CONTENIDO

INTRODUCCIÓN

La gestión de riesgos en Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación Tecnológica permite al Instituto Municipal de Reforma Urbana y de Vivienda de Interés Social de Yumbo – IMVIYUMBO identificar, analizar y tratar los riesgos relacionados con la seguridad y privacidad de la información. Este enfoque integral refuerza la capacidad institucional para prevenir incidentes y reducir la probabilidad de que dichos riesgos afecten la operación del Instituto, garantizando la protección y confidencialidad de los datos y la continuidad de sus procesos tecnológicos.

OBJETIVO

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información tiene como objetivo identificar, gestionar y mitigar los riesgos asociados a la información que administra el Instituto Municipal de Reforma Urbana y Vivienda de Interés Social de Yumbo - IMVIYUMBO. Este plan busca garantizar la protección de la confidencialidad, integridad y disponibilidad de los datos, asegurando su manejo en cumplimiento con la normativa vigente y alineado con las mejores prácticas internacionales en materia de seguridad y privacidad.

ALCANCE

Realizar una eficiente gestión de riesgos de Seguridad Privacidad de la información, Seguridad Digital y Continuidad de la Operación de los servicios, que permita integrar en los procesos de la entidad, buenas prácticas que contribuyan a la toma de decisiones y prevenir incidentes que puedan afectar el logro de los objetivos. Adicionalmente dar los lineamientos para poder identificar, analizar, tratar, evaluar y monitorear los riesgos de seguridad y privacidad de la información en el Instituto Municipal de Reforma Urbana y de Vivienda de Interés Social de Yumbo – IMVIYUMBO.

MARCO NORMATIVO

NORMA	DESCRIPCIÓN
Decreto 103 de 2015	“por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones”
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 1377 de 2013	“Por el cual se reglamenta parcialmente la Ley 1581 de 2012, Derogado Parcialmente por el Decreto 1081 de 2015.
ISO 27001 de 2013.	Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la Información (SGSI). Requisitos.
ISO/IEC 27002:2013.	Describe los objetivos de control y controles recomendables en cuanto a seguridad de la información.
Ley 1581 de 2012	“Por la cual se dictan disposiciones generales para la protección de datos personales.”

TÉRMINOS Y DEFINICIONES

- ✓ **Riesgo:** Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.

- ✓ **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. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

- ✓ **Amenaza:** es un 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).

- ✓ **Vulnerabilidad:** es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.

- ✓ **Probabilidad:** se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando.

- ✓ **Impacto:** consecuencias que puede ocasionar a la organización la materialización del riesgo.

- ✓ **Control o Medida:** Medida que permite reducir o mitigar un riesgo.

MARCO REFERENCIAL

Política de administración de riesgos

La política de administración de riesgos del Instituto Municipal de Reforma Urbana y de Vivienda de Interés Social de Yumbo – IMVIYUMBO, tiene un carácter estratégico y está fundamentada en el Modelo Integrado de Planeación y Gestión - MIPG, la Guía para la administración del riesgo y el diseño de controles en entidades públicas, con un enfoque preventivo de evaluación permanente de la gestión y el control, promoviendo el mejoramiento continuo y la participación de todos los servidores de la entidad.

Aplica para todos los niveles y procesos de la entidad e involucra el contexto, la identificación, valoración, tratamiento, monitoreo, revisión, comunicación, consulta y el análisis de los siguientes riesgos:

- ✓ Los riesgos de gestión de proceso que pueda afectar el cumplimiento de la misión y objetivos institucionales.

- ✓ Los riesgos de posibles actos de corrupción a través de la prevención de la ocurrencia de eventos en los que se use el poder para desviar la gestión de lo público hacia un beneficio privado.

- ✓ Los riesgos de seguridad de la información que puedan afectar la confidencialidad, integridad y disponibilidad de la información de los procesos de la entidad.

- ✓ Los riesgos fiscales impiden el daño sobre recursos públicos o bienes o intereses patrimoniales de naturaleza pública.

ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

El análisis del riesgo de seguridad de la información busca establecer la probabilidad de ocurrencia de este y sus consecuencias, evaluándolos con el fin de obtener información para calificar su nivel.

Para tener en cuenta en el análisis de los riesgos identificados, se han establecido dos aspectos: probabilidad e impacto.

Por probabilidad se entiende la posibilidad de ocurrencia del riesgo y puede ser medida con criterios de frecuencia si se ha materializado, o de factibilidad teniendo en cuenta la presencia de factores internos y externos, que pueden propiciarlo, aunque éste no se haya materializado.

