PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2023
SANATORIO DE AGUA DE DIOS E.S.E.

ANA MILENA MONTES CRUZ

GERENTE (E)

ADRIANA MARÌA CHÀVEZ GALEANO
Coordinador Grupo Interno Trabajo Administrativo

HERNAN AGUDELO SÁNCHEZ
Coordinador Grupo Interno de Trabajo Financiero con función de Control Interno

OSWALDO SARMIENTO RINCON
Profesional de apoyo Control Interno

EDGAR ANGELICO GAMBOA MUR
Coordinador Grupo Interno de Trabajo Planeación, G. Documental y TICS

KARINA GARCIA VILLAMIZAR
Profesional de apoyo GIT de Planeación, G. Documental y TICS

CAROLINA CARLOS PLATA.
Coordinadora Grupo Interno Trabajo Asistencial

GLORIA ESMERALDA ALVAREZ GARCIA
Responsable Atención al Usuario

FREDY YAMID DIAZ TRIANA
Coordinadora Grupo Interno Trabajo Talento Humano

En colaboración con
Coordinadores de Grupos Internos de Trabajo y responsables de áreas

1. INTRODUCCIÓN.

Para el Sanatorio de Agua de Dios E.S.E. los activos de la información son parte fundamental para el apoyo en una atención integral a los usuarios que acceden a cada uno de los servicios ofrecidos por la entidad, es por ello que salvaguardar la información y cumplir con todo lo establecido en el marco del Modelo de Seguridad y privacidad de la información propuesto por el Ministerio de las Tecnologías de la información y las comunicaciones MINTIC.

De acuerdo con la política de Gobierno Digital liderada por el MINTIC, que impulsa los servicios centrados en el ciudadano a través de las TIC, quienes permiten mayor cobertura y realizar consultas y transacciones en menos tiempo y desde cualquier lugar, para ello los datos que viajan por las diferentes herramientas requieren ser protegidos y controlados para ofrecer confianza en el uso de dichas herramientas, para ello las entidades deben establecer diferentes mecanismos como procesos y procedimientos que le permitan regular el manejo y uso de la información que recolecta de terceros.

Para ofrecer una mejora continua el plan de seguridad y privacidad de la información requiere marcar un camino en su implementación guiado por las diferentes normas, estatutos y leyes que reglamenten el sector y que garanticen la estabilidad la transparencia y el acceso a la información pública.

Las entidades deben contar con un responsable de la información que tenga la capacidad de vigilar que la información custodiada por la entidad este seguro sin importar el medio en el que repose, para esto el Sanatorio de Agua de Dios E.S.E trabajara en el fortalecimiento e implementación del modelo de seguridad y privacidad de la información.

Carrera 9 No. 10- 69 – Edificio Carrasquilla - Agua de Dios –Cundinamarca Colombia. Nit 890.680.014-9
Tel. (57) 8345000 Ext 1101 Fax: (57) 8342677 - E.mail: gerencia@sanatorioaguadedios.gov.co - www.sanatorioaguadedios.gov.co

2. OBJETIVOS Y ALCANCE.

2.1 OBJETIVO GENERAL

Establecer los lineamientos principales de gobierno y gestión de la seguridad y privacidad de la información para el Sanatorio de Agua de Dios E.S.E.

2.2 OBJETIVOS ESPECIFÍCOS

- Continuar con las fases de implementación del sistema de seguridad y privacidad de la información.
- Definir estrategias para mitigar los riesgos expuestos en el mapa de riesgos de la entidad.
- Contribuir con la implementación de la política de Gobierno Digital.

2.3. ALCANCE.

El plan contempla la estructura de gobierno y los lineamientos principales para la seguridad y privacidad de la información en el Sanatorio de Agua de Dios E.S.E. lo aquí definido debe ser conocidos y cumplidos por todos los servidores públicos, contratistas y todos los terceros que tengan acceso, almacenen, procesen o trasmitan información de la institución o sus usuarios.

3. DEFINICIONES Y NORMATIVIDAD RELACIONADA

3.1. DEFINICIONES.

Acceso a la Información Pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

Activo de Información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

Análisis del impacto al negocio (BIA por sus siglas en inglés). Proceso del análisis de actividades las funciones operacionales y el efecto que una interrupción del negocio podría tener sobre ellas.

