PLAN DE TRATAMIENTO DE RIESGOS Y SEGUIRIDAD DE LA INFORMACION

SGSI
SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION

UNIDAD FUNCIONAL SISTEMAS DE INFORMACION, ESTADISTICA Y GESTION DOCUMENTAL

Santiago de Cali - 2022

Tabla de contenido

INTRODUCCION

El Hospital desde el año 2015 inicio su proceso de implementación gradual de los componentes de seguridad de la información y largo de estos años se fortaleció con elementos físicos de ti que deben acompañar la política de seguridad, nombrando el siso, u oficial de seguridad, socializando la política y cerrando las brechas en los controles implementados, la implementación del modelo de privacidad y seguridad de la información en el Hospital Departamental Mario Correa Rengifo se establece con conjunto de actividades basado en el ciclo PHVA (Planificar-Hacer-Verificar-Actuar) para crear condiciones de uso confiable en el entorno digital y físico de la información, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información las metodologías utilizadas para valorar la madurez de la seguridad en el Hospital son basado en la Norma Técnica Colombiana ISO27001:2013 y la autoevaluación MSAT de Microsoft.

La madurez de la seguridad incluye los controles (tanto físicos como técnicos), la Competencia técnica de los recursos informáticos, las directivas, los procesos y las prácticas sostenibles. La madurez de la seguridad se puede medir únicamente a través de la capacidad de la empresa para utilizar de forma eficaz las herramientas disponibles de forma que se cree un nivel de seguridad sostenible a lo largo de muchas disciplinas. Debe establecerse una línea de partida de la madurez de la seguridad y usarse para definir las áreas en las que centrar los programas de seguridad de la empresa. No todas las empresas deben esforzarse por alcanzar el nivel óptimo, pero todas deben evaluar en qué punto se encuentran y determinar el lugar que deberían ocupar en vista de los riesgos comerciales a los que se enfrentan. Por ejemplo, puede que una empresa con un entorno de bajo riesgo no necesite nunca subir encima del límite superior del nivel básico o el límite inferior del nivel estándar. Las empresas con un entorno de alto riesgo probablemente entren de lleno en el nivel optimizado. Los resultados del perfil de riesgos para la empresa le permiten hacer un balance de los riesgos.

Este documento contiene objetivos, generalidades, contexto, alcance, contexto normativo, definiciones, metodología de implementación y mapa de ruta con las actividades a ejecutar con sus correspondientes fechas y responsables.

Se define para el 2021, siguiendo los lineamientos de MINTIC quien adopta la norma ISO27000 con frameford de gestión de seguridad de la información para implementar en las organizaciones del estado, con base en estos lineamientos se aprueba en enero del 2022 el plan de tratamiento a riesgos de seguridad de la información donde se definen 4 fases y 7 etapas para ejecutar para la implementación de las buenas prácticas de seguridad de la información, 7 etapas (1. SGSI como un proyecto transversal a la organización, 2.-

inventario de activos, 3.- levantamiento e identificación de riesgos, 4.-implementacion de controles y requisitos de la iso 27002, 5.- pruebas de la seguridad de la información, 6.- capacitacion y socialización. 7 mantenimientos y actualizaciones, por ser una norma ISO con una puesta en marcha largo plazo se define una metodología para gestionar el indicador que evalué la implementación y se realiza de acuerdo a madurez de controles de CMM que referir a: Capability Maturity Model), quien define una metodología evaluar el modelo basados en la madurez con las siguientes variables, Inexistente, Inicial / Ad-hoc,Reproducible, pero intuitivo, Proceso definido, Gestionado y medible y Optimizado, la evuacion se realiza sobre los 114 controles del sistema de gestiona de seguridad de la información y se evalúan los procesos definidos, donde los procesos definidos evidencian proceso de adherencia al uso de las buenas practicas de gestiona de la seguridad de la información en la ESE

RESEÑA HISTORICA

El Hospital es una institución de Nivel II de complejidad, de carácter público Departamental, creado desde 1.972 para atender a la población de escasos recursos económicos del Municipio de Cali - Colombia, ubicado en el barrio Mario Correa de la Comuna 18. Inicialmente funciona como un centro de atención para la tuberculosis y con el correr del tiempo, el Hospital sufrió muchos cambios a su interior, con la apertura progresiva de nuevos servicios asistenciales, fortaleciendo su recurso humano y tecnológico, para satisfacer la demanda creciente, especialmente en servicios como urgencias, cirugía y hospitalización. En los años 80 el hospital genera una expansión de sus servicios asistenciales y se construyen nuevas áreas administrativas y para la atención de pacientes en Urgencias, Pediatría y Pensionados. El hospital entonces se constituye en pieza clave y protagónica de la red de prestadores de servicios de salud de Cali y el Valle del Cauca. Adecuándose a la Ley de Seguridad Social en Salud, las directivas de la entidad, tomaron la decisión de reorganizar y modernizar cada uno de los servicios asistenciales y de apoyo administrativo, con el fin de convertir la entidad, en una Institución Prestadora de Servicios (IPS) fundamentado en los principios de calidad y eficiencia. En el año de 1995 se convierte en Empresa Social del Estado descentralizada (Decreto 1808 del 7 de noviembre de 1995), con autonomía administrativa y patrimonio propio.

UBICACIÓN

La ESE Hospital Mario Correa Rengifo, está ubicado en la comuna 18 de la ciudad Santiago de Cali, más específicamente en la carrera 78 Oeste No. 2ª -00, teniendo como área de influencia las comunas 1, 3, 9, 17, 18,19, 20 y corregimientos aledaños como la Buitrera y Pance y demás que colindan con el occidente de Cali.

MISION

Somos una institución prestadora de servicios de salud de mediana complejidad, que brinda una atención oportuna, humanizada, segura e incluyente, para nuestros usuarios y clientes, con talento humano calificado y comprometido con el mejoramiento continuo.

