Modelo de Seguridad y Privacidad de la Información (MSPI) de la E.S.E. Hospital Universitario San Rafael de Tunja (HUSRT).

Israel Camilo Gayón Acevedo

Universidad de Manizales

Facultad de Ciencias e Ingeniería

Maestría en Seguridad de la Información

Manizales, 2023

Modelo de Seguridad y Privacidad de la Información (MSPI) de la E.S.E. Hospital Universitario San Rafael de Tunja (HUSRT).

Israel Camilo Gayón Acevedo

Propuesta de trabajo de grado presentado como requisito parcial para optar al título de Magíster en Seguridad de la Información

Director:

Francisco Javier Valencia Duque

Ingeniero de Sistemas

PhD en Ingeniería, Industria y Organizaciones

Línea de Investigación:

Gestión de la Seguridad de la Información en las Organizaciones

Grupo de Investigación y Desarrollo en Informática y Telecomunicaciones

Universidad de Manizales

Facultad de Ciencias e Ingeniería

Maestría en Seguridad de la Información

Manizales, 2023

Tabla de Contenido

Resumen

La información es sin duda el activo más importante de cualquier organización pública o privada en el siglo XXI, de allí, entonces que protegerla deberá ser una de las razones de ser de la organización y para ello se hace vital entender ¿cómo? y ¿con qué recursos puede lograrse? El presente proyecto tiene como objetivo definir un Modelo de Gestión de Seguridad de la Información que se implemente hasta la Declaración de Aplicabilidad de los Controles aprobados por la Entidad, alineado con la norma ISO 27001 bajo el Modelo de Privacidad y Seguridad de la Información -MPSI- del Ministerio de Tecnologías de la Información y las Comunicaciones -MinTIC- para la E.S.E. Hospital Universitario San Rafael de Tunja (HUSRT). Para tal fin, se determinará el estado actual de la gestión de la seguridad y privacidad de la información al interior de la entidad, identificando su estado de madurez, donde posteriormente se implementará la identificación de los Activos de Información con Criticidad Alta, la Gestión de los Riesgos y estableciendo los Controles de Seguridad y Privacidad de la Información aprobados en la Declaración de Aplicabilidad.

En las fases se identificará y establecerá El Plan del MSPI, los Activos de Información, el Manual de Políticas de Seguridad y Privacidad bajo el MPSI, Roles y Responsabilidades, el Plan de Comunicaciones, el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información, los Indicadores de Gestión y la Declaración de Aplicabilidad. Finalmente, el producto obtenido será un modelo de gestión aplicable a la organización alineado con la norma ISO 27001 bajo los lineamientos MPSI para la E.S.E Hospital Universitario San Rafael de Tunja, que aprobará por medio de la Dirección bajo la Declaración de Aplicabilidad los controles a implementar con los recursos que cuenta.

Palabras clave: Modelo de gestión, Seguridad de la Información, ISO 27001, Modelo de Privacidad y Seguridad de la Información -MPSI-, MinTIC, HUSRT.

Abstract

Information is undoubtedly the most important asset of any public or private organization in the 21st century, hence protecting it must be one of the reasons for the organization's existence and for this it is vital to understand how? And with what resources can it be achieved? The objective of this project is to define an Information Security Management Model that is implemented up to the Declaration of Applicability of the Controls approved by the Entity, aligned with the ISO 27001 standard under the Information Privacy and Security Model -MPSI. - from the Ministry of Information and Communications Technologies -MinTIC- for the E.S.E. San Rafael de Tunja University Hospital (HUSRT). For this purpose, the current state of information security and privacy management within the entity will be determined, identifying its state of maturity, where the identification of Information Assets with High Criticality, the Management of Risks and establishing the Information Security and Privacy Controls approved in the Applicability Statement.

In the phases, the MSPI Plan, the Information Assets, the Security and Privacy Policy Manual under the MPSI, Roles and Responsibilities, the Communications Plan, the Security and Privacy Risk Treatment Plan of the information, the Management Indicators and the Declaration of Applicability. Finally, the product obtained will be a management model applicable to the organization aligned with the ISO 27001 standard under the MPSI guidelines for the E.S.E Hospital Universitario San Rafael de Tunja, which will be approved by the Management under the Declaration of Applicability the controls to be implemented. with the resources it has.

