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

EMPAS S.A.

CUADRO DE CONTROL DE CAMBIOS		
Versión	**Fecha**	**Descripción de la modificación**
00	29/01/2021	Creación y codificación del documento
01	20/12/2021	Actualización general del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2022
02	29/01/2022	Aprobación por el Comité Institucional de Gestión y Desempeño

RESUMEN EJECUTIVO

Mediante la definición del Plan de Tratamiento de Riesgos se busca mitigar los riesgos presentes en el análisis de riesgos (Perdida de la Confidencialidad de los activos, Perdida de Integridad de los activos y Perdida de Disponibilidad de los activos) evitando que estas situaciones dificulten el cumplimiento de la misión y los objetivos estratégicos de EMPAS S.A. El Plan de Tratamiento de Riesgo se define con el propósito de evaluar las posibles acciones que se deben tomar para mitigar los riesgos existentes, estas acciones son organizadas en forma de medias de seguridad y controles a los riesgos, documentados en la matriz de riesgos de la empresa.

Las medidas se definieron teniendo en cuenta la información del análisis de riesgos, el cual brindó información acerca de las necesidades del Proceso de Gestión Informática de EMPAS S.A. en cuanto a la seguridad de la información.

La metodología se basa en el fomento de una cultura de carácter preventivo, de manera que, al comprender el concepto de riesgo, así como el contexto, se planean acciones que reduzcan la afectación a la entidad, igualmente se implementan una serie de controles para reducir la probabilidad de ocurrencia y en caso de que el riesgo se llegue a materializar, se incluyen las acciones correctivas pertinentes en la matriz de riesgos.

Lo anterior dando cumplimiento a la normativa establecida por el estado colombiano, CONPES 3854 de 2016 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 5 emitida por el DAFP.

TABLA DE CONTENIDO

1. INTRODUCCIÓN

La información es un recurso que, como el resto de los activos, tiene valor para la Empresa y por consiguiente debe ser debidamente protegida, garantizando la continuidad de los sistemas de información, minimizando los riesgos de daño y contribuyendo de esta manera, a una mejor gestión.

Para que los principios de Seguridad de la Información sean efectivos, resulta necesaria la implementación de Políticas que formen parte de la cultura organizacional de la Empresa, lo que implica que debe contarse con el compromiso de todos los funcionarios de una manera u otra vinculados a la gestión, para contribuir a la difusión, consolidación y cumplimiento de las mismas. Es así como a través de un Plan de Tratamiento de Riesgos se busca mitigar aquellos riesgos previamente identificados, evitando la Perdida de confidencialidad, perdida de integridad y perdida de disponibilidad de los activos de información de las entidades, para de esta manera cumplir con los lineamientos establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones.

En etapas previas, se revisó el documento con el diagnóstico de seguridad de la información de la entidad, donde se conoció la situación actual de la organización y se desarrolló el inventario de activos de información, para continuar con la medición de riesgos existentes y sugerir las protecciones necesarias que permitan cumplir los objetivos institucionales.

Por otro lado, dado que la Administración General de EMPAS S.A. provee a Directivos, Funcionarios, Empleados y Trabajadores, de medios técnicos e informáticos con herramientas de trabajo que garantizan la rapidez y eficacia en la prestación de sus servicios de acuerdo a sus actividades, entre las que se encuentran equipos, software y sistemas para el uso de herramientas TIC, redes internas y externas, correo electrónico, línea telefónica y otros sistemas de información, se hace necesario el diseño e implementación de Planes para proteger tanto la información que se genera, recibe y almacena en la entidad, como los equipos y programas utilizados para tal fin. Además, Como resultado de la creciente conectividad, los sistemas de información y las redes son más vulnerables ya que están expuestos a un número creciente de amenazas. Esto hace que surjan nuevos retos que deben abordarse en el tema de seguridad y por lo tanto sugieren la necesidad de tener una mayor conciencia y entendimiento de los aspectos relacionados con la información.

Por las razones anteriormente expuestas, se ha visto la necesidad de desarrollar un análisis de riesgo de seguridad digital aplicado en La Empresa Pública de Alcantarillado de Santander S.A. E.S.P.- EMPAS S.A. en virtud de las competencias de la Gerencia General sobre la administración de los bienes tangibles e intangibles de la Empresa, en este documento se establecen las directrices para el tratamiento de los riesgos de seguridad y privacidad de la información, dando cumplimiento a la normativa establecida por el estado colombiano, CONPES 3854 de 2016 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. MARCO LEGAL

A continuación, se relacionan las normas que enmarcan la planeación, implementación, ejecución y medición del presente plan.

