

POLITICA DE ADMINISTRACION DEL RIESGO

AGUAS DEL HUILA S.A E.S.P.



aguas del huila

...llevamos más que agua.

[www.aguasdelhuila.gov.co]



Contenido

INTRODUCCION	3
OBJETIVO	4
OBJETIVOS ESPECIFICOS	4
ALCANCE	4
TERMINOS Y DEFINICIONES	5
MARCO NORMATIVO	6
METODOLOGIA PARA LA ADMINISTRACION DEL RIESGO	7
1. CONOCIMIENTO Y ANALISIS DE LA ENTIDAD	7
1.1 MISION	7
1.2 VISION	7
1.3 MAPA DE PROCESOS	7
2. POLITICA DE ADMINISTRACION DEL RIESGO	7
3. IDENTIFICACION DEL RIESGO	8
4. EVALUACIÓN DEL RIESGO	13
LINEAS DE DEFENSA	14
PRIMERA LINEA DE DEFENSA	14
SEGUNDA LINEA DE DEFENSA	14
TERCERA LINEA DE DEFENSA	14
APLICABILIDAD	15
NIVEL DE CUMPLIMIENTO	15
EVALUACION Y SEGUIMIENTO	15
RECOMENDACIONES	15
VIGENCIA	16

INTRODUCCION

La política de Administración de Riesgo de Aguas del Huila S.A E.S.P. en pro del cumplimiento de su misión y estrategia a dispuesto acciones encaminadas al control preventivo de los Riesgos, con el propósito de garantizar la adecuada prestación de servicios y el cumplimiento de sus objetivos institucionales, ha determinado directrices relativas a la administración de la gestión del riesgo, teniendo en cuenta el contexto de la entidad y la planeación estratégica.

La Política de Administración de Riesgo tiene el propósito de orientar a los servidores públicos de AGUAS DEL HUILA S.A E.S.P. responsables de los procesos del Modelo de Operación, sobre la identificación, análisis y valoración de los riesgos con el fin de tener un panorama general de las posibles desviaciones que pueden ocurrir y crean inquietud en el logro de los objetivos.

De igual manera, se establecen los lineamientos generales, responsabilidades y mecanismos para la administración de los riesgos que permitan el manejo adecuado, de igual manera el control en todos los niveles de la entidad que brinden una seguridad adecuada en el cumplimiento de los objetivos, para controlar y responder los acontecimientos potenciales o aquellos en los que se pueden desencadenar situaciones de corrupción en concordancia con las directrices en materia de gestión pública y con los lineamientos de carácter técnico establecidos por el Departamento Administrativo de la Función Pública - DAFP y el Modelo Integrado de Planeación y Gestión –MIPG, en la “Guía para la Administración de riesgos y el Diseño de controles en Entidades Públicas – Riesgos de Gestión, Corrupción y Seguridad Digital.”

....llevamos 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).

OBJETIVO

Establecer en el marco general para la administración de los riesgos en AGUAS DEL HUILA S.A E.S.P. los principios básicos de la gestión del riesgo mediante la ejecución de un proceso metódico y continuo que contribuya al mejoramiento constante de las actividades y al cumplimiento de los objetivos de la Entidad.

OBJETIVOS ESPECIFICOS

- Ofrecer herramientas a la entidad para la identificación, valoración y seguimiento de los riesgos y determinar roles y responsabilidades de cada uno de los colaboradores de acuerdo al esquema de las líneas de defensa en los riesgos de gestión, seguridad digital y corrupción.
- Orientar a los servidores públicos de la entidad, responsable de los procesos, con el fin de tener un panorama general de las posibles desviaciones que pueden ocurrir en el proceso y cumplimiento de los objetivos.
- Establecer las acciones correctivas ante la materialización de los riesgos identificados.

ALCANCE

La Política de Administración de Riesgo Aplica a todos los procesos, proyectos, servicios y planes de AGUAS DEL HUILA S.A.E.S.P conforme a cada tipo y clasificación de riesgo, bajo la responsabilidad de los líderes de proceso y líneas de defensa, su monitoreo y seguimiento de los mismos.

TERMINOS Y DEFINICIONES

Mapa de Riesgos Institucional: Contiene a nivel estratégico los mayores riesgos a los cuales está expuesta la entidad, permitiendo conocer las políticas inmediatas de respuesta ante ellos.

