

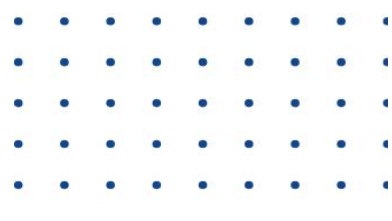






PLAN DE TRATAMIENTO Y RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION



aguas del huila
...llevamos más que agua.

2024



	AGUAS DEL HUILA S.A. E.S.P. NIT. 800.100.553-2	  
	PLAN DE TRATAMIENTO Y RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN VERSIÓN: 6.0	





INTRODUCCIÓN

La Seguridad de la Información en las empresas tiene como objetivo la protección de los activos de información en cualquiera de sus estados ante una serie de amenazas o brechas que atenten contra sus principios fundamentales de confidencialidad, integridad y su disponibilidad, a través de la implementación de medidas de control de seguridad de la información, que permitan gestionar y reducir los riesgos e impactos a que está expuesta y se logre alcanzar el máximo retorno de las inversiones en las oportunidades de negocio.

Aguas del Huila S.A. E.S.P., decide entonces vincular el modelo de administración de los riesgos de seguridad de la información y las actividades de valoración de mismos riesgos en cumplimiento de la política de seguridad de la información aprobada por la Alta Dirección, y como medio o herramienta para el logro de los objetivos de mantener la información de la Entidad confidencial, íntegra y disponible, a través de su ciclo de vida desde su captura, almacenamiento, explotación, hasta su eliminación.

Los principios de protección de la información se enmarcan en:

- **Confidencialidad:** Propiedad que la información sea concedida únicamente a quien esté autorizado.
- **Integridad:** Propiedad que la información se mantenga exacta y completa.
- **Disponibilidad:** Propiedad que la información sea accesible y utilizable en el momento que se requiera.





	AGUAS DEL HUILA S.A. E.S.P. NIT. 800.100.553-2	 ISO 9001 LL-C (Certification)  ISO 14001 LL-C (Certification)  OHSAS LL-C (Certification)
	PLAN DE TRATAMIENTO Y RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN VERSIÓN: 6.0	

OBJETIVO GENERAL

Brindar Aguas del Huila S.A. E.S.P., una herramienta con enfoque sistemático que proporcione las pautas necesarias para desarrollar y fortalecer una adecuada gestión de los riesgos de seguridad de la información, a través de métodos que faciliten la determinación del contexto estratégico, la identificación de riesgo y oportunidades, el análisis, la valoración y expedición de políticas, así como el seguimiento y monitoreo permanente enfocado a su cumplimiento y mejoramiento continuo.

OBJETIVOS ESPECIFICOS

- Brindar lineamientos y principios que propendan por la unificación de criterios para la administración de los riesgos de seguridad de la información.
- Fortalecer el sistema de gestión de riesgos de la Entidad incorporando controles y medidas de seguridad de la información que estén acordes al entorno operativo de la Entidad.
- Proteger el valor de los activos de información mediante el control de implementación de acciones de mitigación frente al riesgo y potencializar las oportunidades asociadas
- Generar una cultura y apropiación de trabajo enfocada a la identificación de los riesgos de seguridad de la información, y su mitigación.
- Reducir toda posibilidad de que una brecha o evento produzca determinado impacto bien en la información o cualquier otro activo de información asociado, a través de la gestión adecuada de los riesgos de la seguridad de la información.

	AGUAS DEL HUILA S.A. E.S.P. NIT. 800.100.553-2	  
	PLAN DE TRATAMIENTO Y RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN VERSIÓN: 6.0	





- Lograr y mantener a través de la implementación de medidas de control el nivel de probabilidad e impacto residual de los riesgos a el nivel aceptable por parte de la Alta Gerencia.

ALCANCE





La gestión de riesgos de seguridad de la información y su tratamiento, podrá ser aplicada sobre cualquier proceso de Aguas del Huila S.A. E.S.P., a cualquier sistema de información o aspecto particular de control de la Entidad, a través de los principios básicos y metodológicos para la administración de los riesgos de seguridad de la información, así como las técnicas, actividades y formularios que permitan y faciliten el desarrollo de las etapas de reconocimiento del contexto, identificación de los riesgos de seguridad de la información, análisis y evaluación, opciones de tratamiento o manejo del riesgo según la zona de riesgo; incluye además pautas y recomendaciones para su seguimiento, monitoreo y evaluación..

