Plan

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

GTE-PL-03-V4

Gestión Tecnológica
UNIDAD NACIONAL DE PROTECCIÓN
20-01-2022

Tabla de Contenido

1. OBJETIVO

Generar el Plan de Tratamiento de Riesgos de Seguridad de la Información alineado a la metodológica de Gestión del Riesgo de la entidad, que permita a los responsables de los procesos de la UNP gestionar los riesgos en materia de seguridad y privacidad de la información, identificados a partir del inventario de activos de información y valorados por dueños de los procesos de acuerdo con el nivel de importancia respecto a su confidencialidad, integridad y su disponibilidad.

2. ALCANCE

La gestión de riesgos de seguridad de la información inicia con la identificación de los activos de información de la entidad y termina con el plan de tratamiento de los riesgos a los cuales están expuestos dichos activos, siguiendo las normas vigentes, la metodología definida por la entidad para la gestión del riesgo, las pautas y recomendaciones previstas en la ISO 27005 para su seguimiento, monitoreo y evaluación enfocado al cumplimiento y mejoramiento continuo.

3. DEFINICIONES

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. Fuente: https://www.mintic.gov.co/gestionti/615/articles-5482_Guia_Seguridad_informacion_Mypimes.pdf

Activos de información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal. Fuente: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

Administración del riesgo: Conjunto de elementos de control que al Interrelacionarse brindan a la entidad la capacidad para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia. Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 4 - Riesgos de Gestión, Corrupción y Seguridad Digital Función Pública octubre 2018

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. Fuente: https://www.iso27000.es/glosario.html

Análisis de riesgos: uso sistemático de la información para identificar las fuentes y estimar el riesgo. Fuente: NTC-ISO/IEC 27001

Apetito al riesgo: magnitud y tipo de riesgo que una organización está dispuesta a buscar o retener. Fuente: Guía para la administración del riesgo y el diseño de controles en entidades

públicas – Versión 4 - Riesgos de Gestión, Corrupción y Seguridad Digital Función Pública octubre 2018

Causa: todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo. Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 4 - Riesgos de Gestión, Corrupción y Seguridad Digital Función Pública octubre 2018

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. Fuente NTC-ISO/IEC 27000).

Consecuencia: Los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas. Control: medida que modifica el riesgo (procesos, políticas, dispositivos, prácticas u otras acciones). Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 4 - Riesgos de Gestión, Corrupción y Seguridad Digital Función Pública octubre 2018

Control: Medida por la que se modifica el riesgo. Los controles incluyen procesos, políticas, dispositivos, prácticas, entre otras acciones que modifican el riesgo. Es posible que los controles no siempre ejerzan el efecto de modificación previsto o supuesto. Los términos salvaguardan o contramedida son utilizados frecuentemente como sinónimos de control. Fuente: https://www.iso27000.es/glosario.html

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada. Fuente: https://www.iso27000.es/glosario.html

Evaluación de riesgos: proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo. Fuente: NTC-ISO/IEC 27001

Evitación del riesgo. Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación. Fuente: NTC-ISO/IEC 27005

Factores de Riesgo: Situaciones, manifestaciones o características medibles u observables asociadas a un proceso que generan la presencia de riesgo o tienden a aumentar la exposición, pueden ser internos o externos a la entidad. Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 4 - Riesgos de Gestión, Corrupción y Seguridad Digital Función Pública octubre 2018

Identificación del riesgo: Proceso para encontrar, enumerar y caracterizar los elementos de riesgo. Fuente: NTC-ISO/IEC 27005

Impacto. Cambio adverso en el nivel de los objetivos del negocio logrados. NTC-ISO 27005:2008. Tecnologías de la Información. Técnicas de seguridad. Gestión del riesgo en la seguridad de la información. Términos y definiciones. P. 2.