VISION

Para el año 2024 seremos una institución acreditada, reconocida por la prestación de servicios de salud con énfasis quirúrgico, apoyada con una adecuada tecnología y una cultura organizacional humanizada, sostenible y amigable con el medio ambiente.

OBJETIVO GENERAL

Implementar el SGSI Sistema de Seguridad de la Información en Hospital Departamental Mario Correa Rengifo ESE, para lograr la preservación de la confidencialidad, disponibilidad e integridad de la información, estableciendo un esquema de seguridad bajo la gestión del riesgo.

Objetivos específicos

Actualizar los activos de información de la entidad e operación y técnicos y su criticidad en relación de integridad, confidencialidad y disponibilidad de la información en el 2021

Identificar en el 2021 los riesgos en los procesos del Hospital, que puedan afectar la integridad, confidencialidad y disponibilidad de la información.

Atender de manera adecuada con el oficial de seguridad del Hospital los incidentes de seguridad de la información que afecte la integridad, confidencialidad y disponibilidad de la misma durante el año.

4. Cumplir la normatividad legal vigente de transparencia y derecho de acceso a la información pública nacional, la estrategia de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones - Min TIC, la norma ISO 27001:2013, la Ley estatutaria de protección de datos personales (Ley 1581 de 2012) y sus decretos reglamentarios y las normas que las modifiquen, adicionen o sustituyan.

5. Realizar campaña de cultura en seguridad y privacidad de la información en el año 2021, socialización de la política de seguridad y acuerdo de confidencialidad para los funcionarios, contratistas, terceros, aprendices, practicantes y proveedores.

LA POLÍTICA DE SEGURIDAD DE INFORMACIÓN DEL HOSPITAL

La Gerencia del Hospital Departamental Mario Correa Rengifo Ese, está comprometida con la preservación de la confidencialidad, disponibilidad e integridad de la información de la institución y con el apoyo de la Unidad Funcional de Sistemas de Información, supervisara la protección de los bienes de la información contra uso, modificación, acceso o destrucción no autorizada

El comité de seguridad de la información definirá la estrategia para la implementación y administración el SGSI dentro del HMCR, definirá acuerdos de confidencialidad en la contratación interna (colaboradores) y externa (servicios), delegará roles y responsabilidades a sus colaboradores frente a la seguridad de la información.

El comité de seguridad de la información desarrollara mecanismos que permitan la adecuada identificación y clasificación de los activos de la información conociendo su propietario, ubicación y criticidad dentro de la institución, para gestionar su adecuada protección.

DECLARATORIA DE LA POLÍTICA GENERAL DEL MANEJO DE LA INFORMACIÓN

La información interna y externa manejada en el Hospital Departamental Mario Correa Rengifo ESE, es identificada de acuerdo a las necesidades de los diferentes procesos, siendo tratada con el debido control y seguimiento, garantizando que al interior de la institución fluya de manera oportuna, segura, accesible y confidencial, constituyéndose en un instrumento válido para la toma de decisiones gerenciales.

ALCANCE

La política debe ser cumplida por los miembros de la institución: funcionarios, Contratistas, Proveedores, clientes y/o visitantes, que utilicen información generada a través de un aplicativo, transmitida por redes, en medio magnético o medio impreso

ACUERDO DE CONFIDENCIALIDAD

Las partes se obligan mutuamente a guardar la confidencialidad y reserva de los secretos que conozcan con motivo de las conversaciones precontractuales y las subsiguientes que llevaron a la celebración de este contrato y a no divulgar, ceder, prestar, revelar, vender, usar, disertar, publicar o autorizar revelar a persona alguna ninguna información confidencial ni información alguna de propiedad de la otra parte, bajo ninguna modalidad, incluyendo la información que a partir de la fecha reciban. Devolver toda la información suministrada por la otra parte tan pronto como termine la labor encomendada o en el momento en que sea solicitada. Mantener en estricta reserva toda información que en razón de este contrato reciba de manera directa o indirecta, en forma verbal, escrita, gráfica, en medio magnético o bajo cualquier otra forma o modalidad, tomando todas las medidas necesarias para que la información no llegue por ningún motivo a manos de terceros bajo ninguna circunstancia y utilizarla únicamente para adelantar las tareas que se deriven directamente del cumplimiento del presente contrato

POLITICA GOBIERNO DIGITAL

La Gerencia del Hospital Departamental Mario Correa Rengifo Ese, está comprometida con la preservación de la confidencialidad, disponibilidad e integridad de la información de la institución y con el apoyo de la Unidad Funcional de Sistemas de Información, supervisara la protección de los bienes de la información contra uso, modificación, acceso o destrucción no autorizada. La información interna y externa manejada en el Hospital Departamental Mario Correa Rengifo Ese, es identificada de acuerdo a las necesidades de los diferentes procesos, siendo tratada con el debido control y Seguimiento, garantizando que al interior de la institución fluya de manera oportuna, segura, accesible y confidencial, constituyéndose en un instrumento válido para la toma de decisiones gerenciales.

La Gerencia del Hospital Departamental Mario Correa Rengifo Ese, está comprometida con la promoción, uso y aprovechamiento de las tecnologías de información y comunicaciones generando entorno digital de confianza, que permita el Hospital Departamental Mario Correa

Rengifo Ese, transformarse en una empresa del sector salud, competitiva, proactiva e innovadora en la prestación de los servicios integrales de Salud a los ciudadanos.
Que tiene como objetivo "Promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital".

CONTEXTO ESTRATÉGICO

El presente plan está alineado y contribuye al logro de la misión, visión y mega y demás elementos del direccionamiento estratégico del Hospital, los cuales se estipulan en el Plan de desarrollo – vigente (2020-2023).