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3).

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Confidencialidad: La propiedad que esa información esté disponible y no sea divulgada a personas o procesos no autorizados.

Datos Personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

Datos Personales Públicos: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art3)

Datos Personales Privados: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)

Datos Personales Mixtos: Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.

Datos Personales Sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3)

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

Carrera 9 No. 10- 69 – Edificio Carrasquilla - Agua de Dios –Cundinamarca Colombia. Nit 890.680.014-9
Tel. (57) 8345000 Ext 1101 Fax: (57) 8342677 - E.mail: gerencia@sanatorioaguadedios.gov.co - www.sanatorioaguadedios.gov.co

Derecho a la Intimidad: Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

Disponibilidad: La propiedad de estar disponible y utilizable cuando lo requiera una entidad autorizada.

Encargado del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento. (Ley 1581 de 2012, art 3)

Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

Información Pública Clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

Información Pública Reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

Información Pública: Es aquella información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad.
Integridad: La propiedad de salvaguardar la exactitud e integridad de los activos de información.

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

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

Mecanismos de protección de datos personales: Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, cifrado etc.

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

Privacidad: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Seguridad de la información: Son todos los controles técnicos y metodológicos que permiten mitigar los riesgos a los que se expone la información.

Sistema de Gestión de Seguridad de la Información SGSI: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

Tecnología de la Información: (TI) Es el estudio, diseño, desarrollo, implementación, soporte y administración de los sistemas de información basados en computadoras, particularmente aplicaciones de software y hardware de computadoras".

Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

Vulnerabilidad: Son la capacidad, las condiciones y características del sistema mismo (incluyendo la entidad que lo maneja), que lo hace susceptible a amenazas, con el resultado de sufrir algún daño.

3.2. NORMATIVIDAD RELACIONADA.

- Constitución Política de Colombia.
- Ley 489 de 1998.
- Ley Estatutaria 1266 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”.
- Ley 1273 de 2009, "Protección de la Información y de los datos”
- Ley 1581 de 2012, "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”
- Decreto 943 de 2014.

Carrera 9 No. 10- 69 – Edificio Carrasquilla - Agua de Dios –Cundinamarca Colombia. Nit 890.680.014-9
Tel. (57) 8345000 Ext 1101 Fax: (57) 8342677 - E.mail: gerencia@sanatorioaguadedios.gov.co - www.sanatorioaguadedios.gov.co

- Decreto Único Reglamentario 1078 de 2015 "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las comunicaciones"
- Decreto 1008 de 2018.
- ISO/IEC 27001- Seguridad de la Información.
- ISO 31000 – Gestión de Riesgos.

4. ROLES Y RESPONSABILIDADES

4.1. COMPROMISO DE LA DIRECCIÓN

La Junta Directiva y el Gerente del Sanatorio de Agua de Dios E.S.E. muestra su compromiso y apoyo en el diseño, implementación y mantenimiento del Sistema de Gestión de Seguridad y Privacidad de la Información a través de la asignación de recursos, la definición de la política de información, los lineamientos de seguridad y el establecimiento del Gobierno de seguridad, cuya conformación y responsabilidades se describen a continuación.

4.2 GOBIERNO DE SEGURIDAD

La definición de un modelo de gobierno de seguridad adecuado representado en una estructura organizacional definida y aprobada por la institución permite la correcta toma de decisiones y ofrece una alineación y rumbo adecuado en las actividades para proteger los activos de información.

Una estructura organizacional es un organismo viviente dentro de la organización que puede cambiar según la estructura y las necesidades de la institución pero que en todo momento debe ser clarificada con el fin de que se conozca la cadena de toma de decisión de cada uno de los temas necesarios para la gestión de la seguridad de la información.

Cada rol dentro del Gobierno debe tener unas responsabilidades asociadas para realizar su tarea, estas responsabilidades se asignan haciendo uso de una matriz RACI donde cada tipo de responsabilidad se asigna a los roles definidos. Los tipos de responsabilidades usados son los siguientes:

Descripción	
Responsable	Este rol corresponde a quien efectivamente realiza la tarea. Lo más habitual es que exista sólo un encargado (R) por cada tarea.