AÑO	NORMA	DESCRIPCIÓN
2009	Ley 1341	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 –TI, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.
2014	Decreto 2573	Decreto mediante el cual se dan los tiempos de implementación de la Estrategia de Gobierno en Línea y donde se establece que el modelo de seguridad y privacidad de la información pertenece al componente de Elementos Transversales.
2015	Decreto 1078	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
2016	Decreto 415	Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones.
2017	Decreto 1499	Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015; artículo 1. Sustituir el Título 22 de la Parte 2 del Libro 2 del Decreto 1083 de 2015.
2018	Decreto 1008	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.
2018	Decreto 612	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. Artículo 2: Transición. Las entidades del Estado de manera progresiva deberán integrar los planes a que se refiere el presente Decreto al Plan de Acción y publicarlo en la página web a más tardar el 31 de julio de 2018.
2016	CONPES 3854	Política Nacional De Seguridad Digital
	NTC / ISO 27001	Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI).
	NTC / ISO 31000	Gestión del Riesgo

Tabla 1. Marco legal para el plan.

3. DOCUMENTOS DE REFERENCIA

- MADE-01. Manual de Administración de Riesgos de EMPAS S.A.

- FOGI-01. Inventario de Activos de Información.

- PLGI-02. Plan Estratégico de Tecnologías de la Información.

- PLGI-03. Plan de Seguridad y Privacidad de la Información

- Modelo de Seguridad y Privacidad de la Información – MINTIC

- Fode-13. Matriz de Riesgos por procesos – EMPAS S.A.

- Modelo Integrado de Planeación y Gestión – MIPG

- NTC ISO 9001:2015

4. OBJETIVO

OBJETIVO GENERAL

Identificar, controlar y minimizar los riesgos asociados a los procesos tecnológicos existentes, en EMPAS S.A., mediante la construcción de una hoja de ruta que permita salvaguardar los activos de información.

OBJETIVOS ESPECIFICOS

- Concientizar a todos los funcionarios, contratistas y terceros en general sobre la necesidad e importancia de gestionar de manera adecuada, los activos de información.

- Gestionar los riesgos en materia de Seguridad y privacidad de la información que se puedan presentar de acuerdo al contexto de la entidad.

- Proteger los recursos de información de EMPAS S.A y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad y legalidad de la información.

- Cumplir la normatividad TI vigente para el desarrollo y aplicación de los procesos tecnológicos en la Empresa.

5. ALCANCE

Salvaguardar los activos de información de la Empresa Pública de Alcantarillado de Santander S.A. E.S.P., a través de una adecuada y eficiente gestión de los riesgos de seguridad y privacidad de la información, con el propósito de contribuir al cumplimiento de los objetivos y metas institucionales de EMPAS S.A.

Así mismo, se dan los lineamientos para el análisis, tratamiento, evaluación y monitoreo de los riesgos de seguridad y privacidad de la información en la empresa. La entidad,soportada

en el área de Sistemas de Información, decide incluir en el Plan de Tratamientode Riesgos aquellos riesgos que se encuentren en niveles altos o extremos en la matriz de riesgos de la compañía, aceptando los demás riesgos que se hayan identificado y caracterizado.

La mitigación de los riesgos debe ser establecida bajo un proceso estructurado y sistemático es por ello que esta guía contiene la definición de los roles y responsabilidades, y hace mención de los formatos y documentos que tienen relación.

6. VIGENCIA

El presente documento entrará en vigencia una vez sea revisado y aprobado por el comité Gestión y Desempeño Institucional, así como por la Gerencia General de la Empresa Pública de Alcantarillado de Santander EMPAS S.A. para la vigencia 2022.

7. RECURSOS

EMPAS S.A. cuenta con los siguientes recursos para establecer el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, así como para su implementación:

Recurso Humano

La Subgerencia de Planeación e Informática, a través del área de Sistemas de Información, se encarga del liderazgo, coordinación, implementación, seguimiento y ajuste de las políticas, estrategias, tácticas y procedimientos en la organización, referentes a la seguridad y privacidad de la información. De ser necesario se debe contar con el apoyo de otras áreas como la de gestión documental y planeación estratégica.

Recursos Técnicos

Dentro de los recursos técnicos se cuenta con la Guía para la administración del riesgo y diseño de controles en entidades públicas del DAFP. Igualmente se cuenta con la guía de gestión de riesgos de seguridad y privacidad de la información proporcionada por el Ministerio de las TIC, así como con el Plan de Gestión de Riesgos de Seguridad y Privacidad de la Información.

Recursos Logísticos

Todos aquellos recursos necesarios para socializar las políticas, transferir conocimiento y realizar el seguimiento de los riesgos, dentro de los que se encuentran todas las herramientas (computadores, software, equipo de oficina) empleadas en la elaboración del Plan.

