Agencia Nacional Digital

Plan de Tratamiento de Riesgos de Seguridad Digital y Privacidad de la Información

BOGOTÁ, ENERO DE 2025

CONTENIDO

1. INTRODUCCIÓN

La Corporación Agencia Nacional Digital, en la adopción de la metodología para la administración del riesgo[1], emitida por El Departamento Administrativo de la Función Pública -DAFP, como entidad técnica, estratégica y transversal del Gobierno nacional, para la Gestión de Riesgos de Seguridad de la Información en realizar la identificación, análisis, valoración, evaluación y tratamiento, a fin de contribuir al cumplimiento de los requisitos de la Entidad, propendiendo el cumplimiento de sus objetivos estratégicos, requisitos legales y reglamentarios, visión y misión, conservación de la confidencialidad, integridad y disponibilidad de la información.

En relación con lo anterior para la aplicación de los lineamientos para La Gestión de Riesgos de Seguridad Digital en Entidades Públicas, se deben identificar los riesgos de seguridad de la información de los procesos en la AND, con el fin de mitigar los posibles efectos de su materialización el cumplimiento de las disposiciones legales, la misión institucional y los objetivos estratégicos, Establece actividades de control para mitigar los riesgos de seguridad de la información asociados a los diferentes procesos, Monitorea los riesgos de seguridad de la información que se identifiquen y establezcan en la matriz de riesgos y Genera la cultura de la gestión del Riesgo de Seguridad y Privacidad de la Información.

Como parte de la gestión de riesgos, la Entidad, mediante la definición del Plan de Tratamiento de Riesgos de Seguridad Digital y Privacidad de la Información, en el cual se proyectan actividades y acciones preventivas para la mitigación de los riesgos, con el fin de mantener en su valoración un riesgo residual aceptable, a través de estrategias, identificación, análisis, tratamiento, evaluación y seguimiento, periódico de los riesgos de seguridad digital para cada uno de los procesos de la entidad identificados y promover una cultura de seguridad digital en relación a la importancia de dar un tratamiento adecuado a la información alineado contexto de los riesgos asociados que podrían comprometer el cumplimiento de los objetivos de la Entidad.

Teniendo en cuenta lo anterior, se actualiza el presente documento dando cumplimiento a lo establecido en el Decreto 612 de 2018, el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información al interior La Corporación Agencia Nacional Digital, aprobado por comité del Modelo Integrado de Gestión.

[1] https://www1.funcionpublica.gov.co/documents/28587410/34299967/Guia_administracion_riesgos_capitulo_riesgo_fiscal.pdf

2. OBJETIVO

Definir y aplicar acciones pertinentes que permitan identificar y tratar los riesgos de seguridad digital y privacidad de la información por los responsables de los procesos de Entidad, así como gestionar los riesgos en materia de seguridad digital, identificados a partir del inventario de activos de información y valorados de acuerdo con el nivel de criticidad, protegiendo y preservando su confidencialidad, integridad y disponibilidad.

3. OBJETIVOS ESPECIFICOS

- ✓ Identificar los riesgos de seguridad de la información asociados a los activos de seguridad digital críticos de los procesos de la Corporación Agencia Nacional Digital, con el fin de mitigar los posibles efectos de su materialización en el cumplimiento de las disposiciones legales, la misión institucional y los objetivos estratégicos.
- ✓ Gestionar los riesgos de seguridad. Digital mediante ejercicios de análisis, evaluación, valoración y seguimiento periódicos para preservar la integridad, disponibilidad y confidencialidad de los activos identificados por proceso.
- ✓ Fortalecer y apropiar cultura en los colaboradores referente a la gestión Riesgos de Seguridad Digital y Privacidad de la Información cumplir con los requisitos legales, reglamentarios, regulatorios y de las normas técnicas colombianas.

4. ALCANCE

Ejecutar una gestión efectiva de riesgos de seguridad digital y privacidad de la información, que faciliten la integración de los procesos de la Entidad, con prácticas óptimas que contribuyan a la prevención de incidentes y a la resolución de problemas que puedan afectar el cumplimiento de los objetivos. Adicionalmente establecer las directrices para poder identificar, analizar, tratar, evaluar y monitorear los riesgos de seguridad digital y privacidad de la información desde su identificación que se encuentren en los niveles “Alto” y “Extremo” en la Matriz de riesgos de Seguridad de la Información de AND hasta la definición del plan de tratamiento, responsables, fechas de implementación y seguimiento, teniendo en cuenta que los riesgos que se encuentren en niveles inferiores serán aceptados por la Corporación Agencia Nacional Digital.