Quien rinde cuentas	Este rol se responsabiliza de que la tarea se realice y es quien debe rendir cuentas sobre su ejecución. Sólo puede existir una persona que deba rendir cuentas (A) de que la tarea sea ejecutada por su responsable (R).
Consultado	Este rol posee alguna información o capacidad necesaria para realizar la tarea. Se le informa y se le consulta información (comunicación bidireccional)
Informado	Este rol debe ser informado sobre el avance y los resultados de la ejecución de la tarea. A diferencia del consultado (C), la comunicación es unidireccional.

A continuación, se presenta la estructura de roles para el gobierno de seguridad de la información el Sanatorio de Agua de Dios E.S.E.

Carrera 9 No. 10- 69 – Edificio Carrasquilla - Agua de Dios –Cundinamarca Colombia. Nit 890.680.014-9
Tel. (57) 8345000 Ext 1101 Fax: (57) 8342677 - E.mail: gerencia@sanatorioaguadedios.gov.co - www.sanatorioaguadedios.gov.co

Estructura de roles

Rol	Objetivo
Comité Institucional de gestión y desempeño	• Tomar las responsabilidades en el Sanatorio de Agua de Dios E.S.E. de lo relacionado con seguridad de la información. • Realizar la aprobación de lineamientos estratégicos en cuanto a seguridad de la información, garantiza los recursos y la toma de decisiones orientadas al cumplimiento de la estrategia por ellos definida. • Supervisar la aplicación de los requisitos definidos por gobierno en línea en lo relacionado con la seguridad de la información.
Oficial de seguridad de la información	• Tiene la responsabilidad de guiar y realizar el seguimiento de la implementación de los planes de seguridad definidos.
Administrador de seguridad de la información	• Tienen la responsabilidad de la gestión de los esfuerzos de seguridad de la información, encargado de labores específicas de seguridad.
Líderes y/o responsables de procesos	• Tienen la responsabilidad de dar la cobertura de los lineamientos de seguridad a cada uno de sus procesos operacionales.
Responsable de Sistemas	• Responsable de aplicar los controles y las iniciativas de seguridad de tipo tecnológico definidas en el comité.
Coordinador GIT Talento Humano	• Responsable de aplicar las iniciativas de seguridad concernientes a la vinculación, mantenimiento y retiro o cambio de personal.
Responsable de Archivo	• Responsable de definir el manejo de la información a nivel documental que se maneja en toda la institución.
Coordinador GIT Asistencial y/o responsable de calidad	• Apoya la definición de lineamientos de seguridad para las áreas asistenciales aportando su conocimiento en pro de evitar en mayor medida los impactos operacionales. • Debe tener una comprensión de los riesgos de las áreas asistenciales en cuanto al manejo de la información y sobre los requisitos específicos de seguridad de la información aplicables al hospital.

4.2.1 COMUNICACIÓN CON EL GOBIERNO DE SEGURIDAD

Para que el gobierno de seguridad pueda cumplir con sus actividades y tomar las decisiones pertinentes según los acontecimientos en la entidad, se debe llevar la información necesaria. Dentro de la agenda de reunión el comité institucional de gestión y desempeño realizado para ese fin y debe recibir la siguiente información como mínimo:

- El estado de las acciones de las revisiones previas:
  - Seguimiento de las decisiones o actividades asignadas por el comité.
  - Solicitudes al comité para lograr el cumplimiento de las actividades designadas.
  - Resultados de las acciones finalmente implementadas.
- Cambios externos e internos que son relevantes para el sistema de gestión de seguridad de la información:
  - Cambios en regulaciones.
  - Cambios en ambiente físico y social.
  - Cambios de herramientas o infraestructura que soporta los procesos.
- Retroalimentación sobre el desempeño de la seguridad de la información, incluyendo las tendencias en:
  - Estado de los hallazgos de auditoría, las no conformidades y acciones correctivas.
  - Seguimiento y medición de las actividadesde seguridad desarrolladas.
- Retroalimentación de las partes interesadas:
  - o Resultados de encuestas de satisfacción de los cambios implementados.
- Resultados de la evaluación del riesgo y el estado del plan de tratamiento de riesgos.
- Las oportunidades o propuesta de mejora en temas relacionados con la seguridad de la información.

