MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI)

VIGENCIA 2025

CONTROL DE CAMBIOS		
VERSIÓN	**FECHA DE APROBACIÓN**	**DESCRIPCIÓN DEL CAMBIO**
1	05-05-2025	Creación del documento con base en el Marco de Referencia de Arquitectura TI, el Modelo Integrado de Planeación y Gestión (MIPG) y La Guía para la Administración del Riesgo y el Diseño Controles en entidades Públicas, este modelo pertenece al habilitador transversal de Seguridad y Privacidad, de la Política de Gobierno Digital y se desarrolla mediante el Documento Maestro del Modelo de Seguridad y Privacidad de la Información y sus guías de orientación

	ELABORADO POR	**REVISADO POR**	**APROBADO POR**
Cargo/rol/CPS	Profesional III Adscrito a la Subgerencia Administrativa y Financiera	Comité Institucional de Gestion y Desempeno	Comité Institucional de Coordiancion de Control Interno
Nombre	Rafael Lastre	Erika Jimena Osorio C.	Sandra Paola León Diaz
Firma			
Fecha	Mayo de 2025	Acta No. 09 de 05-0-2025	Acta No. 06 de 05-06-2025

TABLA DE CONTENIDO

LISTA DE IMÁGENES

LISTA DE TABLAS

1 INTRODUCCIÓN

Aguas de Barrancabermeja S.A. E.S.P. es una empresa pública de carácter oficial que presta servicios públicos domiciliarios de acueducto y saneamiento básico en la zona urbana de Barrancabermeja, a través de la gestión integral de procesos para la satisfacción de los grupos de valor. Su experiencia, fortaleza en la ciudad, así como la transparencia y la capacidad técnica con altos estándares de calidad a través de la optimización de los procesos y el compromiso constante de la medición y mejora, son los principales rasgos que identifican a esta organización, cuyo enfoque principal es su responsabilidad social y ambiental, llevando servicios públicos a más de 67 mil usuarios en Acueducto y a más de 56 mil en Alcantarillado.

En Aguas de Barrancabermeja S.A. E.S.P., el Plan de Seguridad y Privacidad de la Información tiene como fin identificar y dar a conocer su implementación el cual concientice a los trabajadores, contratistas y usuarios en general del correcto tratamiento de la información teniendo siempre muy presente la privacidad de la información como objetivo principal.

El modelo busca que las entidades públicas incorporen la seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y, en general, en todos los activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.

La Política de Gobierno Digital tiene como objetivo promover lineamientos, planes, programas y proyectos en el uso y apropiación de las TIC para generar confianza en el uso del entorno digital, propendiendo el máximo aprovechamiento de las tecnologías de la información y las comunicaciones. Además establece como habilitador transversal la seguridad y privacidad de la información, mediante el cual se definen de manera detallada la implementación de controles de seguridad físicos y lógicos con el fin de asegurar de manera eficiente los trámites, servicios, sistemas de información, plataforma tecnológica e infraestructura física y del entorno de las entidades públicas de orden nacional y territorial, gestionando de manera eficaz, eficiente y efectiva los activos de información, infraestructura critica, los riesgos e incidentes de seguridad y privacidad de la información y así evitar la interrupción en la prestación de los servicios de la entidad enmarcados en su modelo de operación por procesos.

Por lo anterior, el Modelo de Seguridad y Privacidad de la Información – MSPI define los lineamientos para la implementación de la estrategia de seguridad digital, con el objetivo de formalizar al interior de las entidades un sistema de gestión de seguridad de la información – SGSI y seguridad digital, el cual contempla su operación basado

en un ciclo PHVA (Planear, Hacer, Verificar y Actuar), así como los requerimientos legales, técnicos, normativos, reglamentarios y de funcionamiento; el modelo consta de cinco (5) fases las cuales permiten que las entidades puedan gestionar y mantener adecuadamente la seguridad y privacidad de sus activos de información:

1. Diagnóstico: Se debe iniciar con un diagnóstico o un análisis GAP o de brechas, cuyo objetivo es identificar el estado actual de la entidad respecto a la adopción del MSPI. Se recomienda usar este diagnóstico al iniciar el proceso de adopción, con el fin de que su resultado sea un insumo para la fase de planificación y luego al finalizar la Fase 5 de mejora continua.

2. Planificación: Determina las necesidades y objetivos de seguridad y privacidad de la información teniendo en cuenta su mapa de procesos, el tamaño y en general su contexto interno y externo. Esta fase define el plan de valoración y tratamiento de riesgos, siendo ésta la parte más importante del ciclo.

3. Operación: La entidad implementa los controles que van a permitir disminuir el impacto o la probabilidad de ocurrencia de los riesgos de seguridad de la información identificados en la etapa de planificación.

4. Evaluación de desempeño: La entidad determina de qué manera va a ser evaluado la adopción del modelo.

5. Mejoramiento Continuo: se establecen procedimientos para identificar desviaciones en las reglas definidas en el modelo y las acciones necesarias para su solución y no repetición.

Cada una de las fases se dará por completada, cuando se cumplan todos los requisitos definidos en cada una de ellas.

Imagen 1. Ciclo del Modelo de Seguridad y Privacidad de la Información

2 JUSTIFICACIÓN

Este documento “Modelo de Seguridad y Privacidad de la Información – MSPI”, busca preservar la confidencialidad, integridad y disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación del proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos.

3 OBJETIVO

Implementar las actividades del Plan de Seguridad y Privacidad de la Información alineadas con la NTC/IEC ISO 27001:2013, la estrategia de Gobierno Digital, la Política Nacional de Seguridad Digital, CONPES 3854, en cumplimiento de las disposiciones legales vigentes.

