REPUBLICA DE COLOMBIA

DEPARTAMENTO DEL VALLE DEL CAUCA

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

VALLECAUCANA DE AGUAS S.A. E.S.P.

ENERO 2019

TABLA DE CONTENIDO

GLOSARIO

- **Seguridad informática:** Se ocupa de la implementación técnica y de la operación para la protección de la información.
- **Seguridad de la información:** Se Ocupa de evaluar el riesgo y las amenazas, traza el plan de acción y esquemas normativos. Es la línea estratégica de las Seguridad.
- **Amenazas:** Cualquier evento, persona, situación o fenómeno que pueda causar daño.
- **Vulnerabilidades:** Falla o debilidad en un sistema que puede ser explotada por quien la conozca.
- **Riesgo:** Probabilidad de ocurrencia de una amenaza.
- **Controles:** Conjunto de mecanismos que regulan el funcionamiento de un sistema.
- **ISO:** Organización Internacional de Normalización es una organización para la creación de estándares internacionales.
- **Activo:** Bienes, recursos o derechos que tenga valor para una organización.
- **Activo de Información:** Toda la información que maneja con la que cuenta una organización para un correcto funcionamiento.
- **Análisis de brechas:** es una herramienta de análisis para comparar el estado y desempeño real de una organización, estado o situación en un momento dado.
- **Análisis de Riesgo:** Método empleado para evaluar los riesgos informáticos y obtener respuesta de peligro.
- **Gestión del Riesgo Informáticos:** Actividades empleadas para mitigar los riesgos informáticos.
- **Incidente de seguridad informática:** daño que puede comprometer las operaciones de la alcaldía municipal.
- **Evento:** Acción que puedo haber causado daño, pero fue controlado**.**
- **Información:** Conjunto de datos que tienen un significado.

- **Probabilidad:** Posibilidad de que una amenaza se materialice.
- **Impacto:** Daño que provoca la materialización de una amenaza.
- **SGSI:** Sistema de Gestión de seguridad de la Información
- **MSPI:** Modelo de seguridad y privacidad de la información
- **PHVA:** Planear, hacer, verificar, actuar.

INTRODUCCIÓN

La norma ISO 27005:2011 es un estándar internacional diseñado para la gestión del riesgo en la seguridad de la información dentro de un sistema de gestión de seguridad de la información. Contiene diferentes procedimientos y directrices, que permiten establecer los riesgos que enfrenta una organización y poder mitigarlos de la mejor manera. Se realiza la identificación, el análisis, la evaluación de los riesgos, las políticas y controles que permiten reaccionar ante una posible materialización del riesgo mediante el plan de tratamiento de riesgos.

El no contar con una buena gestión de la seguridad de la información, para la entidad de Vallecaucana de Aguas S.A. E.S.P. puede traer consecuencias graves, como pérdida fuga o robo de información, alteración de documentos, navegación de servicios etc.

1. OBJETIVOS

1.1 OBJETIVO GENERAL

- Mitigar los riesgos informáticos en Vallecaucana de Aguas S.A. E.S.P., mediante la aplicación de la norma ISO 27005.

1.2 OBJETIVOS ESPECÍFICOS

- Identificar la ubicación y propietarios de los activos de información a través del inventario del mismo.
- Categorizar y valorar los activos de información.
- Establecer los controles y políticas de la seguridad de la información que garantice la confidencialidad integridad y disponibilidad de la información.
- Proyectar el mapa de riesgos informáticos de Vallecaucana de Aguas S.A. E.S.P. donde se establece el contexto.

2. MARCO TEORICO

2.1 SEGURIDAD INFORMATICA

La seguridad Informática y la seguridad de la información son métodos y técnicas físicas y documentales empleadas para mantener siempre la confidencialidad, integridad y disponibilidad de la información.

Ilustración 1: Pilares de la seguridad informática.

2.2 MODELO PHVA PARA EL SGSI

Un SGSI establece una serie de procesos y lineamientos que se deben seguir mediante la estandarización de la norma ISO 27001 para asegurar los activos de información como Bases de datos, oficios, actas etc. de una organización. El objetivo es mantener siempre la confidencialidad, integridad y disponibilidad de la información.