5. NORMATIVIDAD

La normatividad asociada al desarrollo de las actividades del presente plan se encuentra en el Normograma actualizado de Corporación Agencia Nacional Digital.

6. MARCO CONCEPTUAL

A continuación, se listan algunas de los Conceptos básicos relacionados con la gestión del riesgo:

Riesgo: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. **Nota:** Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.	**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 27001).	**Gestor público:** Es todo aquel que participa, concurre, incide o contribuye directa o indirectamente en el manejo o administración de bienes, recursos o intereses patrimoniales de naturaleza pública, sean o no gestores fiscales, por lo tanto, son todos los gestores públicos y no sólo los que desarrollan gestión fiscal, los llamados a prevenir riesgos fiscales"3. A título de ejemplo, además de los gestores fiscales, son gestores públicos, entre otros (sin perjuicio de las particularidades de cada entidad): los contratistas, los interventores, los supervisores en general todos los servidores públicos.	**Recurso público:** Los recursos de inversión y recursos de funcionamiento de cada entidad; los recursos generados por actividades comerciales, industriales y de prestación de servicios, por parte de entidades estatales; los recursos parafiscales; los recursos que resultan del ejercicio de funciones públicas por particulares.
Patrimonio público: Se entiende como el conjunto de bienes o recursos o intereses patrimoniales de naturaleza pública, susceptibles de estimación económica (artículo 6 Ley 610 de 2000 y sentencia C-340-07).	**Activo:** En relación con la segundad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización.	**Bien público:** Son todos aquellos muebles e inmuebles de propiedad pública (este concepto comprende: bienes del Estado y aquellos productos del ejercicio de una función pública a cargo de particulares). Estos se clasifican en bienes de uso público y bienes fiscales, definidos así: a) **Bien de uso público**: aquellos cuyo uso pertenece a todos los habitantes del territorio nacional. Ejemplos: Las calles, plazas, puentes, vías, parques etc. b) **Bienes fiscales:** aquellos que están destinados al cumplimiento de las funciones o servicios públicos (Consejo de Estado, 2012), es decir, afectos al desarrollo de su misión y utilizados para sus actividades. Ejemplos: Los terrenos, edificios, oficinas, colegios, hospitales, otras construcciones, fincas, granjas, equipos, enseres, mobiliario etc.	**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.
Causa: todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la	**Causa Inmediata:** Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el	**Causa Raíz:** Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo. **Causa Raíz (Causa Eficiente o Causa Adecuada):** Es el evento (acción u omisión) que de	**Consecuencia:** los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad,

materialización de un riesgo	riesgo. **Nota:** Tratándose de riesgo fiscal, se usa el término circunstancia inmediata (Causa Inmediata, pero se asocia a la misma causa inmediata.	presentarse es generador directo de un efecto dañoso sobre los bienes, recursos o intereses patrimoniales de naturaleza pública. Es la condición necesaria, de tal forma que, si ese hecho no se produce, el daño no se genera. Así las cosas, la causa raíz se asocia con aquel hecho potencial generador del daño.	sus grupos de valor y demás partes interesadas. **Nota:** Tratándose de riesgo fiscal, el impacto siempre será económico y se identificará en la redacción de riesgos como efecto dañoso, sobre bienes públicos, recursos públicos o intereses patrimoniales públicos.
Riesgo Inherente: Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.	**Control:** Medida que permite reducir o mitigar un riesgo.	**Punto de Riesgo:** Actividades en las que potencialmente se genera riesgo. Tratándose de riesgo fiscal los puntos de riesgo son todas las actividades que representen gestión fiscal, por ejemplo, aquellas de administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos o intereses de naturaleza pública. Para la identificación y priorización de los puntos de riesgo, la entidad deberá tener en cuenta aquellas actividades en las cuales se han presentado advertencias, alertas, hallazgos fiscales y/o fallos con responsabilidad fiscal, así como, aquellas actividades que la organización identifique que pueden generar riesgos fiscales. Para facilitar el ejercicio de identificación de puntos de riesgo consulte el Anexo: Catálogo Indicativo y Enunciativo de Puntos de riesgo fiscal y Circunstancias Inmediatas.	**Riesgo Residual:** El resultado de aplicar la efectividad de los controles al riesgo inherente.
Factores de Riesgo: Son las fuentes generadoras.	**Confidencialidad:** Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados	**Integridad:** Propiedad de exactitud y completitud.	**Disponibilidad:** Propiedad de ser accesible y utilizable a demanda por una entidad.
Vulnerabilidad: Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.	**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,	**Nivel de riesgo:** Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad	**Apetito de riesgo**: Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus Objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano

	entre otros, que utiliza la organización para funcionar en el entorno digital.	institucional de alcanzar los objetivos. En general la fórmula del Nivel del Riesgo poder ser Probabilidad * Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto.	de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.
Tolerancia del riesgo: Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del Apetito de riesgo determinado por la entidad.	**Capacidad de riesgo**: Es el máximo valor del nivel de riesgo que una Entidad puede soportar y a partir del cual se considera por la Alta Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la Entidad.	**Segundad digital:** es la situación de normalidad y de tranquilidad en el entorno digital(ciberespacio), derivada de la realización de los fines esenciales del Estado mediante (i) la gestión del nesgo de segundad digital; (ii) la implementación efectiva de medidas de cibersegundad; y (iu) el uso efectivo de las capacidades de ciberdefensa; que demanda la voluntad social y política de las múltiples partes interesadas y de los ciudadanos del país. (Política Nacional de Confianza y Seguridad Digital [Documento CONPES 3995], 2020).	**Tratamiento de Datos Personales:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley Estatutaria 1581. Art 3.2012).

Tabla 1 Conceptos Riesgo de Seguridad Digital

El Departamento Administrativo de la Función Pública, como entidad técnica, estratégica y transversal del Gobierno nacional, pone a disposición de las entidades la metodología para la administración del riesgo , la cual para la administración del riesgo requiere de un análisis inicial relacionado con el estado actual de la estructura de riesgos y su gestión en las entidades del estado, además del conocimiento de estas desde un punto de vista estratégico de la aplicación de los tres (3) pasos básicos para su desarrollo y, finalmente, de la definición e implantación de estrategias de comunicación transversales a toda la entidades para que su efectividad pueda ser evidenciada. A continuación se puede observar la estructura completa con sus desarrollos básicos:

