PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

OFICINA DE SISTEMAS

DIRECCIÓN ADMINISTRATIVA Y FINANCIERA

2022

1. INTRODUCCIÓN

El objetivo primordial del Sistema de Gestión de la Seguridad y Privacidad 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.

2. OBJETIVO GENERAL

Elaborar el Plan de Tratamiento para los riesgos de seguridad y privacidad de la información, identificados en los procesos incluidos en el alcance del SGSI de la empresa Aguas del Cesar S.A. E.S.P.

3. OBJETIVOS ESPECÍFICOS

- ✓ Identificar los riesgos asociados a los procesos que hacen parte del alcance del SGSI.
- ✓ Calcular los niveles de riesgos.
- ✓ Establecer el plan de tratamiento de riesgos de seguridad y privacidad de la información.
- ✓ Realizar seguimiento y control a la eficacia del plan de tratamiento de riesgos.

4. MARCO NORMATIVO

A continuación, se enuncian las normas que rigen la gestión del riesgo operativo:

- 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 943 de 2014: Por el cual se actualiza el Modelo Estándar de Control Interno (MECI).

5. MARCO TEÓRICO

La técnica de análisis de riesgo para activos de información nos permite comprender los riesgos sobre los activos de información a los que puede estar expuesto 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:

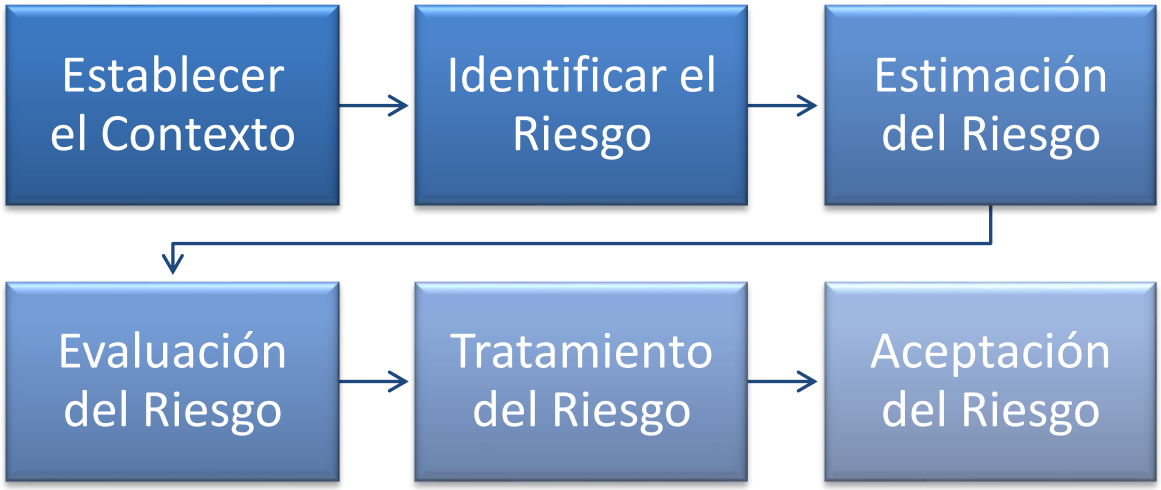

Gráfico 1. *Estructura general de la metodología de riesgos.*

5.1 MODELO PHVA

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

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):

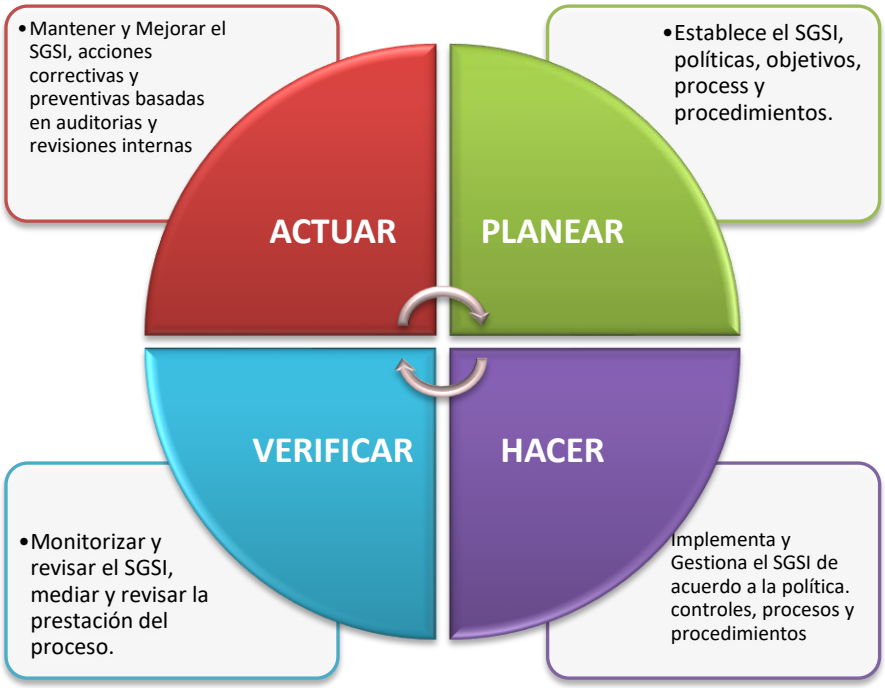

Gráfico 2. *Ciclo PHVA y Gestión de riesgos.*

5.2 METODOLOGÍA MAGERIT

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

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

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

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

Esta metodología tiene como objetivos concientizar a los funcionarios y responsables de la información, los riesgos que enfrentan y como mitigarlos. De igual manera establecer el tratamiento de los riesgos para evitar que los mismos se materialicen.