3.1 OBJETIVOS ESPECÍFICOS

- Mediante la implementación eficiente, eficaz y efectiva del MSPI, se busca contribuir al incremento de la transparencia en la gestión pública.

- Conservar los lineamientos establecidos para el manejo de la información tanto física como digital en el marco de una gestión documental basada en Seguridad y Privacidad de la Información.

- Mitigar los incidentes de Seguridad y Privacidad de la Información, Seguridad Digital de forma efectiva, eficaz y eficiente.

- Concientizar a los funcionarios, contratistas y proveedores de Aguas de Barrancabermeja S.A. E.S.P., sobre la seguridad de la información y su importancia.

- Cumplir con los requisitos legales y normativos en materia de Seguridad y Privacidad de la información, seguridad digital y protección de la información personal.

- Apoyar en el desarrollo y ejecución del plan estratégico institucional a través del plan de seguridad y privacidad de la información.

4 ALCANCE

La Empresa Aguas de Barrancabermeja S.A. E.S.P., establece e implementa el Modelo de Seguridad de la Información (MSPI), que busca proteger la Confidencialidad, Integridad y Disponibilidad de los activos de información, garantizando los recursos necesarios para la mejora continua del modelo, y para exigir el cumplimiento de las directrices, políticas y demás lineamientos de seguridad que se definan, los cuales deben ser conocidos, entendidos y aceptados por todas las partes interesadas del Modelo de Seguridad y Privacidad de la Información (MSPI).

Este modelo aplica para todos los usuarios internos en todos los niveles jerárquicos, usuarios externos, contratistas, proveedores y terceros; que produzcan, administren, custodien o que tengan acceso a la información de Aguas de Barrancabermeja S.A. E.S.P.

5 MARCO JURÍDICO

Conforme con lo establecido en la normatividad vigente el Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC, hace referencia a las siguientes normas, que se deben tener en cuenta para el desarrollo de la apropiación del MSPI en la entidad:

- Constitución Política de Colombia. Artículo 15.

- Artículos 209 y 269 de la Constitución política

- Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.

- Decreto 2609 de 2012. Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las entidades del Estado.

- Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.

- Decreto 886 de 2014. Por el cual se reglamenta el Registro Nacional de Bases de Datos.

- Ley 1712 de 2014. 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.

- Decreto 103 de 2015. Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.

- Decreto 1074 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.

- Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

- Decreto 1080 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Cultura.

- Decreto 1081 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia.

- Decreto 1083 de 2015 establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de “11. Gobierno Digital, antes Gobierno en Línea” y “12. Seguridad Digital”.

- CONPES 3854 de 2016. Política Nacional de Seguridad Digital.

- Decreto 728 de 2017. Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico.

- 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.

- Decreto 1008 del 2018. Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

- Ley 1915 de 2018. Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.

- Decreto 612 de 2018. Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.

- Decreto 2106 de 2019, establece que las autoridades que realicen trámites, procesos y procedimientos por medios digitales, deberán disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.

- Ley 1952 de 2019. Por medio de la cual se expide el Código General Disciplinario

6 GLOSARIO

Acceso a la Información Pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados (Ley 1712 de 2014, Art. 4).

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas,

soportes, edificios, personas…) que tenga valor para la organización (ISO/IEC 27000).

Activo de Información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

Archivo: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura (Ley 594 de 2000, Art. 3).

Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización (ISO/IEC 27000).

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría (ISO/IEC 27000).

Bases de Datos Personales: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, Art. 3).

Ciberseguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética (CONPES 3701).

Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo

de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Datos Abiertos: Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, Art. 6).

Datos Personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, Art. 3).

Datos Personales Públicos: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva (Decreto 1377 de 2013, Art. 3).

Datos Personales Privados: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular (Ley 1581 de 2012, art 3 literal h).

Datos Personales Mixtos: Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.

Datos Personales Sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, Art. 3).

Derecho a la Intimidad: Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad,

que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información (ISO/IEC 27000).

MRAE: Marco de Referencia Arquitectura Empresarial.

MSPI: Modelo de Seguridad y Privacidad de la Información.

Mecanismos de protección de datos personales: Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado o cifrado.

Plan de continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro (ISO/IEC 27000).

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma (ISO/IEC 27000).

Privacidad: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias (ISO/IEC 27000).

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información.

Sistema de Gestión de Seguridad de la Información SGSI: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas,

planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua (ISO/IEC 27000).

Tratamiento de Datos Personales: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión (Ley 1581 de 2012, Art. 3).

Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad (ISO/IEC 27000).

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas (ISO/IEC 27000).

7 MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – MSPI

El Modelo de Seguridad y Privacidad de la Información contempla un ciclo de operación que consta de cinco (5) fases, que permiten una adecuada gestión de la seguridad y privacidad de los activos de información.

Imagen 2. Fases del Ciclo MSPI

8 FASES DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – MSPI

8.1 FASE DE DIAGNÓSTICO

La fase de diagnóstico permite a Aguas de Barrancabermeja S.A. E.S.P. establecer el estado actual de la implementación de la seguridad y privacidad de la información, para tal fin se debe utilizar el “Instrumento de Evaluación MSPI” con el que se identifica de forma específica los controles implementados y faltantes y así tener insumos fundamentales para la fase de planificación.

Este autodiagnóstico se debe realizar antes de iniciar la fase de planificación, y actualizarlo posterior al término de la fase de evaluación de desempeño, esto con el fin de identificar los avances en la implementación del Modelo en la entidad, el resultado que se obtenga posterior a la fase de evaluación de desempeño será incluido como un insumo, en la fase de mejoramiento continuo.