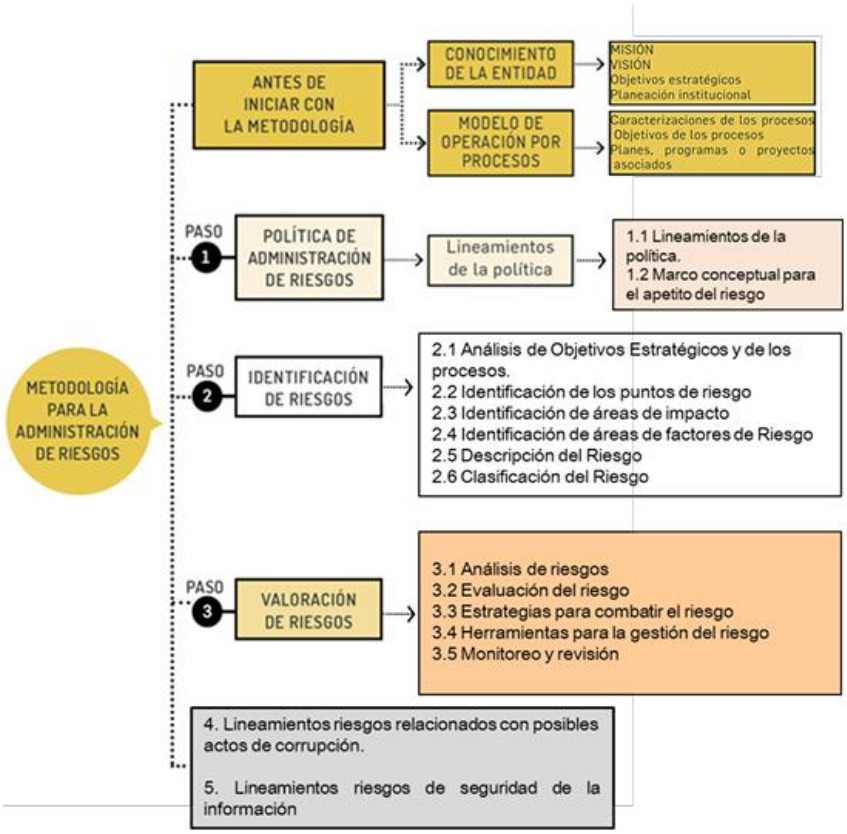

Ilustración 1 Metodología para la gestión del Riesgo en la AND

Fuente: Guía para la Administración del riesgo y el diseño de controles en entidades públicas versión 6, Departamento Administrativo de la Función Pública

En el cumplimiento de la metodología establecida, la Corporación Agencia Nacional Digital realiza la actualización de la Política Gestión Integral Del Riesgo y establece que para los riesgos de seguridad de la información serán identificados, valorados y tratados de acuerdo con la metodología descrita en la Guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP.

Igualmente se tendrá en cuenta que la seguridad de la información en la AND, este acuerdo con las políticas de transparencia, acceso a la información pública y lucha contra la corrupción liderada por la Secretaría de Transparencia y la de Gobierno Digital, específicamente frente a la seguridad de la información en cabeza del Ministerio de Tecnologías de la Información y Comunicaciones, esto teniendo en cuenta la integralidad frente a la gestión del riesgo y la articulación de dichas políticas en el marco del modelo integrado de planeación y gestión (MIPG).

6.1. Líneas de Defensas

De conformidad con lo establecido en el MIPG, se describe en la Política gestión integral del riesgo- AND, el esquema de las líneas de defensa adoptado por la Corporación Agencia Nacional Digital en relación a los riesgos de seguridad digital, es el siguiente:

LINEAS DE DEFENSA	ROL / RESONSABLE	ACTIVIDAD
Primera Línea de Defensa **1. Línea Estratégica** **2. Alta Dirección**	**Líderes de Procesos con el apoyo de los Enlaces designados por Procesos**	Este nivel analiza los riesgos y amenazas institucionales al cumplimiento de los planes estratégicos, tendrá la responsabilidad de definir el marco general para la gestión del riesgo (política de administración del riesgo) y garantiza el cumplimiento de los planes de la entidad. 1) Dar a conocer a su equipo de trabajo la política de administración del riesgo institucional. 2) Identificar y valorar los riesgos que puedan afectar el logro de los objetivos institucionales y de los procesos. 3) Establecer los controles idóneos que permitan administrar los riesgos identificados. 4) Realizar seguimiento permanente a los mapas de riesgos y reporta de acuerdo con la periodicidad establecida. 5) Hacer modificaciones al mapa de riesgos del proceso cuando se requiera.
Segunda Línea de Defensa	**Planeación**	1)Realizar asesoría y acompañamiento en la identificación de los riesgos y en la aplicación de la metodología establecida. 2) Realizar seguimiento a la administración de riesgos ejecutada por los procesos, asegurando que los resultados sean los esperados, de no ser así, deben pronunciarse y asesorar a los procesos en los cambios a los que haya lugar. 3) Consolida los seguimientos a los mapas de riesgos.
Segunda Línea de Defensa	**Funcionarios y/o contratista – delegados**	1) Informa sobre la materialización de los riesgos, la identificación de nuevos riesgos potenciales y evalúan si la valoración del riesgo es la apropiada. 2) Adelantar seguimiento a los mapas de riesgos. 3) Socializa al interior de los procesos los mapas de riesgos.
Tercera Línea de Defensa	**Control Interno**	1)El Control Interno alerta situaciones que generen un posible riesgo (corrupción, gestión, seguridad de la información) en el desarrollo de las actividades ejecutadas por los procesos de la entidad, como resultado de las auditorías internas. 2) Se encarga comunicar a la Dirección posibles cambios e impactos en la evaluación del riesgo, detectados en las auditorías. 3) Se encarga de revisar la efectividad y la aplicación de controles establecidos en los mapas de riesgos.

