Diseño del Sistema de Gestión de Seguridad de la Información, basado en el - MSPI -, Dirección Territorial de Salud de Caldas

Juan Pablo Henao Pereira

Universidad de Manizales

Facultad de Ciencias e Ingeniería

Maestría en seguridad de la información

Manizales, 2023

Resumen

Este trabajo busca realizar el diseño del sistema de gestión de seguridad de la información SGSI, basado en las buenas prácticas del modelo de seguridad y privacidad de la información MSPI de MINTIC, para proporcionar apoyo en la gestión de los activos de información, así como en la clasificación y valoración de las amenazas que podrían afectar las operaciones estratégicas de la Dirección Territorial de Salud de Caldas.

Bajo la gran demanda de información que es requerida para el ejercicio normal de las funciones de la entidad, La implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) es fundamental en una entidad de salud pública por varias razones, protección de datos personales acerca de la salud ya que se presentan demasiados riesgos ante la divulgación de estos, cumplimiento normativo al ser una entidad pública y rectora que vigila controla y acompaña los procesos de salud del departamento de Caldas, debe acogerse a el cumplimiento de las directrices del ministerio de tecnologías y comunicaciones MINTIC realizando la adopción del modelo de seguridad y privacidad de la información MSPI.

Palabras Clave: ISO 27001, Modelo de seguridad y privacidad de la información MSPI, Sistema de gestión de seguridad de la información SGSI, Riesgos, Seguridad de la información.

Abstract

This work aims to design the Information Security Management System (ISMS) based on best practices from the Information Security and Privacy Model (ISPM) by MINTIC. This system is intended to provide assistance in managing assets, classifying and evaluating threats that pose risks to the strategic operations of the territorial health department of Caldas.

Due to the high demand for information required for the normal functioning of the entity, the implementation of an Information Security Management System (ISMS) is crucial for a public health organization for several reasons. It involves the protection of personal health data, as there are significant risks associated with their disclosure. Additionally, compliance with regulations is essential since the entity is a public governing body responsible for overseeing, controlling, and supporting the health processes in the Caldas department. Therefore, it must adhere to the guidelines provided by the Ministry of Information Technologies and Communications (MINTIC) by adopting the Information Security and Privacy Model (ISPM).

Contenido

Diseño del Sistema de Gestión de Seguridad de la Información, basado en el - MSPI -, Dirección Territorial de Salud de Caldas 1

Resumen 2

Abstract 3

Tabla de Figuras 8

Lista de tablas 9

Lista de anexos 10

1. Planteamiento del problema de investigación y su justificación 11

1.1 Descripción del área problemática 11

1.2 Formulación del problema 12

1.3 Justificación 12

2. Objetivos 14

2.1 Objetivo general: 14

2.2 Objetivo específicos: 14

3. Antecedentes 15

4. Referente normativo y legal 21

4.1 LEY 1273 Protección de la Información y los Datos 21

4.2 Ley 1581 Protección de Datos Personales 21

4.3 Ley 599 del 2000. Artículo 269d. Daño informático 22

4.4 Constitución Política de Colombia Articulo 15 y 20. 22
4.5 Ley 1266 de 2008 22
4.6 Ley 1712 de 2014 23
4.7 Ley 1928 de 2018 23
4.8 Conpes 3701 de 2011 23
4.9 CONPES 3854 de 2016 23
5. Referente Teórico 24
5.1 Seguridad informática 24
5.2 ISO/IEC 27001:2013 25
5.3 Sistema de Gestión de Seguridad de la Información (SGSI) 26
5.4 Modelo de Seguridad y Protección de la Información (MSPI) 26
FASE 0. DIAGNOSTICO. 31
FASE 1. PLANIFICACIÓN DEL MSPI. 31
FASE 2. IMPLEMENTACIÓN del MSPI. 33
FASE 3. EVALUACIÓN DEL DESEMPEÑO DEL MSPI. 33
FASE 4. MEJORAMIENTO CONTINUO 33
5.5 Sistema de Gestión de Riesgos 33
Datos y recursos de TI: 34
6. Metodología 46
6.1 Enfoque metodológico 46
6.2 Tipo de Estudio 46

6.3 Procedimiento 46

6.4 Alcance de la investigación 48

Contexto de la entidad 48

7. Resultados 52

Fase 1. Diagnóstico de la Dirección territorial de salud de caldas en cuanto a la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI). 52

Fase 2. Identificación y clasificación de los activos de información de la Dirección territorial de salud de caldas. 56

Fase 3. Identificar los riesgos de la Dirección territorial de salud de caldas. 58

Definición de Roles 76

Declaración de aplicabilidad 94

Conclusiones 99

Recomendaciones 100

Referencias 101

Lista se símbolos y abreviaturas

Abreviatura	**Termino**
MINTIC	Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia
SGSI	Sistema de gestión de seguridad de la información
MSPI	Modelo de privacidad y seguridad de la información
ISO	International Organization for Standardization
DTSC	Dirección territorial de salud de Caldas
TI	Tecnologías de la información
CID	Confidencialidad, integridad, disponibilidad
PHVA	Planear, hacer, verificar, actuar
TICS	Tecnologías de la Información y Comunicación

Tabla de Figuras

Figura 1. Ciclo MSPI.....30

Figura 2. Pasos MSPI.....32

Figura 3. Ciclo PHVA.....44

Figura 4. Organigrama DTSC.....49

Figura 5. Portafolio de servicios DTSC.....50

Figura 6. Factores asociados al riesgo.....59

Figura 7. Clasificación de controles por tipología.....66

Figura 8. Clasificación (CID).....88

Figura 9. Clasificación de los activos según la confidencialidad.....89

Figura 10. Clasificación de los activos según la integridad.....89

Figura 11. Clasificación de los activos según la Disponibilidad.....90

Figura 12. Nivel de importancia de los activos.....90

Figura 13. Clasificación de la información.....92

Lista de tablas

Tabla 1 Evaluación efectividad de los controles**.** 53

Tabla 2 Brecha anexo A ISO 27001:2013 54

Tabla 3 Tiempos avance PHVA**.** 55

Tabla 4 avance PHVA - DTSC 56

Tabla 5 Parámetros de evaluación de los activos 57

Tabla 6 Nivel de importancia de los activos 58

Tabla 7 Criterios de evaluación de probabilidades 60

Tabla 8 Criterios de evaluación del impacto 60

Tabla 9 Criterios de aceptabilidad del riesgo 62

Tabla 10 Mapa de riesgos inherente 63

Tabla 11 Matriz de riesgo residual 64

Tabla 12 Clasificación de controles según tipología 65

Tabla 13 Criterios de valoración de los controles 67

Tabla 14 Amenazas y vulnerabilidades conocidas 68

Tabla 15 Fuente y tipo de amenazas 75

Tabla 16 Roles de seguridad de la información 76

Tabla 17 Clasificación de la información (CID) 87

Tabla 18 Clasificación de la información 91

Lista de anexos

Anexo 1. Instrumento de evaluación MSPI.

Anexo 2. Inventario de activos

Anexo 3. Políticas de seguridad de la información.

Anexo 4. Matriz análisis de riesgos.

Anexo 5. Declaración de aplicabilidad de los controles.

Anexo 6. Plan de sensibilización, Capacitación, educación y comunicación.

1. Planteamiento del problema de investigación y su justificación

1.1 Descripción del área problemática

Hoy en día la información se ha convertido en uno de los activos más importantes tanto para empresas como para personas naturales, y es esto lo que lleva a los usuarios a emplear diferentes tipos de dispositivos electrónicos y aplicaciones para crear, almacenar, procesar o difundir dicha información y la Dirección Territorial de Salud de Caldas no es ajena a esto ya que por su naturaleza misional de vigilar inspeccionar y controlar, maneja información de datos personales y que se consideran como confidenciales y sensibles que deben ser protegidos, para garantizar su confidencialidad, integridad y disponibilidad.

La implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) se convierte en una prioridad estratégica para la Dirección Territorial de Salud de Caldas, Ya que actualmente la entidad no tiene identificado el nivel de madurez ni el diseño de un SGSI, no se cuenta con la identificación de los riesgos de los activos de información, y tampoco se cuenta con los roles y responsabilidades definidas frente a las políticas las cuales requerían de una actualización, así que no solo se trata de proteger los datos sensibles de los pacientes, sino también de asegurar la continuidad operativa y la reputación de la institución. Un SGSI eficaz proporciona un marco estructurado para identificar, evaluar y gestionar los riesgos de seguridad de la información de manera proactiva. Esto implica la el diseño de políticas, procedimientos y controles de seguridad, sensibilización y capacitación del personal, con el fin de fortalecer las defensas contra amenazas internas y externas, como el acceso no autorizado, el robo de datos y los ataques cibernéticos. En última instancia, un SGSI bien diseñado permite a la Dirección

Territorial de Salud de Caldas cumplir con su compromiso de inspección, vigilancia y control mientras protege la confidencialidad y privacidad de los datos que se manejan.

1.2 Formulación del problema

Actualmente en la Dirección Territorial de Salud de Caldas el personal en el área de tecnologías de la información es insuficiente, a pesar de que existen algunas políticas respecto a seguridad de la información es necesario hacer una revisión para actualizar políticas debido a los cambios en procesos y normatividad que rige a la entidad, no se encuentra documentado un sistema de gestión de seguridad de la información, no está definido el inventario de activos de información, y se desconoce el nivel de madurez actual, hace falta una estrategia de socialización de las políticas y finalmente no está establecido el comité de seguridad de la información.

Por lo anterior surge el interrogante: ¿Cómo diseñar un Sistema de Gestión de Seguridad de la Información que se adapte a las necesidades específicas de la Dirección Territorial de Salud de Caldas?

1.3 Justificación

Este trabajo se fundamenta en que las instituciones públicas deben dar cumplimiento a la ley 1341 de 2009 y los decretos 2573 de 2014 y 1078 de 2015 en donde se estipula la importancia de brindar condiciones de ciberseguridad en los activos de información, tanto como la información almacenada en dispositivos que están conectados a una red. así como la ley 1581 de 2012 de protección de datos personales.

En Colombia, según el Observatorio de Cibercrimen y su balance más reciente en el año 2020, se registraron diversos delitos informáticos, incluyendo acceso abusivo a un sistema informático (5,584 casos), interceptación de datos informáticos (1,231 casos), violación de datos personales (7,001 casos), suplantación de sitios web (4,353 casos), obstaculización ilegítima de sistemas informáticos o redes de telecomunicaciones (242 casos), daño informático (507 casos), uso de software malicioso (513 casos), hurto por medios informáticos y similares (13,212 casos), y transferencia no consentida de activos (2,632 casos), lo que representa un incremento del 82% con respecto al año 2019. Estas cifras reflejan la creciente importancia de fortalecer los sistemas de seguridad de la información para proteger tanto a los individuos como a las organizaciones contra las amenazas cibernéticas.(CSIRT POLICÍA NACIONAL COLOMBIANA, 2020)

Es por esto que se realizará el diseño del modelo de seguridad y privacidad de la información MSPI- dado por MINTIC con el fin de proteger de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.

Ese trabajo solo contempla la etapa del diseño ya que, por cuestión de tiempos, aprobación, destinación de recursos públicos, y de acuerdo al (PETI) Plan Estratégico de Tecnologías de la Información y las Comunicaciones, no es posible desarrollar la etapa de implementación.

2. Objetivos

2.1 Objetivo general:

Diseñar el Sistema de Gestión de Seguridad de la Información -SGSI-, basado en el Modelo de Seguridad y Privacidad de la Información - MSPI -, para la Dirección Territorial de Salud de Caldas.

2.2 Objetivo específicos:

- Determinar el estado actual de la gestión de seguridad de la información de la Dirección Territorial de Salud de Caldas.
- Identificar y gestionar los riesgos de seguridad en el área de Tecnología de la entidad.
- Establecer controles y políticas aplicables bajo las normas respectivas para minimizar los riesgos más significativos o de alto impacto.

3. Antecedentes

Márquez H. realizó el diseño de un sistema de gestión de seguridad de la información en una institución de la salud el proyecto está basado en la norma ISO/IEC 27001:2013 y el uso de Magerit la cual es autor describe como una metodología que permite un buen nivel de calidad administrativa y procesos de mejora continua, incluyendo el desarrollo de políticas y la evaluación de riesgos. Se detalla la ejecución del Sistema de Gestión de Seguridad de la Información (SGSI), abordando la gestión de riesgos, la identificación de controles y las asignaciones de responsabilidades. Se menciona la elaboración de la declaración de aplicabilidad del modelo y la asignación de recursos humanos, se incluye un plan detallado para la realización de auditorías internas. (Márquez H, 2020, p. 11).El estudio de (Criollo I, 2022, pag.13;21) realizó la planeación de un SGSI basado en la norma ISO/IEC 27001:2013 para una institución prestadora de servicios de salud privada, también haciendo uso de la metodología Magerit, además se establecen fases metodológicas para implementar medidas de seguridad, realiza la identificación de los riesgos y amenazas que pueden afectar la información. Se destaca la importancia de la gestión de incidentes de seguridad y la concientización del personal. En el trabajo (Carreño I. et al., 2021) a diferencia de los 2 trabajos anteriores usaron como metodología Cobit, para el diseño de un SGSI en una empresa del sector salud basándose la norma ISO/IEC 27001:2013, El documento aborda la importancia de revisar la valoración de riesgos y realizar auditorías internas para actualizar los planes de seguridad, enfatizando la implementación de un Sistema de Gestión de Seguridad de la Información y el análisis de vulnerabilidades. Se establecen políticas de seguridad de la información basadas en la norma ISO 27001:2013 para proteger los activos tecnológicos, destacando la necesidad de monitorear y mejorar continuamente las medidas de seguridad en

la organización. Se sugiere realizar auditorías periódicas y mantener actualizados los sistemas operativos para prevenir posibles ataques. Además, se abordan aspectos como la identificación de activos tecnológicos, diseño de red, análisis de brechas GAP y diseño de políticas de seguridad, resaltando la importancia de la documentación de referencia. (Ruiz J., 2018) realizó un modelo para la implementación de la ley 1581 de protección de datos personales, basados en la norma ISO/IEC 27001:2013 usando la metodología Magerit y el ciclo Deming buscando Establecer medidas, procedimientos y buenas prácticas para prevenir incidentes relacionados con el tratamiento de datos personales. La investigación de (Enríquez A., 2018) diseñó un modelo de Sistema de Gestión de Seguridad de la Información (SGSI) para la Clínica Médica Fértil, abordando la situación actual de la clínica y realizando un análisis de gestión de riesgos. Se desarrollan políticas basadas en normas ISO/IEC 27001:2013, ISO/IEC 27005:2008, ISO/IEC 27002:2013 e ISO 27799:2008, enfocadas en principios como Confidencialidad, Integridad, Disponibilidad, Seguridad en el manejo de la información y Secreto Médico. Se implementan controles y políticas de seguridad para garantizar la confidencialidad, integridad y disponibilidad de la información de los pacientes, incluyendo aspectos como la protección de datos sensibles, la gestión de activos informáticos y la concientización del personal sobre seguridad de la información. Por su parte (Erik M., 2019) presenta una metodología para implementar un Sistema de Gestión de Seguridad de la Información basado en ISO/IEC 27001 en áreas de admisión y atención de un hospital público, enfatizando la protección de la confidencialidad, integridad y disponibilidad de la información de salud. Se destaca la automatización de funciones administrativas y clínicas a través de sistemas de información hospitalaria, resaltando la importancia de las Tecnologías de la Información y Comunicación (TICS) en el sector de la salud. Se subraya la necesidad de contar con el respaldo de la alta dirección para una implementación efectiva del SGSI, que permita proteger y administrar la información sensible de la institución de manera sistemática, fortaleciendo la seguridad, el acceso, la disponibilidad, el control, la autenticidad, la integridad, la confidencialidad y la

conservación de los datos. En el trabajo de (Palma M., 2019) presenta un exhaustivo análisis y diseño de una política de seguridad de la información para garantizar el control de acceso a la infraestructura de red de un hospital. Se basa en la norma ISO27002:2013 y aborda aspectos clave como la identificación de activos, la gestión de riesgos, la seguridad física y lógica, la concienciación del personal, el trabajo destaca la importancia de implementar medidas de seguridad efectivas para proteger la información sensible y garantizar la integridad, confidencialidad y disponibilidad de los datos en un entorno hospitalario. (Niquen L, 2019) realizó un Modelo de Gestión de Seguridad de la Información, usando estándares y metodologías adaptados para instituciones de salud, con la finalidad de apoyar los procesos de atención al paciente. En la investigación de (Tamayo J., 2020) el documento aborda la importancia de aplicar metodologías de evaluación y gestión de riesgos informáticos en el sector de la salud, realiza una comparación entre varias metodologías para definir cuál es la mejor que se adapta para pequeñas empresas, donde se analizan metodologías como ISO 27005, IS0 31000, MARISMA - AGR, Y MAGERIT siendo seleccionada la metodología MARISMA - AGR, ya que cumple con varios puntos claves que la hacen más fácil adaptar a pequeñas empresas.