Se recomienda por parte del MinTic revisar aspectos internos tales como el talento humano, procesos y procedimientos, estructura organizacional, cadena de servicio, recursos disponibles, cultura organizacional, entre otros.

8.1.1 ESTADO ACTUAL DE LA EMPRESA

8.1.1.1 Misión

Somos una Empresa que presta servicios públicos domiciliarios de acueducto y saneamiento básico en el área de influencia, a través de la gestión integral de procesos para la satisfacción de los grupos de valor.

8.1.1.2 Visión

Ser una Empresa posicionada y sostenible, con altos estándares de calidad a través de la optimización de los procesos y el compromiso constante de medición y mejora.

8.1.1.3 Objetivos Estratégicos

- Garantizar una excelente satisfacción de nuestros usuarios mediante la optimización de procesos tanto operativos como estratégicos y de apoyo, realizando una mejor planificación, así como inversiones encaminadas al cumplir con altos estándares de calidad y continuidad, aumentar participación en el mercado, conservación y preservación de los recursos naturales y capacitación a nuestros colaboradores.

- Generar un clima de confianza y mejorar imagen frente a nuestras partes interesadas mediante la adopción las mejores prácticas de gobierno transparente, implementando herramientas y actividades de seguimiento y control.

- Ampliación e implementación de nuevas líneas de negocios que permitan captar recursos para ser reinvertidos en proyectos que mejoren la prestación de los servicios, la cobertura y por ende la calidad de vida de nuestros usuarios.

- Mejorar la gestión de recursos económicos y financieros, mediante la correcta planificación de presupuesto y reducción de costos y gastos, generando estrategias para el recaudo, así como y la gestión de fuentes de financiación con los mejores beneficios para la empresa.

8.1.1.4 Organigrama

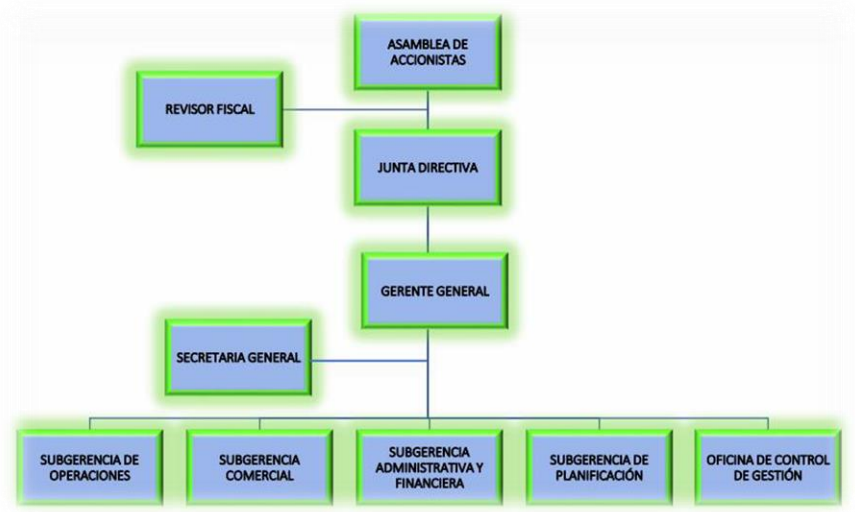

Imagen 3. Organigrama de Aguas de Barrancabermeja S.A. E.S.P.

8.1.2 IDENTIFICACIÓN DEL NIVEL DE MADUREZ

Para identificar el Nivel de Madurez que tiene la Empresa con respecto a la seguridad y privacidad de la información, se utilizó la herramienta “Instrumento de Evaluación MSPI de MINTIC”, el cual arrojo el siguiente resultado:

Imagen 4. Resultado “Instrumento de Evaluación MSPI de MINTIC” aplicado

8.1.3 LEVANTAMIENTO DE INFORMACIÓN

Son partes interesadas de Aguas de Barrancabermeja S.A. E.S.P., las entidades públicas y privadas legalmente constituidas, que interactúan con la misma; teniendo presente los requisitos normativos internos, legales o reglamentarios y las obligaciones contractuales.

PARTE INTERESADA	DEFINICIÓN
Gobierno	Ministerio de las TIC, órganos de control, función pública, superintendencia de servicios públicos, entre otras.
Funcionarios	Servidores Públicos: Personas que prestan sus servicios en las Empresas Industriales y Comerciales del Estado.
	Contratistas: Personas naturales que apoyan las labores administrativas mediante la modalidad de prestación de servicio.
Proveedores	Persona natural, jurídica u organización que tiene vínculo contractual con la empresa para suministrar bienes, obras o servicios.
Usuarios / Comunidad	Ciudadanos que están interesados en la misión propia de la Empresa.

Tabla 1. Partes interesadas de Aguas de Barrancabermeja S.A. E.S.P.

8.2 FASE PLANIFICACIÓN

Para el desarrollo de esta fase, se deben utilizar los resultados de la fase anterior y proceder a elaborar el Plan de Seguridad y Privacidad de la Información con el objetivo de que la entidad realice la planeación del tiempo, recursos y presupuesto de las actividades que va a desarrollar relacionadas con el MSPI.

8.2.1 PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA EMPRESA AGUAS DE BARRANCABERMEJA S.A. E.S.P.

El Plan de Seguridad y Privacidad de la Información de Aguas de Barrancabermeja S.A. E.S.P. tiene como fin identificar y dar a conocer la implementación de un plan el cual concientice a los trabajadores, contratistas y usuarios en general del correcto tratamiento de la información teniendo siempre muy presente la privacidad de la información como objetivo principal.