LINEAS DE DEFENSA	ROL / RESONSABLE	ACTIVIDAD
Responsabilidad de Seguridad Digital	**Profesional de seguridad de la información /Oficial de seguridad**	Además de las líneas de defensa mencionadas y de acuerdo con lo establecido por el Ministerio de Tecnologías de la información y las comunicaciones, la AND delega la responsabilidad de gestionar los riesgos de seguridad de la información, al encargado de seguridad de la información, quien apoya en la identificación de los activos de información de seguridad digital, su clasificación e identificación de infraestructuras criticas cibernéticas, establecimiento de controles para evitar la pérdida de confidencialidad, integridad y/o disponibilidad de la información de la entidad. El oficial de seguridad de la información es el encargado de realizar el análisis de riesgos anualmente, realizar el seguimiento y cada vez que se presente un cambio representativo en los activos tecnológicos o informáticos debe actualizar la información respectiva.
Responsabilidad de Seguridad Digital	**El profesional de datos personales**	Efectuar el análisis de riesgos correspondientes la protección de los datos personales recolectados por la entidad para mitigación los riesgos del Tratamiento de Datos personales

Tabla 2 Líneas de Defensa

6.2. Lineamientos riesgos de seguridad de la información

Tener en cuenta que la política de seguridad digital que vincula al modelo de seguridad y privacidad de la información (MSPI), el cual se encuentra alineado con el marco de referencia de arquitectura TI y soporta transversalmente los otros habilitadores de la política de gobierno digital: seguridad de la información, arquitectura, servicios ciudadanos digitales.

Por lo anterior la Corporación Agencia Nacional de Gobierno Digital – AND, se compromete por medio de la adopción de la política gestión integral del riesgo fortalecer la cultura de prevención, por medio de una adecuada gestión de riesgos, dirigiendo sus esfuerzos hacia el establecimiento de los mecanismos necesarios para evitar, reducir/mitigar, compartir/transferir y/o asumir los riesgos relacionados con el desarrollo de todos sus procesos y que pudieran afectar negativamente a las personas, las instalaciones y/o los bienes de la entidad; para tal efecto realizará la identificación, análisis, valoración e intervención de los riesgos inherentes al que hacer institucional, contribuyendo de esta forma al logro de los objetivos y la misión de la entidad.

El tratamiento de riesgos es la respuesta establecida por la primera línea de defensa, es decir, el líder o responsable del proceso junto con su equipo de trabajo para la mitigación de los diferentes riesgos.

El tratamiento o respuesta dada al riesgo, se enmarca en las siguientes categorías:

Aceptar el riesgo: No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo. (Ningún riesgo de corrupción es aceptado). La aceptación del riesgo puede ser una opción viable en la entidad, para los riesgos bajos, pero también pueden existir escenarios de riesgos a los que no se les puedan aplicar controles y, por ende, se acepta el riesgo. En ambos escenarios debe existir un seguimiento continuo del riesgo.

Reducir el riesgo: Se adoptan medidas para reducir la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles. Deben seleccionarse controles apropiados y con una adecuada segregación de funciones, de manera que el tratamiento al riesgo adoptado logre la reducción prevista sobre este.

Evitar el riesgo: Se abandonan las actividades que dan lugar al riesgo, es decir, no iniciar o no continuar con la actividad que lo provoca.

Compartir el riesgo: Se reduce la probabilidad o el impacto del riesgo transfiriendo o compartiendo una parte de este. Los riesgos de corrupción se pueden compartir, pero no se puede transferir su responsabilidad. Los dos principales métodos de compartir o transferir parte del riesgo son: seguros y tercerización.

