CONTENIDO

1. OBJETIVO

Establecer los lineamientos y procedimiento para identificar, analizar, evaluar y tratar los riesgos a los que están expuestos los activos de información de la entidad comprendidos dentro del alcance del SGSI, con el fin de implementar las medidas de control necesarias para asegurar un adecuado nivel de confidencialidad, integridad y disponibilidad de la información.

2. ALCANCE

El presente procedimiento es administrado por la Unidad de Sistemas de Información y es fuente de consulta y aplicación para las áreas comprendidas en el alcance del SGSI del Área Metropolitana del Valle de Aburra. El procedimiento se inicia con la determinación del alcance para la gestión de riesgos e identificación de involucrados por parte del Profesional Universitario con especialización en seguridad de la información adscrito a la Unidad de Sistemas de Información con el rol de Oficial de Seguridad de la Información (OSI) y culmina con la implementación del Plan de Tratamiento de Riesgos.

Este procedimiento es aplicable a los procesos comprendidos dentro del alcance del SGSI, bajo la norma ISO 27001.

DOCUMENTOS A CONSULTAR
Reglamento y Funciones del Área Metropolitana del Valle de Aburra.
Manual del Sistema de Gestión Seguridad de la Información.
Serie de Normas ISO 27000.

GLOSARIO DE TÉRMINOS
CSI: Comité para la Gestión de la Información
OSI: Oficial de Seguridad de la Información
SGSI: Sistema de Gestión de Seguridad de la Información
USI: Unidad de Sistemas de Información

3. DEFINICIONES

Para efectos del presente procedimiento se consideran las siguientes definiciones, las mismas que se encuentran señaladas en la norma ISO 27002:

3.1. **Activo:** Algo que tenga valor para la entidad. Los tipos de activos pueden ser:

- Activos de Información: Archivos, bases de datos, documentación del sistema, manuales de los usuarios, material de formación, procedimientos operativos o de soporte, planes de continuidad, información archivada, etc.
- Activos de software: Software de aplicación, software del sistema, herramientas y programas de desarrollo.
- Activos físicos: Equipos de cómputo, comunicaciones, medios magnéticos u otro equipo técnico.

- Servicios: Servicios de cómputo, comunicaciones y demás servicios generales (calefacción, alumbrado, energía, aire acondicionado).
- Personas: Sus calificaciones, habilidades y experiencia.
- Intangibles: Como la reputación y la imagen institucional.

3.2. **Amenaza:** Causa potencial de un incidente no deseado que puede resultar en daño al sistema y/o entidad.
3.3. **Control:** Herramienta de la gestión del riesgo, incluido políticas, pautas, estructuras organizacionales, que pueden ser de naturaleza administrativa, técnica, gerencial o legal.
3.4. **Riesgos:** Combinación de la probabilidad de un evento y sus consecuencias.
3.5. **Vulnerabilidad:** Debilidad de un activo o grupo de activos que pueden ser explotados por una o más amenazas.

Además, se consideran las siguientes definiciones, las mismas que se encuentran señaladas en la norma ISO 27001:

3.6. **Análisis de riesgos:** Uso sistemático de información para identificar amenazas y estimar el riesgo.
3.7. **Confidencialidad:** Garantizar que la información sea accesible sólo para quienes tengan acceso autorizado.
3.8. **Disponibilidad:** Garantizar que los usuarios autorizados tengan acceso a la información y activos asociados cuando sea necesario.
3.9. Evaluación de riesgos: Proceso de comparación del riesgo estimado frente a los criterios de riesgo para determinar el significado del riesgo.
3.10. **Gestión de riesgos:** Actividades coordinadas para dirigir y controlar el riesgo en una organización.
3.11. **Incidente de seguridad de la información:** Una serie de eventos no deseados que tienen una probabilidad significativa de comprometer operaciones del negocio y amenazar la seguridad de la información.
3.12. Integridad: Salvaguardar la exactitud e integridad de la información y activos asociados.
3.13. **Riesgo residual:** Riesgo remanente después de un tratamiento del riesgo.
3.14. Seguridad de la información: Preservar la confidencialidad, integridad y disponibilidad de la información; además, también pueden ser involucradas otras características como la autenticidad, responsabilidad, no repudio y fiabilidad.
3.15. **Tratamiento de riesgos:** Proceso de selección e implementación de controles para minimizar el riesgo.

