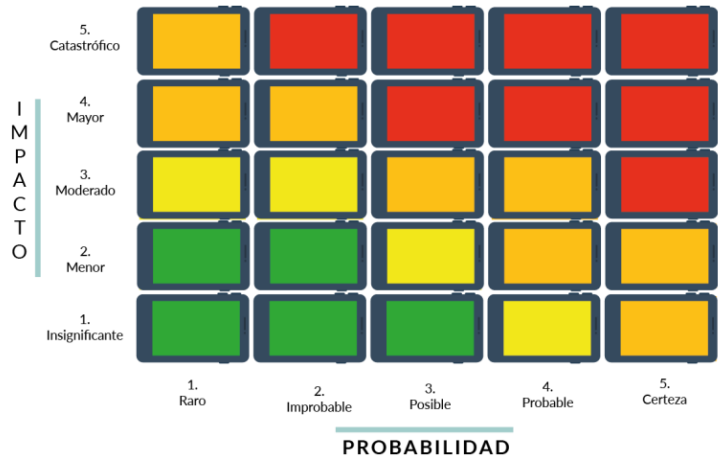
Criterios para definir el nivel de Impacto

	Afectación Económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV .	El riesgo afecta la imagen de algún área de la organización.
Menor-40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

Fuente: Guía DAFP

Ahora bien, la combinación de impacto y probabilidad estará representada por unos intervalos de valor y una descripción que establece a su vez una representación gráfica que se denomina en el contexto de la gestión de riesgos, “mapa de calor”, como se observa en la siguiente ilustración.

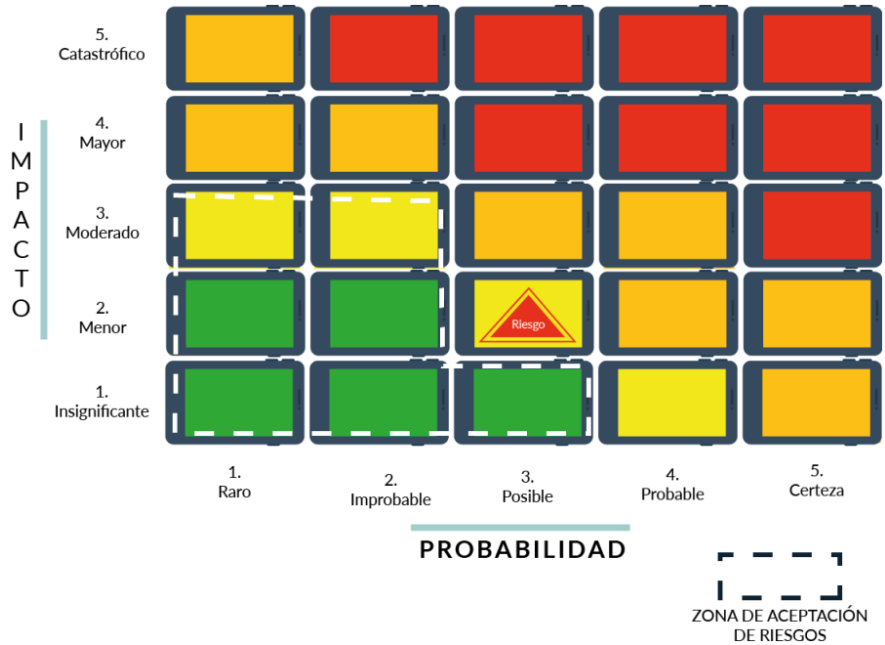
Mapa de Calor



Fuente: Guía GRSD, MinTIC

Avanzando en la definición de los elementos que son claves para el tratamiento de los riesgos, se tiene un concepto y es el correspondiente al apetito o zona de aceptación del riesgo, que corresponde al máximo nivel de riesgo que la organización está dispuesta aceptar. En la siguiente imagen se presenta en línea punteada la definición del apetito de riesgo que la entidad puede definir evaluando sus factores ambientales.

Probabilidad de ocurrencia e Impacto



Fuente: Guía GRSD, MinTIC

6.1.4.2 Análisis de Riesgos

Los análisis de riesgos de una organización, se puede decir que consisten en una serie de técnicas y evaluaciones, de carácter cualitativo y cuantitativo, que ayudan a encontrar riesgos de distinta naturaleza para una institución, hoy en día es totalmente sustentable que, gracias a esta función, el análisis de riesgos es una herramienta muy apreciada por los directivos de cualquier entidad. Esta es una herramienta de prevención con la que se puede pronosticar las amenazas con potencial de afectar el desempeño de algún proceso (cambio, escalada, proyecto o incursión). La idea es que se tenga siempre un plan por adelantado para gestionar lo que podría impactar de manera negativa el desempeño de una organización.