8.2.1.1 OBJETIVO DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Describir las medidas necesarias por parte de Aguas de Barrancabermeja S.A. E.S.P. para la protección de los activos de información, los recursos y la tecnología de la entidad, con el propósito de evitar accesos no autorizados, divulgación, duplicación, interrupción de sistemas, modificación, destrucción, pérdida, robo, o mal uso, que se pueda producir de forma intencional o accidental, frente a amenazas internas o externas, asegurando el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

8.2.1.2 ALCANCE DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Plan de Seguridad y Privacidad de la Información y su política son aplicables a todos los trabajadores de Aguas de Barrancabermeja S.A. E.S.P., a sus recursos, procesos y procedimientos tanto internos como externos, así mismo al personal vinculado a la entidad, contratistas y terceras partes, que usen activos de información que sean propiedad de la entidad. Basados en los resultados de la etapa anterior, se procede a la elaboración del plan de seguridad y privacidad de la información alineado con el objetivo misional de la entidad, con el propósito de definir las acciones a implementar a nivel de seguridad y privacidad de la información, a través de una metodología de gestión del riesgo.

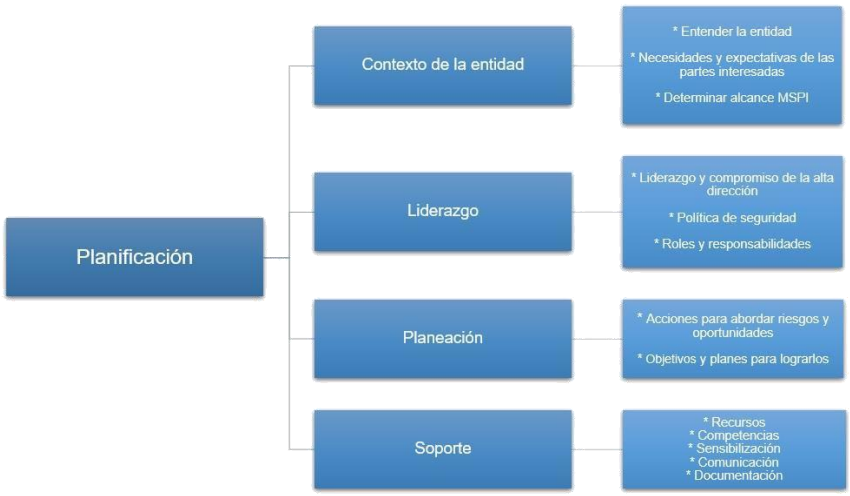

Imagen 5. Contextualización de las Etapas de la Planificación

8.2.2 CONTEXTO DE LA ENTIDAD

La Empresa tiene como mayor accionista al Distrito de Barrancabermeja. Su experiencia, fortaleza en la ciudad, así como la transparencia y capacidad técnica, son los principales rasgos que identifican a esta organización, cuyo enfoque principal es su responsabilidad social y ambiental, llevando servicios públicos a más de 67 mil usuarios en Acueducto y a más de 56 mil usuarios en Alcantarillado.

La Empresa Aguas de Barrancabermeja S.A. E.S.P. es una entidad ubicada en Barrancabermeja, un municipio del Departamento de Santander, Colombia que se encuentra a 114 km de Bucaramanga, capital del departamento. Tiene como misión satisfacer las necesidades de acueducto y saneamiento básico con procesos eficientes y del más alto nivel de calidad de los habitantes de la zona urbana de Barrancabermeja, a través de un equipo multidisciplinario que participa de la formación en atención al cliente y en nuevas tecnologías, buscando la mejora continua al incrementar los indicadores de responsabilidad social, sostenibilidad ambiental y crecimiento financiero que contribuyen con el desarrollo del Distrito.

Por tal motivo, es importante vincular las nuevas tecnologías de la información en los procesos propios y misionales de la Empresa, teniendo como base las mejoras en los sistemas de información, innovando e implementando infraestructura tecnológica de acuerdo con las necesidades propias de la entidad y modernizando los canales de comunicación tanto de manera interna como externa logrando un desarrollo tecnológico considerable.

8.2.2.1 CONTEXTO TECNOLÓGICO DE LA EMPRESA AGUAS DE BARRANCABERMEJA S.A. E.S.P.

Conectividad: La conectividad de la entidad se establece con un canal dedicado de 100 MB con el ISP (Proveedor de Servicios de Internet) Movistar, permitiendo la comunicación con las diferentes sedes y además brindado la conexión a internet al edificio administrativo, logrando que el canal de comunicación soporte las necesidades de la entidad. La Empresa Aguas de Barrancabermeja S.A. E.S.P. debido a su personal, tanto de planta como contratista y acorde al número de sedes y las distintas infraestructuras físicas, la arquitectura de conectividad que se desea para su funcionamiento es híbrida, es decir, debe tener conectividad por cable y por medios inalámbricos.