En conformidad con la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas. los riesgos sobre seguridad de la información, se debe definir la incorporación del Anexo 4 modelo nacional de gestión de riesgo de seguridad de la información en entidades públicas, de manera tal que los responsables analicen y establezcan, en el marco de sus procesos, los activos de información asociados y se identifiquen los riesgos correspondientes, para lo cual se adopta le implantación de los siguientes pasos identificados en la siguiente ilustración:

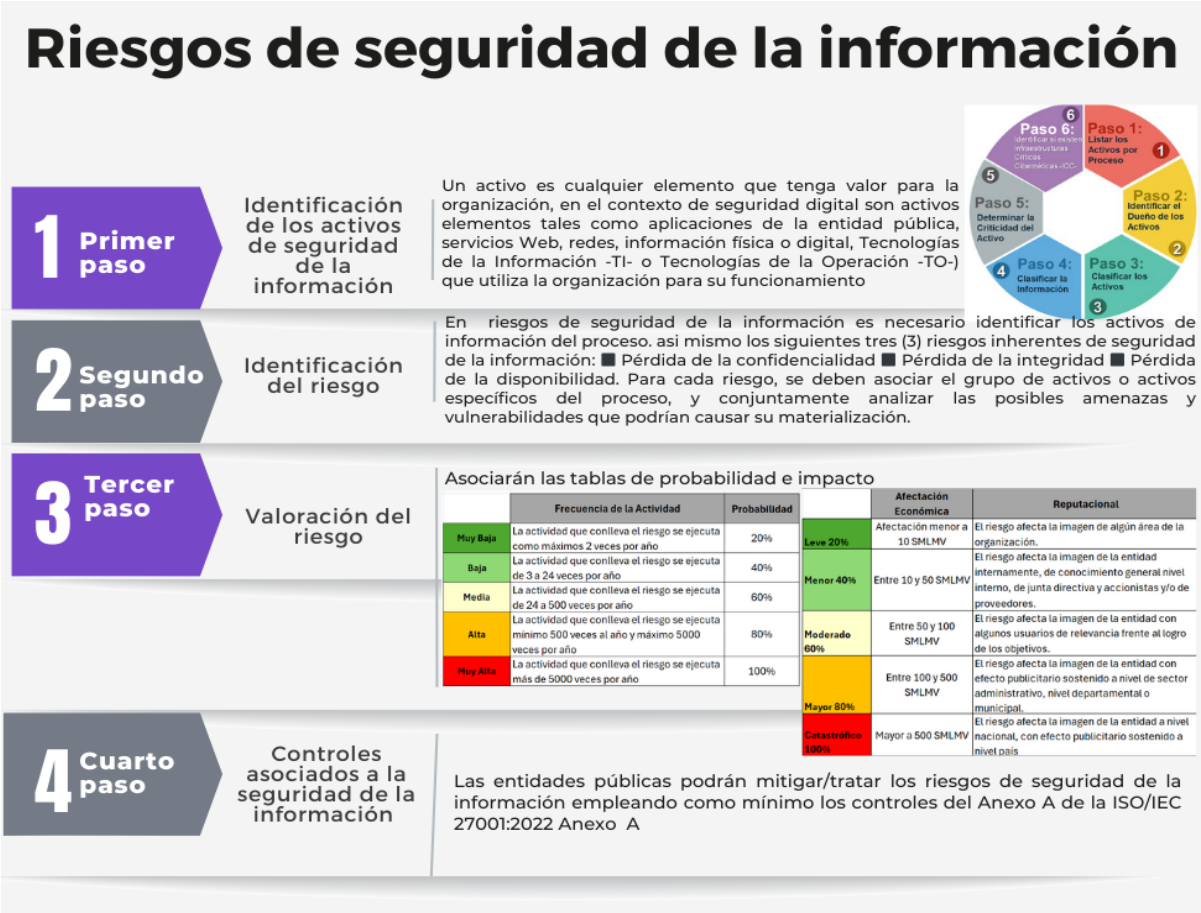

Ilustración 2 Pasos para Lineamientos riesgos de seguridad de la información

6.2.1. Identificación del riesgo

Para la identificación de riesgos de Seguridad Digital y Privacidad de la Información, se debe tener en cuenta diferentes aspectos como infraestructura física, áreas de trabajo, entorno y ambiente en general, para lo cual se hace indispensable que cada uno de los procesos tenga identificado los activos de información, y reconocer las situaciones potenciales que causarían daño a la entidad poniendo en riesgo el logro de los objetivos establecidos.