Asimismo, para el caso específico del presente procedimiento se consideran las siguientes definiciones:

3.16. **Criterio de aceptación del riesgo:** Condición, establecida formalmente, que ayuda a determinar cuáles son aquellos riesgos con los que puede convivir la entidad.

3.17. **Custodios de los activos de información:** Son los responsables de administrar, proteger y mantener los activos de información haciéndolos accesibles a los usuarios; asimismo, de monitorear el cumplimiento de los controles de seguridad en los activos que se encuentran bajo su custodia.

3.18. **Dirección:** Se refiere al nivel más alto de gerencia del proceso comprendido en el alcance del SGSI.

3.19. **Impacto:** Grado de daño legal, económico, imagen institucional y operacional que sufrirá la entidad en caso se materialice un riesgo.

3.20. **Nivel de exposición al riesgo:** Grado en el que un riesgo puede materializarse causando un impacto.

3.21. **Plan de Tratamiento de Riesgos:** Documento que contempla las decisiones relacionadas con el tratamiento de los riesgos y las acciones para la implementación de los objetivos de control y controles seleccionados.

3.22. **Probabilidad de ocurrencia del riesgo:** Probabilidad de que una amenaza explote una vulnerabilidad.

3.23. **Propietarios de los activos de información:** Son las personas o entidades responsables de garantizar la protección, mantenimiento, seguridad y uso adecuado de los activos de información empleados en los órganos o unidades orgánicas de la entidad.

3.24. **Riesgo efectivo:** Nivel de riesgos previo a un tratamiento de riesgos.

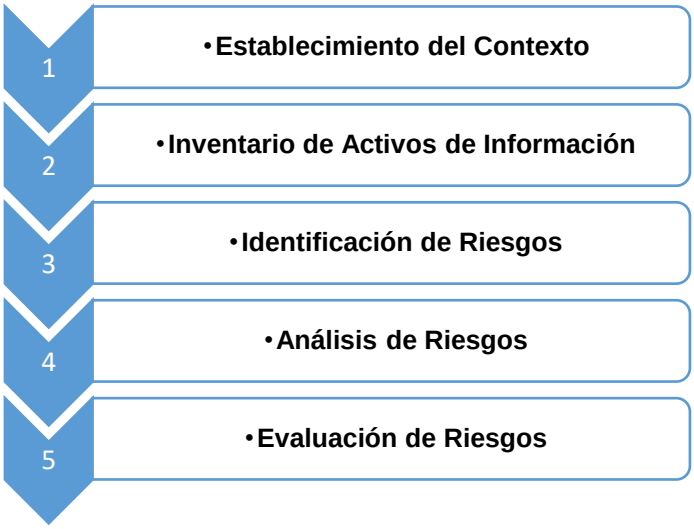
3.25. **Usuarios de los activos de información:** Son aquellas personas, llámese personal permanente, personal temporal, consultores y proveedores de bienes y/o servicios, y personas externas a la entidad que utilizan los activos de información de ésta, para el desarrollo de sus actividades.

4. CONDICIONES BÁSICAS

4.1. Se determinará el alcance para la gestión de riesgos, éste estará comprendido por el(los) proceso(s) a los cuales se les identificará sus activos de información, para su consiguiente análisis, evaluación y tratamiento de riesgos.

4.2. Para cada uno de los procesos del alcance para la gestión de riesgos se conformará un Equipo de Gestión de Riesgos, el cual estará integrado por los propietarios y custodios de los activos de información, y por el dueño del proceso; y de ser necesario, por personal de dicho proceso.

4.3. La evaluación de riesgos de seguridad de la información se llevará a cabo de acuerdo a la metodología que se presenta de manera esquemática en la siguiente figura. Dicha metodología permitirá asegurar que la evaluación de riesgos produzca resultados comparables y reproducibles.