6. INDENTIFICACIÓN DE LOS RIESGOS

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, 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.

Posterior a la identificación del listado de activos, sus amenazas y las medidas que ya se han tomado, a continuación, se revisarán las vulnerabilidades que podrían aprovechar las amenazas y causar daños a los activos de información de la empresa.

Para cada una de las amenazas analizaremos las vulnerabilidades (debilidades) que podrían ser explotadas.

Finalmente se identificarán las consecuencias, es decir, cómo estas amenazas y vulnerabilidades podrían afectar la confidencialidad, integridad y disponibilidad de los activos de información.

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 y pueden afectar la confidencialidad, integridad y disponibilidad de la información.

INFORMÁTICOS	CAUSAS	EFECTO
Perdida Robo o Fuga de Información.	-Fallas en el proceso de copia de respaldo o de restauración de la información, o pérdida de esta. -Fallas en los análisis y socialización de las vulnerabilidades de la infraestructura de IT -No contar con acuerdos de confidencialidad con los empleados y terceros -Falta de autorización para la extracción de información generadas por requerimientos. -Ingreso a la red y acceso a los activos de TI por parte de máquinas ajenas a la entidad -Habilitación de puertos USB en modo lectura y escritura para medios de almacenamiento -Ataques cibernéticos internos o externos. -Acceso no autorizado a las dependencias. -Conectar dispositivos externos a los equipos. -Falta de implementación de la política escritorio limpio -Empleados no capacitados en los temas de riesgos informáticos. -Desconocimiento del riesgo. -Prestar los equipos informáticos a personal no autorizado. -No cerrar sesión cuando se desplaza del puesto.	-Afectación parcial o total de la continuidad de las operaciones de los servicios del Incumplimiento normativo -Vulneración de los sistemas de seguridad operando actualmente -Mala imagen, multas, sanciones y pérdidas económicas -Generación de consultas, funcionalidades o reportes con información sensible de los clientes -Pérdida o fuga de información.

Correos electrónicos de extraña procedencia	-Empleados no capacitados en los temas de riesgos informáticos. - Desconocimiento del riesgo. - No generar una Cultura de Seguridad de la Información - Falta de Filtros en el Servidor de Correo - Programas de DLP (Data Lost Prevention) - Falta de instalación de EndPoint (programa seguridad punto final) en las estaciones de trabajo.	-Cifrado de la información. - Captura de las pulsaciones del teclado. - Monitoreo de las actividades realizadas en el equipo. - Ataque remoto mediante un troyano o gusano. - Robo de contraseñas. - Robo de documentos y/o archivos. - Sistema con mal funcionamiento.
Daño en los equipos tecnológicos	-Manejo inadecuado de los equipos - Falta de mantenimiento o mala conexión de estos en las instalaciones eléctricas - Falta de equipos de potenciación - Fallas por defectos de fabrica - Derrame de líquido - Falta de ambiente adecuado para los equipos - Falta Educación a los usuarios en el manejo de los equipos de computo	-Perdida de información -Perdidas de los quipos informáticos - Indisponibilidad del Servicio - Traumatismos en los procesos
Perdida de conectividad	Daño externo del ISP (Internet service provider) -Ataque DDoS o DOS (denegación de servicios distribuidos o Denegación de servicios)	

7. IDENTIFICACIÓN DE LAS AMENAZAS

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

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

8. IDENTIFICACIÓN DE LAS VULNERABILIDADES

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

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

9. IDENTIFICACIÓN DE CONTROLES EXISTENTES

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

10. EVALUACIÓN DE RIESGO

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

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

TABLA DE PROBABILIAD

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

Tabla Probabilidad de Riesgo

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

Tabla Impacto del Riesgo

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

B:Zona de Riesgo Baja:Asumir el riesgo

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

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

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

11. RESULTADOS Y DISCUSIÓN

La gestión de Riesgos informáticos permitió conocer las vulnerabilidades, las amenazas y los riesgos informáticos de la empresa Aguas del Cesar S.A. E.S.P., Este Análisis permite a la entidad fortalecer la estructura de la seguridad de la información y prepararse para cualquier evento o incidente.

LINA ROSA PRADO GALINDO
Gerente

Proyectó: Jonathan C. - Profesional de sistemas
Revisó: Ledys N. - Directora Administrativa y Financiera