TERMINOS





- **Administración del riesgo:** Conjunto de elementos de control que al Interrelacionarse brindan a la entidad la capacidad para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.

	AGUAS DEL HUILA S.A. E.S.P. NIT. 800.100.553-2	 ISO 9001 <small>LL-C (Certification)</small>  ISO 14001 <small>LL-C (Certification)</small>  OHSAS <small>LL-C (Certification)</small>
	PLAN DE TRATAMIENTO Y RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN VERSIÓN: 6.0	





- **Activo de Información:** En relación con la seguridad de la información, se refiere a cualquier información o elemento de valor para los procesos de la Organización.
- **Análisis de riesgos:** Es un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.
- **Amenaza:** Es la causa potencial de una situación de incidente y no deseada por la organización
- **Causa:** Son todo aquello que se pueda considerar fuente generadora de eventos (riesgos). Las fuentes generadoras o agentes generadores son las personas, los métodos, las herramientas, el entorno, lo económico, los insumos o materiales entre otros.
- **Confidencialidad:** Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
- **Consecuencia:** Resultado de un evento que afecta los objetivos.
- **Criterios del riesgo:** Términos de referencia frente a los cuales la importancia de un riesgo se evaluada.
- **Control:** Medida que modifica el riesgo.
- **Disponibilidad:** Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

	AGUAS DEL HUILA S.A. E.S.P. NIT. 800.100.553-2	 ISO 9001 <small>LL-C (Certification)</small>  ISO 14001 <small>LL-C (Certification)</small>  OHSAS <small>LL-C (Certification)</small>
	PLAN DE TRATAMIENTO Y RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN VERSIÓN: 6.0	

- **Evaluación de riesgos:** Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.
- **Evento:** Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.
- **Estimación del riesgo:** Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.
- **Evitación del riesgo:** Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.
- **Factores de Riesgo:** Situaciones, manifestaciones o características medibles u observables asociadas a un proceso que generan la presencia de riesgo o tienden a aumentar la exposición, pueden ser internos o externos a la entidad.
- **Gestión del riesgo:** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, se compone de la evaluación y el tratamiento de riesgos.
- **Identificación del riesgo:** Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.
- **Incidente de seguridad de la información:** Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información (Confidencialidad, Integridad y Disponibilidad).
- **Integridad:** Propiedad de la información relativa a su exactitud y completitud.

	AGUAS DEL HUILA S.A. E.S.P. NIT. 800.100.553-2	 ISO 9001 <small>LL-C (Certification)</small>  ISO 14001 <small>LL-C (Certification)</small>  OHSAS <small>LL-C (Certification)</small>
	PLAN DE TRATAMIENTO Y RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN VERSIÓN: 6.0	

