Hacienda

Plan de Riesgo de Seguridad y Privacidad de la Información

Versión 1
27 de enero 2026

TABLA DE CONTENIDO

1. INTRODUCCIÓN

Mediante la definición del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, el Ministerio de Hacienda y Crédito Público busca establecer medidas para mitigar los riesgos asociados a los activos de información, como la pérdida de confidencialidad, integridad y disponibilidad, procurando así, evitar situaciones que generen incertidumbre en el cumplimiento de la misionalidad de la Entidad.
El presente plan se elabora con el fin de orientar las acciones que permitan mitigar los riesgos identificados en los procesos de la entidad. Estas acciones se concretan mediante actividades que se definen teniendo en cuenta la información obtenida del seguimiento a los riesgos de seguridad y privacidad de la información, las necesidades y el contexto de la entidad a partir de las cuales se establecen tareas, responsables y fechas de ejecución durante la vigencia.
El plan de tratamiento de riesgos de Seguridad y Privacidad de la información se elabora con el fin de dar cumplimiento a lo establecido en el Decreto 612 de 2018 y tiene como base los lineamientos establecidos por el Departamento Administrativo de la Función Pública en la guía de administración de Riesgos y Diseño de Controles, el modelo de Seguridad y Privacidad de la Información - MSPI y el plan de Seguridad y Privacidad de la información, donde se establecen recomendaciones para la identificación, análisis, tratamiento, evaluación y monitoreo de los riesgos y los lineamientos de los estándares ISO 27001, ISO 31000.

2. OBJETIVOS

- Cumplir con los requisitos legales, reglamentarios, regulatorios relacionados con riesgos de seguridad digital y seguridad de la información.

- Realizar una adecuada gestión de riesgos de Seguridad y Privacidad de la información, teniendo en cuenta los lineamientos establecidos em el Ministerio de Hacienda y Crédito Público.

- Fortalecer y apropiar conocimiento referente a la gestión de riesgos de Seguridad y Privacidad de la información en el MHCP.

3. ALCANCE

El Plan de Tratamiento incluye los riesgos de Seguridad de la Información que se encuentren en los niveles alto, medio y bajo acorde con los lineamientos

definidos en la política de riesgos del MHCP, todos aquellos clasificados en niveles inferiores tendrán tratamiento de aceptación por parte de la Entidad. Lo contenido en este plan será aplicable a todos los procesos de la entidad.

4. MARCO DE REFERENCIA

4.1 Política de Administración de riesgo.

La Alta Dirección del MHCP se compromete a administrar los riesgos de gestión, corrupción y seguridad de la información, a través del establecimiento de lineamientos que permitan orientar el direccionamiento estratégico y la gestión institucional, para evitar su materialización, de forma que se asegure el rigor y la calidad en la producción estadística; así mismo, asignar los recursos pertinentes que se requieran para la prevención y el tratamiento adecuado de los riesgos.
La siguiente imagen representa la metodología de la administración del riesgo en el Ministerio de Hacienda y Crédito Público.

Ilustración1. Ciclo de administración del riesgo MHCP.

4.2 Contexto

El primer paso para la elaboración del diagnóstico y la determinación del contexto es la recopilación y análisis de la documentación e información

que resulte relevante para realizar un diagnóstico inicial del estado de la administración de los riesgos de seguridad digital dentro de la entidad.

Esta documentación e información es también necesaria para el desarrollo de cada una de las actividades que se describen a continuación, en especial para el análisis del contexto y su incidencia en el proceso de gestión de los riesgos asociados a seguridad digital y ciberseguridad
La información y documentación que podría ser relevante para este proceso sería la siguiente:

Información sobre la naturaleza jurídica y objeto del MHCP	Normas que regulan la entidad
Funciones generales de la entidad	Planes de capacitación en ciberseguridad
Políticas de Seguridad de la Información	Objetivos estratégicos
Código de Buen Gobierno	Organigrama institucional, descripción de funciones
Plan de respuesta antes incidentes	Evaluación de vulnerabilidades
Evaluaciones de riesgos previas	Pruebas de penetración (Pentesting)
Descripción de herramientas y plataformas tecnológicas con la que cuenta la entidad para el desarrollo de sus funciones.	Lista de proveedores y servicios críticos
Plan de continuidad del negocio (BCP)	Planes de respaldo y recuperación de proveedores
Otros documentos que consideren relevantes	

