UNIDAD ADMINISTRATIVA ESPECIAL
CONTADURÍA GENERAL DE LA NACIÓN - CGN

GRUPO INTERNO DE TRABAJO DE APOYO INFORMÁTICO

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

DICIEMBRE DE 2023

Dirección: Calle 26 # 69 - 76 | Edificio Elemento
Torre 1 (Aire) - Piso 15
Código Postal: 111071, Bogotá, Colombia
www.contaduria.gov.co | contactenos@contaduria.gov.co
PBX: +57 (601) 492 64 00

CONTROL DE CAMBIOS

VERSIÓN	SECCIÓN	TIPO	FECHA (DD/MM /AAAA)	AUTOR	OBSERVACIONES
1.0	Todas	Creación	29-12-2023	Git de Apoyo Informático	Elaboración del plan

Contenido

1. Introducción

La Contaduría General de la Nación, en adelante CGN, al igual que la mayoría de las entidades públicas en Colombia mueve gran parte de su operación misional en un entorno cada vez más digital y amenazante. Los riesgos asociados con violaciones de seguridad, pérdida de datos o interrupciones en los servicios pueden tener un impacto directo en su capacidad operar de manera eficiente y cumplir con sus metas estratégicas.

La pérdida de la confianza de los grupos de valor debido a brechas de seguridad puede resultar en una disminución significativa de las oportunidades institucionales, por lo tanto, puede afectar negativamente los objetivos estratégicos relacionados con el fortalecimiento, crecimiento y expansión.

La gestión proactiva de riesgos de seguridad y privacidad de la información no solo ayuda a cumplir con las regulaciones vigentes, sino que también demuestra un compromiso serio con la responsabilidad institucional y la protección de los intereses de todas las partes involucradas, lo que se alinea directamente con los objetivos estratégicos centrados en la integridad y la excelencia operativa.

En cumplimiento del Decreto 1008 de 2018 para el desarrollo del habilitador transversal "Seguridad de la Información" de la Política de Gobierno Digital, así como para dar cumplimiento a la Resolución 500 de 2021 que da lineamientos para el desarrollo de la estrategia de seguridad digital y conforme al decreto 767 de 2022, expedidos por MinTIC que desarrolla el habilitador de Seguridad y Privacidad de la Información; se estructura este documento en el contexto de la CGN. De igual manera, el presente documento se alinea con las disposiciones prescritas en los siguientes documentos: CONPES 3701 de 2011, Lineamiento de Políticas de Ciberseguridad y Ciberdefensa; CONPES 3854 de 2016, Política Nacional de Seguridad Digital; CONPES 3975 de 2019, Política Nacional para la Transformación Digital e Inteligencia Digital; y CONPES 3995 de 2020, Política Nacional de Confianza y Seguridad Digital; con lo cual se define de manera integral en el presente documento el Plan Institucional de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, para la vigencia 2024.

2. Objetivo

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información establece los lineamientos metodológicos para la administración de los riesgos de seguridad de la información que permitan fortalecer el enfoque preventivo para mitigar los riesgos de Seguridad Digital que superan el nivel de riesgo aceptable para la Entidad, y que su materialización pueda impactar el logro de los objetivos estratégicos de la Contaduría General de la Nación.

3. Alcance

La gestión de riesgos de seguridad de la información aplica a todos los activos de información que forman parte de los procesos institucionales de la Contaduría General de la Nación y demás partes interesadas que comparten, utilicen, recolecten, procesen, intercambien o consulten cualquier tipo de activo de información, identificados en el Sistema de Gestión de la Seguridad de la Información, en adelante SGSI, de la entidad.

Inicia con la definición del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, continua con la ejecución del Plan y finaliza con el seguimiento y evaluación de la gestión realizada.

Aplica a todos los activos de información creados, procesados o utilizados sin importar el medio, formato o presentación y lugar en el cual se encuentre.

4. Definiciones

Activos de información: se refiere a cualquier dato o recurso vinculado al procesamiento de la información (como sistemas, dispositivos de almacenamiento, infraestructura física locativa y de TI o recursos humanos) que posea un valor significativo para la organización.

Amenaza: una amenaza informática es toda circunstancia, evento o acción que tiene el potencial de causar daño, degradar la seguridad o comprometer activos de la entidad. Estas amenazas pueden surgir tanto de fuentes internas como externas y pueden ser intencionadas o accidentales.

