TABLA DE CONTENIDO

INTRODUCCIÓN.

En la actualidad, la gestión de la seguridad y privacidad de la información es un elemento crítico para el éxito y la sostenibilidad de cualquier organización. Este plan de tratamiento de riesgos ha sido diseñado con el objetivo de abordar de manera efectiva los riesgos asociados a la seguridad y privacidad de la información, siguiendo las directrices establecidas en el Modelo de Seguridad y Privacidad de la Información (MSPI) y la política de gestión de riesgos de nuestra organización.

La adopción de este plan nos permitirá identificar, evaluar y gestionar los riesgos de manera proactiva, asegurando así la integridad, confidencialidad y disponibilidad de nuestra información crítica. Es un enfoque integral que no solo abarca los aspectos tecnológicos, sino también los procesos organizativos y el factor humano.

A continuación se ilustra en que acciones del MPSI se tendrá interacción directa con el Modelo de Gestión de Riesgos de Seguridad de la información:

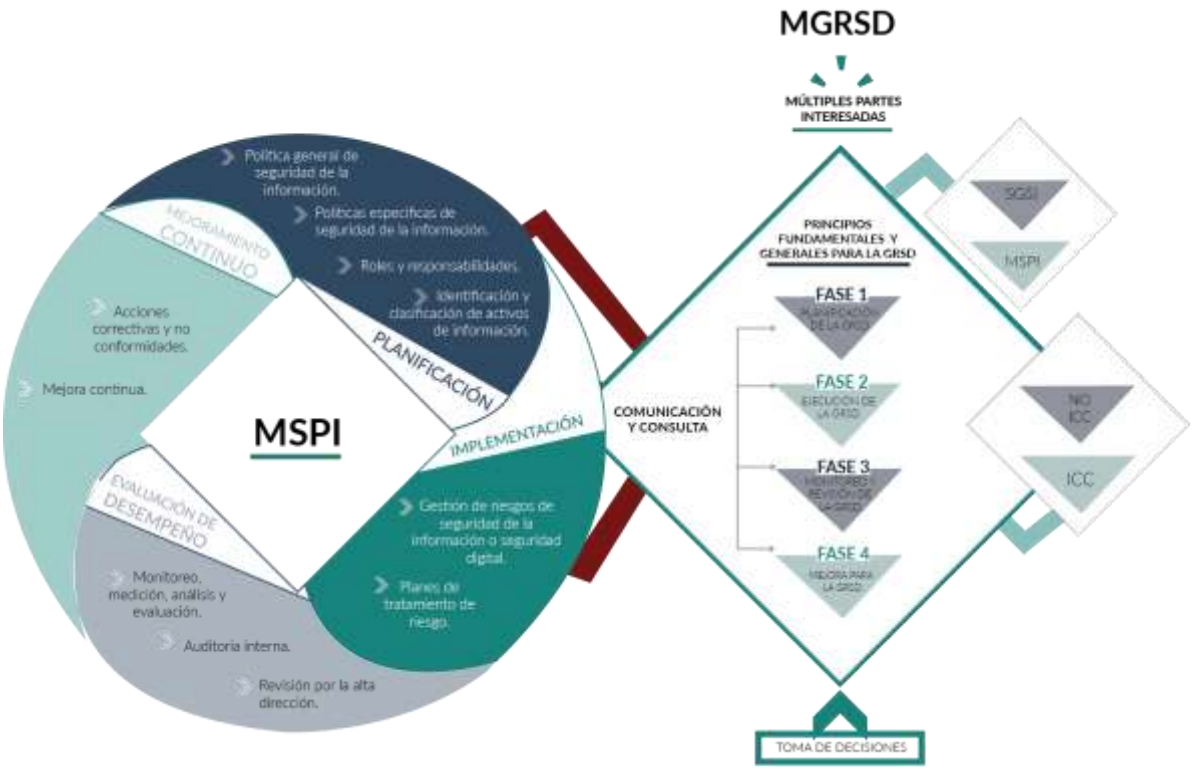

Ilustración 1.Fuente: MinTic.

1. OBJETIVO

Definir y aplicar los lineamientos para la gestión de riesgos de seguridad de la información y seguridad digital que permita preservar la integridad, confidencialidad y disponibilidad de la información institucional.

2. ALCANCE

Este documento es aplicable para todas las oficinas, gerencias y subgerencias pertenecientes a la Entidad, por tal motivo en su ciclo de ejecución se involucran todos los procesos.