FORMULACION ESTRATEGICA 2020 – 2023 TRANVERSAL CON TI

PERSPECTIVAS	ESTRATEGIAS	OBJETIVOS RELACIONADOS TI
P2: Perspectiva Financiera:		
Eje estratégico 2: Fortalecimiento de la gestión financiera institucional (Modelo de gestión orientado desde políticas de sostenibilidad financiera y uso adecuado de los recursos)	**3. Fortalecimiento del proceso de proyección presupuestal de ingresos, realizando seguimiento a su comportamiento, la oportunidad y la veracidad de la información**	**X**
P3: Perspectiva clientes.		
Eje estratégico 3: Generar valor para nuestros clientes	**6. Ejecutar el programa de mantenimiento incluyendo los ajustes en la infraestructura y de renovación de tecnología dura que den respuesta a**	**X**

PERSPECTIVAS	ESTRATEGIAS	OBJETIVOS RELACIONADOS TI
	los requerimientos del sistema obligatorio.	
	9. Mejorar la experiencia del usuario mediante el fortalecimiento de la aplicación de las políticas de humanización, seguridad al paciente, gestión del riesgo y gestión del a tecnología, alineadas al modelo de prestación de salud enfocado en identificar las expectativas del usuario durante los procesos de atención	X
P5: Perspectiva aprendizaje:		
	15. Identificar expectativas institucionales para que sean resueltas a partir del cumplimiento de los lineamientos y normatividad planteadas por el gobierno digital y PETI.	X
	16.Implementar proyectos (Formalización de procesos) que faciliten la universalización de la Historia Clínica Sistematizada en el Valle y el empleo de las TICS para generar apoyos intra e interinstitucionales, a partir de la puesta en marcha de estrategias de Interoperabilidad	X

PERSPECTIVAS	ESTRATEGIAS	OBJETIVOS RELACIONADOS TI
	18. Promover la presentación de proyectos investigación e innovación como motor de desarrollo institucional.	**X**

ARTICULACION CON MIPG

Gestión y Desempeño Institucional - MIPG	Política Gobierno Digital Política de Seguridad Digital Política de Gestión Documental Política de Transparencia, acceso a la información pública y lucha contra la corrupción Gestión del conocimiento y la innovación

El 33% de los objetivos estratégicos del plan de desarrollo están relacionados con TI., razón a lo anterior evidencia que las estrategias de TI, tienen en un papel preponderante en el crecimiento y proyección de la organización.

ALCANCE

La implementación del SGSI Sistema de Gestión de Seguridad de la Información de los procesos del Hospital Departamental Mario Correa Rengifo ESE y donde exista recolección, procesamiento, almacenamiento, recuperación, intercambio y consulta de información, para el desarrollo de la misión institucional y cumplimiento de sus objetivos estratégicos y tiene como finalidad resguardar la información almacenada en los componentes informáticos de la institución y aplica específicamente a los datos sensibles del personal de la institución y los usuarios que utilizan los servicios del hospital.

CONTEXTO NORMATIVO

Ley 44 de 1993 "por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944." (Derechos de autor).

Ley 527 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".

Ley 1273 de 2009 "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones"

Ley 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales".

Ley 1712 de 2014 "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones".

Decisión Andina 351 de 2015 "Régimen común sobre derecho de autor y derechos conexos".
CONPES 3854 de 2016 – Política de Seguridad Digital del Estado Colombiano.

Decreto 1078 de 2015 modificado por el Decreto 1008 de 2018 - Política de Gobierno Digital que contiene el Modelo de Seguridad y Privacidad - MSPI de MINTIC.

Decreto 1499 de 2017, el cual modificó el Decreto 1083 de 2015 – Modelo Integrado de Planeación y Gestión.

Guía para la administración del riesgo y el diseño de controles en entidades públicas. RIESGOS DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL año 2018.

Norma Técnica Colombiana ISO27001:2013.

GLOSARIO

TERMINO	DEFINICION
Confidencialidad:	Propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.
AoAs	Áreas de análisis que son la infraestructura, las aplicaciones, operaciones, y la gente.
Disponibilidad:	Propiedad de ser accesible y utilizable a demanda por una entidad.
Estándar:	Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. En este documento se habla de las Norma Técnica Colombiana ISO27001
Gestión del riesgo:	Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.
Incidente de seguridad de la información:	Resultado de intentos intencionales o accidentales de romper las medidas de seguridad de la información impactando en la confidencialidad, integridad o disponibilidad de la información.
Información:	Es un conjunto organizado de datos, que constituyen un mensaje sobre un determinado ente o fenómeno. Indicación o evento llevado al conocimiento de una persona o de un grupo. Es posible crearla, mantenerla, conservarla y transmitirla
Integridad:	Propiedad de exactitud y completitud.
Aplicaciones	Software informático que proporciona funcionalidad al usuario final. Requiere la existencia de un sistema operativo en el que ejecutarse. Algunos ejemplos son los procesadores de texto, las hojas de cálculo o los programas de gestión de bases de datos.
Inventario de activos:	Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos
Política de seguridad de información:	Es el instrumento que adopta una entidad para definir las reglas de comportamiento aceptables en el uso y tratamiento de la información

TERMINO	DEFINICION
Antivirus (AV)	Software o tecnología de hardware que protege al entorno informático frente a cualquier software peligroso.
Perfil de riesgos para la empresa (BRP)	Medida del riesgo al que está expuesto una empresa, según el entorno empresarial y el sector en que compite.
Riesgo:	Es la posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos institucionales Se expresa en términos de probabilidad y consecuencias.
Riesgo de seguridad y privacidad:	Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización. Se mide en términos de probabilidad y consecuencias
Índice de defensa en profundidad (DiDl)	Medida de las defensas de seguridad utilizadas en el personal, los procesos y la tecnología para contribuir a reducir los riesgos identificados en una empresa.
Zona desmilitarizada (DMZ)	Parte de la red separada de la red interna mediante un cortafuego y conectada a Internet a través de otro cortafuego.
Servidor de seguridad (cortafuegos)	Dispositivo de hardware o software que ofrece protección a los equipos frente al acceso no autorizado a través de la red.
Infraestructura	Funcionalidad de red, así como su administración y mantenimiento para ofrecer compatibilidad con la defensa de red, respuesta frente a incidentes, disponibilidad de red y análisis de errores. Incluye compatibilidad con los procesos empresariales internos y externos, y acerca de cómo se crean e implementan los hosts.
Autenticación multifactor	Autenticación que requiere una combinación de al menos dos de los siguientes elementos: algo que se sabe; algo que se tiene; o algo propio del usuario. Por ejemplo, la tarjeta de débito de su banco es una autenticación de dos factores: requiere algo que tiene (la tarjeta) y algo que sabe (el número PIN). Solicitar a alguien que teclee múltiples contraseñas para la autenticación, supone una autenticación de un solo factor al tratarse únicamente de algo que sabe el usuario. Por lo general, cuantos más factores, más

