Sanatorio de Agua de Dios
Empresa Social del Estado

RESOLUCIÓN No. 10.39.060 DE 2026
(Enero 28)

Por la cual se adopta el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información del Sanatorio de Agua de Dios E.S.E., para la vigencia 2026

EL GERENTE DEL SANATORIO DE AGUA DE DIOS E.S.E.

En uso de sus atribuciones legales y estatutarias, y

CONSIDERANDO

Que el Sanatorio de Agua de Dios, es una Empresa Social del Estado, de naturaleza pública, descentralizada del orden nacional, con personería jurídica, patrimonio propio y autonomía administrativa, adscrita al Ministerio de Salud y Protección Social, cuyo objeto es prestar el servicio de salud a los enfermos de Hansen en todo el territorio Nacional, y a la comunidad en general.

Que los artículos 2.2.21.3.3 y 2.2.21.3.4 del Decreto 1083 de 2015 hacen referencia a la planeación como uno de los procesos fundamentales de la administración, considerándola como una herramienta gerencial que articula y orienta las acciones de la entidad, para el logro de los objetivos institucionales en cumplimiento de sumisión particular y los fines del Estado en general; es el principal referente de la gestión, puesto que a través de ella se definen y determinan las estrategias, objetivos y metas.

Que el ejercicio de la planeación organizacional debe llevar implícitas dos características importantes: debe ser eminentemente participativo y concertado, así como tener un despliegue adecuado y suficiente en todos los niveles y espacios de la institución; por tanto, la planificación de la gestión debe asumirse como una responsabilidad corporativa, tanto en su construcción como en su ejecución y evaluación.

Que el Plan de Tratamiento de Riegos de Seguridad y Privacidad de la Información es una herramienta básica del proceso administrativo, que permitirá establecer una guía de acción clara y precisa para la administración de las Tecnologías de Información y Comunicaciones de esta entidad, mediante la propuesta de seguridad que garantice el control de los riesgos asociados a los procesos tecnológicos existentes, en el Sanatorio de Agua de Dios E.S.E. con la finalidad de salvaguardar la información y los demás activos tanto de hardware como de software.

Que según Decreto 612 de 2018 de Abril 4 *"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"*, estableció que el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información hace parte de la integración de los planes institucionales y debe publicarse en la página web, según *ARTÍCULO 1. Adicionar al Capítulo 3 del Título 22 de la Parte 2 del Libro 2 del Decreto 1083 de 2015, Único*

RESOLUCIÓN No. 10.39.060 DE 2026
(Enero 28)

Por la cual se adopta el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información del Sanatorio de Agua de Dios E.S.E., para la vigencia 2026

Reglamentario del Sector de Función Pública, los siguientes artículos:"2.2.22.3.14. Integración de los planes institucionales y estratégicos al Plan de Acción. Las entidades del Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión, al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011, deberán integrar los planes institucionales y estratégicos que se relacionan a continuación y publicarlo, en su respectiva página web, a más tardar el 31 de enero de cada año.

Que, en virtud de lo anterior, se hace necesario adoptar y aprobar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información del Sanatorio de Agua de Dios E.S.E. para la vigencia 2026, el cual fue socializado y aprobado en el Comité Institucional de Gestión y Desempeño llevado a cabo el día 20 de enero de 2026 el cual se encuentra soportado mediante acta No. 001 de 2026.

Que, en mérito a lo expuesto,

RESUELVE:

ARTICULO 1°. Aprobar y adoptar el **PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN** para la vigencia 2026, para el Sanatorio de Agua de Dios Empresa Social del Estado el cual forma parte integral del presente acto administrativo.

ARTICULO 2°. Para el cabal cumplimiento y el desarrollo del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información los líderes de proceso son los responsables de las acciones para el logro de los indicadores; quienes contaran con el apoyo y colaboración permanente de todas las áreas y funcionarios del Sanatorio de Agua de Dios E.S.E.

ARTICULO 3°. La presente Resolución rige a partir de su expedición y deroga las disposiciones que le sean contrarias.

COMUNIQUESE Y CUMPLASE

Dada en Agua de Dios, a los veintiocho (28) días del mes de Enero de dos mil veintiséis (2026).