Mapa de Riesgos por Proceso: Facilita la elaboración del mapa institucional, que se alimenta de estos, teniendo en cuenta que solamente se trasladan al institucional aquellos riesgos que permanecieron en las zonas más altas de riesgo y que afectan el cumplimiento de la misión institucional y objetivos de la entidad.

Riesgo de gestión: Posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.

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 seguridad digital: Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

Riesgos Inherente: Es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.

Riesgo Residual: Nivel de riesgo que permanece luego de tomar sus correspondientes medidas de tratamiento.

Control: Medida que modifica el riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).

Causa: Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.

Amenazas: Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

Impacto: Se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.

MARCO NORMATIVO

- 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.
- Decreto 1083 de 2015 “por el cual se expide el Decreto Único Reglamentario del sector de Función Pública.”

METODOLOGIA PARA LA ADMINISTRACION DEL RIESGO

1. CONOCIMIENTO Y ANALISIS DE LA ENTIDAD

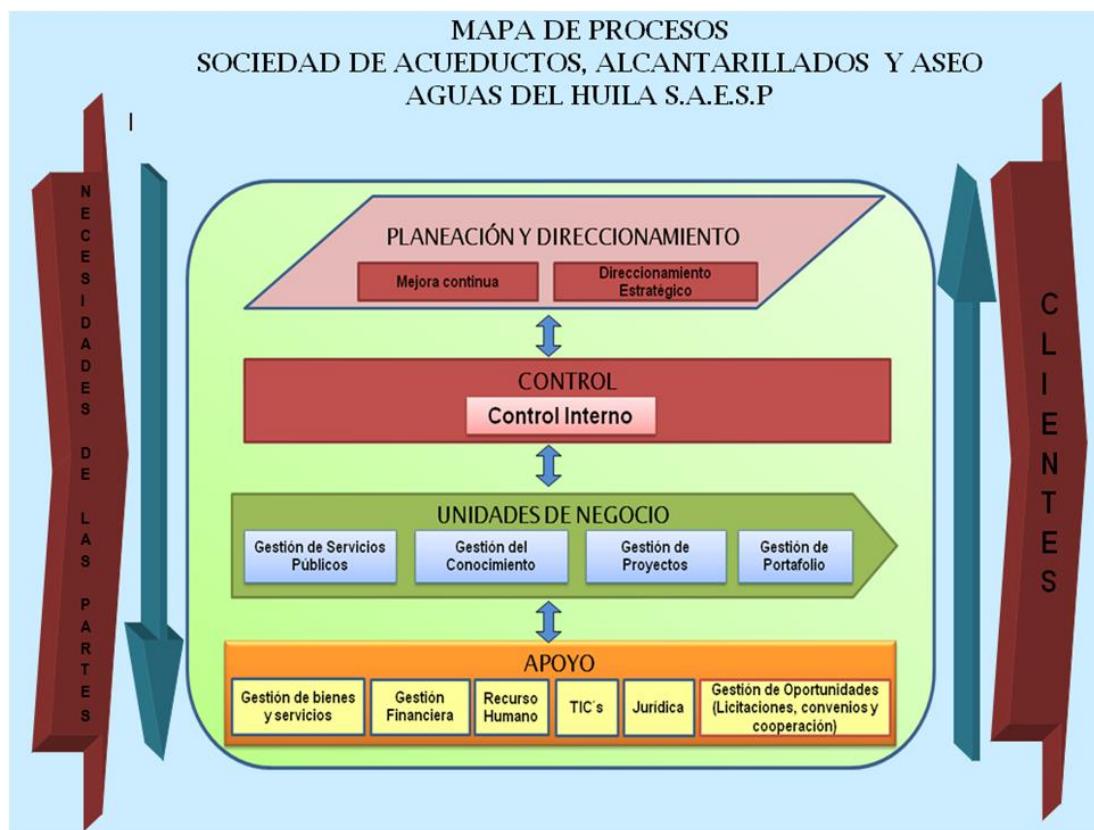
1.1 MISION

AGUAS DEL HUILA S.A E.S.P., es una empresa prestadora de servicios integrales con proyección nacional que genera bienestar social y responsabilidad sociambiental.

1.2 VISION

En el 2031, Aguas del Huila será el operador especializado Surcolombiano de servicios públicos domiciliarios y servicios integrales.

