EMPRESA DE ACUEDUCTO, ALCANTARILLADO Y ASEO DE SAN GIL

Nit 800.120.175-7

Elaboro:
DIEGO ANDRES SUPELANO AMAYA
Ingeniero de Sistemas
Esp. En Seguridad Informática
Jefe de Sistemas y Estadística
2018-2019

Km 1 via al Aeropuerto
San Gil – Santander
(7) 7242590 – 7242564 – 7244433
Contactenos@acuasan.gov.co
www.acuasan.gov.co

#acuasaneice
#acuasaneice
Acuasan San Gil

INTRODUCCIÓN

Con el fin de garantizar el manejo eficaz de la información con la cual trabaja la EMPRESA DE ACUEDUCTO, ALCANTARILLADO YA SEO DE SAN GIL ACUASAN EICE-ESP, por medio de las aplicaciones tecnológicas y demás medios con los cuales interactúan diariamente los funcionarios y usuarios en general, se hace necesario identificar y gestionar las actividades que se relacionan con la Seguridad de la Información.

La gestión de los riesgos de seguridad de la información son aquellos procesos que reducen las pérdidas y brindan protección de la información, permitiendo conocer las vulnerabilidades que afectan todo el ciclo de vida del servicio.

El presente documento tiene como fin generar una cultura de prevención contra los riesgos a los que día a día se pudieran ver sometidos los activos de información de la EMPRESA DE ACUEDUCTO, ALCANTARILLADO YA SEO DE SAN GIL ACUASAN EICE-ESP. Basados en un enfoque del Modelo Integrado de Planeación y Gestión – MIPG, se pretende realizar una estrategia que permita diagnosticar, evaluar, implementar y desarrollar la gestión de incidentes que afectan al activo de información e implantar unas contramedidas en el sistema de gestión informático para disminuir la probabilidad de su materialización.

1. PLATAFORMA ESTRATÉGICA

1.1 OBJETIVO

Establecer las políticas, procedimientos y metodologías para identificar, analizar, valorar, monitorear, medir y controlar los riesgos de mayor probabilidad de ocurrencia que puedan afectar el cumplimiento de la Misión, y los Objetivos de los procesos del Sistema de Gestión de la Calidad.

1.2 OBJETIVOS ESPECÍFICOS

- Consolidar una administración de riesgos acorde con las necesidades de ACUASAN EICE-ESP.
- Proteger los activos de información de ACUASAN EICE-ESP de acuerdo a su clasificación y criterios de Confidencialidad, Integridad y Disponibilidad
- Crear compromiso en los usuarios del proceso en la Formulación y desarrollo del presente plan en aras de la prevención y administración del riesgo de seguridad de la información.
- Crear conciencia a nivel institucional de la importancia y la necesidad de una correcta gestión del riesgo de seguridad de la información

2. METODOLOGÍA PARA LA ADMINISTRACIÓN DEL RIESGO

2.1 Términos y Definiciones

Consecuencia
Resultado de un evento expresado cuantitativa o cualitativamente, como por ejemplo una pérdida, lesión desventaja o ganancia. Puede haber una serie de resultados posibles asociados con un evento.

Evento
Incidente o situación que ocurre en un lugar particular durante un intervalo de tiempo particular.

Frecuencia
Medida de la tasa de ocurrencia de un evento, expresada como el número de ocurrencia de un evento en un tiempo determinado (véase posibilidad y probabilidad).

Posibilidad
Se emplea como una descripción cualitativa de la probabilidad o frecuencia.

Pérdida
Cualquier consecuencia negativa, financiera u otra.

Probabilidad
Posibilidad de que ocurra un evento o resultado específico, medida por la relación entre los eventos o resultados específicos y el número total de eventos y resultados posibles.

Riesgo
Posibilidad de que suceda algo que tendrá impacto en los objetivos. Se mide en términos de consecuencias y posibilidad de ocurrencia.

Análisis de riesgo
Uso sistemático de la información disponible, para determinar la frecuencia con la que pueden ocurrir eventos especificados y la magnitud de sus consecuencias.

Valoración del riesgo
Proceso general de análisis del riesgo y evaluación del riesgo.

Evitar el riesgo
Decisión informada de no involucrarse en una situación de riesgo.

Identificación del riesgo
Proceso para determinar lo que puede suceder, por qué y cómo.

Gestión del riesgo
Cultura, procesos y estructuras que se dirigen hacia la gestión eficaz de las oportunidades potenciales y los efectos adversos.