Keywords: Management model, Information security, ISO 27001, Information Privacy and Security Model - MPSI-, MinTIC, HUSRT.

Lista de figuras

Lista de tablas

INTRODUCCIÓN

En la actualidad, debido al avance significativo de la tecnología, a la gran apertura de conectividad mundial y la necesidad de las empresas de ofrecer sus servicios en línea, la información y los datos se han convertido en uno de sus activos más importantes en las organizaciones, la cual, sólo tiene sentido cuando está disponible y es utilizada de forma adecuada, integra, oportuna, responsable y segura, lo que implica, que es necesario que las empresas tengan una adecuada gestión de sus recursos y activos de información con el objetivo de asegurar y controlar el debido acceso, tratamiento y uso de la información.

La necesidad de proteger la información ante los altos riesgos que se presentan, ha permitido que la seguridad de la información y la gestión del riesgo se conviertan en mecanismos importantes en las organizaciones para mitigar los riesgos a los que están expuestos los activos de información.

El presente trabajo de grado busca proponer un Modelo de Gestión de la Seguridad y Privacidad de la Información, que permita garantizar una adecuada identificación, clasificación, valoración, gestión y tratamiento de los riesgos, que pueden afectar la seguridad y que sirva como punto de partida para implementar salvaguardas efectivos que permitan estar preparados ante situaciones adversas que puedan comprometer la seguridad y privacidad de la información de la E.S.E Hospital Universitario San Rafael de Tunja (HUSRT).

Inicialmente en el proyecto se plantea el problema y la justificación que se presenta en la E.S.E. HUSRT junto con sus objetivos estableciendo una metodología y definiendo un plan de análisis. Acorde a lo anterior se realiza una investigación en donde se identifican los antecedentes y el referente normativo legal que van acorde a la temática de investigación.

En el referente conceptual se aclara que es Seguridad de la Información, los Sistemas de Gestión de Riesgos con sus diferentes metodologías, los Sistemas de Gestión de Seguridad de la Información y el Modelo de Seguridad y Privacidad de la Información, el cual se aplica en este proyecto hasta la fase de Implementación.

Cabe destacar que para el desarrollo y ejecución del proyecto se debe investigar y conocer la entidad, su contexto interno y externo enfocado en Seguridad y Privacidad de la Información, infraestructura tecnológica, sistemas de información, redes, etc. para posteriormente definir el Alcance del proyecto y las partes interesadas.

Posteriormente a la investigación y aclaración del marco referencia y cómo se encuentra la entidad en Seguridad y Privacidad de la Información, se procede a, implementar la primera fase del MSPI, que es en donde se utiliza y diligencia la herramienta GAP propuesta por el MinTIC, para realizar un examen mas especifico que arroja en que está y no está cumpliendo la entidad en Seguridad de la Información, Ciberseguridad, cuál es el Nivel de Madurez, etc. así como el desarrollo de una encuesta que se ejecuta de acuerdo a un estudio poblacional de la entidad.

La entidad debe implementar todas las fases del MSPI y por ende se especifican los Roles y Responsabilidades en donde se detallan las actividades de cada uno de los roles para poder continuar con el diseño y desarrollo del proyecto. Definiendo lo anterior se procede a la recolección y análisis de los activos de información de la entidad y de los cuales solo se seleccionan los que contienen Criticidad Alta para desarrollar el Manual de Políticas de Seguridad y Privacidad de la Información, así como la Gestión de Riesgos, que posteriormente se utiliza para definir la Declaración de Aplicabilidad en la cual se estipula el tratamiento, quién es el responsable de aplicarlo y de realizarle el seguimiento. La declaración de aplicabilidad se

aprueba por el comité de Seguridad y Privacidad de la Información acorde a los recursos con los que cuenta y un cronograma que debe proyectar y actualizar periódicamente.

El presente proyecto consta de los siguientes capítulos, estructurados de la siguiente manera:

En el capítulo I, se realiza el planteamiento del problema, definiendo en dicho capítulo su descripción, formulación, justificación, objetivos generales, específicos de la investigación y metodología.

En el capítulo II, se presentan los antecedentes investigativos, la fundamentación normativa y legal, los principios teóricos referidos a la seguridad de la información, sistemas de gestión de la seguridad de la información.