Incidente de seguridad de la información: un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información. Fuente: NTC-ISO/IEC 27001:2006

Integridad: Propiedad de la información relativa a su exactitud y completitud. Fuente: https://www.iso27000.es/glosario.html

Probabilidad: se entiende como la posibilidad de ocurrencia del riesgo. Esta puede ser medida con criterios de frecuencia o factibilidad. Fuente: Guía para la administración del riesgo y el

diseño de controles en entidades públicas – Versión 4 - Riesgos de Gestión, Corrupción y Seguridad Digital Función Pública octubre 2018

Reducción del riesgo: Acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo. Fuente NTC-ISO/IEC 27005

Retención del riesgo: Aceptación de la pérdida o ganancia proveniente de un riesgo particular Fuente: ISO 27005

Riesgo de corrupción: posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado. **Fuente:** Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 4 - Riesgos de Gestión, Corrupción y Seguridad Digital Función Pública octubre 2018

Riesgo de seguridad de la información: Posibilidad de que una amenaza concreta que pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información. Seguridad de la información: preservación de la confidencialidad, integridad, y disponibilidad de la información. Fuente (NTC-ISO/IEC 27005).

Riesgo de seguridad digital: combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas. Fuente: (DAFP 2018)

Riesgo Inherente: Es el nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles. Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 4 - Riesgos de Gestión, Corrupción y Seguridad Digital Función Pública octubre 2018

Riesgo Residual: Nivel de riesgo remanente como resultado de la aplicación de medidas de seguridad sobre el activo. **Fuente** Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 4 - Riesgos de Gestión, Corrupción y Seguridad Digital Función Pública octubre 2018

Riesgo: En el contexto de los sistemas de gestión de seguridad de la información, los riesgos de seguridad de la información pueden expresarse como un efecto de incertidumbre sobre los objetivos de seguridad de la información. El riesgo de seguridad de la información está asociado con el potencial de que las amenazas exploten las vulnerabilidades de un activo de información o grupo de activos de información y, por lo tanto, causen daños a una organización. Fuente: https://www.iso27000.es/glosario.html

Seguridad de la Información: preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad (Accountability), no repudio y fiabilidad: Fuente: NTC-ISO/IEC 27001

Sistema de Gestión de Seguridad de la información SGSI: parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información. fuente: NTC-ISO/IEC 27001

Tratamiento del Riesgo: Proceso para modificar el riesgo" Fuente: https://www.iso27000.es/glosario.html

Valoración del Riesgo: Proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.

Vulnerabilidad: debilidad de un activo o control que puede ser explotada por una o más amenazas. Fuente: https://www.iso27000.es/glosario.html

4. MARCO LEGAL

I. Teniendo en cuenta lo dispuesto en el Decreto 612 de 2018 respecto a la integración de planes institucionales y estratégicos al plan de acción, el presente documento desarrolla la siguiente actividad descrita en el Plan de Acción 2019: “Adoptar las guías del sistema de gestión de seguridad de información - SGSI del modelo de seguridad y privacidad de la información - MSPI del Min Tic en la UNP”, del cual se presentará el producto “Documento informe de seguimiento de implementación del sistema de gestión de seguridad de la información.”.
II. Decreto 1078 de 2015 - Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
III. CONPES 3854 de 2016 - Política Nacional de Seguridad Digital
IV. NTC / ISO 27001:2013 - Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI).
V. NTC/ISO 31000:2009 - Gestión del Riesgo. Principios y directrices
VI. Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 4 - Riesgos de Gestión, Corrupción y Seguridad Digital Función Pública octubre 2018
VII. Modelo de Seguridad y Privacidad de la Información V.3.0.2 – MPSI de la Estrategia de Gobierno en Línea – GEL hoy Gobierno Digital.
VIII. Norma Técnica Colombiana NTC-ISO/IEC 27001 Sistemas de Gestión de la Seguridad de la Información.
IX. Norma Técnica Colombiana NTC-ISO/IEC 27002 Tecnología de la Información. Técnica de Seguridad. Código de Práctica para Controles de Seguridad de la Información.
X. Norma Técnica Colombiana NTC-ISO/IEC 27005 Tecnología de la Información. Técnica de Seguridad. Gestión del Riesgo en la Seguridad de la Información.
XI. Norma Técnica Colombiana NTC-ISO/IEC 9001 Sistema de Gestión de a Calidad.
XII. Normas Internacionales ISO 9001-ISO 27001-ISO 14001-ISO 45001

5. CONDICIONES GENERALES

El presente documento está enmarcado en las pautas gobierno nacional la Política Nacional de Seguridad Digital y las directrices de manejo de riesgos establecidas por la entidad y busca determinar las acciones y mejores prácticas para tratar los posibles riesgos de seguridad y el manejo de la privacidad de información.