Ilustración 2: Ciclo PHVA de SGSI

2.3 METODOLOGÍA MAGERIT

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de la Administraciones**.** MAGERIT se basa en *analizar el impacto* que puede tener una organización al ser vulnerada, *buscando identificar las amenazas* que pueden llegar a afectar el funcionamiento de la compañía**.**

Esta metodología, guía paso a paso cómo llevar a cabo el análisis de riesgos. Está dividida en tres partes. La primera parte hace referencia al Método, donde se describe la estructura que debe tener el modelo de gestión de riesgos de acuerdo a la norma ISO 27001.

La segunda parte es el inventario activo de información que puede utilizar la empresa para enfocar el análisis de riesgo**,** las características que deben tenerse en cuenta para valorar los activos identificados y además un listado con las amenazas y controles que deben tenerse en cuenta.

Por último, son las técnicas que Contiene ejemplos de análisis con tablas, algoritmos, árboles de ataque, análisis de costo beneficio, técnicas gráficas y buenas prácticas para llevar adelante sesiones de trabajo para el análisis de los riesgos.

2.4 OBJETIVOS DE LA METODOLOGÍA MAGERIT

- Concientizar a los funcionarios y responsables de la información, los riesgos que enfrentan y como mitigarlos.
- Establecer el tratamiento de los riesgos para evitar que los mismos se materialicen.
- Proyectar a las organizaciones para la auditoria y certificación de la Norma ISO 27001.

3. ETAPAS PARA LA ADMINISTRACIÓN DEL RIESGO DEL PROYECTO

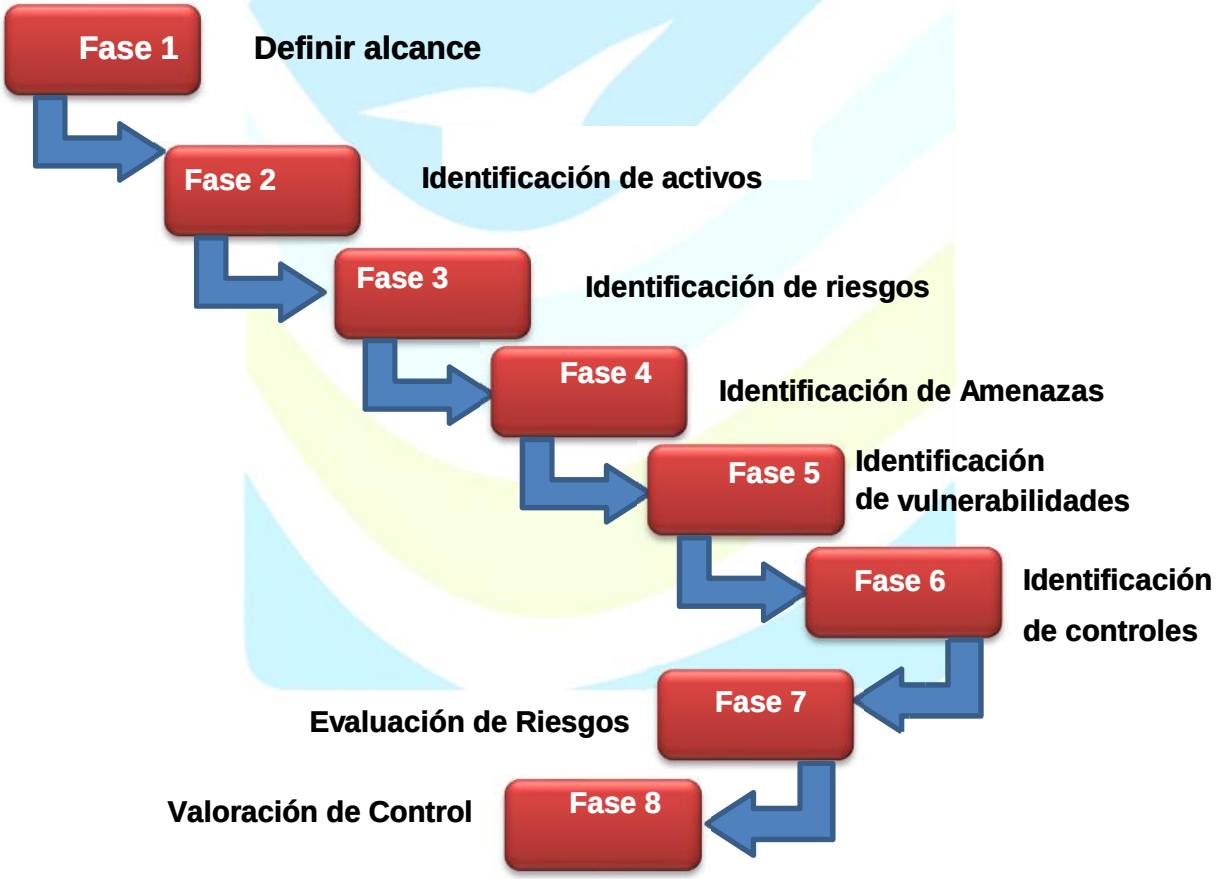

Ilustración 3: Guía para el Desarrollo.

