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

AGUAS DE BARRANCABERMEJA S.A. E.S.P.

Datos de Contacto:

Empresa	AGUAS DE BARRANCABERMEJA SA ESP
NIT	900045408-1
Representante Legal	Sergio Jesus Amaris Fernandez
Documento preparado por	Rafael Andres Lastre Gomez
Conmutador	+57 6216504 +57 6102491
Fax	+57 8 5121350
Correo Notificaciones Judiciales	notificaciones@aguasdebarrancabermeja.gov.co
Correo contacto y PQRD	atenciónalciudadano@aguasdebarrancabermeja.gov.co
Sitio Web	www.aguasdebarrancabermeja.gov.co
Horario de Atención al Público	lunes a Jueves 7:00 am a 12:00 pm y de 2:00 pm a 6:00 pm y Viernes de 7:00 am a 03:00 pm
Dirección	Planta de Tratamiento de Aguas de Barrancabermeja Vía Carretera Nacional Barrio el Boston

INTRODUCCIÓN

Administración de riesgos es un método lógico y sistemático para establecer el contexto, identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados con una actividad, función o proceso de tal forma que permita a las entidades minimizar pérdidas y maximizar oportunidades.

Todos los servidores públicos, en cumplimiento de sus funciones, están sometidos a riesgos que pueden hacer fracasar una gestión; por lo tanto, es necesario tomar las medidas, para identificar las causas y consecuencias de la materialización de dichos riesgos. Por esa razón, la presente guía tiene como objetivo orientar y facilitar la implementación y desarrollo de una eficaz, eficiente y efectiva gestión del riesgo en el contexto de la seguridad y privacidad de la información, desde la identificación hasta el monitoreo; enfatizando en la importancia de la administración del riesgo, sus fundamentos teóricos y da una orientación para facilitar su identificación, reconocimiento de las causas, efectos, definición de controles y da lineamientos sencillos y claros para su adecuada gestión.

2. OBJETIVOS

2.1 Objetivo general

Definir los riesgos de seguridad y privacidad de la información contemplando: Identificación de activos de información, amenazas, vulnerabilidades, riesgos y controles, los niveles aceptables y tratamiento de riesgo en la empresa Aguas de Barrancabermeja SA ESP.

2.2 Objetivos específicos

- Realizar un análisis y valoración de los riesgos de seguridad de la información en cuanto al impacto y la probabilidad de ocurrencia.
- Identificar las medidas de protección que contribuyan al correcto tratamiento de los riesgos a través de una adecuada selección y relación de controles.

3. Alcance

El Análisis de Riesgos de Seguridad y Privacidad de la Información provee los mecanismos necesarios para identificar, analizar, evaluar y tratar de manera adecuada los riesgos asociados a los activos de información de la Empresa Aguas de Barrancabermeja SA ESP.

4. Ámbito de Aplicación

La presente Guía aplica para el Sistema Integrado de Gestión de la Empresa Aguas de Barrancabermeja SA ESP.

5. Definiciones

Para la administración del riesgo, se tendrán en cuenta los siguientes términos y definiciones:

- **Acciones asociadas:** son las acciones que se deben tomar posterior a determinar las opciones de manejo del riesgo (asumir, reducir, evitar compartir o transferir), dependiendo de la evaluación del riesgo residual, orientadas a fortalecer los controles identificados.

- **Administración de riesgos:** conjunto de etapas secuenciales que se deben desarrollar para el adecuado tratamiento de los riesgos.