6. CONTENIDO

6.1 Estrategias

La Unidad Nacional de Protección – UNP, a través de la adopción e implementación del Modelo de Seguridad y Privacidad de la Información, enmarcado en el Sistema de Gestión de Seguridad de la información - SGSI, tiene como objeto proteger, preservar y administrar la confidencialidad, integridad y disponibilidad de la información, mediante una gestión integral de riesgos y la implementación de controles físicos y digitales reduciendo la probabilidad de ocurrencia de incidentes y dando cumplimiento a los requisitos legales y reglamentarios, orientados a la mejora continua y al alto desempeño del Sistema de Gestión de Seguridad de la Información, propendiendo así por el acceso, uso efectivo y apropiación masiva de las Tecnologías de la Información y las Comunicaciones- TIC.

Para lograr el cumplimiento del Plan se definen las siguientes estrategias:

1. Compromiso de la alta gerencia para promover, apoyar y financiar la realización de los proyectos asociados a gestionar los riesgos de seguridad de la información.
2. Integración de los riesgos de seguridad de la información al marco de gestión de riesgos de la UNP por parte de la Oficina Asesora de Planeación e Información.
3. Gestionar los riesgos de seguridad y privacidad de la información, de manera integral.
4. Mitigar los impactos y reducir la ocurrencia de posibles incidentes de Seguridad y Privacidad de la Información, de forma efectiva, eficaz y eficiente.
5. Adopción de la cultura de seguridad de la información y compromiso de todos los servidores públicos / Contratista y grupos de interés de la UNP frente los riesgos de seguridad de la información y su tratamiento.