Transferencia del riesgo
Traslado de la responsabilidad o carga por la pérdida a otra parte, por medio de la legislación, contratos, seguros u otros medios. La transferencia del riesgo también se puede referir al traslado de un riesgo físico o parte de mismo a cualquier otra parte.

Tratamiento del riesgo
Selección e implementación de las opciones apropiadas para ocuparse del riesgo

3. IMPORTANCIA DE LA GESTIÓN DE RIESGOS

En el ámbito empresarial se está dando mayor prioridad a salvar, proteger y custodiar el activo de la información, debido a que los sistemas de información y los avances tecnológicos están siendo implementados en todas las empresas del mundo.

La EMPRESA DE ACUEDUCTO, ALCANTARILLADO Y ASEO DE SAN GIL ACUASAN EICE-ESP, sigue los lineamientos trazados por el Gobierno Nacional en cumplimiento de la Ley de Transparencia 1712 de 2014 y Gobierno en Línea que viene impulsando actividades dentro de las entidades públicas para que se ajusten a modelos y estándares que permitan brindar seguridad a la información dando cumplimiento al Decreto 1078 de 2015.

Los riesgos por desastres naturales, riesgos inherentes relacionados con procesos no adecuados en el tratamiento de la misma información, desconocimiento de normas y políticas de seguridad y el no cumplimiento de estas, suelen ser los temas más frecuentes y de mayor impacto presentes en las empresas. Una entidad sin un plan de gestión de riesgos está expuesta a perder su información.

Todas las organizaciones deberían implementar planes para gestionar los riesgos que afectan a los sistemas de información, tecnologías de información y activos informáticos, considerando que en la actualidad los riesgos más comunes son generados por ataques dirigidos al software empresarial, afectando la disponibilidad e integridad de la información almacenada o transportada a través de los equipos de comunicación.

Por esta razón hay que estar preparados para prevenir todo tipo de ataques o desastres, ya que cuando el costo de recuperación supera al costo de prevención es preferible tener implementados planes de gestión de riesgos que permitan la continuidad del negocio tras sufrir alguna pérdida o daño en la información de la entidad.

Considerando la situación actual de la EMPRESA DE ACUEDUCTO, ALCANTARILLADO Y ASEO DE SAN GIL ACUASAN EICE-ESP, para reducir los niveles de riesgo, es indispensable diseñar un plan para iniciar las prácticas de las normas y políticas de seguridad e implementar procesos que aseguren la continuidad de los servicios.

3.1 ETAPAS PARA LA ADMINISTRACIÓN DEL RIESGO

El proceso de gestión del riesgo en la seguridad de la información puede ser iterativo para las actividades de valoración del riesgo y/o el tratamiento del mismo. Este enfoque puede incrementar la profundidad y el detalle de la valoración en cada iteración como se muestra en la figura tomada de la NTC ISO IEC 27005.