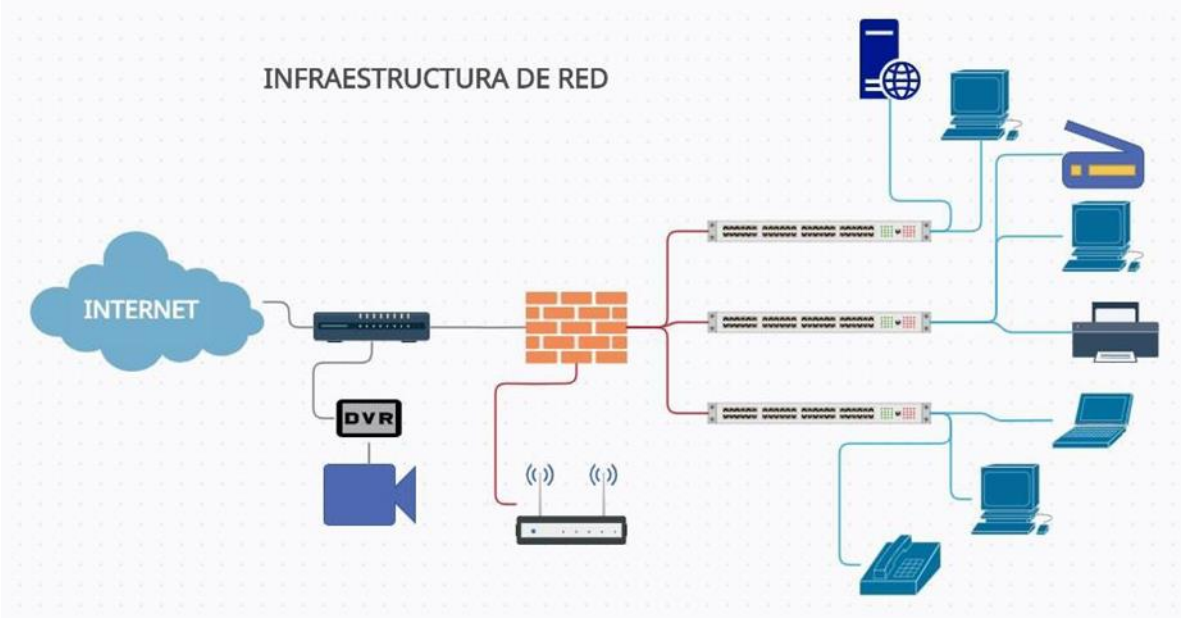

Imagen 6. Infraestructura de Red de Aguas de Barrancabermeja S.A. E.S.P.

Red local: La red de área local (LAN) debe garantizar que al backbone llegue la conexión dedicada en fibra y pueda ser distribuida a través de cableado al menos en categoría 5e en la sede administrativa.

Red local inalámbrica: Se realiza una revisión de la red WiFi actual para optimizar la calidad de su diseño, dentro de los cuales se debe incluir la perfilación de usuarios para su utilización y manejo. En los pisos 1, 2 se encuentran los dispositivos que brindan la conexión wifi a trabajadores, contratistas y demás usuarios tipificados.

8.2.2.2 EXPECTATIVAS DE LAS PARTES INTERESADAS

Partes Interesadas	Interno / Externo	Necesidades	Requisitos	Expectativas
Entes de control	Externo	Disponibilidad, integridad y confidencialidad en la información Disponibilidad, accesibilidad de la información	Cumplir con la normatividad aplicable tanto gubernamentales como las del MSPI Ley de transparencia y acceso a la Información Pública y Ley anticorrupción	Cumplir con los requerimientos y las directrices establecidas por los diferentes entre de control.
Junta Directiva	Interno	Disponibilidad, integridad y confidencialidad en la información.	Cumplir con la normatividad aplicable tanto gubernamentales como las del MSPI. Acuerdos de Niveles del Servicio.	Información solicitada y generada por la entidad para la toma de decisiones.
Directivos, Trabajadores	Interno	Contar con herramientas de nuevas tecnologías de la información. Disponibilidad, continuidad del Servicio de Sistemas de Información y su mantenimiento preventivo y correctivo. Continuidad y disponibilidad correo institucional.	Soporte tecnológico que establezca las directrices establecidas del SGSI. Disponibilidad del servicio. Política de Seguridad de la Información.	Aprobación del SGSI a través de aplicacion de las políticas. Obtener una disponibidad del servicio. Minimizar el riesgo del uso inadecuado de la información. Apropiación e implementación de las Nuevas Tecnologías.
Contratistas, Proveedores	Interno / Externo	Especificaciones técnicas de los requerimientos, acorde a las políticas de seguimiento del SGSI. Disponibilidad y continuidad de los sistemas de información y portal web. Contar con herramientas de nuevas tecnologías de la información	Cumplimiento en tiempos de entrega pactados. Acuerdo de confidencialidad con terceros. Política de Seguridad de la Información.	Cumplimiento de los acuerdos de nivel de servicio. Reducir el riesgo del uso inadecuado de la información. Aplicar protocolos y controles de seguridad de la información. Minimizar documentos físicos por medio de certificados en línea.

Partes Interesadas	Interno / Externo	Necesidades	Requisitos	Expectativas
Suscriptores, comunidad	Externo	Transparencia en el desarrollo de los procesos institucionales de la entidad. Consistencia y veracidad de la información suministrada por la empresa. Disponibilidad y accesibilidad de la información.	Aplicar las directrices establecidas por Gobierno Digital. Ley de transparencia y acceso a la Información Pública y Ley anticorrupción.	Disponibilidad de la información. Facilitar el acceso a la información pública de manera permanente dando cumplimiento a la Transparencia y acceso a la información (Ley 1712 de 2014).

Tabla 2. Expectativas de partes interesadas Aguas de Barrancabermeja

8.2.2.3 ALCANCE MSPI

El alcance del Modelo de Seguridad y Privacidad de la información - MSPI de Aguas de Barrancabermeja S.A. E.S.P. es aplicable a todos los procesos, trabajadores, contratistas, proveedores y comunidad en general, quienes, en cumplimiento de sus funciones compartan, hagan uso, recolecten, procesen, se consulte e intercambie información; así como a los entes de control o entidades que accedan ya sea de manera interna o externamente a cualquier tipo de información independientemente de su ubicación, logrando como objetivo buscar proteger y preservar la integridad y disponibilidad de los activos de información.