Recursos Financieros

Recursos destinados para la adquisición de conocimiento, recursos humanos y técnicos, necesarios para desarrollar las acciones y actividades que se planteen después del análisis de los riesgos y su valoración.

8. DEFINICIONES

Para la administración del riesgo, se tendrán en cuenta los siguientes términos y definiciones:

Activo de Información: se refiere a cualquier elemento que contiene información de valor para la empresa y que por tanto debe ser protegido.

Amenaza: Situación extrema que no controla la entidad y que puede afectar su operación

Causa: Medios, circunstancias y/o agentes que generan riesgos.

Consecuencia: Efectos que se pueden presentar cuando un riesgo se materializa

Control: Acción o conjunto de acciones que minimiza la probabilidad de ocurrencia de un riesgo o el impacto producido ante su materialización.

Gestión del Riesgo: se refiere a las actividades llevadas a cabo por la dirección para dar tratamiento integral a los riesgos que puedan afectar a la organización.

Impacto: Medida para estimar cuantitativa y cualitativamente el posible efecto de la materialización del riesgo.

Materialización del Riesgo: Ocurrencia del riesgo identificado.

Matriz de Riesgos: Documento que, de manera sistemática, muestra el desarrollo de las etapas de la administración del riesgo.

Probabilidad: Medida para estimar cuantitativa y cualitativamente la posibilidad de ocurrencia del riesgo.

Procedimiento: Conjunto de especificaciones, relaciones, responsabilidades, controles y ordenamiento de las actividades y tareas requeridas para cumplir con el proceso.

Proceso: Conjunto de entradas tangibles o intangibles, suministradas por un proveedor, a estas entradas se les asigna recursos y se aplican controles, obteniendo salidas tangibles o intangibles, destinadas a un usuario, generando un impacto en estos. Se clasifican en estratégicos, misionales, de apoyo y de evaluación.

Riesgo: Eventualidad que tendrá un impacto negativo sobre los objetivos institucionales o del proceso.

Seguridad de la Información: práctica que vela por salvaguardar la confidencialidad, la integridad y la disponibilidad de la información.

Vulnerabilidad: es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.

9. MARCO TEÓRICO

De acuerdo a las directrices del Departamento Administrativo de la Función Pública – DAFP, es necesario desarrollar un plan que permita dar tratamiento integral a los riesgos que se puedan presentar dentro de las entidades públicas. Este plan debe tener base en la metodología para la administración del riesgo diseñada por el DAFP, como se muestra en el siguiente esquema.

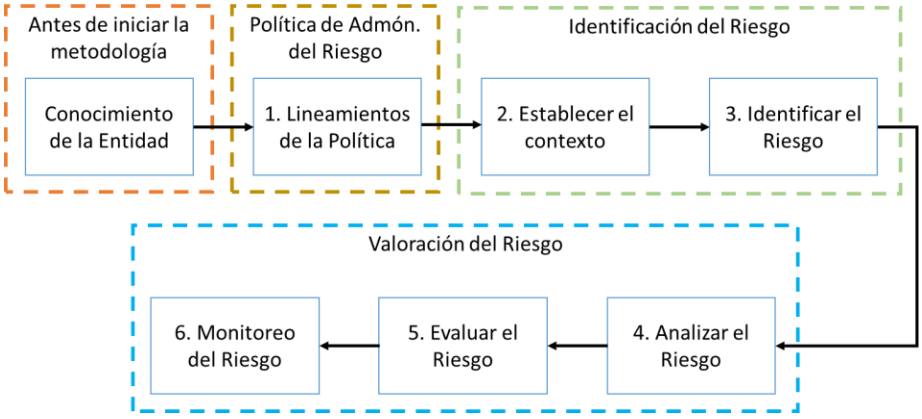

Ilustración 1. Esquema de la metodología de Administración del Riesgo. Adaptado de DAFP