Maria Jose B. en su trabajo aborda la gestión de riesgos en bibliotecas universitarias, enfocándose en las normas ISO/IEC 27001:2013, se evalúan amenazas, vulnerabilidades y Controles. Se identifican riesgos como daños por agua, fuego, suplantación de identidad y condiciones inadecuadas de producción de documentos. Se menciona la falta de planes de recuperación de desastres y continuidad del negocio. Se proponen medidas como copias de seguridad, protección de equipos informáticos y plan de recuperación de desastres. Se detallan zonas de riesgo, amenazas y controles específicos. Se concluye con recomendaciones para mejorar la seguridad informática en bibliotecas., además realizo una compresión de diferentes metodologías para identificar sus puntos fuertes, entre las metodologías analizadas se

encuentran MAGERIT v.3, OCTAVE v.2 y NIST 800-30.MAGERIT y OCTAVE. (Bravo M., 2018), de igual manera (Guerra et al., 2021) ha llevado a cabo un estudio sobre el desarrollo de un sistema de gestión para la seguridad de la información en bibliotecas universitarias, con un análisis exhaustivo de amenazas tanto internas como externas. Se destaca la importancia crítica de adoptar estándares de seguridad y se recomienda la aplicación de la norma ISO/IEC 27001:2013 para la identificación y evaluación de riesgos. Se detallan riesgos financieros, de cumplimiento y de incumplimiento de compromisos institucionales, proponiendo la elaboración de un protocolo escrito para la gestión del sistema de préstamo, junto con la capacitación del personal y la implementación de controles rigurosos. Se aborda específicamente el desafío de errores en el préstamo interbibliotecario, proponiendo una revisión y rediseño de procesos. para prevenir problemas como recepción de material incompleto o retrasos en los procesos de adquisición. Asimismo, se plantea validar el plan de evacuación y capacitar al personal en el uso adecuado de equipos informáticos, junto con un plan de redistribución de espacios para mitigar riesgos físicos, y se sugiere la implementación de medidas para mejorar la catalogación y clasificación bibliográfica, aplicando la norma ISO/IEC 27001:2013 adaptando la metodología Magerit. El documento de (Sierra M. & Hurtado J., 2018) se centra en la implementación del modelo de seguridad y privacidad de la información del MINTIC en su fase de planificación en la Alcaldía de Puerto Asís. Se destaca la importancia de evaluar la situación actual en seguridad y privacidad de la información, establecer controles adecuados, identificar activos de información, y promover la actualización continua de políticas de seguridad. El objetivo principal es definir una metodología para el plan de seguridad de la información, con el fin de mejorar la gestión de la información en la entidad pública, garantizando la protección de los datos sensibles de los ciudadanos y cumpliendo con los lineamientos establecidos por el gobierno nacional.

Rienzo A, y colaboradores realizaron una investigación basada en encuestas para determinar el nivel de implementación de NCh-ISO 27001 en instituciones de salud en chile donde se obtuvo como resultados, el grado de implementación de la norma, el grado de conocimiento de esta y los principales controles y dominios implementados (Rienzo & Gastón, 2018, p. 1,6). También (Perez D. et al., 2019), realizaron una encuesta donde el objeto de investigación fue los efectos de las prácticas organizacionales de seguridad de la información, intercambio de conocimientos sobre seguridad, educación sobre seguridad de la información y visibilidad de la seguridad de la información en las pymes de Cantabria, así mismo en(Peikari et al., 2018) se realizó una encuesta para determinar la percepción de los pacientes de centros médicos sobre la gestión de seguridad de la información, encontrando que factores como la protección técnica, física y el monitoreo tienen una relación positiva con la confianza de los pacientes. En el estudio presentado por (Rodriguez G., 2020) se realizó un análisis comparativo de 2 modelos de implementación de sistemas de gestión de la información, Defensa en Profundidad (Defense in Depth) DID y MSPI en donde se presentan ventajas y desventajas al elegir uno de los dos modelos, para ayudar a las empresas a tomar una decisión al momento de elegir el modelo que más se adapte a sus necesidades.

En el trabajo de (Zapata, 2021) se describe el análisis de los factores críticos que influyen en el éxito de la implementación de un sistema de gestión de seguridad de la información, obteniendo como resultado que el factor más importante es la sensibilización lo que permitirá emplear el SGSI, de igual manera la investigación de (Zammani et al., 2019, p. 348) logró determinar los 14 factores y los 45 elementos que influyen en el éxito de la implementación de una SGSI. caso contrario en el estudio (Tatiara et al., 2018) donde se analizaron los factores que dificultan o inhiben la implementación de un SGSI. En el estudio (Saminu, 2019) se desarrolló una investigación cualitativa dónde a través de encuestas se logró determinar cuáles son los desafíos en materia de seguridad de la información de un centro médico en katsina.

En (Arafat, 2018, p. 1) se realizó la aplicación de un sistema de gestión de seguridad en la nube basado en la familia de normas ISO/IEC 27000, y pretende demostrar cuáles fueron los principales desafíos al realizar esta implementación en la nube. Por su parte (Pleskach et al., 2019) también hacen uso en su trabajo de esta norma, con enfoque para el diseño de algoritmos de gestión de la seguridad de la información en sistemas distribuidos basados en análisis adaptativo de tráfico de redes. el trabajo desarrollado por (Achmadi D et al., 2018) usan como base la norma ISO/IEC 27001 para crear un framework para la implementación de un SGSI en un centro de datos.

Por su parte (Proença & Borbinha, 2018, p. 102) presentan un modelo que sirve como una herramienta de evaluación para que las organizaciones la utilicen con el fin de obtener su nivel de madurez del Sistema de Gestión de Seguridad de la Información, planteando cuales son los requisitos clave para lograr una buena calificación en el modelo de madurez de una empresa, también realizan una comparación varios modelos de madurez de la gestión de la seguridad de la información, además se muestran los resultados de las evaluaciones realizadas cinco organizaciones diferentes.

García J. y colaboradores realizaron un modelo de gestión de riesgos de seguridad de la información para pymes en Perú basados en la metodología OCTAVE-S y la norma ISO/IEC 27005 en el proceso de ventas de una empresa, El documento analiza la implementación de un marco de gestión de riesgos de seguridad de la información. Cubre la identificación de áreas críticas para la evaluación, la construcción de perfiles de amenazas y el uso de enfoques cuantitativos y cualitativos para la evaluación de riesgos, también menciona la incorporación de planes de seguridad de la información en los programas de capacitación, la documentación formal de procesos y procedimientos, y el uso de diversos controles y medidas de seguridad.(García J. et al., 2018, p. 47)

4. Referente normativo y legal

4.1 LEY 1273 Protección de la Información y los Datos

En Colombia a través de la “Ley 1273 de 2009 por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado - denominado 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”. [LEY 1273 DE 2009]

En la cual se establecen los siguientes artículos:

“Artículo 269A: Acceso abusivo a un sistema informático. Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación. Artículo 269C: Interceptación de datos informáticos. Artículo 269D: Daño Informático. Artículo 269E: Uso de software malicioso. Artículo 269F: Violación de datos personales. Artículo 269G: Suplantación de sitios web para capturar datos personales”. [LEY 1273 DE 2009]

4.2 Ley 1581 Protección de Datos Personales

“Ley 1581 DE 2012 donde se define lo protección de datos personales que son todos los datos asociados a una persona que puedan identificarla individualmente, como su documento de identidad, número de identificación, el lugar de nacimiento, estado civil, edad, lugar de residencia, así mismo hay información considerada sensible y es la que está relacionada con su estado de salud, sus características físicas, ideología política, vida sexual, entre otros” [ley 1581]

4.3 Ley 599 del 2000. Artículo 269d. Daño informático

"El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión".(Ley 599 de 2000 - Gestor Normativo - Función Pública)

4.4 Constitución Política de Colombia Articulo 15 y 20.

"ARTÍCULO 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas". (MinTic,1991)

"ARTÍCULO 20. Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, informar y recibir información veraz e imparcial, y la de fundar medios de comunicación masiva. Estos son libres y tienen responsabilidad social. Se garantiza el derecho a la rectificación en condiciones de equidad. No habrá censura". (MinTic,1991)

4.5 Ley 1266 de 2008

Se establecen normativas generales sobre el tratamiento de datos personales, en particular aquellos relacionados con información financiera, crediticia, comercial, de servicios y datos provenientes de otros países, con el fin de regular su gestión y protección.(Ley 1266, 2008)

4.6 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”.(Congreso de la República de Colombia, 2014)

4.7 Ley 1928 de 2018

Convenio sobre la ciberdelincuencia. Se aprueba el convenio sobre la ciberdelincuencia adoptado el 23 de noviembre de 2001, en Budapest. El objetivo es concretar una política criminal común en relación a la ciberdelincuencia mediante la implementación de lineamientos.(Congreso de la República de Colombia, 2018)

4.8 Conpes 3701 de 2011

Tiene como objetivo establecer estándares de política en materia de ciberseguridad y ciberdefensa para crear una estrategia nacional que combata el aumento de las amenazas informáticas que tienen un impacto significativo en el país.(Conpes 3701, 2011)

4.9 CONPES 3854 de 2016

es un documento que establece la Política Nacional de Seguridad Digital en Colombia, con el objetivo de garantizar la seguridad de la información y las comunicaciones en el país, proteger los derechos de los ciudadanos en el entorno digital y promover la cooperación internacional en materia de seguridad digital. El documento establece una estructura de gobierno, estrategias y acciones para alcanzar los objetivos de la política, y mecanismos de seguimiento y evaluación para medir su impacto.(Conpes 3854, 2016)

5. Referente Teórico

5.1 Seguridad informática

Álvaro Gómez en su libro enciclopedia de la seguridad informática define seguridad de la información como cualquier medida que impida la ejecución de acciones no autorizadas sobre un sistema o red informática, que puedan afectar la confidencialidad, autenticidad o la integridad y causen daños graves sobre la información. (Álvaro gomez,2011)

Los principales aspectos de la seguridad informática son los siguientes:

Confidencialidad: propiedad que garantiza que la información se mantenga oculta y protegida frente a accesos no autorizados. Y permitirá accesos y divulgación de información solo para aquellas personas que tengan los permisos necesarios para acceder a ella. (Alfonso et al., 2020)

Disponibilidad: propiedad de garantizar que tanto el sistema, recursos y la información van a estar disponibles y accesibles cuando sean requeridos por el usuario autorizado en todo momento. Esto implica que la información y los servicios se encuentren operativos y listos para su uso legítimo en todo momento. La disponibilidad busca prevenir interrupciones no planificadas, ataques cibernéticos u otras amenazas que puedan afectar la continuidad de los sistemas, garantizando que los usuarios autorizados puedan acceder y utilizar la información y los recursos de manera oportuna y confiable.(Alfonso et al., 2020)

Integridad: propiedad que garantiza que la información se mantenga completa, precisa y sin modificaciones no autorizadas a lo largo de su ciclo de vida, implica proteger la exactitud, consistencia y fiabilidad de los datos, así como prevenir alteraciones, manipulaciones o corrupciones tanto accidentales como intencionales. (Alfonso et al., 2020)

No repudio: propiedad que impide que una persona niegue haber realizado una acción o transacción específica. Es un mecanismo que proporciona evidencia irrefutable de la

participación o autoría de una persona en una acción determinada, como el envío de un mensaje o la firma de un documento digital, ya que en toda comunicación hay 2 participantes remitente(origen), receptor(destino), se consideran los 2 siguientes tipos de no repudio:

No repudio en origen: esta característica se obtiene mediante el uso de mecanismos de registro y técnicas criptográficas que proporcionan pruebas irrefutables de la identidad del remitente y la integridad del mensaje o transacción. De esta manera, el no repudio en origen protege a las partes involucradas en una comunicación o transacción electrónica y evita que el remitente niegue haber enviado el mensaje o tomar las medidas necesarias.(Valencia Martínez et al., 2023)

No repudio en destino: una característica que garantiza que el destinatario de un mensaje o transacción no puede negar haber recibido o accedido a la información. Esta característica se logra mediante el uso de mecanismos de registro y técnicas criptográficas que proporcionan evidencia irrefutable de que la información se entregó. (Valencia Martínez et al., 2023)

5.2 ISO/IEC 27001:2013

La adopción de un sistema de gestión de seguridad de la información es una decisión estratégica para una organización. El establecimiento e implementación del sistema de gestión de seguridad de la información de una organización está determinada por las necesidades y objetivos de la organización.

La norma ISO/IEC 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa ya sea de naturaleza privada o pública, grandes o pequeñas y proporciona

una metodología que permite implementar un sistema de gestión de seguridad en cualquier organización. (adversia, s/f)

Haciendo uso de buenas prácticas, para reducir el riesgo de que las amenazas puedan aprovechar las vulnerabilidades en el área de tecnologías de la información una compañía.

5.3 Sistema de Gestión de Seguridad de la Información (SGSI)

un sistema de gestión de seguridad de la información es un conjunto de políticas definidas con el fin de gestionar eficazmente la disponibilidad, integridad, y confidencialidad de los activos de información de una organización y a través de este lograr la disminución de los riesgos (Bravo M., 2018)

Desde el punto de vista de la norma internacional ISO/IEC 27001: 2013 el SGSI es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización para si alcanzar sus objetivos comerciales.

5.4 Modelo de Seguridad y Protección de la Información (MSPI)

Modelo de seguridad y privacidad de la información, es un lineamiento dado por MINTIC en el cual se describe como las entidades públicas, deben hacer uso de buenas prácticas, teniendo como referentes estándares internacionales, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos. El Modelo de Seguridad y Privacidad se encuentra basado en las buenas prácticas de seguridad de la norma 27001 del 2013, legislación de la Ley de Protección de Datos Personales, Transparencia y Acceso a la Información Pública, entre otras, las cuales se deben tener en cuenta para la gestión de la

información, el MSPI está compuesto por cinco fases, las cuales permiten que las entidades puedan gestionar la seguridad y privacidad de los activos de información, las fases son: Diagnostico, Planeación, Implementación, Evaluación del Desempeño, Mejora Continua. (Mintic, s/f)

ACTIVOS DE INFORMACIÓN: son aquellos recursos y componentes que poseen un valor significativo para una organización en términos de su confidencialidad, integridad y disponibilidad. Estos activos pueden ser, datos, información, sistemas de información, infraestructura tecnológica, hardware, software, redes, aplicaciones, documentos y procesos empresariales.

IMPACTOS: se refieren a las consecuencias o efectos negativos que pueden surgir como resultado de la materialización de una amenaza o incidente de seguridad. Estos impactos pueden afectar la confidencialidad, integridad y disponibilidad de los activos de información de una organización. Algunos ejemplos de impactos pueden incluir la divulgación no autorizada de información confidencial, la alteración o manipulación de datos críticos, el bloqueo o interrupción de servicios y sistemas, la pérdida de productividad, daños a la reputación de la organización y posibles implicaciones legales o regulatorias. La evaluación de los impactos en seguridad de la información es esencial para comprender las implicaciones y consecuencias potenciales de los incidentes de seguridad, y así poder tomar medidas preventivas y de respuesta adecuadas para minimizar los daños y mitigar los riesgos asociados. (Alex Richar Silva Guerrero, 2021)

AMENAZAS: las amenazas están presentes en todo momento y son aquellas acciones que pueden traer consecuencias negativas en el desarrollo de las actividades misionales de la empresa. se refieren a eventos, acciones o circunstancias que tienen el potencial de causar

daños, pérdidas o alteraciones en los activos de información de una organización. Estas amenazas pueden provenir de fuentes internas o externas y pueden ser intencionales o accidentales. Algunos ejemplos de amenazas incluyen ataques cibernéticos, malware, robo o pérdida de dispositivos, errores humanos, desastres naturales, fallas en el sistema y abuso de privilegios de acceso. La identificación y comprensión de las amenazas es fundamental para desarrollar estrategias de seguridad efectivas, ya que permite implementar medidas de prevención, detección y respuesta adecuadas para proteger los activos de información y mitigar los riesgos asociados.(Alex Richar Silva Guerrero, 2021)

VULNERABILIDAD: debilidad o fallo en los sistemas, hardware, arquitectura, redes, aplicaciones o procesos de una organización que puede ser explotada por amenazas para comprometer la confidencialidad, integridad o disponibilidad de los activos de información. Las vulnerabilidades pueden surgir debido a errores de diseño, configuraciones inseguras o configuraciones por defecto, falta de parches de seguridad, falta de capacitación del personal, falta de actualizaciones.

INCIDENTE DE SEGURIDAD: se refiere a cualquier evento o acción no autorizada que compromete la confidencialidad, integridad o disponibilidad de los sistemas, datos o recursos informáticos de una organización. Estos incidentes pueden variar en gravedad y pueden incluir acciones maliciosas, errores humanos o fallas técnicas que ponen en riesgo la seguridad de la información.

DATOS SENSIBLES: se refieren a información que, si se divulga o se accede de manera no autorizada, podría causar daño, perjuicio o consecuencias negativas significativas para un individuo, una organización o una entidad. Estos datos suelen ser de naturaleza

personal o confidencial y pueden incluir información que se considera privada o que debe protegerse para garantizar la privacidad y la seguridad. Ejemplos comunes de datos sensibles incluyen:

Información personal: Datos como nombres completos, direcciones, números de identificación personal (como el número de seguridad social o el número de cédula), números de teléfono, direcciones de correo electrónico, fechas de nacimiento y datos biométricos (como huellas dactilares o imágenes faciales).