CIGD – Sigla de Comité Institucional de Gestión y Desempeño

Confidencialidad: es un principio de seguridad de la información que garantiza

que los datos sensibles o privados se mantengan protegidos y solo estén disponibles para aquellos usuarios autorizados que tienen permiso explícito para acceder a ellos.

Control: es una medida o procedimiento implementado para proteger los activos, minimizar riesgos y asegurar el cumplimiento de políticas de seguridad. Estos controles pueden ser tecnológicos, físicos o de procedimiento, diseñados para mitigar amenazas y garantizar la confidencialidad, integridad y disponibilidad de la información.

Disponibilidad: es un principio de seguridad de la información que se refiere a la garantía de que los datos estén accesibles y disponibles para aquellos que tienen autorización para utilizarlos, en el momento en que se necesitan. Esto implica asegurar que los sistemas y recursos estén operativos y funcionando correctamente para permitir el acceso a la información cuando sea requerida.

GIT: Sigla Grupo Interno de Trabajo.

Incidente de seguridad de la información: es un evento que compromete la confidencialidad, integridad o disponibilidad de los datos o sistemas de una organización. Estos incidentes pueden ser intencionados o accidentales e incluyen acciones no autorizadas, fallos en la seguridad, intrusiones o pérdidas de datos que representan una amenaza para la seguridad de la información.

Integridad: es un principio de seguridad de la información que se refiere a la calidad de los datos que se encuentran completos, precisos y no han sido modificados de manera no autorizada. Este principio de seguridad de la información asegura que la información se mantenga íntegra, es decir, que no haya sido alterada, manipulada o dañada de manera intencionada o accidental, y que permanezca exacta y fiable a lo largo del tiempo y en su transmisión o almacenamiento.

MINTIC: Sigla Ministerio de Tecnologías de la Información y las Comunicaciones.

MSPI: Sigla Modelo de Seguridad y Privacidad de la Información.

PTRSPI: Sigla Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

Riesgo*:* Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales (tomado de PLAN DE TRATAMIETO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – MinTIC)

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. (ISO/IEC 27000).

Seguridad de la información: preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

SGD: sigla de Sistema de Gestión y Desempeño

SGSI: sigla de Sistema de Gestión de la Seguridad de la Información.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

5. Condiciones generales

La Alta Dirección respalda activamente la gestión de riesgos de seguridad y privacidad de la información mediante el cumplimiento de la política de privacidad y protección de datos, la Estrategia de Seguridad Digital, la implementación del SGSI y la adopción del marco regulatorio correspondiente.

En la preparación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, en adelante PTRSPI, de la Contaduría General de la Nación, además, se da enfoque en la alineación de los procesos y la evaluación interna a través del instrumento de autodiagnóstico del MSPI del MINTIC, con el fin de identificar y aplicar las actualizaciones pertinentes en este documento.

6. Estrategias de cumplimiento

La Contaduría General de la Nación, mediante la adopción e implementación del MSPI enmarcado en el SGSI, protege, preserva y gestiona la confidencialidad, integridad, 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/o las consecuencias de la materialización de los incidentes.

Para lograr el cumplimiento del PTRSPI se definen las siguientes estrategias enmarcadas en el ciclo de mejora continua PHVA:

1. Definir las actividades del *planear* de tratamiento de riesgos.
2. Definir las actividades del *hacer* de tratamiento de riesgos.
3. Definir las actividades del *verificar* de tratamiento de riesgos.
4. Definir las actividades del *actuar* de tratamiento de riesgos.

7. Roles y responsabilidades

Rol		Responsabilidad
Rol Estratégico	Comité Institucional de Gestión y Desempeño	- Aprobar el PTRSPI. - Aprobar la Matriz de Tratamiento de Riesgos de Seguridad - Tomar decisiones sobre los asuntos de la gestión de riesgos de seguridad.
Rol Táctico	Oficial de Seguridad de la Información o quien haga sus veces.	- Preparar, presentar y hacer seguimiento a la Matriz de Tratamiento de Riesgos de Seguridad. - Gestionar los activos de información - Apoyar a los responsables de los activos de información en la identificación de los riesgos asociados. - Realizar seguimiento al cumplimiento del PTRSPI por parte de los responsables.
Rol Funcional y operativo	GIT Apoyo Informático	- Implementar controles de tipo tecnológico que ayuden a mitigar los riesgos de seguridad de la información. - Velar por la protección de los activos de información del proceso

Rol		Responsabilidad
	Líderes de Procesos	- Participar y apoyar la gestión del PTRSPI del proceso y la Matriz de Tratamiento de Riesgos de Seguridad correspondiente. - Velar por la protección de los activos de información del proceso. - Aplicar y promover los controles y buenas prácticas de seguridad de la información y seguridad digital.

