POLÍTICA
ADMINISTRACIÓN GENERAL DE RIESGOS Y OPORTUNIDADES

Fecha	Versión	Identificación del Cambio
15-10-2019	01	Versión inicial del documento.
30-10-2020	02	Actualización del logo en el encabezado, cambio de título de la política, modificación del índice, actualización de la normatividad aplicable, ajuste del orden alfabético de las definiciones, inclusión de las oportunidades en la definición de roles y responsables en materia de riesgos y oportunidades, actualización de la estructura para la Gestión del Riesgo, inclusión de las tablas de probabilidad de ocurrencia y nivel de impacto de riesgos, actualización de riesgos de seguridad digital, inclusión de manejo de oportunidades
23-03-2021	03	Cambio de logo y tipo de letra, actualización de la normatividad aplicable, definiciones, estructura para la gestión del riesgo, tratamiento del riesgo, riesgos de seguridad de la información, inclusión de gestión de riesgos de corrupción. Se realizan cambios según la actualización de la Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 5. 2020

ISAURA MENDOZA M.					
Isaura Mendoza Miranda	María Alejandra Tuta Zaldúa	Aleida Lucero Gómez Quintero	Claudia Liliana Guerrero Tarazona	Luisyan López Solórzano	Néstor Enrique Rodríguez Blanco
Profesional Estrategia Empresarial	**Profesional Control de Gestión**	**Profesional Control de Gestión**	**Directora de Estrategia Empresarial**	**Asesor Gerencia General**	**Gerente General**
Elaborado por	**Revisado Por**				**Aprobado por**

ÍNDICE

1. OBJETIVO

El objetivo de esta política es dimensionar los riesgos en cada uno de los procesos, identificando y evaluando los controles existentes, e implementar nuevas acciones que los minimicen. Así como definir las oportunidades de cada uno de los procesos con el fin de gestionar su logro.

2. ALCANCE

Esta política tiene su alcance a todos los procesos definidos en el Mapa de Procesos EE-MP-001 vigente en la empresa.

3. NORMATIVIDAD APLICABLE

NORMATIVIDAD	DESCRIPCIÓN
Ley 1474 de 2011	Protocolo para la identificación de Riesgos de Corrupción asociados a la prestación de trámites y servicios
Ley 1581 de 2012	Ley de Protección de Datos Personales.
Ley 1712 de 2014	Ley de Transparencia y del Derecho al acceso de la información Pública Nacional.
NTC - ISO 9001:2015	Norma Internacional que contiene los requisitos para la implementación de un Sistema de Gestión de Calidad
Decreto 1499 de 2017	Por medio del cual se modifica el Decreto 1083 de 2015, Decreto único reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
Guía para la Administración del Riesgo y el diseño de Controles en Entidades Públicas. Versión 4. 2018	Para la gestión de riesgos de corrupción continúan vigentes los lineamientos contenidos en esta versión.
NTC - ISO 31000:2018	Estándar Internacional que proporciona los principios y directrices a seguir por las organizaciones en materia de Gestión del Riesgo.
Política de Gobierno Digital. 2018.	Lineamientos para la gestión de Riesgos de seguridad digital en entidades públicas, Anexo 4, Modelo de Gestión de Riesgos de Seguridad Digital (MGRSD)
Manual Operativo del Modelo Integrado de Planeación y Gestión (MIPG). 2019	MIPG promueve el mejoramiento continuo de las entidades, razón por la cual éstas deben establecer acciones, métodos y procedimientos de control y de gestión del riesgo, así como mecanismos para la prevención y evaluación de éste. El Control Interno es la clave para asegurar razonablemente que las demás dimensiones de MIPG cumplan su propósito.
Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 5. 2020	Metodología para la administración del riesgo en entidades públicas. Departamento Administrativo de la Función Pública.