TERMINO	DEFINICION
	segura es la autenticación. Así, un sistema que requiera una tarjeta identificativa (algo que posee), un PIN (algo que sabe) y una huella dactilar escaneada (algo propio) es más seguro que cualquier otro que únicamente solicite el nombre de usuario/contraseña (factor único) o una tarjeta de identidad y el PIN.
Operaciones	Los miembros de una empresa, así como las directivas, los procesos, los procedimientos y las prácticas que se relacionan con su protección y la de la empresa.
Personal	Los miembros de una empresa, así como las directivas, los procesos, los procedimientos y las prácticas que se relacionan con su protección y la de la empresa.
Infraestructura de clave pública (PKI)	Conjunto integrado de tecnologías necesario para proporcionar un cifrado por clave pública y firmas digitales. Utiliza una combinación de cifrado por clave pública y privada que ofrece gestión de claves e integridad y confidencialidad de los datos.
Proceso	Serie documentada de tareas secuenciales que se utiliza para realizar una función del negocio.

DESARROLLO DEL PLAN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

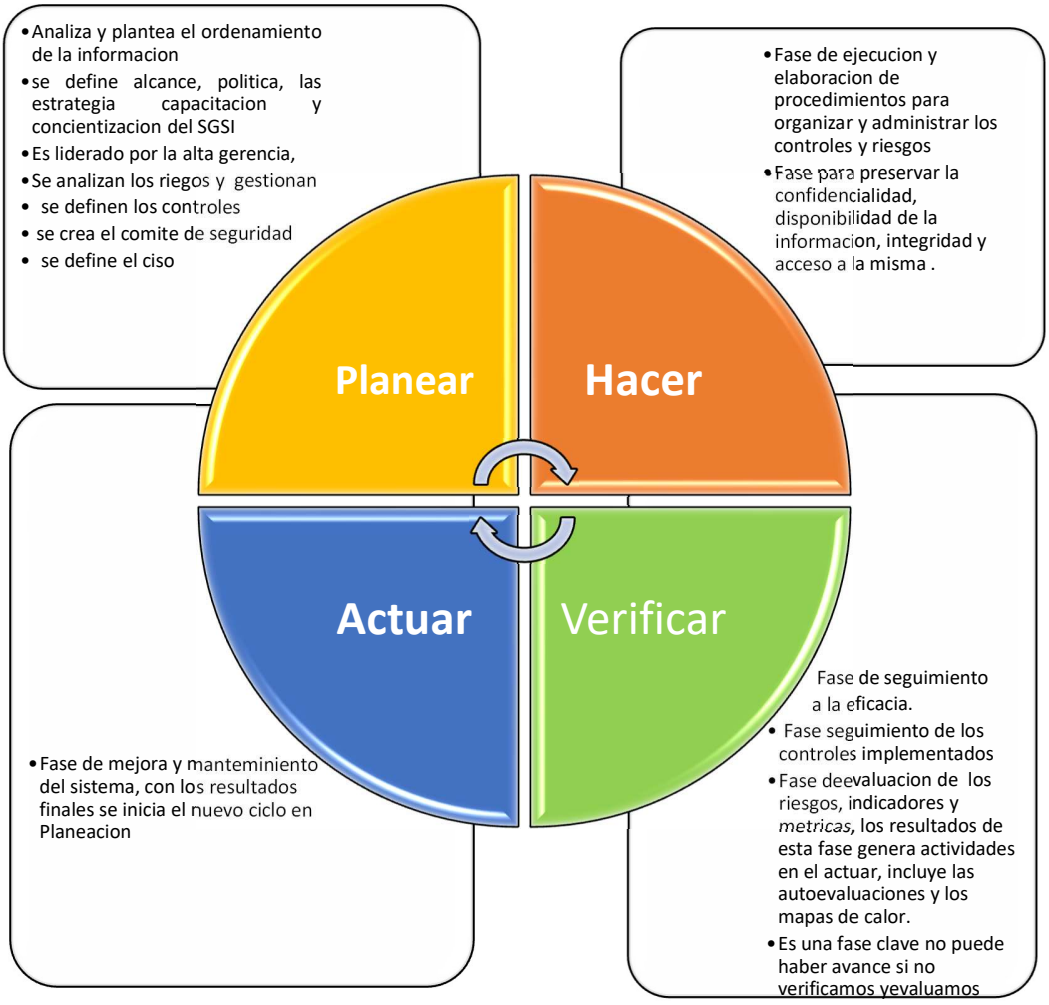
METODOLOGÍA DE IMPLEMENTACIÓN

La metodología de implementación del Plan de Seguridad y Privacidad para el Hospital Departamental Mario Correa Rengifo ESE, está basado en el ciclo PHVA (Planificar-Hacer-Verificar-Actuar) y lo establecido en el Modelo de Seguridad y Privacidad del Ministerio de Tecnologías de la Información y las Comunicaciones – Min TIC:

CICLO DEL SGSI SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION

El sistema de gestión de la seguridad de la información tiene un enfoque sistémico, se administra bajo el enfoque PHVA planear, hacer, verificar y actuar.