La falta de apropiación en temas referentes a la seguridad de la información o la ausencia de controles (vulnerabilidades) puede ser aprovechadas por una amenaza causando la materialización de un riesgo (Incidente), por lo que es preciso identificar en el formato del mapa de riesgos: El atributo de la triada de la información afectado (Confidencialidad, Integridad, Disponibilidad), dueño del riesgo (líder del proceso), activo de información afectado, amenazas, vulnerabilidades y consecuencias.

Para determinar los activos afectados es necesario validarlos dentro del inventario de activos de información del proceso en donde en su valoración se estableció la criticidad, la clasificación de la información y otros atributos importantes a tener en cuenta en el análisis del posible riesgo. Es importante mencionar que la identificación de los activos de información se realizó de acuerdo con los lineamientos establecidos por la entidad.

Por otra parte, la identificación de las posibles amenazas y vulnerabilidades es apoyada por el catálogo definido en el anexo 4 "Lineamientos para la gestión del riesgo en entidades públicas" las cuales son analizadas, validadas y complementadas en las mesas de trabajo con los diferentes procesos, y de acuerdo con éstas se establecen las posibles consecuencias.

6.2.2. Valoración del riesgo

La valoración de los riesgos de Seguridad digital y Privacidad de la Información se realizará acorde a la metodología para la administración de riesgos mencionada en la Guía para la administración del riesgo y el diseño de controles en entidades públicas emitida por el Departamento Administrativo de la Función Pública y adoptada para la gestión del riesgo y las tablas de impacto definidas para el AND.

Es así como en mesas de trabajo con los procesos 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 amenazas, vulnerabilidades y consecuencias e identificando los controles asociados al anexo A de la Estándar ISO 27001:2022 para mitigarlas. A estos controles se le identifican las variables a evaluar para su adecuado diseño como son: la asignación de un responsable, segregación y autoridad del responsable, tipo de control (preventivo, detectivo o correctivo), implementación (manual o automático), periodicidad, propósito, cómo se realiza la actividad de control, qué pasa con las 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.

6.2.3. Definición y aprobación de mapas y planes de tratamiento riesgos

Una vez concluidas las etapas de la administración de riesgos y se obtenga la valoración de los riesgos de Seguridad Digital y Privacidad de la Información, del Ministerio, los líderes de los procesos apoyados por los gestores, deberán realizar a través de la plataforma de formalización de documentación definida por el Ministerio

TIC, el proceso de aprobación de los mapas de riesgos y de los planes de tratamiento con las actividades requeridas que permitan mitigar aquellos riesgos cuyo nivel residual este en zona Moderada, Alta o Extrema.

6.2.4. Materialización

En el caso de materializarse un riesgo, este debe ser reportado de acuerdo con el procedimiento de gestión de incidentes de seguridad y privacidad de la información. Así mismo se deberá analizar el riesgo y validar en qué nivel queda 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 el mapa de riesgos.

7. RECURSOS

La estimación y asignación del presupuesto para el plan de tratamiento de Riesgos de Seguridad Digital y Privacidad de la Información identificados en la Entidad, corresponderá al dueño del riesgo, quien es el responsable de contribuir con el seguimiento y control de la gestión, además de la implementación de los controles definidos en el plan de tratamiento en la Corporación Agencia Nacional Digital.

8. PLAN DE TRABAJO

El Plan de implementación de Riesgos de Seguridad Digital y Privacidad de la Información, para la aplicación del habilitador de seguridad de la información de la Política de Gobierno Digital, se proyecta con el fin de proteger y preservar la integridad, disponibilidad y confidencialidad de la información de la AND y se ejecutara de acuerdo con el siguiente cronograma, al cual se le hace seguimiento por parte de oficial de Seguridad de información y el Plan de Acción Institucional

FASE	ACTIVIDADES	FECHA DE INICIO	FECHA FIN	META	RESPONSABLE
PLANEACIÓN	Actualizar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	1/01/2025	30/01/2025	Documento Plan de Tratamiento de Riesgos de Seguridad Digital y Privacidad de la Información 2025	Profesional de Seguridad de la Información / Oficial de seguridad de Información