4. DEFINICIONES

CONCEPTO	DEFINICIÓN
Activo	En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, Hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.
Apetito de riesgo	Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus Objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.
Capacidad de riesgo	Es el máximo valor del nivel de riesgo que una Entidad puede soportar y a partir del cual se considera por la Alta Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la Entidad.
Causa	Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo
Causa Inmediata	Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.
Causa Raíz	Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.
Confidencialidad	Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados
Consecuencia	Los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.
Control	Medida que permite reducir o mitigar un riesgo.
Datos Sensibles	Son aquellos datos que afectan la intimidad del titular: sexo, raza, orientación política, orientación sindical. Se prohíbe el tratamiento de este tipo de datos salvo que estén expresamente autorizados por el titular, con el fin de salvaguardar el interés vital del titular o que dicho tratamiento sea realizado por fundaciones u ONGS
Disponibilidad	Propiedad de ser accesible y utilizable a demanda por una entidad.
Factores de Riesgo	Son las fuentes generadoras de riesgos.
Fuente de Riesgos	Conjunto de factores o circunstancias que pueden generar riesgos
Identificación del Riesgo	Proceso para encontrar, reconocer y describir el riesgo
Impacto	Las consecuencias que puede ocasionar a la organización la materialización del riesgo.

CONCEPTO	DEFINICIÓN
Información Pública	Corresponde a toda información que un sujeto obligado genere, obtenga, adquiera, transforme o controle
Información Pública Clasificada	Que pertenece al ámbito propio y su acceso puede ser negado o restringido
Información Pública Reservada	Información que no es acceso al público
Integridad	Propiedad de exactitud y completitud.
Mapa de Riesgos	Documento que de manera sistemática muestra el desarrollo de las etapas de la Administración del riesgo
Materialización del Riesgo	Ocurrencia del riesgo identificado
Nivel de Impacto	Herramienta de análisis que permite identificar la fuerza de un riesgo en un proceso
Nivel de riesgo	Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos. En general la fórmula del Nivel del Riesgo poder ser Probabilidad * Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto.
Oportunidad	Aprovechar situaciones apropiadamente para obtener un provecho o cumplir un objetivo
Plan Anticorrupción y de Atención al Ciudadano	Plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal.
Probabilidad	Se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.
Proceso	Secuencia de pasos dispuesta con una lógica que se enfoca en lograr algún resultado específico. Los procesos son mecanismos de comportamiento cuyo objetivo es mejorar la productividad, establecer un orden o eliminar un problema.
Riesgo	Incertidumbre resultante de la posible ocurrencia de un evento que pueda impactar en forma negativa el cumplimiento de los objetivos de una organización
Riesgo de Corrupción	Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado
Riesgo de Cumplimiento	Posibilidad de ocurrencia de eventos que afecten la situación jurídica o contractual
Riesgo de Reputación	Posibilidad de ocurrencia de eventos que afecten la imagen o el buen nombre ante los clientes y partes interesadas

CONCEPTO	DEFINICIÓN
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).
Riesgo Estratégico	Posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos de toda la organización
Riesgo Financiero	Posibilidad de ocurrencia de eventos que afecten los estados financieros y todas aquellas áreas involucradas con el proceso financiero
Riesgo Gerencial	Posibilidad de ocurrencia de eventos que afecten los procesos gerenciales y/o la Alta Dirección
Riesgo Inherente	Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad
Riesgo Operativo	Posibilidad de ocurrencia de eventos que afecten los procesos misionales de una empresa
Riesgo residual	El resultado de aplicar la efectividad de los controles al riesgo inherente.
Riesgo Tecnológico	Posibilidad de ocurrencia de eventos que afecten la totalidad o parte de la infraestructura tecnológica
Tolerancia del riesgo	Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del Apetito de riesgo determinado por la entidad.
Vulnerabilidad	Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

5. DOCUMENTOS INTERNOS RELACIONADOS

DOCUMENTO	FECHA DE APROBACIÓN
Reglamento Interno de Trabajo	24 de noviembre de 2017 o posteriores que lo actualicen
EE-POL-001 Política de Gestión Integral	17 de diciembre de 2019 o posteriores que la actualicen
Se adopta el Modelo Integrado de Planeación y Gestión – MIPG; se crea y reglamenta el comité institucional de gestión y desempeño de la Empresa	Decisión de Gerencia 245 de 2019 o las posteriores que la derogue o actualice
Reasigna codificación de cada una de las áreas de la Empresa; modifica decisión de gerencia 235 de 2019	Decisión de Gerencia 246 de 2019 o las posteriores que la derogue o actualice
Lineamientos Generales sobre transparencia y el derecho de acceso a la información Pública	Decisión de Gerencia 247 de 2019 o las posteriores que la derogue o actualice

