2026 - 2029

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

DIRECCIÓN ADMINISTATIVA Y FINANCIERA

OFICINA DE SISTEMAS

AguasdelCesar S.A. E.S.P.

Tabla de Contenido

1. INTRODUCCIÓN

El objetivo primordial del Plan de Tratamiento de Riesgos de Seguridad y Seguridad de la Información es garantizar que los riesgos de la seguridad de la información sean conocidos, gestionados y tratados por la Entidad de una forma documentada, sistemática, estructurada, repetible y eficiente, para lo cual, es esencial identificar y valorar los riesgos que pueden afectar la seguridad y privacidad de la información y por consiguiente establecer los mecanismos más convenientes para protegerla.

Lo anterior implica, que la Entidad requiere como conocer el estado actual de sus activos de información, clasificarlos, priorizarlos y determinar su valor en caso de pérdida de información, y conocer los posibles riesgos que puedan afectar la seguridad y privacidad de la información y de esta forma determinar las medidas orientadas a minimizar el impacto en caso de presentarse la materialización de una amenaza.

En la medida que se tenga una visión general de los riesgos que pueden afectar la seguridad y privacidad de la información, la Entidad puede establecer controles y medidas efectivas, viables y transversales con el propósito de salvaguardar la disponibilidad, integridad y confidencialidad de su información, para lo cual, es necesario definir los lineamientos que se deben seguir para el análisis y evaluación de los riesgos de Seguridad de la Información de la Entidad.

La Seguridad de la Información en las empresas tiene como objetivo la protección de los activos de información en cualquiera de sus estados ante una serie de amenazas o brechas que atenten contra sus principios fundamentales de confidencialidad, integridad y su disponibilidad, a través de la implementación de medidas de control de seguridad de la información, que permitan gestionar y reducir los riesgos e impactos a que está expuesta y se logre alcanzar el máximo retorno de las inversiones en las oportunidades de negocio.

Por este motivo, AGUAS DEL CESAR decide realizar un modelo de administración de los riesgos de seguridad de la información y las actividades de valoración de mismos riesgos en cumplimiento de la política de seguridad de la información aprobada por Gerencia, y como medio o herramienta para el logro de los objetivos de mantener la información de la Entidad confidencial, integra y disponible.

Lo anterior dando cumplimiento a la normativa establecida por el estado colombiano, CONPES 3854 de 2016, Modelo de Seguridad y Privacidad de MINTIC y lo establecido en el decreto 1008 de 14 de junio 2018, adoptando las buenas prácticas y los lineamientos de los estándares ISO 27001:2013, ISO 31000:2018 y la guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 4 emitida por el DAFP.

2. DEFINICIONES

- **AMENAZA:** Causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.
- **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:** Se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo.
- **ANÁLISIS DEL RIESGO:** Proceso sistemático para comprender la naturaleza del riesgo y determinar el nivel de riesgo.
- **CAUSAS:** Son los medios, las circunstancias y agentes generadores de riesgo. Los agentes generadores que se entienden como todos los sujetos u objetos que tienen la capacidad de originar un riesgo.
- **CIBERCRÍMEN (DELITO CIBERNÉTICO):** Conjunto de actividades ilegales asociadas con el uso de las tecnologías de la información y las comunicaciones, como fin o como medio.
- **CONSECUENCIA:** Resultado o impacto de un evento que afecta a los objetivos.
- **CONTROL:** Medida que modifica al riesgo. (NTC ISO 31000:2011), medios para gestionar el riesgo e incluye políticas, procedimientos, directrices, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal.
- **CRITERIOS DEL RIESGO:** Términos de referencia frente a los cuales se evalúa la importancia de un riesgo.
- **DESCRIPCIÓN:** Se refiere a las características generales o las formas en que se observa o manifiesta el riesgo identificado.
- **ENTORNO DIGITAL ABIERTO:** En el que no se restringe el flujo de tecnologías, de comunicaciones o de información, y en el que se asegura la provisión de los servicios esenciales para los ciudadanos y para operar la infraestructura crítica.
- **ESTABLECIMIENTO DEL CONTEXTO:** Definición de los parámetros internos y externos que se han de tomar en consideración cuando se gestiona el riesgo y establecimiento del alcance y los criterios del riesgo para la política para la gestión del riesgo.