3.1 DEFINIR EL ALCANCE

En esta fase se establece los objetivos, justificación del procedimiento que se va a realizar, los funcionarios implicados y el contexto de seguridad informática con el que cuenta Vallecaucana de Aguas S.A. E.S.P.

3.2 IDENTIFICACIÓN DE LOS ACTIVOS DE INFORMACION

El principal activo de una organización es la información en sí, la cual puede estar en hardware o software tales como documentos impresos o escritos a mano, en medios electrónicos almacenados en Discos Duros Externos, Memorias USB o en forma digital, en los equipos de cómputo o en la Nube. Toda esta información requiere ser analizada para su protección. (Un activo es todo aquello que genera valor para una empresa u organización.)

CLASIFICACIÓN DEL ACTIVO DE INFORMACIÓN:

Nivel del Criterio.

Confidencialidad / Se evalúa con los siguientes valores

Tabla 1: Evaluación de la confidencialidad

Nivel	Descripción Criterio de Confidencialidad	Denominación
0	Información que puede ser conocida y utilizada sin autorización por cualquier persona, sea empleado de Vallecaucana de Aguas S.A. E.S.P. o no	Publico
1	Información que puede ser conocida y utilizada por todos los empleados de Vallecaucana de Aguas S.A. E.S.P. y algunas entidades externas debidamente autorizadas, y cuya divulgación o uso no autorizados podría ocasionar riesgos o pérdidas leves para Vallecaucana de Aguas S.A. E.S.P., el Sector Público Nacional o terceros.	Reservada – Uso Interno
2	Información que sólo puede ser conocida y utilizada por un grupo de empleados, que la necesiten para realizar su trabajo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas a Vallecaucana de Aguas S.A. E.S.P. o a terceros.	Reservada - Confidencial
3	Información que sólo puede ser conocida y utilizada por un grupo muy reducido de empleados, generalmente de la alta dirección de Vallecaucana de Aguas S.A. E.S.P., y cuya divulgación o uso no autorizados podría ocasionar pérdidas graves al mismo o a terceros.	Reservada Secreta

Integridad / / Se evalúa con los siguientes valores

Tabla 2: Evaluación de Integridad

Nivel	Descripción Criterio de Integridad
0	Información cuya modificación no autorizada puede repararse fácilmente, o no afecta la operatoria de Vallecaucana de Aguas S.A. E.S.P..
1	Información cuya modificación no autorizada puede repararse, aunque podría ocasionar pérdidas leves para la Vallecaucana de Aguas S.A. E.S.P. o terceros
2	Información cuya modificación no autorizada es de difícil reparación y podría ocasionar pérdidas significativas para Vallecaucana de Aguas S.A. E.S.P. o terceros.
3	Información cuya modificación no autorizada no podría repararse, ocasionando pérdida a Vallecaucana de Aguas S.A. E.S.P. o a terceros.

Disponibilidad / / Se evalúa con los siguientes valores

Tabla 3: Evaluación de Disponibilidad.

Nivel	Descripción Criterio de Disponibilidad
0	Información cuya inaccesibilidad no afecta la operatoria de Vallecaucana de Aguas S.A. E.S.P.
1	Información cuya inaccesibilidad permanente durante una semana podría ocasionar pérdidas significativas para Vallecaucana de Aguas S.A. E.S.P. o terceros.
2	Información cuya inaccesibilidad permanente durante un día podría ocasionar pérdidas significativas a Vallecaucana de Aguas S.A. E.S.P. o a terceros.
3	Información cuya inaccesibilidad permanente durante una hora podría ocasionar pérdidas significativas a Vallecaucana de Aguas S.A. E.S.P. o a terceros.