6. DEFINICIÓN DE ROLES Y RESPONSABLES EN MATERIA DE RIESGOS Y OPORTUNIDADES

Las responsabilidades sobre la Administración y Gestión del riesgo, al interior de Aguas de Bogotá S.A. ESP., se conforman de la siguiente forma:

6.1. GERENTE GENERAL – LÍNEA DE DEFENSA ESTRATÉGICA

- Revisa y aprueba la política de Administración General de Riesgos y Oportunidades, presentada por la Dirección de Estrategia Empresarial, así como su cumplimiento dentro de la compañía.
- Promueve la administración del riesgo y oportunidades como un componente fundamental dentro de la operación de Aguas de Bogotá S.A. ESP.
- Estipula el nivel del riesgo aceptado por la compañía.

6.2. COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO – LÍNEA DE DEFENSA ESTRATÉGICA

- Orienta y articula las acciones y estrategias para la correcta implementación, desarrollo, seguimiento y evaluación del Modelo Integrado de Planeación y Gestión – MIPG.
- Hace seguimiento a la gestión y a los resultados de las matrices de riesgos y oportunidades, teniendo en cuenta el nivel de aceptación al riesgo fijado para la compañía.

6.3. GERENTES Y LÍDERES DE PROCESOS – PRIMERA LÍNEA DE DEFENSA

- Identifica, analiza, evalúa y valora los riesgos y oportunidades de su proceso.
- Garantiza que la construcción de los riesgos y oportunidades asociados a su proceso fue participativa con todo su equipo.
- Garantiza la ejecución de los controles, su correcta documentación y aplicación.
- Realiza seguimiento periódico al comportamiento de los riesgos y oportunidades.
- En el evento de la materialización de un riesgo, debe implementar actividades de contingencia diseñadas, comunicando a la Dirección de Estrategia Empresarial.

6.4. DIRECCIÓN DE ESTRATEGIA EMPRESARIAL – SEGUNDA LÍNEA DE DEFENSA

- Generar propuestas sobre la metodología, formatos y políticas para la administración y gestión de riesgos y oportunidades de Aguas de Bogotá S.A. ESP, y, presentarlas a la Gerencia General para su aprobación.
- Promueve la activa participación de la organización en la definición de los riesgos y oportunidades.
- Coordina, lidera, capacita y asesora al personal en la metodología y políticas desarrolladas.
- Consolida el mapa de riesgos y oportunidades institucional y los socializa a las partes interesadas.
- Realiza monitoreo periódico al comportamiento de los riesgos y oportunidades.

(*) La segunda línea de defensa también está a cargo de los supervisores y coordinadores, en lo referente a la evaluación directa del monitoreo de los controles.

6.5. TRABAJADOR DESIGNADO POR LA GERENCIA – TERCERA LÍNEA DE DEFENSA

- Revisa la efectividad y la aplicación de los controles, planes de contingencia y actividades de monitoreo vinculadas a riesgos y oportunidades claves.
- Verifica que los controles estén diseñados e implementados de manera efectiva y operen.
- Realiza seguimiento a las acciones establecidas o planes de mejoramiento.
- Alerta sobre el aumento de la probabilidad de riesgo en los procesos auditados.
- Revisa los cambios en el direccionamiento estratégico o en el entorno y cómo éstos pueden afectar los riesgos actuales o generar nuevos riesgos y/o generar nuevas oportunidades.
- Revisa que se hayan identificado los riesgos significativos que afecten el cumplimiento de los objetivos de cada proceso.

6.6. RESPONSABLE DE LA SEGURIDAD DE LA INFORMACIÓN

- Define, en coordinación con la Dirección de Estrategia Empresarial, el procedimiento para la identificación, valoración de los activos digitales, así como de los riesgos existentes. Este procedimiento pasa a aprobación de la Gerencia General.
- Apoya en el seguimiento a los planes de tratamiento de los riesgos definidos.
- Informa a la Gerencia Administrativa y Financiera y la Gerencia General sobre cualquier variación importante en los riesgos de seguridad de la información.

7. ESTRUCTURA PARA LA GESTIÓN DEL RIESGO

Con el fin de determinar los riesgos para cada uno de los procesos de la compañía, el punto inicial es el plan estratégico con sus objetivos definidos y aprobados por los accionistas. Posteriormente se realiza la caracterización de cada uno de los procesos definidos en el alcance de esta política y sobre estos procesos se determinan los riesgos de Aguas de Bogotá S.A. ESP.

