2023 - 2026

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

DIRECCIÓN ADMINISTATIVA Y FINANCIERA

OFICINA DE SISTEMAS

Aguas del Cesar S.A. E.S.P.

Tabla de Contenido

1. INTRODUCCIÓN

Actualmente, la información es considerada como uno de los activos más importantes y por lo tanto valioso dentro de una organización, siempre y cuando sea utilizada de manera adecuada, integra, segura, oportuna y de manera responsable, lo que implica, que se hace necesario que nuestra organización posea o implemente una adecuada gestión de los recursos y activos de información que aseguren y controlen el acceso, tratamiento y uso de la información.

El aseguramiento y la protección de la seguridad de la información de las organizaciones y de los datos de carácter personal de los usuarios, representan un reto al momento de pretender garantizar su confidencialidad, integridad, disponibilidad y privacidad, razón por la cual, la seguridad de la información se ha convertido en uno de los aspectos de mayor preocupación a nivel mundial.

AGUAS DEL CESAR S.A. E.S.P. es consciente que la protección y aseguramiento de su información es fundamental para garantizar su debida gestión financiera, administrativa y operativa, razón por la cual debe establecer un marco normativo de Seguridad de la Información que contemple políticas, límites, responsabilidades y obligaciones frente a la seguridad y privacidad de la información de la entidad.

En atención a lo anterior, la entidad asumió el reto de implementar el Sistema de Gestión de Seguridad de la Información (SGSI), siguiendo los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) de la Estrategia de Gobierno en Línea, a su vez reglamentado a través del Decreto 1078 de 2015 para el sector de tecnologías de la información y comunicaciones y el Decreto 2573 de 2014 por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea.

2. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Definición

Mediante esta política de Seguridad y Privacidad de la Información, la empresa Aguas del Cesar S.A. E.S.P., muestra su posición frente a la protección de los activos de la información que soportan todos los procesos de la Entidad y a su vez, apoya la implementación del SGSI por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

2.1 OBJETIVO GENERAL

Implementar estrategias que permitan garantizar y llevar a cabo el Plan de Seguridad y Privacidad de la Información de la empresa Aguas del Cesar S.A. E.S.P., en cada uno de sus procesos.

2.2 OBJETIVOS ESPECÍFICOS

- Cumplir con la política de Seguridad de la Información.
- Disminuir cualquier riesgo tecnológico que pueda afectar la entidad.
- Proteger los activos de la información de la entidad.
- Fomentar el buen uso de la seguridad de la información en los funcionarios, contratistas y clientes de la empresa.
- Dar lineamientos para la implementación de mejores prácticas de seguridad que permita identificar infraestructuras críticas en las entidades.

3. ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

La política de Seguridad y Privacidad de la Información es aplicable a todos los niveles y procesos de la entidad, servidores públicos, contratistas y terceros que estén relacionados con la empresa Aguas del Cesar S.A. E.S.P. Así mismo, esta Plan aplica a toda la información creada, procesada o utilizada por la entidad, sin importar el medio, formato o presentación o lugar en el cual se encuentre.

3.1 MARCO LEGAL

Marco Legal		
Ítem	Marco Legal	Descripción
1	Decreto 1151 de 2008	Lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamenta parcialmente la Ley 962 de 2005, y se dictan otras disposiciones.
2	Ley 1955 del 2019	Establece que las entidades del orden nacional deberán incluir en su plan de acción el componente de transformación digital, siguiendo los estándares que para tal efecto defina el Ministerio de Tecnologías de la Información y las Comunicaciones (Min TIC).
3	Ley 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
4	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.
5	Ley 1753 de 2015	Por la cual se expide el Plan Nacional de Desarrollo 2014-2018 "TODOS POR UN NUEVO PAIS" "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.
6	Decreto 235 de 2010	Por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones públicas
7	Decreto 2693 de 2012	Por el cual se establecen los lineamentos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009, 1450 de 2011, y se dictan otras disposiciones.
8	Decreto 1377 de 2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012" o Ley de Datos personales.
9	Decreto 2573 de 2014	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
10	Decreto 2433 de 2015	Por el cual se reglamenta el registro de TIC y se subroga el título 1 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.
11	Decreto 1008 de 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.
12	Resolución 2710 de 2017	Por la cual se establecen los lineamientos para la adopción del protocolo IPv6.
13	Resolución 3564 de 2015	Por la cual se reglamentan aspectos relacionados con la Ley de Transparencia y Acceso a la Información Pública.

