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

PROCESO: GESTIÓN DE SISTEMAS DE INFORMACIÓN Y TECNOLOGÍA

Versión: 06 de 30 de diciembre de 2024

**Contenido**

Tabla de contenido

[**1.**](#_heading=h.4d34og8) **Objetivo 1**

[**2.**](#_heading=h.2s8eyo1) **Alcance 1**

[**3.**](#_heading=h.17dp8vu) **Definiciones 2**

[**4.**](#_heading=h.3rdcrjn) **Normatividad 3**

[**5.**](#_heading=h.26in1rg) **Actividades del Plan 5**

[**6.**](#_heading=h.lnxbz9) **Control de Cambios 6**

[**7.**](#_heading=h.35nkun2) **Créditos 6**

1. **Objetivo**

Fortalecer la gestión de riesgos de seguridad de la información mediante un Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información que apoye la identificación, análisis, tratamiento, evaluación y monitoreo de los riesgos de Seguridad Digital, preservando la Confidencialidad, Integridad y Disponibilidad de la información, acorde con los requerimientos de la entidad y en relación con el cumplimiento de requisitos legales y reglamentarios pertinentes a la legislación colombiana.

1. **Alcance**

El presente Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información aplica para todos los procesos de la entidad, incluyendo las actividades para la gestión del riesgo a través de la Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad Digital. Diseño de Controles en Entidades Públicas y Anexo 4 Modelo nacional de gestión de riesgos de seguridad de la información para entidades públicas, logrando así la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI).

1. **Definiciones**

**Amenaza:** Ente o escenario interno o externo, que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo).

**Confidencialidad:** Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

**Concientización:** Acción que se relaciona con tomar conciencia de un asunto determinado, mostrarle una verdad a través del diálogo y hacerle reflexionar sobre un asunto concreto.

**Control:** Acciones o mecanismos definidos, para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una entidad.

**Disponibilidad:** Propiedad de la información, de estar accesible y utilizable, cuando lo requiera una entidad autorizada.

**Impacto:** Consecuencias que genera un riesgo una vez se materialice.

**Información**: Datos organizados, de tal forma que tienen un significado.

**Integridad:** Propiedad de la información relativa a su exactitud y completitud.

**Partes interesadas:** Son todos aquellos individuos, grupos u organizaciones que tengan algún beneficio o perjuicio, relacionado con los intereses y actividades de la entidad.

**Probabilidad**: Posibilidad de que la amenaza aproveche la vulnerabilidad, para materializar el riesgo, en otras palabras, qué tan posible es que el riesgo se materialice.

**Riesgo:** Escenario de incertidumbre, bajo el cual una amenaza puede explotar una vulnerabilidad, generando un impacto negativo al negocio y evitándose cumplir con sus objetivos.

**Sensibilización:** Proceso de comunicación activo que promueve transformación, cambio de actitudes y comportamientos en las personas de la entidad.

**Tecnología de la Información:** Hace referencia a las aplicaciones, información e infraestructura requerida por una entidad, para apoyar el funcionamiento de los procesos y estrategia de negocio.

**Vulnerabilidad:** Falencia o debilidad que es inherente a los activos de información o a los controles.

1. **Normatividad**

**Ley 23 de 1982**. Ley sobre derechos de autor.

**Ley 527 de 1999**. Por medio de la cual se define y reglamenta el acceso y uso de los mensajes

de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

**Ley 1273 de 2009**. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien

jurídico tutelado - denominado de la protección de la información y de los datos- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

**Ley 1450 de 2011**. Por la cual se expide el Plan Nacional de Desarrollo, 2010-2014.

**Ley Estatutaria 1581 de 201**2, Por la cual se dictan disposiciones generales para la protección de datos personales.

**Ley 1712 de 2014**, Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones.

**Decreto 1078 de 2015**, Por medio del cual se expide el Decreto Único. Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

**Resolución Distrital 305 de 2008**, Por la cual se expiden políticas públicas para las entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación, seguridad, democratización, caridad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y Software Libre.

