PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION: 2025

HISTORIAL DE REVISIÓNES DEL PLAN			
FECHA	**VERSIÓN**	**DESCRIPCIÓN**	**AUTOR**
18/12/2024	1.0	Versión inicial	Álvaro Cárdenas

1. VISIÓN GENERAL

La seguridad y privacidad de la Información como habilitador transversal de la Política de Gobierno Digital se desarrolla a través de la implementación del Modelo de Seguridad y Privacidad de la Información -MSPI, alineado con la NTC/IEC ISO 27001:2022, en el desarrollo del modelo se ha identificado la necesidad de incorporar nuevas amenazas presentes no solamente en el mundo físico sino también en el entorno digital, para comprender los riesgos más significativos y gestionar eficazmente la seguridad de la información.

Esto implica la identificación y valoración de los activos de información que se producen y utilizan en todos los procesos, trámites, servicios, sistemas de información e infraestructura del Ministerio de Relaciones Exteriores y su fondo rotatorio, con el fin de identificar el nivel de criticidad de los activos de información, y realizar la identificación, análisis y valoración de los riesgos que podrían afectar a estos activos y en consecuencia el cumplimiento adecuado, efectivo y óptimo de los objetivos institucionales.

El análisis de riesgos nos permite entender de una manera efectiva y eficiente los riesgos de pérdida de confidencialidad, integridad y disponibilidad sobre cada uno de los activos críticos del Ministerio y en consecuencia la aplicación de las opciones apropiadas de tratamiento de riesgos de seguridad de la información a través de la implementación de los controles que permitan mitigar su impacto y probabilidad y mantenerlos controlados y monitoreados garantizando la Confidencialidad, integridad y disponibilidad de los Activos de información del Ministerio de relaciones exteriores y su fondo rotatorio.

El Sector de Relaciones Exteriores, en el desarrollo de su estrategia de TI, definió el siguiente objetivo, que se constituye en las directrices a seguir en el Plan Estratégico de Tecnologías de la Información de las entidades que lo conforman: *Desarrollar capacidades en el Sector de Relaciones Exteriores para garantizar la confidencialidad, integridad, disponibilidad y privacidad de los datos, a través de la implementación del proyecto "Implementación del Modelo de Seguridad de la Información para el Sistema de Gestión de Seguridad de la Información, de acuerdo con el estándar ISO/IEC 27001, versión 2022 "*

EL Ministerio de Relaciones Exteriores y su fondo Rotatorio definió para el periodo 2023-2026 el siguiente objetivo estratégico: *"Fortalecer integralmente las capacidades de gestión del Ministerio de Relaciones Exteriores y su Fondo Rotatorio para cumplir los objetivos y metas del Gobierno del Cambio. y* en el marco de este objetivo se define la estrategia Transformación digital para la generación de valor público y el mejoramiento del Ministerio de Relaciones Exteriores y su Fondo Rotatorio con la siguiente iniciativa orientada a Seguridad de la Información: "*Fortalecimiento integral del modelo de seguridad y privacidad de la información del Ministerio de Relaciones Exteriores y su Fondo Rotatorio".*

Adicionalmente, siguiendo los lineamientos de la Política de Gobierno Digital, reglamentada a través del Decreto 1078 de 2015 modificado por el Decreto 1008 de 2018, que en el artículo 2.2.9.1.1.3. Principios. Define la seguridad de la información como principio de la Política de Gobierno Digital, y de igual manera en el artículo 2.2.9.1.2.1 define la estructura de los Elementos de la Política de Gobierno Digital a través de componentes y habilitadores transversales los cuales son los elementos fundamentales de Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, los cuales permiten el desarrollo de los anteriores componentes y el logro de los propósitos de la Política de Gobierno Digital.

Teniendo en cuenta lo anterior y con lo establecido por el Artículo 1 del Decreto 612 del 2018 expedido por el Gobierno Nacional, la Política de Administración del Riesgo del Ministerio y las directrices dadas por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, se formula el presente Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2025, en donde se definen las acciones para gestionar los riesgos de seguridad de la información identificados, salvaguardando los principios de integridad, confidencialidad y disponibilidad de la información.