Para establecer y evaluar tanto los riesgos inherentes como residuales se cuenta con el formato ***EE-MT-005 Matriz de Gestión de Riesgos Generales,*** el cual desarrolla un esquema completo acorde con los contenidos metodológicos de la Guía para la Administración del Riesgo y el diseño de controles.

Se encuentra la totalidad de la estructura para la identificación y valoración de los riesgos por proceso de la siguiente forma:

Columna	Descripción - Lineamientos para el diligenciamiento
Referencia	Permite definir un consecutivo de riesgos. Esta información debe ser administrada por la Dirección de Estrategia Empresarial, cuando un el riesgo salga de la matriz no existirá otro riesgo con el mismo número.
Proceso	Elegir de la lista desplegable parametrizada el proceso al que pertenece el riesgo.
Área	Elegir de la lista desplegable parametrizada el área a la que pertenece el riesgo.
Impacto	Redactar de forma concreta las consecuencias que puede ocasionar en la organización la materialización del riesgo.
Causa Inmediata	Redactar de forma concreta las circunstancias bajo las cuales se presenta el riesgo, es la situación más evidente frente al riesgo.
Causa Raíz	Redactar de forma concreta la causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.
Descripción del Riesgo	Consolidar los análisis sobre impacto + causa inmediata + causa raíz, permitiendo contar con una redacción clara y concreta del riesgo identificado. Inicia con Posibilidad de+ Impacto para la entidad (Qué) + Causa Inmediata (Cómo) + Causa Raíz (Por qué)
Clasificación del Riesgo	Elegir de la lista desplegable parametrizada una de las siguientes opciones: Daños Activos Físicos, Ejecución y Administración de procesos, Fallas Tecnológicas, Fraude Externo, Fraude Interno, Relaciones Laborales, Usuarios, productos y practicas organizacionales.
Frecuencia con la cual se realiza la actividad que conlleva al riesgo	Definir el número de veces que se ejecuta la actividad durante el año, (Recuerde la probabilidad y ocurrencia del riesgo se define como el No. de veces que se pasa por el punto de riesgo en el periodo de 1 año). La matriz automáticamente hará el cálculo para el nivel de probabilidad inherente.
Criterios de Impacto	Elegir de la lista desplegable parametrizada en la cual aparecen las opciones de la tabla de Impacto. La matriz automáticamente hará el cálculo para el nivel de impacto inherente.
Zona de Riesgo Inherente	La matriz automáticamente hará el cálculo para la zona de riesgo inherente de acuerdo con información de probabilidad e impacto ingresada.
Descripción del Control	Definir el control (es) que atacan la causa raíz del riesgo: Responsable de ejecutar el control + Acción + Complemento. El control se define como la medida que permite reducir o mitigar un riesgo.
Cargo responsable de ejecutar el control	Escribir el cargo del responsable de la ejecución del control.
Afectación	Esta casilla no se diligencia, depende de la selección en la columna tipo de atributo.
ATRIBUTOS EFICIENCIA Tipo	Elegir de la lista desplegable parametrizada una de las siguientes opciones: Preventivo, Detectivo, Correctivo.
ATRIBUTOS EFICIENCIA Implementación	Elegir de la lista desplegable parametrizada una de las siguientes opciones: Automático, Manual.
ATRIBUTOS EFICIENCIA Calificación	La matriz automáticamente hará el cálculo para el control analizado
ATRIBUTOS INFORMATIVOS Documentación	Elegir de la lista desplegable parametrizada una de las siguientes opciones: Documentado, Sin documentar.
ATRIBUTOS INFORMATIVOS Frecuencia	Elegir de la lista desplegable parametrizada una de las siguientes opciones: Continua Aleatoria.
ATRIBUTOS INFORMATIVOS Evidencia	Diligenciar la evidencia correspondiente al control.