14	Resolución 3564 2015	Reglamenta algunos artículos y parágrafos del Decreto número 1081 de 2015 (Lineamientos para publicación de la Información para discapacitados)
15	Norma Técnica Colombiana NTC 5854 de 2012	Accesibilidad a páginas web El objeto de la Norma Técnica Colombiana (NTC) 5854 es establecer los requisitos de accesibilidad que son aplicables a las páginas web, que se presentan agrupados en tres niveles de conformidad: A, AA, y AAA.

3.2 BASES METODOLÓGICAS

- Norma ISO/IEC 27001:2013.
- Modelo de Seguridad y Privacidad de la Información de Gobierno Digital –MSPI.
- Instrumento de Evaluación MSPI MINTIC.

3.3 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.

- **Activo de la 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.

- **Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

- **Análisis de Riesgos:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

- **Análisis de Riesgos Cualitativos:** Análisis de riesgos en el que se usa algún tipo de escalas de valoración para situar la gravedad del impacto y la probabilidad de ocurrencia.

- **Análisis de Riesgos Cuantitativo:** Análisis de riesgos en función de las pérdidas financieras que causaría el impacto.

- **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.

- **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.

- **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales.

- **Base de Datos Personales:** Conjunto organizado de datos personales que sea objeto de Tratamiento.

- **Confidencialidad:** Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

- **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.

- **Control Correctivo:** Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas relevantes. Supone que la amenaza ya se ha materializado pero que se corrige.

- **Control Detectivo:** Control que detecta la aparición de un riesgo, error, omisión o acto deliberado. Supone que la amenaza ya se ha materializado, pero por sí mismo no la corrige.

- **Control Disuasorio:** Control que reduce la posibilidad de materialización de una amenaza, p.ej., por medio de avisos o de medidas que llevan al atacante a desistir de su intención.

- **Control Preventivo:** Control que evita que se produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse.

- **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

- **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.

- **Encargado del Tratamiento de Datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento.

- **Estimación de Riesgos:** Proceso de comparar los resultados del análisis de riesgos con los criterios de riesgo para determinar si el riesgo y/o su magnitud es aceptable o tolerable.

- **Evaluación de Riesgos:** Proceso global de identificación, análisis y estimación de riesgos.

- **Fase Diagnostico:** Permite identificar el estado actual de la entidad con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información.

- **Fase Evaluación de Desempeño (VERIFICAR):** Una vez implantada la mejora, se establece un periodo de prueba para verificar el correcto funcionamiento de las acciones implementadas.

- **Fase Implementación (HACER):** En esta fase se ejecuta el plan establecido que consiste en implementar las acciones para lograr mejoras planteadas.

- **Fase Planificación (PLANEAR):** En esta fase se establecen los objetivos a alcanzar y las actividades del proceso susceptibles de mejora, así como los indicadores de medición para controlar y cuantificar los objetivos.

- **Fase Mejora Continua (ACTUAR):** Se analizan los resultados de las acciones implementadas y si estas no se cumplen los objetivos definidos se analizan las causas de las desviaciones y se generan los respectivos planes de acciones.

- **Gestión de Riesgos:** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.

- **Incidente de Seguridad de La Información:** Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

- **Información Pública Clasificada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014.

- **Información Pública Reservada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014.

- **Integridad:** Propiedad de la información relativa a su exactitud y completitud.

- **ISO/IEC 27001:2013:** Norma que establece los requisitos para un sistema de gestión de la seguridad de la información (SGSI). Primera publicación en 2005; segunda edición en 2013. Es la norma en base a la cual se certifican los SGSI a nivel mundial.

- **Ley de Habeas Data:** Se refiere a la Ley Estatutaria 1266 de 2008.

- **Ley de Transparencia y Acceso a la Información Pública:** Se refiere a la Ley Estatutaria 1712 de 2014.

- **Mecanismos de Protección de Datos Personales:** Lo constituyen las distintas alternativas con que cuentan la entidad para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.

- **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, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información.

- **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.

- **Registro Nacional de Bases de Datos:** Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)

- **Responsabilidad Demostrada:** Conducta desplegada por los Responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

- **Responsable del Tratamiento de Datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).

- **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.

- **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

- **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).

- **Titulares de La Información:** Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)

- **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).