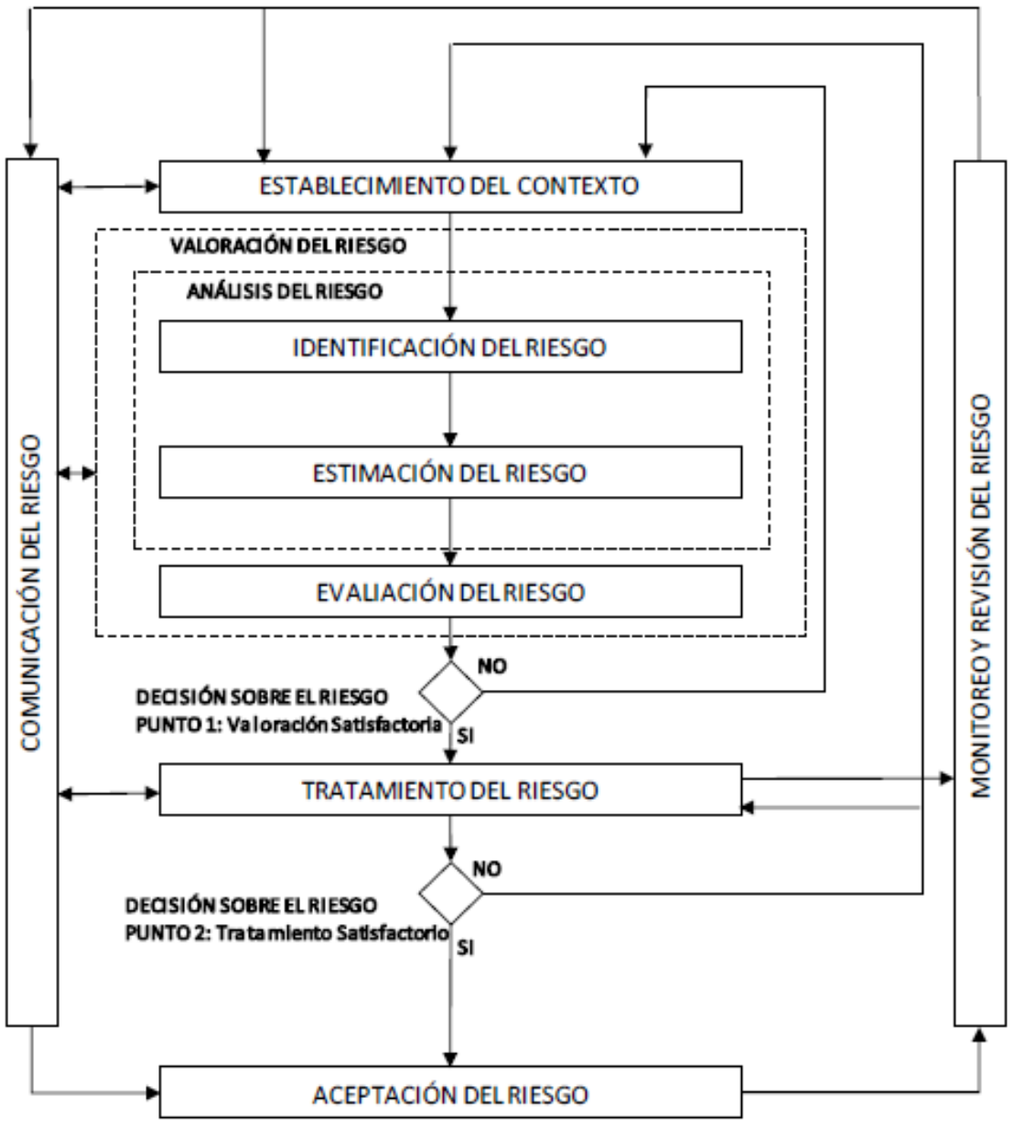

Imagen 2. Tomado de la NTC-ISO/IEC 27005

Las etapas a considerar durante la administración del riesgo para la EMPRESA DE ACUEDUCTO, ALCANTARILLADO Y ASEO DE SAN GIL ACUASAN EICE-ESP, son las siguientes:

Contexto estratégico: Se determinarán los factores externos e internos del riesgo.

Identificación: Se identificarán las causas, riesgo, consecuencias y clasificación del riesgo.

Análisis: Se calificará y evaluará el riesgo inherente.

Valoración: se identificará y evaluaran los controles; se deberá incluir la determinación del riesgo residual.

Manejo: Se determinará, si es necesario, acciones para el fortalecimiento de los controles.

Seguimiento: Se evaluará los riesgos de manera integral.

3.2 ANÁLISIS DEL RIESGO

El análisis permite establecer un mejor entendimiento y comprensión del riesgo, al considerar las consecuencias, posibilidad (causas), el impacto en caso de que llegue a materializarse y la probabilidad (frecuencia) de ocurrencia. La metodología para un adecuado análisis del riesgo se lleva a cabo en las siguientes fases:

a. CONSECUENCIAS: Una vez identificado el riesgo, se deben establecer las posibles consecuencias que se pueden presentar en caso de que el riesgo se materialice, es decir que se vuelva una situación real.

b. POSIBILIDAD: Posteriormente se deberá establecer la posibilidad o causa que origina la presencia del riesgo.

c. CONTROLES EXISTENTES: Establecida la posibilidad o causa, se deberán reconocer los controles existentes en la Empresa para mitigar o reducir el impacto del riesgo, es posible que no se cuente en el momento de la valoración con mecanismos de control asociados al riesgo, por lo tanto, el impacto negativo para la consecución de los objetivos en caso de materializarse el riesgo será mayor.

d. IMPACTO: El impacto del riesgo se mide en términos de las consecuencias que pueda generar el riesgo en la consecución de los objetivos y se debe considerar la existencia o no de controles. Se puede dar una relación inversa entre el número de controles y las consecuencias del riesgo, es decir, que a mayor número de controles eficaces, menores serán las consecuencias del riesgo en caso de materializarse. Para la medición se definió la Tabla 1 IMPACTO donde se establecen rangos.