Las decisiones tomadas por el comité quedarán documentadas en la correspondiente acta de reunión, dentro de la cual para cada una de las decisiones tomadas se establecerá el responsable.

Las actas de comité deben incluir las decisiones relacionadas con las oportunidades de mejora continua y de cualquier necesidad de cambios en el sistema de gestión de seguridad de la información.

Carrera 9 No. 10- 69 – Edificio Carrasquilla - Agua de Dios –Cundinamarca Colombia. Nit 890.680.014-9
Tel. (57) 8345000 Ext 1101 Fax: (57) 8342677 - E.mail: gerencia@sanatorioaguadedios.gov.co - www.sanatorioaguadedios.gov.co

4.3.1 Estructura Del Plan De Seguridad Y Privacidad De La Información

El Sanatorio de Agua de Dios E.S.E. ha establecido el Plan de Seguridad y Privacidad de la Información de acuerdo con lo establecido en los manuales de implementación del Modelo de Seguridad y privacidad de la información para garantizar la Confidencialidad, Integridad y Disponibilidad de la Información presentados anteriormente, que permita cumplir con el objetivo definido en dicho plan, para esto se definen las actividades que se describen a continuación:

4.3.1. Fase de Diagnostico

En esta fase se pretende identificar el estado actual de la organización con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información. Para esta fase tenemos como metas:

Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad.
Determinar el nivel de madurez de los controles de seguridad de la información.
Identificar el avance de la implementación del ciclo de operación al interior de la entidad.
Identificar el nivel de cumplimiento con la legislación vigente relacionada con protección de datos personales.
Identificación del uso de buenas prácticas en ciberseguridad.
Realizar el diagnóstico de las condiciones en que se encuentran los activos de información administrados por la entidad.

Para ello, utilizaremos las siguientes herramientas publicadas en http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html:

- ✓ Herramienta de diagnostico
- ✓ Instructivo para el diligenciamiento de la herramienta
- ✓ Guía No 1 - Metodología de Pruebas de Efectividad.

4.3.2. Fase De Planificación

En esta fase se pretenderá cumplir con las siguientes metas:

ACTUALIZACIÓN DE POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. Se proyectará la Política de Seguridad y Privacidad de la información

Carrera 9 No. 10- 69 – Edificio Carrasquilla - Agua de Dios –Cundinamarca Colombia. Nit 890.680.014-9
Tel. (57) 8345000 Ext 1101 Fax: (57) 8342677 - E.mail: gerencia@sanatorioaguadedios.gov.co - www.sanatorioaguadedios.gov.co

que estará contenida en un documento de alto nivel que incluye la voluntad del comité de seguridad de la información del Sanatorio de Agua de Dios E.S.E. para apoyar la implementación del Modelo de Seguridad y Privacidad de la Información.

La política contendrá una declaración general por parte del comité de seguridad de información, donde se especifique sus objetivos, alcance, nivel de cumplimiento. La política será sometida a aprobación y será divulgada al interior de la entidad. Se tomará de base la Guía 2 – Política General MSPI del Modelo de Seguridad y privacidad de la Información de MinTic.

La actualización de la política debe realizarse al menos una vez al año o cuando se evidencie que nuevas amenazas pueden afectar la Seguridad de la Información en la entidad, todos los cambios que surtan en la política deben ser aprobados y socializados.

- **Políticas de seguridad y privacidad de la información.**

  Se desarrollará un manual de políticas, donde se describe los objetivos, alcances y el nivel de cumplimiento, que garanticen el adecuado uso de los Activos de información; definiendo las responsabilidades generales y específicas para la gestión de la seguridad de la información En el manual de políticas de la entidad, se debe explicar de manera general, las políticas, los principios de seguridad y la normatividad pertinente. El comité de seguridad de la información deberá evaluar los requerimientos necesarios para ser ajustados o desarrollados en la elaboración de las políticas de seguridad y privacidad, así como en la implementación.

- **Procedimientos de seguridad de la información.**

  Se desarrollarán y formalizarán los procedimientos que permitan gestionar la seguridad y privacidad de la información en cada uno de los procesos definidos en el mapa de procesos de la entidad.

  Para desarrollar esta actividad se tendrá como insumo, la Guía 3 - Procedimiento de Seguridad de la Información de MinTic.