ANTONIO RUIZ FLOREZ
GERENTE

Proyectó: César Mauricio Ubaque Téllez – Coordinador GIT Planeación, Gestión Documental y Tic's
Revisó: Luis Jerónimo Pérez Pérez – Asesor Jurídico

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

ELABORADO POR:

GERXON MAURICIO ESPINOSA SATIVA

SANATORIO DE AGUA DE DIOS E.S.E.

MACROPROCESO GESTION DE APOYO

PROCESO GESTION TECNOLOGICA

2026

FECHA DE APROBACIÓN: 20/01/2026

TABLA DE CONTENIDO

1 INTRODUCCIÓN

La Seguridad de la Información, según ISO 27001, describe la confidencialidad, la integridad y la disponibilidad de la información y los datos importantes para la organización, independientemente del formato que tengan; hoy en día la gran mayoría de las entidades cuenta con un sistema de información y reconoce la importancia que esta tiene para su funcionamiento y como esta debe estar adecuadamente identificada y protegida.

El sanatorio de Agua de Dios E.S.E. es una entidad descentralizada proveedora de gran cantidad de información tanto magnética como física, la cual se encuentra en continuo procesamiento para el reporte de diferentes informes tanto internos como externos, hecho que implica un riesgo a la negligente manipulación de la información o a la perdida de la misma, lo que podría traer problemas económicos, legales y/o administrativos por lo cual este documento busca establecer una línea de trabajo que permita a la entidad sortear los riesgos a la cual está expuesta y lograr que su información este segura.

Por lo anterior es fundamental que la entidad vincule el plan de tratamiento de riesgos de seguridad y privacidad de la información en cumplimiento al decreto 612 de 2018, como medio o herramienta para el logro de los objetivos de mantener la información de la Entidad confidencial, integra y disponible.

2 OBJETIVO

Elaborar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información del Sanatorio de Agua de Dios E.S.E.

3 OBJETIVOS ESPECÍFICOS

- Auto diagnóstico de los riesgos de Seguridad y Privacidad de la Información en el Sanatorio de Agua de Dios E.S.E.
- Establecer las fases de implementación del Plan de Tratamiento de Seguridad y Privacidad de la Información.
- Proteger los activos informáticos mediante la implementación de acciones de mitigación frente al riesgo.

4 ALCANCE

El plan de Riesgos de Seguridad y Privacidad aplica a todos los procesos de la institución los cuales manejen, procesen o interactúen con información física y magnética del Sanatorio de Agua de Dios y sus partes interesadas.

5 ENFOQUE DIFERENCIAL

El Sanatorio de Agua de Dios E.S.E, se acoge a los lineamientos normativos del Plan de Atención Integral en Salud, con el desarrollo de estrategias de enfoque de género y enfoque diferencial a la población que demande los servicios de salud ofertados, para la población que se identifique en situación de vulnerabilidad: víctimas del conflicto armado, grupos étnicos, población en situación de discapacidad; personas de talla baja; habitantes de calle; población dispersa; según el curso de vida (gestantes y adulto mayor) de conformidad con la Política de atención diferencial definida por la entidad. ¨Para esto los colaboradores deberán respetar las diferencias socio culturales; identidades de género y orientación sexual; identificarán las condiciones especiales de la población, darán cumplimiento a las estrategias para

atender condiciones especiales aplicables, la Alta Dirección brindará capacitación al talento humano sobre enfoque diferencial y las estrategias adoptadas, contará con los recursos necesarios para implementar las estrategias definidas, realizará seguimiento a la implementación de las mismas, evaluará la efectividad de la implementación y formulará los planes de mejora a que haya lugar, cuando se identifiquen desviaciones en su cumplimiento.

6 MARCO NORMATIVO

- Ley Estatutaria 1581 (17 de octubre de 2012): "Por la cual se dictan disposiciones generales para la protección de datos personales."
- Ley 1266 (31 de diciembre de 2008): "Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones."
- Resolución 3564 de 2015 (31 de diciembre de 2015): Reglamenta aspectos relacionados con la Ley de Transparencia y Acceso a la Información Pública.
- Decreto 1078 (26 de mayo de 2015): "Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones."
- Ley 1712 (06 de marzo de 2014: Ley de Transparencia y acceso a la información pública nacional.
- Ley 57 (05 de julio de 1985): "Por la cual se ordena la publicidad de los actos y documentos oficiales."
- Acuerdo 03 (17 de febrero de 2015) del Archivo General de la Nación; "por el cual se establecen lineamientos electrónicos generados como resultado del uso de medios electrónicos de conformidad con lo establecido en el capítulo IV de

la ley 1437 de 2011, se reglamenta el artículo 21 de la ley 594 de 2000 y el capítulo IV del decreto 2669 de 2011"