3.3 IDENTIFICACIÓN DEL RIESGO

El objetivo de la identificación de riesgos es conocer lo incidentes o eventos que pueden causar pérdidas o alteración en el funcionamiento de Vallecaucana de Aguas S.A. E.S.P. y pueden afectar la confidencialidad, integridad y disponibilidad de la información.

La identificación de los riegos se realiza con observación directa, ingeniería social y con el análisis a los equipos de seguridad perimetral. Por confidencialidad de Vallecaucana de Aguas S.A. E.S.P se presenta la identificación de riesgos general.

RIESGOS INFORMÁTICOS	CAUSAS	EFECTO
Perdida Robo o Fuga de Información	✓ Fallas en el proceso de copia de respaldo o de restauración de la información, o pérdida de la misma. ✓ Fallas en los análisis y socialización de las vulnerabilidades de la infraestructura de IT. ✓ No contar con acuerdos de confidencialidad con los empleados y terceros ✓ Falta de autorización para la extracción de información generadas por requerimientos. ✓ Ingreso a la red y acceso a los activos de TI por parte de máquinas ajenas a la entidad. ✓ Habilitación de puertos USB en modo lectura y escritura para medios de almacenamiento. ✓ Ataques cibernéticos internos o externos	✓ Afectación parcial o total de la continuidad de las operaciones de los servicios del Incumplimiento normativo. ✓ Vulneración de los sistemas de seguridad operando actualmente. ✓ Mala imagen, multas, sanciones y pérdidas económicas. ✓ Generación de consultas, funcionalidades o reportes con información sensible de los clientes. ✓ Pérdida o fuga de información

RIESGOS INFORMÁTICOS	CAUSAS	EFECTO
Perdida Robo o Fuga de Información	✓ Empleados no capacitados en los temas de riesgos informáticos. ✓ Desconocimiento del riesgo. ✓ Prestar los equipos informáticos a personal no autorizado. ✓ No cerrar sesión cuando se desplaza del puesto. ✓ Acceso no autorizado a las dependencias. ✓ Conectar dispositivos externos a los equipos. ✓ Falta de implementación de la política escritorio limpio	✓ Desconfianza a la entidad

RIESGOS INFORMÁTICOS	CAUSAS	EFECTO
Correos electrónicos de extraña procedencia	✓ Empleados no capacitados en los temas de riesgos informáticos. ✓ Desconocimiento del riesgo. ✓ No generar una Cultura de Seguridad de la Información ✓ Falta de Filtros en el Servidor de Correo. ✓ Falta de instalación de EndPoint (programa seguridad punto final) en las estaciones de trabajo.	✓ Cifrado de la información. ✓ Captura de las pulsaciones del teclado. ✓ Monitoreo de las actividades realizadas en el equipo. ✓ Ataque remoto mediante un troyano o gusano. ✓ Robo de contraseñas. ✓ Equipo usado como Zombie para BotNet (usado para atacar otros DDoS). ✓ Robo de documentos y/o archivos. ✓ Sistema con mal funcionamiento.

RIESGOS INFORMÁTICOS	CAUSAS	EFECTO
Daño en los equipos tecnológicos	✓ Manejo inadecuado de los equipos ✓ Falta de mantenimiento o mala conexión de los mismos en las instalaciones eléctricas ✓ Falta de equipos de potenciación ✓ Fallas por defectos de fabrica ✓ Derrame de líquido ✓ Falta de ambiente adecuado para los equipos. ✓ Falta Educación a los usuarios en el manejo de los equipos de computo.	✓ Perdida de información ✓ Perdidas de los quipos informáticos ✓ Indisponibilidad del Servicio ✓ Traumatismos en los procesos

RIESGOS INFORMÁTICOS	CAUSAS	EFECTO
Dumpsterdiving (buceo en la basura)	✓ Desconocimiento del riesgo. ✓ Falta de capacitación y conciencia.	✓ Creación de perfil de ataque. ✓ Captura de información privilegiada
Perdida de conectividad	✓ Daño externo del ISP (Internet service provider). ✓ Ataque DDoS o DOS (denegación de servicios distribuidos o Denegación de servicios).	✓ Incumplimiento laboral. ✓ Niveles de estrés.