- **EVALUACIÓN DEL CONTROL:** Revisión sistemática de los procesos para garantizar que los controles son adecuados y eficaces.
- **EVALUACIÓN DEL RIESGO:** Proceso de comparación de los resultados del análisis del riesgo, con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.
- **EVENTO:** Presencia o cambio de un conjunto particular de circunstancias.
- **EVENTO DE SEGURIDAD DE LA INFORMACIÓN:** Ocurrencia que indica una posible brecha de seguridad de la información o falla de los controles.
- **FUENTE DE RIESGO:** Elemento que solo o en combinación tiene el potencial intrínseco de originar un riesgo.
- **FRECUENCIA:** Medición del número de ocurrencias por unidad de tiempo.
- **GESTIÓN DEL RIESGO:** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.
- **GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL:** Es el conjunto de actividades coordinadas dentro de una organización o entre organizaciones para abordar el riesgo de seguridad digital, mientras se maximizan oportunidades. Es una parte integral de la toma de decisiones y de un marco de trabajo integral para gestionar el riesgo de las actividades económicas y sociales. Se basa en un conjunto flexible y sistemático de procesos cíclicos lo más transparente y lo más explícito posible. Este conjunto de procesos ayuda a asegurar que las medidas de gestión de riesgos de seguridad digital (medidas de seguridad) sean apropiadas para el riesgo y los objetivos económicos y sociales en juego.
- **IMPACTO:** Son las consecuencias que genera un riesgo una vez se materialice.
- **INCIDENTE DIGITAL:** Evento intencionado o no intencionado que puede cambiar el curso esperado de una actividad en el medio digital y que genera impactos sobre los objetivos.
- **INVENTARIO DE ACTIVOS:** Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten, por tanto, ser protegidos de potenciales riesgos.
- **PELIGRO:** Una fuente de daño potencial.
- **PÉRDIDA:** Cualquier consecuencia negativa o efecto adverso, financiero u otro.
- **POLÍTICA PARA LA GESTIÓN DEL RIESGO:** Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo.
- **POSIBILIDAD:** Se utiliza como descripción general de la probabilidad o la frecuencia.

- **PLAN PARA LA GESTIÓN DEL RIESGO:** Esquema dentro del marco de referencia para la gestión del riesgo que especifica el enfoque, los componentes y los recursos de la gestión que se van a aplicar a la gestión del riesgo.
- **PROBABILIDAD:** Oportunidad de que algo suceda.
- **PROCESO PARA LA GESTIÓN DEL RIESGO:** Aplicación sistemática de las políticas, los procedimientos y las prácticas de gestión a las actividades de comunicación, consulta, establecimiento del contexto, y de identificación, análisis, evaluación, tratamiento, monitoreo y revisión del riesgo.
- **REDUCCIÓN DEL RIESGO:** Acciones que se toman para disminuir la posibilidad, las consecuencias negativas o ambas, asociadas con un riesgo.
- **REVISIÓN:** Acción que se emprende para determinar la idoneidad, conveniencia y eficacia de la materia en cuestión para lograr los objetivos establecidos.
- **RIESGO:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.
- **SGC:** Sistema de gestión de calidad.
- **SGSI:** Sistema de gestión de seguridad de la información.
- **TELECOMUNICACIONES:** Toda transmisión y recepción de signos, señales, escritos, imágenes y sonidos, datos o información de cualquier naturaleza por hilo, radiofrecuencia, medios ópticos u otros sistemas electromagnéticos.
- **TI:** Tecnologías de la información.
- **TIC (TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES):** Conjunto de recursos, herramientas, equipos, programas informáticos aplicaciones, redes y medios que permiten la compilación, procesamiento, almacenamiento, transmisión de información como voz, datos, texto, video e imágenes.
- **TRATAMIENTO DEL RIESGO:** Proceso para modificar el riesgo.
- **VULNERABILIDAD:** Es una debilidad, atributo o falta de control que permitiría o facilitaría la actuación de una amenaza contra información clasificada, los servicios y recursos que la soportan.

3. OBJETIVO GENERAL

Implementar los lineamientos y las acciones necesarias que permitan llevar a cabo el perfecto desarrollo del Plan de Tratamiento para los riesgos de seguridad y privacidad de la información y de esta forma mitigar los riesgos identificados, protegiendo y preservando la integridad, confidencialidad, disponibilidad y autenticidad de la información de la Entidad.

3.1 OBJETIVOS ESPECÍFICOS

- ✓ Identificar los activos de información de la entidad.
- ✓ Identificar los riesgos asociados a los procesos.
- ✓ Calcular los niveles de riesgos.
- ✓ Proteger los activos de información, implementando las acciones necesarias para mitigar los riesgos identificados.
- ✓ Realizar seguimiento y control a la eficacia del plan de tratamiento de riesgos.

4. ALCANCE

Con la ejecución de este plan se busca identificar los activos de información que hacen parte de cada uno de los procesos de la entidad para luego implementar, realizar seguimiento y evaluación de los controles que permitan ejecutar buenas prácticas que contribuyan a una excelente toma de decisiones y mitigar o prevenir incidentes que afecten el cumplimiento de los objetivos.

El Plan de Tratamiento de Riesgo tendrá en cuenta los riesgos que se encuentren en los niveles Alto y Extremo acorde con los lineamientos definidos por el Ministerio TIC, los riesgos que se encuentren en niveles inferiores serán aceptados por la Entidad.

5. GENERALIDADES – CONOCIMIENTO DE LA ENTIDAD

5.1 MISIÓN

Liderar articuladamente las políticas de Agua Potable, Saneamiento Básico y Desarrollo Sostenible con efectividad para la gestión y operatividad de la prestación satisfactoria de los servicios públicos del Sector en el Departamento del Cesar.

5.2 VISIÓN

En el 2022 AGUAS DEL CESAR S.A. E.S.P., seguirá liderando la gestión de estrategias y acciones encaminadas a garantizar la prestación eficiente y eficaz de los servicios públicos del sector Agua Potable y Saneamiento Básico para el Desarrollo Económico, Social y Ambiental Sostenible de las comunidades del Departamento del Cesar.