CICLO DEL SGSI



ACTIVIDADES REALIZADAS

Etapas previas a la implementación:

Estado actual de la entidad se identificó frente a la norma iso el estado actual Identificar el nivel de madurez se inició con un nivel de madurez del 18% en el 2019 Levantamiento de información se inició con el requerimiento de necesidades de ti relacionadas con infraestructura de seguridad firewall físico, licenciamiento antivirus, política de seguridad, comité de seguridad

Planificación:
Contexto de la entidad.
Liderazgo para implementar seguridad desde ti hacia las buenas practicas Planeación se conforma comité de seguridad de la información y se nombra siso Soporte se adopta iso27001 como estándar a seguir e implementar Inventario de activos 1era fase físicos y lógicos

Implementación:
Control y planeación operacional
Evaluación de riesgos de Seguridad y Privacidad de la Información
Tratamiento de Riesgos de Seguridad y Privacidad de la Información.
Evaluación de Desempeño:
Monitoreo, medición, análisis y evaluación.
Mejora continua:
Acciones correctivas y no conformidades

Pendiente por realizar:

Evaluación de Desempeño:
Revisión por la dirección
Mejora continua:
Auditoria interna
Inventario de Activos segunda fase

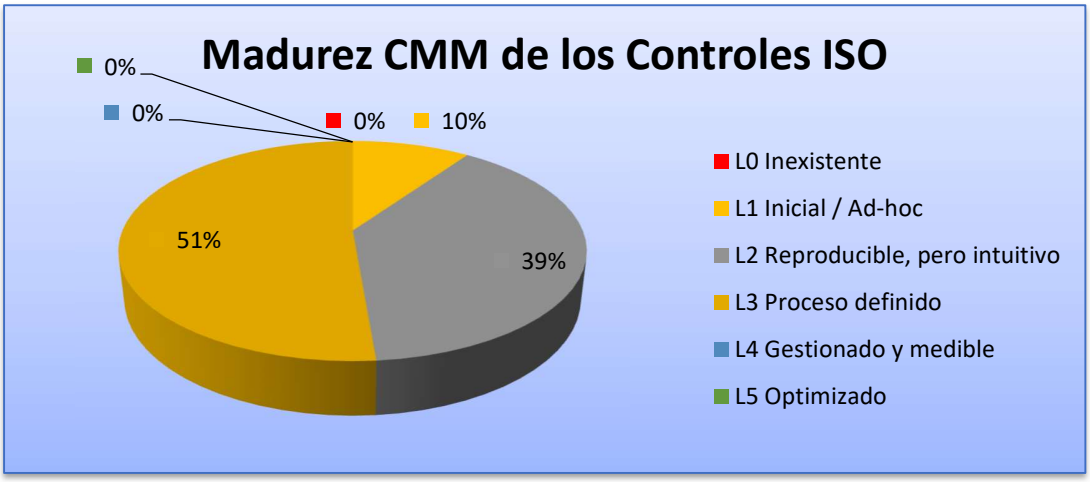
CUMPLIMIENTO DE LA IMPLEMENTACIÓN

En la elaboración del plan de tratamiento de seguridad de la información integramos tres (3) framewors para su consolidación, msat, isaca y iso27001, msat nos permitió realizar una autoevaluación de detallada de cada categoría y subcategoría de los componentes de seguridad de la información, isaca nos permitió evaluar los riesgos materializados para lograr su intervención y iso27001 valorar el avance y madurez de la implementación y de controles y requisitos de seguridad de la información

al finalizar el periodo 2021 Se gestiono el indicador de acuerdo a madurez de controles de CMM que referir a: Capability Maturity Model), quien define una metodología evaluar el modelo basados en la madurez con las siguientes variables, Inexistente, Inicial / Ad-hoc,Reproducible, pero intuitivo, Proceso definido, Gestionado y medible y Optimizado, la evuacion se realiza sobre los 114 controles del sistema de gestión de seguridad de la información y se evalúan los procesos definidos, en el cuarto se llegó a la meta de controles gestionados 57 controles que representan un 51% de los controles a implementar, la implementación se realiza de acuerdo a las guías mintic definidas para la implementación del sistema de gestión de la seguridad que adopta is027000 con framewoks , se logró un avance en el levantamiento del inventario de activos de información y el análisis de la criticidad de la misma con 136 activos de información de 4 procesos , para lo cual se entregaron y socializo un instructivo e instrumento para el diligenciamiento, ningún proceso reporto avances, se realiza las solicitudes para el último trimestre con la entradas y salidas de las caracterizaciones de los procesos , pendiente de levantar proceso algunos procesos administrativos y el total de los asistenciales para continuar en el 2022 con la implementación de controles de la norma is027002