RIESGOS INFORMÁTICOS	CAUSAS	EFECTO
Ataques Informáticos	✓ Estimulo o Reto personal ✓ Rebelión. ✓ Ánimo de lucro. ✓ Espionaje	✓ Daño en los equipos tecnológicos. ✓ incidente en la confidencialidad, integridad y disponibilidad de la información. ✓ Denegación de servicios. ✓ Secuestro de la información. ✓ Divulgación ilegal de la información ✓ Suplantación de identidad. ✓ Destrucción de la información. ✓ Soborno de la información

Tabla 4: Identificación de Riesgos Informáticos.

3.4 IDENTIFICACIÓN DE LAS AMENAZAS

Una amenaza se identifica como un evento, persona, situación o fenómeno que pueda causar daño a los activos de la organización. Las amenazas pueden ser de origen Humano o Ambientales.

AMENAZA	TIPO
Polvo, Corrosión	Evento Naturales
Inundación	Evento Naturales
Incendios	Evento Naturales
Fenómenos Sísmicos	Evento Naturales
Fenómenos Térmicos	Evento Naturales y Daños físicos
Perdida en el suministro de energía	Daño Físico
Espionaje remoto	Acciones no autorizadas
Ingeniería Social	Acciones no autorizadas
Intrusión	Acciones no autorizadas
Accesos forzados al sistema	Acciones no autorizadas
Manipulación del Hardware	Acciones no autorizadas
Manipulación con Software	Acciones no autorizadas
Fallas del equipo	Fallas técnicas
Saturación del sistema de información	Fallas técnicas

Tabla 5: Identificación de Amenazas

3.5 IDENTIFICACIÓN DE LAS VULNERABILIDADES

Las vulnerabilidades son las Fallas o debilidades en un sistema, que puede ser explotada por quien la conozca. Cuando la amenaza encuentra la vulnerabilidad es cuando se crea el riesgo. Por eso es necesario conocer la lista de amenazas y el inventario de activos de información.

VULNERABILIDADES	DESCRIPCION
Fácil acceso a las dependencias o Secretarías.	No existe un control para el acceso de las personas no autorizadas a las secretarías.
Falta de dispositivos de seguridad biométrica para acceso a las secretarias de alto riesgo.	El dispositivo de seguridad biométrica reduce el riesgo de robo de información o equipos electrónicos por fácil acceso.
Falta de Aplicación de la Política de escritorio Limpio.	La política de escritorio limpio, es implementada para que los funcionarios no dejen expuestos: documentos, equipos electrónicos u objetos de valor, sobre los escritorios, que pueden ser robados fácilmente.
Falta de máquina trituradora de papel	La máquina trituradora de papel, evita que las personas arrojen documentos importantes con información personal a la basura, que puedan ser usados para crear perfiles de ataque.
Falta de Capacitación de los funcionarios en temas de seguridad Informática.	El eslabón más débil en términos de seguridad informática en una organización son los funcionarios, dado que no tienen conocimiento sobre las amenazas y riesgos que enfrentan y como poder mitigarlos.
Falta de equipos electrónicos para copias de respaldo.	El no contar con un HDD externo, impide a los funcionarios realizar copias de respaldo o Back ups.
Falta de equipos institucionales.	El no contar con suficientes equipos institucionales, lleva a los funcionarios a traer equipo personal que pueden afectar el funcionamiento de la red o infectarla. Adicionalmente promueve el compartir cuentas de usuarios y claves que pueden afectar al prestador.
Equipo clon.	Los equipos clones, no cuentan con unidad de CD/DVD y puerto de USB en buen estado que pueden afectar el rendimiento laboral.

Tabla 6: Identificación de Vulnerabilidades

3.6 IDENTIFICACIÓN DE CONTROLES EXISTENTES

La identificación de los controles existentes permite realizar la evaluación de riesgos. Lo controles garantizan que al momento de la materialización de un riesgo se reduzcan o mitiguen los riesgos informáticos y la organización funcionen correctamente. Pero se debe tener en cuenta que nunca se va a estar 100% seguros.

Dada la importancia de los controles, con que cuenta Vallecaucana de Aguas S.A. E.S.P. no es adecuado exponerlos en el proyecto, por lo que se pueden crear perfiles de ataque.

3.7 EVALUACIÓN DE RIESGO

La evaluación de riesgo se realiza con enfrentamiento entre la probabilidad de ocurrencia y el impacto que genera el riesgo en los activos de información, dado por la matriz de calificación, evaluación y respuestas a los riesgos.