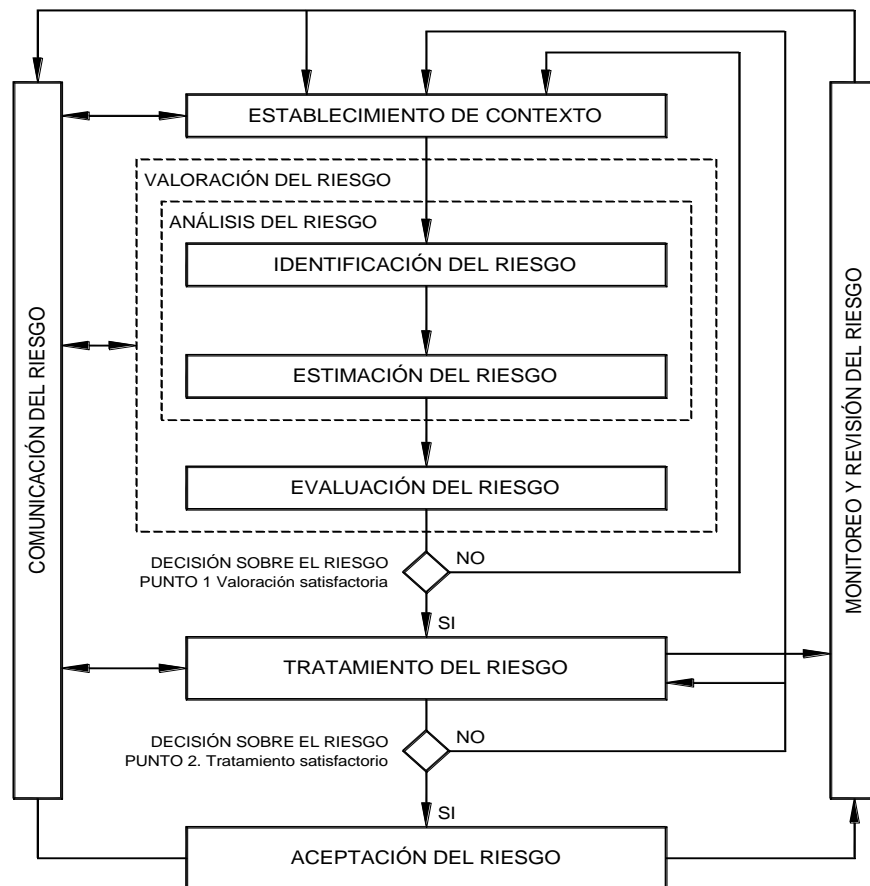
- **Impacto:** Cambio adverso en el nivel de los objetivos del negocio logrados.
- **Nivel de riesgo:** Magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de las consecuencias y su posibilidad.
- **Matriz de riesgos:** Instrumento utilizado para ubicar los riesgos en una determinada zona de riesgo según la calificación cualitativa de la probabilidad de ocurrencia y del impacto de un riesgo.
- **Monitoreo:** Mesa de trabajo anual, la cual tiene como finalidad, revisar, actualizar o redefinir los riesgos de seguridad de la información en cada uno de los procesos, partiendo del resultado de los seguimientos y/o hallazgos de los entes de control o las diferentes auditorías de los sistemas integrados de gestión.
- **Propietario del riesgo:** Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.
- **Proceso:** Conjunto de actividades interrelacionadas o que interactúan para transformar una entrada en salida.
- **Riesgo Inherente:** Es el nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.
- **Riesgo Residual:** El riesgo que permanece tras el tratamiento del riesgo o nivel resultante del riesgo después de aplicar los controles.
- **Riesgo:** Efecto de la incertidumbre sobre los objetivos.
- **Riesgo en la seguridad de la información.** Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización.

	AGUAS DEL HUILA S.A. E.S.P. NIT. 800.100.553-2	 ISO 9001 <small>LL-C (Certification)</small>  ISO 14001 <small>LL-C (Certification)</small>  OHSAS <small>LL-C (Certification)</small>
	PLAN DE TRATAMIENTO Y RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN VERSIÓN: 6.0	





- **Reducción del riesgo.** Acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo.
- **Retención del riesgo:** Aceptación de la pérdida o ganancia proveniente de un riesgo particular
- **Seguimiento:** Mesa de trabajo semestral, en el cual se revisa el cumplimiento del plan de acción, indicadores y metas de riesgo y se valida la aplicación n de los controles de seguridad de la información sobre cada uno de los procesos.
- **Tratamiento del Riesgo:** Proceso para modificar el riesgo” (Icontec Internacional, 2011).
- **Valoración del Riesgo:** Proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.
- **Vulnerabilidad:** Es aquella debilidad de un activo o grupo de activos de información
- **Seguridad de la información:** Preservación de la confidencialidad, integridad y disponibilidad de la información.
- **SGSI:** Sistema de Gestión de Seguridad de la Información.

VISION GENERAL DEL PROCESO DE GESTION DE RIESGO

A continuación, se presenta el modelo de gestión de riesgos de seguridad de la información diseñado basado tanto en la norma ISO/IEC 31000 como en la ISO 27005, adecuada para la administración de riesgos en la seguridad de la información de la entidad; los elementos que lo componen son:



CONTEXTO DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN

	AGUAS DEL HUILA S.A. E.S.P. NIT. 800.100.553-2	  
	PLAN DE TRATAMIENTO Y RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN VERSIÓN: 6.0	

El contexto de gestión de riesgos de seguridad de la información define los criterios básicos que serán necesarios para enfocar el ejercicio por parte de la entidad y obtener los resultados esperados, basándose en, la identificación de las fuentes que pueden dar origen a los riesgos y oportunidades en los procesos de Aguas del Huila S.A. E.S.P.

En el análisis de las debilidades y amenazas asociadas, en la valoración de los riesgos en términos de sus consecuencias para la Entidad y en la probabilidad de su ocurrencia, al igual que en la construcción de acciones de mitigación en beneficio de lograr y mantener niveles de riesgos aceptables.