- **Roles y responsabilidades de seguridad y privacidad de la información.**

  La entidad debe definir mediante un acto administrativo (Resolución) los roles y las responsabilidades de seguridad de la información en los diferentes niveles (Directivo, De procesos y Operativos) que permitan la correcta toma de decisiones y una adecuada gestión que permita el cumplimiento de los objetivos de la Entidad. Para desarrollar estas actividades, el punto de referencia será la Guía No 4 - Roles y responsabilidades de seguridad y privacidad de la información de MinTic.

- **Inventario De Activos De Información.**

  Realizar el Inventario de los activos de información por parte de cada proceso, siendo los procesos de Gestión de la información y Gestión Tecnológica quienes recopilan la información generando un solo documento con todos los activos de la entidad, con el fin de definir la criticidad, sus propietarios, custodios y usuarios.
  Para desarrollar estas actividades, el documento base será La Guía No 5 - Gestión De Activos de MinTic.

- **Identificación, Valoración Y Tratamiento De Riesgos.**

  El Sanatorio de Agua de Dios E.S.E. deberá definir una metodología de gestión del riesgo enfocada a procesos, que le permita identificar, evaluar, tratar y dar seguimiento a los riesgos de seguridad de la información a los que estén expuestos los activos, así como la declaración de aplicabilidad. Para conseguir una integración adecuada entre el MSPI y la guía de gestión del riesgo emitida por el DAFP respecto a este procedimiento, se emplearán los criterios de evaluación (impacto y probabilidad) y niveles de riesgo emitidos por la entidad.
  Para definir la metodología, la entidad hará uso de buenas prácticas vigentes tales como:

  ISO 27005, ISO 31000 y la Guía No 7 - Gestión de Riesgos emitida por el MinTIC.

  Para la elaboración del plan de tratamiento de riesgos y la declaración de aplicabilidad, utilizaremos la Guía No 8 - Controles de Seguridad de MinTic.

- **Plan De Comunicaciones.**

  La Entidad definirá un Plan de comunicación, sensibilización y capacitación que incluya la estrategia para que la seguridad y privacidad de la información se convierta en cultura organizacional, al generar competencias y hábitos en todos los niveles (directivos, funcionarios, terceros) del Sanatorio de Agua de Dios E.S.E.

Este plan será ejecutado, con el aval de la Gerencia, a todas las áreas de la entidad. Para estructurar dicho plan se utilizará la Guía No 14 – plan de comunicación, sensibilización y capacitación de MinTic.

- **Plan De Transición De Ipv4 A Ipv6.**

  Para llevar a cabo el proceso de transición de IPv4 a IPv6 en el Sanatorio de Agua de Dios E.S.E., se ejecutará la fase de planeación establecida en la Guía No 20 – Transición de IPv4 a IPv6 para Colombia que indica las actividades específicas a desarrollar.

4.3.3 Fase De Implementación

- **Planificación Y Control Operacional.**

  El Sanatorio de Agua de Dios E.S.E. deberá planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos de seguridad y privacidad de la información que permitan implementar las acciones determinadas en el plan de tratamiento de riesgos.

  El Sanatorio de Agua de Dios E.S.E. deberá tener información documentada en la medida necesaria para tener la confianza en que los procesos se han llevado a cabo según lo planificado, adicionalmente, deberá llevarse un control de cambios que le permitan tomar acciones para mitigar efectos adversos cuando sea necesario.

- **Implementación Del Plan De Tratamiento De Riesgos.**

  Se deberá implementar el plan de tratamiento de riesgos de seguridad de la información, en el cual se identifica el control a aplicar para llevar cada uno de los riesgos a un nivel aceptable para la entidad, en donde la base para ejecutar esta actividad es la Guía No 8 - de controles de seguridad y privacidad del MSPI de MinTic.

  Es preciso tener en cuenta que la aplicación del control sobre los riesgos detectados debe estar aprobados por el dueño de cada proceso.

- **Indicadores De Gestión.**

  El Sanatorio de Agua de Dios E.S.E. deberá definir indicadores que le permitan medir la efectividad, la eficiencia y la eficacia en la gestión y las acciones implementadas en seguridad de la información.