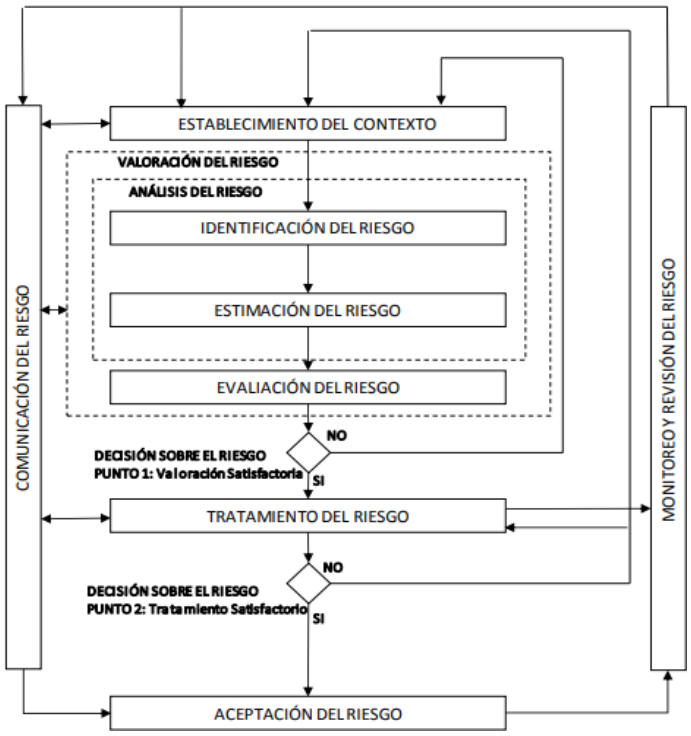

Ilustración 2. Proceso para la gestión del riesgo en seguridad de la información. Tomado de: NTC-ISO/IEC 27005

El conocimiento de la entidad y la Política de Administración del Riesgo, deben estar incluidas en la estrategia de la empresa, de tal manera que el tratamiento de los riesgos se realice en concordancia con los objetivos de la organización. La tabla 2 resume las actividades de gestión del riesgo en la seguridad de la información relacionadas con las cuatro fases del Modelo de Seguridad y Privacidad de la Información.

ETAPA	GESTION DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN
Planear	Establecer Contexto Valoración del Riesgo Planificación del Tratamiento del Riesgo Aceptación del Riesgo
Implementar	Implementación del Plan de Tratamiento de Riesgo
Gestionar	Monitoreo y Revisión Continuo de los Riesgos
Mejora Continua	Mantener y Mejorar el Proceso de Gestión del Riesgo en la Seguridad de la Información

Tabla 2. Etapas de la Gestión del Riesgo a lo Largo del MSPI

Riesgo se define como la posibilidad de que ocurra algún evento que tendrá un impacto sobre el cumplimiento de los objetivos y se expresa en probabilidades y consecuencias. De igual manera los riesgos se pueden clasificar como: Riesgo inherente, cuando la dirección no toma medidas al respecto, o Riesgo Residual cuando se toman medidas de tratamiento y gestión para mitigarlo. Igualmente, define la administración del riesgo como un proceso llevado a cabo por la dirección de la organización junto con todo el personal para lograr un aseguramiento de la consecución de los objetivos.

En cuanto a los riesgos asociados a la seguridad y privacidad de la información, es el Ministerio de las Tecnologías de la Información y las Comunicaciones el encargado de proponer las pautas para la gestión del riesgo asociados con las TIC, regulando los riesgos de los procesos y proyectos para optimizar de manera continua y oportuna la respuesta a los riesgos de seguridad y privacidad de la Información y Seguridad Digital de manera Integral.

La política busca identificar, tratar y manejar los riesgos con base en su valoración, con el propósito de tomar decisiones adecuadas en la gestión de los mismos, al mismo tiempo que transmite las posiciones y mandatos de la dirección, estableciendo las guías de acción y pasos a seguir necesarios para todos los colaboradores de la EMPAS S.A. Dentro de las opciones con las que cuenta la dirección se encuentran:

- Evitar: es eliminar la probabilidad de ocurrencia o disminuir totalmente el impacto, lo que requiere la eliminación de la actividad o fuente de riesgo, eliminar la exposición y su expresión máxima es dejar una actividad. Por ejemplo, para evitar perdida de documentación se prohíbe el ingreso a un área.
- Prevenir: planear estrategias conducentes a que el evento no ocurra o que disminuya su probabilidad. Un ejemplo de ello son las inspecciones el mantenimiento preventivo, las políticas de seguridad o las revisiones periódicas a los procesos
- Reducir o mitigar: corresponde a la protección en el momento en que se presenta el riesgo se encuentra en esta categoría los planes de emergencia planes de continencia equipos de protección personal, ambiental, de acceso mantener copias de respaldo

- Dispersar: es dividir una actividad en diferentes componentes operativos, de manera que las actividades no se concentren en un mismo sitio o bajo una sola responsabilidad. Este es el caso de los contratos de suministro de partes, la ubicación de nodos, plantas alternas, equipos paralelos, contratar obras por tramos
- Compartir: es involucrar a un tercero para que responda en todo o en parte por el riesgo que genera una actividad. Dentro de los mecanismos de transferencia se encuentran los siguientes: contratos de seguro, transferencia explicita por medio de cláusulas contractuales, derivados financieros.