Como criterios para la gestión de riesgos de seguridad de la información se establecen:

CRITERIOS DE EVALUACIÓN DEL RIESGO





La evaluación de los riesgos de seguridad de la información se enfocará en:

- El valor estratégico del proceso de información de Aguas del Huila S.A. E.S.P.
- La criticidad de los activos de información involucrados.
- Los requisitos legales y reglamentarios, así como las obligaciones contractuales.
- La importancia de la disponibilidad, integridad y confidencialidad para las operaciones de Aguas del Huila S.A. E.S.P.
- Las expectativas y percepciones de las partes interesadas y las consecuencias negativas para el buen nombre y reputación de la entidad

Criterios de Impacto

Los criterios de impacto se especificarán en términos del grado, daño o de los costos para Aguas del Huila S.A. E.S.P, causados por un evento de seguridad de la información, considerando aspectos tales como:

- Nivel de clasificación de los activos de información impactados

	AGUAS DEL HUILA S.A. E.S.P. NIT. 800.100.553-2	 ISO 9001 <small>LL-C (Certification)</small>  ISO 14001 <small>LL-C (Certification)</small>  OHSAS <small>LL-C (Certification)</small>
	PLAN DE TRATAMIENTO Y RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN VERSIÓN: 6.0	

- Brechas en la seguridad de la información (pérdida de la confidencialidad, integridad y disponibilidad)
- Operaciones deterioradas (afectación a partes internas o terceras partes)
- Pérdida del negocio y del valor financiero
- Alteración de planes o fechas límites
- Daños en la reputación
- Incumplimiento de los requisitos legales, reglamentarios o contractuales

Criterios de Aceptación





Los criterios de aceptación dependerán con frecuencia de las políticas, metas, objetivos de la entidad y de las partes interesadas, por tanto, las escalas de aceptación de riesgos de seguridad de información se podrán tomar del documento Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 4.

VALORACIÓN DEL RIESGO

Los riesgos se deberán identificar, describir cuantitativamente o cualitativamente y priorizarse frente a los criterios de evaluación del riesgo y los objetivos relevantes para la Aguas del Huila S.A. E.S.P., esta fase consta de las siguientes etapas:

La valoración del Riesgo de seguridad de la información consta de las siguientes actividades:

- Análisis del riesgo
- Identificación de los riesgos
- Estimación del riesgo

	AGUAS DEL HUILA S.A. E.S.P. NIT. 800.100.553-2	 ISO 9001 <small>LL-C (Certification)</small>  ISO 14001 <small>LL-C (Certification)</small>  OHSAS <small>LL-C (Certification)</small>
	PLAN DE TRATAMIENTO Y RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN VERSIÓN: 6.0	

- Evaluación del riesgo





Identificación del riesgo

Para la evaluación de riesgos de seguridad de la información en primer lugar se deberán identificar los activos de información por proceso en evaluación.

Los activos de información se clasifican en dos tipos:

a) **Primarios:**

- Procesos o subprocesos y actividades del Negocio: procesos cuya pérdida o degradación hacen imposible llevar a cabo la misión de la organización; procesos que contienen procesos secretos o que implican tecnología propietaria; procesos que, si se modifican, pueden afectar de manera muy significativa el cumplimiento de la misión de la organización; procesos que son necesarios para el cumplimiento de los requisitos contractuales, legales o reglamentarios.
- Información: información vital para la ejecución de la misión o el negocio de la organización; información personal que se puede definir específicamente en el sentido de las leyes relacionadas con la privacidad; información estratégica que se requiere para alcanzar los objetivos determinados por las orientaciones estratégicas; información del alto costo cuya recolección, almacenamiento, procesamiento y transmisión exigen un largo periodo de tiempo y/o implican un alto costo de adquisición, etc.
- Actividades y procesos de negocio: que tienen que ver con propiedad intelectual, los que si se degradan hacen imposible la ejecución de las tareas de la empresa, los necesarios para el cumplimiento legal o contractual, etc.

	AGUAS DEL HUILA S.A. E.S.P. NIT. 800.100.553-2	 ISO 9001 <small>LL-C (Certification)</small>  ISO 14001 <small>LL-C (Certification)</small>  OHSAS <small>LL-C (Certification)</small>
	PLAN DE TRATAMIENTO Y RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN VERSIÓN: 6.0	





b) De Soporte

- Hardware: Consta de todos los elementos físicos que dan soporte a los procesos (PC, portátiles, servidores, impresoras, discos, documentos en papel, etc.).
- Software: Consiste en todos los programas que contribuyen al funcionamiento de un conjunto de procesamiento de datos (sistemas operativos, paquetes de software o estándar, aplicaciones, mantenimiento o administración, etc.)
- Redes: Consiste en todos los dispositivos de telecomunicaciones utilizados para interconectar varios computadores remotos físicamente o los elementos de un sistema de información (conmutadores, cableado, puntos de acceso, etc.)
- Personal: Consiste en todos los grupos de personas involucradas en el sistema de información (usuarios, desarrolladores, responsables, etc.)
- Sitio: Comprende todos los lugares en los cuales se pueden aplicar los medios de seguridad de la organización (Edificios, sedes, y sus servicios, etc.)
- Estructura organizativa: responsables, áreas, contratistas, etc.