6.2 Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

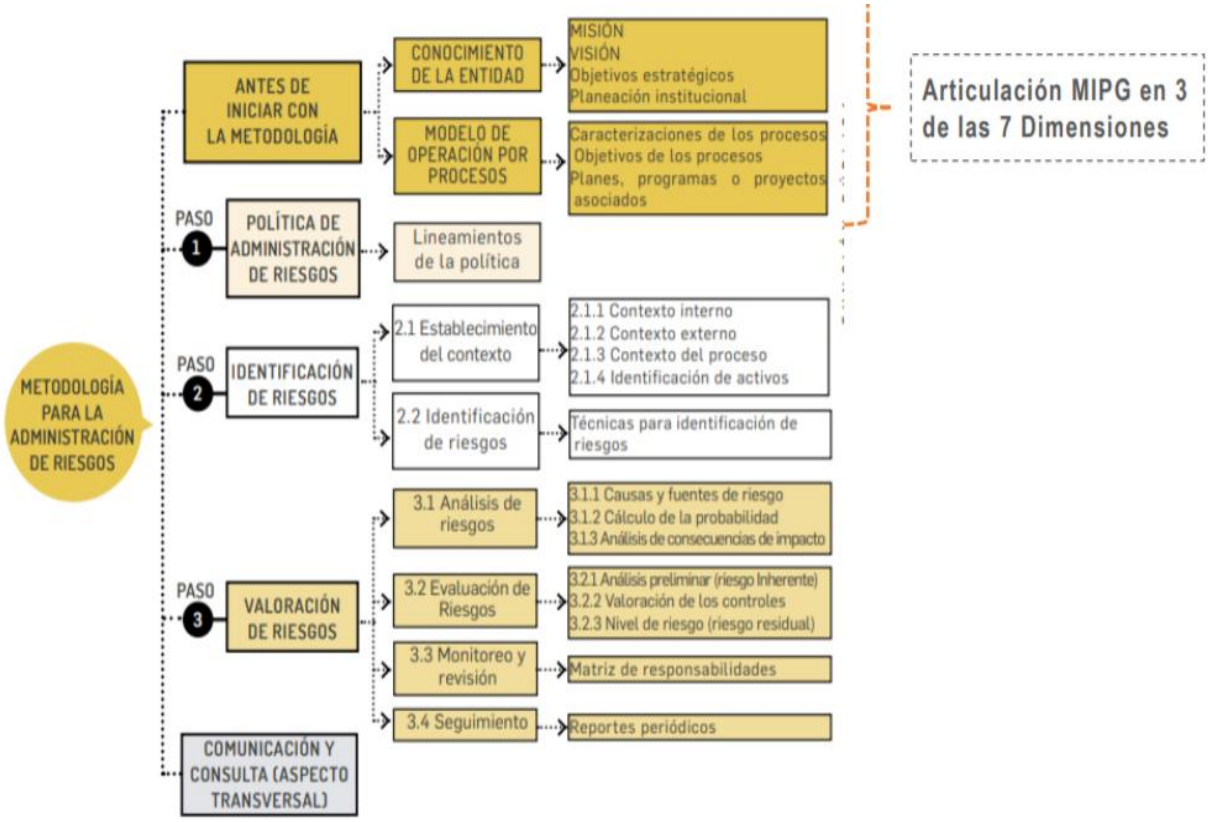
6.2.1 Etapas para la Gestión del Riesgo

De acuerdo con la Guía de Gestión de Riesgos del DAFP – Departamento Administrativo de la Función Pública, las etapas generales para la gestión de riesgos adoptados por la UNP contemplan el compromiso de la dirección de la Entidad, el equipo interdisciplinario encargado de la administración del modelo de gestión de riesgos y las capacitaciones de la metodología, lo cual está a cargo de la Oficina Asesora de Planeación e Información.

En lo que respecta a la seguridad de la información, se integrara a la gestión de riesgos adoptada por la UNP, la norma técnica NTC-ISO 27005:2009 Gestión de Riesgos en la Seguridad de la Información. Esta norma brinda soporte a los conceptos generales que se especifican en la norma NTC-ISO 27001:2013 y está diseñada para facilitar la implementación satisfactoria de la seguridad de la información con base en la gestión de Riesgos.

La guía Metodológica para la Administración del Riesgo del Departamento Administrativo de la función Pública es la carta de navegabilidad para la administración del Riesgo en las Entidades Publica, la cual actúa en concordancia con el componente de Administración del Riesgo establecido en el Manual Estándar de control Interno para el Estado Colombiano en la Identificación, Valoración, análisis y Seguimiento y Monitoreo de los mismo en una entidad.