4.4. Los resultados de la evaluación de riesgos serán revisados en un ciclo de mejora continua que se repetirá anualmente (en casos excepcionales, serán revisados oportunamente) para la identificación y coordinación de cualquier modificación pertinente; de tal forma que se asegure el control continuo de los riesgos de seguridad de la información a niveles aceptables. Para lo cual, se deberá tener en cuenta los cambios que afecten la gestión de riesgos, respecto con:

- La organización.
- La tecnología.
- Los objetivos y procesos de negocio.
- Las amenazas identificadas.
- La efectividad de los controles implementados.
- Los eventos externos, tales como cambios en el entorno legal o regulatorio, cambios en obligaciones contractuales y en el clima social.

4.5. El Equipo de Gestión de Riesgos deberá ser capacitado para llevar a cabo las actividades descritas en el presente procedimiento; asimismo deberá participar activamente y asegurar su disponibilidad para el desarrollo de dichas actividades.

5. CONDICIONES ESPECÍFICAS

5.1. Inventario de Activos de Información:

El OSI convocará reuniones con el Equipo de Gestión de Riesgos para la elaboración o actualización del Inventario de Activos de Información. Se identificarán activos de información importantes correspondientes al alcance del SGSI, sus propietarios, impactos (por pérdidas de confidencialidad, integridad y disponibilidad sobre los activos), clasificaciones de la información asociada al

activo y demás información relevante de los mismos en el formato "Inventario de Activos de Información" (Anexo B).

Los niveles de tasación de activos de información se definirán como: "Bajo", "Medio" y "Alto". En tanto, aquellos activos de información tipificados con un nivel de tasación "Bajo" o "Medio" no serán seleccionados para el análisis de riesgos.

Lo señalado en el párrafo precedente se resume en el cuadro siguiente:

Etapa	Activos no seleccionados
Inventarlo de Activos	Nivel de Tasación "Bajo" o "Medio"

Para la determinación del "Valor del Activo" se estimarán los tres (3) parámetros siguientes; según la escala de Likert, que va del uno (1) (muy bajo) al cinco (5) (muy alto):

a) Nivel de importancia de la confidencialidad del activo
b) Nivel de importancia de la integridad del activo
c) Nivel de importancia de la disponibilidad del activo

Por tanto, el "Valor del Activo" se obtendrá promediando los tres (3) valores resultantes para dichos parámetros. Asimismo, se deberá determinar el "Nivel de Tasación".

5.2. Los criterios de aceptación del riesgo para identificar los niveles del riesgo aceptables son los siguientes:

a) En la etapa de análisis de riesgos, los riesgos aceptables serán aquellos cuyo nivel de probabilidad de ocurrencia es "Bajo" o "Medio". Por tanto, los riesgos a considerar para la evaluación de riesgos serán aquellos tipificados con un nivel de probabilidad de ocurrencia "Alto".
b) En la etapa de evaluación de riesgos, los riesgos aceptables serán aquellos cuyo nivel de riesgo es "Aceptado" o "Moderado". Por tanto, los riesgos a considerar para el tratamiento de riesgos serán aquellos tipificados con un nivel de riesgo "Crítico".
c) En la etapa de tratamiento de riesgos, los riesgos aceptables serán aquellos cuyo nivel de tolerancia es "Aceptado"; ya sea porque el costo de tratamiento del riesgo se estima mayor que el impacto económico generado por su ocurrencia, o porque dicho costo está fuera de presupuesto del año en curso.

Lo señalado en los párrafos precedentes se resume en el cuadro siguiente:

Etapa	Riesgos aceptables
Análisis de riesgos	Nivel de probabilidad de ocurrencia “Bajo” o “Medio”
Evaluación de riesgos	Nivel de riesgo “Aceptado” o “Moderado”
Tratamiento de riesgos	Nivel de tolerancia “Aceptado”

5.3. Análisis de Riesgos:

El OSI convocará reuniones con el Equipo de Gestión de Riesgos para la identificación y análisis de riesgos a los que están expuestos sus activos de información, para lo cual hará uso del formato "Análisis de Riesgos de Seguridad de la Información" (Anexo C).