Después de tener una relación con todos los activos se han de conocer las amenazas que pueden causar daños en la información, los procesos y los soportes. La identificación de las amenazas y la valoración de los daños que pueden producir se puede obtener preguntando a los propietarios de los activos, usuarios, expertos, etc.

Posterior a la identificación del listado de activos, sus amenazas y las medidas que ya se han tomado, a continuación, se revisarán las vulnerabilidades que podrían aprovechar las amenazas y causar daños a los activos de información de la entidad. Existen distintos métodos para analizar amenazas, por ejemplo:

- Entrevistas con líderes de procesos y usuarios
- Inspección física
- Uso de las herramientas para el escaneo automatizado

	AGUAS DEL HUILA S.A. E.S.P. NIT. 800.100.553-2	 ISO 9001 <small>LL-C (Certification)</small>  ISO 14001 <small>LL-C (Certification)</small>  OHSAS <small>LL-C (Certification)</small>
	PLAN DE TRATAMIENTO Y RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN VERSIÓN: 6.0	

Para cada una de las amenazas analizaremos las vulnerabilidades (debilidades) que podrían ser explotadas.

Finalmente se identificarán las consecuencias, es decir, cómo estas amenazas y vulnerabilidades podrían afectar la confidencialidad, integridad y disponibilidad de los activos de información.

Estimación del riesgo



La estimación del riesgo busca establecer la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias, calificándolos y evaluándolos con el fin de obtener información para establecer el nivel de riesgo, su priorización y estrategia de tratamiento de estos. El objetivo de esta etapa es el de establecer una valoración y priorización de los riesgos.

Para adelantar la estimación del riesgo se deben considerar los siguientes aspectos:

- Probabilidad: La posibilidad de ocurrencia del riesgo, representa el número de veces que el riesgo se ha presentado en un determinado tiempo o pudiese presentarse.

Tabla. Criterios para calificar la probabilidad

NIVEL	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.
4	Probable	Es viable que el evento ocurra en la mayoría de las circunstancias.	Al menos 1 vez en el último año.

 aguas del huila ...llevarnos más que agua.	AGUAS DEL HUILA S.A. E.S.P. NIT. 800.100.553-2	 ISO 9001 LL-C (Certification)
	PLAN DE TRATAMIENTO Y RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN VERSIÓN: 6.0	

3	Posible	El evento podrá ocurrir en algún momento.	Al menos 1 vez en los últimos 2 años.
2	Improbable	El evento puede ocurrir en algún momento.	Al menos 1 vez en los últimos 5 años.
1	Rara vez	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales).	No se ha presentado en los últimos 5 años.

Fuente: Guía de Riesgos DAFP, 2018

- **Impacto:** Hace referencia a las consecuencias que puede ocasionar a la entidad la materialización del riesgo; se refiere a la magnitud de sus efectos.

Se sugiere realizar este análisis con todas o las personas que más conozcan del proceso, y que por sus conocimientos o experiencia puedan determinar el impacto y la probabilidad del riesgo de acuerdo con los rangos señalados en las tablas que se muestran más adelante.

Como criterios para la estimación del riesgo desde el enfoque de impacto y consecuencias se podrán tener en cuenta: pérdidas financieras, costes de reparación o sustitución, interrupción del servicio, disminución del rendimiento, infracciones legales, pérdida de ventaja competitiva, daños personales, entre otros.

Además de medir las posibles consecuencias se deberán analizar o estimar la probabilidad de ocurrencia de situaciones que generen impactos sobre los activos de información o la operación del negocio.