ARTICULACION ESTRATEGICA:

El Plan de Tratamiento de riesgos de Seguridad y privacidad de la información se integra al Plan de Acción Institucional 2025, a través de la siguiente articulación estratégica:

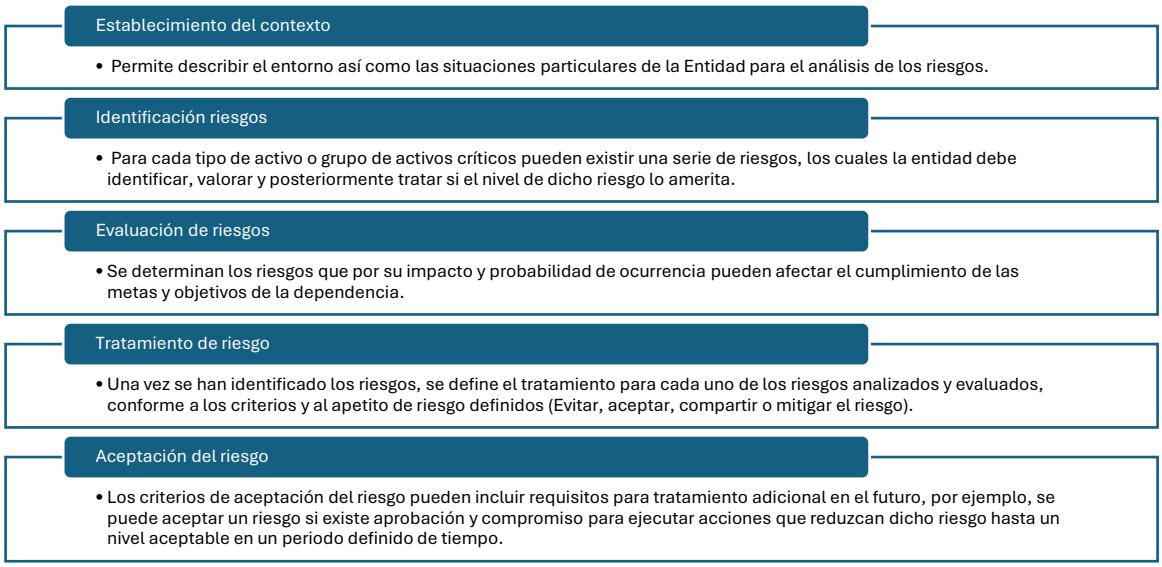
TRANSFORMACIÓN O COMPONENTE	**ODS RELACIONADO**	**PROCESO**	**DIMENSIÓN**	**POLÍTICA**
7. Posicionamiento global y regional de Colombia	16. Paz, justicia e instituciones sólidas	2. Direccionamiento Estratégico	4. Evaluación de Resultados	4.1. Seguimiento y evaluación del desempeño institucional
PLAN	**PROYECTO DE INVERSIÓN**	**OBJETIVO ESTRATÉGICO**	**ESTRATEGIA**	**INICIATIVA**

10. Plan Estratégico de Tecnologías de la Información y las Comunicaciones - PETI 11. **Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información** 12. Plan de Seguridad y Privacidad de la Información	2.Transformación digital del Ministerio de Relaciones Exteriores	3. Fortalecer integralmente las capacidades de gestión del Ministerio de Relaciones Exteriores y su Fondo Rotatorio para cumplir los objetivos y metas del Gobierno del Cambio.	1. Transformación digital para la generación de valor público y el mejoramiento del Ministerio de Relaciones Exteriores y su Fondo Rotatorio.	Fortalecimiento integral del modelo de seguridad y privacidad de la información del Ministerio de Relaciones Exteriores y su Fondo Rotatorio.

2. SITUACIÓN ACTUAL O DIAGNÓSTICO

La metodología para el tratamiento de los riesgos de seguridad y privacidad de la información derivados de los procesos y actividades de la entidad se encuentra integrada en la Política de Administración del Riesgos, "*En el Ministerio de Relaciones Exteriores y su Fondo Rotatorio declaramos nuestro compromiso con la adecuada gestión del riesgo que pueda afectar el cumplimiento de la Constitución, la Ley y demás normas vigentes, los objetivos estratégicos y de los procesos, la buena marcha de la gestión pública, la satisfacción de los usuarios, la seguridad y privacidad de la información, la conservación del ambiente, la seguridad y salud en el trabajo, y la administración transparente de los recursos públicos, mediante la definición e implementación del procedimiento de Administración del Riesgo, que para calificar el impacto de los riesgos, incluye los niveles de aceptación, tratamiento (mecanismos de prevención y mitigación), seguimiento y evaluación",* la cual busca identificar, valorar, planificar y adelantar el tratamiento oportuno y mantener los riesgos en niveles óptimos de control para así preparar al Ministerio ante una posible materialización y adelantar procesos de seguimiento, monitoreo, evaluación, o auditoría, según corresponda.