8.2.3 LIDERAZGO

8.2.3.1 LIDERAZGO Y COMPROMISO DE LA ALTA DIRECCIÓN

La Empresa Aguas de Barrancabermeja S.A. E.S.P. se compromete a liderar la implementación del MSPI, para lo cual delega la responsabilidad de la formulación, ejecución, seguimiento e implementación de los planes de mejoramiento del Modelo de Seguridad y Privacidad de la información a la Subgerencia Administrativa y Financiera, quien debe medir la eficacia del SGSI (Sistema de Gestión de Seguridad de la Información) y solicitar los recursos que sean necesarios, para garantizar la seguridad y privacidad de la información en la entidad.

8.2.3.2 POLÍTICA DE SEGURIDAD

La Empresa Aguas de Barrancabermeja S.A. E.S.P. cuenta con una Política General de Seguridad y Privacidad de la Información, que tiene como objetivo administrar,

proteger y preservar de manera eficiente la información de la Empresa junto con los medios utilizados para la manipulación o procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de las características de confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

Para Aguas de Barrancabermeja S.A. E.S.P., la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta política aplica a la Entidad según como se defina en el alcance, sus trabajadores, contratistas, practicantes, proveedores y la comunidad en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de Aguas de Barrancabermeja S.A. E.S.P.
- Garantizar la continuidad del negocio frente a incidentes.
- La Empresa Aguas de Barrancabermeja S.A. E.S.P. ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

8.2.3.3 ROLES Y RESPONSABILIDADES

ROL	CARGO
Líder del SGSI (Sistema de Gestión de Seguridad de la Información)	Profesional III TICS Subgerencia Administrativa y Financiera

Tabla 3. Roles y responsabilidades del SGSI

Objetivo: Asegurar que los trabajadores de la entidad conozcan qué se espera de ellos, cuál es su impacto en la seguridad de la información y de qué manera contribuyen con la adopción del MSPI.

- Identificación de riesgos realizada por los procesos.
- Generar análisis y evaluación de riesgos, para posteriormente llevar a cabo la gestión y tratamiento de los mismos.
- Validar la implementación y operación del SGSI y MSPI.
- Monitorear la implementación del plan de tratamiento de riesgos para lograr los objetivos de control identificados
- Definir y aplicar los procedimientos de seguimiento y revisión del SGSI.
- Verificar el diseño y definición de los procedimientos y controles para detectar y dar respuesta oportuna a los incidentes de seguridad.
- Coordinar la realización de auditorías internas al SGSI.
- Facilitar y promover el desarrollo de iniciativas sobre seguridad de la información.
- Generar revisiones regulares de la eficacia del SGSI (que incluyen el cumplimiento de la política y objetivos del SGSI, y la revisión de los controles de seguridad) teniendo en cuenta los resultados de las auditorias de seguridad, incidentes, medición de la eficacia sugerencias y retroalimentación de todas las partes interesadas.

8.2.4 PLANEACIÓN

8.2.4.1 ACCIONES PARA ABORDAR LOS RIESGOS Y OPORTUNIDADES

8.2.4.1.1 Identificación Valoración y Tratamiento de los Riesgos

La Empresa Aguas de Barrancabermeja S.A. E.S.P. realiza la identificación y evaluación de las amenazas de las vulnerabilidades relativas a los activos de información, ya sea sistemas de información, infraestructura y recurso humano, la probabilidad de ocurrencia y su impacto.

8.2.4.1.2 Valoración de los riesgos de seguridad de la información

La Empresa Aguas de Barrancabermeja S.A. E.S.P. debe asegurar que las valoraciones repetidas de los riesgos de seguridad y privacidad de la información produzcan resultados consistentes, válidos y comparables. Estructurar una

metodología que permita gestionar los riesgos de seguridad y privacidad de la información.

Para esto es importante tener en cuenta:

- Identificar los riesgos que causen la perdida de confidencialidad, integridad, disponibilidad, privacidad de la información, así como la continuidad de la operación de la entidad dentro del alcance del MSPI.
- Definir criterios para valorar las consecuencias de la materialización de los riesgos, y la probabilidad de su ocurrencia.
- Aplicar el proceso de valoración del riesgo que permita determinar los riesgos asociados a la perdida de confidencialidad, integridad y disponibilidad de la información que se encuentre dentro del alcance.
- Determinar los niveles de riesgo.
- Realizar la comparación entre los resultados del análisis y los criterios de los riesgos establecidos
- Priorización de los riesgos analizados para su tratamiento.

8.2.4.1.3 Plan de tratamiento de los riesgos de seguridad de la información

La Empresa Aguas de Barrancabermeja S.A. E.S.P. cuenta con un Plan de tratamiento de los riesgos de seguridad de la información, que tiene como objetivo controlar y minimizar los riesgos asociados a los procesos tecnológicos existentes, con el fin de salvaguardar los activos de información, el manejo de medios, control de acceso y gestión de usuarios.

La Empresa Aguas de Barrancabermeja S.A. E.S.P. implementará como metodología el Ciclo PHVA, que es una herramienta de mejora continua, permitiendo en la entidad una mejora integral de la competitividad y del servicio con el objetivo de mejorar continuamente la calidad ofrecida a los usuarios, optimizar la productividad y aumentar a través de las nuevas tecnologías la rentabilidad de la empresa.