El impacto se mide por las consecuencias que puede ocasionar a la Entidad la materialización del riesgo. Los pasos para el análisis de los riesgos son:

Calificación del riesgo. Para la definición del impacto se debe tener en cuenta la clasificación del riesgo (estratégico, operativo, financieros, cumplimiento, tecnología, imagen) de acuerdo con la clase del riesgo y la magnitud del impacto se debe determinar el nivel en el que se encuentra.

Evaluación del riesgo. Permite comparar los resultados de la calificación, con los criterios definidos para establecer el grado de exposición al riesgo; de esta forma, se define la zona de ubicación del riesgo inherente (antes de la definición de controles). La evaluación del riesgo se calcula con base en variables cuantitativas y cualitativas.

Con la evaluación del riesgo, previa a la formulación de controles, se obtiene la ubicación del riesgo en la matriz de evaluación; esto se denomina evaluación del riesgo inherente.

DESARROLLO PRÁCTICO:

Identificar los Riesgos: El líder de proceso, en coordinación con su equipo de trabajo, llevará a cabo el ejercicio de identificación de riesgos en materia de seguridad y privacidad de la información aplicables a su proceso.

La identificación comprende los siguientes pasos:

Establecimiento del contexto:
Los integrantes de cada proceso deberán analizar los factores internos (tanto de la organización como del proceso) y externos que afecten o puedan afectar su operación, dentro de los cuales pueden estar los siguientes:

Factores externos: se podrán considerar factores relacionados con el entorno político, económico, social, cultural, tecnológico, legal, ambiental, entre otros.

Factores internos (a nivel organizacional):
Incluyen variables como: Disponibilidad y asignación de personal, recursos presupuestales, competencias y capacidades del personal, condiciones de seguridad y salud en el trabajo, Coordinación y articulación entre procesos, estructura y cultura organizacional, gestión del conocimiento, disponibilidad y calidad de datos, así como de sistemas de información, direccionamiento estratégico, aspectos tecnológicos, entre otros.

Factores internos (a nivel de proceso): se podrán analizar variables tales como: diseño del proceso, articulación, procedimientos asociados, liderazgo al interior, activos de TI del proceso, etc.

Dentro del análisis del contexto interno y de proceso se deberán identificar: las aplicaciones, servicios web, redes, información física o digital, tecnologías de la información, que se utilizan en el Instituto con las cuales tenga interacción el proceso o aquellas que sean propias del mismo.

En el establecimiento del contexto para el proceso, es importante considerar los ejercicios similares que se hayan realizado a nivel estratégico (corporativo), dado que los mismos serán la base para el análisis a nivel de proceso. De igual forma, se deberán identificar y analizar el estado de los activos de TI con los que cuente el proceso.

¿Qué son los activos?	¿Por qué identificar los activos?
Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos elementos tales como: -Aplicaciones de la organización	Permite determinar **qué es lo más importante que cada entidad y sus procesos poseen** (sean bases de datos, archivos, servidores web o aplicaciones clave para que la entidad pueda prestar sus servicios).

Fuente: *Guía administración de riesgos y el diseño de controles en las entidades públicas DAFP*

¿Qué son los activos?	¿Por qué identificar los activos?
-Servicios web -Redes -Información física o digital -Tecnologías de información TI -Tecnologías de operación TO que utiliza la organización para funcionar en el entorno digital	La entidad puede saber **qué es lo que debe proteger para garantizar tanto su funcionamiento interno como su funcionamiento de cara al ciudadano**, aumentando así su confianza en el uso del entorno digital.

Fuente: *Guía administración de riesgos y el diseño de controles en las entidades públicas DAFP*

Valoración de los riesgos:

Es el producto de confrontar la evaluación del riesgo y los controles (preventivos o correctivos) de los procesos. La valoración del riesgo se realiza en tres momentos: primero, identificando los controles (preventivos o correctivos) que pueden disminuir la probabilidad de ocurrencia o el impacto del riesgo; luego, se deben evaluar los controles, y finalmente, con base en los resultados de la evaluación de los controles, determinar la evaluación del riesgo residual y definir la opción de manejo del riesgo.

Para esta etapa, se procederá a asociar las tablas de probabilidad e impacto.