**Resolución 004 de 2017**, Por la cual se modifica la Resolución 305 de 2008 de la CDS.

**MINTIC Resolución 500 de marzo 10 de 2021**, “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”

**MINTIC Decreto 767 de mayo 16 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”

**Documento CONPES 3701 de 2011** - Lineamientos de Políticas sobre ciberseguridad y ciberdefensa.

**Documento CONPES 3854 de 2016** - Política Nacional de Seguridad Digital.

**Documento CONPES 3995 de 2020** - Política Nacional De Confianza y Seguridad Digital.

**Norma NTC-ISO 31000:2018**. Esto con el fin de proteger la información del Instituto, desde la privacidad, la confidencialidad, la integridad y la disponibilidad, lo que facilitará el cumplimiento de los objetivos estratégicos institucionales.

1. **Actividades del Plan**

La implementación para el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información comprende el siguiente cronograma:

| **ID** | **Actividades** | **Responsable** | **Productos** |
| --- | --- | --- | --- |
| 1 | Actualizar, identificar, registrar y valorar los riesgos de seguridad digital durante la vigencia, siguiendo la metodología definida por Mintic a partir del inventario de activos de información de la entidad. | Procesos IDPC / Oficial de Seguridad de la Información. | Tres (3) formatos de valoración de riesgos y/o correos electrónicos.  Matriz de riesgo actualizada. |
| 2 | Sensibilización de riesgos de seguridad digital a los responsables de proceso. | Oficial de seguridad de la información. | Tres (3) actas de reunión y/o correos electrónicos o boletines de seguridad. |
| 3 | Reportar la materialización de riesgo de acuerdo a las definiciones institucionales. | Oficial de seguridad de la información.  Procesos IDPC | Formatos y/o correos electrónicos.  Reportes periódicos. |
| 4 | Determinar el tratamiento y diseño de controles. | Procesos IDPC / Oficial de seguridad de la información. | Un (1) Formato de valoración de riesgos y/o correos electrónicos.  Matriz de riesgo actualizada. |
| 5 | Registrar la aceptación de los riesgos. | Procesos IDPC | Un (1) formato y/o correos electrónicos. |
| 6 | Publicar la matriz riesgos de seguridad digital. | Oficial de seguridad de la información  Subdirección de gestión  Corporativa-Sistemas | Una (1) matriz de riesgos de seguridad digital. |
| 7 | Realizar seguimientos al tratamiento de riesgos de seguridad digital. | Procesos IDPC / Oficial de Seguridad de la  Información. | Tres (3) matriz de riesgo actualizada, actas de reunión y/o correos electrónicos.  Reportes periódicos. |

1. **Control de Cambios**

| **Fecha** | **Versión** | **Cambios Introducidos** | **Simplificación o mejora** | **Origen** |
| --- | --- | --- | --- | --- |
| 28/01/2019 | 01 | Creación del documento. |  |  |
| 28/01/2020 | 02 | Ajuste de formato y contenido. | Mejora |  |
| 20/12/2021 | 03 | Actualización de actividades para el cumplimiento de los requisitos FURAG | Mejora | Requerimiento FURAG. |
| 30/01/2023 | 04 | Actualización de actividades | Mejora | Resultado de revisión y autocontrol. |
| 15/12/2023 | 05 | Cambio de formato, se elimina la normatividad y se corrige el número de la versión. | Mejora | Resultado de revisión y autocontrol |
| 30/01/2024 | 06 | Actualización de actividades | Mejora | Resultado de revisión y autocontrol |
| 30/12/2024 | 07 | Actualización de actividades | Mejora | Resultado de revisión y autocontrol |

1. **Créditos**

| **Elaboró** | **Revisó** | **Aprobó** |
| --- | --- | --- |
| Ángel Antonio Díaz Vega | Mary Rojas |  |
| Cargo – Rol: Contratista – Oficial de  Seguridad de la Información  Subdirección de Gestión  Corporativa | Cargo – Rol: Líder TI  Subdirección de Gestión  Corporativa | Comité Institucional de Gestión y Desempeño |
| Aprobado | Acta del 30-12-2024 Comité Institucional de Gestión y Desempeño | |