Los indicadores buscan medir:

- ✓ Efectividad en los controles.
- ✓ Eficiencia del MSPI al interior de la entidad.
- ✓ Proveer estados de seguridad que sirvan de guía en las revisiones y la mejora
- ✓ continua.
- ✓ Comunicar valores de seguridad al interior de la entidad.
- ✓ Servir como insumo al plan de control operacional.

La Guía No 9 - Indicadores de Gestión de MinTic, brinda información relacionada para poder llevar a cabo la realización de esta actividad.

- **Plan De Transición De Ipv4 A Ipv6.**

Se deberá generar el documento detallado con el plan de transición e implementación del protocolo IPv6 en la entidad.

Las guías de apoyo para esta labor son “Guía de Transición de IPv4 a IPv6 para Colombia” y “Guía de Aseguramiento del Protocolo IPv6”.

4.3.4 Fase de evaluación de desempeño

El proceso de seguimiento y monitoreo del MSPI se hace con base a los resultados que arrojan los indicadores de la seguridad de la información propuestos para verificación de la efectividad, la eficiencia y la eficacia de las acciones implementadas. Se deberán obtener dos documentos:

- **Plan de revisión y seguimiento a la implementación del MSPI.**

En esta actividad la entidad debe crear un plan que contemple las siguientes actividades:

- ✓ Revisión de la efectividad de los controles establecidos y su apoyo al cumplimiento de los objetivos de seguridad.
- ✓ Revisión de la evaluación de los niveles de riesgo y riesgo residual después de la aplicación de controles y medidas administrativas.
- ✓ Seguimiento a la programación y ejecución de las actividades de autorías internas y externas del MSPI.
- ✓ Seguimiento al alcance y a la implementación del MSPI.

Carrera 9 No. 10- 69 – Edificio Carrasquilla - Agua de Dios –Cundinamarca Colombia. Nit 890.680.014-9
Tel. (57) 8345000 Ext 1101 Fax: (57) 8342677 - E.mail: gerencia@sanatorioaguadedios.gov.co - www.sanatorioaguadedios.gov.co

- ✓ Seguimiento a los registros de acciones y eventos / incidentes que podrían tener impacto en la eficacia o desempeño de la seguridad de la información al interior de la entidad.
- ✓ Medición de los indicadores de gestión del MSPI
- ✓ Revisiones de acciones o planes de mejora (solo aplica en la segunda revisión del MSPI).

Este plan deberá permitir la consolidación de indicadores periódicamente y su evaluación frente a las metas esperadas; deben ser medibles permitiendo analizar causas de desviación y su impacto en el cumplimiento de las metas y objetivos del MSPI.

La Guía No 16 - Evaluación del Desempeño de MinTic, brinda información relacionada para poder llevar a cabo la realización de esta actividad.

- **Plan De Ejecución De Auditorias**

La entidad debe generar un documento donde se especifique el plan de auditorías para el MSPI, donde especifique la frecuencia, los métodos, las responsabilidades, los requisitos de planificación y la elaboración de informes. Se debe llevar a cabo auditorías y revisiones independientes a intervalos planificados que permitan identificar si el MSPI es conforme con los requisitos de la organización, está implementado adecuadamente y se mantiene de forma eficaz; así mismo es necesario difundir a las partes interesadas, los resultados de la ejecución de las auditorías.

Es importante conservar la información documentada como evidencia de los resultados de las auditorías.

La Guía No 15 - Guía de Auditoría de MinTic, brinda información relacionada para poder llevar a cabo la realización de esta actividad.

4.3.5 Fase De Mejora Continua

En esta fase la Entidad debe consolidar los resultados obtenidos de la fase de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, tomando las acciones oportunas para mitigar las debilidades identificadas.

5. Cronograma De Ejecución

Se establecerá un cronograma de ejecución aprobado por el comité de gestión y desempeño institucional el cual será antes proyectado por el comité de seguridad de la información.

Carrera 9 No. 10- 69 – Edificio Carrasquilla - Agua de Dios –Cundinamarca Colombia. Nit 890.680.014-9
Tel. (57) 8345000 Ext 1101 Fax: (57) 8342677 - E.mail: gerencia@sanatorioaguadedios.gov.co - www.sanatorioaguadedios.gov.co