En el capítulo III, se realiza la Descripción de la organización, Contextualización, el Diagnostico Actual GAP, Procedimientos MSPI, Roles y Responsabilidades, Gestión de Activos, Políticas de Seguridad y Privacidad de la Información y Plan de Sensibilización, Capacitación y Comunicación del MSPI.

En el capítulo IV, se presentan la Gestión de Riesgos, la Declaración de Aplicabilidad e Indicadores de Seguridad y Privacidad de la Información.

En el capítulo V, por último, se especifican los Resultados Esperados, Impactos Esperados, Cronograma, Presupuesto y Conclusiones del Proyecto.

CAPITULO I

1. Planteamiento del Problema de Investigación y su Justificación

1.1. Descripción del área problemática

Las Tecnologías de la Información y la Comunicación (TIC) han permeado todas las actividades del ser humano. Las organizaciones, sin duda, son una evidencia tangible de ello y los activos de éstas cada vez menos se valoran en terrenos edificios o muebles para volcarse hacia la información que manejan, información que es susceptible de transformarse en conocimiento y por supuesto en propuesta y oferta de valor. En este nuevo escenario, con la información como activo, su protección es fundamental. Ya no se habla de seguros, se habla de gestión de la seguridad de la información. Una organización que no proteja su principal activo está condenada a desaparecer.

Para el caso colombiano y acorde con los estudios realizados por la Cámara Colombiana de Informática y Telecomunicaciones - CCIT, a finales de octubre del 2022, se registraron en Colombia 54.121 eventos de ciberdelitos aumentando un 20,5% con respecto al 2021. de los cuales se incrementó un 34% el hurto por medios informáticos con 24.413 casos, le sigue con 62% el acceso abusivo a sistemas informáticos con 13.318 casos reportados, en tercer lugar, violación de datos personales se incrementó un 3% con 12.775 reportes. Las modalidades más utilizadas y en donde combinan la ingeniería social son el phishing[1],

[1] El término phishing, en informática, denota un uso de la ingeniería social para intentar adquirir información confidencial, por ejemplo, contraseñas, cuentas bancarias, datos de tarjetas de manera fraudulenta.

Smishing, escaneo, sim swapping, la suplantación de identidad, el envío de malware[2] y los fraudes en medios de pago en línea; lo que conlleva a que las empresas colombianas se vean afectadas por pérdida financiera, productividad, daños reputacionales e incluso implicaciones de carácter legal por fuga de información privilegiada y datos sensibles. El cibercrimen seguirá sofisticando su actuar delictivo y utilizará las capacidades tecnológicas disponibles a su favor como lo son [1] La inteligencia artificial y el malware, uso de perfiles falsos en redes sociales para difusión del malware, ataques BEC[3] basados en Deepfake[4], uso de Botnet[5] para difusión de correos extorsivos y el uso de mercados ilegales en DarkNet[6].

Si bien las empresas colombianas han avanzado en el último lustro en el tema, dos estudios concretos, uno realizado por la Cámara Colombiana de Informática y Telecomunicaciones, evidencian que aún hay mucho por hacer y que Colombia está ubicada en el puesto número 65 en el ranking global de seguridad cibernética.

A través de los decretos 2573 de 2014 y 1008 de 2018 del MinTIC, se establecen los lineamientos generales de la Política de Gobierno Digital para Colombia (antes estrategia de Gobierno en Línea) acerca del uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos e innovadores, que generen valor público en un entorno de confianza digital.

Con el fin de garantizar la seguridad de la información en las entidades públicas del orden nacional y territorial, el Gobierno Nacional en su Política de Gobierno Digital estableció

[2] Malware, programa malicioso que tiene como objetivo infiltrarse o dañar una computadora o sistema de información.
[3] De su sigla en inglés Business Email Compromise, o Correos Corporativos Comprometidos.
[4] La tecnología *Deepfake* es una técnica basada en Inteligencia Artificial, que coloca imágenes o videos sobre otro video, así como imitación de voces.
[5] Conjunto de ordenadores controlados remotamente por un atacante, los cuales pueden ser utilizados en conjunto para realizar actividades maliciosas como envío de spam y códigos maliciosos.
[6] Contenido oculto de Internet y solo puede accederse a través de navegadores específicos como Tor o I2P

un Modelo de Seguridad y Privacidad de la Información – MSPI - con la finalidad de conformar un Sistema de Gestión de Seguridad de la Información al interior de las entidades, con el propósito de promover las mejores prácticas de seguridad de la información y contribuir al incremento de transparencia en la gestión pública.