8. Funciones

Comité Institucional de Gestión y Desempeño

Las funciones y responsabilidades en los temas de tratamiento de riesgos de seguridad y privacidad de la información son desarrolladas por el Comité Institucional de Gestión y Desempeño mediante Resolución número 193 del 19 de junio 2019.

Alta Dirección

- Aprobar anualmente o cuando se requiera el PTRSPI de la CGN.
- Aprobar los objetivos de seguridad de la información, los cuales estarán alineados con los objetivos estratégicos de la entidad.
- Asignar y aprobar el presupuesto necesario para el normal funcionamiento del SGSI.
- Proporcionar los recursos necesarios para la ejecución y desarrollo de las actividades del SGSI.
- Promover activamente una cultura de seguridad y privacidad de la información basada en la mitigación de los riesgos para la entidad.

Oficial de Seguridad o quien haga sus veces (resolución 2023):

Tiene el rol de administrador del SGSI y es el responsable de:

- Realizar seguimiento al cumplimiento de los lineamientos y políticas del SGSI.
- Revisar y proponer las políticas, planes, programas, procedimientos en materia de seguridad de la información y seguridad digital para la

aplicación de controles en el sistema.

- Realizar revisiones periódicas al PTRSPI y definir acciones para la mejora continua.
- Asegurar el cumplimiento de las políticas, normas, procedimientos, y demás lineamientos en materia de seguridad de la información y seguridad digital.
- Gestionar el tratamiento de riesgos de seguridad y privacidad de la información y controlar las acciones de tratamiento establecidas.
- Definición de indicadores y su seguimiento.
- Gestionar los activos de información.

Líderes de procesos:

El papel de los líderes de procesos en la ejecución del PTRSPI es fundamental, ya que son responsables de:

- Aceptar la responsabilidad como dueños de los activos de la información del proceso
- Realizar seguimiento a la ejecución de los planes de tratamiento de riesgos en seguridad de la información del proceso.
- Actualización de activos de información.
- Revisión y cumplimiento de los procedimientos, controles y políticas del SGSI.

Coordinador de GIT de Apoyo Informático:

El GIT de Apoyo Informático y su equipo de trabajo serán los responsables de los controles técnicos de seguridad de la información:

- Cierre de vulnerabilidades técnicas y su seguimiento.
- Apoyar la atención y gestión de los eventos e incidentes de seguridad de la información y seguridad digital
- Gestionar los riesgos de seguridad de la información del proceso Gestión TICs.
- Establecer controles de seguridad de la información y seguridad digital en los servicios que presta el GIT de Apoyo Informático para asegurar la confidencialidad, disponibilidad e integridad de la información.
- Velar por la protección de los activos de información del GIT.

Funcionarios y Contratistas

- Adoptar las políticas y procedimientos definidos para el sostenimiento del SGSI.
- Mantener la confidencialidad e integridad de la información que reciben, generan y procesan en la CGN.
- Hacer buen uso de los activos de información de la entidad.
- Respetar la legislación y regulación vigente.
- Notificar a la cuenta de correo electrónico seguridadinformatica@contaduria.gov.co los eventos o incidentes de seguridad de información, así como cualquier eventualidad sospechosa que pueda poner en riesgo la continuidad de las operaciones de la CGN.

9. Desarrollo del Plan de Tratamiento de Riesgos

El PTRSPI de la CGN tiene como propósito definir las actividades para la identificación, evaluación, tratamiento y aceptación de los riesgos de seguridad y privacidad de la información asociados a los activos de información críticos de la entidad, y la materialización de las actividades de tratamiento de riesgos se reflejan en el documento Excel "PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACION" (Matriz de Riesgos de Seguridad de la Información), ver anexos. Para su desarrollo se toma como base el documento Guía Riesgos, Gestión, Corrupción y Seguridad Digital del Departamento Administrativo de la Función Pública.

El PTRSPI se enmarca en el ciclo de mejora continua PHVA y comprende las siguientes actividades:

Planear

a. Establecer el contexto: parámetros internos y externos de la entidad, del proceso y de sus activos de información, que se han de tomar en consideración para la administración del riesgo.
b. Establecer los criterios para la evaluación del riesgo: genera una magnitud de evaluación del riesgo en términos de la frecuencia de ocurrencia y el impacto (consecuencias) de su materialización.
c. Establecer los criterios de aceptación del riesgo: determina cuáles riesgos se aceptan y cuáles riesgos deben mitigarse con un plan de tratamiento, en función de la evaluación y el criterio de aceptación.

d. Identificar los activos de información y su propietario: se elabora un inventario de activos de información del proceso y asigna el propietario del activo.