1.3 MAPA DE PROCESOS



2. POLITICA DE ADMINISTRACION DEL RIESGO

AGUAS DEL HUILA S.A.E.S.P establece su compromiso para gestionar todos aquellos riesgos que representen una amenaza para la organización, a través del fortalecimiento de la cultura de autocontrol y la adopción de metodologías y herramientas prácticas y de fácil

comprensión que permitan ser certeros en su tratamiento, contribuyendo efectivamente al logro de las metas institucionales.

3. IDENTIFICACION DEL RIESGO

Factor	Definición		Descripción
Procesos	Eventos relacionados con errores en las actividades que deben realizar los servidores de la organización.		Falta de procedimientos
			Errores de grabación, autorización
			Errores en cálculos para pagos internos y externos
			Falta de capacitación, temas relacionados con el personal
Talento humano	Incluye seguridad y salud en el trabajo. Se analiza posible dolo e intención frente a la corrupción.		Hurto activos
			Posibles comportamientos no éticos de los empleados
			Fraude interno (corrupción, soborno)
Tecnología	Eventos relacionados con la infraestructura tecnológica de la entidad.		Daño de equipos
			Caída de aplicaciones
			Caída de redes
			Errores en programas
Infraestructura	Eventos relacionados con la infraestructura física de la entidad.		Derrumbes
			Incendios
			Inundaciones
			Daños a activos fijos
Evento externo	Situaciones externas que afectan la entidad.		Suplantación de identidad
			Asalto a la oficina
			Atentados, vandalismo, orden público

Fuente: Adaptado del curso Riesgo Operativo de la Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

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:

....llevamos 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).

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

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

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.).

....llevamos 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).

- 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

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

....llevamos 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).

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.

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.
3	Possible	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.

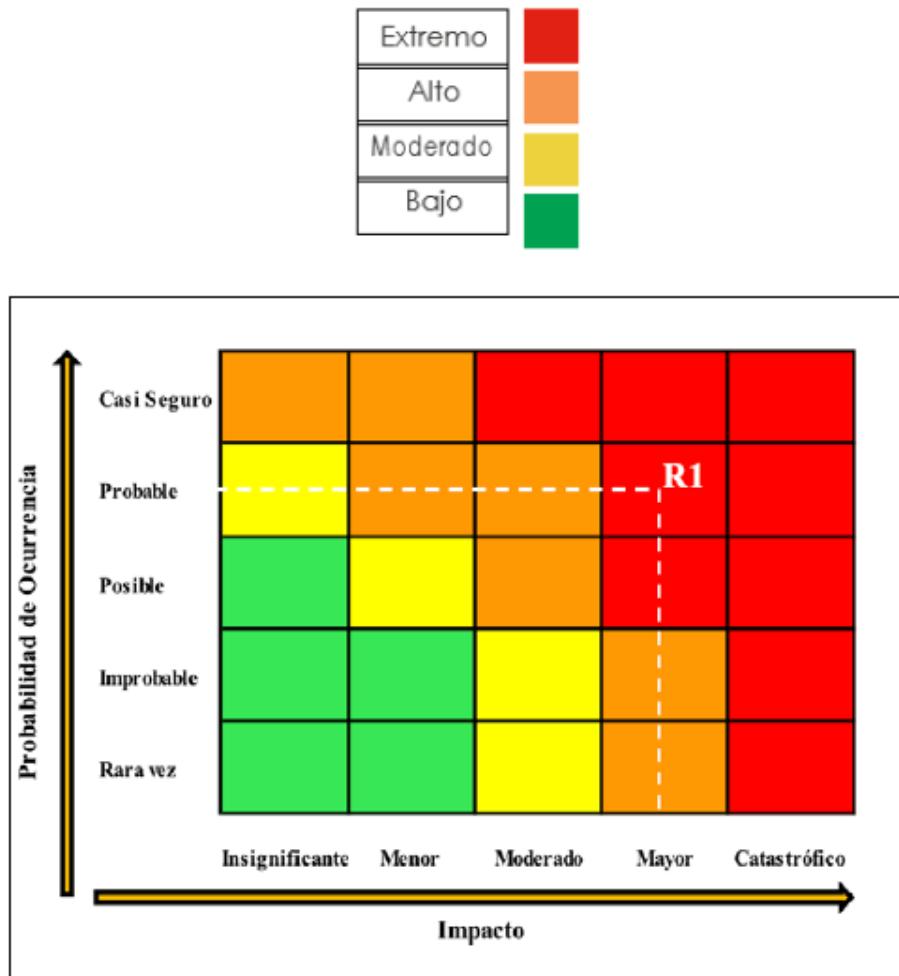
Se sugiere realizar este análisis con todas o las personas que más conozcan del proceso, y que por sus conocimientos o experiencia puedan determinar el impacto y la probabilidad del riesgo de acuerdo con los rangos señalados en las tablas que se muestran más adelante.