La Ley 1581 de 2012 establece las disposiciones generales para el tratamiento de datos personales aplicables a las entidades de naturaleza pública y privada, en donde se encuentran inmersas las entidades de salud, con el fin de garantizar la seguridad, confidencialidad y circulación restringida de la información, todos ellos enmarcados en el principio de responsabilidad demostrada (Accountability). Así mismo, mediante el Decreto 620 de 2020 MinTIC, en su capítulo 5 reitera que todas las entidades que conforman las ramas del poder público deben entre otras obligaciones: implementar un Programa Integral de Gestión de Datos Personales (PIGDP), designar una persona o área que asuma la función de protección de datos personales (oficial de privacidad), evaluar el impacto de sus operaciones en el tratamiento de datos personales; y contar con normas, políticas, procedimientos, recursos técnicos, administrativos y humanos, dirigidos a establecer estrategias de seguridad y privacidad de la información, seguridad digital y continuidad en la prestación del servicio.

La E.S.E. Hospital Universitario San Rafael de Tunja (HUSRT), es un ente social del estado que se rige bajo unas normas, leyes y estándares establecidos por el gobierno nacional que genera lineamientos para la gestión y administración de los recursos y que debe velar para que estos sean utilizados para el bienestar de las personas, en donde se ofrece servicios de salud de mediana y alta complejidad.

Basados en la visión, misión, objetivos corporativos, funciones del HUSRT, en las modelos, estándares, normas, leyes, internacionales y nacionales generados por el MinTIC, se

evidencia que lo que se ha desarrollado e implementado con respecto a el SGSI es muy básico, con incoherencias y de acuerdo al diagnóstico que se ha desarrollado se evidencia que se ha ejecutado el 30 %, lo cual se convierte en una debilidad para la entidad.

1.2. Formulación del problema

De lo anteriormente descrito, surge el siguiente interrogante: ¿Cómo diseñar un Sistema de Gestión de Seguridad de la Información para la E.S.E. Hospital Universitario San Rafael de Tunja(HUSRT), que dé cumplimiento no solo a los requerimientos regulatorios y procedimentales establecidos por el Gobierno Nacional, sino y particularmente importante que permita dar respuesta a las diferentes amenazas y vulnerabilidades a las que está expuesta la entidad, en el marco de las mejores prácticas existentes a nivel internacional?

1.3. Justificación

La información para cualquier organización es de vital importancia, y poder acceder a ella en cualquier momento es indispensable, garantizando su disponibilidad, integridad y seguridad de los datos, ya que ninguna entidad de salud está exenta de riesgos de pérdida y filtrado de información, que puedan utilizarse para alterar la privacidad de estos.

Las diferentes partes interesadas del proyecto manifiestan las siguientes inconformidades en cuestión de equipos e infraestructura tecnológica, sistemas de información, redes, procedimientos:

- Perdida de los equipos de cómputo, tables, celulares, USB, etc.
- Deterioro y daño en los activos de información.

- Accesos no restringidos a áreas muy reservadas.
- Equipos y sistemas obsoletos.
- Equipos sin licencias y sin antivirus.
- Equipos que utilizan varios usuarios.
- No tener claro los procedimientos de cada área por no estar documentados.
- No recibir capacitaciones para el cuidado, mantenimiento y aseguramiento de los activos de información.
- No recibir capacitaciones de seguridad y privacidad de la información.
- La gestión de el tratamiento de datos personales no es la mas adecuada por no tener identificados bien los activos de información
- En ocasiones los servicios tecnológicos (internet, sistemas de información) no funcionan adecuadamente.
- No contar con herramientas para realizar sus backups.
- Algunos formatos están desactualizados y no cumplen con las normas de seguridad de la información y tratamiento de datos.
- Los procedimientos para recibir y entregar los cargos de acuerdo a los activos de información no están bien especificados y se cumple en plenitud.
- El soporte para equipos tecnológicos y sistemas de información en ocasiones es muy lento.
- El no cumplir con la Política de Seguridad Digital en la especificación de algunas de sus directrices.