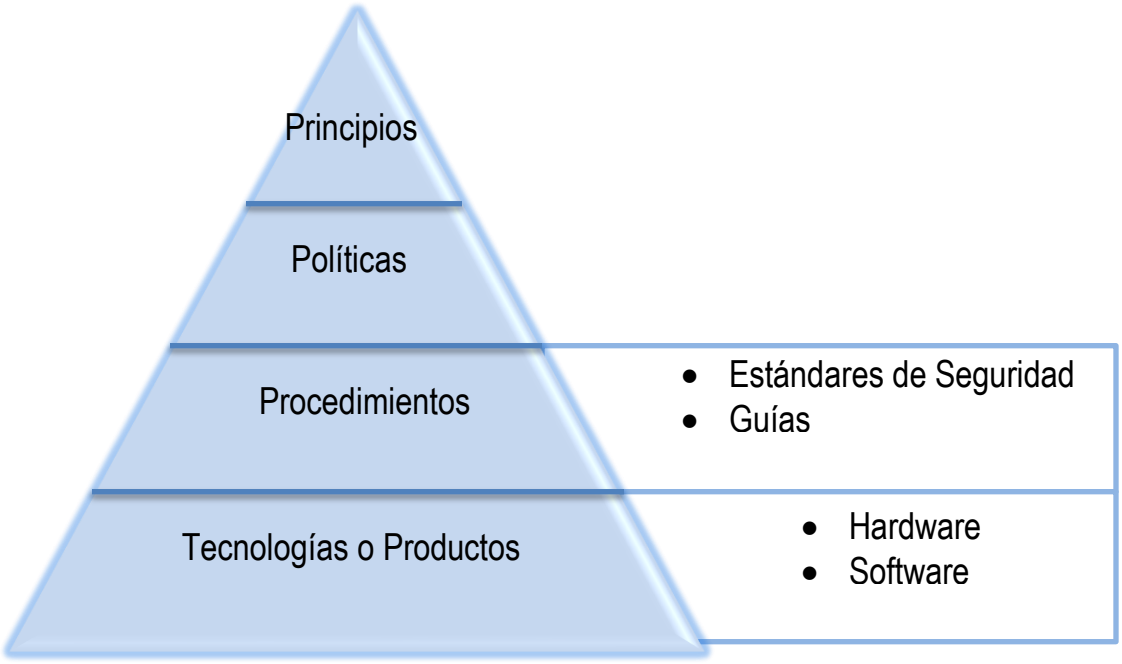
4. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El modelo de seguridad y privacidad de la información contempla un ciclo de operación que consta de cinco (5) fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información.

- **Diagnóstico:** En esta fase se pretende identificar el estado actual de la organización con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información.
- **Planificación:** Para el desarrollo de esta fase la entidad debe utilizar los resultados de la etapa anterior y proceder a elaborar el 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.
- **Implementación:** Esta fase le permitirá a la Entidad, llevar a cabo la implementación de la planificación realizada en la fase anterior del MSPI.
- **Evaluación de Desempeño:** El proceso de seguimiento y monitoreo del MSPI se hace con base a los resultados que arrojan los indicadores de la seguridad de la información propuestos para verificación de la efectividad, la eficiencia y la eficacia de las acciones implementadas.
- **Mejora Continua:** En esta fase la Entidad debe consolidar los resultados obtenidos de la fase de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, tomando las acciones oportunas para mitigar las debilidades identificadas.

DESCRIPCIÓN DEL MODELO DE SEGURIDAD DE LA INFORMACIÓN

En el ámbito de la Seguridad de la información, los componentes del sistema se ubican en diferentes niveles de acuerdo con su importancia, a continuación se ilustran dichos componentes:



4.1 FASE DE DIAGNÓSTICO

OBJETIVO

Identificar el estado de la Entidad con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información.