Se identificarán las amenazas a las que están expuestos aquellos activos de información tipificados con un nivel de tasación “Alto”. Seguidamente, se identificarán los mecanismos de protección existentes (control o controles que se encuentran implementados) frente a la amenaza; y se estimará el "Nivel de Capacidad” (grado de protección que el mecanismo de protección ha alcanzado) y el “Nivel de Amenaza”, según la escala de Likert, que va del uno (1) al cinco (5). Asimismo, se identificarán las vulnerabilidades (con su respectiva clasificación) de los activos de información que podrían ser explotadas por las amenazas identificadas previamente.

Los parámetros a tener en cuenta para la estimación de los riesgos respecto a los activos de información considerados son:

a) Grado de protección brindado por los mecanismos de protección preventivos que se encuentran implementados.
b) Grado de protección brindado por los mecanismos de protección detectores que se encuentran implementados.
c) Grado de protección brindado por los mecanismos de protección correctivos que se encuentran implementados.
d) Nivel de amenaza: Frecuencia estimada de ocurrencia.

Del promedio de los valores resultantes de los tres (3) primeros parámetros se obtendrá el “Nivel de Vulnerabilidad”.
Por tanto, la “Probabilidad de Ocurrencia del Riesgo” se obtendrá promediando los valores resultantes del nivel de vulnerabilidad y del nivel de amenaza (cuarto parámetro). Asimismo, se deberá determinar el “Nivel de Probabilidad de Ocurrencia del Riesgo".

5.4. Evaluación de Riesgos:

Para la determinación del “Nivel de Impacto” se promediarán los valores resultantes de la estimación de los tres (3) parámetros siguientes; según la escala de Likert, que va del uno (1) (muy bajo) al cinco (5) (muy alto), para lo

cual hará uso del formato "Evaluación de Riesgos de Seguridad de la Información" (Anexo D).

a. Impacto legal
b. Impacto económico / imagen institucional
c. Impacto operacional
d. Por tanto, el "Nivel de Exposición al Riesgo" se obtendrá promediando los valores resultantes de los tres (3) parámetros siguientes; para después determinar el "Nivel de Riesgo".
e. Nivel de Impacto
f. Relevancia del Activo-Valor del Activo (Obtenido en el inventario de activos)
g. Probabilidad de Ocurrencia del Riesgo (Obtenido en el análisis de riesgos)

5.5. Opciones para el Tratamiento de Riesgos:

Una vez efectuado el análisis y la evaluación de los riesgos se decidirá cuales acciones se han de tomar para el tratamiento de los riesgos. Para ello, se seguirá alguna de las siguientes opciones:

a. Reducir el riesgo: Implementar controles de seguridad de la información a fin de reducir el riesgo a niveles aceptables; esto podría ser, reduciendo el impacto (detectando eventos no deseado, reaccionando y recuperándose de ellos) si el riesgo ocurriese o reduciendo la posibilidad de que la vulnerabilidad sea explotada por la amenaza. Se utiliza cuando al implementar el control o controles trae beneficios mayores a la inversión de su implementación.
b. Aceptar el riesgo: Aceptar la posibilidad de que pueda ocurrir el riesgo sin tomar medidas de acción concretas (siempre que satisfagan claramente los criterios de aceptación del riesgo). Se utiliza cuando el costo de implementar el control o controles, en términos económicos, recursos de personal y su repercusión de tareas adicionales superan el impacto del riesgo que se desea reducir; o cuando el impacto del riesgo es mínimo.
c. Evitar el riesgo: Eliminar la fuente que genera la amenaza. Se utiliza cuando el nivel de riesgo es "Crítico", la actividad del proceso o sistema que lo genera no es de gran impacto en términos de negocio para la entidad, de modo que puede ser retirada funcionalmente.
d. Transferir el riesgo: Transferir el impacto del riesgo a terceros (empresas aseguradoras o proveedores de servicio). Se utiliza cuando no se puede reducir la probabilidad de ocurrencia del riesgo, pero su impacto es inminente.