6. MARCO NORMATIVO

A continuación, se enuncia el marco normativo que rige toda la documentación que soporta el Plan de Tratamiento de Riesgo de Seguridad de la Información de Aguas del Cesar S.A. E.S.P.

- **Decreto 1078 de 2015:** Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- **NTC / ISO 27001:** La norma ISO 27001 es un estándar internacional que describe cómo implementar el Sistema de gestión de seguridad de la información de una empresa. Investiga como salvaguardar la información mediante una serie de estándares, lineamientos y procesos que facilitan la identificación de los riesgos.
- **NTC / ISO 27005:** La norma ISO 27005 es un soporte a la norma (ISO 27001) la cual proporciona directrices para la gestión de riesgos de seguridad de la información, es aplicable a todos los tipos de organización y no proporciona ni recomienda una metodología específica.
- **NTC/ISO 31000:2009:** Gestión del Riesgo. Principios y directrices.
- **Ley 87 de 1993:** Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones.

- **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.
- **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).
- **Ley 1273 de 2009:** Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- **Ley 1341 de 2009:** Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.
- **Ley 1581 de 2012:** Por la cual se dictan disposiciones generales para la protección de datos personales.
- **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.
- **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.
- **Decreto 4485 de 2009:** Por medio de la cual se adopta la actualización de la Norma Técnica de Calidad en la Gestión Pública.
- **Decreto 235 de 2010:** Por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones públicas.
- **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.
- **Decreto 1377 de 2013:** Por el cual se reglamenta parcialmente la Ley 1581 de 2012" o Ley de Datos Personales.

- **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.
- **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 620 de 2020:** Estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales"
- **Resolución 2710 de 2017:** Por la cual se establecen los lineamientos para la adopción del protocolo IPv6.
- **Resolución 3564 de 2015:** Por la cual se reglamentan aspectos relacionados con la Ley de Transparencia y Acceso a la Información Pública.
- **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.

7. DESARROLLO METODOLÓGICO

El identificar los riesgos y los activos de información nos permite comprender a qué están expuestos los activos de información de nuestra Empresa. Se recomienda contar con técnicas tradicionales para identificar los riesgos específicos asociados a los activos y complementar este proceso en la medida de lo posible con la identificación de puntos críticos de fallas, análisis de disponibilidad, análisis de vulnerabilidad, análisis de confiabilidad y árboles de falla. El plan propuesto en este documento comprende, como se detallará más adelante, las siguientes actividades principales: establecimiento del contexto, identificación riesgos, estimación de riesgos, evaluación de riesgos, tratamiento de riesgo y aceptación del riesgo.

A continuación, se presenta las actividades generales para la implementación del Plan:

Gráfico 1. *Estructura general de la metodología de riesgos.*

7.1 FASE 1. ANÁLISIS DE LA INFORMACIÓN

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

Durante la fase se establecen las actividades para implementar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, las cuales son:

- Aplicar las políticas de administración de riesgos.
- Identificar los riesgos.
- Determinar los controles y valoraciones de los riesgos.

Para el caso de la gestión de riesgo de seguridad digital y seguridad de información se debería utilizar una técnica de recolección de datos primarios que puede ser un cuestionario de preguntas o encuesta, esta herramienta de recolección de datos va dirigida al responsable del riesgo es decir al dueño del proceso, con el fin de identificar de cada proceso y activo de seguridad digital y seguridad de información posibles controles existentes, vulnerabilidades, amenazas, riesgo etc.

La gestión del riesgo dentro de la seguridad de la información se puede también enmarcar dentro del ciclo de planear, hacer, verificar y actuar (PHVA) tal como se muestra en la siguiente ilustración (ISO 27001:2013):

Gráfico 2. *Ciclo PHVA y Gestión de riesgos.*

7.1.1 CONTEXTO EXTERNO E INTERNO DE LA ENTIDAD

Se realizó un análisis del contexto externo e interno de la entidad con el fin de identificar los riesgos de seguridad de la información que se puedan presentar al interior de la empresa.

El objetivo de la identificación de riesgos es conocer lo incidentes o eventos que pueden causar pérdidas o alteración en el funcionamiento de la Empresa Aguas del Cesar, y puedan afectar la confidencialidad, integridad y disponibilidad de la información.

Para la evaluación de riesgos de seguridad de la información en primer lugar se deberán identificar los activos de información por proceso en evaluación.

Los **activos de información** se clasifican en dos tipos:

a) Primarios:

- **Procesos o subprocesos y actividades de la Entidad:** procesos cuya pérdida o degradación hacen imposible llevar a cabo la misión de la organización;

procesos que contienen procesos secretos o que implican tecnología propietaria; procesos que, si se modifican, pueden afectar de manera muy significativa el cumplimiento de la misión de la organización; procesos que son necesarios para el cumplimiento de los requisitos contractuales, legales o reglamentarios.

- **Información:** información vital para la ejecución de la misión o el negocio de la organización; información personal que se puede definir específicamente en el sentido de las leyes relacionadas con la privacidad; información estratégica que se requiere para alcanzar los objetivos determinados por las orientaciones estratégicas; información del alto costo cuya recolección, almacenamiento, procesamiento y transmisión exigen un largo periodo de tiempo y/o implican un alto costo de adquisición, etc.

