2024

Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

Versión: 01

Subdirección de Informática y Sistemas

SECRETARÍA DISTRITAL DE DESARROLLÓ ECONÓMICO

ALCALDÍA MAYOR DE BOGOTÁ D.C.
SECRETARÍA DE DESARROLLO ECONÓMICO
BOGOTÁ

Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

2024

Versión	Elaboró	Revisó	Aprobó	Fecha
01	**Maria Alejandra Suarez** Contratista Subdirección de Informática y Sistemas	**Adriana Montoya Ríos** Subdirectora de Informática y Sistemas	**Adriana Montoya Ríos** Subdirectora de Informática y Sistemas	29/01/2024

Versión	Control de Cambios del Plan
01	Versión para la vigencia 2024. **Aprobado en acta CIGD No.: 001 del 29/01/2024**

ALCALDÍA MAYOR
DE BOGOTÁ D.C.
SECRETARÍA DE DESARROLLO ECONÓMICO

BOGOTÁ

Tabla de Contenido

1. Objetivo General

Establecer y desarrollar un plan de acción integral para la gestión de riesgos de seguridad de la información y digital, con el objetivo primordial de preservar la integridad, confidencialidad y disponibilidad de los activos de información institucional.

1.1. Objetivos Específicos

- Identificar los riesgos asociados con cada uno de los activos de información críticos, enfocándonos en cómo estos riesgos pueden afectar la integridad, confidencialidad y disponibilidad de la información.
- Desarrollar e implementar una serie de controles personalizados y efectivos, mediante planes detallados y específicos. Estos controles estarán diseñados para abordar y mitigar los riesgos identificados asegurando la protección de los activos de información.
- Implementar estrategias proactivas para reducir la probabilidad de que los riesgos identificados afecten a los activos de información. Esto incluye no solo la implementación de controles técnicos y procedimientos, sino también la formación y concienciación de los empleados sobre prácticas de seguridad de la información.

2. Alcance

Este plan se enfocará en la identificación, evaluación y mitigación de riesgos asociados a los activos de información de la institución. Además, se incorporarán prácticas continuas de monitoreo y revisión para adaptarse a las cambiantes amenazas de seguridad y garantizar una protección efectiva de la información.

3. Definiciones y siglas

- Aceptación del riesgo: Decisión informada de tomar un riesgo particular.
- Análisis de riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de este.
- Control: Medida que modifica el riesgo.
- Evaluación de riesgos: Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.
- Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.
- Incidente de seguridad de la información: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información (Confidencialidad, Integridad y Disponibilidad). •

- Propietario del riesgo: Persona o Entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.
- Riesgo Residual: El riesgo que permanece tras el tratamiento del riesgo o nivel resultante del riesgo después de aplicar los controles.
- Riesgo de Seguridad de la Información: Probabilidad de ocurrencia de un evento que genere un impacto sobre la Confidencialidad, Integridad y Disponibilidad de la Información.
- Valoración del riesgo: Proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.
- Tratamiento del Riesgo: Proceso para modificar el riesgo.
- Triada de la información: Conjunto de las propiedades derivadas de la Confidencialidad, Integridad y Disponibilidad de la Información.
- Vulnerabilidad: Debilidad de un activo que puede ser explotada por una o más amenazas.

4. Desarrollo del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

El proceso de gestión de riesgos de seguridad de la información que se llevará a cabo en la entidad se estructura en un ciclo continuo y dinámico, alineado con las metodologías y directrices establecidas por el DAFP y el MinTIC. Este ciclo, detallado a continuación, se fundamenta en la ejecución de las actividades propuestas para asegurar una gestión efectiva y actualizada de los riesgos asociados a la seguridad de la información

4.1. Análisis de Información

El primer paso en el proceso de identificación de riesgos será la identificación, clasificación y actualización periódica de los activos de información en cada una de las áreas. Esta tarea, esencial para una gestión efectiva de la seguridad de la información, involucrará una revisión detallada y precisa de todos los activos de información, asegurando que su clasificación refleje adecuadamente su importancia y sensibilidad.

El líder de cada área desempeñará un papel clave en este proceso, será su responsabilidad no solo identificar y clasificar los activos de información, sino también realizar una priorización cuidadosa de aquellos activos que tengan una calificación de riesgo en nivel alto. Esta priorización debe basarse en criterios establecidos y objetivos, utilizando el formato designado para tal fin. Además de los activos de alto riesgo, el líder del área también deberá considerar incluir en la evaluación aquellos activos que, aunque no estén clasificados inicialmente como de alto riesgo, puedan ser relevantes para la generación y gestión de riesgos debido a su naturaleza, uso o importancia estratégica.

Esta aproximación garantiza un enfoque integral y sistematizado hacia la seguridad de la información, alineando las necesidades y riesgos específicos de cada proceso institucional con las estrategias globales de gestión de riesgos de la entidad.

4.2. Identificación de Riesgos

En la identificación de riesgos, evaluaremos amenazas y vulnerabilidades que puedan afectar nuestros activos de información, analizando sus posibles consecuencias y estimando la probabilidad e impacto en la seguridad de la información.

Este proceso implica examinar cómo cada amenaza detectada podría interrumpir o comprometer uno o varios aspectos de la triada de la información – integridad, confidencialidad y disponibilidad. Se considerarán factores como la naturaleza de la amenaza (interna o externa), la sensibilidad de los activos de información afectados, y el contexto operativo de la entidad.