FASE	ACTIVIDADES	FECHA DE INICIO	FECHA FIN	META	RESPONSABLE
SENSIBILIZACIÓN	Socialización de lineamientos, documentos y/o Herramienta Gestión de Riesgos de Seguridad Digital y Privacidad de la Información	12/03/2025	14/03/2025	Formato listado de asistencia y/o asistencia por Teams Acta y/o grabación	Profesional de Seguridad de la Información / Oficial de seguridad de Información Responsable de Proceso
IDENTIFICACIÓN, ANÁLISIS, VALORACIÓN DE RIESGOS DE SEGURIDAD DIGITAL Y SI	Realizar acompañamiento en la Identificación, Análisis, valoración de controles y definición del manejo de los Riesgos de Seguridad Digital y Privacidad de la Información a los procesos con riesgos asociados	17/03/2025	30/04/2025	Acta de mesa de trabajo Documento Matriz de Riesgos de Seguridad de la Información.	Profesional de Seguridad de la Información / Oficial de seguridad de Información Responsable de Proceso
IDENTIFICACIÓN, ANÁLISIS, VALORACIÓN DE RIESGOS DE SEGURIDAD DIGITAL Y SI	Realizar la realimentación, revisión verificación y aprobación de Riesgos de Seguridad Digital y Privacidad de la Información identificados con sus planes de tratamiento y controles existentes de los procesos.	01/05/2025	09/05/2025	Correo Electrónico Documento actualizado Matriz de Riesgos de Seguridad de la Información	Líderes de Procesos
SEGUIMIENTO, EVALUACIÓN Y MONITOREO DE LOS RIESGOS	Establecer las fechas y avances para el seguimiento de los planes de tratamiento y controles existente por parte del Líder del Proceso	09/05/2025	13/05/2025	Acta de mesa de trabajo Documento Matriz de Riesgos de Seguridad de la Información	Líderes de Procesos Profesional de Seguridad de la Información / Oficial de seguridad de Información

FASE	ACTIVIDADES	FECHA DE INICIO	FECHA FIN	META	RESPONSABLE
SEGUIMIENTO, EVALUACIÓN Y MONITOREO DE LOS RIESGOS	Realizar seguimiento a los Riesgos de Seguridad Digital y Privacidad de la Información identificados asociados a los procesos en el Matriz de Riesgos de Seguridad de la Información.	20/05/2024	30/12/2025	Matriz Mapa de Riesgos de Gestión y Seguridad Digital	Procesos Profesional de Seguridad de la Información / Oficial de seguridad de Información
MONITOREO, REVISIÓN Y MEJORA	Monitorear y reportar el resultado de las actividades actividad de control, que se aplicaron necesarias con el fin de minimizar o mitigar el riesgo y de este modo evitar los daños intrínsecos del factor del riesgo, definidas en los planes de tratamiento de Riesgos de Seguridad Digital y Privacidad de la Información por proceso de AND, así como las oportunidades de mejora .	30/05/2024	30/12/2025	Informe de Riesgos de Seguridad Digital y Privacidad de la Información	Profesional de Seguridad de la Información / Oficial de seguridad de Información Control Interno

Tabla 3 Cronograma Plan Riesgos de Seguridad Digital

9. MEDICIÓN

El monitoreo y seguimiento de los riesgos de Seguridad Digital y Privacidad de la Información de la AND, aprobados por los procesos, así como de sus controles y planes de tratamiento, se realiza por parte del profesional asignado de cada proceso, así como el profesional de Seguridad y Privacidad de la Información con el apoyo de los profesionales Planeación, teniendo 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 los procesos realicen el reporte de cumplimiento de sus planes de tratamiento y controles, el profesional del proceso de Seguridad y Privacidad de la Información realizan 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 y Privacidad de la Información, de la AND.

Se medirá el cumplimiento del presente Plan, a través del resultado del siguiente indicador (#actividades cumplidas / # actividades planificadas) * 100), de las actividades definidas en el plan de tratamiento de Riesgos de Seguridad Digital y Privacidad de la Información que está orientado principalmente a determinar el porcentaje de ejecución de actividades definidas.

10. CONTROL DE CAMBIOS

REVISIÓN No.	FECHA	CAMBIOS
1	30-01-2025	Emisión del documento

Revisó y aprobó: Comité Institucional de Gestión y Desempeño de la Corporación Agencia Nacional Digital, sesión del 28 de enero de 2025.

Elaboró: Catherine Suarez Rodriguez Profesional Seguridad de la Información -AND