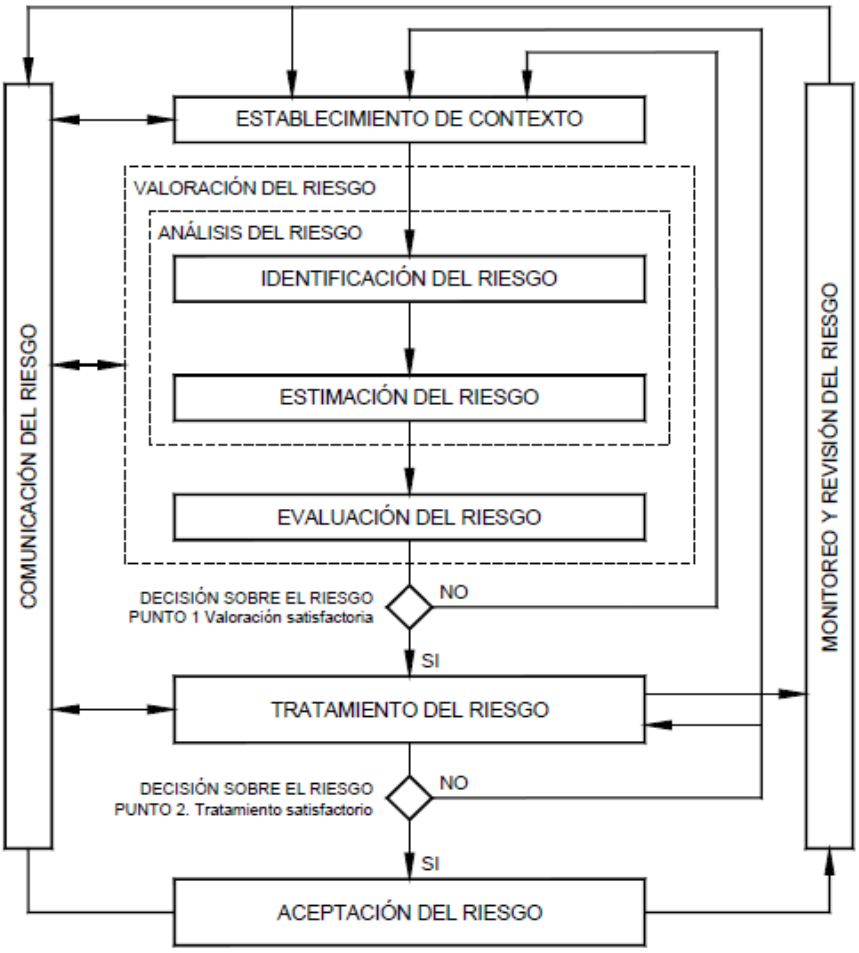
Ilustración 1 Metodología para la Administración de Riesgos



Fuente: *DAFP (2020)*

A continuación, se ilustra el proceso para la administración del riesgo en seguridad de la información.

Ilustración 2 Proceso de gestión del riesgo en la seguridad de la información



***Fuente**: Tomado de la NTC-ISO/IEC 27005*

6.2.2 Visión general para la Administración del Riesgo.

En el marco de la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI, se establecer una serie de actividades relacionadas con la gestión del riesgo, las cuales se presentan a continuación.

ETAPAS DEL MSPI	PROCESO DE GESTION DEL RIESGO EN LA SEGURIDADDE LA INFORMACION
Planear	Establecer Contexto Valoración del Riesgo Planificación del Tratamiento del Riesgo Aceptación del Riesgo
Implementar	Implementación del Plan de Tratamiento de Riesgo
Gestionar	Monitoreo y Revisión Continuo de los Riesgos
Mejora Continua	Mantener y Mejorar el Proceso de Gestión del Riesgo en la Seguridad de la Información.