Información financiera: Datos relacionados con cuentas bancarias, números de tarjetas de crédito, historiales de transacciones financieras y saldos de cuentas.

Información de salud: Datos médicos o de salud, como historias clínicas, diagnósticos, tratamientos médicos, resultados de pruebas de laboratorio y registros de salud mental.

Información de empleo: Datos relacionados con el empleo, como historiales laborales, salarios, números de seguridad social del empleado, informes de rendimiento y registros de recursos humanos.

Información de identificación de usuario y contraseñas: Credenciales de inicio de sesión, contraseñas y otros datos de autenticación que permiten el acceso a sistemas, aplicaciones o cuentas en línea.

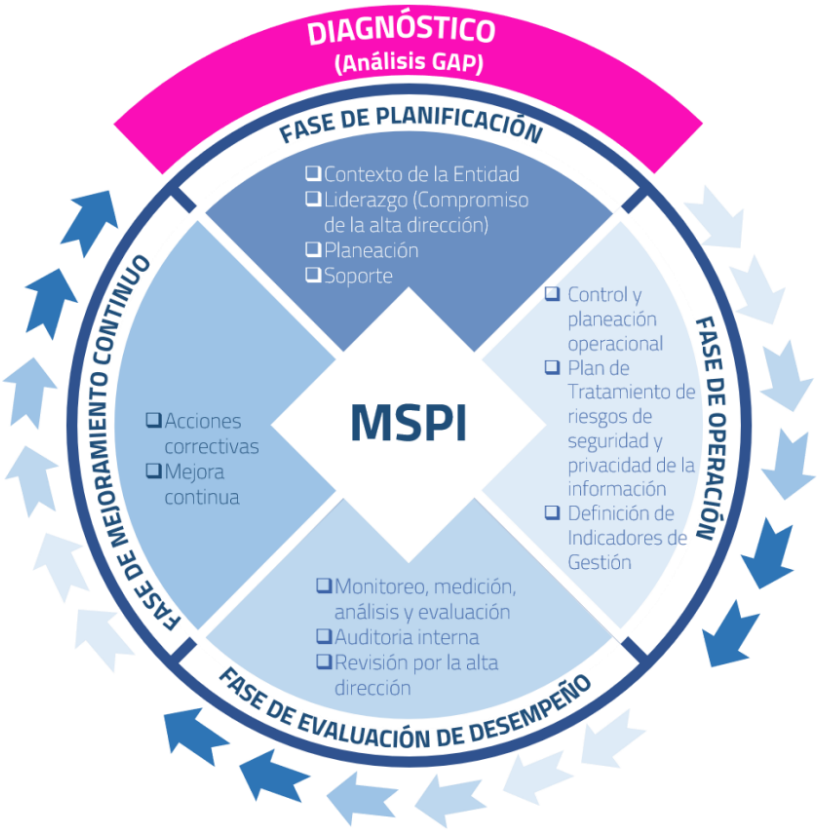
Información de propiedad intelectual: Datos relacionados con secretos comerciales, patentes, diseños, estrategias de negocio y otros activos de propiedad intelectual.

Información confidencial de la empresa: Datos comerciales confidenciales, como planes de negocios, estrategias de marketing, listas de clientes y datos financieros internos.

Información legal: Documentos legales, acuerdos de clientes, contratos, documentos judiciales y cualquier otro dato relacionado con asuntos legales o jurídicos.

Figura 1.

Ciclo MSPI



Nota. Tomado de (MINTIC, Modelo Nacional de gesti'on de riesgo de la información en entidades públicas. Anexo 4, 2021, pág. 8)

FASE 0. DIAGNOSTICO.

En esta fase es importante realizar un autodiagnóstico y entender y determinar el contexto y las necesidades reales de la organización.

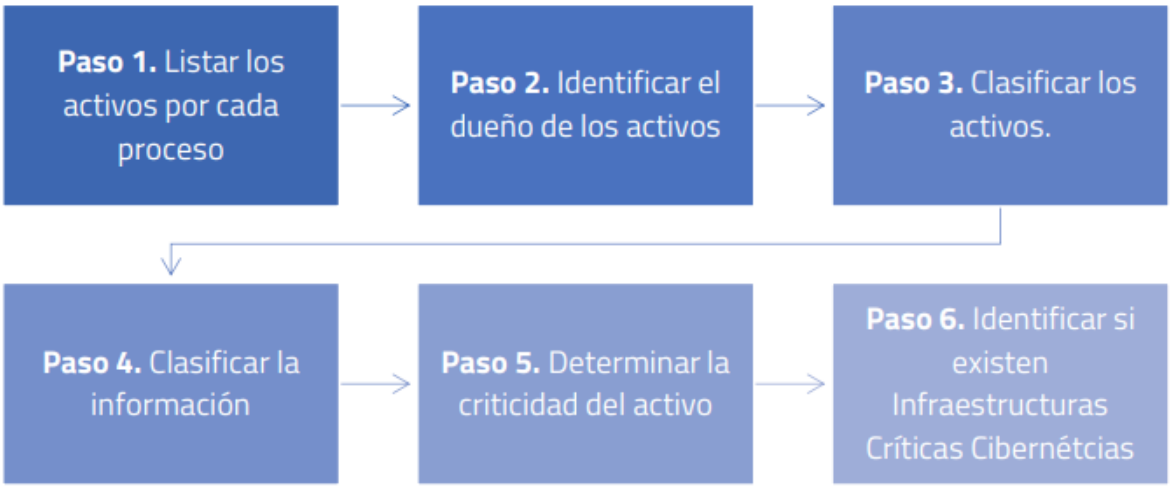
- Determinar el nivel de madurez de los controles de seguridad de la información.
- Identificar el avance de la implementación del ciclo de operación al interior de la entidad.
- Identificar el nivel de cumplimiento con la legislación vigente relacionada con protección de datos personales.
- Identificación del uso de buenas prácticas en ciberseguridad.
- Definición del contexto interno, externo y de los procesos de la entidad pública.

FASE 1. PLANIFICACIÓN DEL MSPI.

Esta fase se debe realizar después realizar la fase de diagnóstico de tener claro el contexto y las necesidades reales de la organización, para crear el Plan de Seguridad y Privacidad de la Información para que la entidad planifique el tiempo, los recursos y el presupuesto de las actividades relacionadas con el MSPI. A continuación, en la figura 2 se muestran los pasos del MSPI.

Figura 2.

Pasos MSPI



Nota. (MINTIC, Modelo nacional de gestión de riesgo de seguridad de la información en entidades públicas. anexo 4, 2021, pág. 14)

En esta fase se deben generar los siguientes documentos

- Alcance MSPI
- Acto administrativo con las funciones de seguridad y privacidad de la información.
- Política de seguridad y privacidad de la información.
- Documento de roles y responsabilidades asociadas a la seguridad y privacidad
- de la información.
- Procedimiento de inventario y Clasificación de la Información e infraestructura Crítica.
- Metodología de inventario y clasificación de la información e infraestructura Crítica.
- Procedimiento de gestión de riesgos de seguridad de la información.
- Plan de tratamiento de riesgos de seguridad de la información.

- Declaración de aplicabilidad.
- Manual de políticas de Seguridad de la Información.
- Plan de capacitación, sensibilización y comunicación de seguridad de la.

Información

FASE 2. IMPLEMENTACIÓN del MSPI.

En esta fase de debe aplicar la planificación creada en la fase anterior, poner en marcha los controles establecidos. Se esper como resultado los siguientes documentos:

- Plan de implementación de controles de seguridad y privacidad de la información.
- Evidencia de la implementación de los controles de seguridad y privacidad de la información.
- Definición de indicadores

FASE 3. EVALUACIÓN DEL DESEMPEÑO DEL MSPI.

Es fundamental que las organizaciones estén al tanto de los progresos en su gestión en cuanto a la seguridad de la información, los logros de los resultados y los objetivos propuestos.

FASE 4. MEJORAMIENTO CONTINUO

Las entidades deben desarrollar un plan de mejoramiento continuo, realizando acciones correctivas, para optimizar procesos o controles y aumentar el grado de madurez del MSPI.

5.5 Sistema de Gestión de Riesgos

Gestión del riesgo es el proceso sistemático y continuo de identificación, evaluación, tratamiento y monitoreo de los riesgos relacionados con la confidencialidad, integridad y disponibilidad de los activos de información de una organización. Este proceso implica la identificación de las amenazas potenciales, la evaluación de su probabilidad de ocurrencia y el impacto asociado, así como la implementación de medidas de control y mitigación adecuadas para reducir los riesgos a un nivel aceptable.

Identificación de riesgos: El proceso comienza con la identificación de todos los riesgos potenciales a los que la organización podría estar expuesta. Esto implica una revisión exhaustiva de las operaciones, procesos, proyectos y entorno empresarial para identificar amenazas y oportunidades.

Identificar los activos: Este es un proceso para identificar los activos que son cruciales para la organización y que afectan la confidencialidad, integridad y disponibilidad de la información.

identificar los activos es un paso fundamental en la gestión de la seguridad de la información y la gestión de riesgos. Los activos son elementos de valor para una organización, y conocerlos es esencial para protegerlos adecuadamente.

Datos y recursos de TI:

Datos confidenciales: Esto incluye información financiera, datos personales de clientes y empleados, secretos comerciales y otra información sensible.

Sistemas y aplicaciones: Identificar los sistemas, servidores y aplicaciones críticos para las operaciones de la organización.

Infraestructura de red: Identificar componentes de red como routers, switches, cortafuegos y servidores de seguridad.

Hardware y dispositivos: Incluye computadoras, servidores, impresoras, dispositivos móviles y otros dispositivos relacionados con la tecnología.

Propiedad intelectual y activos de propiedad industrial: Patentes, marcas comerciales y derechos de autor: Identificar los activos intelectuales registrados y protegerlos adecuadamente.

Diseños, investigaciones y desarrollos: Identificar activos relacionados con la investigación y el desarrollo que tengan un valor comercial.

Recursos físicos:

- Edificios e instalaciones: Identificar las ubicaciones físicas de la organización, así como las instalaciones críticas.

- Equipos físicos: Esto incluye maquinaria, vehículos y otros activos físicos utilizados en las operaciones.

Recursos humanos: Personal: Identificar a los empleados y sus roles, especialmente aquellos con acceso a información sensible o sistemas críticos.

Procesos y operaciones: Procedimientos y flujos de trabajo: Identificar los procesos operativos críticos para el negocio y cómo se relacionan con los activos mencionados anteriormente.

Contratos y acuerdos: Identificar contratos comerciales, acuerdos de socios y otros documentos legales relacionados con activos o compromisos financieros.

Reputación y marca: Reputación de la empresa y marca: La percepción de la empresa y su marca también son activos críticos.

Cumplimiento normativo y legal: Regulaciones y requisitos legales: Identificar las regulaciones y leyes aplicables a la industria y la ubicación geográfica de la organización.

Activos financieros: Dinero en efectivo, cuentas bancarias y activos financieros: Identificar los activos financieros de la organización y cómo se gestionan.

Relaciones comerciales: Clientes, proveedores y socios comerciales: Establecer y mantener un registro de las relaciones comerciales clave.

Una vez que haya identificado todos estos activos, es importante clasificarlos en función de su valor y criticidad para la organización. Esto permite priorizar la asignación de recursos para su protección y establecer medidas de seguridad adecuadas. Además, la identificación de activos es la base para llevar a cabo una evaluación de riesgos y desarrollar un plan de seguridad de la información efectivo.

Identificar amenazas: se enfoca en identificar posibles situaciones que puedan tener un impacto en los activos de información.

Identificar amenazas es un paso esencial en la gestión de la seguridad de la información y en la evaluación de riesgos. Las amenazas son eventos o circunstancias que tienen el potencial de causar daño a los activos de una organización. Aquí tienes una guía para identificar amenazas en una organización:

Amenazas físicas:

- Desastres naturales: Incluyen terremotos, inundaciones, incendios, tormentas y otros eventos climáticos extremos que pueden dañar las instalaciones y los activos físicos.
- Accidentes: Tales como explosiones, derrames químicos, colisiones vehiculares, etc., que pueden dañar propiedades y recursos físicos.

Amenazas de seguridad informática:

Malware: Software malicioso, como virus, troyanos y ransomware, que puede dañar sistemas y robar datos.

Ataques de hackers: Incluyen intentos de intrusión, robo de datos, denegación de servicio (DoS) y otros ataques informáticos.

Phishing: Correos electrónicos o mensajes falsos que engañan a los usuarios para revelar información confidencial.

Ingeniería social: Atacantes que manipulan a las personas para obtener acceso no autorizado a sistemas o información.

Vulnerabilidades de software: Deficiencias en aplicaciones y sistemas que podrían ser explotadas.

Amenazas internas:

- **Empleados deshonestos o negligentes:** Personal interno que puede involucrarse en actividades maliciosas o cometer errores que pongan en riesgo la seguridad de la información.

- **Acceso no autorizado:** Personas que tienen acceso indebido a sistemas o datos internos.
- **Sabotaje interno:** Acciones deliberadas de empleados para dañar la organización o su reputación.

Amenazas regulatorias y legales:

- **Cambios en la legislación:** Nuevas leyes o regulaciones que puedan afectar la operación de la organización.
- **Multas y sanciones legales**: Posibles consecuencias legales y financieras por incumplimiento de regulaciones.

Amenazas de terceros:

- **Competidores**: Acciones competitivas que puedan perjudicar la posición de la empresa.
- **Proveedores:** Problemas con proveedores que pueden afectar el suministro o la calidad de los productos o servicios.
- **Clientes insatisfechos:** Reclamaciones de clientes o mala publicidad que dañen la reputación de la empresa.

Amenazas de seguridad física:

Robo y vandalismo: Actos criminales que pueden afectar las instalaciones y los activos físicos de la organización.

Acceso no autorizado a instalaciones: Personas que ingresan a áreas protegidas sin autorización.

Amenazas de salud y seguridad:

- **Pandemias y enfermedades**: Eventos de salud pública que pueden afectar la disponibilidad de personal y recursos.

Amenazas geopolíticas y sociales:

- **Conflictos políticos o sociales**: Eventos que pueden tener un impacto en la estabilidad y seguridad de la organización en regiones específicas.

Amenazas económicas:

- **Fluctuaciones económicas:** Cambios en las condiciones económicas que pueden afectar la viabilidad financiera de la organización.

Una vez identificadas estas amenazas, es importante evaluar su probabilidad de ocurrencia y su impacto potencial en los activos de la organización. Esto ayudará a priorizar la gestión de riesgos y la implementación de medidas de seguridad adecuadas para mitigar estas amenazas.

Identificación de riesgos: El proceso comienza con la identificación de todos los riesgos potenciales a los que la organización podría estar expuesta. Esto implica una revisión exhaustiva de las operaciones, procesos, proyectos y entorno empresarial para identificar amenazas y oportunidades.

Evaluación de riesgos: Una vez que se han identificado los riesgos, se procede a evaluar su probabilidad de ocurrencia y su impacto potencial. Esta evaluación permite a la organización priorizar los riesgos y centrarse en aquellos que son más críticos.

Mitigación de riesgos: Con base en la evaluación de riesgos, se desarrollan estrategias y planes de mitigación. Estos pueden incluir la implementación de controles internos, cambios en los procesos operativos, la adquisición de seguros o la diversificación de las actividades comerciales.

Planificación de contingencia: A pesar de los esfuerzos de mitigación, algunos riesgos pueden materializarse. Por lo tanto, es importante desarrollar planes de contingencia para responder de manera efectiva a situaciones de crisis. Estos planes describen cómo la organización abordará y se recuperará de eventos adversos.

Monitoreo y seguimiento continuo: La gestión del riesgo no es un proceso estático; debe ser continuo y adaptable. Esto implica monitorear de manera constante los riesgos y las medidas de mitigación para asegurarse de que sigan siendo efectivos y estén alineados con los cambios en el entorno empresarial.

Comunicación y divulgación: Es fundamental comunicar la información relacionada con los riesgos y las medidas de gestión tanto dentro como fuera de la organización. Esto incluye la comunicación con partes interesadas internas y externas, como empleados, accionistas, clientes y reguladores.

Integración en la estrategia empresarial: El SGSI debe estar alineado con los objetivos y la estrategia general de la organización. Debe ser parte integral de la toma de decisiones en todos los niveles, desde la alta dirección hasta los empleados de base.

Cumplimiento normativo: Asegurarse de que la organización cumple con todas las regulaciones y leyes aplicables relacionadas con la gestión de riesgos, especialmente en industrias altamente reguladas.

Aprendizaje organizativo: Un SGSI también debe fomentar un enfoque de aprendizaje continuo. Las lecciones aprendidas de experiencias pasadas deben utilizarse para mejorar la gestión de riesgos en el futuro.

Los sistemas de gestión del riesgo son esenciales para garantizar la sostenibilidad y el éxito a largo plazo de las organizaciones, ya que ayudan a prevenir pérdidas financieras significativas, proteger la reputación de la empresa y garantizar la continuidad operativa. Además, son especialmente importantes en sectores altamente regulados, como la banca, la atención médica y la industria de la energía, donde los riesgos pueden tener un impacto grave en la sociedad en general.

Dentro de los sistemas de gestión del riesgo también es importante identificar la aceptación del riesgo y el apetito del riesgo.