4.3. Identificación de los riesgos

Siguiendo con el proceso, etapas y pasos que recomiendan los lineamientos establecidos en la Guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP y estándares internacionales para la administración y supervisión de riesgos de seguridad digital y ciberseguridad, una vez concluida la etapa del análisis del contexto, definido el marco conceptual y definidas las bases con las cuales se desarrolla el Sistema, se procede a la ejecución del siguiente paso o etapa del Sistema, es decir, la etapa de **IDENTIFICACIÓN DE LOS RIESGOS**, la cual cubre los siguientes aspectos:

- DESCRIPCIÓN DE LOS EVENTOS DE RIESGO DE SEGURIDAD DIGITAL Y CIBERSEGURIDAD
- DISEÑO DE LA MATRIZ DE RIESGO INHERENTE.
- PROCEDIMIENTOS DE IDENTIFICACIÓN DE RIESGOS DE SEGURIDAD DIGITAL Y CIBERSEGURIDAD
- IDENTIFICACIÓN DE LOS EVENTOS DE RIESGO.

4.4. Medición y Evaluación

Concluida la etapa de identificación de riesgos de los eventos de riesgo, debe procederse a la medición y evaluación. El análisis de riesgos de Seguridad digital y Ciberseguridad involucra medir la probabilidad o posibilidad de ocurrencia del riesgo inherente de cada uno de los eventos, así como el impacto en caso de materializarse mediante los riesgos asociados.
Las consecuencias y probabilidades se combinan para producir el nivel de riesgo.
La mejor forma y la más idónea para medir o evaluar el riesgo de Seguridad, es mediante estimaciones cualitativas derivadas del conocimiento de expertos, la experiencia relevante y las prácticas y experiencia del supervisor que reflejen el grado de convicción de que podrá ocurrir un evento o resultado particular.

5. PLAN DE TRATAMIENTO

El Plan de Tratamiento de Riesgos de Seguridad de la Información establece las actividades a desarrollar con el fin de mitigar los riesgos sobre los activos identificados por la entidad, de acuerdo con las recomendaciones de la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información establecida por la Función Pública.

No	Actividad	Tarea	Fecha inicial	Fecha final	Responsable
1.1	Actualizar los lineamientos de riesgos	Apoyar cuando se requiera la actualización de la política, metodología y lineamientos de la gestión de riesgos.	Febrero 01 2026	Noviembre 30 - 2026	Equipo interno de Seguridad de la Información de la Dirección de Tecnología
1.2	Realizar sensibilización	Socializar los lineamientos y Herramientas para la Gestión de los Riesgos de Seguridad y privacidad de la Información	Marzo 01 2026	Mayo 31 2026	

1.3	Identificar los riesgos de Seguridad y privacidad de la Información	Contexto, Identificación, Análisis y Evaluación de Riesgos - Seguridad y Privacidad de la Información y Seguridad Digital	Marzo 01 2026	Julio 31 2026	
1.4	Aceptar los Riesgos Identificados	Aprobar los riesgos identificados y elaborar los planes de tratamiento cuando aplique.	Mayo 01 2026	Julio 31 2026	Gestión de Tecnología y Seguridad de la Información
1.5	Hacer seguimiento	Realizar el seguimiento a la implementación de controles y planes de tratamiento para los riesgos identificados	Febrero 01 20224	Diciembre 20 - 2026	
1.6	Realizar mejoramiento	Revisar o actualizar los lineamientos de Riesgos de Seguridad y privacidad de la información.	Julio 01 2026	Diciembre 20 - 2026	

6. PRESUPUESTO

La estimación y asignación del presupuesto para el plan de tratamiento de riesgos de Seguridad y Privacidad de la Información y Seguridad Digital identificados por el MHCP, corresponderá al dueño del riesgo (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 y del plan de tratamiento.

Plan de Riesgo de Seguridad y Privacidad de la Información

ELABORADO POR:	**Nombre:** Francisco José Ariza Pastor **Cargo:** Contratista **Fecha:** 21-01-2026
REVISADO POR:	**Nombre:** Marly Esther De Moya Amaris **Cargo:** Profesional Especializado **Fecha:** 21-01-2026
VALIDADO POR:	**Nombre:** Diego Fernando Huertas Ortiz **Cargo:** Director de Tecnología **Fecha:** 28-01-2026
APROBADO POR:	**Comité Institucional de Gestión y Desempeño** **Sesión:**

Hacienda

Ministerio de Hacienda y Crédito Público

Dirección: Carrera 8 No. 6C–38, Bogotá D.C., Colombia

Conmutador: (+57) 601 3 81 17 00

Línea Gratuita: (+57) 01 8000 910071

Correo institucional: relacionciudadano@minhacienda.gov.co