5.6. Aquellos riesgos que son "aceptados" serán aprobados por la Dirección; para lo cual deberán contar con documentación de sustento, y cuando corresponda con la justificación de la no implementación de algún control de seguridad.

5.7. El Plan de Tratamiento de Riesgos será elaborado o actualizado de ser el caso en base a las decisiones tomadas por el CSI, respecto al modo en que serán tratados los riesgos de seguridad de la información; asimismo será aprobado por la Dirección para su correspondiente implementación. Este Plan deberá contemplar, como mínimo, lo siguiente:

a) Activo que está expuesto al riesgo.
b) Amenaza a la que está expuesto el activo.
c) Descripción detallada del control a implementar.
d) Priorización para la implementación del control.
e) Responsabilidades de los involucrados.
f) Asignación formal de recursos.
g) Plazo de tiempo estimado para la implementación del control.

5.8. Una vez implementado el Plan de Tratamiento de Riesgos se realizará la revaluación de riesgos, a fin de determinar los riesgos residuales e identificar aquellos que son aceptables, para lo cual se utilizará el formato "Tratamiento de Riesgos de Seguridad de la Información" (Anexo E). Estos riesgos residuales deberán ser comparados con los riesgos efectivos y ser propuestos para su aprobación por la Dirección.

5.9. El OSI será responsable de elaborar el Informe de Evaluación de Riesgos como resultado de la aplicación del presente procedimiento.

6. DESCRIPCIÓN DEL PROCEDIMIENTO

Nro.	Actividad	Responsable
Determinación del Alcance para la Gestión de Riesgos de Seguridad de la Información		
1	· Determinar el alcance para la gestión de riesgos · Conformar el Equipo de Gestión de Riesgos · Evaluar los cambios que afectan la gestión de riesgos (según se refiere el numeral 6.4 del presente), de ser el caso.	Profesional Universitario Rol (OSI)
Inventario de Activos de Información		
2	Coordinar con el Equipo de Gestión de Riesgos la elaboración o actualización del inventario de activos de información.	Profesional Universitario Rol (OSI)
3	Elaborar o actualizar el inventario de activos de información (según se refiere el numeral 7.1 del presente) haciendo uso del formato "Inventario de Activos de información" (Anexo B), bajo la orientación del Profesional Universitario Rol (OSI).	Equipo de Gestión de Riesgos
Identificación y Análisis de Riesgos de Seguridad de la Información		
4	Coordinar con el Equipo de Gestión de Riesgos la identificación y análisis de riesgos de seguridad de la información.	Profesional Universitario Rol (OSI)
5	Realizar en conjunto con el Profesional Universitario Rol (OSI), la identificación y análisis de riesgos de seguridad de la información (según se refiere el numeral 7.4 del presente), haciendo uso del formato "Análisis de Riesgos de Seguridad de la Información" (Anexo C).	Equipo de Gestión de Riesgos
Evaluación de Riesgos de Seguridad de la Información		