NIVEL DE MADUREZ DE SGSI

ESTADO DE AVANCE DE LA MADUREZ DE LA SEGURIDAD ESE NORMA TECNICA NTC-ISO 27001



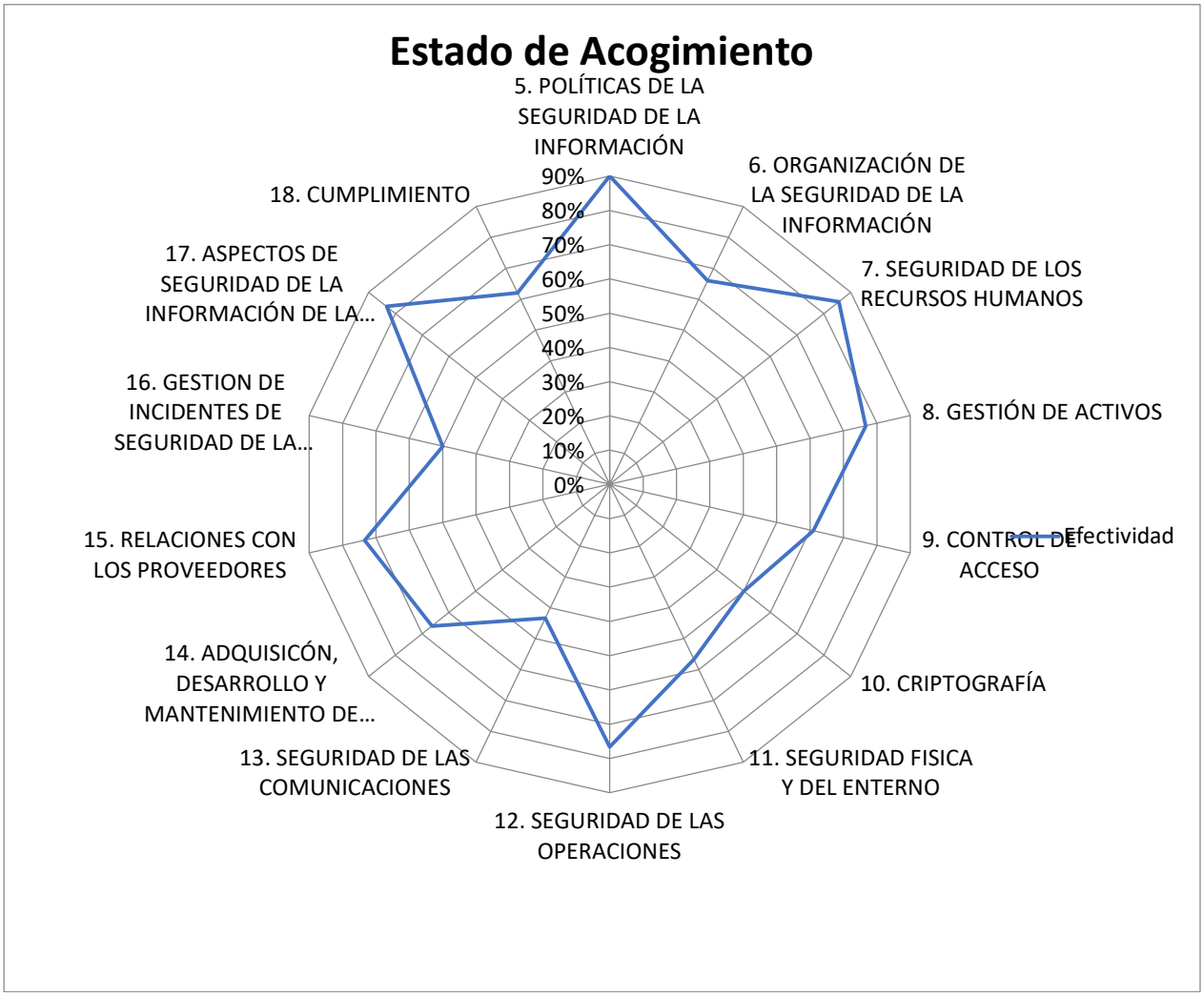
En la evaluación se idéntica que, de los 14 Dominios, 34 Objetivos de control y 114 Controles de la norma de seguridad **NTC-ISO 27001 un 51% procesos definidos,** un 39% reproducible e intuitivo y hace parte de la cultura organización de la ESE y un 10% está en etapa inicial

Porcentaje Cumplimiento 14 Controles de la norma técnica iso27001

Control	Efectividad
5. POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN	90%
6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	66%
7. SEGURIDAD DE LOS RECURSOS HUMANOS	86%
8. GESTIÓN DE ACTIVOS	77%
9. CONTROL DE ACCESO	61%
10. CRIPTOGRAFÍA	50%
11. SEGURIDAD FISICA Y DEL ENTERNO	57%
12. SEGURIDAD DE LAS OPERACIONES	77%
13. SEGURIDAD DE LAS COMUNICACIONES	43%
14. ADQUISICÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	66%
15. RELACIONES CON LOS PROVEEDORES	73%
16. GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	50%
17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO	83%
18. CUMPLIMIENTO	62%

Hoja Radar cumplimiento de la norma técnica ISO27001

En la hoja radar se evidencia que los 14 controles de seguridad de la información de desplegaron del centro hacia los bordes del grafico evidenciando el desarrollo e implementación en la vigencia 2021.



MAPA DE RUTA

Ciclos	Etapas	No.	Actividades	Fecha de inicio	Fecha final	Responsables	Producto o resultado esperado
PLANIFICACION	ETAPA 1.- DEFINCION DEL ALCANCE	1.1	Creación el comité de seguridad de la información	3/05/2021	16/05/2021	Representante Legal	Resolución de comité se seguridad de la información con funciones y responsabilidades
		1.2	diagnóstico y análisis del contexto y exigencias del negocio	19/05/2021	30/06/2021	Miembros del comité de seguridad de la información	Documento con las necesidades organizaciones y de procesos a fortalecer en la implementación del Sistema de Gestión de Seguridad de la información
		1.3	Definición de procesos del Negocio, críticos y claves para la implementación del proyecto SGSI	1/07/2021	9/07/2021	Miembros del comité de seguridad de la información	Procesos del negocio priorizados para la implementación
		1.4	Identificación los Stalholders del Proyecto	12/07/2021	16/07/2021	Miembros del comité de seguridad de la información	Identificar los involucrados en la implementación que generan un efecto sobre el proyecto y que deben ser tenidos en cuenta