3. NORMATIVIDAD ASOCIADA

Normatividad	Entidad	Descripción
Acuerdo 002 de 2023	Comisión Distrital de Transformación Digital	Por la cual se adopta el lineamiento para el desarrollo de evaluaciones de impacto a la privacidad.
Resolución 460 de 2022	Ministerio de Tecnologías de la información y las comunicaciones - MINTIC	Por la cual se expide el Plan Nacional de Infraestructura de Datos y su hoja de ruta en el desarrollo de la Política de Gobierno digital, y se dictan los lineamientos generales para su implementación.
Resolución 500 de 2021	Ministerio de Tecnologías de la información y las comunicaciones - MINTIC	Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital.
Decreto 620 de 2020	Ministerio de Tecnologías de la información y las comunicaciones - MINTIC	Establece los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
Resolución 1519 de 2020.	Ministerio de Tecnologías de la información y las comunicaciones - MINTIC	Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos
Resolución 2893 de 2020	Ministerio de Tecnologías de la información y las comunicaciones - MINTIC	Por la cual se expiden los lineamientos para estandarizar ventanillas únicas, portales específicos de programas transversales, sedes electrónicas, trámites, OPA, y consultas de acceso a información pública, así como en relación con la integración al Portal Único del Estado colombiano, y se dictan otras disposiciones

Normatividad	Entidad	Descripción
Directiva 002 de 2020	Presidencia de la Republica	Medidas para atender la contingencia generada por el covid-19, a partir uso de las tecnologías la información y las telecomunicaciones - TIC
CONPES 3995 de 2020.	Consejo Nacional de Política Económica y Social República de Colombia Departamento Nacional de Planeación	Política Nacional de Confianza y Seguridad Digital.
Decreto 612 de 2018	Presidencia de la Republica	Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado
CONPES 3854 de 2016.	Consejo Nacional de Política Económica y Social República de Colombia Departamento Nacional de Planeación	Política de Seguridad Digital del Estado Colombiano
Decreto 1078 de 2015	Ministerio de Tecnologías de la información y las comunicaciones - MINTIC	Se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
Ley 1712 de 2014	Presidencia de la Republica	Ley de transparencia y el derecho a la información pública nacional
Ley 1581 de 2012	Congreso de Colombia	Se dictan disposiciones generales para la protección de datos personales
CONPES 3701 de 2011.	Consejo Nacional de Política Económica y Social República de Colombia Departamento Nacional de Planeación	Lineamientos de Política para Ciberseguridad y Ciberdefensa.

4. DESARROLLO

Este documento detalla la metodología adoptada para la gestión de riesgos de seguridad de la información en nuestra entidad. Esta metodología se fundamenta en dos guías esenciales: la "Guía para la administración del riesgo y el diseño de controles en entidades públicas" del Departamento Administrativo de la Función Pública (DAFP), en su versión más reciente de noviembre de 2022, y la "Guía de orientación para la gestión de riesgos de seguridad digital" del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

Las fases metodológicas incorporadas en nuestro plan de gestión de riesgos están estrechamente alineadas con la Política de Administración de Riesgos y la Guía Administración de Riesgos de la Agencia Distrital para la Educación Superior, la Ciencia y la Tecnología “Atenea”. Esta alineación abarca desde la integración estratégica en la identificación de los riesgos de seguridad digital, hasta la implementación y seguimiento efectivo de las acciones para la gestión de riesgos institucionales.

El enfoque adoptado asegura una gestión de riesgos coherente y eficaz, cumpliendo con los estándares y recomendaciones establecidos tanto por el DAFP como por el MinTIC. Así, garantizamos que los riesgos de seguridad de la información sean identificados, evaluados y gestionados de manera integral, con un enfoque que promueve la mejora continua y la adaptación a los cambiantes entornos tecnológicos y de seguridad digital.

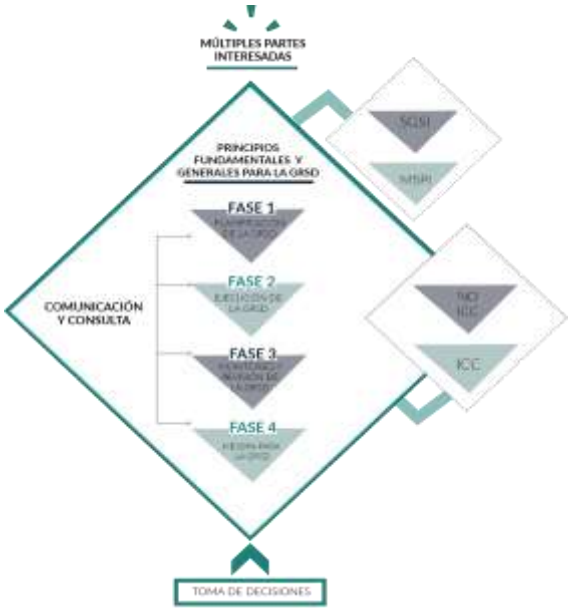

Ilustración 2.Marco conceptual de gestión del riesgo de seguridad digital Fuente: MinTic.