- Decreto 019 de 2012: "Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública".
- Decreto 2364 (22 de noviembre de 2012): Firma electrónica.
- Ley 962 (08 de julio de 2005): "Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos."
- Decreto 1747 (11 de septiembre de 2000): "Por el cual se reglamenta parcialmente la ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales"
- Ley 527 (18 de agosto de 1999): Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y Se establecen las entidades de certificación y se dictan otras disposiciones.
- Decreto Ley 2150 de (05 de diciembre de 1995): "Por el cual se suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública."
- Decreto 1078 (26 de mayo de 2015): "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones"

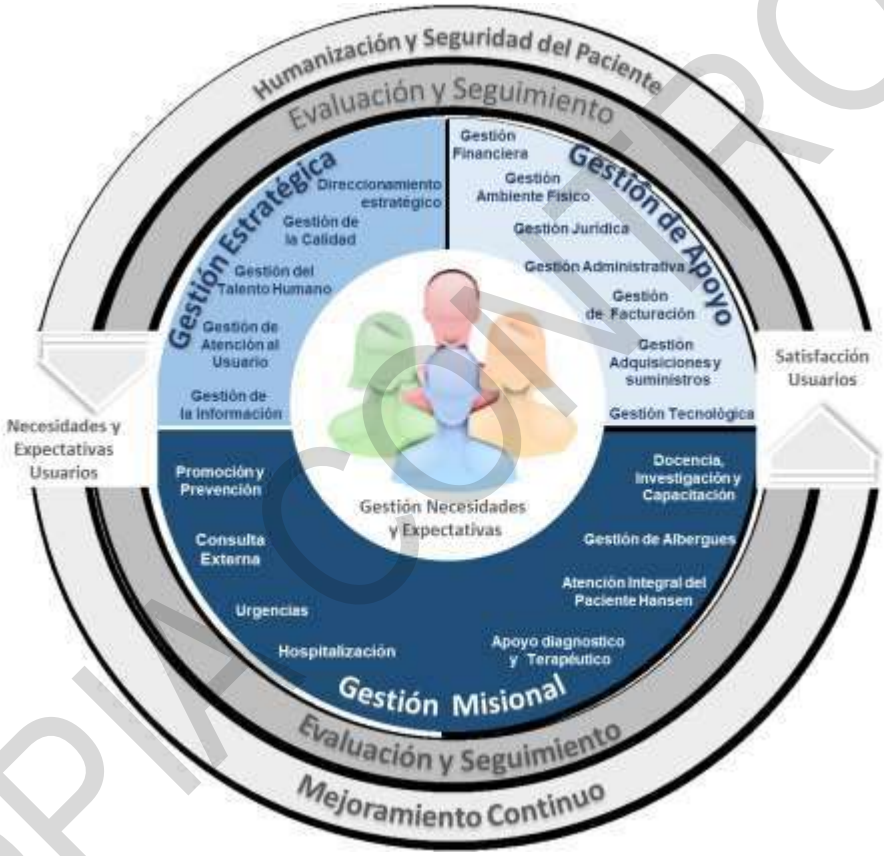
7 DEFINICIONES

- **Riesgo:** situación vulnerable a la que no se está exento que puede ocasionar pérdida o daños en diferente magnitud en la información de una entidad.
- **Riesgo Inherente:** Nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.
- **Riesgo Residual:** Nivel de riesgo que permanece tras el tratamiento del mismo o nivel resultante del riesgo después de aplicar los controles.
- **Seguridad de la información:** Preservación de la confidencialidad, integridad y disponibilidad de la información.
- **Activo de información:** información que tenga valor para la organización.
- **Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.
- **Análisis de Riesgo:** Proceso para formular recomendaciones o respuestas ante un nivel de riesgo.
- **Gestión del riesgo:** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, se compone de la evaluación y el tratamiento de riesgos.
- **SGSI:** Sistema de Gestión de Seguridad de la Información.
- **Plan de tratamiento de riesgos:** Documento que estipula las diferentes acciones para gestionar los riesgos de seguridad de la información inaceptables e instituir los controles necesarios para proteger la misma.