Aceptación del riesgo: La aceptación del riesgo se refiere a la disposición de una organización o individuo para asumir o tolerar un cierto nivel de riesgo. En otras palabras, es la decisión consciente de una entidad de aceptar los posibles impactos negativos que puedan surgir de una actividad o decisión, en lugar de tomar medidas para evitar completamente esos riesgos. Esto puede deberse a una evaluación de costos y beneficios, donde se considera que los beneficios superan los riesgos asumidos.

Apetito por el riesgo: El apetito por el riesgo es una expresión de la cantidad y tipo de riesgo que una organización está dispuesta a tomar en la búsqueda de sus objetivos y metas. Es una declaración formal o informal de los límites y preferencias de una entidad en relación con el riesgo. Por ejemplo, algunas organizaciones pueden tener un alto apetito por el riesgo y estar dispuestas a asumir riesgos significativos en busca de mayores ganancias, mientras que otras pueden tener un apetito por el riesgo más bajo y priorizar la seguridad y la estabilidad.

En la gestión de riesgos, se utilizan diferentes tipos de controles para reducir la probabilidad de que ocurran riesgos y minimizar su impacto si llegan a ocurrir. Los controles de gestión de riesgos se pueden clasificar en varias categorías según su función y propósito. A continuación, se nombran algunos tipos de controles de gestión de riesgo.

Controles Preventivos:

Estos controles se implementan para evitar que los riesgos se materialicen. incluyen políticas y procedimientos, revisiones de diseño, capacitación y educación, y medidas de seguridad física.

Controles Detectivos:

Los controles detectivos están diseñados para identificar riesgos en una etapa temprana. incorpora sistemas de detección de intrusos, auditorías y revisiones periódicas, y sistemas de supervisión.

Controles Correctivos:

Estos controles se aplican para corregir y mitigar el impacto de un riesgo una vez que ha ocurrido. comprende planes de respuesta a incidentes, sistemas de recuperación de desastres y acciones de remediación.

Controles de Transferencia de Riesgos:

La transferencia de riesgos implica externalizar o transferir el riesgo a terceros, como a través de seguros o acuerdos contractuales.

Controles de Aceptación de Riesgos:

En algunos casos, una organización puede decidir aceptar un riesgo si su impacto es bajo o si los costos de mitigación superan los beneficios esperados. En tales casos, se documenta la decisión y se monitorea el riesgo.

Controles de Mitigación de Riesgos:

Estos controles se implementan específicamente para reducir el impacto de un riesgo. Pueden incluir cambios en procesos, tecnologías o recursos.

Controles de Monitoreo Continuo:

La supervisión continua y la revisión de los riesgos y los controles son esenciales para garantizar que la gestión de riesgos sea efectiva. Esto puede implicar la automatización de la supervisión y alertas en tiempo real.

Controles de Evaluación de Riesgos:

Los controles de evaluación de riesgos son herramientas y métodos utilizados para identificar, evaluar y clasificar riesgos. Esto puede incluir análisis cualitativos y cuantitativos de riesgos.

Controles de Comunicación de Riesgos:

La comunicación efectiva de riesgos es fundamental. Los controles de comunicación de riesgos implican informar a las partes interesadas sobre los riesgos, su probabilidad e impacto, y las medidas de control implementadas.

Controles de Respuesta a Riesgos:

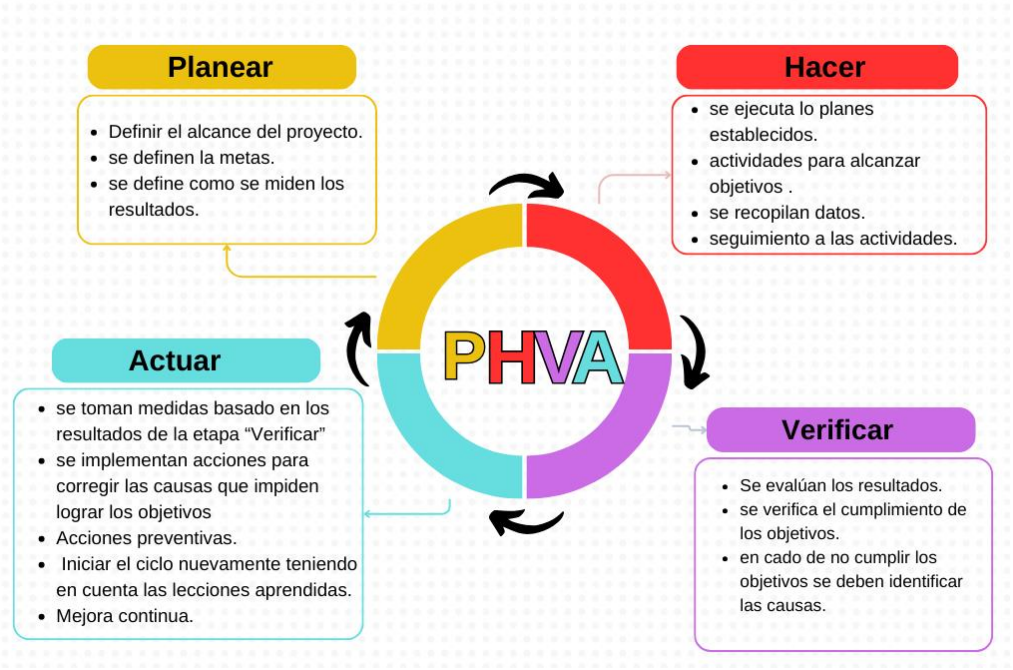
Estos controles se activan en respuesta a eventos de riesgo. Pueden incluir planes de respuesta, estrategias de recuperación y acciones específicas para mitigar el impacto. La selección y aplicación de estos controles dependerá de la naturaleza de los riesgos

identificados y de la estrategia de gestión de riesgos de la organización. Es importante tener un enfoque holístico para la gestión de riesgos que incluya la identificación, evaluación, tratamiento y seguimiento de los riesgos a lo largo del tiempo.

Tanto los sistemas de gestión de seguridad de la información como, la norma ISO/IEC 27001 y el modelo MSPI (modelo de seguridad y privacidad de la información) hace uso de una buena práctica basada en el modelo PHVA (Planear, Hacer; Verificar, Actuar) o sus siglas en ingles PDCA (Plan, Do, Check, Act).

Figura 3.

Ciclo PHVA



Planificar (Plan): En esta etapa, se establecen los objetivos y metas del proceso o proyecto. Se identifican los recursos necesarios, se desarrollan planes y se define cómo se

medirán los resultados. También se consideran los riesgos y se establecen estrategias para abordarlos.

Hacer (Do): En esta etapa, se ejecutan los planes establecidos en la fase de planificación. Se llevan a cabo las actividades necesarias para alcanzar los objetivos del proyecto o proceso. Es importante recopilar datos y realizar un seguimiento de las actividades en esta etapa.

Verificar (Check): En esta etapa, se evalúan los resultados y se comparan con los objetivos establecidos en la fase de planificación. Se analizan los datos recopilados durante la etapa "Hacer" para determinar si se están cumpliendo los objetivos. Si los resultados no son satisfactorios, se identifican las causas y se proponen correcciones.

Actuar (Act): En esta etapa, se toman medidas basadas en los resultados de la fase "Verificar". Si se identifican áreas de mejora o problemas, se implementan acciones correctivas y preventivas. Luego, el ciclo comienza de nuevo, y se ajustan los planes y procesos según sea necesario para mejorar continuamente.

El ciclo PHVA es una metodología ampliamente utilizada en la gestión de calidad y la mejora continua de procesos. Ayuda a las organizaciones a identificar oportunidades de mejora, resolver problemas y mantener un enfoque constante en la eficiencia y la calidad en todas sus actividades. También se conoce como el ciclo de Deming

6. Metodología

6.1 Enfoque metodológico

El presente trabajo se realiza bajo el enfoque metodológico mixto ya que busca realizar una recolección y análisis de información, para entender el contexto y especificaciones de la entidad (componente cualitativo) y de esta manera lograr una mejor adaptación del modelo de seguridad de la información (componente cuantitativo).

6.2 Tipo de Estudio

El tipo de estudio empleado en este trabajo es de tipo descriptivo ya que a través de esta se permite describir la estrategia correcta para dar manejo y ayudar a reducir las riesgos y problemas en seguridad de la información que pueda afrontar la Dirección Territorial de Salud de Caldas de acuerdo a sus necesidades específicas.

6.3 Procedimiento

Para ejecutar el proyecto se llevarán a cabo las siguientes fases y actividades que permitirán a la Dirección territorial de salud de caldas una mejor gestión de sus activos de información y de esta manera mantener la confidencialidad, disponibilidad e integridad de estos.

Fase1. Diagnóstico

Determinar el estado actual de la gestión de seguridad de la información de la Dirección Territorial de Salud de Caldas.

- Para evaluar el nivel de madurez del MSPI en la entidad se utilizará la herramienta proporcionada por MINTIC formato llamado “Instrumento de evaluación MSPI”.

Fase 2. Identificación

Realizar la identificación y clasificación de los activos de información.

para la identificación y clasificación de los activos, para cumplir con esta actividad fue necesario recopilar información sobre los activos de información de la organización. Esto implico revisar registros, documentación existente, entrevistar a personal clave del área de tecnologías de la información de la entidad

- Identificar los activos: se implementó un formato adaptado del MSPI para la identificación de los activos, su clasificación y etiquetado.

Fase3. Gestión del riesgo

La identificación de riesgos es un paso fundamental en la gestión de riesgos, ya que permite a una organización identificar y comprender los posibles peligros o amenazas que podrían afectar sus objetivos y operaciones.

- Contexto de la organización
- Definir los criterios de riesgo: se establecen criterios claros para identificar y evaluar los riesgos. Esto incluye la probabilidad de ocurrencia, el impacto potencial.
- Identificar los riesgos
- Gestionar los riesgos de seguridad en el área de Tecnología de la entidad.

Fase4. Definir controles

- Establecer controles: se definen los controles de seguridad adecuados para mitigar los riesgos identificados. Los controles incluyen medidas técnicas, organizativas y físicas.
- Políticas aplicables bajo las normas respectivas.

6.4 Alcance de la investigación

Diseño de un sistema de Gestión de seguridad de la información y privacidad de la información para la Dirección territorial de salud de caldas, para identificar y gestionar los riesgos del área de tecnologías de la entidad

Contexto de la entidad

Por Decreto Nacional No. 786 de marzo 25 de 1966, se entrega al Servicio Seccional de Salud de Caldas con la Beneficencia de Manizales, los hospitales de todo el departamento, los asilos de ancianos, las instituciones de rehabilitación, las entidades de asistencia social, los organismos dependientes de la Secretaría Departamental de Salud Pública de Caldas, los distritos de salud y los centros y puestos de salud en todo el Departamento.

El 31 de julio de 1967, se aprobó el contrato fundamental de descentralización administrativa con la presencia del Ministerio de Salud Pública. Esto significa que se tendrá más autonomía para administrar el Servicio de Salud y que las Juntas Seccionales de Salud podrán resolver los problemas de manera efectiva, a través de la ordenanza número 02 del 19 de octubre de 1990.

MISIÓN: La Dirección Territorial de Salud de Caldas, es la entidad descentralizada encargada de la rectoría del Sistema General de Seguridad Social en Salud en el Departamento de Caldas, cuyo objetivo principal es realizar las acciones de Asistencia Técnica

e Inspección Vigilancia y Control (IVC) en el cumplimiento de las funciones de Salud Pública, Prestación de Servicios y Aseguramiento.

VISIÓN: En el año 2024 el departamento de Caldas, será reconocido en materia de salud a nivel nacional por su aporte al mejoramiento de los modos, condiciones y estilos de vida de las personas, familias y comunidades caldenses, con la reducción de la morbilidad y mortalidad en todos los grupos poblacionales con un enfoque incluyente, participativo y fundamentado en cuatro líneas estratégicas: en atención integral , transectorialidad de la salud, atención integral, promoción y participación social y fortalecimiento institucional, que permitan impactar los determinantes sociales y de esta manera, avanzar hacia el logro de la equidad en salud.

Figura 4

Organigrama DTSC

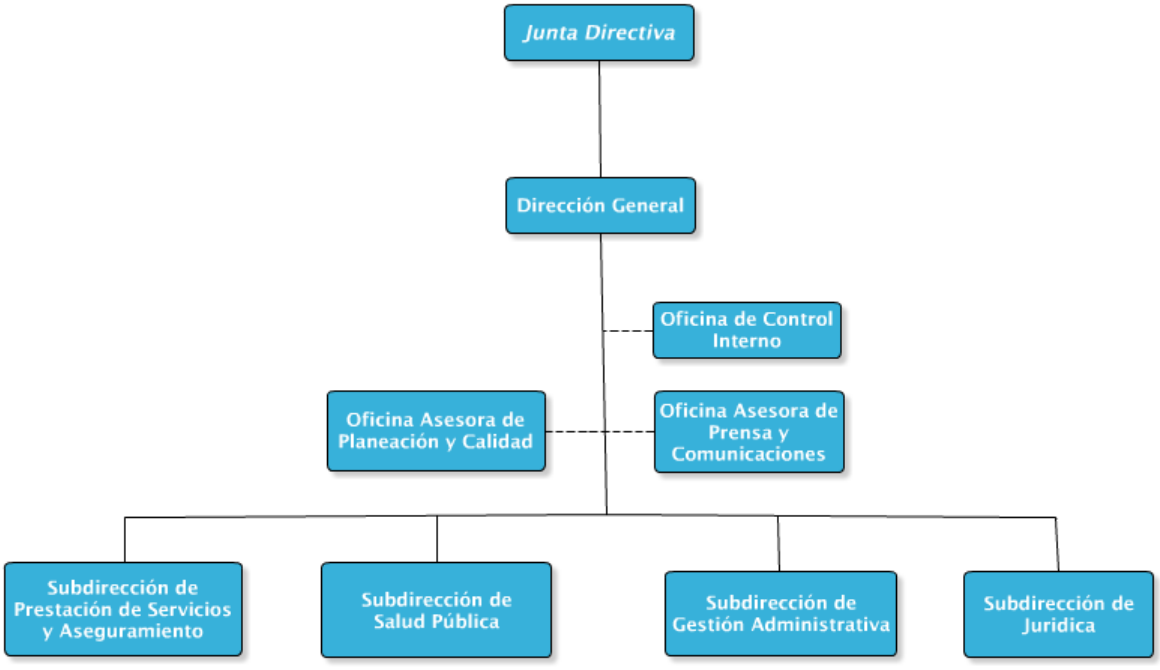


Figura 5

Portafolio de servicios DTSC

Asistencias técnicas: Uno de los principales servicios de la Dirección Territorial de Salud de Caldas es brindar asistencia técnica a los diversos actores del sector salud en el Departamento de Caldas.

Inspección Vigilancia y control: Inspección vigilancia y control de los factores de riesgo del ambiente (físico, químicos, biológicos, sociales y sicosociales) que pueden afectar la salud de la población caldense, mediante la intervención positiva de los determinantes sanitarios, ambientales y sociales en aras de mejorar el bienestar y la calidad de vida de toda la población.

Gestión PPNA: El objetivo de este servicio es asegurar que la población pobre no asegurada reciba servicios y tecnologías en salud que no están cubiertas por la UPC del régimen subsidiado. Para garantizar la prestación de servicios a los usuarios competencia de la DTSC, se realizan contrataciones (red pública del departamento) o se establecen articulaciones

con las EPSS. Adicionalmente, se realizan auditorías continuas para garantizar que la prestación de servicios de salud se lleve a cabo de manera efectiva, accesible y de calidad.

Laboratorio de salud pública: Tiene como objetivo brindar información, acompañar a la Red de Laboratorios clínicos, de citología de cuello uterino, del departamento de Caldas, a través de Evaluación Externa Indirecta del Desempeño en enfermedades de interés en salud pública (Control de calidad), además de los laboratorios de control de calidad de las empresas de alimentos, laboratorios de plantas de tratamiento de agua potable inscrito en la red nacional de Laboratorios.

7. Resultados

Fase 1. Diagnóstico de la Dirección territorial de salud de caldas en cuanto a la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI).

Esta fase inicial permite determinar el estado en que se encuentra la implementación del modelo de seguridad y privacidad de la información en la Dirección territorial de salud de caldas, para esto se usaron los instrumentos proporcionados por el ministerio de las tecnologías de la información y las comunicaciones MINTIC denominado “instrumento de evaluación del MSPI” Identificación del nivel de madurez de la Dirección territorial de salud de caldas en cuanto a la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI)

Como se muestra en la tabla 1 y de acuerdo con el instrumento de evaluación MSPI, esta calificación representa los valores obtenidos por la entidad en cuanto a la efectividad de los controles en cada uno de los dominios frente a la normativa NTC/ISO 27001 de 2013, teniendo en cuenta la evaluación de los componentes administrativos y técnicos implementados por la entidad, esta información fue generada a partir de diligenciamiento del “instrumento de evaluación MSPI” los valores y calificación de la información se dieron gracias a recolección de la información, la observación y a través de entrevistas con el líder de TI de la dirección territorial de salud de caldas, donde se muestra evaluación de la madurez en seguridad y privacidad de la información en la Dirección Territorial de salud de Caldas, obteniendo la evaluación de la competencia técnica, procesos sostenibles y eficiencia interna. Se estableció una línea base para definir las actividades de seguridad mediante la evaluación del MSPI, reflejada en el Anexo 1 identificando el estado actual de la entidad, respondiendo a

los puntos que aparecen en los apartados del instrumento de evaluación MSPI dado por MINTIC.