Tabla 1 Impacto Nivel	***Descripción***	***Orientación o Características del Nivel***
1	*Insignificante*	*El riesgo no genera impacto negativo sobre los objetivos. Ningún daño, Sin pérdidas financieras. Sin impactos ambientales negativos. No se afecta la capacidad del proceso. No se ve afectada la facturación, la potabilización, la distribución o la recolección y el transporte de aguas servidas.*

2	*Menor*	*Efectos que no disminuyen la capacidad del proceso y que se remedian fácilmente. Sin Pérdidas financieras. Interrupción de la prestación del servicio por periodos cortos (Menores a 3 horas).*
3	*Moderado*	*Algunos objetivos o metas afectadas. Pérdidas financieras menores a 15 SMMLV. Se generan problemas o demoras para la facturación de un ciclo o parte de un ciclo. Interrupción de la prestación del servicio por periodos inferior a 6 horas.*
4	*Mayor*	*Algunos objetivos importantes no se pueden lograr. Pérdida financiera entre 16 y 50 SMMLV, pérdida de la capacidad de prestación del servicio. Interrupción de la prestación del servicio entre 6 y 24 horas. Retraso en la facturación de un ciclo completo. Deficiencias en el recaudo. Impactos Ambientales Negativos.*
5	*Catastrófico*	*Más del 50% de los objetivos o sus metas no se pueden lograr. Pérdida financiera mayor a 50 SMMLV Suspensión de la prestación del servicio por más de 24 horas. Incremento significativo de la cartera. Incremento del índice de Agua No Contabilizada IANC por encima del 50%.*

5. PROBABILIDAD: Se debe determina la Probabilidad de que ocurra un evento o resultado específico en términos de frecuencia (Nº de veces), para ello se estableció la Tabla 2.

Tabla 2 Probabilidad

Nivel	***Descripción***	***Características***
A	*Casi Cierto*	*Se espera que ocurra en la mayoría de las circunstancias, varias veces en el semestre, varias veces durante un proyecto, en más de 4 ciclos de facturación. Interrupción del servicio más de 5 veces al mes en un mismo sector hidráulico o sanitario. Incremento sistemático (4 meses consecutivos) de la cartera, el IANC o el número de reformados por encima de las metas establecidas.*

B	*Probable*	*Se espera que ocurra en el año o durante el proyecto dos o tres veces. En 2 o 3 ciclos de facturación. Interrupción del servicio 3 o 4 veces al mes en un mismo sector hidráulico o sanitario. Incremento sistemático por encima de las metas establecidas durante 3 meses consecutivos de la cartera o el IANC*
C	*Posible*	*Puede ocurrir de vez en cuando o en algún lugar durante un proyecto, menos de tres veces al año o durante el proyecto.*
D	*Improbable*	*No se espera que ocurra durante el año, durante el proyecto o durante la consecución del objetivo.*
E	*Raro*	*Evento que puede ocurrir solamente en circunstancias excepcionales (una vez al año o más) durante el proyecto o la consecución del objetivo y que no genera impacto significativo sobre las metas propuestas.*

NIVEL: Para finalizar la etapa de análisis, se debe establecer el nivel del riesgo, es decir, confrontar el impacto contra la probabilidad de ocurrencia, esto se logra haciendo un cruce en la Matriz de Análisis Cualitativo del Riesgo.

Prob.		Impacto				
		Insignificante 1	**Menor 2**	**Moderado 3**	**Mayor 4**	**Catastrófico 5**
Raro	**A**	**B**	**B**	**M**	**A**	**A**
Improbable	**B**	**B**	**B**	**M**	**A**	**E**
Posible	**C**	**B**	**M**	**A**	**E**	**E**
Probable	**D**	**M**	**A**	**A**	**E**	**E**
Casi Cierto	**E**	**A**	**A**	**E**	**E**	**E**

Una vez realizado el cruce, la Matriz establece un Nivel de Riesgo que se clasifica de la siguiente manera:

E:	Riesgo Extremo; se requiere acción inmediata
A:	Rieso Alto; Revisar o redefinir controles, opcional acciones preventivas
M:	Riego Moderado; Mantener controles, no requiere acciones preventivas.
B:	Riesto Bajo; gestionar mediante procedimientos de rutina