Columna	Descripción - Lineamientos para el diligenciamiento
Evaluación del Nivel de Riesgo - Nivel de Riesgo Residual	La matriz automáticamente hará el cálculo, acorde con el control o controles definidos con sus atributos analizados, lo que permitirá establecer el nivel de riesgo residual.
Tratamiento	Elegir de la lista desplegable parametrizada una de las siguientes opciones: Aceptar, Evitar, Reducir (compartir), Reducir (mitigar).
Activos Tecnológicos	Diligenciar según lo definido en el formato GAF-FM-018 Gestión del Riesgo de la Seguridad Digital – Activos, solo para riesgos de seguridad de la información.
Plan de Acción Descripción de la Acción, Cargo Responsable, fecha implementación, fecha seguimiento, seguimiento.	Estas casillas dependerán del tratamiento establecido, si es Aceptar no se requieren acciones adicionales, en caso de escoger Reducir (mitigar) se deben diligenciar las acciones que se adelantarán como complemento a los controles establecidos, no necesariamente son controles adicionales. Para Reducir (compartir), es viable diligenciar la acción que deriva de esta (ejemplo póliza seguros, tercerización), indicando información relevante.
Estado	Elegir de la lista desplegable parametrizada una de las siguientes opciones: Finalizado, En curso, la selección en este caso dependerá de las acciones del plan que se hayan establecido en cada caso.
Plan de Mejora	Elegir de la lista desplegable parametrizada con las opciones sí o no la respuesta a la pregunta ¿Se necesita Plan de Mejora?, en caso de responder la opción Sí, describir las acciones necesarias.

La probabilidad de ocurrencia de un riesgo (posibilidad de ocurrencia de un evento) se encuentra en las siguientes categorías:

	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%

El nivel de impacto está determinado por el daño, que, de materializarse el riesgo, podría afectar el cumplimiento de los objetivos estratégicos. Los niveles de impacto son los siguientes:

	Afectación Económica (o presupuestal)	Pérdida Reputacional
Leve 20%	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de alguna 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 publicitarios sostenible a nivel país

Entre el nivel de impacto y la probabilidad de ocurrencia se determina el nivel del riesgo. La matriz automáticamente lo determina indicando si es Bajo, Moderado, Alto y Extremo; cada uno aparece con un color, así:

NIVEL DEL RIESGO
Bajo
Moderado
Alto
Extremo

La Gerencia General de Aguas de Bogotá ha determinado que todos los riesgos inherentes requieren tratamiento y análisis de los controles existentes. Una vez determinado el nivel del riesgo, se diligencian los controles existentes para cada riesgo.

Luego de realizar la evaluación del riesgo y valoración de controles automáticamente se determina el nivel de riesgo residual.

La Gerencia General ha determinado que los riesgos residuales bajos se aceptan y el resto es necesario implementar tratamiento.

Como anexos a la matriz de gestión de riesgos generales y con el objetivo de facilitar su diligenciamiento y comprensión se tienen: mapa de calor inherente, mapa de calor residual, criterios para definir el nivel de probabilidad, criterios para definir el nivel de impacto y atributos para el diseño del control.

8. TRATAMIENTO DEL RIESGO

Una vez tengamos los riesgos residuales de cada proceso y ya definida la política de aceptación, se procede al tratamiento de los riesgos que consiste en el establecimiento, de alguna de las siguientes categorías, por parte del dueño del proceso:

- **ACEPTAR EL RIESGO**: No se adopta ninguna medida para evitar la materialización del riesgo. La Gerencia General define que los riesgos de nivel bajo se aceptan.
- **REDUCIR EL RIESGO**: Se implementan controles para reducir su probabilidad o impacto.
- **EVITAR EL RIESGO:** Se abandonan las actividades que dan lugar al riesgo, siempre y cuando no sea una actividad crítica.
- **COMPARTIR EL RIESGO**: Se transfiere parte de su probabilidad o impacto.

En el formato ***EE-MT-005 Matriz de Gestión de Riesgos Generales***, se realiza el tratamiento de riesgos con el apoyo de la Dirección de Estrategia Empresarial, cada Gerente o líder del Proceso, implementa el control más adecuado para minimizar el riesgo. Está a cargo del trabajador designado por la Gerencia General como tercera línea de defensa, entre otras funciones, la de monitorear los controles.

En la matriz, ***EE-MT-005 Matriz de Gestión de Riesgos Generales,*** para la opción de tratamiento del riesgo cuenta con una lista desplegable donde están las opciones: Aceptar, Evitar, Reducir (compartir), Reducir (mitigar).

En cuanto a las casillas de plan de acción, cargo responsable, fecha implementación, fecha seguimiento, seguimiento deben ser definidas por cada líder del proceso y/o gerente.