Una vez haya sido detectado el riesgo, este deberá ser analizado con el fin de que se pueda determinar las acciones a seguir para su gestión, identificando el proceso donde se presenta y su responsable.

La política identifica las opciones para tratar y manejar los riesgos basados en su valoración, permiten tomar decisiones adecuadas y fijar los lineamientos para administración de los mismos; a su vez, transmiten la posición de la dirección y establecen las guías de acción necesarias.

10. DESARROLLO METODOLÓGICO

Para llevar a cabo el tratamiento de los riesgos de seguridad de la información en la Empresa EMPAS S.A, se toma como base la metodología PHVA (Planear, Hacer, Verificar, Actuar) y los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las comunicaciones – MinTIC, a través de los decretos emitidos.

La metodología para la administración del riesgo requiere de un análisis inicial relacionado con el estado actual de la estructura de riesgos y su gestión de la empresa, el conocimiento de esta desde un punto de vista estratégico de la aplicación de tres (3) pasos básicos para su desarrollo y de la definición e implantación de estrategias de comunicación transversales a toda la empresa, para que su efectividad pueda ser evidenciada. A continuación, se puede observar la estructura completa con sus desarrollos básicos:

Paso 1: Política de Administración de Riesgos - Lineamiento de la Política de Riesgos

Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo. La gestión o administración del riesgo establece lineamientos precisos acerca del tratamiento, manejo y seguimiento a los riesgos. Esta política puede encontrarse en el documento MADE-01, Manual de Administración de Riesgos de EMPAS S.A.

Paso 2: Identificación de Riesgos – Análisis y Definición de Objetivos

En esta etapa se deben establecer las fuentes o factores de riesgo, los eventos o riesgos, sus causas y sus consecuencias. Para el análisis se pueden involucrar datos históricos, análisis teóricos, opiniones informadas y expertas y las necesidades de las partes involucradas (NTC ISO 31000, Numeral 2.15).

Paso 3. Valoración de Riesgos

Establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el fin de estimar la zona de riesgo inicial.

Para lograr una eficiente mitigación de los riesgos sobre los activos de información, el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información contempla una serie de actividades que se plantean siguiendo las recomendaciones y directrices de la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información, del MINTIC.

	ACTIVIDAD	RESPONSABLE	FECHA LÍMITE
Actualización de lineamientos de riesgos	Entender y Actualizar la política de gestión de riesgos.	Planeación Corporativa	30-Abr-22
	Actualización inventario de activos de información.	Contratista de Gobierno Digital	30-Abr-22
Autodiagnóstico de seguridad de la información.	Desarrollar la herramienta de Autodiagnóstico de seguridad de la información.	Contratista de Gobierno Digital	30-Abr-22
Tratamiento de Riesgos de Seguridad y Privacidad de la Información	Identificación, Análisis y Evaluación de Riesgos de Seguridad y Privacidad de la Información.	Equipo de sistemas de información	31-Ago-22
	Realimentación, revisión y verificación de los riesgos identificados.	Contratista de Gobierno Digital	31-Ago-22
	Evaluación del nivel de impacto vs probabilidad y los controles existentes para calcular el nivel de riesgo.	Equipo de sistemas de información	31-Ago-22
	Aprobación de riesgos identificados e inclusión en la matriz de riesgos de la empresa.	Profesional SIGC	31-Ago-22
Seguimiento	Seguimiento al tratamiento de los riesgos.	Equipo de Gestión de Riesgos	31-Dic-22
Evaluación Riesgos residuales	Cálculo del riesgo residual basado en la eficacia de los controles existentes.	Equipo de Sistemas de Información y Profesional SIGC	31-Dic-22
Mejoramiento y control	Seguimiento a los controles de los riesgos de Seguridad y Privacidad de la Información	Control Interno	31-Dic-22

Tabla 3. Actividades para el desarrollo e implementación del Plan de Gestión de Riesgos de Seguridad y Privacidad de la Información

9.1. Roles y Responsabilidades Frente a la Administración del Riesgo

El éxito de la administración del riesgo depende de diversos factores, aun así, la participación de la alta dirección en este caso de la gerencia lo que permite que el proceso se desarrolle con mayor fluidez y efectividad es por ello que en la identificación de los roles no solo se observa el equipo técnico que hará las labores de análisis y tratamiento del riesgo.

Representante Legal o Gerencia General: Aprueba las directrices para la administración del riesgo en la empresa.

Área de Sistemas de Información: Encargada del planteamiento, implementación y medición de la política.

Secretaria General: Encargada de asignación o autorización de las acciones para implementar la política de seguridad y privacidad de la información.