- **Actividades y procesos:** que tienen que ver con propiedad intelectual, los que si se degradan hacen imposible la ejecución de las tareas de la empresa, los necesarios para el cumplimiento legal o contractual, etc.

b) De Soporte

- **Hardware:** Consta de todos los elementos físicos que dan soporte a los procesos (PC, portátiles, servidores, impresoras, discos externos, etc.).
- **Software:** Consiste en todos los programas que contribuyen al funcionamiento de un conjunto de procesamiento de datos (sistemas operativos, paquetes de software o estándar, aplicaciones, mantenimiento o administración, etc.)
- **Redes:** Consiste en todos los dispositivos de telecomunicaciones utilizados para interconectar varios computadores remotos físicamente o los elementos de un sistema de información (conmutadores, cableado, puntos de acceso, etc.)
- **Personal:** Consiste en todos los grupos de personas involucradas en el sistema de información (usuarios, desarrolladores, responsables, etc.)
- **Sitio:** Comprende todos los lugares en los cuales se pueden aplicar los medios de seguridad de la organización (Edificios, salas, y sus servicios, etc.)
- **Estructura organizativa:** responsables, áreas, contratistas, etc.

Después de tener una relación con todos los activos se han de conocer las amenazas que pueden causar daños en la información, los procesos y los soportes. La identificación de las amenazas y la valoración de los daños que pueden producir se puede obtener preguntando a los propietarios de los activos, usuarios, expertos, etc.

Para establecer el contexto externo, se debe tener en cuenta los siguientes factores relacionados con la Gestión de Riesgo de seguridad de Información.

	FACTORES EXTERNOS	TIPO DE RIESGO
1	- Embargo a La Entidad	Riesgo Financiero
2	- Catástrofe Natural - Falla de Energía	Riesgo Financiero Riesgo Operativo
3	- Cambio de Gobierno	Riesgo Estratégico
4	- Vandalismo - Situaciones que afecten el orden público	Riesgo Operativo
5	- Interrupciones en los operadores de servicios tecnológicos	Riesgo Tecnológico

El contexto interno, puede generar unos factores de riesgo de seguridad de la información que afectan de forma directa a la entidad tales como:

	FACTORES INTERNOS	TIPO DE RIESGO
1	- Disponibilidad de Activos - Capacidad Operativa de los Activos	Riesgo Operativo
2	- Infraestructura de la Entidad - Seguridad en el Trabajo - Salud Ocupacional - Competencias Laborales	Riesgo Operativo
3	- Funciones y Responsabilidades - Errores en los Procesos	Riesgo Operativo
4	- Disponibilidad de Datos - Sistemas de Información y/o Servicios - Mantenimiento de los Sistemas de Información - Seguridad de la Información	Riesgo Tecnológico

	- Sistema de Gestión - Manipulación de Hardware - Manipulación de Software indebido	
5	- Falta de Presupuesto - Falta de Inversión - Falta de Infraestructura	Riesgo Operativo

7.1.2 DEFINICIÓN DE ROLES Y RESPONSABILIDADES

Según la "Guía para la administración del - Riesgos de gestión, corrupción y seguridad digital - V4 Octubre de 2018", existen tres (3) líneas de defensas para monitorear y revisar la gestión del riesgo de la entidad.

Para los riesgos de la entidad, le corresponde a la primera línea de defensa desarrollar e implementar procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora.

7.1.2.1 PRIMERA LÍNEA – ROLES Y RESPONSABILIDADES

Responsable: Líderes de los procesos, programas y proyectos de la entidad.

Rol principal: Ejecutar, diseñar, implementar y monitorear los controles, además de gestionar de manera directa en el día a día los riesgos de la entidad, encargados de realizar la identificación de riesgos de seguridad de digital, sobre los procesos que tiene a su cargo, con el acompañamiento del Profesional Especializado del Grupo de Recursos Físicos y Tecnológicos.

Así mismo, orientar el desarrollo e implementación de políticas y procedimientos internos y asegurar que sean compatibles con las metas y objetivos de la entidad y emprender las acciones de mejoramiento para su logro.

7.1.2.2 SEGUNDA LÍNEA – ROLES Y RESPONSABILIDADES

Responsable: Servidores públicos que tienen responsabilidades directas en el monitoreo y evaluación de los controles y la gestión del riesgo: jefes de planeación,

supervisores e interventores de contratos o proyectos, coordinadores de otros sistemas de gestión de la entidad, comités de riesgos (donde existan), comités de contratación, entre otros.

Rol principal: monitorear la gestión de riesgo y control ejecutada por la primera línea de defensa, complementando su trabajo.

7.1.2.3 TERCERA LÍNEA – ROLES Y RESPONSABILIDADES

Responsable: La oficina de control interno, auditoría interna o quien haga sus veces.

Rol principal: Proporcionar un aseguramiento basado en el más alto nivel de independencia y objetividad.

7.1.3 DEFINICIÓN DE LOS RECURSOS PARA LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Los líderes de proceso, los cuales son los propietarios de los riesgos, y los responsables de implementar los controles de seguridad de información, deben informar sobre los recursos necesarios que necesitan para el desarrollo de la gestión de riesgos de seguridad de información, (capital, tiempo, personal, procesos, sistemas y tecnologías), teniendo en cuenta que la entidad debe tener un responsable de la coordinación, seguimiento, reporte de los avances, logros e inconvenientes relacionados con la gestión de los riesgos de seguridad digital y seguridad de la información.