SISTEMA DE GESTIÓN DE SEGUIDAD Y PRIVACIDAD DE LA INFORMACIÓN				
PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN				
FASE DE DIAGNÓSTICO				
ÍTEM	ACTIVIDAD	RESPONSABLE	INSTRUMENTO	REALIZADO
1	Fortalecer el estado actual de la gestión de seguridad y privacidad de la información al interior de la interior de la Entidad.	Profesional asignado a la Oficina de Sistemas	Herramienta de Diagnóstico MSPI – MINTIC	100%
2	Mantener y Fortalecer el nivel de madurez de seguridad y privacidad de la información en la Entidad.	Profesional asignado a la Oficina de Sistemas	Herramienta de Diagnóstico MSPI – MINTIC	100%
3	Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación.	Profesional asignado a la Oficina de Sistemas	Herramienta de Diagnóstico MSPI – MINTIC	100%
4	Identificar el avance de la implementación del ciclo de operación al interior de la Entidad.	Profesional asignado a la Oficina de Sistemas	Herramienta de Diagnóstico MSPI – MINTIC	100%
5	Identificar el nivel de cumplimiento con la legislación vigente relacionada con protección de datos personales.	Profesional asignado a la Oficina de Sistemas	Herramienta de Diagnóstico MSPI – MINTIC & Política de protección de datos personales	100%
6	Identificar y fortalecer el uso de buenas prácticas en ciberseguridad.	Profesional asignado a la Oficina de Sistemas	Herramienta de Diagnóstico MSPI – MINTIC	100%

Para la recolección de la información, en esta fase se utilizarán mecanismo como:

• Documentación existente en el sistema de calidad de la entidad relacionada con la información de las partes interesadas de la entidad y los roles y funciones asociados a la seguridad de la información.

• Fuentes externas, como las guías de autoevaluación, encuesta y estratificación dispuestas por la estrategia de gobierno en línea Ministerio de Tecnologías de la Información y las Comunicaciones.

4.2 FASE DE PLANIFICACIÓN

OBJETIVO

Definir la estrategia metodológica, que permita establecer el alcance, objetivos, procesos y procedimientos, pertinentes a la gestión del riesgo y mejora de seguridad de la información, en procura de los resultados que permitan dar cumplimiento con las metas propuestas del SGSI.

SISTEMA DE GESTIÓN DE SEGUIDAD Y PRIVACIDAD DE LA INFORMACIÓN				
PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN				
FASE DE PLANIFICACIÓN				
ÍTEM	ACTIVIDAD	RESPONSABLE	INSTRUMENTO	REALIZADO
1	Fortalecer la Política de seguridad y privacidad de la información.	Profesional asignado a la Oficina de Sistemas	Documento con la política de seguridad de la información, aprobado por la alta Dirección y socializada al interior de la Entidad.	100%
2	Fortalecer los Procedimientos de seguridad de la información.	Profesional asignado a la Oficina de Sistemas	Procedimientos, debidamente documentados, socializados y aprobados.	100%
3	Fortalecimiento en la identificación del Inventario de activos de información.	Profesional asignado a la Oficina de Sistemas	Matriz con la identificación, valoración y clasificación de activos de información.	100%
4	Fortalecer la Integración del MSPI con el Sistema de Gestión documental.	Secretaría General.	PINAR	100%
5	Plan de Comunicaciones.	Profesional asignado al área de comunicaciones.	Documento con el plan de comunicación sensibilización y capacitación para la entidad.	100%
6	Plan de transición Pv4 a IPv6. Fase I. PLANEACION.	Profesional asignado a la Oficina de Sistemas	Documentación Fase I. PLANEACIÓN IPv4 a IPv6.	0%
7	Plan de transición Pv4 a IPv6. Fase. III PRUEBAS DE FUNCIONAMIENTO.	Profesional asignado a la Oficina de Sistemas	Documentación IPv4 a IPv6. Fase. III PRUEBAS DE FUNCIONAMIENTO.	0%

4.3 FASE DE IMPLEMENTACIÓN

OBJETIVO

Llevar a cabo la implementación de la fase de planificación del SGSI, teniendo en cuenta para esto los aspectos más relevantes en los procesos de implementación del Sistema de Gestión de Seguridad de la Información de la entidad.