Las acciones de este ciclo se contemplan en la hoja identificada como "Descripción del riesgo" en el documento Excel "PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACION"; En particular, para la CGN se ha identificado una matriz de 22 riesgos negativos y un riesgo positivo y se exponen atributos como el tipo de riesgo, la causa o vulnerabilidad, las consecuencias en caso de materializarse, proceso al que aplica y la valoración inicial del riesgo.

Hacer

a. Identificar los riesgos: aplicar el proceso de evaluación de riesgos de seguridad de la información para identificar los riesgos asociados con la pérdida de confidencialidad, integridad y disponibilidad de la información dentro del alcance del PTRSPI y del SGSI.
b. Identificar los propietarios de los riesgos: asignar la responsabilidad de gestionar los riesgos a los propietarios de estos, que son los propietarios de los activos de información por proceso.
c. Analizar los riesgos: evaluar las consecuencias potenciales que se producirían si se materializan los riesgos identificados en el literal a. de este aparte; evaluar la probabilidad realista de que se produzcan los riesgos identificados en el literal a. de este aparte.
d. Valorar los riesgos: comparar los resultados del análisis de riesgos con los criterios de aceptación de riesgos.
e. Priorizar los riesgos valorados para su tratamiento.
f. Seleccionar las opciones de tratamiento de riesgos adecuadas (controles), en conjunto entre el propietario del riesgo, el Oficial de Seguridad de la Información y el GIT de Apoyo Informático.
g. Documentar el formato "PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACION.xls" para registro, seguimiento y control de los riesgos y su tratamiento.
h. Obtener, de parte de los dueños de los riesgos, la aprobación del plan de tratamiento de riesgos residuales (evaluación después de controles).
i. La entidad debe realizar evaluaciones de los riesgos de seguridad y privacidad de la información a intervalos planificados o cuando se produzcan cambios significativos y gestionar al plan de tratamiento correspondiente.

Esta acción se contempla en la hoja identificada como "Mapa y tratamiento" en el

documento Excel "PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACION"; Ahí se evalúa cada uno de los riesgos hallados en la sección anterior y se valora su riesgo residual, además se plantean opciones de tratamiento mediante la aplicación de acciones basadas en los 114 controles de seguridad que contiene la norma ISO-27001 de 2013 articulado con lo establecido en el "Plan de seguridad y privacidad de la información". También se dispone la manera de mantener la trazabilidad del riesgo a través de un soporte y un indicador de materialización para cada uno de ellos.

Verificar

a. El Oficial de Seguridad de la Información deberá hacer seguimiento, medición, análisis y evaluación al plan de tratamiento de los riesgos identificados.
b. Los resultados de la evaluación del plan de tratamiento de riesgos deberán ser presentados al Comité Institucional de Gestión y Desempeño.

Para la ejecución de estas acciones se revisará con periodicidad mensual las matrices anteriores con apoyo en documentación adicional como el flujograma de gestión de incidentes de seguridad digital y el formato "Registro de incidentes de seguridad de la información" y los casos reportados y asociados en la herramienta de soporte (GLPI) de la mesa de servicio.

Actuar

a. La entidad deberá mejorar continuamente la conveniencia, adecuación y eficacia del PTRSPI.

Para esto, se establece una revisión anual de los riesgos con el propósito de identificar nuevos potenciales riesgos o eliminar riesgos cuyo potencial de materialización sea mínimo o se puedan asumir.

10. Anexos

Archivo Excel "11. PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACION" (Matriz de Riesgos de Seguridad de la Información) publicado en el siguiente enlace: https://www.contaduria.gov.co/documents/20127/5781528/11.+PLAN+DE+TRTAMIENTO+DE+RIESGOS+DE+SEGURIDAD+DE+LA+INFORMACION++2023..xls/856c5b57-f9c4-fb98-cd83-371c161cdc48

11. Bibliografía

MINTIC, (2021). Política de gobierno digital. Recuperado el 10 de junio de 2022 de https://gobiernodigital.mintic.gov.co/portal/Manual-de-Gobierno-Digital/

Elaboró: Juan Pablo Peralta Silva
Revisó: Jamir Mosquera R./Martha Patricia Zornosa G.
Aprobó: Freddy Armando Castaño Pineda