Para cada riesgo identificado, se calculará tanto la probabilidad de ocurrencia como la magnitud del impacto potencial. Este enfoque dual asegura que se preste atención tanto a los riesgos altamente probables como a aquellos que, aunque menos probables, podrían tener un impacto significativo en la entidad.

Además, este proceso será dinámico y continuo, adaptándose a los cambios en el entorno de la entidad, así como a las nuevas amenazas y vulnerabilidades que surjan en el panorama de la seguridad de la información. La identificación efectiva y precisa de riesgos es un paso fundamental para desarrollar estrategias de mitigación adecuadas y garantizar una gestión integral y proactiva de los riesgos de seguridad de la información.

4.3. Evaluación y análisis del riesgo

En el proceso de gestión de riesgos, se definen criterios específicos para dos etapas clave: el análisis y la evaluación del riesgo. Estos criterios son fundamentales para garantizar un enfoque sistemático y coherente en la gestión de riesgos de seguridad de la información.

- Análisis del Riesgo: Los criterios establecidos para el análisis del riesgo deben incluir la identificación de las fuentes de riesgo, la naturaleza de las amenazas y vulnerabilidades, y la manera en que estas podrían afectar a los activos de información.

  Este análisis también debe considerar la interconexión entre diferentes riesgos y cómo estos pueden influirse mutuamente.

- Evaluación del Riesgo: Una vez analizado el riesgo, se procede a su evaluación. Este paso establece la probabilidad de ocurrencia de cada riesgo identificado, así como el nivel de consecuencia o impacto que tendría en caso de materializarse. Los criterios para esta evaluación deben ser claros y consistentes, permitiendo una estimación precisa de la zona de riesgos inherentes. Esto puede incluir el uso de escalas cuantitativas o cualitativas para medir tanto la probabilidad como el impacto, y la consideración de factores como la severidad del daño potencial, la sensibilidad de los activos afectados y la capacidad de la entidad para responder al riesgo.

4.4. Control del riesgo

En respuesta a los riesgos identificados en la gestión de la seguridad de la información, la Entidad implementará controles específicos destinados a mitigar o tratar dichos riesgos. Para la selección y aplicación de estos controles, se tomará como referencia los estándares establecidos en el Anexo de la NTC-ISO-IEC 27002:2022. Estos controles serán cuidadosamente seleccionados y adaptados a las necesidades y contextos específicos de la Entidad, con el objetivo principal de reducir la probabilidad de materialización de los riesgos asociados a incidentes de seguridad. Esto incluirá, pero no se limitará a, controles

organizativos, técnicos y físicos, así como políticas y procedimientos relevantes para asegurar la protección eficaz de la información.

4.5. Monitoreo y revisión de riesgos

Para asegurar la efectividad y relevancia continua de las estrategias de tratamiento de riesgos, la Subdirección de Sistemas e Informática llevará a cabo una revisión periódica de los avances del plan de tratamiento de riesgos de seguridad de la información. Esta revisión se realizará cuatrimestralmente. Este monitoreo incluirá la evaluación del desempeño de los controles implementados, la identificación de nuevas vulnerabilidades o cambios en el panorama de riesgos y, si es necesario, la realización de ajustes en el plan para mejorar su eficacia.

Estos ajustes y complementos refuerzan la importancia de un enfoque sistemático y continuo en la gestión de riesgos de seguridad de la información, garantizando que la Entidad se mantenga resiliente y protegida contra amenazas y vulnerabilidades en un entorno digital en constante cambio.

ANEXO 1 Cronograma de Actividades

No.	ACTIVIDAD	PRESUPUESTO	RESPONSABLE	ENTREGABLE	FECHA INICIO	FECHA FIN
1	Actualizar y publicar la guía de riesgos de seguridad de la información.	Recurso humano	Responsable de la seguridad de la información	Guía publicada en la intranet	9/01/2024	31/01/2024
2	Elaborar y remitir memorando de solicitud para realizar seguimiento al plan de tratamiento de los riesgos	Recurso humano	Responsable de la seguridad de la información y subdirector de sistemas e informática	Memorando radicado en GesDoc	7/02/2024	9/02/2024
3	Identificar, analizar y evaluar los riesgos de aquellos activos de información con criticidad alta	Recurso humano	Líderes de área	Formato con riesgos identificados	12/02/2024	22/02/2024
4	Establecer controles y planes de tratamiento sobre los riesgos	Recurso humano	Líderes de área	Formato con riesgos identificados, controles y planes de mejora asociados.	12/02/2024	22/02/2024
6	Aceptar y aprobar los riesgos identificados por cada uno de los líderes de área	Recurso humano	Líderes de área	Memorando de entrega con la respectiva matriz de riesgos	23/02/2024	29/02/2024
6	Realizar seguimiento a los planes de manejo de riesgo de seguridad de la información establecidos por cada uno de los líderes de las áreas, con sus respectivas evidencias.	Recurso humano	Líderes de área Responsable de la seguridad de la información	Memorando radicado en GesDoc	2/05/2024 2/09/2024	10/05/2024 10/05/2024
7	Identificar oportunidades de mejora conforme los resultados de la evaluación del riesgo residual	Recurso humano	Responsable de la seguridad de la información	Oportunidad de mejora documentada	1/11/2024	15/12/2024