La guía de Gestión de Riesgo de seguridad digital recomienda que la alta dirección debe asignar entre otros, recursos tales como:

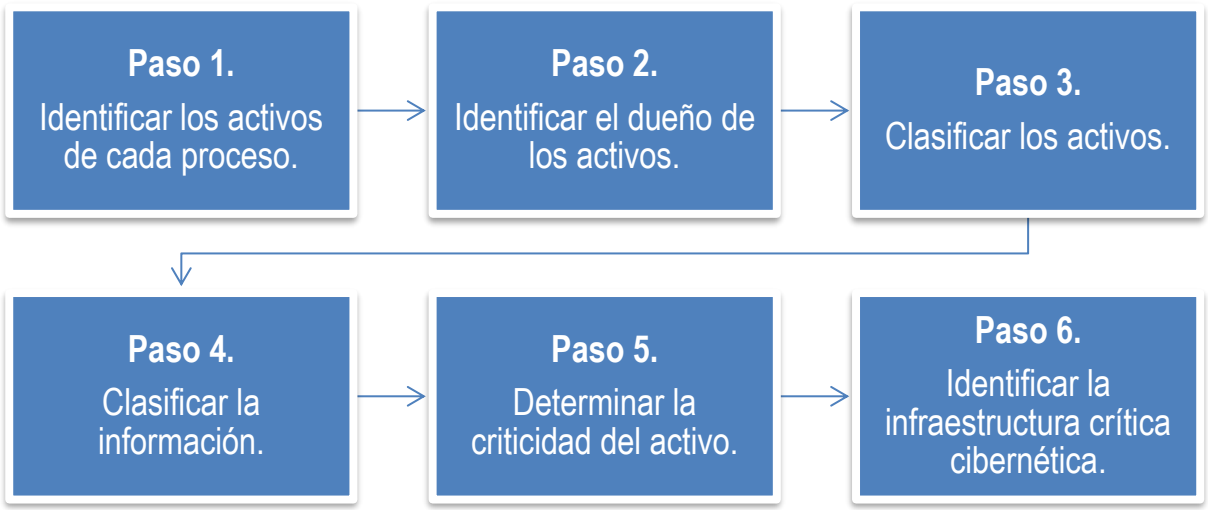
- Personal capacitado e idóneo para la gestión del riesgo de seguridad digital.
- Recursos económicos para la implementación de controles de mitigación de riesgos (Con base al análisis de riesgo realizado).
- Recursos para los aspectos de mejora continua, monitoreo y auditorías.

7.1.4 IDENTIFICACIÓN DE LOS ACTIVOS DE SEGURIDAD DIGITAL Y SEGURIDAD DE LA INFORMACIÓN

Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos los elementos que utiliza la organización para funcionar en el entorno digital tales como: aplicaciones de la organización, servicios Web, redes, información física o digital, tecnologías de información -TI, tecnologías de operación –TO.

La identificación de los activos de seguridad de información que se encuentren en un nivel de clasificación ALTA será tomada del Plan Institucional de Archivo publicado en la página web de la entidad, con el fin de elaborar el mapa o matriz de riesgo de seguridad de información.

7.1.5 COMO IDENTIFICAR LOS ACTIVOS DE SEGURIDAD DIGITAL Y SEGURIDAD DE LA INFORMACIÓN



Paso 1. Identificar los activos de cada proceso

Los activos de seguridad de la información están identificados dentro del inventario de activos de información de la Entidad.

Paso 2. Identificar el dueño de los activos

Los de los activos de información se encuentran identificados dentro del inventario de activos de información y en las tablas de retención documental de la entidad.

Paso 3. Clasificar los activos

Clasificación de Activos	
Tipo de Activo	**Descripción**
Información	Información almacenada en formatos físicos (papel, carpetas, CD, DVD) o en formatos digitales o electrónicos (bases de datos, correos electrónicos, archivos o servidores), teniendo en cuenta lo anterior, se puede distinguir como información: Contratos, manuales, procedimientos operativos o de soporte, planes, registros contables, estados financieros, archivos ofimáticos, documentos y registros del sistema integrado de gestión, bases de datos con información personal o con información relevante para algún proceso (bases de datos de nóminas, estados financieros) entre otros.
Software	Activo informático lógico como programas, herramientas ofimáticas o de sistemas.
Hardware	Equipos físicos de cómputo y de comunicaciones como servidores, computadores de escritorio y portátiles, discos duros externos que por su criticidad son considerados activos de información.
Servicios	Servicio brindado por la entidad para el apoyo de las actividades de los procesos, tales como: Servicios WEB, intranet, Aplicaciones entre otros (Pueden estar compuestos por hardware y software)
Intangibles	Se consideran intangibles aquellos activos inmateriales que otorgan a la entidad una ventaja competitiva relevante, uno de ellos es la imagen corporativa, reputación entre otros.

Componentes de Red	Medios necesarios para realizar la conexión de los elementos de hardware y software en una red, por ejemplo, el cableado estructurado y tarjetas de red, routers, switches, entre otros.
Personas	Aquellos roles que, por su conocimiento, experiencia y criticidad para el proceso, son considerados activos de información, por ejemplo: personal con experiencia y capacitado para realizar una tarea específica en la ejecución de las actividades.
Instalaciones	Espacio o área asignada para alojar y salvaguardar los datos considerados como activos críticos para la empresa.