Subgerencias: (Comercial y Tarifaria, Administrativa y Financiera, Alcantarillado, Planeación e Informática y Tratamiento Integral de Aguas y Residuos) Apoyan la ejecución de las etapas de gestión del riesgo a nivel de los procesos.

Servidores Públicos y Contratistas: Ejecutar los controles y acciones definidas para la administración de los riesgos definidos, aportar en la identificación de posibles riesgos que puedan afectar la gestión de los procesos y/o de la empresa.

Responsables de los Procesos: Identifican, analizan, evalúan y valoran los riesgos de la empresa (por procesos e institucionales) al menos una vez al año. Si bien los Líderes del SIGC apoyan la ejecución de las etapas de gestión del riesgo a nivel de los procesos, esto no quiere decir que el proceso de administración de riesgos este solo bajo su responsabilidad. Al contrario, cada responsable de proceso se encarga de garantizar que en el proceso a su cargo se definan los riesgos que le competen, se establezcan las estrategias y responsabilidades para tratarlos y, sobre todo, que se llegue a cada funcionario que trabaja en dicho proceso. No se debe olvidar que son las personas que trabajan en cada uno de los procesos los que mejor conocen los riesgos existentes en el desarrollo de sus actividades.

Oficina de Control Interno: Debe realizar evaluación y seguimiento a la política, los procedimientos y los controles propios de la administración del riesgo.

9.2. Política de Administración del Riesgo de EMPAS S.A.

EMPAS S.A adelantará las acciones pertinentes para la implementación y mantenimiento del proceso de Administración del Riesgo, y para ello todos los servidores de la empresa se comprometen a:

1. Conocer y cumplir las normas internas y externas relacionadas con la administración de los riesgos.

2. Fortalecer la cultura de la administración de los riesgos para crear conciencia colectiva sobre los beneficios de su aplicación y los efectos nocivos de su desconocimiento.

3. Someter los procesos y procedimientos permanentemente al análisis de riesgos con base en la aplicación de las metodologías adoptadas para el efecto.

4. Mantener un control permanente sobre los cambios en la calificación de los riesgos para realizar oportunamente los ajustes pertinentes.

5. Reportar los eventos de riesgo que se materialicen, utilizando los procedimientos e instrumentos establecidos para el efecto.

6. Desarrollar e implementar planes de contingencia para asegurar la continuidad de los procesos, en los eventos de materialización de los riesgos que afecten a los objetivos institucionales previstos y los intereses de los usuarios y partes interesadas.

7. Presentar propuestas de mejora continua que permitan optimizar la forma de realizar y gestionar las actividades de la empresa para así aumentar nuestra eficacia y efectividad.

9.3. Evaluación del Riesgo

Para realizar un análisis de los riesgos, se procede a identificar los activos de información que deben ser protegidos, los daños que pueden sufrir, sus posibles fuentes de daños y oportunidad, su impacto en la compañía, y su importancia dentro del mecanismo de funcionamiento. Posteriormente se procede a realizar los pasos necesarios para minimizar o anular la ocurrencia de eventos que posibiliten los daños, y en último término, en caso de ocurrencia de estos, se procede a fijar un plan de emergencia para su recomposición o minimización de las pérdidas y/o los tiempos de remplazo o mejoría.

9.4. Etapas para la Administración del Riesgo

A continuación, se presenta cada una de las etapas a desarrollar durante la administración del riesgo; en la descripción de cada etapa se desplegarán los aspectos conceptuales y operativos que se deben tener en cuenta.

9.4.1. Análisis Contexto Estratégico

Definir el contexto estratégico marca la pauta o ruta que la empresa debe asumir frente a la exposición al riesgo, ya que permite conocer las situaciones generadoras de riesgos de seguridad y privacidad de la información, evitando establecer las condiciones ideales para la materialización.

Para la definición del contexto estratégico, es fundamental tener claridad sobre cuál es el Plan Estratégico de Gestión y Resultados de EMPAS S.A. y cuáles son los planes programas o proyectos a ejecutarse.

9.4.2. Identificación de Riesgos

En esta fase del documento el objetivo es evaluar todos los activos que se encuentran expuestos a riesgos de seguridad y privacidad de la información. De esta forma se definirá claramente un punto de salida de todos los activos, sean estos tangibles o no, dentro de la compañía y pudiendo analizar a qué amenazas podrían estar expuestos.

Una vez se dispone de un listado de las amenazas reales que pueden afectar a los activos de información, se procede a realizar la evaluación del impacto que sufrirá la compañía en caso de que se materialicen estas amenazas. Como resultado de esta fase, se obtiene:

- El inventario de activos de información de EMPAS S.A. actualizado.
- Matriz de riesgos actualizada.