Fuente: *Tomado de la Guía 7 – Gestión de Riesgos -MPSI - Mintic*

6.2.3 Identificación de Riesgos

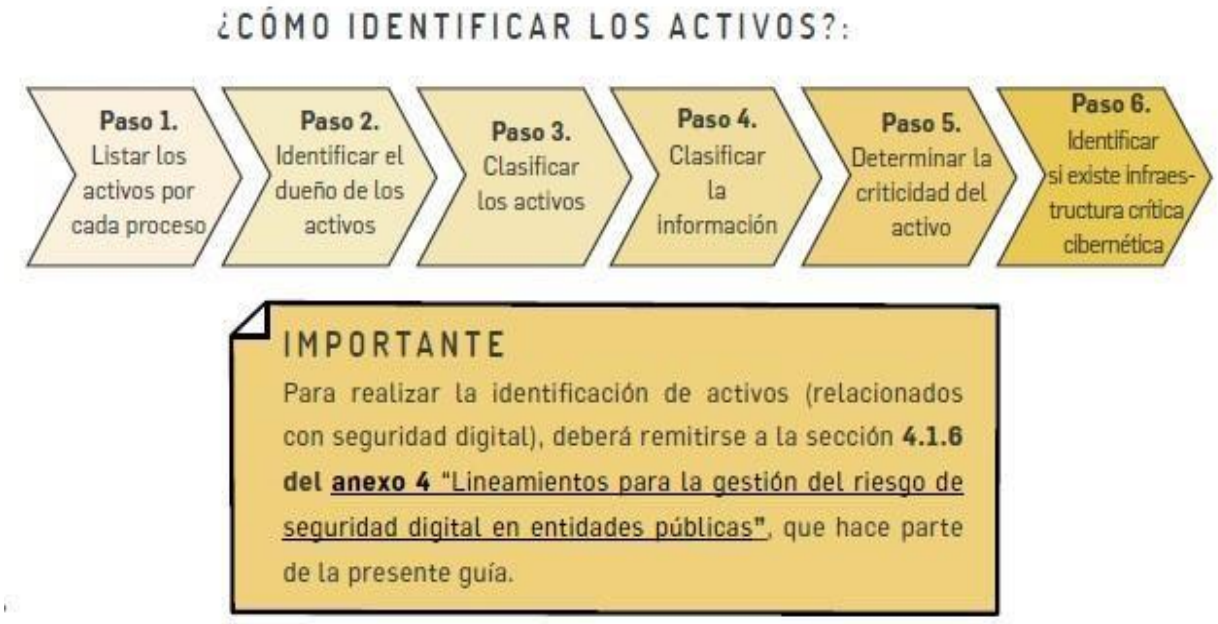
De acuerdo con DAFP[1] esta etapa tiene como objetivo identificar los riesgos que estén o no bajo el control de la organización, teniendo en cuenta el contexto estratégico en el que opera la entidad, la caracterización de cada proceso que contempla su objetivo y alcance, y el análisis frente a los factores internos y externos que pueden generar riesgos que afecten el cumplimiento de los objetivos

Es aquí donde se identifican los factores internos y externos que se han de tener en consideración para la administración del riesgo (NTC ISO31000, Numeral 2.9). Adicionalmente es requisito conocer los activos de cada proceso y realizar los análisis correspondientes frente los posibles riesgos. Amenazas y vulnerabilidades que los puedan afectar.

[1] Gestión del Riesgo (Modificaciones - Guía para la administración del riesgo y el diseño de controles en entidades públicas (DAFP 2020)

CONTEXTO EXTERNO	POLÍTICOS: cambios de gobierno, legislación, políticas públicas, regulación.
	ECONÓMICOS Y FINANCIEROS: disponibilidad de capital, liquidez, mercados financieros, desempleo, competencia.
	SOCIALES Y CULTURALES: demografía, responsabilidad social, orden público.
	TECNOLÓGICOS: avances en tecnología, acceso a sistemas de información externos, gobierno en línea.
	AMBIENTALES: emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible.
	LEGALES Y REGLAMENTARIOS: Normatividad externa (leyes, decretos, ordenanzas y acuerdos).
CONTEXTO INTERNO	FINANCIEROS: presupuesto de funcionamiento, recursos de inversión, infraestructura, capacidad instalada.
	PERSONAL: competencia del personal, disponibilidad del personal, seguridad y salud ocupacional.
	PROCESOS: capacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento.
	TECNOLOGÍA: integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento de sistemas de información.
	ESTRATÉGICOS: direccionamiento estratégico, planeación institucional, liderazgo, trabajo en equipo.
	COMUNICACIÓN INTERNA: canales utilizados y su efectividad, flujo de la información necesaria para el desarrollo de las operaciones.
CONTEXTO DEL PROCESO	DISEÑO DEL PROCESO: claridad en la descripción del alcance y objetivo del proceso.
	INTERACCIONES CON OTROS PROCESOS: relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios o clientes.
	TRANSVERSALIDAD: procesos que determinan lineamientos necesarios para el desarrollo de todos los procesos de la entidad.
	PROCEDIMIENTOS ASOCIADOS: pertinencia en los procedimientos que desarrollan los procesos.
	RESPONSABLES DEL PROCESO: grado de autoridad y responsabilidad de los funcionarios frente al proceso.
	COMUNICACIÓN ENTRE LOS PROCESOS: efectividad en los flujos de información determinados en la interacción de los procesos.
	ACTIVOS DE SEGURIDAD DIGITAL DEL PROCESO: información, aplicaciones, hardware entre otros, que se deben proteger para garantizar el funcionamiento interno de cada proceso, como de cara al ciudadano. Ver conceptos básicos relacionados con el riesgo páginas 8 y 9.