El análisis de riesgos tiene dos vertientes muy conocidas, que son el análisis cualitativo y cuantitativo de los riesgos, estas herramientas permiten determinar el nivel de impacto y probabilidad del riesgo y la urgencia de acuerdo con la tolerancia de los riesgos establecida para la institución. La matriz de impacto y probabilidad que antes reseñamos contiene los valores contemplados para el análisis de los riegos según su ubicación en el mapa de calor, teniendo esta clasificación se realiza a su vez el análisis cualitativo del cual se obtiene un insumo para establecer las estrategias de tratamiento de los riesgos y también el valor de la reserva de contingencias que se puede estimar para sustentar las inversiones que se requieren para establecer un tratamiento de los riesgos de forma sustentada.

6.1.4.3 Priorización de Riesgos

La organización de los riesgos en el mapa de calor permite tener claridad en cuanto al impacto y la urgencia de los riesgos, ahora, con base en este análisis se realiza la correspondiente priorización, actividad que es muy importante con el propósito de concentrar los esfuerzos por parte de los responsables en la entidad, especialmente de los riesgos de alto impacto, para esto es recomendable organizar una lista que ubique los riesgos con base en la calificación establecida en la matriz de probabilidad.

6.1.4.4 Plan de respuestas a los riesgos priorizados

Durante la etapa de planificación de la gestión de los riesgos, una vez que los riesgos se identifican, analizan y priorizan el siguiente paso es elaborar el plan de respuesta a los mismos, que consiste en desarrollar procedimientos y técnicas que permitan mejorar las oportunidades y disminuir las amenazas que inciden en los objetivos, este proceso tal vez es el más importantes dentro de la gestión de riesgos dado que aquí se toman las

decisiones de cómo responder a cada riesgo, en particular a los más críticos o a los priorizados.

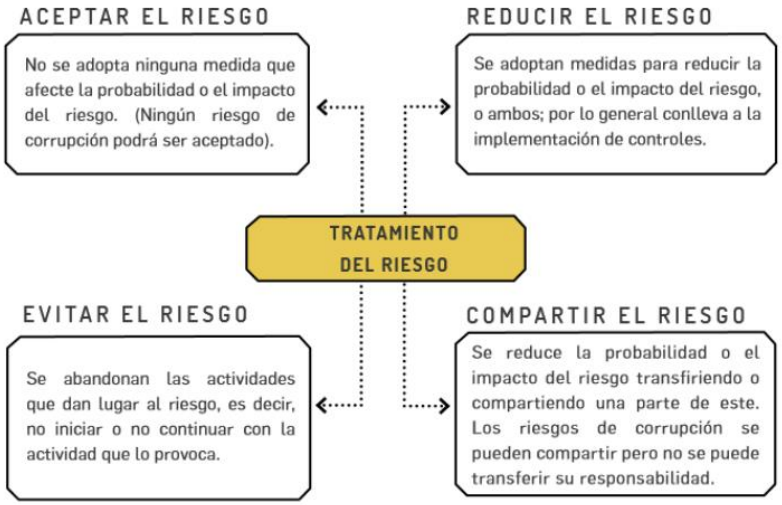
De igual manera, como parte del proceso de respuestas a los riesgos se plantean estrategias que se combinan con un plan específico acorde con la estrategia y los efectos que está tiene sobre el riesgo. Para algunos riesgos, resulta apropiado elaborar un plan de respuesta que sólo se ejecutará bajo determinadas condiciones predefinidas, si se cree que habrá suficientes señales de advertencia para implementar el plan, es decir estas acciones deben ser estructuradas, cuantificadas, presupuestadas y se deben designar recursos para su ejecución, así como nombrar a la persona responsable de implementar la respuesta a dicho riesgo.

Plan de tratamiento de riesgos

A través de la definición del Plan de Tratamiento de Riesgos se tiene como propósito mitigar los riesgos presentes en el análisis de riesgos (Perdida de la Confidencialidad de los activos, Perdida de Integridad de los activos y Perdida de Disponibilidad de los activos) evitando aquellas situaciones que impidan el logro de los objetivos de la Agencia Nacional de Tierras - ANT.

La figura se representa los procedimientos en el tratamiento o respuesta dada al riesgo.

Tratamiento de riesgos



Fuente: DAFP 2020.

6.1.5 Definición y aprobación mapa de riesgos

Al finalizar la administración de riesgos que incluye la valoración de los riesgos de Seguridad Digital, el Subdirector de Sistemas de Información de Tierras deberá emitir memorandos de la aprobación del mapa de riesgos y de aprobación del Plan de Tratamiento de Riesgos de Seguridad Digital con las actividades requeridas que permitan mitigar aquellos riesgos cuyo nivel residual este en zona Moderada, Alta o Extrema.