	AGUAS DEL HUILA S.A. E.S.P. NIT. 800.100.553-2	 ISO 9001 LL-C (Certification)  ISO 14001 LL-C (Certification)  OHSAS LL-C (Certification)
	PLAN DE TRATAMIENTO Y RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN VERSIÓN: 6.0	

Tabla. Criterios para calificar el impacto

NIVEL	VALOR DEL IMPACTO	CRITERIOS DE IMPACTO PARA RIESGOS DE SEGURIDAD DIGITAL	
		IMPACTO (CONSECUENCIAS) CUALITATIVO	IMPACTO (CONSECUENCIAS) CUANTITATIVO
INSIGNIFICANTE	1	<p>Afectación $\geq X\%$ de la población.</p> <p>Afectación $\geq X\%$ del presupuesto anual de la entidad.</p> <p>No hay afectación medioambiental.</p>	<p>Sin afectación de la integridad.</p> <p>Sin afectación de la disponibilidad.</p> <p>Sin afectación de la confidencialidad.</p>
MENOR	2	<p>Afectación $\geq X\%$ de la población.</p> <p>Afectación $\geq X\%$ del presupuesto anual de la entidad.</p> <p>Afectación leve del medio ambiente requiere de $\geq X$ días de recuperación.</p>	<p>Afectación leve de la integridad.</p> <p>Afectación leve de la disponibilidad.</p> <p>Afectación leve de la confidencialidad.</p>
MODERADO	3	<p>Afectación $\geq X\%$ de la población.</p> <p>Afectación $\geq X\%$ del presupuesto anual de la entidad.</p> <p>Afectación leve del medio ambiente requiere de $\geq X$ semanas de recuperación.</p>	<p>Afectación moderada de la integridad de la información debido al interés particular de los empleados y terceros.</p> <p>Afectación moderada de la disponibilidad de la información debido al interés particular de los empleados y terceros.</p> <p>Afectación moderada de la confidencialidad de la información debido al interés particular de los empleados y terceros.</p>

MAYOR	4	<p>Afectación $\geq X\%$ de la población.</p> <p>Afectación $\geq X\%$ del presupuesto anual de la entidad.</p> <p>Afectación importante del medio ambiente que requiere de $\geq X$ meses de recuperación.</p>	<p>Afectación grave de la integridad de la información debido al interés particular de los empleados y terceros.</p> <p>Afectación grave de la disponibilidad de la información debido al interés particular de los empleados y terceros.</p> <p>Afectación grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.</p>
CATASTRÓFICO	5	<p>Afectación $\geq X\%$ de la población.</p> <p>Afectación $\geq X\%$ del presupuesto anual de la entidad.</p> <p>Afectación muy grave del medio ambiente que requiere de $\geq X$ años de recuperación.</p>	<p>Afectación muy grave de la integridad de la información debido al interés particular de los empleados y terceros.</p> <p>Afectación muy grave de la disponibilidad de la información debido al interés particular de los empleados y terceros.</p> <p>Afectación muy grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.</p>

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones. 2017

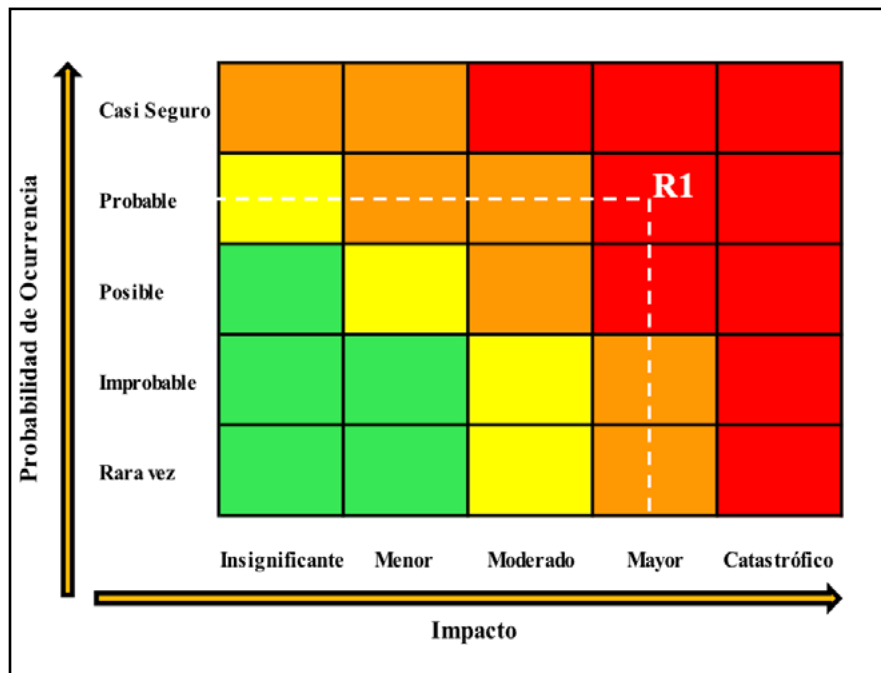
Mapa de calor

Se toma la calificación de probabilidad resultante de la tabla “Matriz de priorización de probabilidad”, para este ejemplo se tomará la probabilidad de ocurrencia en “probable” y la calificación de

impacto en “mayor”, ubique la calificación de probabilidad en la fila y la de impacto en las columnas correspondientes, establezca el punto de intersección de las dos y este punto corresponderá al nivel de riesgo, que para el ejemplo es nivel extremo – color rojo (R1), así se podrá determinar el riesgo inherente.