El trabajador designado por la Gerencia General como tercera línea de defensa, tiene entre otras funciones, la de realizar seguimiento periódico al cumplimiento de las acciones; se han definido dos (2) seguimientos anuales con el fin de generar alertas y recomendaciones de acuerdo con el avance de cada acción.

Se cuenta con las casillas del estado final de cada acción la cual tiene una lista desplegable con las opciones finalizado y en curso, por último, se tienen las columnas correspondientes al plan de mejora al que haya lugar.

9. RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Vale la pena contar con un capítulo aparte para los riesgos tecnológicos, qué, aunque su tratamiento es el mismo que para los otros tipos de riesgos, son de especial cuidado por su criticidad, confidencialidad y completitud en buena parte de los procesos de la organización. Es por esta

razón que el responsable de la seguridad de la información, designado por la Gerencia General, debe diligenciar el Formato ***GAF-FM-018 Gestión del Riesgo de la Seguridad Digital – Activos*** cuyo objetivo es definir cada uno de los activos digitales; cuenta dicho formato con las siguientes columnas, la mayoría de ellas con lista desplegable:

- **PROCESO AL QUE PERTENECE EL ACTIVO:** Se elige de la lista despegable.
- **ACTIVO:** Se elige de la lista despegable.
- **DUEÑO DEL ACTIVO (CARGO):** Debe ser diligenciado
- **TIPO DE ACTIVO:** Se elige de la lista despegable.
- **BREVE DESCRIPCIÓN:** debe ser corto, claro y concreto; no cuenta con lista desplegable.
- **CLASIFICACIÓN DE LA INFORMACIÓN:** Ley 1712 de 2014, la información puede ser pública, pública clasificada, pública reservada o no aplica. Para la aplicación de la Ley 1581 de 2012, dicha información puede contener datos personales (sensibles), no contener datos sensibles o no le aplica. Para estas clasificaciones, el Formato cuenta con listas desplegables.
- **CRITICIDAD DEL ACTIVO:** Cuenta con lista desplegable (alta, media o baja) para cada variable que lo define, a saber, Confidencialidad, Disponibilidad, Completitud y Total de Criticidad.
- **INFRAESTRUCTURA CRÍTICA CIBERNÉTICA:** Un activo es considerado infraestructura crítica cibernética si presenta impacto social (afecta a más de 250.000 personas), impacto económico (impacta más de $464.619.736) o impacto ambiental (su recuperación es superior a 3 años). En Aguas de Bogotá S.A. ESP no se maneja infraestructura crítica cibernética; por esto, la casilla se diligencia con las siglas “N/A”.

Una vez definidos estos activos, en el Formato ***GAF-FM-018 Gestión del Riesgo de la Seguridad Digital – Activos*** se ubican en la casilla activos tecnológicos de la matriz ***EE-MT-005 Matriz de Gestión de Riesgos Generales.*** Para el resto de los riesgos no se debe diligenciar dicha casilla. La persona designada por la Gerencia General como responsable de la seguridad de la información, ubica cada activo tecnológico en el proceso correspondiente.

10. GESTIÓN DE RIESGOS DE CORRUPCIÓN

Para la gestión de riesgos de corrupción, continúan vigentes los lineamientos contenidos en la versión 4 de la Guía para la administración del riesgo y el diseño de controles en entidades públicas de 2018. Para determinar y evaluar los riesgos de corrupción se cuenta con el formato ***EE-MT-002 Matriz de Gestión de Riesgos de Corrupción.*** Esta matriz contiene las listas desplegables para facilitar el proceso de identificación del riesgo, nivel del impacto del riesgo, probabilidad de ocurrencia, valoración de controles existentes.

En la columna riesgo se debe escoger de la lista desplegable la opción corrupción, las causas pueden ser seleccionadas en listas desplegables. Un riesgo puede tener una o varias causas.