Tabla de Probabilidad

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

Fuente: *Guía administración de riesgos y el diseño de controles en las entidades públicas DAFP*

La tabla busca realizar un cálculo más preciso de la probabilidad, considerando que, a medida que una actividad se ejecuta con mayor frecuencia, aumenta la probabilidad de que el riesgo se materialice, ya que la exposición al riesgo es mayor.

Tabla de Impacto

	Afectación Económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV .	El riesgo afecta la imagen de algún área de la organización.
Menor-40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

Fuente: *Guía administración de riesgos y el diseño de controles en las entidades públicas DAFP*

Valoración de los riesgos (riesgo residual):

En esta etapa se evaluará la probabilidad y el impacto de los riesgos identificados, considerando el efecto de los controles implementados para mitigar su materialización. Como resultado, se determinará el riesgo residual, el cual se calcula al establecer la probabilidad y el impacto del riesgo después de identificar y valorar los controles existentes. Este proceso se lleva a cabo en dos fases: (1) identificación y valoración de los controles aplicados a cada riesgo, y (2) evaluación del riesgo residual en términos de probabilidad e impacto, tomando en cuenta la efectividad de los controles identificados.

Identificación y valoración de controles:

Conceptualmente, un control se define como una medida destinada a reducir o mitigar el riesgo. Para llevar a cabo la valoración de los controles, es importante considerar los siguientes aspectos:

- ✓ La identificación de los controles debe realizarse para cada riesgo mediante mesas de trabajo con los líderes de procesos.

- ✓ Los líderes de proceso, con el apoyo de su equipo de trabajo, son responsables de implementar y monitorear los controles establecidos.

Se establece la siguiente estructura para una redacción adecuada de los controles.

- ✓ **Responsable de ejecutar el control:** Indica el cargo del líder encargado de llevar a cabo el control.
- ✓ **Acción:** Define la actividad que forma parte del control, utilizando verbos que describan claramente la tarea a realizar.
- ✓ **Complemento:** Proporciona los detalles necesarios para identificar de manera precisa el objeto del control.

Tratamiento de los riesgos

El tratamiento de los riesgos comprende dos pasos: Determinar la acción de tratamiento y Formular acciones específicas, las cuales se implementarán para reducir la probabilidad y/o mitigar el impacto del riesgo.

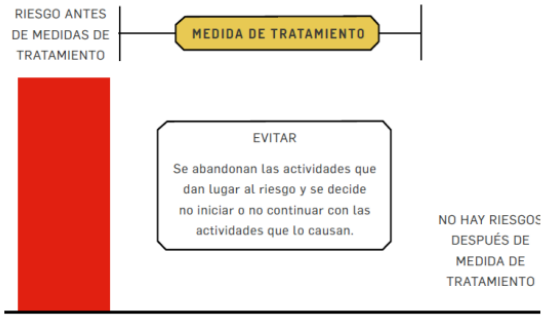
Determinar la acción de tratamiento
En este paso, se debe seleccionar una o una combinación de las acciones de tratamiento que correspondan al riesgo. Entre las acciones se tienen.

Aceptar: No se implementa ninguna medida que modifique la probabilidad o el impacto del riesgo.

Si bien la aceptación de un riesgo implica convivir con él sin poder tomar acciones adicionales, es fundamental que el proceso tenga un conocimiento completo del riesgo para poder planificar adecuadamente el desarrollo de las actividades.

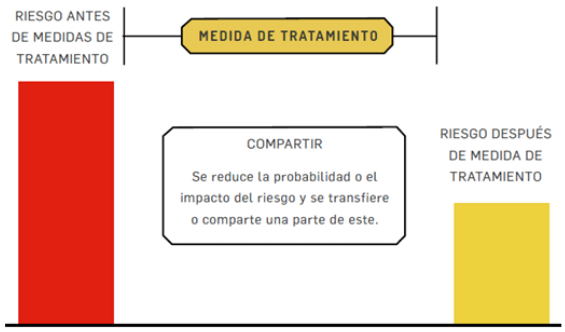
Fuente: *Guía administración de riesgos y el diseño de controles en las entidades públicas DAFP*

Evitar: Se suspenden las actividades que generan el riesgo y se decide no iniciar ni continuar con aquellas que lo provocan.



Fuente: *Guía administración de riesgos y el diseño de controles en las entidades públicas DAFP*

Reducir - Compartir: Se reduce la probabilidad o el impacto del riesgo y se transfiere o comparte una parte de éste.