4. ETAPAS PARA LA GESTIÓN DE RIESGOS

4.1 Etapa de medición

PROBABILIDAD

Nivel		Descriptor	Orientación
	A	Raro	Evento que puede ocurrir solamente en circunstancias excepcionales (una vez cada 2 años) durante el proyecto o la consecución del objetivo y que no genera impacto significativo sobre las metas propuestas.
	B	Improbable	No se espera que ocurra durante el año, durante el proyecto o durante la consecución del objetivo. En caso de presentarse puede ocurrir máximo 1 vez al año durante el proyecto. Interrupción del servicio más de 10 veces al mes, en un mismo sector hidráulico o sanitario. Incumplimiento sistemático de proveedores (En cada pedido, en cada entrega, en cada obra).
	C	Posible	Puede ocurrir durante un proyecto entre 2 y 5 veces al año. En 2 ciclos de facturación. Interrupción del servicio 2 o 3 veces al mes en un mismo sector hidráulico o sanitario.
	D	Probable	Se espera que ocurra en el año o durante el proyecto (Entre 6 y 10 veces). En 3 o 4 ciclos de facturación. Interrupción del servicio 4 o 5 veces al mes en un mismo sector hidráulico o sanitario. Incremento sistemático de al Cartera o el IANC por encima de los rangos admisibles durante 3 meses consecutivos.
	E	Casi cierto	Se espera que ocurra en la mayoría de las circunstancias, varias veces en el año (Más de 10 veces) o varias veces durante un proyecto, en más de 4 ciclos de facturación. Interrupción del servicio más de 5 veces al mes en un mismo sector hidráulico o sanitario. Incremento sistemático (4 meses consecutivos) de la cartera, el IANC o el número de reformados por encima de los rangos admisibles o las metas establecidas por la empresa.

IMPACTO

Nivel	Descriptor	Orientación
1	Insignificante	El riesgo no genera impacto negativo sobre los objetivos. Ningún daño, sin pérdidas financieras. Sin impactos ambientales negativos. No se afecta la capacidad del proceso. No se ve afectada la facturación, la potabilizción, la distribución o la recolección y el transporte de aguas servidas. Caudal de captacion 850 lps
2	Menor	Efectos que no disminuyen la capacidad del proceso y que se remedian fácilmente. Sin Pérdidas financieras. Interrupción de la prestación del servicio por periodos cortos (Menores a 3 horas). Caudal de captación entre 800 y 850
3	Moderado	Algunos objetivos o metas afectadas. Pérdidas financieras menores a 15 SMMLV. Se generan problemas o demoras para la facturación de un ciclo o parte de un ciclo. Interrupción de la prestación del servicio por periodos inferior a 6 horas. Caudal de captacion entre 750 y 849 lps
4	Mayor	Algunos objetivos importantes no se pueden lograr. Pérdida financiera entre 16 y 50 SMMLV, pérdida de la capacidad de prestación del servicio. Interrupción de la prestación del servicios entre 6 y 24 horas. Retraso en la facturación de un ciclo completo. Deficiencias en el recaudo. Impactos Ambientales Negativos. Incremento del IANC hasta un 50%. Caudal de captación entre 500 y 749 lps
5	Catastrófico	Más del 50% de los objetivos o sus metas no se pueden lograr. Pérdida financiera mayor a 50 SMMLV. Suspensión de la prestación del servicio por más de 24 horas. Incremento significativo de la cartera. Incremento del índice de Agua No Contabilizada IANC por encima del 50%. Caudal de captación menor a 300 lps

IMPACTO

PROBABILIDAD

Prob.		Impacto				
		Insignificante 1	Menor 2	Moderado 3	Mayor 4	Catastrófico 5
Raro	A	B	B	M	A	A
Improbable	B	B	B	M	A	E
Posible	C	B	M	A	E	E
Probable	D	M	A	A	E	E
Casi Cierto	E	A	A	E	E	E