Paso 4. Clasificar la información.

La clasificación de la información de la entidad se realizó conforme lo establece la Ley 712 de 2014 y Ley 1581 de 2012.

Ley 712 de 2014

Información pública: Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal.

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 esta ley.

Información pública reservada: Es aquella información" que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada 1, 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 esta ley.

Ley 1581 de 2012

La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.

Los activos de seguridad de información se deben identificar en cada proceso, y está en responsabilidad de cada líder de proceso.

Paso 5. Determinar la criticidad del activo.

Niveles de Clasificación de Activos	
Nivel	**Descripción**
ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

Paso 6. Identificar la infraestructura crítica cibernética.

Aguas del Cesar S.A. E.S.P., considera que no cuenta con una infraestructura crítica cibernética, debido que sus activos de información no generan ningún tipo de afectación o impacto negativo. Los tres parámetros para tener en cuenta son:

1. **Impacto social:** El momento de materializarse un riesgo de unos de los activos de información de la entidad generaría un impacto social que afectaría aproximadamente al 0.5% de la Población Nacional.

2. **Impacto económico:** En el momento de materializarse un riesgo de unos de los activos de información de la entidad generaría un impacto económico que afectaría a la entidad en el PIB de un Día o en el 0.123% del PIB Anual.

3. **Impacto Ambiental:** El momento de materializarse un riesgo de unos de los activos de información de la entidad generaría un impacto ambiental que afectaría el ecosistema y duraría 3 años en su recuperación.

7.1.6 IDENTIFICAR LOS RIESGOS DE SEGURIDAD DIGITAL Y SEGURIDAD DE LA INFORMACIÓN

Para la identificación de los riesgos de seguridad digital y seguridad de la información, se podrán identificar los siguientes tres (3) riesgos inherentes:

- Pérdida de la confidencialidad
- Pérdida de la integridad
- Pérdida de la disponibilidad

Para cada riesgo, se deben asociar el grupo de activos o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización.

7.1.7 TIPOS DE RIESGOS

Clasificación de Riesgos	
Tipo de Riesgo	**Descripción**
Estratégico	Posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos de la organización pública.
Tecnológico	Posibilidad de ocurrencia de eventos que afecten la totalidad o parte de la infraestructura tecnológica (hardware, software, redes, etc.) de una entidad.

Gerencial	Posibilidad de ocurrencia de eventos que afecten los procesos gerenciales y/o la alta dirección.
Corrupción	Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
Operativo	Posibilidad de ocurrencia de eventos que afecten los procesos misionales de la entidad.
Imagen o Reputación	Posibilidad de ocurrencia de un evento que afecte la imagen, buen nombre o reputación de una organización ante sus clientes o usuarios y partes interesadas.
Seguridad Digital	Posibilidad de combinación de amenazas y vulnerabilidades en el entorno digital.
Seguridad Física	Posibilidad de ocurrencia de un evento que afecte la seguridad física. Se conoce como seguridad física al conjunto de elementos que conforman un plan de seguridad, para proteger un espacio determinado con el fin de evitar daños y minimizar amenazas.
Financiero	Posibilidad de ocurrencia de eventos que afecten los estados financieros y todas aquellas áreas involucradas con el proceso financiero como presupuesto, tesorería, contabilidad, cartera, central de cuentas, costos, etc.
Ambiental	Posibilidad de que se produzca un daño o catástrofe en el medio ambiente debido a un fenómeno natural o a una acción humana, que pueda afectar a la Entidad.
Cumplimiento	Posibilidad de ocurrencia de eventos que afecten la situación jurídica o contractual de la organización debido a su incumplimiento o desacato a la normatividad legal y las obligaciones contractuales.

7.1.8 VALORACIÓN DE RIESGOS

7.1.8.1 ANÁLISIS DE RIESGOS

En materia de seguridad digital se identifican los siguientes tres (3) riesgos inherentes: Pérdida de la confidencialidad, Pérdida de la integridad y Pérdida de la disponibilidad.

7.1.8.2 ANÁLISIS DE LAS CAUSAS

Los objetivos estratégicos y de proceso se desarrollan a través de actividades, pero no todas tienen la misma importancia, por tanto, se debe establecer cuáles de ellas contribuyen mayormente al logro de los objetivos y estas son las actividades críticas o factores claves de éxito; estos factores se deben tener en cuenta al identificar las causas. Para los riesgos de seguridad digital, no es necesario realizar DOFA a nivel de activos, se toma la realizada para el proceso.

7.1.9 CÁLCULO DE LA PROBABILIDAD

Se analiza qué tan posible es que ocurra el riesgo, se expresa en términos de frecuencia, es decir número de eventos en un periodo determinado, se trata de hechos que se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo.