- **Amenaza:** situación externa que no controla la entidad y que puede afectar su operación
- **Análisis del riesgo:** etapa de la administración del riesgo, donde se establece la probabilidad de ocurrencia y el impacto del riesgo antes de determinar los controles (análisis del riesgo inherente).
- **Asumir el riesgo:** opción de manejo donde se acepta la pérdida residual probable, si el riesgo se materializa.
- **Causa:** medios, circunstancias y/o agentes que generan riesgos.
- **Calificación del riesgo:** estimación de la probabilidad de ocurrencia del riesgo y el impacto que puede causar su materialización.
- **Compartir o transferir el riesgo:** opción de manejo que determina traspasar o compartir las pérdidas producto de la materialización de un riesgo con otras organizaciones mediante figuras como outsourcing, seguros, sitios alternos.
- **Consecuencia:** efectos que se pueden presentar cuando un riesgo se materializa.
- **Contexto estratégico:** son las condiciones internas y del entorno, que pueden generar eventos que originan oportunidades o afectan negativamente el cumplimiento de la misión y objetivos de una institución.
- **Control:** acción o conjunto de acciones que minimiza la probabilidad de ocurrencia de un riesgo o el impacto producido ante su materialización.
- **Control preventivo:** acción o conjunto de acciones que eliminan o mitigan las causas del riesgo; está orientado a disminuir la probabilidad de ocurrencia del riesgo.
- **Control correctivo:** acción o conjunto de acciones que eliminan o mitigan las consecuencias del riesgo; está orientado a disminuir el nivel de impacto del riesgo.
- **Debilidad:** situación interna que la entidad puede controlar y que puede afectar su operación.
- **Evaluación del riesgo:** resultado del cruce cuantitativo de las calificaciones de probabilidad e impacto, para establecer la zona donde se ubicará el riesgo.

- **Evitar el riesgo:** opción de manejo que determina la formulación de acciones donde se prevenga la materialización del riesgo mediante el fortalecimiento de controles identificado.
- **Frecuencia:** ocurrencia de un evento expresado como la cantidad de veces que ha ocurrido un evento en un tiempo dado.
- **Identificación del riesgo:** etapa de la administración del riesgo donde se establece el riesgo con sus causas (asociadas a factores externos e internos de riesgo), consecuencias y se clasifica de acuerdo con los tipos de riesgo definidos
- **Impacto:** medida para estimar cuantitativa y cualitativamente el posible efecto de la materialización del riesgo.
- **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
- **Opciones de manejo:** posibilidades disponibles para administrar el riesgo posterior a la valoración de los controles definidos (asumir, reducir, evitar compartir o transferir el riesgo residual).
- **Plan de contingencia:** conjunto de acciones inmediatas, recursos, responsables y tiempos establecidos para hacer frente a la materialización del riesgo y garantizar la continuidad del servicio
- **Probabilidad:** medida para estimar cuantitativa y cualitativamente la posibilidad de ocurrencia del riesgo.
- **Procedimiento:** conjunto de especificaciones, relaciones, responsabilidades, controles y ordenamiento de las actividades y tareas requeridas para cumplir con el proceso.
- **Riesgo:** eventualidad que tendrá un impacto negativo sobre los objetivos institucionales o del proceso.
- **Riesgo de corrupción:** posibilidad de que por acción u omisión, mediante el uso indebido del poder, de los recursos o de la información, se lesionen los intereses de una entidad y en consecuencia del Estado, para la obtención de un beneficio particular.
- **Riesgo inherente:** es aquel al que se enfrenta una entidad o proceso en ausencia de controles y/o acciones para modificar su probabilidad o impacto.

- **Riesgo institucional**: Son los que afectan de manera directa el cumplimiento de los objetivos o la misión institucional. Los riesgos institucionales, son producto del análisis de los riesgos por proceso y son denominados de este tipo cuando cumplen las siguientes características:

  - Los riesgos que han sido clasificados como estratégicos: en el paso de identificación deben haber sido marcados como de clase estratégica, es decir, se relacionan con el cumplimiento de objetivos institucionales, misión y visión.
  - Los riesgos que se encuentran en zona alta o extrema: después de valorar el riesgo (identificación y evaluación de controles), el riesgo residual se ubica en zonas de riesgo alta o extrema, indicando que el grado de exposición a la materialización del riesgo aún se encuentra poco controlado.
  - Los riesgos que tengan incidencia en usuario o destinatario final externo: en el caso de la materialización del riesgo la afectación del usuario externo se presenta de manera directa.
  - Los riesgos de corrupción: todos los riesgos identificados que hagan referencia a situaciones de corrupción, serán considerados como riesgos de tipo institucional.

- **Riesgo residual:** nivel de riesgo que permanece luego de determinar y aplicar controles para su administración.