8 DIAGNÓSTICO SITUACIONAL

8.1 Roles y responsabilidades

La estructura organizacional de los procesos responsables de la realización del plan de Riesgos de Seguridad y Privacidad es la siguiente:



8.2 Descripción Del Plan

Inicialmente se hace una breve descripción de los activos informáticos con que cuenta el Sanatorio de Agua de Dios ESE, con el fin de reconocer el tipo de información y su clasificación.

Para cada una de las amenazas se analiza las vulnerabilidades (debilidades) que se podrían presentar en el proceso.

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

Finalmente se describen acciones que se deben llevar a cabo para solucionar las problemáticas presentadas.

8.2.1 Identificación De Activos De La Información

Los activos de información se clasifican en dos tipos:

8.2.1.1 Primarios:

Procesos o subprocesos y actividades de la entidad: procesos cuya pérdida o degradación hacen imposible llevar a cabo la misión de la organización:

- Información del área de Facturación, Inventarios, Financiera e historias clínicas.
- Información: información 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; información de alto costo

cuya recolección, almacenamiento, procesamiento y transmisión exigen un largo periodo de tiempo.

- Información del área de tesorería, presupuesto y contabilidad.
- Información del área de contratación.
- Información de talento humano.
- Inventarios del área de farmacia.
- Inventarios área de almacén.
- Actividades y procesos de negocio: 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.
- Información del área de tesorería.
- Información del área de contratación.
- Información de procesos jurídicos de la entidad.

8.2.1.2 De Soporte

Hardware: Consta de todos los elementos físicos que dan soporte a los procesos.

- 142 computadores de escritorio.
- 2 servidores de dominio.
- 1 servidor VoIP.
- 1 servidor del sistema de Gestión documental ORFEO.
- 1 Servidor Aplicación Novasoft
- 2 servidores ERP institucional (Base de datos y Aplicaciones).
- 1 Servidor intranet
- 20 impresoras
- 1 XVR (Hospital), Sistema CCTV
- 3 NVRS sistema CCTV, Edificio carrasquilla y Albergues San Vicente y Ospina Pérez)
- 2 DVRS Sistema CCTV (Albergue Boyacá y San Vicente)

Software: Consiste en todos los programas que contribuyen al funcionamiento de un conjunto de procesamiento de datos.

- ERP Software integrado institucional Panacea.
- Synergia, costos Hospitalarios.
- Orfeo, Sistema de Gestión documental.
- Elastix, Servidor de telefonía.
- Digiturno, servidor Digiturno de los usuarios.
- Novasoft, nómina subsidios.
- Administrador de contenidos Joomla, intranet

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.)

La red interna esta discriminada así:

- Conexión de fibra óptica en topología anillo entre CARRASQUILLA - HOSPITAL HERRERA,ALBERGUE SAN VICENTE, CASA MEDICA, ALBERGUE OSPINA PEREZ y ALBERGUE BOYACA
- 4 SWITCH Capa 3, Ubicado en el DATACENTER EDIFICIO
- CARRASQUILLA, Albergue San Vicente, Albergue Boyacá y Hospital
- Herrera,
- 4 SWTICH de distribución ubicados en el DATA CENTER EDIFICIO CARRASQUILLA, Albergues Boyacá, San Vicente y Ospina Pérez.
- Sistema de cableado estructurado, DATA CENTER ubicado en el
- EDIFICIO CARRASQUILLA, sede administrativa de la entidad, y la red
- LAN que se distribuye en cada uno de los edificios interconectados.
- Cortafuegos CISCO, ubicado en el DATA CENTER Edificio Carrasquilla.

Personal: Consiste en todos los grupos de personas involucradas en el sistema de información (usuarios, personal de apoyo, responsables, etc.)

- Personal a cargo de elementos de cómputo de la institución.

8.2.1.3 Identificación de Riesgos

Tipología de riesgo

La identificación de amenazas de que posiblemente causen daños a la información que cuenta el Sanatorio de Agua de Dios E.S.E. se realiza a partir de herramientas importantes como:

- Entrevistas con coordinadores de oficinas.
- Análisis de vulnerabilidad física.
- Verificación Mensual de roles y perfiles en los sistemas de información.

