TABLA DE CONTENIDO

1. OBJETIVO

Presentar el Plan para el Tratamiento de Riesgos asociados con la seguridad y privacidad de la información para el año 2024, que permita avanzar en la implementación del modelo de seguridad de la información del habilitador de Seguridad y Privacidad de la Información de la política de Gobierno Digital del estado colombiano.

De esta forma, se definirán los lineamientos y actividades a seguir, para la identificación, valoración y tratamiento de los riesgos inherentes a la seguridad de la información, a fin de evitar su materialización, protegiendo de esta forma la confidencialidad, integridad y disponibilidad de la información de la entidad.

2. ALCANCE

Este plan inicia con la identificación de los activos de información de la entidad hasta el monitoreo y evaluación de la disminución de los riesgos residuales. Para el respectivo tratamiento, solo se tomarán en cuenta los riesgos clasificados igual o mayor clasificación “Alto; mientras que aquellos que tienen evaluación inferior podrán ser aceptados por la entidad.

3. ROLES Y RESPONSABILIDADES

La responsabilidad de su ejecución recae sobre todos los procesos de la entidad, en especial en la etapa de identificación y priorización de activos de información como la identificación y tratamiento de los riesgos de Seguridad de la información.

La responsabilidad de la aplicación correcta de la metodología, así como el soporte en la ejecución de las diferentes etapas, es compartida entre los procesos Gestión de Tecnologías de la Información y las Comunicaciones y Direccionamiento Estratégico.

4. ÁMBITO DE APLICACIÓN

Toda la entidad

5. CONDICIONES GENERALES Y/O POLÍTICAS DE OPERACIÓN

Seguimiento de la Política de Gobierno Digital establecida por el Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC, relacionadas en el Modelo de Privacidad y Seguridad de la Información – MSPI, la Guía No. 7 – Guía de Gestión de Riesgos y la Guía No. 8 – Controles de Seguridad y Privacidad de la Información – Política de Riesgos de la Entidad.

Seguimiento de los lineamientos que la entidad determine para la identificación de activos de información

6. GLOSARIO

- **Activo de información:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma, el cual tiene valor para la SCRD por lo tanto para ello se tienen contemplados los siguientes activos de información: personas, información/dato, hardware, software, redes, infraestructura y servicios.
- **Amenaza:** Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización. Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
- **Análisis del Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).
- **Apetito del riesgo**: Es la cantidad de riesgo que una organización está dispuesta a asumir para alcanzar sus objetivos estratégicos.
- **Causa**: Todo factor interno y externo que solo o en combinación con otros, puede producir

la materialización de un riesgo.

- **Confidencialidad:** Propiedad que impide la divulgación de información a personas o sistemas no autorizados.
- **Control:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
- **Disponibilidad:** Característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.
- **Evaluación del riesgo**: Busca confrontar los resultados del análisis de riesgo inicial frente a los controles establecidos, con el fin de determinar la zona de riesgo final (Riesgo Residual).
- **Gestión del riesg**o: Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.
- **Identificación del riesgo:** Se deben establecer las fuentes o factores de riesgo, los eventos o riesgos, sus causas y sus consecuencias. Para el análisis se pueden involucrar datos históricos, análisis teóricos, opiniones informadas y expertas y las necesidades de las partes involucradas.
- **Impacto:** son las consecuencias que genera un riesgo una vez se materialice.
- **Integridad:** Garantía de la exactitud y completitud de la información de la información y los métodos de su procesamiento.
- **Probabilidad:** es la posibilidad de que la amenaza aproveche la vulnerabilidad para materializar el riesgo.
- **Riesgo inherente:** Es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.
- **Riesgo residual:** Nivel de riesgo que permanece luego de tomar medidas de tratamiento de riesgo.
- **Seguridad de la información**: Conjunto de medidas que toman las personas y las organizaciones, que les permiten resguardar y proteger los activos de información, preservando su Confidencialidad, Integridad y Disponibilidad.
- **Sistema de Gestión de Seguridad y privacidad de la información:** Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.
- **Vulnerabilidad:** es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.

7. RECURSOS

Para el desarrollo del plan de tratamiento de riesgos de seguridad digital, la Secretaría de Cultura Recreación y Deporte dispone de los siguientes recursos:

- **Humanos**: De la Oficina de Tecnologías de la Información- Grupo de Seguridad de la Información y responsables de los procesos y procedimientos que intervienen en el desarrollo del plan.
- **Técnicos:** Se dispone de documentación técnica como; NTC-ISO/IEC 27002:2015, NTC-ISO/IEC 27001:2013, la guía para la administración del riesgo y el diseño de controles en entidades públicas v6, la política de administración del riesgo, el mapa de riesgos para el registro y evidencia del proceso.
- **Físicos:** Se cuenta con la infraestructura tecnológica y física para el desarrollo de actividades como socializaciones, transferencia de conocimientos, comunicación del riesgo, seguimiento y evaluación a la gestión del riesgo.
- **Financieros:** La SCRD dispone de recursos financieros para la implementación de las acciones que requieran la contratación de servicios o la compra de bienes, los cuales son descritos en los planes de compras anuales.

8. DESCRIPCIÓN DE ACTIVIDADES

Actividad	Fecha Inicio	Fecha Fin	Responsable
Definición del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	2/01/2024	30/01/2024	OTI
Revisión y/o actualización del Manual de Gestión de Riesgos de Seguridad de la Información, en caso de requerirse.	1/03/2024	30/04/2024	OTI
Socialización Manual de Gestión de Riesgos de Seguridad de la Información.	1/05/2024	30/05/2024	OTI

Actividad	Fecha Inicio	Fecha Fin	Responsable
Apoyo en la identificación de riesgos de seguridad y privacidad de la información en los activos de información	1/06/2024	10/11/2024	OTI
Formalización y aprobación en ORFEO de las matrices de los riesgos identificados	1/06/2024	17/11/2024	Dependencias de la SCRD
Entrega a la OAP de las matrices de riesgos aprobadas.	1/11/2024	24/11/2024	OTI

9. INDICADOR

Seguimiento de actividades del cronograma ejecutado vs Seguimiento de actividades del cronograma planeado. Periodicidad trimestral.