Las fuentes del riesgo, en lista desplegable, se discriminan así: Relaciones Comerciales, Relaciones Contractuales, Relaciones de Cooperación, Política, Normativas, Económicas, Grupos externos, Grupos internos, Infraestructura, Eventos Naturales, Métodos de trabajo. El tipo de riesgo está discriminado en interno o externo.
La probabilidad de ocurrencia de un riesgo (posibilidad de ocurrencia de un evento) se encuentra en las siguientes categorías:

NIVEL	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA
1	Rara vez	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales).	No se ha presentado en los últimos 5 años.
2	Improbable	El evento puede ocurrir en algún momento.	Al menos 1 vez en los últimos 5 años.
3	Posible	El evento podrá ocurrir en algún momento.	Al menos 1 vez en los últimos 2 años.
4	Probable	Es viable que el evento ocurra en la mayoría de las circunstancias.	Al menos 1 vez en el último año.
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año

El nivel de impacto está determinado por el daño, que, de materializarse el riesgo, podría afectar el cumplimiento de los objetivos estratégicos. Es importante aclarar que en el tipo de riesgo **CORRUPCION**, el nivel de impacto siempre será moderado, mayor o catastrófico, ya que uno de los principios de MIPG es evitar la corrupción en las entidades, por lo que ese tipo de riesgos siempre requiere especial atención. Los niveles de impacto son los siguientes:

NIVEL	IMPACTO (CONSECUENCIAS) CUANTITATIVO	IMPACTO (CONSECUENCIAS) CUALITATIVO
Insignificante	- Impacto que afecte la ejecución presupuestal en un valor ≥0,5%. - Pérdida de cobertura en la prestación de los servicios de la entidad ≥1%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥0,5%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥0,5% del presupuesto general de la entidad	- No hay interrupción de las operaciones de la entidad. - No se generan sanciones económicas o administrativas. - No se afecta la imagen institucional de forma significativa.
Menor	- Impacto que afecte la ejecución presupuestal en un valor ≥1%. - Pérdida de cobertura en la prestación de los servicios de la entidad ≥5%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥1%. - Pago de sanciones económicas por	- Interrupción de las operaciones de la entidad por algunas horas. - Reclamaciones o quejas de los usuarios, que implican investigaciones internas disciplinarias. - Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos.

NIVEL	IMPACTO (CONSECUENCIAS) CUANTITATIVO	IMPACTO (CONSECUENCIAS) CUALITATIVO
	incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥1% del presupuesto general de la entidad.	
Moderado	- Impacto que afecte la ejecución presupuestal en un valor ≥5%. - Pérdida de cobertura en la prestación de los servicios de la entidad ≥10%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥5%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥5% del presupuesto general de la entidad.	- Interrupción de las operaciones de la entidad por un (1) día. - Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad. - Inoportunidad en la información, ocasionando retrasos en la atención a los usuarios. - Reproceso de actividades y aumento de carga operativa. - Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación del servicio a los usuarios o ciudadanos. - Investigaciones penales, fiscales o disciplinarias.
Mayor	- Impacto que afecte la ejecución presupuestal en un valor ≥20%. - Pérdida de cobertura en la prestación de los servicios de la entidad ≥20%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥20%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥20% del presupuesto general de la entidad.	- Interrupción de las operaciones de la entidad por más de dos (2) días. - Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta. - Sanción por parte del ente de control u otro ente regulador. - Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno. - Imagen institucional afectada en el orden nacional o regional por incumplimientos en la prestación del servicio a los usuarios o ciudadanos.
Catastrófico	-Impacto que afecte la ejecución presupuestal en un valor≥50%. - Pérdida de cobertura en la prestación de los servicios ≥50%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥50%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥50% del presupuesto general de la entidad.	- Interrupción de las operaciones de la entidad por más de cinco (5) días. - Intervención por parte de un ente de control u otro ente regulador. - Pérdida de información crítica para la entidad que no se puede recuperar. - Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal. - Imagen institucional afectada en el orden nacional o regional por actos o hechos de corrupción comprobados.

Entre el nivel de impacto y la probabilidad de ocurrencia se determina el nivel del riesgo. La matriz automáticamente lo determina indicando si es Bajo, Moderado, Alto y Extremo; cada uno aparece con un color, así:

NIVEL DEL RIESGO
Bajo
Moderado
Alto
Extremo

La Gerencia General de Aguas de Bogotá ha determinado que todos los riesgos inherentes requieren tratamiento y análisis de los controles existentes. Una vez determinado el nivel del riesgo, se diligencian los controles existentes para cada causa de riesgo.