IDENTIFICACIÓN DEL RIESGO			SEGUIMIENTO AL PLAN DE TRATAMIENTO		
FACTOR / FUENTE DE RIESGO	**CAUSA**	**RIESGO**	**PLAN DE ACCIÓN**	**RESPONSABLE**	**SEGUIMIENTO**
Malas prácticas de los usuarios en el uso de los recursos compartidos	cargue de informacion que no cumple OCR (reconocimiento optimo de caracteres: busqueda, pdf editable) ni TRD que no viabiliza backup en la Nube	Posibilidad de afectación económica y reputacional por daño o pérdida de información	Impartir lineamiento requisito cargue de informacion digital OCR y con base en la TRD, en los recursos compartidos socializado en todas las dependencias, solo los recursos compartidos que cumplan el requisito seran objeto de backup en nube a. Realizar revisión y depuración de las carpetas de información compartidas que no cumplan con estructura de TRD y OCR..	Profesional III TICS Subgerencia Administrativa y Financiera	Semestral
Recursos insuficientes para actualizacion de infraestructura tecnologica	Recursos insuficientes para actualizacion de infraestructura tecnologica	Posibilidad de fallas en el acceso a la informacion de los sistemas de información institucionales (comercial, financiero, nómina, orfeo, otros), por falta de infaestructura tecnologica actualizada,	Actualización periódica de los componentes de hardware y software (sistemas de información) con base en los recursos disponibles	Profesional III TICS Subgerencia Administrativa y Financiera	Trimestral

IDENTIFICACIÓN DEL RIESGO			SEGUIMIENTO AL PLAN DE TRATAMIENTO		
FACTOR / FUENTE DE RIESGO	**CAUSA**	**RIESGO**	**PLAN DE ACCIÓN**	**RESPONSABLE**	**SEGUIMIENTO**
1.Vulnerabilidades técnicas sin conocer, uso de software desactualizado. 2. Falta de sensibilización del personal sobre ataques cibernéticos.	1. Vulnerabilidades técnicas sin conocer, uso de software desactualizado. 2. Falta de sensibilización del personal sobre ataques cibernéticos.	Ataques informáticos internos/externos a la infraestructura tecnológica (páginas web, software misional, hardware, aplicaciones, equipos de comunicación, equipos de seguridad, red interna) Pérdida de integridad - disponibilidad de los sistemas de información institucionales (comercial, financiero, nómina, orfeo, otros)	1. Migración de los sistemas de información a la nube con componentes de seguridad actualizados (100%) 2. Jornada de sensibilización al personal sobre seguridad de la información	Profesional III TICS Subgerencia Administrativa y Financiera	Trimestral Semestral

Tabla 4. Identificación y seguimiento de riesgos de seguridad de información

8.2.5 SOPORTE

8.2.5.1 RECURSOS

Dada la importancia del Sistema de Gestión de Seguridad de la información – SGSI que hace parte del Sistema Integrado de Gestión de Aguas de Barrancabermeja S.A. E.S.P., para mantenerlo en operación, hacerle seguimiento y mejora, es necesario contar con recursos económicos, humanos con las competencias específicas, la infraestructura tecnológica actualizada y el apoyo de la Alta Dirección, asignando los recursos anuales, para la adquisición y sostenimiento del mismo. En cuanto al seguimiento y mejora continua, se realiza de conformidad con el procedimiento Formulación y Evaluación Plan de Acción, Planes de Mejora, Plan de Auditorías Internas y Externas, capacitaciones, asesorías y cursos relacionadas, en conformidad con el procedimiento que hace parte del MIPG.

8.2.5.2 COMPETENCIA, TOMA DE CONCIENCIA Y COMUNICACIÓN

La Empresa Aguas de Barrancabermeja S.A. E.S.P. deberá garantizar una correcta comunicación, sensibilización y concientización con respecto a la seguridad y privacidad de la información, en la que todos sus funcionarios estén al tanto de la política de seguridad y privacidad, cuál es su rol en el cumplimiento del MSPI, beneficios y consecuencias de no poner en práctica las reglas definidas en el modelo (desde el punto de vista de seguridad y privacidad de la información).

8.3 FASE DE OPERACIÓN

8.3.1 PLANIFICACIÓN E IMPLEMENTACIÓN

En esta fase y basado en la Norma ISO 27001:2013, Capítulo 8 - Operación, indica que la entidad debe planificar, implementar y controlar los procesos necesarios para cumplir los objetivos y requisitos de seguridad y llevar a cabo la valoración y tratamiento de los riesgos de la seguridad de la información.

Imagen 7. Diagrama de Implementación

8.3.1.1 CONTROL Y PLANEACIÓN OPERACIONAL

La implementación y operación del sistema gestión de seguridad de la información de Aguas de Barrancabermeja S.A. E.S.P., se basa en la administración del riesgo de la seguridad de la información. Por este enfoque, la entidad se compromete a implementar los controles procedimentales, tecnológicos y de talento humano que sean necesarios para llevar los riesgos de seguridad de la información a niveles aceptables.

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

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de Aguas de Barrancabermeja S.A. E.S.P. se encuentra publicado en el sitio web www.aguasdebarrancabermeja.gov.co

8.3.1.3 INDICADORES DE GESTIÓN

En la siguiente tabla se observan los indicadores registrados para el Sistema de Gestión de Seguridad SGSI articulados con los objetivos del sistema:

ITEM	DESCRIPCIÓN	INDICADORES
POLÍTICAS SGSI (Sistema de Gestión de la Seguridad de la Información)	Política de Backups	(N° Backups realizados / N° equipos de cómputo) x 100
	Política de Escritorio y Pantalla Limpia	(N° Revisiones Pcs / N° Equipos de cómputo) x 100

Tabla 5. Indicadores de Gestión SGSI de Aguas de Barrancabermeja

8.4 FASE EVALUACION DE DESEMPEÑO

Una vez culminada las actividades del MSPI, se evalúa la efectividad de las acciones tomadas a través de los indicadores definidos en la Fase de Implementación que debe incluir la correcta interacción entre el MSPI, MIPG y los requerimientos de la Ley 1581 de 2012 “Protección de datos personales”, Ley 1712 de 2014 “Ley de Transparencia y Acceso a la Información Pública”, Decreto 2106 de 2019 o cualquier norma que las reglamente, adicione, modifique o derogue.