Fuente: *DAFP (2020)*



Fuente : Identificación de activos – DAFP:

Para el levantamiento de activos asociados a los procesos, nos apoyamos en la GDT-FT-20 MATRIZ DE INVENTARIO DE ACTIVOS DE INFORMACIÓN que es un instrumento que permite identificar los activos de información y su tránsito a través de ciclo de vida del documento, desde su creación hasta la disposición final.

En concordancia con la metodología de riesgos adoptada por la Entidad, se incorporan los riesgos cuya tipología corresponde a "Riesgos de Seguridad Digital" conforme lo indica la guía del DAFP.

Tabla 1: Tipo de Riesgo Digital

TIPO DE RIESGOS	DEFINICIÓN
Riesgo de seguridad digital	Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas. (DAFP 2018)

Fuente: (DAFP 2018)

Los activos de información de acuerdo con su nivel de importancia respecto a los criterios de Confidencialidad, Integridad y Disponibilidad se clasifican en cinco niveles (Anexo-01- Riesgos de Seguridad de la información - Hoja TRIADA).

En concordancia con lo anterior, los activos de información también deben valorados y clasificados de acuerdo con su clasificación y deben estar alineados con las disposiciones

legales vigentes. En la UNP existen diferentes tipos de información Altamente Confidencial (Reservada), Confidencial (Clasificada), Interna y pública, las cuales están alineados y homologados con los que define la Ley 1712 de transparencia y derecho de acceso a la información Pública. (Anexo-01- Riesgos de Seguridad de la información - Hoja VALORACIÓN).

Los criterios para definir la probabilidad y el impacto son los adoptados por la entidad y de acuerdo con la metodología de Gestión de Riesgos del DAFP. Estos criterios se encuentran incluidos en Anexo-01- Riesgos de Seguridad de la Información.

La identificación correcta de las amenazas y vulnerabilidades es un aspecto clave del SGSI - Sistema de seguridad de la información dentro del proceso de evaluación de riesgos, razón por la cual van de la mano y deben ser consideradas en su conjunto. En este orden de ideas, se deben tomar como referencia las Amenazas y vulnerabilidades definidas en la norma NTC-ISO 27005, las cuales se incluyen en el Anexo-01- Riesgos de Seguridad de la Información (Ver Hojas de Amenazas y Vulnerabilidades).

Una vez identificadas las variables que hacen parte de la gestión de riesgos, se procede a registrarlo y gestionarlos de acuerdo con la metodología adoptada por la UNP.

Para la gestión de los riesgos, se tienen como documentos de referencias la norma NTC-ISO 27005, la guía de Gestión de Riesgos de DAFP y una matriz en Excel denominada Anexo-01- Riesgos de Seguridad de la Información la cual se establece como herramientas de consulta la diligenciar el instrumento de riesgos definido por la entidad.

6.3 Acciones

Las acciones abajo listadas son la requeridas para dar cumplimiento a los objetivos propuestos para el plan de tratamiento de riesgos de seguridad y privacidad de la información de acuerdo con el estado actual de la Entidad, definiendo metas, productos, responsables y cronograma de ejecución:

Tabla 2: Cronograma Plan de Tratamiento de Riegos de seguridad y privacidad de la Información

Cronograma de Actividades					
Ámbito	**Actividad**	**Tareas**	**Responsable**	**Fecha de Cumplimiento**	
Gestión de Riesgos	Actualización de lineamientos de riesgos	Actualizar política y metodología de gestión de riesgos	OAPI, CIO – CISO	I Trimestre 2022	I Trimestre 2022