10. DOCUMENTOS ASOCIADOS

NOMBRE	CÓDIGO	FÍSICO	ELECTRÓNICO	APLICATIVO
Anexo 1 Modelo de Seguridad y Privacidad de la Información	N.A.	N.A.	https://gobiernodigital.mintic.gov.co/692/articles162623_recurso_1. pdf	Página web

11. MARCO LEGAL

Dentro del marco legal más relevante para justificar el presente plan de seguridad y privacidad de la información se encuentran las siguientes normas:

- **Ley 1437 de 2011,** Capítulo IV, “utilización de medios electrónicos en el procedimiento administrativo”. “Los procedimientos y trámites administrativos podrán realizarse a través de medios electrónicos. Para garantizar la igualdad de acceso a la administración, la autoridad deberá asegurar mecanismos suficientes y adecuados de acceso gratuito a los medios electrónicos, o permitir el uso alternativo de otros procedimientos.”

- **Ley 1581 de 2012, Articulo 4**, g) Principio de seguridad: “La información sujeta a Tratamiento por el responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento”.

  - **Artículo 17**, ítem d: “Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento”.

- **Ley 1712 de 2014, Articulo 3,** “principio de transparencia”: “Principio conforme al cual toda la información en poder de los sujetos obligados definidos en esta ley se presume pública, en

consecuencia de lo cual dichos sujetos están en el deber de proporcionar y facilitar el acceso a la misma en los términos más amplios posibles y a través de los medios y procedimientos que al efecto establezca la ley, excluyendo solo aquello que esté sujeto a las excepciones constitucionales y legales y bajo el cumplimiento de los requisitos establecidos en esta ley".

- **Artículo 7:** "Disponibilidad de la información" "En virtud de los principios señalados, deberá estar a disposición del público la información a la que hace referencia la presente ley, a través de medios físicos, remotos o locales de comunicación electrónica. Los sujetos obligados deberán tener a disposición de las personas interesadas dicha información en la web, a fin de que estas puedan obtener la información, de manera directa o mediante impresiones. Asimismo, estos deberán proporcionar apoyo a los usuarios que lo requieran y proveer todo tipo de asistencia respecto de los trámites y servicios que presten."

- **Título III** "Excepciones acceso a la información" "Información exceptuada por daño de derechos a personas naturales o jurídicas. Es toda aquella información pública clasificada, cuyo acceso podrá ser rechazado o denegado de manera motivada y por escrito."

- **Conpes 3854 de 2016,** objetivo general "Fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país".

- **Decreto 767 de 2022** " Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.".

- **Decreto 612 de 2018**, artículo 1. "Integración de planes institucionales y estratégicos. Las entidades del Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión, al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011, deberán integrar los planes institucionales y estratégicos que se relacionan a continuación y publicarlo, en su respectiva página web."

12. CONTROL DE CAMBIOS

No.	CAMBIOS REALIZADOS
1	Este documento sustituye el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información GOT-PN-03 con radicado 20231700039873. Fecha: 30/01/2023. Se modificaron en el cronograma las fechas de las actividades: Apoyo en la identificación de riesgos de seguridad y privacidad de la información en los activos de información, Formalización y aprobación en ORFEO de las matrices de los riesgos identificados y Segunda entrega a la OAP de las matrices de riesgos aprobadas, conforme a lo registrado en el acta con radicado 20231700181733. En la sección de Roles y responsabilidades, se cambió la parte del texto en la que se mencionaban los procesos Gestión Operativa de TI y Gestión Estratégica de TI y se dejó registrado el proceso de Gestión de Tecnologías de la Información y las Comunicaciones, conforme a la resolución 153 del 13 de marzo de 2023 con la cual se actualizó la plataforma estratégica de la entidad. En la sección Recursos técnicos se actualizó la referencia a la Guía para la administración del riesgo y el diseño de controles en las entidades públicas puesto que la versión vigente es la no. 6.
2	Ver Solicitud de elaboración, actualización o eliminación de documento / Radicado: **20241700041403** Fecha: **31/01/2024**

13. RESPONSABLES DE ELABORACIÓN, REVISIÓN Y APROBACIÓN

ELABORADO POR *Persona(s) responsable(s) de crear, proyectar la modificación y/o ajuste del documento*	APROBADO POR *Líder del Proceso quién debe hacer cumplir el contenido establecido en el documento*	REVISADO POR *Persona(s) de la OAP Responsable(s) de verificar que el documento contenga los lineamientos establecidos*	AVALADO POR *Jefe de la Oficina Asesora de Planeación y Comité Institucional de Gestión y Desempeño*
NOMBRE: Nidia Patricia Rodríguez Rodríguez Jairo Enrique León León	NOMBRE: Fabio Fernando Sánchez Sánchez	NOMBRE: Nelson Javier Velandia Castro	NOMBRE: Comité Institucional de Gestión y Desempeño de la SCRD
CARGO: Contratistas Oficina de Tecnologías de la Información	CARGO: Jefe Oficina de Tecnologías de la Información (E.)	CARGO: Profesional universitario	CARGO: N/A
FIRMA: Electrónica	FIRMA: Electrónica	FIRMA: Electrónica	FIRMA: Acta No. 2 de la sesión del 30 de enero de 2024