De acuerdo a la calificación obtenida por la entidad de 70 puntos la entidad se encuentra en un estado intermedio de adopción e implementación del modelo de seguridad y privacidad de la información, pero aún falta la implementación de algunos controles con el fin de fortalecer y disminuir las brechas de seguridad y privacidad de la información.

Tabla 1.

Evaluación efectividad de los controles

No.	Evaluación de Efectividad de controles			
	DOMINIO	**Calificación Actual**	**Calificación Objetivo**	**EVALUACIÓN DE EFECTIVIDAD DE CONTROL**
A.5	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	60	100	**EFECTIVO**
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	53	100	**EFECTIVO**
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	52	100	**EFECTIVO**
A.8	GESTIÓN DE ACTIVOS	89	100	**OPTIMIZADO**
A.9	CONTROL DE ACCESO	96	100	**OPTIMIZADO**
A.10	CRIPTOGRAFÍA	0	100	**INEXISTENTE**
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	82	100	**OPTIMIZADO**
A.12	SEGURIDAD DE LAS OPERACIONES	81	100	**OPTIMIZADO**
A.13	SEGURIDAD DE LAS COMUNICACIONES	79	100	**GESTIONADO**
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	75	100	**GESTIONADO**
A.15	RELACIONES CON LOS PROVEEDORES	100	100	**OPTIMIZADO**
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	77	100	**GESTIONADO**
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	50	100	**EFECTIVO**
A.18	CUMPLIMIENTO	85	100	**OPTIMIZADO**
PROMEDIO EVALUACIÓN DE CONTROLES		**70**	**100**	**GESTIONADO**

Nota. (MINTIC, portada “instrumento de evaluación MSPI”, 2016)

De acuerdo a los resultados obtenidos en la tabla 1. se obtiene la gráfica para evidenciar la brecha existente frente a la norma ISO 27001:2013

Tabla 2.

Brecha anexo A ISO 27001:2013

Nota. (MINTIC, portada “instrumento de evaluación MSPI”, 2016)

Con base en los resultados obtenidos de los componentes administrativos y técnicos se determina la calificación de los dominios, permitiendo establecer la brecha de estos frente a la norma NTC/ISO 27001:2013, así logrando determinar cuáles de estos requieren un fortalecimiento con el fin de mejorar el nivel de madurez e implementación del modelo de seguridad y privacidad de la información (MSPI), dentro de estos dominios se encuentra que el A.10 criptografía es uno de los que requiere ser gestionado ya que se encuentra con una calificación de 0 puntos, seguido del A.17 aspectos de seguridad de la información de la gestión de la continuidad del negocio, A.7 seguridad de los recursos humanos, A.6

organización de la seguridad de la información, A.5. políticas de seguridad de la información, estos son los dominós que deben ser gestionados para mejorar el nivel de madurez de la seguridad y privacidad de la información.

En cuento al avance del ciclo PHVA la entidad obtuvo una calificación del 53% como se muestra en la tabla 4, la calificación para cada uno de las etapas del ciclo obteniendo en el componente de planificación una puntuación de 28%, implementación 10%, evaluación y desempeño 3% y en el componente de mejora continua un 12%, se evidencia que no se ha dado el cumplimiento de los plazos establecidos en el decreto 1008 de 2018, puesto que para el año 2018 se debería tener una adopción del 100%, como se muestra en la tabla 3.

Tabla 3.

Tiempos avance PHVA

TIPO DE ENTIDAD	2015	2016	2017	2018	2019	2020
De Orden Nacional	40%	60%	80%	100%	Mantener 100%	Mantener 100%
De Orden Territorial A	35%	50%	80%	100%	Mantener 100%	Mantener 100%
De Orden Territorial B y C	10%	30%	50%	65%	80%	100%

Fuente: Documento Modelo de Seguridad y Privacidad de la Información MSPI, de Mintic

Tabla 4

avance PHVA - DTSC

Año	AVANCE PHVA		
	COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
2020	Planificación	28%	40%
	Implementación	10%	20%
	Evaluación de desempeño	3%	20%
	Mejora continua	12%	20%
TOTAL		53%	100%

Nota. (MINTIC, portada “instrumento de evaluación MSPI”, 2016)

Fase 2. Identificación y clasificación de los activos de información de la Dirección territorial de salud de caldas.

para esta fase se elaboró un formato donde a cada activo se le asigna un código de manera consecutiva, se identifica y nombra el activo de información, una breve descripción de que es este, ubicación del activo, propietario, custodio de la información, luego se determina el nivel de importancia de cada activo haciendo una clasificación de estos teniendo en cuenta los pilares de la seguridad informática, la triada (CID) Confidencialidad, Integridad, Disponibilidad. Se adapta del modelo de seguridad y privacidad de la información (MSPI) las escalas de calificación para una más fácil comprensión de la valoración de cada uno de los componentes.

A continuación, se describen los criterios y parámetros de evaluación de los activos de información y así poder a partir de estos determinar el nivel de importancia del activo frente a cada uno de los pilares de la información.

Tabla 5

Parámetros de evaluación de los activos

CONFIDENCIALIDAD		INTEGRIDAD		DISPONIBILIDAD	
Información pública reservada (5)	Información disponible sólo para un proceso de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica.	Alta (5)	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas de la entidad.	Alta (5)	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas a entes externos.
Información pública clasificada (3)	Información disponible para todos los procesos de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo para los procesos de la misma. Esta información es propia de la entidad o de terceros y puede ser utilizada por todos los funcionarios de la entidad para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del propietario.	Media (3)	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado a funcionarios de la entidad.	Media (3)	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado de la entidad.
Información pública (1)	nformación 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.	Baja (1)	Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo para la entidad o entes externos.	Baja (1)	La no disponibilidad de la información puede afectar la operación normal de la entidad o entes externos, pero no conlleva implicaciones legales, económicas o de pérdida de imagen.

Nota. Adaptado de (MINTIC, Inventario y clasificación de activos de información e infraestructura critica cibernética nacional, 2021)

el nivel de importancia de los activos de información se identifica de la siguiente manera, posterior al evaluar los criterios referentes a la confidencialidad, disponibilidad e integridad de los activos, se realiza una sumatoria del resultado de cada uno de los pilares de la seguridad de la información, y se clasifican según los criterios definidos en la siguiente tabla.

Tabla 6

Nivel de importancia de los activos

Nivel de importancia	Criterio
ALTA	Activos de información en los cuales su clasificación es mayor a 10
MEDIA	Activos de información en los cuales su clasificación menor o igual a 10 o mayor o igual a 6
BAJA	Activos de información en los cuales su clasificación es menor a 6

Nota. Adaptado de (MINTIC, Inventario y clasificación de activos de información e infraestructura critica cibernética nacional, 2021)

Fase 3. Identificar los riesgos de la Dirección territorial de salud de caldas.

Para la identificación de los riesgos se diseñó una plantilla donde se evalúan los diferentes escenarios de riesgo con base en su probabilidad de ocurrencia y el impacto que tendría en la organización si se materializa la amenaza, posterior a esto se vuelve a evaluar después de aplicar los controles y realizar la evaluación de estos teniendo en cuenta la tabla 13 donde se establen los criterios de valoración de los controles para así obtener el riesgo inherente.

Figura 6.

Factores asociados al riesgo

Activo: Cualquier elemento o recurso de la organización que tiene valor y debe ser protegido. En seguridad informática, los activos de información pueden incluir datos, hardware, software, infraestructura de red, documentos y cualquier otro elemento relacionado con la información.

Amenaza: Cualquier evento o circunstancia que tiene el potencial de causar daño o pérdida a los activos de información. Puede ser intencional (como un ataque cibernético) o no intencional (como un desastre natural).

Vulnerabilidad: Una debilidad o fallo en un sistema, proceso o procedimiento de seguridad que puede ser explotado por una amenaza para comprometer la confidencialidad, integridad o disponibilidad de un activo de información.

Probabilidad: La medida de la posibilidad de que una amenaza específica explote una vulnerabilidad y cause un impacto negativo en los activos de información. Puede expresarse en términos cualitativos (baja, moderada, alta) o cuantitativos (porcentaje).

Impacto: La consecuencia o resultado de una amenaza que se materializa y afecta a un activo de información. El impacto puede manifestarse en términos de pérdida financiera, daño a la reputación, interrupción de operaciones, entre otros efectos negativos.

Se definen los criterios de evaluación de la probabilidad de ocurrencia a través de escalas de probabilidad donde se establece una escala que represente los diferentes niveles de probabilidad de ocurrencia de un evento como se muestra en la tabla 7. considerar factores relevantes Identificando los que pueden influir en la probabilidad de ocurrencia de un evento. A través de la frecuencia histórica de eventos similares, las vulnerabilidades conocidas en los sistemas de información, las amenazas y riesgos identificados tanto al interior como al exterior de la entidad.

Tabla 7

Criterios de evaluación de probabilidades

CRITERIOS DE EVALUACIÓN DE PROBABILIDADES		
VALOR	**PROBABILIDAD**	**DESCRIPCIÓN**
5	Casi seguro	Más de 20 veces al año
4	Probable	entre 15 y 20 veces al año
3	Posible	Entre 10 y 15 veces al año
2	Improbable	Entre 2 y 9 veces al año
1	Raro	ocurre 1 vez al año

Se define los criterios de evaluación del impacto

Tabla 8

Criterios de evaluación del impacto

Niveles de Impacto para Confidencialidad	Niveles de Impacto para Integridad	Niveles de Impacto para Disponibilidad
Nivel 1: Insignificante	Nivel 1: Insignificante	Nivel 1: Insignificante
- La divulgación no autorizada tiene un impacto mínimo y no afecta significativamente a la confidencialidad de la información.	- Modificaciones no autorizadas tienen un impacto mínimo y no afectan significativamente a la integridad de los datos.	- Interrupciones no planificadas tienen un impacto mínimo y no afectan significativamente a la disponibilidad de los servicios.
Nivel 2: Menor	Nivel 2: Menor	Nivel 2: Menor
- La divulgación no autorizada tiene un impacto limitado, pero puede tener consecuencias menores en la confidencialidad de la información.	- Modificaciones no autorizadas tienen un impacto limitado y pueden afectar parcialmente la integridad de los datos.	- Interrupciones no planificadas tienen un impacto limitado y pueden afectar parcialmente la disponibilidad de los servicios.
Nivel 3: Moderado	Nivel 3: Moderado	Nivel 3: Moderad o
- La divulgación no autorizada tiene consecuencias significativas y afecta parcialmente la confidencialidad de la información.	- Modificaciones no autorizadas tienen consecuencias significativas y afectan parcialmente la integridad de los datos.	- Interrupciones no planificadas tienen consecuencias significativas y afectan parcialmente la disponibilidad de los servicios.
Nivel 4: Mayor	Nivel 4: Mayor	Nivel 4: Mayor
- La divulgación no autorizada tiene un impacto severo y afecta significativamente la confidencialidad de la información.	- Modificaciones no autorizadas tienen un impacto severo y afectan significativamente la integridad de los datos.	- Interrupciones no planificadas tienen un impacto severo y afectan significativamente la disponibilidad de los servicios.
Nivel 5: Catastrófico	Nivel 5: Catastrófico	Nivel 5: Catastrófico
- La divulgación no autorizada tiene un impacto crítico y tiene consecuencias catastróficas en la confidencialidad de la información.	- Modificaciones no autorizadas tienen un impacto crítico y tienen consecuencias catastróficas en la integridad de los datos.	- Interrupciones no planificadas tienen un impacto crítico y tienen consecuencias catastróficas en la disponibilidad de los servicios.

Se definen los criterios de aceptabilidad del riesgo tabla 9, ya que estos criterios de aceptación del riesgo en un Sistema de Gestión de Seguridad de la Información (SGSI) son los umbrales predefinidos que establecen cuándo un riesgo es aceptable para la organización y brindan una clara indicación de cuándo se deben tomar medidas adicionales para mitigarlo, y si el nivel de riesgo es aceptable y la organización lo asume ya se su atención o solución representa un gasto elevado frente al beneficio que otorga en cuanto a la seguridad de la información

Tabla 9

Criterios de aceptabilidad del riesgo

CRITERIOS DE ACEPTABILIDAD DEL RIESGO			
MAPA DE CALOR	**CRITERIO**	**DESCRIPCIÓN**	ACCIONES
	ACEPTABLE	Vulnerabilidad < 25%	Mantener los controles existentes de forma eficaz
	TOLERABLE	Vulnerabilidad entre el 25 y el 50%	Implementar controles de forma secundaria y/o mejorar los controles existentes
	INACEPTABLE	Vulnerabilidad superior al 50%	Implementar controles de forma prioritaria y/o mejorar los controles existentes

Después de identificar y valorar los riesgos teniendo en cuenta la probabilidad de ocurrencia por el impacto que podría ocasionar la materialización de estos se obtiene la matriz de riesgos inherente, es de considerar que los riesgos identificados en la entidad corresponden a 11 riegos los cuales son evaluados por separado para cada uno de los activos identificados

en el área de sistemas de la dirección territorial de salud de Caldas ya que cada activo tiene una valoración diferente frente al impacto que pueda ocasionar la ocurrencia de un incidente de seguridad de la información, lo que supone que en la matriz de riesgos se encuentra 231 puntos ubicando el riesgo de cada activo de información.

El mapa de calor tabla10 surge de calificar y determinar el impacto que tendría cada amenaza en caso de materializarse, evaluando el daño potencial en términos de perdida financiera, daño a la reputación, interrupción del ejercicio normal de las funciones específicas de la entidad, este cálculo se realiza por cada combinación de una amenaza contra cada activo, Probabilidad de ocurrencia por impacto.

Tabla 10

Mapa de riesgos inherente

Matriz de Calificación, Evaluación y respuesta a los Riesgos (Inherente)						
MAPA DE CALOR INHERENTE		IMPACTO				
		Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
PROBABILIDAD	Raro (1)	6	22	22	28	65
	Improbable (2)	1	4	5	4	15
	Posible (3)	0	0	0	0	0
	Probable (4)	0	0	0	0	0

	Casi seguro (5)	0	10	9	0	40

B	**ZONA DE RIESGO BAJA**		Asumir el riesgo	33
M	**ZONA DE RIESGO MODERADA**		Asumir el riesgo, Reducir el riesgo	27
A	**ZONA DE RIESGO ALTO**		Reducir, evitar, compartir	107
E	**ZONA DE RIESGO EXTREMO**		Reducir, evitar, compartir, transferir el riesgo	64
			Total	231

Después de identificar los controles aplicables a los riesgos identificados y valorar nuevamente la probabilidad de ocurrencia por el impacto se obtuvo la matriz de riesgos residual

Tabla 11

Matriz de riesgo residual

Matriz de Calificación, Evaluación y respuesta a los Riesgos (Residual)						
MAPA DE CALOR RESIDUAL		**IMPACTO**				
		Insignificante (1)	**Menor (2)**	**Moderado (3)**	**Mayor (4)**	**Catastrófico (5)**
PROBABILIDAD	**Raro (1)**	**42**	**126**	**0**	**0**	**0**
	Improbable (2)	**0**	**0**	**3**	**20**	**0**
	Posible (3)	**0**	**1**	**39**	**0**	**0**
	Probable (4)	**0**	**0**	**0**	**0**	**0**

	Casi seguro (5)	**0**	**0**	**0**	**0**	**0**
B	**ZONA DE RIESGO BAJA**		Asumir el riesgo			168
M	**ZONA DE RIESGO MODERADA**		Asumir el riesgo, Reducir el riesgo			4
A	**ZONA DE RIESGO ALTO**		Reducir, evitar, compartir			59
E	**ZONA DE RIESGO EXTREMO**		Reducir, evitar, compartir, transferir el riesgo			0
					Total	231