Extremo	
Alto	
Moderado	
Bajo	

Mapa de calor



Fuente: Adaptado de Instituto de Auditores Internos. COSO ERM. 2017.

Determinación del riesgo inherente y residual

El análisis del riesgo determinado por su probabilidad e impacto permite tener una primera evaluación del riesgo inherente (escenario sin controles) y ver el grado de exposición al riesgo que tiene la entidad. La exposición al riesgo es la ponderación de la probabilidad e impacto, y se puede ver gráficamente en la matriz de riesgo, instrumento





....llevarnos más que agua.

Calle 21 No. 1C -17

Teléfonos 8 75 31 81 – 8 75 23 21 fax: Ext. 124

www.aguasdelhuila.gov.co

Neiva – Huila (Colombia).

	AGUAS DEL HUILA S.A. E.S.P. NIT. 800.100.553-2	 ISO 9001 <small>U-C (Certification)</small>  ISO 14001 <small>U-C (Certification)</small>  OHSAS <small>U-C (Certification)</small>
	PLAN DE TRATAMIENTO Y RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN VERSIÓN: 6.0	

que muestra las zonas de riesgos y que facilita el análisis gráfico. Permite analizar de manera global los riesgos que deben priorizarse según la zona en que quedan ubicados los mismos (zona de riesgo bajo, moderado, alto o extremo) facilitando la organización de prioridades para la decisión del tratamiento e implementación de planes de acción.

EVALUACIÓN DEL RIESGO

Una vez se valoran los impactos, la probabilidad y las consecuencias de los escenarios de incidentes sobre los activos de información, se obtendrán los niveles de riesgo, para los cuales se deberán comparar frente a los criterios básicos del contexto, para una adecuada y pertinente toma de decisiones basada en riesgos de seguridad de la información y en beneficio de reducir su impacto en la Entidad.

TRATAMIENTO DEL RIESGO

Como resultado de la etapa de evaluación del riesgo tendremos una lista ordenada de riesgos o una matriz con la identificación de los niveles de riesgo de acuerdo con la zona de ubicación, por tanto, se deberá elegir la(s) estrategia(s) de tratamiento del riesgo en virtud de su valoración y de los criterios establecidos en el contexto de gestión de riesgos. De acuerdo con el nivel evaluación de los riesgos, se deberá seleccionar la opción de tratamiento adecuada por cada uno de los riesgos identificados; el costo/beneficio del tratamiento deberá ser un factor de decisión relevante para la decisión.

COSTO - BENEFICIO OPCION DE TRATAMIENTO

El nivel de riesgo está muy alejado del nivel de tolerancia, su costo y tiempo del tratamiento es muy superior a los beneficios Evitar el riesgo, su propósito es no





....llevamos más que agua.

Calle 21 No. 1C -17

Teléfonos 8 75 31 81 – 8 75 23 21 fax: Ext. 124

www.aguasdelaHuila.gov.co

Neiva – Huila (Colombia).

	AGUAS DEL HUILA S.A. E.S.P. NIT. 800.100.553-2	 ISO 9001 <small>LL-C (Certification)</small>  ISO 14001 <small>LL-C (Certification)</small>  OHSAS <small>LL-C (Certification)</small>
	PLAN DE TRATAMIENTO Y RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN VERSIÓN: 6.0	

proceder con la actividad o la acción que da origen al riesgo (ejemplo, dejando de realizar una actividad, tomar otra alternativa, etc.)

El costo del tratamiento por parte de terceros (internos o externos) es más beneficioso que el tratamiento directo Transferir o compartir el riesgo, entregando la gestión del riesgo a un tercero (ejemplo, contratando un seguro o subcontratando el servicio).