El proceso de identificación de riesgos de Seguridad de la información inicia con la ejecución de la guía IT-GS-005 Guía para la gestión y clasificación de activos de Información, a través de la cual se realiza la identificación, valoración y clasificación de los activos de información de cada uno de los procesos del Ministerio y continua con el desarrollo de las siguientes actividades, las cuales permiten la identificación de los riesgos de seguridad de la información, su valoración y el establecimiento de los controles necesarios para su mitigación:



La matriz de riesgos institucional se encuentra publicada en el portal web del Ministerio de relaciones exteriores y su fondo rotatorio en el siguiente enlace: https://www.cancilleria.gov.co/plan-anticorrupcion-y-atencion-al-ciudadano

Como resultado de la aplicación de la metodología actualmente se tienen identificados un total 233 riesgos de los cuales 7 riesgos corresponden a seguridad de la información, la valoración de los controles determinó un riesgo residual moderado para 3 riesgos y extremo para 4 riesgos los cuales requieren acciones de mitigación.

Así mismo es necesario continuar con la identificación de los riesgos para los demás procesos del Ministerio de relaciones exteriores y su fondo Rotatorio, esto teniendo en cuenta que a la fecha se cuenta con un total de 221 activos de información identificados con criticidad alta a los que es necesario realizar el proceso de identificación de riesgos y la gestión correspondiente del riesgo.

Por lo anteriormente expuesto y con el fin de dar cumplimiento a lineamientos institucionales, el Ministerio realiza el Plan de Tratamiento de Riesgos basado en los lineamientos para la Gestión del Riesgos de Seguridad Digital en Entidades Públicas, Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC) y el DE-PT-028 Procedimiento de Administración de Riesgo, establece el presenta plan de tratamiento de riesgos de seguridad de la información.

3. OBJETIVOS

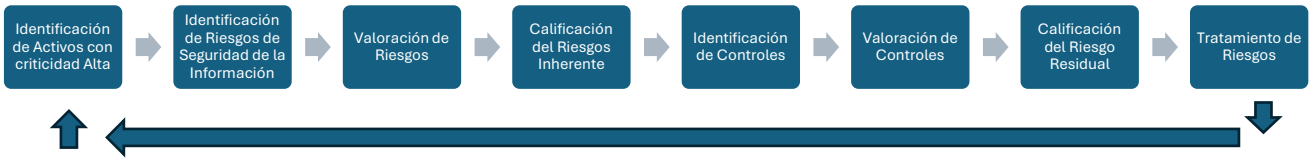
Establecer las actividades y acciones necesarias para mantener la integridad, confidencialidad, disponibilidad y privacidad de la información a través de la gestión adecuada de los riesgos, definiendo y aplicando lineamientos y controles para el tratamiento y mitigación de los riesgos de seguridad y privacidad de la información.

4. ALCANCE

El presente plan comprende las actividades a realizar para la identificación, valoración y gestión de los riesgos de seguridad de la información sobre los activos de información y la definición del conjunto de operaciones o tareas propias a realizar por los lideres de procesos durante la vigencia 2025, para la mitigación de riesgos no aceptables que estén o sean identificados.

5. ESTRATEGIAS, HERRAMIENTAS Y ACTIVIDADES

Con el fin de continuar con al proceso de identificación de riesgos de seguridad de la información, se establece la siguiente estrategia de operación:



5.1. Identificación de activos con Criticidad Alta: De acuerdo con el resultado de la matriz de activos de información cada uno de los procesos debe realizar la identificación de los activos cuya valoración de criticidad del activo sea alta, hacer el análisis de los activos teniendo en cuenta la calificación en términos de confidencialidad, integridad y disponibilidad.

5.2. Identificación y valoración de riesgos de seguridad de la información: En esta etapa se realizan actividades tendientes a apoyar a los procesos a través de mesas de trabajo en la identificación de los riesgos de seguridad de la información sobre los activos valorados con criticidad ALTA, y se realizan las siguientes actividades:

5.1.1. PROGRAMACIÓN Y AGENDAMIENTO DE MESAS DE TRABAJO: Se realiza la programación de reuniones con los líderes de activos asignados por cada uno de los procesos.