Cronograma de Actividades					
Ámbito	**Actividad**	**Tareas**	**Responsable**	**Fecha de Cumplimiento**	
	Activos de información y escenarios de riesgos	Consolidación de los activos de información y elaboración de los escenarios de riesgos	OAPI, CIO – CISO	I Trimestre 2022	II Trimestre 2022
	Sensibilización sobre la metodología	Socialización Guía y Herramienta - Gestión de Riesgos de Seguridad y privacidad de la Información, Seguridad Digital y Continuidad de la Operación	OAPI, CIO – CISO	II Trimestre 2022	II Trimestre 2022
	Ejecución de metodología de identificación de riesgos de seguridad digital	Diligenciamiento del MIR (Instrumento del Mapa Integral de Riesgos): Identificación, Análisis y Evaluación de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación. Aceptación, aprobación Riesgos identificados y planes de tratamiento	OAPI, CIO – CISO, TODOS LOS PROCESOS	II Trimestre 2022	II Trimestre 2022
	Publicación	Publicación Matriz de riesgos	OAPI, CIO – CISO, TODOS LOS PROCESOS	III Trimestre 2022	III Trimestre 2022

Cronograma de Actividades					
Ámbito	**Actividad**	**Tareas**	**Responsable**	**Fecha de Cumplimiento**	
	Seguimiento Fase de Tratamiento	Seguimiento Estado planes de tratamiento de riesgos identificados y verificación de evidencias	OAPI, CIO – CISO, TODOS LOS PROCESOS	III Trimestre 2022	IV Trimestre 2022
	Evaluación de riesgos residuales	Evaluación de riesgos residuales	OAPI, CIO – CISO, TODOS LOS PROCESOS	III Trimestre 2022	IV Trimestre 2022
	Mejoramiento	Identificación de oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de riesgos residuales	OAPI, CIO – CISO, TODOS LOS PROCESOS	III Trimestre 2022	IV Trimestre 2022

Fuente: Elaboración Propia

7. INDICADOR

El indicador del plan es el seguimiento al cumplimiento de las actividades, este seguimiento se hace de manera trimestral.

Indicador = Actividades ejecutadas trimestral / actividades programadas trimestral * 100%

La meta será del 85% de cumplimiento

8. DOCUMENTOS RELACIONADOS

- Acta de Reunión (SGE-FT-02)
- Listado de Asistencia. (SGE -FT-03)
- Matriz Inventario Activos de Información (GDT-FT-20)

9. CONTROL DE CAMBIOS

VERSIÓN INICIAL	DESCRIPCIÓN DE LA CREACIÓN O CAMBIO DEL DOCUMENTO	FECHA	VERSIÓN FINAL
00	Creación del Plan Seguridad y Privacidad de la Información	31/01/2019	01
01	Actualización del Plan de Seguridad y Privacidad de la Información para la vigencia 2020	31/01/2020	02
02	Actualización del Plan de Tratamiento de riesgos de Seguridad y Privacidad de la Información para la vigencia 2021	20/01/2021	03
03	Actualización del Plan de Tratamiento de riesgos de Seguridad y Privacidad de la Información para la vigencia 2022	20/01/2022	04

10. CRÉDITOS

FIRMAS DE ELABORACIÓN, REVISIÓN Y APROBACIÓN DEL DOCUMENTO	
Elaboró Nombre: Maria Berenice Parra Parraga Cargo y/o Vinculación/dependencia: Enlace MIPG-SIG. Contratista - Grupo de Gestión de las Tecnologías de Información / Oficina Asesora de Planeación e Información	
Elaboró Nombre: Franz Edwar Rojas Montañez Cargo y/o Vinculación/dependencia: Contratista-CIO-Grupo de Gestión de las Tecnologías de Información / Oficina Asesora de Planeación e Información	
Revisó: Nombre: Samir Manuel Berrio Scaff Cargo: Jefe de la Oficina Asesora de Planeación e Información	
Aprobó: Nombre: Alfonso Campo Martinez Cargo: Director General	
FIRMA DE OFICIALIZACIÓN DEL DOCUMENTO- SISTEMA INTEGRADO DE GESTIÓN MIPG -SIG	
Oficializó: Nombre: Samir Manuel Berrio Scaff Cargo: Jefe de la Oficina Asesora de Planeación e Información	