Clasificación de los controles según su tipología

Tabla 12

Clasificación de controles según tipología

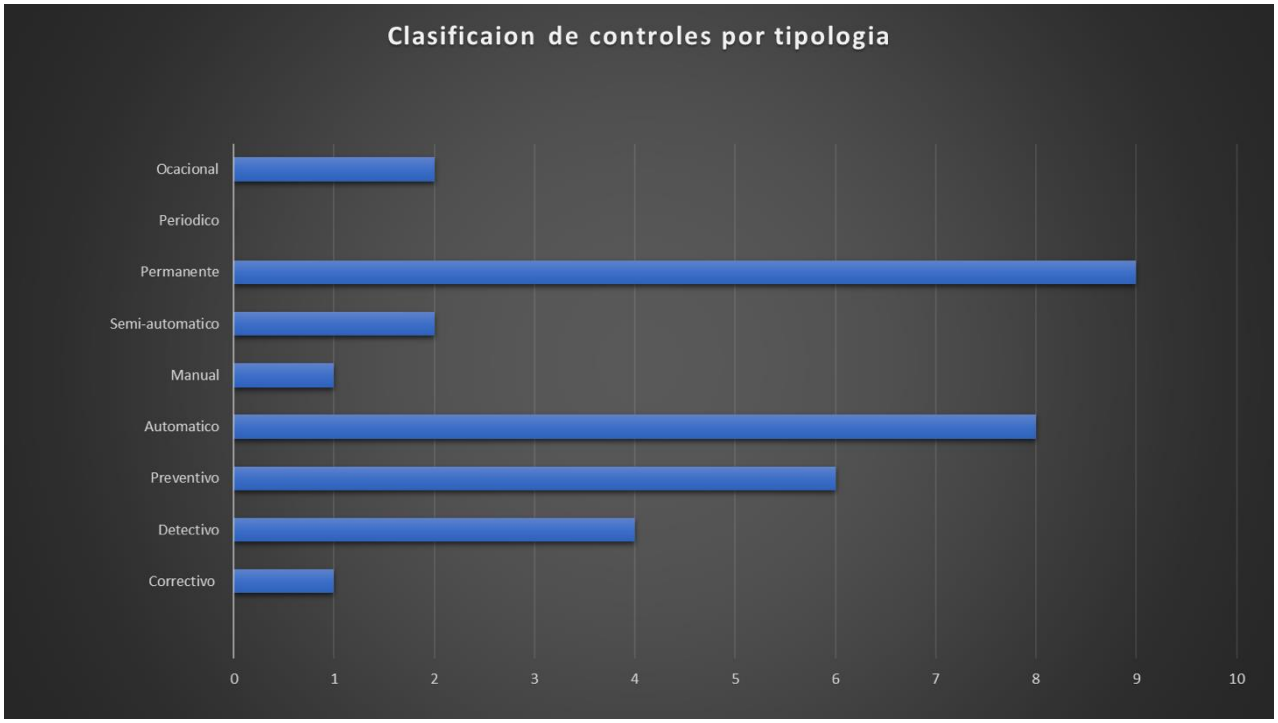
Oportunidad de aplicación	Correctivo	1
	Detectivo	4
	Preventivo	6
Automatización	Automático	8
	Manual	1
	Semiautomático	2
Periodicidad de aplicación	Permanente	9
	Periódico	0
	Ocasional	2

como se muestra en la tabla 12 control correctivo: Estos controles se implementan después de que se haya producido un incidente o una vulnerabilidad en la seguridad de la información. Su objetivo es corregir la situación y restaurar la normalidad lo más rápido posible. Por ejemplo, la aplicación de parches de seguridad después de una brecha de seguridad. Control detectivo: Estos controles están diseñados para identificar y detectar posibles incidentes o vulnerabilidades en la seguridad de la información después de que hayan ocurrido. Su objetivo es detectar eventos no autorizados o anómalos lo antes posible para poder responder adecuadamente. Por ejemplo, la implementación de sistemas de detección de intrusiones. Control preventivo: Estos controles están diseñados para evitar que ocurran incidentes de seguridad de la información. Su objetivo es mitigar los riesgos y evitar que las amenazas afecten a los activos de información. Por ejemplo, la aplicación de políticas de acceso restrictivas y la capacitación del personal en seguridad de la información. Automático: Estos controles se ejecutan de manera automática sin intervención humana directa. Se activan según ciertas condiciones predefinidas o eventos. Por ejemplo, la configuración de firewalls para bloquear automáticamente el tráfico malicioso. Manual: Estos controles requieren intervención humana directa para su ejecución. Se basan en procedimientos manuales y dependen de la acción y supervisión del personal. Por ejemplo, la revisión manual de registros de seguridad. Semi-automático: Estos controles combinan elementos automáticos y manuales. Algunas partes del proceso pueden ser automatizadas, mientras que otras requieren intervención humana. Por ejemplo, la revisión automática de registros de seguridad seguida de una verificación manual por parte del personal de seguridad. Permanente: Estos controles están en vigor de forma continua y constante. Se aplican de manera continua para garantizar la seguridad de la información en todo momento. Por ejemplo, la monitorización continua de la red y los sistemas. Control periódico: Estos controles se aplican en intervalos regulares según un calendario predefinido. Se realizan de manera programada para mantener la seguridad de la información a lo largo del tiempo. Por ejemplo, la realización de auditorías de seguridad

anuales. Control ocasional: Estos controles se aplican en situaciones específicas o eventos puntuales que requieren medidas de seguridad adicionales. No son parte de las operaciones regulares del SGSI, sino que se activan según sea necesario. Por ejemplo, la implementación de controles temporales durante la migración de datos.

Figura 7.

Clasificación de controles por tipología



Se definen los criterios de valoración de los controles

Tabla 13.

Criterios de valoración de los controles

CRITERIOS DE VALORACIÓN DE CONTROLES			
CALIFICACIÓN DE LA EFICIENCIA DEL CONTROL	**RANGO DE EFICIENCIA**	**MAPA DE CALOR**	**DESCRIPCIÓN**
ALTA	>=50%		El control presenta un adecuado diseño. Disminuye 2 niveles
MEDIA	ENTRE EL 20% Y EL 50%		El control presenta un buen diseño susceptible de ser mejorado. Disminuye 1 nivel
BAJA	<=20%		El control presenta deficiencias en su diseño. No disminuye ningún nivel

Es importante evaluar los controles ya que permite determinar si los controles de seguridad implementados están funcionando como se espera. Esto ayuda a identificar posibles deficiencias o áreas donde los controles pueden no ser efectivos en la protección de los activos de información, evaluar si el riesgo residual después de aplicar los controles es aceptable para la entidad o si es necesario actualizar o reemplazar los controles establecidos inicialmente, además permite realizar una adecuada gestión de los recursos y priorizar las inversiones.

Gestionar los riesgos de seguridad en el área de Tecnología de la entidad, en este paso se realizan en el mismo formato donde se definieron los controles para disminuir la probabilidad y el e impacto de cada uno de los escenarios de riesgo, y permite calcular el riesgo residual.

A continuación, se describen los tipos de vulnerabilidades y amenaza conocidas que afectan a diferentes tipos de activos.

Tabla 14

Amenazas y vulnerabilidades conocidas

TIPO DE ACTIVO	EJEMPLOS DE VULNERABILIDADES	EJEMPLOS DE AMENAZAS
HARDWARE	Poco mantenimiento /Mala instalación de los dispositivos de almacenamiento	No realizar en los tiempos establecidos los mantenimientos de los sistemas de información.
	carencia de procedimientos de reemplazo periódico	Mala disposición final de equipos.
	Sensibilidad a la humedad, agua, polvo y la suciedad	Polvo, corrosión, agua, humedad
	Susceptible a los campos electromagnética	Radiación de campos electromagnéticos
	falta de controles de cambios de configuración	Error en la configuración
	Sensibilidad por los cambios de voltaje	Mal funcionamiento del aprovisionamiento de Energía
	Sensibilidad por los cambios de temperatura	Fenómenos Climáticos
	Almacenamiento sin protección	Robo de equipos o información.
	Falta procedimientos para la disposición final	Robo de equipos o información.
	Falta de procedimientos de copias seguras	Robo de equipos o información.
SOFTWARE	Falta de pruebas al software	Abuso de privilegios
	Vulnerabilidades conocidas en los sistemas	Abuso de privilegios
	No cerrar la sesión al dejar el equipo	Abuso de privilegios
	Reutilización de los equipos de almacenamiento sin adecuado borrado.	Abuso de privilegios
	Falta de auditorías de control	Abuso de privilegios

	Mala asignación de los privilegios de acceso	Abuso de privilegios
	Software ampliamente distribuido	Alteración de datos
	En términos de tiempo utilización de datos errados en los programas de aplicación	Alteración de datos
	Interfaz de usuario compleja	Uso inadecuado
	Falta de documentación	Uso inadecuado
	Configuración incorrecta/ por defecto	Uso inadecuado
	Fechas erróneas	Uso inadecuado
	Falta de métodos de autentificación de usuario	Falsificación de derechos
	Tablas de contraseñas sin codificación	Falsificación de derechos
	Mala gestión de las contraseñas	Falsificación de derechos
	Habilitación de servicios innecesarios	Mal procedimiento
	Software nuevo o inmaduro	Errores en el desempeño del software
	Especificaciones incompletas o no claras para los desarrolladores	Errores en el desempeño del software
	Falta de control de cambios	Errores en el desempeño del software
	Descarga y uso no controlado de software	Manipulación a través de software
	Ausencia de copias de recuperación	Mal procedimiento
	Falta de controles de seguridad física de la edificación	Robo de equipos o información.
	Fallas en la elaboración de informes	Uso sin autorización del Equipo

RED	Falta de evidencia de envío o recepción de mensajes	Refutar el acto
	Líneas de comunicación sin protección	Escucha encubierta
	Tráfico sensible sin encriptación	Escucha encubierta
	Conexión deficiente de los cables	Fallas del equipo de telecomunicaciones
	Punto único de fallas	Fallas del equipo de telecomunicaciones
	Deficiencias en la identificación y autentificación del emisor y el receptor	Falsificación de derechos
	Arquitectura de red insegura	Espionaje remoto
	Envió de contraseñas en plano	Espionaje remoto
	Gestión inadecuada de la red	Saturación del sistema de información
	Conexiones de red pública sin protección	Uso sin autorización del Equipo
PERSONAL	Ausencia del personal	Falta de disponibilidad del personal
	Procedimientos inadecuados de contratación	Destrucción de equipos y medios
	Entrenamiento insuficiente en seguridad	Uso inadecuado
	Uso incorrecto de software y hardware	Uso inadecuado
	Falta de conciencia acerca de la seguridad	Uso inadecuado
	Falta de monitoreo	Falta de control
	Trabajo no supervisado del personal externo o de limpieza	Robo de equipos o información.

	Falta de políticas para el uso adecuado de los equipos de telecomunicaciones y mensajería	Uso sin autorización del Equipo
LUGAR	Uso inadecuado o Falta del control de acceso físico a las instalaciones	Falta de control
	Ubicación en área susceptible deinundación	Falta de protocolo
	Red de energía inestable	Mal funcionamiento del aprovisionamiento de energía
	Falta de seguridad física de las instalaciones	Falta de control
ORGANIZACIÓN	Falta de procedimiento establecido para el registro y eliminación de usuarios	Abuso de los privilegios
	Falta de procedimiento para la revisión delos privilegios de acceso	Abuso de los privilegios
	Falta de Clausulas sobre la seguridad de la información en los contratos con clientes o partes interesadas	Abuso de los privilegios
	Falta de Protocolos para el monitoreo de los recursos de procesamiento de la información	Abuso de los privilegios
	Falta de auditorías de control	Abuso de los privilegios
	Ausencia de protocolos de identificación y calificación de riesgos	Abuso de los privilegios
	Falta de informes de fallas en los registros de	Abuso de los privilegios

	administradores y operadores	
	mantenimiento inapropiado del servicio	irregularidad en el mantenimiento del sistema de información
	Falta de acuerdos de niveles de servicio	irregularidad en el mantenimiento del sistema de información
	Falta de protocolos de gestión y control de cambios	irregularidad en el mantenimiento del sistema de información
	Falta de protocolo para la documentación del MSPI	Alteración de datos
	Falta de protocolo para la supervisión del registro del MSPI	Alteración de datos
	Falta de protocolo para la autorización de la información disponible al público	Datos de origen dudoso
	Falta de definición clara de los roles y responsabilidades de seguridad de la información	Refutar el acto, evasión de responsabilidades
	Falta de planes de continuidad	Falla del equipo
	Falta de políticas del correcto uso del correoelectrónico	Uso inadecuado
	Falta de protocolo para introducción del software en los sistemas operativos	Uso inadecuado
	Falta de registros en bitácoras	Uso inadecuado

	Falta de protocolo para el tratamiento de información clasificada	Uso inadecuado
	Falta de responsabilidades en seguridad de la información en los contratos	Uso inadecuado
	Falta de lo protocolos o procedimientos disciplinarios establecidos en caso de incidentes de seguridad de la información	Robo de equipos o información.
	Falta de política sobre el uso adecuado de computadores portátiles	Robo de equipos o información.
	Falta de control sobre los activos ubicados fuera de la entidad	Robo de equipos o información.
	Falta de política de pantalla y escritorio limpio	Robo de equipos o información.
	Falta de autorización de los recursos de procesamiento de información	Robo de equipos o información.
	Falta de herramientas de monitoreo para las brechas en seguridad	Robo de equipos o información.
	Carencia de inspecciones periódicas por parte de la gerencia	Uso sin autorización del Equipo
	Falta de protocolo para el majeo de informes sobre las debilidades en la seguridad	Uso no autorizado deequipo

	Falta de Protocolos del cumplimiento de las disposiciones con los derechos de autor.	Uso de software no licenciado

Nota. Adaptado de (MINTIC, Modelo nacional de gestión de riesgo de seguridad de la información en entidades públicas. anexo 4, 2021)

Tabla 14

fuente y tipo de amenazas

TIPO	AMENAZA	ORIGEN
Daño físico	Fuego	A, D, E
	Agua	A, D, E
	Contaminación	A, D, E
	Accidente Importante	A, D, E
	Destrucción del equipo o medios	A, D, E
	Polvo, corrosión, congelamiento	A, D, E
Eventos naturales	Fenómenos climáticos	E
	Fenómenos sísmicos	E
	Fenómenos volcánicos	E
	Fenómenos meteorológicos	E
	Inundación	E
Perdida de los servicios esenciales	Fallas en el sistema de suministro de agua o aire acondicionado	E
	Perdida de suministro de energía	E
	Falla en equipo de telecomunicaciones	
Perturbación debida a la radiación	Radiación electromagnética	
	Radiación térmica	
	Impulsos electromagnéticos	
	Interceptación de señales de interferencia comprometida	
	Espionaje remoto	
	Escucha encubierta	
	Hurto de medios o documentos	
	Hurto de equipo	

Compromiso de la información	Recuperación de medios reciclados o desechados	
	Divulgación	
	Datos provenientes de fuentes no confiables	
	Manipulación con hardware	
	Manipulación con software	
	Detección de la posición	
Fallas técnicas	Fallas del equipo	
	Mal funcionamiento del equipo	
	Saturación del sistema de información	
	Mal funcionamiento del software	
	Incumplimiento en el mantenimiento del sistema de información.	

Nota. D= Deliberadas, A= Accidentales, E= Ambientales, tomado de (MINTIC, Modelo nacional de gestión de riesgo de seguridad de la información en entidades públicas. anexo 4, 2021)

Definición de Roles

Cuando se definen perfiles y roles en seguridad de la información, se establece de manera clara quién es responsable de qué aspectos de la seguridad de la información. Esto evita confusiones y asegura que cada tarea y responsabilidad esté asignada a alguien específico. Lo que permite la optimización de recursos Al asignar roles específicos, se puede aprovechar de manera más eficiente el talento y los recursos disponibles. Las personas pueden enfocarse en las áreas en las que son expertas, lo que mejora la calidad del trabajo y reduce la probabilidad de errores.

A continuación, se definen los roles para el SGSI.

Tabla 15

Roles de seguridad de la información

Roles	Descripción	Responsabilidades
Comité directivo (alta dirección)	Encargado de realizar revisiones periódicas del Sistema de Gestión de la Información de la entidad a fin de asegurar que la pertinencia, idoneidad y eficacia continúen siendo prioritarias.	• Garantizar la provisión de los recursos requeridos para instaurar y mantener el sistema de gestión de la seguridad de la información. • Asegurarse de que se asignen y comuniquen de manera adecuada las responsabilidades asociadas a los roles relacionados con la seguridad de la información. • Respaldar la capacitación del personal técnico para que adquiera competencias en el ámbito de la seguridad de la información.
Comité de seguridad de la Información o equivalente	Encargado de autorizar las distintas pautas y regulaciones vinculadas a la seguridad de la información, además de dar el	• Coordinar la implementación del Modelo de Seguridad y Privacidad de la Información en la

	visto bueno al plan de reducción de riesgos del Sistema de Gestión de Seguridad de la Información (SGSI).	organización y evaluar el estado de la seguridad de la información. • Facilitar y fomentar la concepción de proyectos relacionados con la seguridad. • Definir los recursos de información en consonancia con los objetivos y metas de la entidad, garantizando un entorno seguro. • Recomendar roles y responsabilidades específicas para resguardar la información. • Autorizar la utilización de procedimientos y métodos particulares para salvaguardar la información.