Nro.	Actividad	Responsable
6	Coordinar con el Equipo de Gestión de Riesgos la evaluación de riesgos de seguridad de la información.	Profesional Universitario Rol (OSI)
7	Realizar en conjunto con el Profesional Universitario Rol (OSI), la evaluación de riesgos de seguridad de la información (según se refiere el numeral 7.5 del presente), haciendo uso del formato "Evaluación de Riesgos de Seguridad de la Información" (Anexo D).	Equipo de Gestión de Riesgos
Tratamiento de Riesgos de Seguridad de la Información		
8	Seleccionar y proponer controles para aquellos riesgos sujetos a tratamiento, (en base a objetivos de control y controles) que permitan reducir el impacto y probabilidad de ocurrencia del riesgo al que está expuesto el activo de información, haciendo uso del formato "Tratamiento de Riesgos de Seguridad de la Información" (Anexo E). **Nota:** Los controles propuestos serán considerados en cuanto a su costo en recursos y tiempo de implementación.	Profesional Universitario Rol (OSI)
9	Validar con el Equipo de Gestión de Riesgos y áreas involucradas la viabilidad de los controles propuestos, haciendo uso del formato "Tratamiento de Riesgos de Seguridad de la Información" (Anexo E).	Profesional Universitario Rol (OSI)
10	Proponer controles y opciones para el tratamiento de cada uno de los riesgos (según se refiere el numeral 7.6 del presente) al CSI, a través del formato "Tratamiento de Riesgos de Seguridad de la Información".	Profesional Universitario Rol (OSI)
11	Evaluar y emitir su conformidad sobre las opciones propuestas para el tratamiento de cada uno de los riesgos, a fin de establecer la forma en que serán atendidos los controles propuestos para dicho riesgo.	Comité para la Gestión de la Información
12	Elaborar o actualizar de ser el caso el Plan de Tratamiento de Riesgos, en base a las decisiones tomadas por el CSI: (según se refiere el numeral 7.8 del presente) en coordinación con el Equipo de Gestión de Riesgos.	Profesional Universitario Rol (OSI)
13	Solicitar la revisión del Plan de Tratamiento de Riesgos al CSI para su aprobación por la Dirección, y su correspondiente implementación.	Profesional Universitario Rol (OSI)
14	Revisar y recomendar la aprobación del Plan de Tratamiento de Riesgos a la Dirección.	Comité para la Gestión de la Información
15	Aprobar y remitir el Plan de Tratamiento de Riesgos al CSI y a la Dirección.	Profesional Universitario Rol (OSI)
16	Coordinar con los responsables designados la implementación del Plan de Tratamiento de Riesgos.	Profesional Universitario Rol (OSI)

7. REGISTROS

DESCRIPCIÓN	CÓDIGO	LUGAR DE ARCHIVO	TIEMPO DE ARCHIVO
Inventario de Activos de Información	FO-GSI-001	Sistemas de información	Permanente
Análisis de Riesgos de Seguridad de la Información	FO-GSI-002	Sistemas de información	Permanente