E:	RIESGO EXTREMO:	*Eliminar la actividad que lo genera en la medida de lo posible. Establecer el tratamiento mediante controles:* ***PREVENTIVOS*** *para evitar o disminuir la Probabilidad, o* ***DE PROTECCIÓN*** *para disminuir el Impacto, como compartir o transferir el Riesgo. Si durante la valoración del riesgo, el impacto ha sido calificado como Catastrófico, se deben elaborar Planes de Contingencia para protegerse de su ocurrencia. La División Control Interno debe realizar seguimiento a la ejecución de las acciones de tratamiento formuladas y a la aplicación de los controles definidos.*
A:	RIESGO ALTO:	*El tratamiento del riesgo es opcional. El responsable del proceso debe asegurarse que los controles identificados son efectivos y la División Control Interno debe establecer un seguimiento permanente al cumplimiento de los controles establecidos. Si durante la valoración del riesgo, el impacto ha sido calificado como Catastrófico, se deben elaborar Planes de Contingencia para protegerse de su ocurrencia.*
M:	RIESGO MODERADO:	*El nivel del riesgo Moderado y Bajo, es aceptable y la empresa lo puede Asumir mediante procedimientos de rutina y la aplicación continua de los controles ya establecidos.La División Control Interno debe establecer un seguimiento permanente al cumplimiento de los controles establecidos.*
B:	RIESGO BAJO:	

5. METODOLOGÍA DE IMPLEMENTACIÓN

Para llevar a cabo la implementación del Modelo de Seguridad y Privacidad de la Información en ACUASAN EICE-ESP, se toma como base la metodología PHVA (Planear, Hacer, Verificar y Actuar) y los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, a través de los decretos emitidos.

De acuerdo con esto, se definen las siguientes fases de implementación del MSPI (Modelo de Seguridad y Privacidad de la Información):

1. **Diagnosticar**
2. **Planear**
3. **Hacer**
4. **Verificar**
5. **Actuar**

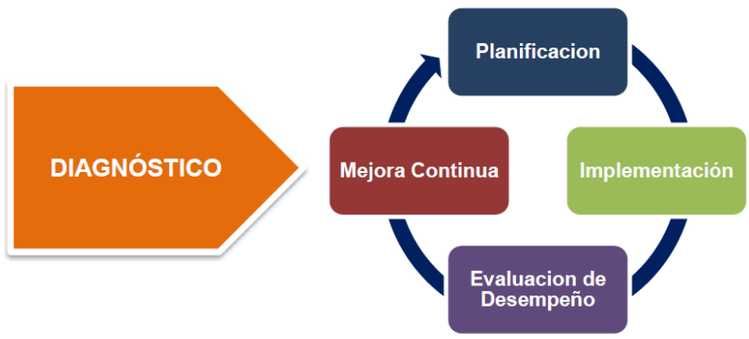

Figura 1 – Ciclo de operación del Modelo de Seguridad y Privacidad de la Información

ACTIVIDADES

1. Realizar Diagnóstico
2. Elaborar el Alcance del Plan del Tratamiento de Riesgo de Seguridad y Privacidad de la Información
3. Realizar la Identificación de los Riesgos con los líderes del Proceso.

a. Entrevistar con los líderes del Proceso

4. Valorar del riesgo y del riesgo residual
5. Realizar Mapas de calor donde se ubican los riesgos
6. Plantear al plan de tratamiento de riego aprobado por los lideres

CRONOGRAMA

CRONOGRAMA DE ACTIVIDADES PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION																											
ACTIVIDAD	ABRIL				MAYO				JUNIO				JULIO				AGOSTO				SEPTIEMBRE				OCTUBRE			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Realizar el Diagnostico																												
Elaborar el alcance del plan de tratamiento de riesgo de seguridad y privacidad de la información																												
Realizar la identificacion de los riesgos con los lideres del proceso																												
Entrevista con los lideres del proceso																												
Valoracion de los riesgos y los riesgos residuales																												
Mapas de calor donde se ubican los riesgos																												
Plantear el plan de tratamiento de riegos de seguridad																												
Seguimiento y control																												

6. SEGUIMIENTO y EVALUACIÓN

Cada seis (6) meses Control Interno realizará seguimiento a todo el componente de administración de riesgos y verificará aspectos como:

- **Cumplimiento de las políticas y directrices para la administración del riesgo**: metodología de Administración del Riesgo (diseño y funcionamiento).

- **Administración de los riesgos por proceso e institucionales**: calificación y evaluación, efectividad de los controles y cumplimiento de las acciones.

Los resultados de la evaluación y las observaciones de la persona que haga las veces de Control Interno deben ser presentados a la Alta Dirección, para que se tomen las decisiones pertinentes que garanticen la sostenibilidad de la Administración del Riesgo en la organización.

Descripción	Elaboró	Revisó	Aprobó
Nombre: Cargo: Fecha: Firma:	Diego Andres Supelano A Jefe de Sistemas 24/01/2019	Manuel Fabian Carvajal B. Jefe Asesor de Planeación 31/01/2019	Hector Alberto Ardila S. Gerente 31/01/2019