En esta matriz se analizan los controles existentes para cada causa del riesgo; recordemos que un riesgo puede tener múltiples causas. El control existente puede ser un formato, un procedimiento, la firma de un superior, etc. La evaluación del diseño del control debe responder las siguientes preguntas, las cuales tienen lista desplegable, así:

- **RESPONSABLE**: Asignado o no asignado.
- **AUTORIDAD DEL RESPONSABLE**: Adecuado o inadecuado.
- **PERIDIOCIDAD DEL CONTROL**: Oportuna o inoportuna.
- **PROPOSITO DEL CONTROL**: prevenir, detectar o no es un control.
- **CONFIABILIDAD DE LA FUENTE DE CONTROL**: confiable o no confiable.
- **SEGUIMIENTO A LAS DESVIACIONES**: Se investigan o no se investigan.
- **EVIDENCIA DEL CONTROL**: Completa, incompleta, no existe.
- **TIPO DE EVIDENCIA**: Se diligencia el tipo de la evidencia. No tiene lista desplegable.

El diligenciamiento de cada casilla de evaluación del control existente nos arroja un resultado que se mide por puntaje y nos ubica en un rango, definido de la siguiente manera:

RANGO CALIFICACIÓN DEL DISEÑO	RESULTADO (PESO EVALUACIÓN DEL DISEÑO DE CONTROL)
Fuerte	Calificación entre 96 y 100
Moderado	Calificación entre 86 y 95
Débil	Calificación inferior a 85

Luego de evaluar el diseño del control, se califica la ejecución del control con los mismos rangos que el diseño: FUERTE, MODERADO, DÉBIL.

La matriz automáticamente nos determina si hay que establecer acciones para fortalecer el control existente para cada causa del riesgo y posterior, determina el promedio de la solidez del conjunto de los controles existentes para cada riesgo. Los puntajes se muestran a continuación:

CALIFICACIÓN DE LA SOLIDEZ DEL CONJUNTO DE CONTROLES	
Fuerte	El promedio de la solidez del conjunto de controles es igual a 100
Moderado	El promedio de la solidez del conjunto de controles está entre 50 y 99
Débil	El promedio de la solidez del conjunto de controles es igual o inferior a 49

En el caso del nivel de impacto del riesgo inherente, la Gerencia General ha determinado que no se desplaza, pese a tener un conjunto de controles fuerte. En el caso de los riesgos de corrupción se puede reducir su probabilidad de ocurrencia a la categoría inferior (si era probable baja a posible), pero nunca puede quedar el nivel del riesgo inferior a moderado.

En cuanto a la opción de manejo de los riesgos de corrupción se cuenta con una lista desplegable con las opciones: reducir el riesgo, aceptar el riesgo, evitar el riesgo, compartir el riesgo, las cuales tienen el mismo tratamiento que las descripciones que se encuentran en el numeral 8 de la presente política, así mismo es necesario aclarar que los riesgos de corrupción se pueden transferir, pero no su responsabilidad.

El seguimiento al cumplimiento de las acciones correspondientes a los riesgos de corrupción se realiza con una periodicidad cuatrimestral por cada una de las líneas de defensa, según corresponda, con el fin de tener avances parciales de cada acción y se determina el plan de mejora al que haya lugar; adicionalmente la actualización de los riesgos de corrupción está a cargo de la segunda línea de defensa y se realizará como mínimo una vez al año o según la necesidad del área responsable de cada riesgo.

11. MANEJO DE OPORTUNIDADES

Dado que el monitoreo de las oportunidades le permite a Aguas de Bogotá aprovechar situaciones para alcanzar los objetivos estratégicos, se ha diseñado la ***EE-MT-009 Matriz de Oportunidades***, cuyo diligenciamiento es el siguiente:

- **PROCESO**: Se elige de la lista despegable.
- **OPORTUNIDAD:** Se describe de una manera sencilla, corta y clara.
- **TIPO DE OPORTUNIDAD**: Puede ser una oportunidad interna o externa. Lista desplegable.
- **ACCIONES PARA EL LOGRO**: Se describen de manera corta y puntual cómo se va a aprovechar la oportunidad.
- **ESTADO DE LA OPORTUNIDAD**: Casilla desplegable, seleccionar entre las opciones abierta o cerrada.
- **SEGUIMIENTO DE LA OPORTUNIDAD**: La Gerencia General ha determinado dos seguimientos anuales a las oportunidades y lo realiza la Dirección de Estrategia Empresarial en conjunto con el proceso que identificó la oportunidad.