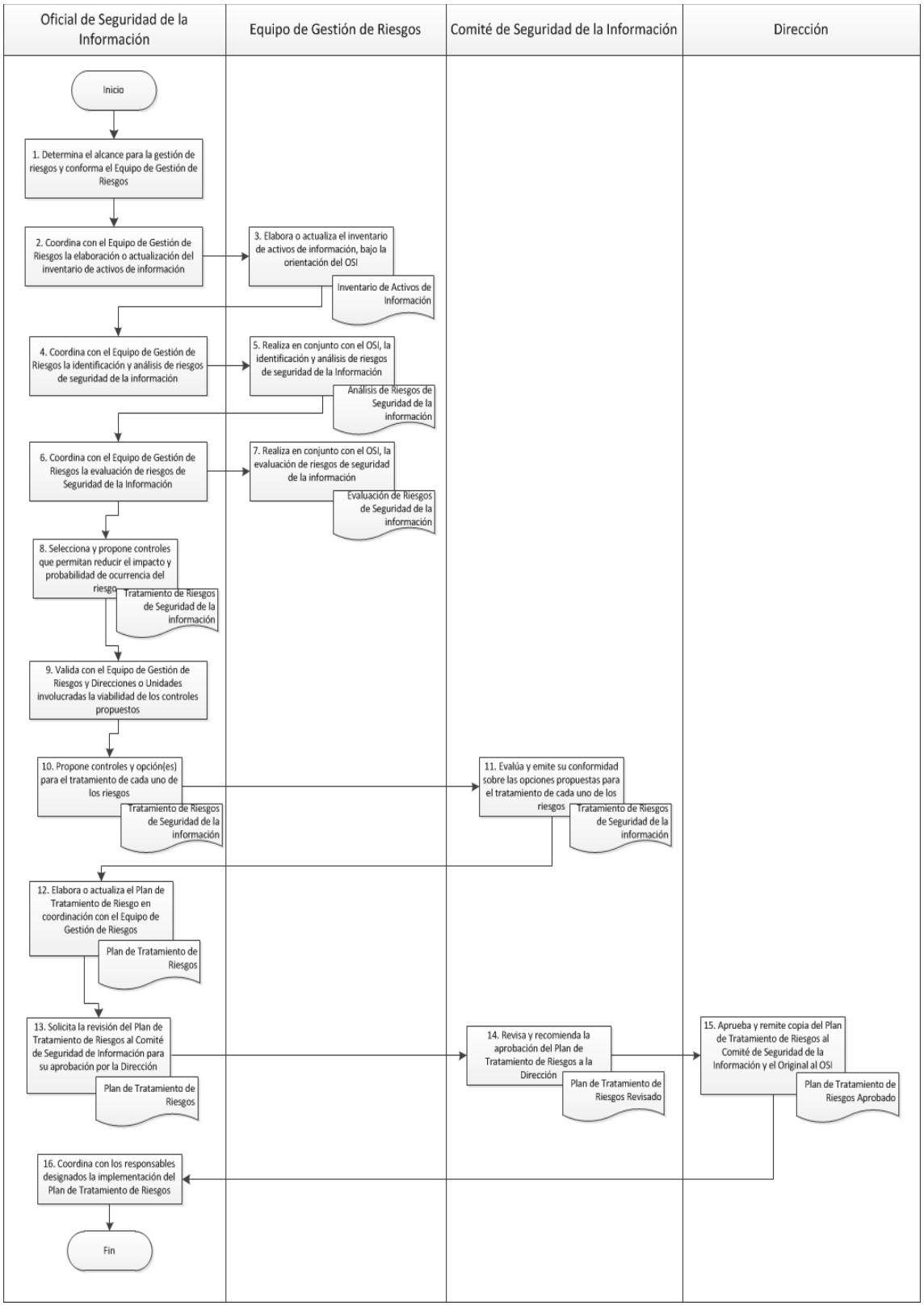
DESCRIPCIÓN	CÓDIGO	LUGAR DE ARCHIVO	TIEMPO DE ARCHIVO
Evaluación de Riesgos de Seguridad de la Información	FO-GSI-003	Sistemas de información	Permanente
Tratamiento de Riesgos de Seguridad de la Información	FO-GSI-004	Sistemas de información	Permanente
Informe de Evaluación de Riesgos	No aplica	Sistemas de información	Permanente
Plan de Tratamiento de Riesgos	No aplica	Sistemas de información	Permanente

VERSIÓN	FECHA	REVISIÓN
1	16-10-2018	Versión inicial
2	31-01-2023	Actualización de los responsables

ANEXOS

DESCRIPCIÓN	ANEXO
Diagrama de Flujo del Procedimiento	A
F-GSI-01 Formato Inventario de Activos de Información	B
F-GSI-01 Formato Análisis de Riesgos de Seguridad de la Información	C
F-GSI-01 Formato Evaluación de Riesgos de Seguridad de la Información	D
F-GSI-01 Formato Tratamiento de Riesgos de Seguridad de la Información	E

ANEXO A: DIAGRAMA DE FLUJO DEL PROCEDIMIENTO



ANEXO A: F-GSI-01 FORMATO INVENTARIO DE ACTIVOS DE INFORMACIÓN

Área METROPOLITANA Valle de Aburrá	**INVENTARIO DE ACTIVOS DE INFORMACIÓN**	Código: F-GSI-01 Versión: 01 Fecha: 17/11/2018

DATOS DEL PROCESO			
1. Nombre del Proceso		4. Cargo del Responsable	
2. Nombre de la Dependencia		5. No. ext del responsable	
3. Nombre del Responsable		6. Email del Responsable	

Nro.	Activo	Descripción	Categoría	bicación Físi	Ubicación Electrónica (Lógica)	Clasificación			Frecuencia de Uso					Propietario	Custodio	Usuario	Requisitos legales y contractuales	Valor del Activo y Nivel de Tasación				Observaciones
						Pública	Uso Interno	Confidencial	Diario	Semanal	Quincenal	Mensual	Eventual					Confidencialidad	Integridad	Disponibilidad	Valor del Activo	Nivel Tasación	
ACTIVOS DE INFORMACIÓN																						
ACTIVOS DE SOFTWARE																						
ACTIVOS FÍSICOS																						
AMENAZAS AL TALENTO HUMANO (CLIENTES, USUARIOS INTERNOS Y EXTERNOS, CIUDADANOS)																						