Probabilidad de Ocurrencia			
Nivel	***Probabilidad***	***Descripción***	***Frecuencia***
5	Casi Seguro	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de (1) una vez al año.
4	Probable	Se espera que el evento ocurra en la mayoría de las circunstancias	Al menos (1) una vez en el último año.
3	Posible	El evento probablemente ocurrirá en la mayoría de las circunstancias.	Al menos (1) una vez en los últimos 2 años.
2	Improbable	El evento puede ocurrir en algún momento.	Al menos (1) una vez en los últimos 5 años.
1	Raro	El evento puede ocurrir sólo en circunstancias excepcionales.	No se ha presentado en los últimos 5 años.

7.1.10 ANÁLISIS DE IMPACTO

Criterios de Impacto para Riesgos de Seguridad Digital			
Nivel de Impacto	***Valor del Impacto***	***Impacto Cuantitativo***	***Impacto Cualitativo***
Insignificante	1	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. No hay afectación medioambiental.	Sin afectación de la integridad. Sin afectación de la disponibilidad. Sin afectación de la confidencialidad.
Menor	2	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. Afectación leve del medio ambiente requiere de ≥X días de recuperación.	Afectación leve de la integridad. Afectación leve de la disponibilidad. Afectación leve de la confidencialidad.
Moderado	3	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. Afectación leve del medio ambiente requiere de ≥X semanas de recuperación.	Afectación moderada de la integridad de la información debido al interés particular de los empleados y terceros. Afectación moderada de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación moderada de la confidencialidad de la información debido al interés particular de los empleados y terceros.

Mayor	4	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. Afectación importante del medio ambiente que requiere de ≥X meses de recuperación.	Afectación grave de la integridad de la información debido al interés particular de los empleados y terceros. Afectación grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.
Catastrófico	5	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. Afectación muy grave del medio ambiente que requiere de ≥X años de recuperación.	Afectación muy grave de la integridad de la información debido al interés particular de los empleados y terceros. Afectación muy grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación muy grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.

Matriz de Probabilidad de Ocurrencia							
Probabilidad de Ocurrencia		*Casi Seguro*	B	B	M	A	A
		Probable	B	B	M	A	E
		Posible	B	M	A	E	E
		Improbable	M	A	A	E	E
		Rara Vez	A	A	E	E	E
			Insignificante	*Menor*	*Moderado*	*Mayor*	*Catastrófico*
		Impacto					

Zonas de Riesgo		
B	Zona de Riesgo Baja	Asumir el Riesgo
M	Zona de Riesgo Moderada	Asumir el Riesgo y Reducir el Riesgo
A	Zona de Riesgo Alta	Reducir el Riesgo, Evitar, Compartir o Transferir
E	Zona de Riesgo Extrema	Reducir el Riesgo, Evitar, Compartir o Transferir

El impacto se debe analizar y calificar a partir de las consecuencias identificadas en la fase de descripción del riesgo. En la matriz de priorización de probabilidad de ocurrencia como ejemplo el impacto fue identificado como mayor por cuanto puede generar interrupción de las operaciones por más de dos días. En el mapa de color se toma la calificación de probabilidad resultante de la tabla "Matriz de priorización de probabilidad", para este ejemplo se tomará la probabilidad de ocurrencia en "probable" y la calificación de impacto en "mayor", nos ubicamos en la calificación de probabilidad en la fila y la de impacto en las columnas correspondientes, se establece el punto de intersección de las dos y este punto corresponderá al nivel de riesgo, que para el ejemplo es nivel extremo – color rojo (R1), así se podrá determinar el riesgo inherente.

7.1.11 VALORACIÓN DE CONTROLES EXISTENTES

La identificación de los controles existentes permite realizar la evaluación de riesgos. Lo controles garantizan que al momento de la materialización de un riesgo se reduzcan o mitiguen los riesgos informáticos y la organización funcionen correctamente. Pero se debe tener en cuenta que nunca se va a estar 100% seguros.
Una vez identifique, establezca y valore los riesgos inherentes deberá identificar y evaluar los controles existentes, teniendo en cuenta que en algunos casos los controles establecidos podrán estar documentados pero no implementados o en su defecto mal implementados.

7.1.12 DISEÑO DE CONTROLES

Para una buena valoración de los controles primero se debe tener en cuenta los seis (6) pasos que se deben realizar para el diseño de un buen control, teniendo en cuenta que en materia de seguridad digital la mayoría de los controles se encuentran establecidos.

Paso 1: Debe tener definido el responsable de llevar a cabo la actividad de control.
Paso 2: Debe tener una periodicidad definida para su ejecución.
Paso 3: Debe indicar cuál es el propósito del control.
Paso 4: Debe establecer el cómo se realiza la actividad de control.
Paso 5: Debe indicar qué pasa con las observaciones o desviaciones resultantes de ejecutar el control.
Paso 6: Debe dejar evidencia de la ejecución del control.

En la valoración de los controles para la mitigación de los riesgos se debe asegurar que el control este bien diseñado y que permita mitigar el riesgo, recordemos que no solamente es necesario tener un buen control sino que el control se ejecute oportunamente, porque un control que se ejecute que este mal diseñado no mitiga ningún riesgo.

7.1.13 NIVELES DE RIESGOS

Se ha evidenciado que ningún riesgo con una medida de tratamiento se puede evitar o eliminar, la entidad debe buscar el desplazamiento de los riesgos inherente que se

encuentren en zona de riesgo Alta o Extrema a una zona de riesgo Moderada o Baja de tal forma que la probabilidad o de ocurrencia o impacto disminuya.