		• Participar en la elaboración y evaluación de planes de acción destinados a reducir, eliminar y mitigar riesgos. • Realizar revisiones regulares del Sistema de Gestión de Seguridad de la Información (SGSI), al menos una vez al año, y determinar las acciones requeridas a partir de los hallazgos. • Trabajar en incrementar la concienciación sobre la seguridad de la información en la entidad. • Compartir con la organización los documentos generados en el comité de seguridad de

		la información que tengan un impacto en toda la entidad.
Equipo técnico	Encargado de supervisar y coordinar todas las tareas vinculadas a la gestión de la seguridad de la información.	• Utilizar conocimientos, destrezas, herramientas y técnicas en las labores relacionadas con la seguridad de la información. • Identificar las diferencias entre el Modelo de Seguridad y Privacidad de la Información y la situación actual de la entidad. • Elaborar el plan temporal para llevar a cabo la implementación del Modelo de Seguridad y Privacidad de la Información. • Planificar, ejecutar y dar seguimiento a las tareas, plazos, costos y objetivos

		específicos establecidos en el cronograma. • Supervisar continuamente la ejecución de los planes de trabajo, vigilando los posibles riesgos del proyecto y tomando medidas oportunas, incluso comunicándolos al Comité de Seguridad si fuera necesario. • Trabajar de manera conjunta con los grupos o áreas asignados. • Contribuir al enriquecimiento del sistema de gestión del conocimiento del proyecto mediante la documentación de las experiencias adquiridas.
Líder TI	Encargado de diseñar, estructurar, supervisar y	• Identificar y notificar a través de los canales

	administrar la estrategia para la utilización y adopción efectiva de Tecnologías de la Información.	establecidos los riesgos, sucesos o incidentes relacionados con la ciberseguridad. • Supervisar la gestión y configuración de los recursos informáticos en el interior de la organización. • Desplegar controles tecnológicos destinados a mitigar los riesgos en cuanto a la seguridad de la información. • Implementar medidas tecnológicas para contrarrestar los riesgos específicos identificados en relación con la seguridad de la información. • Ejecutar campañas de concienciación y educación sobre temas de privacidad y seguridad de la información.

		• Informar al Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT) acerca de incidentes de ciberataques.
Líderes de Proceso	Responsables de la información que se genera en su proceso.	• Comprobar la inclusión de los activos en el inventario. • Informar al líder de TI o al equipo técnico sobre cualquier irregularidad o indicios de incidentes que puedan afectar la privacidad y seguridad de la información. • Adherirse a las políticas de seguridad de la información y garantizar que su equipo siga dichas directrices. • Participar en programas de sensibilización relacionados con la seguridad de la información. • Establecer los usuarios y sus respectivas funciones para determinar quiénes

		tienen autorización de acceso a la información, teniendo en cuenta la competencia y responsabilidad de los usuarios.
Usuarios de la Información (Funcionarios, Contratistas, Terceros)	Personas que emplean la información y los recursos tecnológicos en la organización para el desarrollo de sus labores cotidianas.	• Colaborar con los líderes de proceso en la ejecución de tareas como la gestión de activos y de riesgos. • Adherirse todas las políticas relacionadas con la privacidad y seguridad de la información. • Informar al líder de TI o al equipo técnico acerca de cualquier anomalía o sospecha de incidentes que puedan afectar la privacidad y seguridad de la información. • Garantizar la seguridad de los activos de información bajo su responsabilidad.

		• Participar en programas de sensibilización sobre seguridad de la información. • Mantener en estricta confidencialidad las credenciales y contraseñas de acceso a aplicaciones y sistemas de información.
Auditor SGSI	Responsable de revisar el cumplimiento del SGSI	• Llevar a cabo auditorías y evaluaciones internas con el propósito de obtener una visión de la eficacia del sistema de seguridad y privacidad de la información (estas auditorías deben realizarse al menos una vez al año). • Generar informes de las auditorías que faciliten la implementación de mejoras continuas en el SGSI.
Área Jurídica y Contratación	Responsable de contratación	• Comprobar y aplicar las disposiciones de seguridad de la información junto con

		los empleados, proveedores y contratistas de la organización. • Garantizar la salvaguardia de la seguridad de la información de todos los activos que puedan estar relacionados con el proceso de contratación • Asistir en capacitaciones de sensibilización en temas de seguridad de la información.
Área Comunicación	Divulgación de información y comunicados internos	• Apoyar la divulgación de información y comunicados internos en favor de fortalecer las campañas de privacidad y seguridad de la información
Archivista	Gestión documental de la entidad	• Asegurar y salvaguardar los archivos y activos de la información físicos que deben ser archivados o almacenados

Nota. Adaptado de (MINTIC, Guia 4. Roles y responsabilidades, 2016)

Clasificación de la información

Se realizo el Anexo 2 “inventario de activos” donde se enumeran los activos relevantes para la dirección de salud de caldas en el área de TI, donde se determina el nivel de importancia para cada activo se le asigna un código de identificación, se realiza una breve descripción del activo, se identifica la ubicación de este y su custodio, después de esto se precede a realizar la clasificación de estos según su criterio de los pilares de la seguridad de la información, triada (CID) confidencialidad, integridad, disponibilidad de terminando así que de 21 activos identificados en el área de sistemas se clasifican de la siguiente manera ver tabla 17.

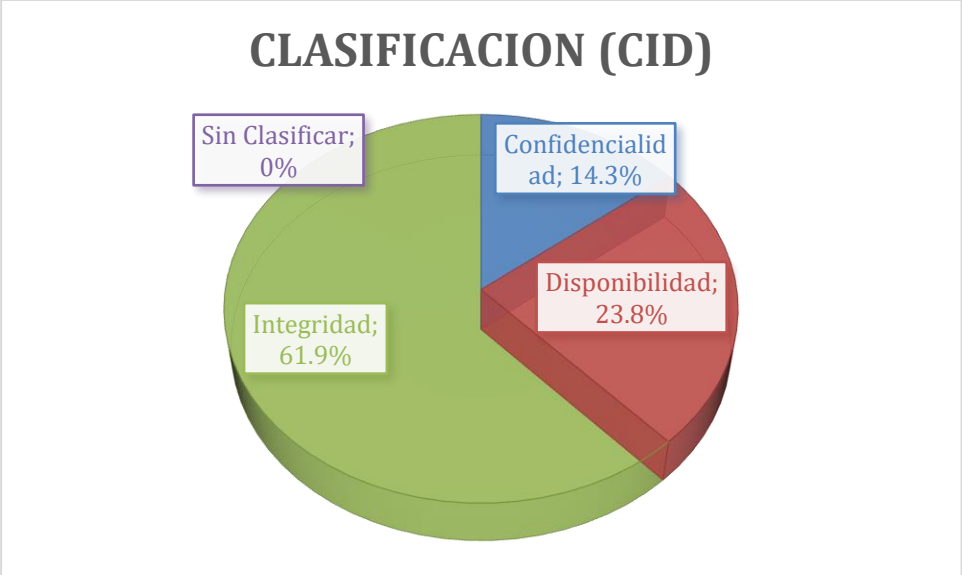
Tabla 16

Clasificación de la información (CID)

Clasificación (CID)	**Cantidad**
Confidencialidad	14.3%
Disponibilidad	23.8%
Integridad	61.9%
Sin Clasificar	0%

Figura 8

Clasificación (CID)



La clasificación de los activos de información según la confidencialidad, integridad, disponibilidad se encuentra descrita en la Figura 8, donde el 14.3% de los activos su componente principal corresponde a la confidencialidad, el 23.8% deben tener una buena disponibilidad y el 61.9% su atributo principal es la integridad, no se encuentra ningún activo sin clasificar en cuanto a la confidencialidad, integridad y disponibilidad, en la Figura 9,

Se describe la clasificación de la confidencialidad de los activos de la entidad encontrado que de estos el 23.81% deben tener una alta confidencialidad, el 9.52% una confidencialidad media, mientras que el 66.67% están clasificados con una confidencialidad baja, en la Figura 10, se presenta la distribución porcentual del nivel de integridad que deben presentar los activos de la entidad teniendo así que el 38.10% tiene una clasificación alta, el 47.62% tienen una clasificación media y el 14.29% se encuentra en baja. Por su parte la

Figura 11, muestra en nivel de disponibilidad que deben tener los activos, presentando un porcentaje 14.29% clasificados como alta, 42.86% con media y 42.86% con disponibilidad baja.

Clasificación de los activos de información según la Confidencialidad

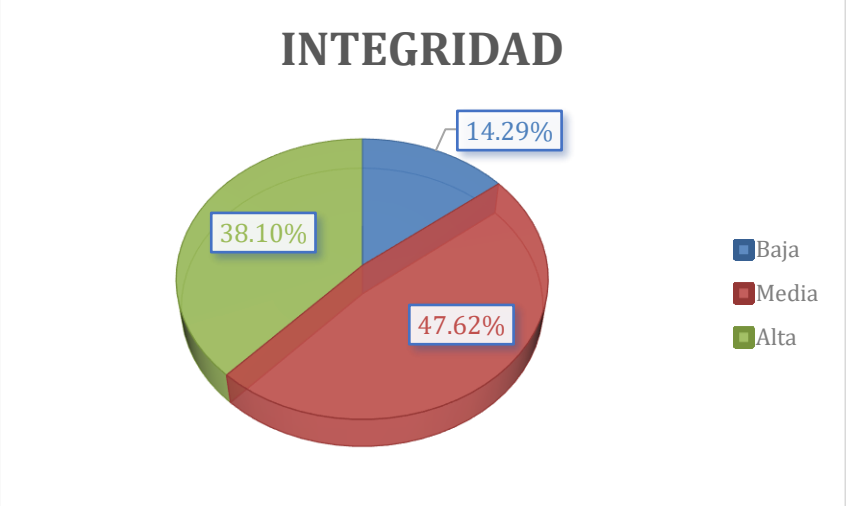
Figura 9

Clasificación de los activos según la confidencialidad

Clasificación de los activos de información según la Integridad

Figura 10

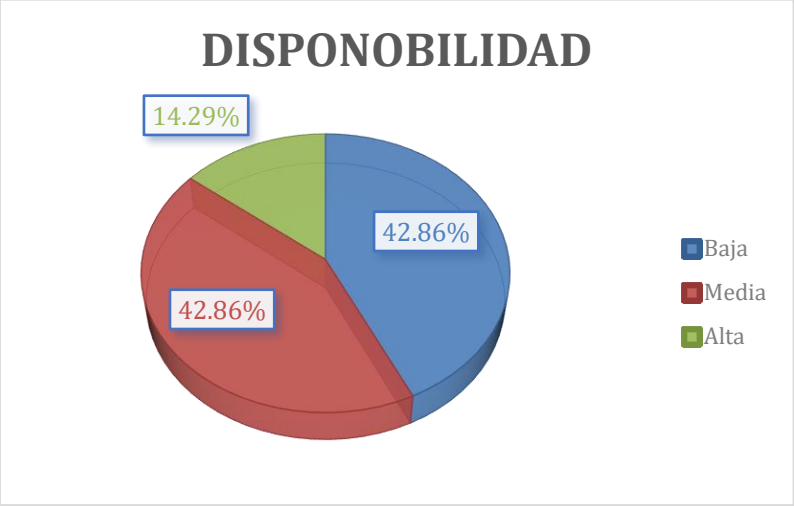
Clasificación de los activos según la integridad



Clasificación de los activos de información según la Disponibilidad

Figura 11

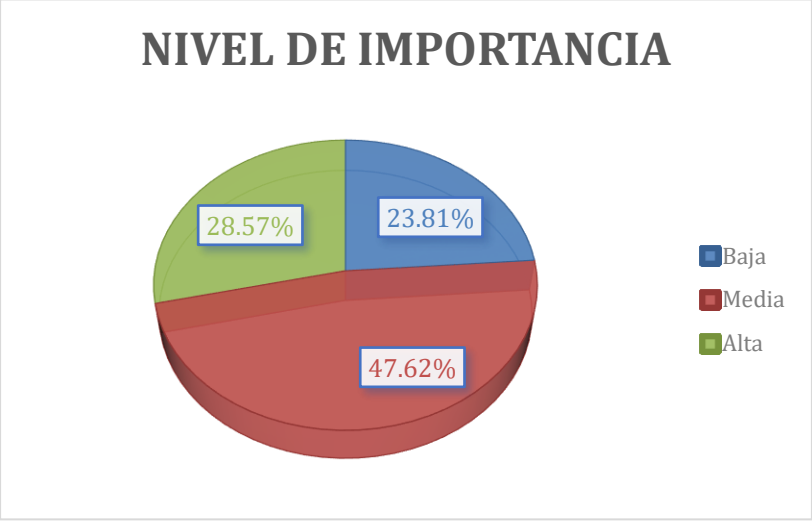
Clasificación de los activos según la Disponibilidad



Clasificación de los activos de información según el Nivel de importancia

Figura 12.

Nivel de importancia de los activos



Como se muestra en la Figura 12, se determinó el nivel de importancia de los activos del área de tecnología de la Dirección territorial de salud de Caldas Clasificando los en nivel Bajo un 23.81%, Nivel Medio 47.62%, y alta 28.57% siendo estos los activos que deben ser priorizados para dar tratamiento frente a los riesgos que estos presentan, La clasificación del nivel de importancia de los activos de información es fundamental para garantizar la seguridad de la información en cualquier organización. Esta práctica permite identificar y priorizar los activos críticos, lo que a su vez ayuda a asignar recursos y medidas de seguridad de manera eficiente. Al determinar qué activos son más valiosos y susceptibles a amenazas, las empresas pueden enfocarse en protegerlos de manera más efectiva, reduciendo riesgos y mitigando posibles pérdidas financieras y daños a la reputación. Además, la clasificación de activos de información también es esencial para cumplir con regulaciones de privacidad y protección de datos, lo que respalda la confianza de los usuarios y partes interesadas.

Así mismo se realizó la clasificación de la información

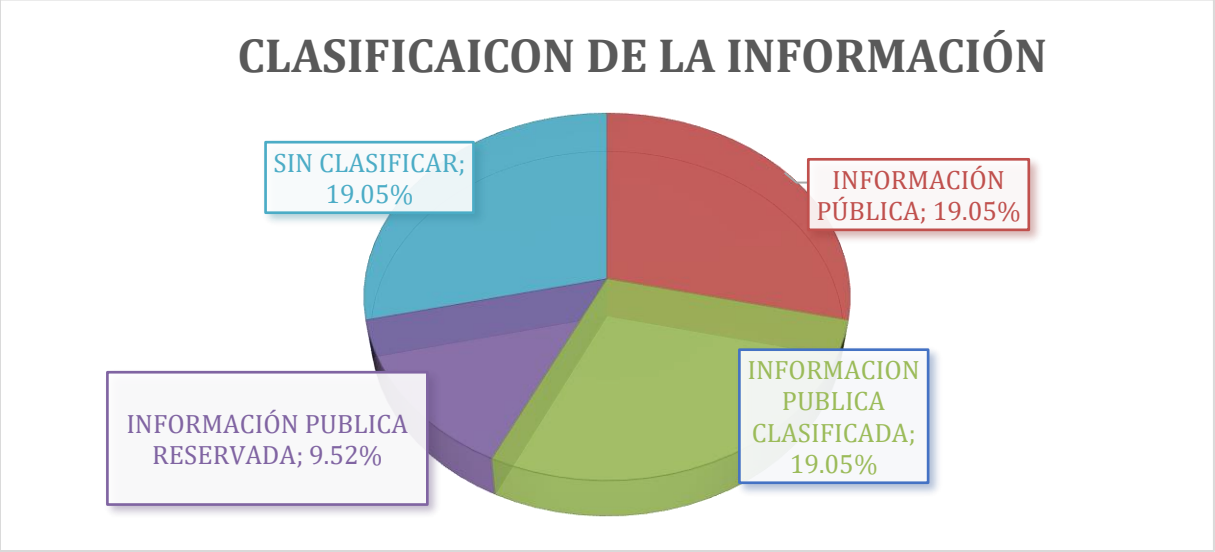
Tabla 17

Clasificación de la información

Clasificación de la información	**cantidad**
INFORMACIÓN PÚBLICA	19.05%
INFORMACIÓN PUBLICA CLASIFICADA	19.05%
INFORMACIÓN PUBLICA RESERVADA	9.52%
SIN CLASIFICAR	19.05%

Figura 13

Clasificación de la información



Los activos de información de la entidad se encuentran clasificados según el criterio de clasificación de la información como se evidencia en la Figura13. presentando 9.52% información pública reservada esto se refiere a activos o información que solo puede ser accedida por quien tenga los privilegios o autorización expresa del dueño o custodio del activo, 19.05% información púbica clasificada, información o activos que son de dominio público pero tienen restricciones temporales o limitaciones de acceso debido a consideraciones legales o de seguridad, el 19.05% corresponde a información pública, esto implica datos información o documento que están disponibles para el acceso y uso por parte del público en general, sin restricciones significativas.

Fase 4. Definir Políticas

Política general de seguridad y privacidad de la información

La Dirección Territorial de Salud de Caldas debe asegurar la gestión adecuada de la información que está bajo su resguardo, con el fin de garantizar la confidencialidad y la privacidad de los datos de los ciudadanos, tal como se establece en el artículo 15 de la Constitución Política de Colombia. La Dirección reconoce la importancia de la administración de la información y se ha comprometido a establecer un sistema de gestión de seguridad de la información con el propósito de crear un ambiente de confianza en su cumplimiento de deberes ante el Estado y la sociedad, siguiendo rigurosamente la normativa legal y en concordancia con la misión y visión de la entidad.

La Dirección Territorial de Salud de Caldas tiene como objetivo principal la mitigación del impacto de los riesgos que afectan a sus activos de información. Esto se realiza con el propósito de mantener un nivel de exposición que sea capaz de satisfacer las necesidades de los distintos grupos de interés identificados en lo que respecta a la integridad, confidencialidad y disponibilidad de la información. En virtud de lo anterior, esta política es de aplicación a toda la organización, abarcando su alcance, su personal, los terceros, los aprendices, los practicantes, los proveedores y la comunidad en general.

Las premisas del SGSI están enmarcadas en:

- Reducir el riesgo en las funciones más importantes de la empresa.
- Adherirse a los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Generar y conservar la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Salvaguardar los recursos tecnológicos.