Vallecaucana de Aguas S.A. E.S.P. cuenta con Sistema de Gestión Documental que realiza el análisis de riesgos con la información recolectada.

TABLA DE PROBABILIAD			
NIVEL	**DESCRIPTOR**	**DESCRIPCIÓN**	**FRECUENCIA**
1	Raro	El evento puede ocurrir solo en circunstancias excepcionales	No se ha presentado en los últimos 5 años
2	improbable	El evento puede ocurrir en algún momento	Al menos una vez en los últimos 5 años
3	posible	El evento podría ocurrir en algún momento	Al menos una vez en los últimos 2 años
4	probable	El evento probablemente ocurra en la mayoría de las circunstancias	Al menos una vez en el último año
5	Casi Seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de una vez al año

Tabla 6: Probabilidad de riesgo

TABLA DE IMPACTO		
NIVEL	**DESCRIPTOR**	**DESCRIPCIÓN**
1	Insignificante	Si el hecho llegara a presentarse, tendría consecuencias o efecto mínimos sobre la entidad
2	Menor	Si el hecho llegara a presentarse, tendría bajo impacto o efecto mínimos sobre la entidad
3	Moderado	Si el hecho llegara a presentarse, tendría medianas consecuencias o efecto sobre la entidad
4	Mayor	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad
5	Catastrófico	si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad

Tabla 7 Impacto del riesgo

PROBABILIDAD	IMPACTO				
	Insignificante(1)	**Menor(2)**	**Moderado(3)**	**Mayor(4)**	**Catastrófico (5)**
Raro(1)	B	B	M	A	A
improbable(2)	B	B	M	A	E
posible(3)	B	M	A	E	E
probable(4)	M	A	A	E	E
Casi Seguro (5)	A	A	E	E	E

B: Zona de Riesgo Baja: Asumir el riesgo

M: Zona de Riesgo Moderada: Asumir el riesgo, Reducir el riesgo

A: Zona de Riesgo Alta: Reducir, Evitar, Compartir o Transferir

E: Zona de Riesgo extrema: Reducir el riesgo, evitar compartir o transferir

Tabla 8: Matriz de calificación, evaluación y respuestas a los riesgos.

ANÁLISIS DE RIESGOS					
RIESGO	**CALIFICACIÓN**		**TIPO DE IMPACTO**	**EVALUACIÓN**	**MEDIDAS RESPUESTAS**
	PROBABILIDAD	**IMPACTO**		**ZONA DE RIESGO**	
Perdida, Robo o fuga de información	3	5	Disponibilidad, integridad y confidencialidad de la información	Extrema	Reducir el riesgo, Evitar o Transferir
Correos electrónicos de extraña procedencia	3	2	Confidencialidad de la información 4, Operativo 4	Baja	Asumir el riesgo
Daños en los equipos tecnológicos	3	4	Credibilidad o Imagen 2.	Alta	Reducir el riesgo, evitar, compartir o transferir
Perdida de Información de la Entidad por robo informático	2	4	Confidencialidad de la información 4.	Alto	Reducir el riesgo, evitar, compartir o transferir
Perdida de conectividad	4	3	Credibilidad o Imagen 4	Moderado	Asumir el riesgo, reducir el riesgo
Ataques informáticos	2	4	Credibilidad o Imagen 4	Baja	Asumir el riesgo

Tabla 9: Análisis de riesgo

PROBABILIDAD	IMPACTO				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Raro (1)	B	B	M	A	A
Improbable (2)	B	B	M	A	E
Posible (3)	B	M	A	E	E
Probable (4)	M	A	A	E	E
Casi Seguro (5)	A		E	E	E

B: Zona de Riesgo Baja: Asumir el riesgo

M: Zona de Riesgo Moderada: Asumir el riesgo, Reducir el riesgo

A: Zona de Riesgo Alta: Reducir ,Evitar, Compartir o Transferir

E: Zona de Riesgo extrema: Reducir el riesgo, evitar compartir o transferir

ORIGINAL FIRMADO

MOISES CEPEDA RESTREPO
Gerente General
VALLECAUCANA DE AGUAS S.A. E.S.P.

Elaboró y proyectó: Jesús Migdonio Mosquera –Contratista Técnico en Sistemas
Revisó: Divier Velásquez Londoño– Director Administrativo
Aprobó: El Firmante