- **Valoración del riesgo:** establece la identificación y evaluación de los controles para prevenir la ocurrencia del riesgo o reducir los efectos de su materialización. En la etapa de valoración del riesgo se determina el riesgo residual, la opción de manejo a seguir, y si es necesita.

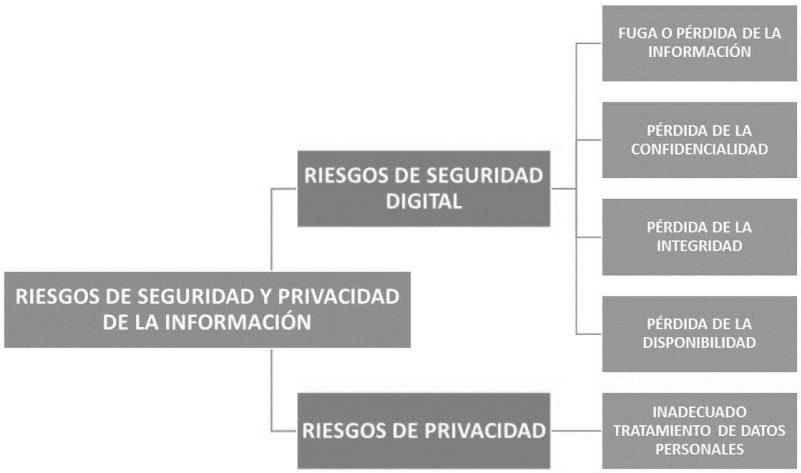
6. Contexto de Seguridad y Privacidad de la Información

La información de la Empresa Aguas de Barrancabermeja SA ESP sin importar el tipo, es crucial para el desarrollo de su objeto misional, su correcto desempeño dentro de la política pública y su relación con el ciudadano, es por ello que debe ser protegida de cualquier posibilidad de ocurrencia de eventos de riesgo de seguridad de la información y que pudiese significar un impacto indeseado generando una consecuencia negativa para el normal progreso de las actividades de la entidad. De acuerdo con lo anterior y tomando como referencia el Modelo de Seguridad y Privacidad de la información del MINTIC.

7. Riesgos de Seguridad y Privacidad de la Información

7.1 Definición del Riesgo

De acuerdo con la norma NTC-ISO/IEC 27000:2014, se define el riesgo como la "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". De igual manera el objetivo general de dicha norma es gestionar el riesgo para identificar y establecer controles efectivos que garanticen la confidencialidad, integridad y disponibilidad de la información de la Superintendencia Nacional de Salud.
De acuerdo con lo anterior y en el marco de la Política Nacional de Seguridad Digital, la estrategia de administración de riesgos para el flujo de la información en los procesos de la Empresa Aguas de Barrancabermeja SA ESP, busca diseñar una metodología ágil enfocada en la identificación, gestión y tratamiento de los Riesgos de Seguridad y Privacidad de la Información:



7.2 Riesgos de Seguridad Digital

Riesgos que resultan de la combinación de amenazas y vulnerabilidades en el ambiente digital y dado su naturaleza dinámica incluye también aspectos relacionados con el entorno físico. En la tipificación de dichos riesgos, se encuentran los siguientes:

Fuga o Pérdida de la Información: Información que hace que esta llegue a personas no autorizadas, sobre la que su responsable pierde el control o el estado que genera una condición irreparable en el tratamiento y procesamiento de la Información. Ocurre cuando un sistema de información o proceso diseñado para restringir el acceso sólo a sujetos autorizados revela parte de la información que procesa o transmite debido

a errores en la ejecución de los procedimientos de tratamiento, las personas o diseño de los Sistemas de Información.
Pérdida de la Confidencialidad: Violación o incidente a la propiedad de la información que impide su divulgación a individuos, entidades o procesos no autorizados.
Pérdida de la Integridad: Pérdida de la propiedad de mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.
Pérdida de la Disponibilidad: Pérdida de la cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

7.3 Riesgos de Privacidad

Riesgos que afectan a las personas cuyos datos son tratados y que se concreta en la posible violación de sus derechos, la pérdida de información necesaria o el daño causado por una utilización ilícita o fraudulenta de los mismos. Como riesgo tipificado se cuenta con lo siguiente:

Inadecuado Tratamiento de Datos Personales: Uso no adecuado de la información que identifica a las personas, lo que repercute en una violación de los derechos constitucionales

8. Metodología de Valoración del Activo y Análisis de Riesgos de Seguridad de la Información

La Empresa Aguas de Barrancabermeja SA ESP utiliza una metodología para valorar los riesgos de la Seguridad de la Información, basado en el Sistema de Gestión de Riesgos ya establecido en la entidad. La Matriz de Valoración de Activos y Análisis de Riesgos de Seguridad de la Información, contribuyen al Sistema Integrado de Gestión abarcando los siguientes aspectos:

Se identifican los activos de información en el flujo de cada proceso, teniendo en cuenta las Tablas de Retención Documental, con el objetivo de valorarlos e identificar los riesgos de seguridad y privacidad de la información asociada a los factores.

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

Con base en el resultado del análisis de riesgos de seguridad y privacidad de la información y con el fin de gestionar el riesgo residual, se proponen acciones de mejora los cuales pueden estar en marcha por medio de planes de acción o de tratamiento con la finalidad de que la información siempre conserve las características de confidencialidad, integridad y disponibilidad de la misma, desarrollándose como un proceso de seleccionar e implementar medidas para modificar el nivel de riesgo.

El Plan de Tratamiento de Riesgos de Seguridad de la Información se integra a la presente Guía Metodológica y a la Matriz de Valoración de Activos y Análisis de Riesgos de Seguridad de la Información, contribuyendo al fortalecimiento de los mecanismos de Gestión de Riesgos del Sistema Integrado de Gestión de la Empresa Aguas de Barrancabermeja SA ESP.

10. Establecimiento del contexto.
Consideraciones generales
Entrada: Toda la información de la Organización
Acción: El contexto para la gestión de riesgos de seguridad de la información debería ser establecida:

- Criterios Básicos
    - Criterios de Evaluación de Riesgos
    - Criterios de Impacto
    - Criterios de Aceptación de Riesgos
- Alcance y Limites
- Organización de gestión de Riesgos de seguridad de la información
    - Cargos: Responsable y Administrador del proceso de gestión de riesgos
    - Roles y responsabilidades
    - Nivel de reporte
    - Registros

Salida: Criterios Básicos, alcance, límites y organización para proceso de gestión de riesgos de seguridad**.**
Asignación de recursos: Técnicos.

Análisis de Riesgos
Identificación de Riesgos

- **Identificación de Activos**
    - **Entrada:** Alcance y límites para la gestión de riesgos de TI, lista de componentes con propietarios, ubicación, función
    - **Acción:** Los activos deberían ser identificados dentro del alcance establecido:
        - Activo
        - Propietario
        - Custodio

      Existen varios tipos de activos:
        - Software
        - Hardware
        - Documentos electrónicos y físicos
        - Personas
        - Procesos

Salida: Lista de activos de Informacion con propietarios
Asignación de Recursos: Técnicos

- **Identificación de Amenazas**
  - **Entrada:** Informacion de amenazas obtenidas de revisión de incidentes, propietarios de activos, usuarios y otras fuentes.
  - **Acción:** Amenazas y sus fuentes deben ser identificadas
  - **Salida:** Una lista de amenazas con la identificación de tipo de amenaza y fuente

  Asignación de recursos: Técnicos
- **Identificación de controles existentes**
  - **Entrada:** Documentación de controles, plan de implementación de tratamiento de riesgos
  - **Acción:** Los controles existentes y planificados deberían ser identificadas
  - **Salida:** Una lista de controles existentes y planificados, su estado de Implementacion y uso

  Asignación de Recursos: Técnicos y Económicos

11. Cronograma

CRONOGRAMA DE ACTIVIDADES PLAN DE TRATAMIENTO DE RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION																								
ACTIVIDAD	2018												2019											
	Octubre				Noviembre				Diciembre				Enero - Abril				Mayo -Agosto				Septiembre- Diciembre			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Análisis de Riesgos de Seguridad y Privacidad de la información																								
Tratamiento de Riesgos de Seguridad y Privacidad de la Informacion																								
Implementacion de actividades de tratamiento																								
Entrevista con los lideres del Proceso																								
Seguimiento y Control																								