- Crear las directrices, procesos y guías de seguridad de la información.
- Fomentar una cultura y conciencia de la seguridad de la información entre los funcionarios, terceros y practicantes y clientes de La dirección territorial de salud de Caldas
- Asegurar la Continuidad de la Entidad frente a situaciones inesperadas o incidentes.

Las políticas específicas de encuentran como información anexa en el documento "Política de Seguridad de la Información"

Declaración de aplicabilidad de controles

Según la guía N°8 controles de seguridad y privacidad de la información y la norma ISO 27001:2013, se debe establecer la declaración de aplicabilidad de los controles de seguridad de la información, especificando cuales de estos serán aplicables en el contexto de la organización para generar una optimización del tratamiento de los riesgos identificados, disminuir la probabilidad e impacto de ocurrencia de riegos o amenazas. La declaración de aplicabilidad de controles para la Dirección territorial de salud de Caldas se encuentra en el Anexo 5 "Declaración de aplicabilidad"

El formato implementado para la declaración de aplicabilidad de los controles en la Dirección territorial de salud de Caldas cuenta con los siguientes campos:

N°: campo de identificación según la numeración de los controles por parte de la norma ISO 27001:2013

Dominio: Domino al que pertenece el control

Control: objetivo del control

Aplica (SI/NO): establece si el control es aplicable a la entidad

Control implementado (SI/NO): se determina si el control esta implementado o no

Control a implementar: se describe que control, procedimiento o acciones se deben implementar para dar cumplimiento.

Evidencia: se relaciona la evidencia de que el control o las políticas asociadas a esta se aplicaran a la entidad.

La calificación promediada de los controles dentro de la entidad fue de 70, según el análisis y los resultados obtenidos en Tabla 1, lo que indica que la entidad se encuentra en un proceso Gestionado de implementación de medidas para la seguridad y privacidad de la información, pero esto no quiere decir que la entidad deba minimizar los esfuerzos por seguir el camino de la mejora continua y llegar a alcanzar la puntuación de 100 que propone el MINTIC como se muestra en la Tabla 3 puntuación que debió haber sido alcanzada en el año 2018 . Actualmente, los controles existentes se están revisando y mejorando.

Sin embargo, para su fortalecimiento, se requieren los 9 dominios que deben incluirse en las acciones actuales:

- A.5. Políticas de seguridad de la información
- A.6. Organización de la seguridad de la información

- A.7 Seguridad de los recursos humanos
- A.8. Gestión de los activos
- A.10 Criptografía
- A.13 Seguridad de las comunicaciones
- A.14 Adquisición, desarrollo y mantenimiento de sistemas
- A.16 Gestión de incidentes de seguridad y privacidad de la información
- A.17 Aspectos de seguridad de la información de la gestión de la continuidad del negocio

Los controles seleccionados se encuentran en el Anexo 5 “declaración de aplicabilidad”

Anexos

Los anexos se encuentran como archivos separados debido a las características de su diseño y su tamaño en tablas estructuradas, algunos de estos se encuentran en archivos de Excel.

Anexo 1. Instrumento de evaluación MSPI.

Archivo “Instrumento Evaluación MSPI.xlsx” en este se encuentran la calificación obtenida por la entidad en los componentes administrativos y técnicos, esta es una herramienta proporcionada por MINTIC para saber el nivel de madurez del MSPI.

Anexo 2. Inventario de activos

Archivo “INVENTARIO DE ACTIVOS ÁREA DE SISTEMAS.xlsx” Este documento contiene la definición del inventario de activos del área de sistemas de la

Dirección Territorial de Salud de Caldas, incluyendo su nivel de importancia y clasificación en términos de confidencialidad, integridad y disponibilidad, así como los parámetros de clasificación de la información pública, información pública reservada, información pública clasificada.

Anexo 3. Políticas de seguridad de la información.

Archivo “Política de seguridad de la información.docx” este documento contiene la actualización de las políticas de seguridad de la información, así como los roles y responsabilidades frente a cada una de estas.

Anexo 4. Matriz análisis de riesgos.

Archivo “Matriz de riesgos.xlsx” este contiene la matriz de análisis de riesgos de los activos, el mapa de calor del riesgo inherente y riesgo residual, se definen los parámetros de impacto y los parámetros de probabilidad, se definen los criterios de aceptabilidad del riesgo, y criterios de valoración de los controles.

Anexo 5. Declaración de aplicabilidad de los controles.

Archivo “Declaración de aplicabilidad.xlsx” en este archivo se encuentra la declaración de aplicabilidad de los controles, el dominio al que pertenecen según la norma ISO/IEC 27001

Anexo 6. Plan de sensibilización, Capacitación, educación y comunicación.

Archivo “Plan de capacitación sensibilización y educación.docx” este documento contiene los roles y responsables de participar en la ejecución y desarrollo de capacitaciones, ejemplos de temas a tratar y opciones de difusión para compartir los temas relacionados a seguridad de la información, la importancia de

este documento toma importancia debido a que se puede contar con sistemas de seguridad eficientes pero si el personal no está bien capacitado estos puede generar brechas por desconocimiento omisión o malas configuraciones

Conclusiones

Determinar la situación actual en el nivel de madurez del SGSI permite realizar una evaluación detallada de la situación actual en cuanto a seguridad y privacidad de la información en la Dirección Territorial de Salud de Caldas, identificando posibles vulnerabilidades y riesgos.

Tener el diseño del SGSI permitirá tener una hoja de ruta para la implementación, ayuda a anticiparse a posibles incidentes relacionados con la gestión de la información y los recursos públicos, lo que permite una respuesta proactiva y eficaz.

Tener unos controles se seguridad de la información bien definidos y estructurados conlleva a tener una protección de los activos críticos, reducción de riesgos, reducción de costos, ayuda a la entidad a tener un cumplimiento normativo en cuanto a la seguridad de la información, así como mantener la buena reputación de la entidad y la confianza de sus clientes o partes interesadas.

Es importante tener definidos los roles y responsabilidades frente a cada una de las políticas definidas, permitiendo una coordinación de esfuerzos, optimización de recursos y tiempos de respuesta frente a la posible ocurrencia de incidentes en la seguridad.

Aunque la entidad logro una puntuación de 70 en la evaluación de efectividad de los controles, es importante seguir en la implantación de políticas y mejoramiento continuo con el fin de alcanzar la meta de los tiempos establecidos para la aplicación del modelo según MINTIC.

Es de vital importancia tener implementado el procedimiento para la sensibilización capacitación, educación y comunicación, para funcionarios, contratistas, y partes interesadas ya que a menudo las vulnerabilidades de seguridad provienen de errores humanos, es por esto que la capacitación efectiva puede ayudar a reducir significativamente los factores de riesgo, frente a amenazas de seguridad de la información.

El compromiso de la alta gerencia como de las partes involucradas y el desarrollo de las actividades acatando las políticas de seguridad y privacidad de la información contribuyen a una disminución de la probabilidad de ocurrencia de eventos o incidentes informáticos o en los que se vea comprometida la seguridad y privacidad de la información

Recomendaciones

Es crucial llevar a cabo un nuevo diagnostico después de 4 meses desde la implementación del Sistema de Gestión de Seguridad de la Información (SGSI), con el objetivo de comparar y valorar la eficacia de los controles sugeridos y así conocer el nuevo nivel de madurez alcanzado por la entidad.

Tanto el inventario de activos como las políticas y los controles deben ser revisado periódicamente, el mapa de riesgos ya que según los cambios de las normativas leyes y estándares pueden ser susceptibles a cambios, se recomienda hacerle una revisión al menos una vez al año, actualizar en caso de ser necesario.

Se debe realizar reuniones del comité con la alta dirección con una frecuencia que no supere los 2 meses con el fin de identificar acciones de mejora aplicables al SGSI de la entidad.

Las copias de seguridad y recuperación deben ser almacenas en un lugar físico diferente al del centro de datos con fin de disminuir el riesgo ante un incidente físico o ambiental que pueda alterar, modificar o dañar la información.

Se recomienda el uso de métodos de criptografía para proteger la información clasificada con alta confidencialidad, reservada o privada.

Se recomienda que las labores de seguridad de la información no sean desempeñadas por los administradores de sistemas especialmente las labores de auditoría y análisis de vulnerabilidades.

Se recomienda realizar un análisis de vulnerabilidades con el fin de identificar los controles que deben ser gestionados con mayor prioridad ya que la entidad no permitió realizarlo en el momento del desarrollo de este proyecto. Así como la realización de pruebas de efectividad de controles.

Referencias

Achmadi D, Suryanto Y, & Ramli K. (2018). *On Developing Information Security Management System (ISMS) Framework for ISO 27001-based Data Center*. IEEE.

adversia. (s/f). *¿Qué es norma ISO 27001?* Recuperado el 30 de septiembre de 2023, de https://advisera.com/27001academy/es/que-es-iso-27001/

Alex Richar Silva Guerrero. (2021). *Implementación de un Sistema de Gestión de Seguridad de la Información para mejorar la Seguridad de la Información en una empresa MYPE*.

Alfonso, E., Montalbán, R., Martelo Gómez, R. J., Antonio, D., & Borré, F. (2020). *DESIGN OF AN INFORMATION SECURITY MANAGEMENT SYSTEM FOR THE PROCESS OF MANAGING THE TECHNOLOGICAL INFRASTRUCTURE OF ACADEMIC INSTITUTIONS BASED ON MAGERIT* (Vol. 11, Número 1).

Arafat, M. (2018, junio 26). Information security management system challenges within a cloud computing environment. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3231053.3231127

Bravo M. (2018). *DESARROLLO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DELA INFORMACIÓN PARA BIBLIOTECAS BASADO EN UNA METODOLOGÍA MEJORADA DE ANÁLISIS DE RIESGOS COMPATIBLE CON LA NORMA ISO/IEC 27001:2013*.

Carreño I., Mendoz S., & Montañez M. (2021). *DISEÑO DE UN SGSI PARA UNAEMPRESA DEL SECTOR SALUDBASADO EN EL ESTÁNDAR ISO 27001:2013*.

Conpes 3701. (2011). *Consejo Nacional de Política Económica y Social República de Colombia Departamento Nacional de Planeación*.

Conpes 3854. (2016). CONPES CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL REPÚBLICA DE COLOMBIA DEPARTAMENTO NACIONAL DE PLANEACIÓN POLÍTICA NACIONAL DE SEGURIDAD DIGITAL. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ

Criollo I. (2022). Etapa de planificación de un sistema de gestión de seguridad de la información para el área de tecnología de la IPS Garper Médica SAS basado en la norma ISO-IEC 27001-2013.

MINTIC. (s.f.).

MINTIC. (2016). *Guia 4. Roles y responsabilidades.*

MINTIC. (2016). *portada "instrumento de evaluación MSPI".*

MINTIC. (2021). *Inventario y clasificación de activos de información e infraestructura critica cibernética nacional.*

MINTIC. (2021). *Modelo Nacional de gesti'on de riesgo de la información en entidades públicas. Anexo 4.*

MINTIC. (2021). *Modelo nacional de gestión de riesgo de seguridad de la información en entidades públicas. anexo 4.*

CSIRT POLICIA NACIONAL COLOMBIANA. (2020). *balance ciber crimen*.

Enríquez A. (2018). *MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA INSTITUCIONES DE SALUD, BASADO EN LAS NORMAS ISO 27799:2008, ISO/IEC 27005:2008 E ISO/IEC 27002:2013 APLICADA A LA CLÍNICA MÉDICA FÉRTIL*.

Erik M. (2019). *METODOLOGÍA PARA LA IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓNDE SEGURIDAD DE LA INFORMACIÓN ISO/IEC 27001:*

PARA SOPORTE DE ÁREAS DE ADMISIÓN Y ATENCIÓN DE UN HOSPITAL PÚBLICO.

Garcia J., Huamani S., & Lomparte R. (2018). Artículo de Contribución Modelo de gestión de riesgos de seguridad de la información para PYMES peruanas Information security risk management model for Peruvian PYMES. *Revista PeRuana de ComPutaCión y sistemas*, *1*(1), 47–56. https://doi.org/10.15381/xxxxxxs

Guerra, E., Neira, H., Díaz, J. L., & Patiño, J. (2021). Desarrollo de un sistema de gestión para la seguridad de la información basado en metodología de identificación y análisis de riesgo en bibliotecas universitarias. *Información tecnológica*, *32*(5), 145–156. https://doi.org/10.4067/s0718-07642021000500145

Ley 599 de 2000 - Gestor Normativo - Función Pública. (s/f). Recuperado el 2 de junio de 2023, de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=6388

Congreso de la República de Colombia. (2018). *Ley 1266 de 2008*.

Congreso de la República de Colombia. (2014). *Ley 1712 de 2014*.

Congreso de la República de Colombia. (2018). *Ley 1928 de 2018*.

Márquez H. (2020). *DISEÑO DELSISTEMADEGESTIÓNDELASEGURIDAD DEINFORMACIÓN(SGSI) EN LA INSTITUCIÓN PRESTADORA DE SERVICIOS DE SALUDCENTRODE TERAPIAS INTEGRALES MISALUD S.A.S*.

Articulo-15. Recuperado el 2 de junio de 2022, de https://www.mincit.gov.co/ministerio/normograma-sig/procesos-estrategicos/gestion-de-informacion-y-comunicacion/constitucion-politica/derechos/articulo-15.aspx

Mintic. (s/f). *MSPI*. Recuperado el 20 de septiembre de 2022, de https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/

MinTic. (2016). *Guía de gestión de riesgos*.

Niquen L. (2019). *IMPLEMENTACIÓN DE UN MODELO DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN PARA APOYAR EL PROCESO DE ATENCIÓN AL PACIENTE EN INSTITUCIONES DE SALUD*.

Palma M. (2019). *DISEÑO DE UNA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN BASADA EN LA NORMA ISO27002:2013PARA EL CONTROL DE ACCESO A LA INFRAESTRUCTURA DE REDDE AXXIS HOSPITAL*.

Peikari, H. R., Ramayah, T., Shah, M. H., & Lo, M. C. (2018). Patients' perception of the information security management in health centers: The role of organizational and human factors 17 Psychology and Cognitive Sciences 1701 Psychology 11 Medical and Health Sciences 1117 Public Health and Health Services. *BMC Medical Informatics and Decision Making*, *18*(1). https://doi.org/10.1186/s12911-018-0681-z

Perez D., Preciado S., & Solana P. (2019). Organizational practices as antecedents of the information security management performance: An empirical investigation. *Information Technology and People*, *32*(5), 1262–1275. https://doi.org/10.1108/ITP-06-2018-0261

Pleskach, V., Pleskach, M., & Zelikovska, O. (2019). *Information Security Management System in Distributed Information Systems*.

Proença, D., & Borbinha, J. (2018). Information security management systems - A maturity model based on ISO/IEC 27001. *Lecture Notes in Business Information Processing*, *320*, 102–114. https://doi.org/10.1007/978-3-319-93931-5_8

Rienzo, A., & Gastón, C. (2018). *Evaluation of the Degree of Knowledge and Implementation of Information Security Management Systems, based of the NCh-ISO 27001 Standard, in Health Institutions*.

Rodriguez G. (2020). *ANÁLISIS COMPARATIVO DE LOS MODELOS DEFENSA EN PROFUNDIDAD Y MSPI, PARA LA IMPLEMENTACIÓN DE LA SEGURIDAD INFORMÁTICA EN EL SECTOR PRIVADO DEL PAÍS*.

Ruiz J. (2018). *MODELO PARA LA IMPLEMENTACIÓN DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES BASADO EN EL SGSI DE LA NORMA ISO 27001*.

Saminu, A. (2019). A FRAMEWORK FOR EFFECTIVE INFORMATION SYSTEM SECURITY MANAGEMENT IN KATSINA STATE HEALTHCARE ORGANIZATIONS. En *International Journal of Engineering Applied Sciences and Technology* (Vol. 4). http://www.ijeast.com

Sierrra M., & Hurtado J. (2018). *MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN PARA LA ALCALDÍA DE PUERTO ASÍS EN SU FASE DE DIAGNOSTICO Y PLANIFICACIÓN*.

Tamayo J. (2020). *Adaptación de una Metodología Para el Análisis y Gestión de Riesgos Informáticos Para Organizaciones del Sector Salud en Colombia*.

Tatiara, R., Fajar, A. N., Siregar, B., & Gunawan, W. (2018). Analysis of factors that inhibiting implementation of Information Security Management System (ISMS) based on ISO 27001. *Journal of Physics: Conference Series*, *978*(1). https://doi.org/10.1088/1742-6596/978/1/012039

Valencia Martínez, N. A., Yulán Valencia, C. M., & Chipe Valencia, B. D. (2023). Resiliencia en la informática. *RECIMUNDO*, *7*(1), 79–86. https://doi.org/10.26820/recimundo/7.(1).enero.2023.79-86

Zammani, M., Razali, R., & Singh, D. (2019). Factors Contributing to the Success of Information Security Management Implementation. En *IJACSA) International Journal of Advanced Computer Science and Applications* (Vol. 10, Número 11). www.ijacsa.thesai.org

Zapata, D. (2021). *Análisis de Factores Críticos de Éxito para la Implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en la Empresa Inversiones Prisco S.A.C–Sechura*.