5.1.2. ENTREVISTA CON LOS LÍDERES DE ACTIVOS: Se entrevista a cada líder asignado, se realiza la revisión de los activos cuya criticidad sea alta y se validan los criterios (confidencialidad, integridad y disponibilidad) cuya calificación haya sido alta, con el fin de identificar que riesgos podría afectar ese cada criterio valorado como alto.

5.1.3. IDENTIFICACIÓN Y CALIFICACIÓN DE RIESGOS INHERENTES: En esta fase es clave contar con información coherente y actualizada de las actividades que se llevan a cabo en los diferentes procesos, los

resultados esperados de las mismas y orígenes de riesgos, identificando el nivel de riesgo inherente de acuerdo con la metodología establecida en el procedimiento DE-PT-028 Administración de Riesgos.

5.3. IDENTIFICACION DE CONTROLES: Con el fin de fortalecer el enfoque preventivo, correctivo y detectivo se determinan los controles actuales que permiten gestionar de manera efectiva los riesgos teniendo en cuenta y sin limitarse al anexo A. de la norma ISO 27001:2022, identificando el responsable, la frecuencia de ejecución del control, el propósito, procedimiento como se aplica el control, las observaciones y desviaciones y la evidencia, en consonancia con los lineamientos institucionales.

5.4. VALORACIÓN DE CONTROLES: En esta etapa de acuerdo con los criterios establecidos en la metodología se hace una proyección de la eficacia de los controles para calcular el riesgo residual, esto permite determinar si el control responde de manera efectiva al tratamiento del riesgo.

5.5. CALIFICACION DEL RIESGO RESIDUAL: En esta fase se ubican los riesgos en el mapa de calor para visualizar su comportamiento a medida que se van aplicando los controles y se determina el riesgo final que queda después de la aplicación de los controles, con base en los resultados obtenidos en la determinación real de riesgos, es necesario tomar decisiones aplicando el apetito de riesgos definido por el Ministerio. Si el riesgo se ubica en una zona No Aceptable (Altos y Extremos), cada líder de proceso es responsable de los riesgos identificados y con el apoyo del Oficial de Seguridad de la Información, define e implementan los controles que permitan disminuir el impacto y la probabilidad para llevar el riesgo a un nivel Aceptable.

5.6. TRATAMIENTO DE RIESGOS:

A continuación, se visualiza el resultado del proceso de gestión de riesgos de seguridad de la información realizado al cierre de la vigencia 2024, se define la estrategia de tratamiento, consistente en asumir los riesgos Bajos y Moderados a través del monitoreo, y gestionar los riesgos Altos y Extremos a través de la implementación de controles por parte de los responsables del cada uno de los Procesos.

Para la gestión y tratamiento de los 7 riesgos encontrados en la vigencia año 2024, como estrategia de mitigación, se definirán y aplicarán actividades asociadas a los siguientes controles de la norma ISO 27001: 2022 Anexo A. 94 controles de seguridad.

Control ISO	Nombre del control	Tipo de Control
A.5.3	Segregación de funciones	Preventivo
A.5.8	Seguridad de la información en la gestión de proyectos	Preventivo
A.5.10	Seguimiento, revisión y gestión de cambios de servicios de proveedores	Preventivo
A.5.15	Control de acceso	Preventivo

Control ISO	Nombre del control	Tipo de Control
A.5.18	Derechos de acceso	Preventivo
A.5.19	Seguridad de la información en las relaciones con los proveedores	Preventivo
A.5.20	Abordar la seguridad de la información en los acuerdos con proveedores	Preventivo
A.5.21	Gestión de la seguridad de la información en la cadena de suministro de las TIC	Preventivo
A.5.22	Seguimiento, revisión y gestión de cambios de servicios de proveedores	Preventivo
A.5.23	Seguridad de la información para el uso de servicios en la nube	Preventivo
A.5.24	Planificación y preparación de la gestión de incidentes de seguridad de la información	correctivo
A.5.26	Respuesta a incidentes de seguridad de la información	correctivo
A.5.29	Seguridad de la información durante la interrupción	correctivo
A.5.30	Preparación de las TIC para la continuidad del negocio	correctivo
A.5.33	Protección de registros	Preventivo
A.8.1	Dispositivos de punto final de usuario	Preventivo
A.8.2	Derechos de acceso privilegiado	Preventivo
A.8.3	Restricción de acceso a la información	Preventivo
A.8.6	Gestión de la capacidad	Preventivo
A.8.7	Protección contra códigos maliciosos	Preventivo
A.8.8	Gestión de vulnerabilidades técnicas	Preventivo
A.8.9	Gestión de la configuración	Preventivo
A.8.13	Copia de seguridad de la información	correctivo
A.8.14	Redundancia de las instalaciones de procesamiento de información	Preventivo
A.8.16	Actividades de seguimiento	correctivo
A.8.22	Segregación de redes	Preventivo