7.1.14 TRATAMIENTO DE LOS RIESGOS

Como resultado de la etapa de evaluación del riesgo tendremos una lista ordenada de riesgos o una matriz con la identificación de los niveles de riesgo de acuerdo con la zona de ubicación, por tanto, se deberá elegir la(s) estrategia(s) de tratamiento del riesgo en virtud de su valoración y de los criterios establecidos en el contexto de gestión de riesgos mencionados anteriormente.

De acuerdo con el nivel evaluación de los riesgos, se deberá seleccionar la opción de tratamiento adecuada por cada uno de los riesgos identificados; el costo/beneficio del tratamiento deberá ser un factor de decisión relevante para la decisión.

Tratamiento de los Riesgos	
Tratamiento	*Ejemplo*
Evitar el Riesgo: Su propósito es no proceder con la actividad o la acción que da origen al riesgo.	• Tomar otra alternativa. • Eliminar una actividad, un procedimiento o un proceso que puede ser la causa del incidente
Transferir o Compartir el Riesgo: Entregar la gestión del riesgo a un tercero.	• Contratar servicios en la Nube para salvaguardar la información. • Contratar o Subcontratar el servicio.
Reducir o Mitigar el Riesgo: Seleccionando e implementando los controles o medidas adecuadas que logren que se reduzca la probabilidad o el impacto.	• Establecer controles que permitan reducir el riesgo.
Asumir el Riesgo: No se tomará la decisión de implementar medidas de control adicionales. Monitorizarlo para confirmar que no se incrementa.	• Elaboración de controles de tipo preventivo y/o correctivo.

7.2 FASE 2. EJECUCIÓN

En la fase de ejecución se debe implementar y ejecutar cada una de las actividades contempladas en la fase 1. La entidad a través de la línea Estratégica debe disponer los recursos que permitan la implementación y ejecución de la Gestión de Riesgo de Seguridad Digital y Seguridad de la Información.

La primera línea de defensa en articulación con la Oficina de Sistemas debe supervisar y acompañar la ejecución de las tareas en los tiempos establecidos.

7.3 FASE 3. MONITOREO Y REVISIÓN

La Entidad debe hacer un seguimiento a los planes de tratamiento para determinar su efectividad, de acuerdo con lo definido a continuación:

- Realizar seguimiento y monitoreo al plan de acción en la etapa de implementación y Finalización de los planes de acción.
- Revisar periódicamente las actividades de control para determinar su relevancia y actualizarlas de ser necesario.
- Realizar monitoreo de los riesgos y controles tecnológicos.
- Efectuar la evaluación del plan de acción y realizar nuevamente la valoración de los riesgos de seguridad digital para verificar su efectividad.
- Verificar que los controles están diseñados e implementados de manera efectiva y operen como se pretende para controlar los riesgos.
- Suministrar recomendaciones para mejorar la eficiencia y eficacia de los controles.

Es muy importante que la entidad monitoree y revise la gestión del riesgo con el fin de lograr los objetivos estratégicos y misionales que permitan alcanzar las metas establecidas en cada vigencia, para eso es necesario establecer los roles y responsabilidades de todos los actores del riesgo y control de la entidad.

7.3.1 REGISTRO DE INCIDENTES DE SEGURIDAD DIGITAL

Es importante que la entidad cuente con el registro de los incidentes de seguridad digital que se hayan materializado, con el fin de analizar las causas, las deficiencias de los controles implementados y las pérdidas que se pueden generar. El propósito fundamental del registro de incidentes es garantizar que se tomen las acciones adecuadas para evitar o disminuir su ocurrencia, retroalimentar y fortalecer la identificación y gestión de dichos riesgos y enriquecer las estadísticas sobre amenazas y vulnerabilidades y, con esta información, adoptar nuevos controles.

7.4 FASE 4. MEJORA CONTINUA DE LA GESTIÓN DE RIESGO DE LA SEGURIDAD DIGITAL

La Entidad debe realizar acciones que permitan garantizar el mejoramiento continuo de la gestión de riesgos de seguridad digital, en ese sentido deben existir políticas claras que establezcan las actividades a realizar, de tal forma que cuando se evidencien hallazgos, falencias o incidentes de seguridad digital, se tomen medidas para controlarlos y prevenirlos.

Algunas acciones recomendadas por la guía de administración del riesgo de seguridad digital son las siguientes:

- Revisar y evaluar los hallazgos encontrados en las auditorías internas, otras auditorías e informes de los entes de control realizados.
- Establecer las posibles causas y consecuencias del hallazgo.
- Determinar si existen otros hallazgos similares para establecer acciones correctivas y evitar así que se lleguen a materializar.
- Emprender acciones de revisión continua, que permitan gestionar el riesgo a tiempo, disminuir el impacto y la probabilidad de ocurrencia del riesgo detectado, así como la aparición de nuevos riesgos que puedan afectar el desempeño de la entidad pública o de los servicios que presta al ciudadano.

8. PUBLICACIÓN

Su publicación se realizará a través de la página web de la entidad www.aguasdelcesar.gov.co, y en caso de modificación o actualización al "Plan de Tratamiento de Riesgo de Seguridad de la Información", se realizará una nueva publicación por los medios dispuestos.