Se realizo la identificación de riesgos de acuerdo con la guía de riesgos de DAFP, donde se establecieron los siguientes tipos:

Riesgo Estratégico: Está relacionado con la forma en que se administra la Entidad. El manejo del riesgo estratégico se enfoca en asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos y la definición de políticas.

Riesgo de Imagen: Es principalmente la percepción y la confianza que tiene la ciudadanía hacia la entidad.

Riesgo Operativo: Está relacionado con el funcionamiento y operatividad de los sistemas de información, la definición de los proceso, la estructura de la entidad y la articulación entre dependencias.

Riesgo Financiero: Se basa en el manejo de los recursos de la entidad que incluyen: la ejecución presupuestal, la elaboración de los estados

financieros, los pagos, manejo de excedentes de tesorería y el manejo sobre los bienes.

Riesgo de cumplimiento: Esta asociado con la capacidad de la entidad para dar cumplimiento a los requisitos legales, contractuales, éticos y en general con su compromiso ante la comunidad.

Riesgo de Tecnología: Se relaciona con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales, futuras y el cumplimiento de la misión.

El proceso de gestión de riesgo en la seguridad de la información consta de la definición del enfoque organizacional para la valoración del riesgo y su posterior tratamiento.

- Proceso para administración de riesgos:

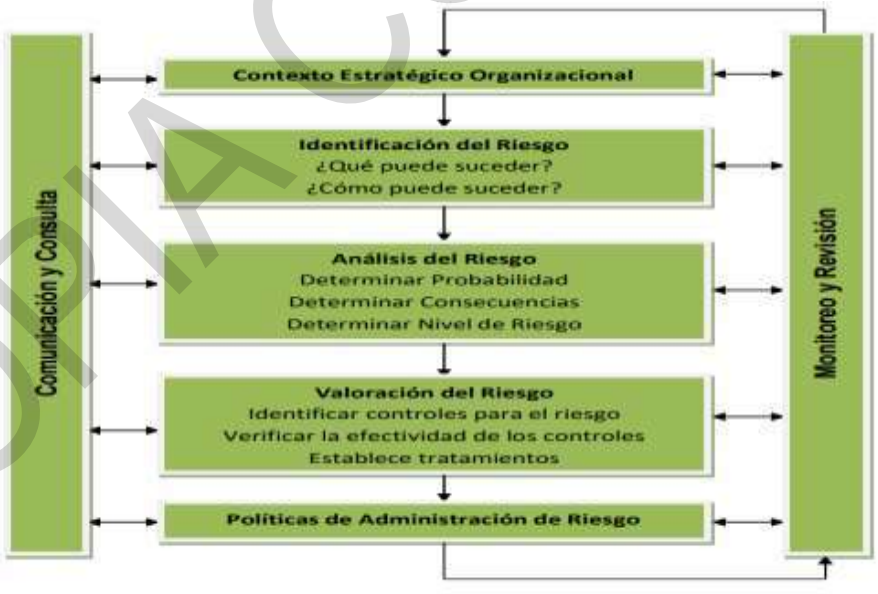


Imagen 1. Tomado de la Cartilla de Administración de Riesgos del DAFP

- Proceso para administración del riesgo en seguridad de la información:

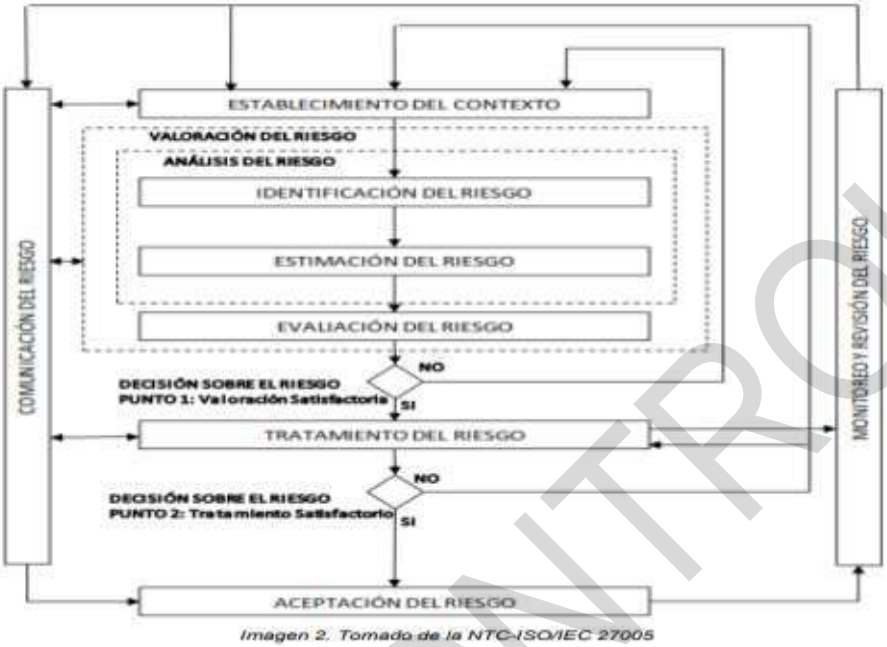


Imagen 2. Tomado de la NTC-ISO/IEC 27005

Descripción de las causas

Los riegos pueden generados por personas, procesos, equipos, tiempo, entre otras que provocan un mal uso, una inadecuada acción o mal trabajo como origen de un hecho ya sea positivo o negativo.

Consecuencias

Son los efectos asociados a la materialización del riesgo, estos pueden ser de diferente índole de acuerdo a la acción realizada y al perjuicio que se presente después de lo acontecido.

8.2.1.4 Análisis del Riesgo

Para ello se utilizará una escala cuantitativa de valoración donde uno (1) es el valor más bajo y cinco (5) más alto, ello con el fin proyectar una

comparación y priorización del riesgo de la información tanto en su seguridad como en la privacidad.

Probabilidad

Concepto	Descripción	Frecuencia	Valor
Raro	El evento puede ocurrir sólo en circunstancias	No se ha presentado en los últimos 5 años.	1
Improbable	Es muy poco factible que el evento se presente.	Al menos de 1 vez en los últimos 5 años.	2
Posible	El evento podría ocurrir en algún	Al menos de 1 vez en los últimos 2 años.	3
Probable	El evento probablemente ocurrirá en la mayoría de las	Al menos de 1 vez en el último año.	4
Casi certeza	Se espera que ocurra en la mayoría de las	Más de 1 vez al año.	5

Impacto

Concepto	Descripción	Valor
Insignificante	El acontecimiento puede ser controlado y las consecuencias son mínimas.	1
Menor	Tiene un bajo impacto, no afectando al proceso de información de la entidad.	2
Moderado	Si el hecho llega a presentarse tendría medianas consecuencias o efectos sobre la entidad.	3
Mayor	El impacto sería significativo y tendría altas consecuencias y/o efectos sobre la entidad.	4

Catastrófico	La materialización del riesgo imposibilita el cumplimiento de los objetivos de la Agencia, tiene un impacto y las	5

8.2.1.5 Evaluación del riesgo

Permite una comparación entre los riesgos que se presenta en la institución con el fin de discernir cuan peligrosos pueden ser, de tal forma que se tomen medidas para mitigar sus consecuencias.

Concepto	Descripción	Valor
Zona de riesgo baja	El acontecimiento puede ser controlado y las consecuencias son mínimas.	B
Zona de riego moderada.	Tiene un bajo impacto, no afectando al proceso de información de la entidad.	M
Zona de riego alta	Si el hecho llega a presentarse tendría medianas consecuencias o efectos sobre la entidad.	A
Zona de riesgo extrema	El impacto sería significativo y tendría altas consecuencias y/o efectos sobre la entidad.	E

8.2.1.6 Responsable

Es la persona encargada y responsable de tomar medidas para dar solución a las circunstancias presentadas ya sea en mediano, corto o largo plazo, con el fin de remitir respuesta y dar solución a los eventos presentados.