6. PRESUPUESTO

La estimación y asignación de los recursos para la implementación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, para los riesgos identificados, corresponderá al líder del proceso, quien es el responsable de contribuir con el seguimiento y control de la gestión, además de la implementación de los controles definidos para la mitigación de los riesgos.

Si el establecimiento de los controles implica la adquisición de herramientas o servicios tecnológicos bajo la responsabilidad de la Dirección de gestión de información y tecnología, los recursos se tomarán del proyecto de inversión:

AÑO 2025	
PROYECTO	**Inversión**
Objetivo 3: Implementar un modelo de Seguridad y Privacidad de la información. Producto 3.1 Documentos de política - Modelo de políticas y lineamientos de Seguridad y Privacidad de la Información Certificación ISO	$2.800.000.000

7. CRONOGRAMA Y ENTREGABLES

Para dar cumplimiento al ciclo de riesgo, se establece anualmente las actividades a realizar de manera conjunta con todos los procesos, los riesgos de seguridad de la información identificados se reflejarán en la publicación de la matriz de riesgos año 2025, allí se establecen las acciones de control y las fechas para implementar dichas actividades, la Dirección de gestión de información y tecnología apoyará el proceso de definición e implementación de los controles con los líderes de cada uno de los procesos. El ciclo de identificación, valoración, monitoreo y seguimiento se describe a continuación:

Actividad	Fecha de Inicio	Fecha Final
Identificación de activos con criticidad alta	ene-25	feb-25
Identificación de riesgos de seguridad de la información	feb-25	dic-25
Valoración de riesgos	feb-25	dic-25
Clasificación de riesgos inherente	feb-25	dic-25
Identificación de controles	feb-25	dic-25
Entrega de Matriz actualizada por cada proceso o dependencia a la OAP	jun-25	dic-25
Definición del Plan de Tratamiento de riesgos	oct-25	dic-25

8. RIESGOS

RIESGO	PROBABILIDAD	IMPACTO	CONTROL PROPUESTO
Disponibilidad de recursos: La falta de recursos necesarios, como personal capacitado, equipos o materiales, puede retrasar o incluso detener la ejecución del plan	MEDIA	ALTO	Se debe asegurar la contratación del personal requerido para ejecutar las actividades definidas en el Plan
Gestión de recursos: Una mala gestión de los recursos, como la asignación ineficiente o la falta de coordinación entre equipos, puede llevar a sobrecargas de trabajo, errores y fallos en la implementación del plan	BAJA	ALTO	Se debe realizar una correcta coordinación del tiempo, alcance, y personas capacitadas para la ejecución de las actividades del plan

Nota: Medir Probabilidad e Impacto en: Alto, Medio, Bajo.

9. MEDICIÓN DE RESULTADOS

Toda vez que el presente Plan está integrado al Plan de Acción Institucional de la vigencia, el seguimiento se realizará cuatrimestralmente y se reportará el resultado de cada período, en el instrumento de seguimiento al Plan de Acción, en el compromiso asociado al Plan de Seguridad y Privacidad de la Información.

La medición se realiza con el indicador “Riesgos de Seguridad de la información mitigados” que está orientado principalmente a disminuir el número de riesgos identificados con nivel alto y extremo, a través de la implementación de controles asociados al cumplimiento de la Norma ISO 27001:2022, de manera que se disminuya el riesgo no aceptable a menos del 30%.

Nivel de Riesgo no aceptable de Seguridad de la Información:

$$\frac{\text{No. de riesgos residuales con nivel no aceptable}}{\text{Total, de riesgos de seguridad de la información identificados}} * 100$$