El costo y el tiempo del tratamiento es adecuado a los beneficios Reducir o Mitigar el riesgo, seleccionando e implementando los controles o medidas adecuadas que logren que se reduzca la probabilidad o el impacto

La implementación de medidas de control adicionales no generará valor agregado para reducir niveles de ocurrencia o de impacto. Retener o aceptar el riesgo, no se tomará la decisión de implementar medidas de control adicionales. Monitorizarlo para confirmar que no se incrementa

El resultado de esta fase se concreta en un plan de tratamiento de riesgos, es decir, la selección y justificación de una o varias opciones para cada riesgo identificado, que permitan establecer la relación de riesgos residuales, es decir, aquellos que aún siguen existiendo a pesar de las medidas tomadas.

Nota: Será conveniente que para la selección de los controles se consideren posibles restricciones o limitantes que impidan su elección tales como: restricciones de tiempo, financieras, técnicas, operativas, culturales, éticas, ambientales, legales, uso, de personal o las restricciones para la integración de controles nuevos y existentes.

MONITOREO Y SEGUIMIENTO DE LOS RIESGOS

	AGUAS DEL HUILA S.A. E.S.P. NIT. 800.100.553-2	 ISO 9001 <small>LL-C (Certification)</small>  ISO 14001 <small>LL-C (Certification)</small>  OHSAS <small>LL-C (Certification)</small>
	PLAN DE TRATAMIENTO Y RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN VERSIÓN: 6.0	

Periódicamente se revisará el valor de los activos, impactos, amenazas, vulnerabilidades y probabilidades en busca de posibles cambios, que exijan la valoración iterativa de los riesgos de seguridad de la información.

Los riesgos son dinámicos como la misma Entidad por tanto podrán cambiar de forma o manera radical sin previo aviso. Por ello es necesaria una supervisión continua que detecte: (1) nuevos activos o modificaciones en el valor de los activos, (2) nuevas amenazas (3) cambios o aparición de nuevas vulnerabilidades (4) aumento de las consecuencias o impactos, (5) incidentes de seguridad de la información.

Con el propósito de conocer los estados de cumplimiento de los objetivos de la gestión de los riesgos de seguridad de la información, se deberán definir esquemas de seguimiento y medición al sistema de gestión de riesgos de la seguridad de la información que permitan contextualizar una toma de decisiones de manera oportuna.

CRONOGRAMA Y VALORACIÓN DE LOS RIESGOS

La Entidad definirá y mantendrá un cronograma de actividades para la realización de la valoración de los riesgos de seguridad de la información en los procesos de la organización, basado con su criticidad y su valor para el cumplimiento de la misionalidad de Aguas del Huila S.A. E.S.P.

PLAN DE TRATAMIENTO Y RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION													
ACTIVIDAD / TAREA	RESPONSABLE	ENERO	FEBRERO	MARZO	ABRIL	MAYO	JUNIO	JULIO	AGOSTO	SEPTIEMBRE	OCTUBRE	NOVIEMBRE	DICIEMBRE
Definición y publicación del plan de tratamiento y riesgos de seguridad y privacidad de la información en la página web de la entidad	TIC												
Identificar los riesgos y amenazas a los que la entidad está expuesta en materia de seguridad y privacidad de la información	TIC												
Realizar monitoreos y evaluaciones periódicas a los riesgos y al plan de Tratamiento y riesgos de seguridad y privacidad de la información	TIC												
Capacitar a los funcionarios sobre los posibles ataques y riesgos a los que están expuestos y como se pueden mitigar	TIC												
Identificación de oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de riesgos	TIC												





....llevamos más que agua.

Calle 21 No. 1C -17

Teléfonos 8 75 31 81 – 8 75 23 21 fax: Ext. 124

www.aguasdelaHuila.gov.co

Neiva – Huila (Colombia).

	AGUAS DEL HUILA S.A. E.S.P. NIT. 800.100.553-2	 ISO 9001 <small>LL-C (Certification)</small>  ISO 14001 <small>LL-C (Certification)</small>  OHSAS <small>LL-C (Certification)</small>
	PLAN DE TRATAMIENTO Y RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN VERSIÓN: 6.0	

MARCO NORMATIVO

NORMA	OBJETO
Guía para la administración del riesgo	<i>“Guía para la administración del riesgo y el diseño de controles en entidades públicas Versión 4”</i>
Decreto 2573 de 2014	<i>“Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta la Ley 1341 de 2009 y se dictan otras disposiciones.”</i>
Decreto 1078 de 2015	<i>Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones</i>
Ley 1712 de 2014	<i>“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.”</i>

Tabla. Marco Normativo