9.4.2.1. Inventario de Activos

El primer punto para el análisis es estudiar los activos vinculados a la información. Es habitual agrupar los activos por grupos para ello. En el caso de EMPAS S.A., se agrupan de la siguiente manera:

Sigla	Tipo o grupo de activo
I	Información
HW	Hardware
SW	Software
S	Servicio
P	Recurso Humano

Tabla 4. Agrupación por tipo de activo de información

Una vez identificados los activos de información, se ha de realizar la valoración de los mismos. Esta valoración mide la criticidad a las cuatro dimensiones de la seguridad de la información gestionada por los procesos de EMPAS S.A. Esta valoración nos permitirá, a posteriori, valorar el impacto que tendrá la materialización de la amenaza sobre la parte del activo expuesto.

Las cuatro dimensiones de seguridad son:

Confidencialidad. Únicamente las personas autorizadas tienen acceso a la información sensible o privada.

Integridad. La información y los métodos de procesamiento de esta información son exactos y completos, y no se han manipulado sin autorización.

Disponibilidad. Los usuarios que están autorizados pueden acceder a la información cuando lo necesiten.

Clasificación. Define si el tipo de información contenida es clasificada, reservada, pública o de uso interno, según Ley 1712 de 2014 y norma ISO 27001:2013.

Una vez detalladas las cinco dimensiones se ha de tener presente la escala en que se realizarán las valoraciones, de acuerdo al Manual de Gestión del Riesgo de EMPAS S.A.

9.4.2.2. Posibilidad de Daños

Los posibles daños pueden referirse a imposibilidad de acceso a los recursos debido a problemas físicos en las instalaciones donde se encuentran los bienes, sean por causas naturales o humanas o imposibilidad de acceso a los recursos informáticos por razones lógicas en los sistemas en utilización, sean estos por cambios involuntarios o intencionales.

Las posibles fuentes de daño que pueden causar la no operación normal de la Empresa EMPAS S.A. son:

a) Acceso no autorizado por vulneración de los sistemas de seguridad en operación (Ingreso no autorizado a las instalaciones). Ruptura de las claves de acceso a los sistemas computacionales.
b) Instalación de software de comportamiento errático y/o dañino para la operación de los sistemas computacionales en uso (Virus, sabotaje).
c) Intromisión no calificada a procesos y/o daños de los sistemas, ya sea por curiosidad o malas intenciones.
d) Falla en el Servidor de Aplicaciones y Datos, tanto en sus discos duros como en el procesador central.
e) Falla en el hardware o infraestructura de Red.
f) Falla en el Router, o en alguno de los servidores secundarios.

9.4.2.3. Medidas Preventivas

- **Control de Accesos**

Se definen las siguientes medidas para controlar los diferentes accesos a los activos computacionales:

a) Acceso físico únicamente de personas autorizadas.
b) Acceso restringido a los aplicativos (FOGI-04).
c) Acceso restringido a través de cuentas de usuario administrador.

- **Previsión de Desastres Naturales**

La previsión de desastres naturales sólo se puede hacer bajo el punto de vista de minimizar los riesgos innecesarios en los equipos de la Empresa EMPAS S.A., en la medida de no dejar objetos en posición tal que ante un movimiento telúrico pueda generar mediante su caída y/o destrucción, la interrupción del proceso de operación normal. Además, bajo el punto de vista de respaldo, el tener en claro los lugares de resguardo, vías de escape y de la ubicación de los archivos, discos con información vital de respaldo de aquellos que se encuentren aun en las instalaciones. Igualmente, la infraestructura de EMPAS S.A. cuenta con servidor redundante para minimizar la posibilidad de pérdida de la información.

- **Adecuado Soporte de Utilitarios**

Las fallas de los equipos de procesamiento de información se minimizan mediante el uso de otros equipos, a los cuales también se les debe controlar periódicamente su buen funcionamiento, específicamente a UPS de respaldo de actual servidor de Red o de estaciones críticas y a UPS de respaldo switches y servidores.

- **Seguridad Física del Personal**

Se deberá tomar las medidas para recomendar, incentivar y lograr que el personal de EMPAS S.A. comparta sus conocimientos con sus colegas dentro de cada área, en lo

referente a la utilización de software y elementos de soporte relevantes. Estas acciones permitirán mejorar los niveles de seguridad, permitiendo los reemplazos en caso de desastres, emergencias o periodos de ausencia ya sea por vacaciones o enfermedades.

- **Seguridad de la Información**

La información y programas de los Sistemas de Información que se encuentran en el servidor, o de otras estaciones de trabajo (portátiles o equipos de cómputo) críticas se protegen mediante claves de acceso y a través de un plan de respaldo adecuado (Plan de copias de seguridad y Backup).