ANEXO B: F-GSI-01 FORMATO ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

	ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	Código: F-GSI-02 Versión: 01 Fecha: 1/11/2018

1. Nombre del Proceso	
2. Nombre de la Dependencia	

Nro.	Activo	Amenaza		Mecanismo de Protección Existente						Vulnerabilidad			Riesgo	
		Descripción	Nivel de Amenaza	Preventivo	Nivel de Capacidad	Detectivo	Nivel de Capacidad	Correctivo	Nivel de Capacidad	Descripción	Clasificación	Nivel de Vulnerabilidad	Probabilidad Ocurrencia	Nivel de Probabilidad de Ocurrencia
AMENAZAS A LOS ACTIVOS DE INFORMACIÓN														
AMENAZAS A LOS ACTIVOS DE SOFTWARE														
AMENAZAS A LOS ACTIVOS FÍSICOS														
AMENAZAS A LOS SERVICIOS (TERCEROS)														
AMENAZAS AL TALENTO HUMANO (CLIENTES, USUARIOS INTERNOS Y EXTERNOS, CIUDADANOS)														

ANEXO C: F-GSI-03 FORMATO EVALUACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Área METROPOLITANA Valle de Aburrá	**EVALUACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN**	Código: F-GSI-03 Versión: 01 Fecha: 17/12/2018

1. Nombre del Proceso	
2. Nombre de la Dependencia	

Nro.	Activo	Amenaza	Criterios de Evaluación						Riesgo Efectivo	
			Impacto				Probabilidad de Ocurrencia del Riesgo	Relevancia del Activo (Valor del Activo)	Nivel de Exposición al Riesgo	Nivel de Riesgo
			Impacto Legal	Impacto Económico / Imagen Institucional	Impacto Operacional	Nivel de Impacto				
AMENAZAS A LOS ACTIVOS DE INFORMACIÓN										
AMENAZAS A LOS ACTIVOS DE SOFTWARE										
AMENAZAS A LOS ACTIVOS FÍSICOS										
AMENAZAS A LOS SERVICIOS (TERCEROS)										
AMENAZAS AL TALENTO HUMANO (CLIENTES, USUARIOS INTERNOS Y EXTERNOS, CIUDADANOS)										

ANEXO D: F-GSI-04 FORMATO TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Área METROPOLITANA Valle de Aburrá	**TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN**	Código: F-GSI-04 Versión: 01 Fecha: 11/11/2018

1. Nombre del Proceso	
2. Nombre de la Dependencia	

Nro.	Activo	Amenaza	Riesgo Efectivo					Control Propuesto	Descripción / Observaciones	Costo Aprox.	Tiempo Aprox.	Opción del Tratamiento	Riesgo Residual													Responsable
														Vulnerabilidad						Impacto						
			Nivel Impacto	Probabilidad Ocu	Relevancia Activo	Nivel Exposición	Nivel Tolerancia						Nivel Amenaza al Ri	Mecanismo Preventivo (Nivel	Mecanismo Detectivo (Nivel	Mecanismo Correctivo (Nivel	Nivel Vulnerabilidad	Probabilidad Ocurre	Legal	Económico	Operacional	Nivel Impacto	Relevancia Activo (I	Nivel de Exposición	Nivel de Tolerancia	
AMENAZAS A LOS ACTIVOS DE INFORMACIÓN																										
AMENAZAS A LOS ACTIVOS DE SOFTWARE																										
AMENAZAS A LOS ACTIVOS FÍSICOS																										
AMENAZAS A LOS SERVICIOS (TERCEROS)																										
AMENAZAS AL TALENTO HUMANO (CLIENTES, USUARIOS INTERNOS Y EXTERNOS, CIUDADANOS)																										