SISTEMA DE GESTIÓN DE SEGUIDAD Y PRIVACIDAD DE LA INFORMACIÓN				
PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN				
FASE DE IMPLEMENTACIÓN				
ÍTEM	ACTIVIDAD	RESPONSABLE	INSTRUMENTO	REALIZADO
1	Formular el plan de tratamiento de riesgo de seguridad de información.	Profesional asignado a la Oficina de Sistemas	Documentar el plan de tratamiento de riesgo de seguridad de información.	100%
2	Implementar el plan de tratamiento de riesgo de seguridad de información.	Profesional asignado a la Oficina de Sistemas	Ejecución de la Fase de Planificación de la gestión de riesgo de la seguridad de información.	100%
3	Implementación de controles de seguridad de información.	Profesional asignado a la Oficina de Sistemas	Documento con el plan de tratamiento de riesgos.	100%
4	Elaborar o Diseñar herramienta que permita medir la eficacia de los controles de seguridad de la información.	Profesional asignado a la Oficina de Sistemas	Formato.Doc o Formato.xls	100%
5	Gestionar los recursos del MSPI	Profesional asignado a la Oficina de Sistemas	Recurso Humano Recurso Tecnológico. Recurso Audiovisual.	100%
6	Implementar procedimientos y otros controles para detectar y dar respuesta oportuna a los incidentes de seguridad de información	Profesional asignado a la Oficina de Sistemas	Procedimientos, Controles o Políticas.	100%
7	Plan de transición Pv4 a IPv6. Fase. II IMPLEMENTACION.	Profesional asignado a la Oficina de Sistemas	IPv4 a IPv6. Fase II. IMPLEMENTACIÓN Documento aprobado con las estrategias del plan de implementación de IPv6	0%

4.4 FASE DE EVALUACIÓN

OBJETIVO

Evaluar el desempeño y la eficacia del SGSI, a través de instrumentos que permita determinar la efectividad de la implantación del SGSI.

SISTEMA DE GESTIÓN DE SEGUIDAD Y PRIVACIDAD DE LA INFORMACIÓN				
PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN				
FASE DE EVALUACIÓN Y DESEMPEÑO				
ÍTEM	ACTIVIDAD	RESPONSABLE	INSTRUMENTO	REALIZADO
1	Seguimiento y revisión a la implementación del MSPI.	Profesional asignado a la Oficina de Sistemas – Oficina de Control Interno	Registros de Seguimiento y revisión.	100%
2	Realizar auditorías internas del MSPI a intervalos planificados.	Profesional asignado a la Oficina de Sistemas – Oficina de Control Interno	Registros de Seguimiento y revisión.	100%
3	Seguimiento y revisión a la Auditoria Interna de seguridad de información.	Profesional asignado a la Oficina de Sistemas – Oficina de Control Interno	Registros de Seguimiento y revisión.	100%
4	Seguimiento y revisión al cumplimiento de la política de seguridad de la información y Controles.	Profesional asignado a la Oficina de Sistemas – Oficina de Control Interno	Registros de Seguimiento y revisión.	100%

4.5 FASE DE MEJORA

OBJETIVO

Consolidar los resultados obtenidos del componente de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, que permita realizar el plan de implementación de las acciones correctivas identificadas para el SGSI

SISTEMA DE GESTIÓN DE SEGUIDAD Y PRIVACIDAD DE LA INFORMACIÓN				
PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN				
FASE DE MEJORA CONTINUA				
ÍTEM	ACTIVIDAD	RESPONSABLE	INSTRUMENTO	REALIZADO
1	Mejorar uso de la política de seguridad de la información.	Profesional asignado a la Oficina de Sistemas	Registros de Mejora y/o Actualización	80%
2	Mejorar los objetivos de seguridad de la información.	Profesional asignado a la Oficina de Sistemas	Registros de Mejora y/o Actualización	90%
3	Mejora los resultados de la auditoría interna de seguridad de información.	Profesional asignado a la Oficina de Sistemas	Registros de Mejora y/o Actualización	0%
4	Mejorar el Uso e Implementación de los controles de seguridad de información.	Profesional asignado a la Oficina de Sistemas	Registros de Mejora y/o Actualización	90%
5	Mejorar el resultado de los indicadores	Profesional asignado a la Oficina de Sistemas	Registros de Mejora y/o Actualización	80%

5. JUSTIFICACIÓN

Aguas del Cesar S.A. E.S.P., con el propósito de salvaguardar la información de la entidad en todos sus aspectos, garantizando la seguridad de los datos y el cumplimiento de las normas legales, ha establecido realizar un Plan de Seguridad y Privacidad de la información con el ánimo de que no se presenten pérdidas, robos, accesos no autorizados y duplicación de la misma, igualmente promueve una política de seguridad de la información física y digital de acuerdo a la caracterización de los usuarios tanto internos como externos.

La seguridad de la información se entiende como la preservación de las siguientes características:

- ✓ ***Confidencialidad:*** se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
- ✓ ***Integridad:*** se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
- ✓ ***Disponibilidad:*** Se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.