Identificación

Esta etapa implica el reconocimiento y la documentación de los riesgos potenciales que pueden impactar la seguridad de la información en la entidad. Siguiendo las directrices de las guías mencionadas, se debe realizar un mapeo detallado de los activos de información con criticidad alta, identificar las amenazas y vulnerabilidades asociadas a estos activos, y considerar tanto factores internos como externos que puedan influir en la seguridad de la información

Evaluación de riesgos

Una vez identificados los riesgos, se procede a su evaluación, empleando un enfoque tanto cualitativo como cuantitativo. Esto implica determinar la probabilidad de ocurrencia de cada riesgo y su impacto potencial, en caso de materializarse.

La evaluación de riesgos se realiza considerando el contexto de la entidad y los criterios de valoración de riesgos establecidos, lo que permite priorizar los riesgos y tomar decisiones informadas sobre su tratamiento

Mitigación y tratamiento de riesgos

Basándose en la evaluación realizada, se desarrollan e implementan estrategias para manejar los riesgos. Esto puede incluir la reducción del riesgo mediante la implementación de controles, la transferencia del riesgo a través de seguros o contratos, la aceptación del riesgo cuando su impacto es tolerable, o la evitación del riesgo.

Las estrategias de tratamiento deben ser alineadas con los objetivos de la entidad y la eficiencia en el uso de los recursos.

Monitoreo y revisión continua

La gestión de riesgos es un proceso dinámico, por lo que requiere un monitoreo y revisión constantes. Esto asegura que las estrategias de tratamiento de riesgos sigan siendo efectivas y pertinentes frente a cambios en el entorno interno o externo de la entidad.

Esta fase incluye la supervisión de los controles implementados, la revisión periódica del contexto de riesgo y la actualización de la evaluación de riesgos, así como la documentación y comunicación de los hallazgos pertinentes a las partes interesadas.

Estrategia de Implementación

Para el año 2024, se ejecutarán las siguientes actividades de acuerdo con el ciclo de gestión de los riesgos.

Actividades	Entregable	Responsable	Finalización
Declaración de aplicabilidad	Matriz con los criterios definidos.	Subgerencia TIC	30-nov-2024
Plan de tratamiento de riesgos de seguridad de la información	Plan aprobado y publicado en la página web institucional	Subgerencia TIC	09-feb-2024
Elaborar y remitir memorando de solicitud para realizar actualización de los riegos de seguridad.	Memorando radicado	Subgerencia TIC	30-03-2024
Identificar, analizar y evaluar los riesgos de aquellos	Matriz de riesgos	Lideres de área	30-04-2024

Actividades	Entregable	Responsable	Finalización
activos de información con criticidad alta			
Establecer controles y planes de tratamiento sobre los riesgos	Matriz de riesgos	Lideres de área	30-04-2024
Aceptar y aprobar los riesgos identificados por cada uno de los lideres de área	Memorando radicado	Lideres de área	30-04-2024
Realizar seguimiento a los planes de manejo de riesgo de seguridad de la información establecidos por cada uno de los lideres de las áreas, con sus respectivas evidencias.	Matriz de riesgos	Lideres de área	15-dic-2024

5. CONTROL DE CAMBIOS

Fecha (De la Versión del documento que se está actualizando)	**Versión** (Relacionar la última versión y código del documento que se está actualizando)	**Descripción del Cambio**
12/01/2024	1	Creación del documento para codificación

VALIDACIÓN	NOMBRE	CARGO	FECHA
Elaboró	Maria Alejandra Suarez Rojas	Contratista – Subgerencia Tecnologías de la información y las comunicaciones	12 de enero del 2024
Revisó	Lira Jazmin Pineda Moreno	Subgerente Tecnologías de la información y las comunicaciones	15 de enero del 2024
Aprobó	Comité Institucional de Gestión y Desempeño	Comité Institucional de Gestión y Desempeño	