Ciclos	Etapas	No.	Actividades	Fecha de inicio	Fecha final	Responsables	Producto o resultado esperado
		1.5	Definición de los objetivos estratégicos del proyecto SGSI	19/01/2021	20/08/2021	Miembros del comité de seguridad de la información	metas esperadas en la implementación del sistema de gestión de seguridad de la información
		1.6	Articular y alinear los objetivos estratégicos del proyecto SGSI con los objetivos del plan de desarrollo	23/01/2021	31/06/2021	Miembros del comité de seguridad de la información y Planeación	identificar como impactan los objetivos de la implementación dentro del microsistema de la organización
		1.7	Construir aprobar y socializar la Política de seguridad de la información y los acuerdos de confidencialidad	1/02/2021	31/12/2021	Miembros del comité de seguridad de la información, planeación y comunicaciones	Marco de directriz y gestión, intensión de construcción
		1.8	Definir los Frameworks para la implementación, evaluación y seguimiento del Proyecto SGSI	13/01/2021	28/03/2021	Miembros del comité de seguridad de la información	Contar con herramientas sistematizadas y lógicas para apoyar la implementación, evaluación y resultados
		1.9	Elaborar, aprobar y socializar el Plan de gestión de la seguridad de la información	1/02/2021	31/03/2021	Miembros del comité de seguridad de la información, Planeación y comunicaciones	Guía de implementación de Sistema de gestión de seguridad de la información

Ciclos	Etapas	No.	Actividades	Fecha de inicio	Fecha final	Responsables	Producto o resultado esperado
		1.10	aprobar por la alta gerencia de los recursos financieros, personas, responsabilidades y tiempos para la ejecución del proyecto SGSI	1/02/2021	31/12/2021	Representante legal	Contar con los recursos disponibles para la viabilidad financiera del Plan de gestión de Seguridad de la Información
IMPLEMENTACION	ETAPA 2.- GESTION DE ACTIVOS DE INFORMACION	2.1	Construir y Actualizar y aprobar instrumentos de identificación de activos de información	15/07/2021	30/07/2021	Miembros del comité de seguridad de la información, Planeación y comunicaciones	Instrumentos de identificación de activos de información
		2.2	Socializar Instrumentos de activos de información	1/09/2021	10/12/2021	Miembros del comité de seguridad de la información, Planeación y comunicaciones y líder SGSI	Página Web, correos instituciones, drive institucional
		2.3	Realizar Mapeo e inventario de Activos de información por mapa de procesos y responsables	13/12/2021	31/01/2022	Jefes de Procesos y líder del SGSI	Inventario y matrices de Activos de información por procesos
		2.4	Realizar análisis de criticidad de la información por proceso CID (Confiabilidad, Integridad, Disponibilidad)	1/02/2022	30/03/2022	Comité de Seguridad, jefes de procesos y líder SGSI	Matrices y resultados de criticidad

Ciclos	Etapas	No.	Actividades	Fecha de inicio	Fecha final	Responsables	Producto o resultado esperado
		2.5	Establecer responsabilidades ley 1712 transparencia y del derecho de acceso a la información pública nacional	1/07/2021	30/03/2022	Planeación, comunicaciones y líder SGSI	Matrices de activos de información publica que administre la empresa
		2.6	Establece la responsabilidad ley 1581 de 2012 protección de datos personales	1/07/2021	30/03/2022	Planeación, comunicaciones y líder SGSI	Informe de identificación de datos personales
	ETAPA 3.- LEVANTAMIENTO E IDENTIFICACION DE RIESGOS DE LOS ACTIVOS DE INFORMACION	3.1	Construir, Actualizar y aprobar instrumentos de identificación de Riesgos de activos de información y reporte de incidentes de seguridad de la información	1/05/2022	30/05/2022	Comité de Seguridad, y líder SGSI	Instrumentos de identificación de riesgos de activos de información
		3.2	Socializar Instrumentos de identificación de riesgos de activos de información	1/06/2022	15/06/2022	Comité de Seguridad y líder SGSI y procesos	Página Web, correos instituciones, drive institucional
		3.3	Realizar Análisis de vulnerabilidades sobre 3 pilares PPT (Personas, Procesos y Tecnología)	16/06/2022	15/08/2022	Comité de Seguridad y líder SGSI y procesos	Matrices y resultados de vulnerabilidades

Ciclos	Etapas	No.	Actividades	Fecha de inicio	Fecha final	Responsables	Producto o resultado esperado
		3.4	Identificación de Brechas de Seguridad de la información PPT	16/06/2022	15/08/2022	Comité de Seguridad y líder SGSI y procesos	Matriz Análisis de brechas
		3.5	Identificación de Amenazas de seguridad de la información PPT	16/06/2022	15/08/2022	Comité de Seguridad y líder SGSI y procesos	Matriz Análisis de amenazas
		3.6	Análisis y evaluación de Riesgos Seguridad de la información vulnerabilidades, brechas y amenazas	16/08/2022	16/09/2022	Comité de Seguridad y líder SGSI y procesos	Matriz análisis de riesgos
		3.7	Tratamiento de Riesgos Seguridad de la Información	17/09/2022	16/12/2022	Comité de Seguridad y líder SGSI y procesos	Informe tratamiento a riesgos
		3.8	informe de Seguimiento a Riesgos y revisión de seguridad de la información	15/12/2022	31/12/2022	Comité de Seguridad y líder SGSI	Informe de riesgos
	ETAPA 4.- IMPLEMENTACION DE CONTROLES Y REQUISITOS DE LA SEGURIDA DE LA	4.1	Construir, Actualizar y aprobar instrumentos para elaborar procedimientos para administrar controles registros y Riesgos de seguridad de la información	1/01/2023	31/01/2023	Comité de Seguridad y líder SGSI ,planeación y calidad	Instrumentos para elaborar procedimientos para administrar controles, registros y riesgos

Ciclos	Etapas	No.	Actividades	Fecha de inicio	Fecha final	Responsables	Producto o resultado esperado
	INFORMACION	4.2	Socializar Instrumentos para elaborar procedimientos para la implementación y administración de controles y riesgos de seguridad de la información	1/02/2023	28/02/2023	Comité de Seguridad y líder SGSI , comunicaciones, calidad y planeación	Página Web, correos instituciones, drive institucional
		4.3	Elaborar, socializar e Implementar procedimientos para la gestión de controles, riesgos y registros de seguridad de la información	1/03/2023	30/06/2023	Comité de Seguridad, calidad, planeación, líder SGSI y procesos	Procedimientos para la administración y seguimiento a controles de seguridad de la información
VALIDACION	**ETAPA 5.- PRUEBA DE SEGURIDAD DE LA INFORMACION**	5.1	Elaborar, aprobar y socializar plan de auditoria al sistema de gestión de seguridad de la información	1/07/2023	20/07/2023	Comité de Seguridad, planeación, líder SGSI	Plan de Auditorias al SGSI
		5.2	Implementar escenarios de pruebas de seguridad de la información	21/07/2023	5/07/2023	líder SGSI Y Jefe de TI	Escenario seguro de Pruebas

