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

PROCESO: GESTIÓN DE SISTEMAS DE INFORMACIÓN Y TECNOLOGÍA

Versión: 5 del 29 de diciembre de 2023

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.

2. 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).

3. 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.

4. 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	Presentar informes mediante matriz de riesgo, analizando las vulnerabilidades de seguridad en los sistemas de información utilizados por los servicios ofrecidos en el IDCP a la ciudadanía.	Oficial de Seguridad de la Información	Informe de vulnerabilidades de seguridad a los sistemas de información del IDPC.
2	Sensibilización de riesgos de seguridad digital a los responsables de proceso.	Oficial de Seguridad de la Información.	Actas de reunión y/o correos electrónicos.
3	Identificación, clasificación y valoración de Activos de Información	Oficial de Seguridad de la Información. Procesos IDPC	Formatos de valoración de riesgos y/o correos electrónicos.
4	Identificación de Amenazas y Vulnerabilidades. Determinación del Impactos de las amenazas por activo Determinación de Probabilidad de Ocurrencia	Oficial de Seguridad de la Información. Procesos IDPC	Formatos de valoración de riesgos y/o correos electrónicos.
5	Identificación, registro y valoración de riesgos de seguridad digital durante la vigencia.	Procesos IDPC / Oficial de Seguridad de la Información.	Formatos de valoración de riesgos y/o correos electrónicos. Matriz de riesgo actualizada.
6	Determinación, tratamiento y diseño de controles.	Procesos IDPC / Oficial de Seguridad de la Información.	Formatos de valoración de riesgos y/o correos electrónicos.
7	Publicación matriz riesgos de seguridad digital.	Oficial de Seguridad de la Información. Subdirección de gestión	Matriz de riesgos de seguridad digital.

ID	Actividades	Responsable	Productos
		Corporativa-Sistemas	
8	Seguimiento al tratamiento de riesgos de seguridad digital.	Procesos IDPC / Oficial de Seguridad de la Información.	Formatos de valoración de riesgos, actas de reunión y/o correos electrónicos.
9	Monitoreo de riesgos de seguridad digital.	Procesos IDPC / Oficial de Seguridad de la Información.	Formatos de valoración de riesgos, actas de reunión y/o correos electrónicos.

5. 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.
29/12/2023	05	Cambio de formato, se elimina la normatividad y se corrige el número de la versión	Mejora	Resultado de revisión y autocontrol.

6. Créditos

Elaboró	Revisó	Aprobó
Ángel Antonio Diaz Vega	Mary Rojas	Aura Herminda López Salazar
Cargo – Rol: Contratista – Oficial de Seguridad de la Información Subdirección de Gestión Corporativa	Cargo – Rol: Líder TI Subdirección de Gestión Corporativa	Cargo – Rol: subdirectora de la Subdirección de Gestión Corporativa. Comité Institucional de Gestión y Desempeño
Aprobado	Memorando interno con N° radicado 20235600183403 del 29-12-2023	