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.

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.



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 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.

4. 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.

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.

AGUAS DEL HUILA S.A.E.S.P. 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 misión de Aguas del Huila S.A. E.S.P.

LINEAS DE DEFENSA

PRIMERA LINEA DE DEFENSA

- Realizar la identificación y actualización de los Riesgos en todas sus etapas (Contexto Estratégico, identificación, análisis y valoración del riesgo) que pueden afectar los objetivos, programas, proyectos y planes asociados a su proceso y/o subprocesso.
- Definir, adoptar, aplicar y hacer seguimiento a los controles para mitigar los riesgos identificados y proponer mejoras para su gestión.
- Realizar el monitoreo y revisión de los riesgos de manera permanente; deben diligenciar el respectivo formato cuatrimestralmente y remitir a la Oficina de Planeación y Gestión. Informando sobre la efectividad de sus controles internos.

SEGUNDA LINEA DE DEFENSA

- Aplicar los diferentes controles identificados para cada riesgo. Monitorear y evaluar el estado de los controles y la gestión del riesgo de manera permanente.
- Acompañar y orientar a los procesos sobre la metodología para la Administración de Riesgos.
- El área de TIC y Gobierno Abierto brindará asesoría a los procesos y/o subprocessos en la Construcción del mapa de Riesgos de seguridad digital todas sus etapas (Contexto Estratégico, identificación, análisis y valoración del riesgo).
- La Oficina de Planeación y Gestión realizará la consolidación del mapa de riesgos de corrupción y elabora el informe consolidado de monitoreo y revisión a riesgos.

TERCERA LINEA DE DEFENSA

- Realizar el seguimiento y evaluación a los mapas de riesgos de los procesos de la Gobernación.
- Elaborar informes de seguimiento a los mapas de riesgo de la entidad y remitir a los responsables de procesos y/o subprocesso y los resultados con el fin que emprendan las acciones necesarias.

APLICABILIDAD

La política de Administración del Riesgo será aplicable a todos los servidores de Aguas del Huila S.A. E.S.P., con un enfoque preventivo, que sirva de guía de comportamiento de los servidores públicos. Es compromiso y responsabilidad de los servidores públicos y demás colaboradores conocer la Política y es su deber cumplirla y respetarla en el desarrollo de cualquiera de sus actividades, servicios o consultas.

La presente política será renovada cuando se presenten nuevas normativas y/o lineamientos establecidos por la ley o la función pública.

NIVEL DE CUMPLIMIENTO

La Política de Administración del Riesgo de Aguas del Huila S.A. E.S.P. Es obligatorio para todos los funcionarios, contratistas, practicantes, proveedores y terceros en función de la entidad; Todas las agencias e individuos dentro del alcance y aplicabilidad deben cumplir con la política al 100%. La política se evalúa a través de mecanismos de mejora continua que incluyen la participación pública, el compromiso, la colaboración, la adaptación de la entidad.

EVALUACION Y SEGUIMIENTO

El seguimiento debe efectuarse en forma cuatrimestral, tomando como base el mapa de riesgos de corrupción

Primer seguimiento: Con corte al 30 abril

Segundo seguimiento: Con corte al 31 de agosto.

Tercer seguimiento: Con corte al 31 de diciembre.

Su publicación debe efectuarse dentro de los diez (10) primeros días del mes siguiente en la página Web de la entidad o en un lugar de fácil acceso al ciudadano.

RECOMENDACIONES

- Monitorear el cumplimiento de la política de Administración del Riesgos de la entidad, por parte del comité institucional y asegurar que los riesgos identificados

....llevamos 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).

sean monitoreados por parte del responsable de cada proceso de acuerdo a la periodicidad establecida.

- Identificar factores asociados a posibles actos de corrupción en la entidad que puede afectar negativamente el cumplimiento de los objetivos institucionales.
- Fomentar la generación de acciones para apoyar la segunda línea de defensa frente al seguimiento del riesgo, por parte del comité y de los responsables de cada proceso.
- Tener en cuenta los resultados de la evaluación

VIGENCIA

La Política de Administración del Riesgo de Aguas del Huila S.A. E.S.P., será divulgada y publicada en la página web, www.aguasdelhuila.gov.co.

....llevamos 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).