9.4.3. Plan de Recuperación (Copias de seguridad)

El plan de respaldo o plan de copias de seguridad muestra cómo y cuándo se llevan a cabo los controles para evitar pérdida de información a través de la creación de un Backup.

9.4.3.1. Respaldo de Datos Vitales

Se deberá identificar las áreas para realizar respaldos:

a) Sistemas de información.
b) Sitio WEB.
c) Bases de datos.
d) Ejecutables de aplicaciones.
e) WebServices.
f) Repositorios de archivos.

9.4.3.2. Objetivos del Plan de Recuperación

Los objetivos del plan de Recuperación son:

a) Determinación de las políticas y procedimientos para respaldar las aplicaciones y datos.
b) Planificar la reactivación después de producido un desastre, todo el sistema de procesamiento y sus funciones asociadas.
c) Permanente mantenimiento y supervisión de los sistemas y aplicaciones.
d) Establecimiento de una disciplina de acciones a realizar para garantizar una rápida y oportuna respuesta frente a un desastre.

9.4.3.3. Alcance del Plan de Recuperación

Restablecer en el menor tiempo posible el nivel de operación normal de los sistemas de información de EMPAS S.A. La responsabilidad sobre el Plan de Recuperación es de la Administración, la cual debe considerar la combinación del personal, equipos, datos, sistemas, comunicaciones y suministros.

Todos los miembros del área de sistemas de información deben estar informados y entrenados, así como poseer una copia del Plan de Contingencia. Una copia del plan debe mantenerse almacenada en EMPAS S.A., junto con los respaldos. Las copias de seguridad se almacenan en la nube y en medios físicos en la sede de alcantarillado.

9.4.4. Plan de Contingencias

De acuerdo al análisis de riesgos y a la revisión de seguridad realizada, se presentan las sugerencias de los casos para combatir cada uno de los riesgos potenciales a los que se enfrenta la red informática.

9.4.4.1. Contra la Acción de Virus

Es necesario mantener actualizado el software de antivirus en todas las estaciones de trabajo y servidores, tarea que se desarrolla de forma anual a través de la adquisición del licenciamiento.

9.4.4.2. Contra Accesos No Autorizados

Los servidores físicos no deben ser accesible físicamente a cualquier persona. Es conveniente que exista un espacio físico donde se ubique cada servidor, con acceso restringido al personal autorizado, y que cumpla con los requisitos adecuados para su funcionamiento, como temperatura ambiental adecuada, aislado del polvo y plagas dañinas. En este espacio, además de ubicar el servidor, se ubican los elementos más sensibles de la red corporativa como Switches y el Firewall. Se debe continuar con el plan de mantenimiento preventivo a los equipos y correctivos.

9.4.4.3. Implementación de Procedimiento de Manejo de Incidentes de Seguridad

Cuando se habla de incidente de seguridad, se hace referencia a un suceso que se presentó o que tiene una gran posibilidad de darse en un momento determinado. Este suceso puede ser por voluntad o accidental. Dependiendo de la gravedad de la situación este puede afectar el funcionamiento normal de la organización. Por lo general el manejo del incidente implica que este se debe solucionar en el menor tiempo posible para evitar una afectación mayor y se debe buscar documentar cada uno de los eventos presentados y el tiempo que transcurrió entre cada uno de ellos, con el fin de poderlo analizar posteriormente y aplicar correcciones del caso para que en un futuro este no se vuelva a presentar o al menos su impacto sea lo menor posible. Para ello, se establece el formato FODE-44 a través del cual se documentan los incidentes de seguridad de la información.

9.5. Seguimiento, Medición, Análisis y Evaluación

Para evidenciar la efectividad de la gestión de riesgos de seguridad y privacidad de información, es necesario realizar revisiones con una periodicidad anual del valor de los activos, impactos amenazas, vulnerabilidad y probabilidad, con el propósito de anticiparse a los cambios que requieran una nueva valoración del riesgo, de esta manera EMPAS S.A. completará el ciclo PHVA en el que se basa la metodología para la gestión del riesgo, y lo más importante, contará con una política para administrar y dar tratamiento a estos riesgos.

11. PRESUPUESTO

El presupuesto asignado para el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información será incluido en los gastos de funcionamiento del área de sistemas de información, dependencia encargada de gestionar los riesgos de seguridad digital. Para otro tipo de riesgos que se identifiquen, la estimación y asignación del presupuestorequerido para implementar los controles corresponderá al dueño del riesgo.

Actualizo	Revisó	Aprobó
Contratista Área de Sistemas de información	Asesor de Gerencia Sistemas deinformación.	Comité Institucional de Gestión y Desempeño