Ciclos	Etapas	No.	Actividades	Fecha de inicio	Fecha final	Responsables	Producto o resultado esperado
		5.3	Implementar Escaneo de Activos de Información con frameworks definidos en la etapa uno (1)	6/07/2023	30/08/2023	líder SGSI Y jefe de TI	Información escaneada de activos de la empresa para general Análisis
		5.4	Implementar evaluación independiente del sistema de gestión de seguridad de la información por empresa especializada	15/09/2023	15/10/2023	Comité de Seguridad de la información, líder SGSI, Jefe TI y Evaluador independiente	Evaluar independiente del estado seguridad de la información de la empresa
		5.5	Implementar buenas prácticas de Hacking Ético y ingeniería Social al sistema de gestión de seguridad	15/09/2023	15/10/2023	Comité de Seguridad de la información, líder SGSI y Jefe TI	Evaluación interna del estado de seguridad la información de la empresa
	ETAPA 6.- CAPACITACION Y SENSIBILIZACION	6.1	Elaborar, aprobar y socializar Plan de sensibilización y capacitación en Seguridad y Privacidad de la información	16/10/2023	16/11/2023	Comité de Seguridad de la información, líder SGSI, talento humano y comunicaciones	Documento Plan de Concienciación en Seguridad y Privacidad

Ciclos	Etapas	No.	Actividades	Fecha de inicio	Fecha final	Responsables	Producto o resultado esperado
		6.2	implementar Plan de sensibilización y capacitación del Sistema de Gestión de Seguridad de la información	17/11/2023	18/12/2023	Comité de Seguridad de la información, líder SGSI, talento humano y comunicaciones	Informe de ejecución Plan de Concienciación en Seguridad y Privacidad
		6.3	Análisis de resultados del Plan de sensibilización y capacitación del Sistema de Gestión de Seguridad de la información	19/12/2023	31/12/2023	Comité de Seguridad de la información, líder SGSI, talento humano y comunicaciones	Informe de resultados Plan de Concienciación en Seguridad y Privacidad
REVISION Y ACTUALIZACION	**ETAPA 7.- MANTENIMIENTO Y ACTUALIZACION**	7.1	Elaborar, aprobar y socializar programa para la evaluación y seguimiento a la implementación del Sistema de Gestión de Seguridad de la Información	1/01/2024	15/02/2024	Comité de Seguridad de la información, líder SGSI y planeación	Programa de auditoria
		7.2	Evaluar Acciones Correctivas y Acciones de Mejora del Sistema de Gestión de	1/03/2024	30/03/2024	Comité de Seguridad de la información, líder SGSI y planeación	Actas de reunión / correos electrónicos

Ciclos	Etapas	No.	Actividades	Fecha de inicio	Fecha final	Responsables	Producto o resultado esperado
			Seguridad de la Información				
		7.3	Revisar y gestionar e intervenir resultados de las Auditorías al Sistema de Gestión de Seguridad de la Información	1/04/2024	30/04/2024	Comité de Seguridad de la información, líder SGSI y planeación	Actas de participación en el Plan de auditoria
		7.4	Revisar, gestionar e intervenir los reportes de Incidentes de Seguridad de la Información	1/05/2024	30/05/2024	Comité de Seguridad de la información, líder SGSI y planeación	Aplicativo para Incidentes de Seguridad de la información.
		7.5	Evaluar los resultados y tendencias de los indicadores trazadores del Sistema de Gestión de Seguridad de la Información	1/11/2021	30/05/2024	Comité de Seguridad de la información, líder SGSI y planeación	Evidencia para evaluación de los indicadores

CARGA DE LA IMPLEMENTACIÓN POR ETAPAS, ACTIVIDADES Y TIEMPO

Orden	Etapas	No. De actividades
1	Definición del alcance del proyecto	10
2	Gestión de inventario de activos de información	6
3	Levantamiento e identificación de riesgos de los activos de información	8
4	Implementación de controles y requisitos de la seguridad de la información	3
5	Pruebas de seguridad de la información	5
6	Capacitación y sensibilización	3
7	Mantenimiento y actualización	5
	Totales	**40**

implementación y mantenimiento del Sistema de Gestión de la Información (SGSI) en el Hospital , genera como resultado la ejecución para las 7 etapas de 40 actividades en un tiempo promedio de 3 años, como se revela en la tabla de la carga de la implementación. Aquí, se identifica que la etapa inicial de planeación del proyecto son 10 actividades superiores a las siguientes, debido a que esta es la etapa más importante para garantizar la ejecución del proyecto.

De igual manera, es importante resaltar que la implementación de este plan plantea grandes desafíos al interior del Hospital, debido a que no se limita a solo implementar un proyecto, sino, que tiene una ejecución proyectada a 3 años de duración. Por lo que se requiere del compromiso de la alta gerencia y todos los procesos, de la asignación de los recursos requeridos en cada etapa, así como la designación de un sponsor, un líder del proyecto y un oficial de seguridad, pero, sobre todo, en la concentración de una apuesta por trabajar en la transformación de la cultura

organizacional de la empresa, para la adopción de este proceso estricto de gestión de la información.

_____

LUZ YAMILETH GARZON SANCHEZ
GERENTE GENERAL

Proyecto y elaboro: Mario Gonzalez Hernández
Jefe sistemas de información, estadística y Gestión Documental