Fuente: *Guía administración de riesgos y el diseño de controles en las entidades públicas DAFP*

Reducir – Mitigar: Se adoptan medidas para reducir la probabilidad o el impacto del riesgo o ambos, esto conlleva a la implementación de controles.

Fuente: *Guía administración de riesgos y el diseño de controles en las entidades públicas DAFP*

Formular acciones específicas

Una vez seleccionadas las acciones de tratamiento en el paso anterior, es necesario formular actividades específicas que permitan implementar dichas acciones de manera efectiva.

Para los riesgos clasificados en las zonas extrema y alta, se debe priorizar el registro de acciones preventivas. En el caso de los riesgos ubicados en las zonas moderada y baja, es necesario plantear acciones que mejoren los controles existentes o implementen nuevos controles, con el objetivo de reducir su probabilidad o impacto.

Es fundamental monitorear continuamente el comportamiento de los riesgos para asegurar que aquellos en las zonas extrema y alta se desplacen hacia las zonas moderada o baja y se mantengan en esta última.

Al formular acciones, debe considerarse que el control de una causa identificada para un riesgo en un proceso podría depender de otro proceso. Por ello, se requiere una articulación efectiva entre procesos, de modo que cada uno, dentro de sus competencias, documente las acciones necesarias.

Monitoreo y Seguimiento

El monitoreo de los riesgos debe realizarse de manera continua, y es responsabilidad del líder de cada proceso, apoyado por su equipo de trabajo. El líder del proceso consolidará un seguimiento trimestral de la matriz de riesgos de SPI, el cual deberá ser enviado a la Oficina Asesora de Planeación. En colaboración con los enlaces del proceso, con el propósito de centralizar los datos que posteriormente serán remitidos a la Oficina de Control Interno.

La Oficina Asesora de Planeación se encargará de consolidar un monitoreo global sobre la administración de riesgos, utilizando como insumo la información proporcionada por cada proceso y la obtenida en las mesas de trabajo. Este monitoreo será presentado al Comité Institucional de Coordinación de Control Interno para su revisión, análisis y la toma de decisiones estratégicas correspondiente.

En caso de materialización de un riesgo, el líder del proceso afectado deberá tomar acciones inmediatas para corregir la situación e implementar una acción correctiva basada en el análisis de causas. La materialización deberá ser reportada a la Oficina

de Planeación mediante correo electrónico, por el líder del proceso, y ambas partes actualizarán la información correspondiente en la matriz de riesgos de SPI.

Seguimiento de riesgos

La efectividad de los controles y cumplimiento de las acciones de mitigación de riesgos se realiza por parte de la Oficina de Control Interno. Los resultados de la evaluación y las observaciones de Control Interno serán presentados al Comité Institucional de Coordinación de Control Interno en el momento que lo considere pertinente, para que se tomen las decisiones necesarias que garanticen la sostenibilidad de la Administración de estos riesgos en IMVIYUMBO.

Matriz de Riesgos de Privacidad y seguridad de la información

El Instituto Municipal de Reforma Urbana y de Vivienda de Interés Social de Yumbo - IMVIYUMBO incluirá en su matriz de riesgos los riesgos tecnológicos y de seguridad digital, los cuales serán el objeto de tratamiento para mantener la integridad y confidencialidad de la información.

DESARROLLO DEL PLAN

Para la vigencia 2025 se establecen las actividades de acuerdo con el enfoque en Riesgos, realizando el respectivo cruce entre lo establecido en el Modelo de Seguridad y Privacidad de la Información, la Política de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, la guía para la administración del riesgo y el diseño de controles de la DAFP, y las buenas prácticas aplicables.

De igual manera se tiene en cuenta los siguientes recursos disponibles:

Humanos: Incluyen al gerente, líderes de procesos y personal de apoyo, quienes desempeñan un papel esencial en la implementación, supervisión y mantenimiento de las medidas de seguridad de la información en el instituto.

Tecnológicos: Se destacan servidores y software especializados para salvaguardar la información, asegurando su disponibilidad, confidencialidad e integridad en los procesos internos del IMVIYUMBO.

Físicos: Comprenden herramientas clave como firewalls, equipos de cómputo y dispositivos de comunicación, que respaldan la infraestructura tecnológica de la institución.

Logísticos: Gestión de recursos para realizar socializaciones, transferencia de conocimientos y seguimiento a la gestión de riesgos. Con base en lo anterior, se cuenta con recursos para plasmar acciones de mejora que permitan enfocar a la entidad hacia la meta establecida, considerando actividades concretas, medibles y alcanzables, que admitan la mejora continua.