6.1.6 Materialización de riesgo

En el evento de ocurrencia de la materialización de un riesgo, este debe ser reportado de acuerdo con el procedimiento de gestión de incidentes de seguridad y privacidad de la información de la ANT “GINFO-P-011-PROCEDIMIENTO GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN”.

Se deberá analizar el riesgo y validar su nivel posterior a la materialización, registrando los cambios respectivos en el mapa de riesgos.

En caso de que se materialice un riesgo que no esté identificado, deberá ser reportado para que se inicie su correspondiente identificación en la matriz.

7. EVALUACIÓN Y MEJORA

El desarrollo de las etapas del plan de tratamiento de riesgos ofrece como valor agregado, es el insumo necesario para la identificación de oportunidades, es decir, este plan se debe entender como el desarrollo de actividades enfocadas hacia la mejora siempre pensando en positivo.

La Agencia Nacional de Tierras debe asegurar el logro de sus objetivos anticipándose a los eventos negativos relacionados con la gestión de la entidad.

8. RECURSOS

Recursos	Variable
Humanos	La Subdirección de Sistemas de Información a través del equipo de Arquitectura es responsable de coordinar, implementar, modificar y realizar seguimiento a las políticas, estrategias y procedimientos en

	la Entidad en lo concerniente a la seguridad y privacidad de la información lo cual contribuye a la mejora continua.
Técnicos	Guía para la administración del riesgo y el diseño de controles en entidades públicas Versión 5 -DAFP 2020. Guía para la gestión de riesgos de seguridad digital para el Gobierno nacional, territoriales y sector público. MinTIC 2018. Herramienta para la gestión de riesgos (Matriz de Riesgos SGSI)
Logísticos	Gestión de recursos para realizar socializaciones, transferencia de conocimientos y seguimiento a la gestión de riesgos.
Financieros	Recursos para la adquisición de conocimiento, recursos humanos, técnicos y desarrollo de consultorías y auditorías.

9. PRESUPUESTO

El líder del proceso es el responsable de contribuir con el seguimiento y control de la gestión, además de la implementación de los controles definidos y del plan de tratamiento.

10. MEDICIÓN

La medición hace referencia a la verificación de la efectividad de los controles de seguridad través de la verificación de los indicadores implementados frente al nivel de para evaluar los controles de seguridad de la información.

La SSIT a través del Equipo de Arquitectura de TI deberá tener en cuenta la periodicidad y fechas de cumplimiento establecidas, validando los resultados de los seguimientos realizados, así como el cargue de los soportes correspondientes a los controles definidos. Una vez se reporte el cumplimiento de los planes de tratamiento y controles, el equipo de Arquitectura realiza la revisión y validación de esta información, con el fin de reportar la medición de la gestión del riesgo a través del indicador que tiene como propósito medir el nivel de implementación de los controles de los riesgos de Seguridad Digital.

11. REFERENCIAS

MinTIC, (2018). Modelo nacional de gestión de riesgos de seguridad digital (MGRSD).

MinTIC, (2018). Guía para la gestión de riesgos de seguridad digital para el Gobierno nacional, territoriales y sector público.

DAFP, (diciembre de 2020). Guía para la administración del riesgo y el diseño de controles en entidades públicas VERSIÓN 5.

MinTIC, (2018). Guía para la gestión de riesgos de seguridad digital para el Gobierno nacional, territoriales y sector público.

Lledo, P. (2017). *Administración de proyectos: El ABC para un director de proyectos exitoso.* Pablo Lledó.

HISTORIAL DE CAMBIOS		
Fecha	**Versión**	**Descripción**
	1	Primera versión del documento. Se elabora este documento como parte de la implementación de la gestión de riesgos de seguridad digital para asegurar la confidencialidad, integridad y disponibilidad de los activos de información.

Elaboró: Carlos Eduardo Alfonso Pinilla	**Revisó: Fabian Ricardo Mejía Ospina**	**Aprobó: Comité Institucional de Gestión y Desempeño** (Resolución 183 de 2018)
Cargo: Contratista - Subdirección de Sistemas de Información de Tierras	**Cargo:** Subdirector de Sistemas de Información de Tierras	**Cargo:** Comité Institucional de Gestión y Desempeño, Sesión 1 del 23 de enero de 2023
Firma: **ORIGINAL FIRMADO**	**Firma:** **ORIGINAL FIRMADO**	**Firma:** **ACTA FIRMADA**