8.3 Interpretación del Plan

El resultado de esta fase se concreta en un plan de tratamiento de riesgos, que nos permite entender como la información generada por el Sanatorio de Agua de Dios E.S.E. se encuentra expuesta a eventos adversos especialmente provocados por prácticas inadecuadas del personal de la entidad y falta de dotación de equipos

idóneos para cumplirlas, hecho que ponen en riesgo el cumplimiento de la misión encaminada a satisfacer las necesidades y expectativas de sus clientes bajo los principios de responsabilidad, rentabilidad económica y social, por tanto es conveniente que las partes responsables, en este caso la gerente general encamine medidas para solventar la problemática presentada y disminuir la exposición al riesgo en al que la información se ve expuesta, con medidas correctivas, precautorias y de mejora.

En cuanto a la privacidad de la información la entidad cumple este requisito protegiendo sus datos, dando acceso únicamente a personal autorizado y a personas externas únicamente cuando hacen la solicitud formal y realizan los tramites respectivos, ello en cumplimiento a lo estipulado en el Código de Integridad y "Código de Buen Gobierno 2016" en los artículos mencionados a continuación: "Artículo 20. Compromiso de Confidencialidad. El Sanatorio de Agua de Dios E.S.E., Se compromete a que los servidores públicos que manejan información privilegiada firmen acuerdos de confidencialidad para que se asegure que la información que es reserva de la institución no sea publicada o conocida a terceros. Quienes incumplan estos acuerdos o compromisos de confidencialidad serán sancionados de acuerdo con las leyes colombianas que sancionan este tipo de delitos. Con este fin se adoptarán mecanismos para que la información llegue a sus grupos de información de manera integral, oportuna, actualizada, clara y veraz y por el cual se adoptaran los mecanismos de información a los cuales haya acceso, de acuerdo con las condiciones de la comunidad a la que va dirigida."

También es de tener en cuenta que el desarrollo de las actividades estará sujeto a la disponibilidad de recursos (humanos, técnicos, tecnológicos, financieros) que faciliten el cumplimiento de las actividades; de acuerdo con la disponibilidad presupuestal oportuna, al apetito de riesgo institucional y a las orientaciones de la alta dirección, en cuanto al apetito de riesgo corporativo que han adoptado para afrontar el desarrollo y cumplimiento de las actividades planificadas

8.4 Plan de tratamiento de riesgos de seguridad y privacidad de activos de tecnologías de información por categorías frente a ciberamenazas.

Según lo expuesto en la guía para la administración del riesgo y el diseño de controles en entidades públicas por el DAFP Departamento Administrativo de la Función Pública, el tratamiento de riesgos es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos, por lo tanto dicha planeación en este caso en particular, hace alusión al tratamiento de riesgos de seguridad y privacidad de la información enfocado en la seguridad informática sobre los activos de tecnologías de información frente a amenazas cibernéticas, para lo cual se realizan actividades durante la vigencia orientadas a implementar los controles requeridos y priorizados.

9 REFERENCIAS

Tomada cartilla de administración del riesgo DAFP, https://www1.funcionpublica.gov.co/documents/418537/506911/1592.pdf/73e5a159-2d8f-41aa-8182-eb99e8c4f3ba

Tomada de la NTC-ISO/IEC 27005, https://www.iso.org/es/contents/data/standard/08/05/80585.html

10 APROBACIÓN

ELABORÓ	REVISÓ	APROBÓ	GESTIÓN DOCUMENTAL
GERXON MAURICIO ESPINOSA SATIVA Ingeniero de Sistemas	CESAR MAURICIO UBAQUE TELLEZ Coordinador GIT Planeación, Gestión Documental y TIC'S EDGAR ANGELICO GAMBOA MUR Supervisor Grado 23 Comité Institucional de Gestión y Desempeño Acta 001 de 2026	ANTONIO RUIZ FLÓREZ Gerente	CESAR MAURICIO UBAQUE TELLEZ Coordinador GIT Planeación, Gestión Documental y TIC'S
FECHA	FECHA	FECHA	FECHA
20/01/2026	20/01/2026	20/01/2026	20/01/2026

11 CONTROL DE CAMBIOS

TIPO DE MODIFICACIÓN	DESCRIPCIÓN DEL CAMBIO	RESPONSABLE	FECHA DEL CAMBIO	VERSIÓN
CREACIÓN	Creación del documento	EDGAR ANGÉLICO GAMBOA MUR	29/01/2025	01
ACTUALIZACIÓN	Actualización de documento	GERXON MAURICIO ESPINOSA SATIVA	20/01/2026	02

FECHA DE APROBACIÓN: 20/01/2026