Hoja de ruta Se establece la siguiente hoja de ruta, detallando en el plan de trabajo las actividades – tareas, responsables para la vigencia 2025.

GESTIÓN	ACTIVIDADES	TAREAS	RESPONSABLE	FECHAS PROGRAMACIÓN TAREAS VIGENCIA 2025
Gestión de Riesgos de Seguridad y Privacidad de la Información	Identificación de Activos	Inventario y clasificación de los activos de información.	Líderes de procesos con acompañamiento de la Oficina Asesora de Planeación	Marzo 2025
	Identificación de Riesgos de Seguridad y Privacidad de la Información	Identificación de Riesgos de Seguridad y Privacidad de la Información.	Proceso de Gestión TI y líderes de procesos	Abril 2025
		Revisión y verificación de los riesgos identificados (Ajustes).	Jefe Oficina Asesora de Planeación	Abril 2025
	Aprobación de Riesgos identificados	Aprobación de riesgos identificados y planes de tratamiento.	Comité Institucional de Coordinación de Control Interno y Comité Institucional de Gestión y Desempeño	Abril 2025
	. Identificación de Controles	Identificación de controles para mitigar los riesgos de Seguridad y Privacidad de la Información, considerando medidas preventivas, detectivas y correctivas.	Líderes de procesos con acompañamiento de la Oficina Asesora de Planeación	Abril 2025

	Matriz de Riesgos de Seguridad y Privacidad de la Información	Consolidar Riesgos de Seguridad y Privacidad de la Información con sus respectivos controles y planes de tratamiento en la Matriz de Riesgos de SPI.	Equipo de trabajo delegado por la Jefe Oficina Asesora de Planeación y Proceso de Gestión TI	Mayo 2025
	Monitoreo	Monitoreo a la implementación de controles y planes de tratamiento.	Jefe Oficina Asesora de Planeación	Julio 2025
	Medición	Definición y seguimiento de indicadores de desempeño.	Jefe Oficina Asesora de Planeación	Julio 2025
	Seguimiento	Seguimiento a la implementación de controles y planes de tratamiento. efectividad de los controles implementados y del nivel de riesgo residual.	Jefe Oficina de Control Interno	Agosto 2025
	Sensibilización	Socialización de lineamientos de la Gestión de Riesgos de Seguridad y privacidad de la Información.	Oficina Asesora de Planeación y Proceso de Gestión TI	Octubre 2025

Oportunidad de mejora

El Instituto Municipal de Reforma Urbana y de Vivienda de Interés Social – Yumbo - IMVIYUMBO no solo debe centrarse en la gestión de los riesgos identificados, sino también utilizar el análisis y la valoración de estos como una base para identificar oportunidades. En este contexto, la oportunidad debe entenderse como el resultado positivo derivado del tratamiento adecuado del riesgo, permitiendo mejoras significativas en los procesos.

Medición

La medición y monitoreo de este plan se realiza mediante el siguiente indicador el cual se describe a continuación:

Indicador: Cumplimiento del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

Objetivo: Monitorear el avance en la ejecución del plan de tratamiento de riesgos de seguridad y privacidad de la información.

Fórmula de cálculo:

cumplimiento (%) = (No de Actividades realizadas en el periodo/No de Actividades programada en el periodo) *100

Interpretación: Un mayor porcentaje indica un avance significativo en la ejecución del plan, reflejando la eficacia en la implementación de las actividades programadas.

Frecuencia de medición: Cuatrimestral

RUTA DE APROBACIÓN VERSION 6					
Elaboró		**Revisó**		**Aprobó**	
Nombre	Jhon Alexander Pino	Nombre	Evelyn Loaiza Gómez	Comité Institucional de Gestión y Desempeño	
Cargo	Personal de Apoyo	Cargo	Jefe Oficina Asesora de Planeación	Fecha	Acta No 110-02-06-01 24/01/2025

ANEXO

Control de Cambios

Nota: *Los documentos obsoletos se les da de baja del Sistema Integrado de Gestión Institucional.*

Versión	Fecha (dd/mm/aa)	Descripción de la actualización
1	06/07/2018	Creación del Documento.
2	29/01/2021	Actualización periodo 2021
3	17/01/2022	Actualización periodo 2022
4	20/01/2023	Actualización periodo 2023
5	24/01/2024	Actualización periodo 2024
6	24/01/2024	Actualización periodo 2025