La Fase EVALUACIÓN DEL DESEMPEÑO en la Norma ISO 27001:2013 descrita en el Capítulo 9 - Evaluación del desempeño, define los requerimientos para evaluar periódicamente el desempeño de la seguridad de la información y eficacia del sistema de gestión de seguridad de la información.

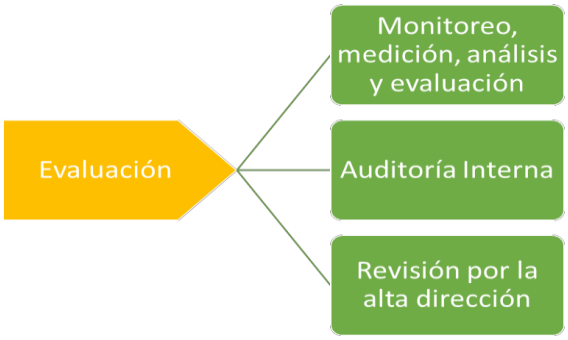

Imagen 8. Diagrama de Evaluación

8.4.1 MONITOREO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN

Se deben llevar a cabo actividades para realizar seguimiento a:

- La programación y ejecución de las actividades de auditorías internas del SGSI.
- La programación y ejecución de las revisiones por parte del Líder del proceso al alcance del sistema de gestión y las mejoras del mismo.
- Los Planes de seguridad tanto para el establecimiento como la ejecución y actualización de los mismos, como respuesta a los aspectos identificados a nivel de las revisiones y seguimientos realizados en esta fase del SGSI.
- A los registros de incidentes de seguridad que podrían tener impacto en la eficacia o el desempeño del SGSI.

8.4.2 AUDITORÍA INTERNA

La Empresa Aguas de Barrancabermeja S.A. E.S.P. deberá garantizar la realización de las Auditorías Internas con el fin de obtener información sobre el cumplimiento del MSPI.

8.4.3 REVISIÓN POR LA DIRECCIÓN

La revisión por la Alta Dirección se realiza una vez al año o cuando la Alta Dirección lo considere pertinente y dejando un informe de manera escrita denotando las acciones de mejora, con el fin de asegurar la conveniencia, adecuación, eficacia, eficiencia y efectividad del Sistema de Gestión de Seguridad de la Información. La información presentada incluye aspectos de gestión del servicio, basados en las

buenas prácticas del Estándar ISO 20000- 1:2018 e ISO 27000 – 1:2013, Decreto 1581 de 2012 (por la cual se dictan disposiciones generales para la protección de datos personales. Aquellas actividades que se inscriben en el marco de la vida privada o familiar de las personas naturales.) y Decreto 1377 de 2013 (Por el cual se reglamenta parcialmente la Ley 1581 de 2012).

8.5 FASE DE MEJORAMIENTO CONTINUO

Una vez culminada las actividades del MSPI de la fase evaluación y desempeño, se debe consolidar los resultados obtenidos de la Fase de Evaluación de Desempeño y diseñar el Plan de mejoramiento continuo de seguridad y privacidad de la información, tomando las acciones oportunas para mitigar las debilidades identificadas.

En esta FASE DE MEJORAMIENTO CONTINUO en la Norma ISO 27001:2013 Capítulo 10 – Mejora – “se establece para el proceso de mejora del Sistema de Gestión de Seguridad de la Información a partir de las no-conformidades que ocurran, las organizaciones deben establecer las acciones más efectivas para solucionarlas y evaluar la necesidad de acciones para eliminar las causas de la no conformidad con el objetivo de que no se repitan”.

Imagen 9. Diagrama de Fase de Mejoramiento Continuo

8.5.1 ACCIONES CORRECTIVAS

El objetivo de estas acciones es eliminar la causa de problemas asociados con los requisitos del SGSI, con el fin de prevenir que ocurran nuevamente.

- Determinar y evaluar las causas de los problemas del SGSI e incidentes de seguridad de la información.

- Diseñar e implementar la acción correctiva necesaria.
- Revisar la acción correctiva tomada.

8.5.2 MEJORA CONTINUA

Una vez el Sistema de Gestión de Seguridad de la Información se haya diseñado e implementado se hace necesario cerrar el ciclo con el mejoramiento continuo del mismo.

Para esto se diseña un Plan de Auditorías Internas teniendo en cuenta el estado e importancia de los procesos y la criticidad de la información y recursos informáticos. Estos planes incluirán el alcance, frecuencia de realización, métodos de la auditoría, pruebas y selección de los auditores.

El objetivo de la Auditoría Interna es determinar si los objetivos de control, procesos, y procedimientos del MSPI:

- Están implementados y se desarrollan correctamente de acuerdo con los requisitos del Estándar de ISO 27001:2013.
- Cumplen los requisitos normativos.

Estas auditorías se encuentran enmarcadas dentro del procedimiento, que define las responsabilidades y requisitos para la planificación y realización de las mismas, la presentación de resultados y mantenimiento de los registros.

Además de los resultados de las auditorías, como entrada a este procedimiento se prevé también la retroalimentación de todos los participantes del SGSI y de la entidad, la revisión de los requisitos de la norma, el manejo de no conformidades, medición de los indicadores y sugerencias.

Dentro de la Fase de Mantenimiento y Mejora se definen las acciones y se deben tener en cuenta algunas consideraciones especiales cuando se refiera a Auditorías especificas a los Sistemas de Información.