Mejorar o mitigar las inconformidades descriptas anteriormente inicialmente se puede realizar mediante la implementación de un modelo adecuado para la gestión de seguridad de la información, que reduciría el impacto que genera una alteración a la integridad de los datos, así

se pueden generar políticas, controles en los procedimientos utilizados en la organización y metodologías para análisis de riesgo de la información.

El adoptar un sistema de gestión basado en la Norma ISO 27001 alienado con el MPSI y que se complemente con los planes estratégicos de la empresa, permitirá abarcar los diferentes puntos de seguridad en los que se pueden exponer la información, lo cual constituye una gran ventaja tecnológica que permite a la empresa asegurar la continuidad del negocio y evitar filtración de información relevante que pueda ser usada para perjudicar o generar una desventaja frente a las empresas del gremio, así mismo al estar conscientes de los riesgos a los que está expuesta, permitiendo generar estrategias que abarquen o mitiguen estos riesgos.

Finalmente, este proyecto es factible, ya que puede ayudar a identificar que procesos, que son realizados al interior de la entidad pueden estar arriesgando la información ante una posible vulnerabilidad que no estaba siendo detectada y le permitirán mejorar la calidad de éstos, manteniendo los datos seguros ante cualquier riesgo y la entidad cumpliría con la Política de Seguridad Digital.

2. Objetivos

2.1. Objetivo General

Diseñar el sistema de gestión de seguridad de la información (SGSI) bajo el Modelo de Seguridad y Privacidad de la Información (MSPI) establecido por MinTIC, implementando la identificación de los Activos de Información con Criticidad Alta, la Gestión de los Riesgos y estableciendo los Controles de Seguridad y Privacidad de la Información para la E.S.E. Hospital Universitario San Rafael de Tunja (HUSRT) plasmados en la Declaración de Aplicabilidad.

2.2. Objetivos Específicos

a. Determinar e identificar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad y su nivel de madurez.
b. Realizar el diseño e implementar la identificación de los Activos de Información con Criticidad Alta, la Gestión de los Riesgos y establecer los Controles de Seguridad y Privacidad de la Información.
c. Generar la Declaración de Aplicabilidad que la entidad analizara para aprobar el tratamiento e implementación de controles de seguridad y privacidad de la información.

3. Metodología

Para cumplir de manera efectiva con los objetivos que se plantean en la presente investigación es necesario definir adecuadamente los elementos metodológicos en los cuales se contextualiza el presente trabajo.

3.1. Enfoque metodológico

Esta investigación es de tipo cualitativa la cual se caracteriza por no ser experimental; en este caso, el trabajo no posee hipótesis que requiere ser comprobada debido a que se parte de una realidad representada por la inexistencia de un modelo de gestión de seguridad de la información, con lo cual, se asocian una serie de riesgos y vulnerabilidades potenciales. Además, no se generan datos estadísticos, los resultados se traducen en un modelo expresado en palabras y no en cifras, es decir, se describe y analiza una situación y con base a esta se emite una opinión.

3.2. Tipo de estudio

La metodología investigativa del proyecto, alineada con la norma ISO 27001, permitirá que el diseño metodológico logre describir la estrategia de seguridad de la información que requiere la organización -el Ingenio Carmelita S.A.- de acuerdo con sus necesidades y características, y generar una transferencia de conocimiento que contribuye a la solución de problemas de seguridad de la información; por lo tanto, es posible afirmar que esta investigación es de tipo descriptiva con implementación práctica y aplicada.

3.3. Diseño de la investigación

El diseño del presente estudio es de tipo no experimental y transversal, pues las circunstancias y características del objeto de estudio no son modificables, no posee control pues ya han ocurrido, además no se tiene control sobre los efectos causados por las circunstancias vigentes en la organización

.

3.4. Técnicas e instrumentos de recolección de información

Para recolectar la información del presente trabajo de investigación se requiere lo siguiente:

a) La técnica de análisis documental, se emplearán documentos que tengan relación con la investigación.
b) La técnica de recolección de datos es la observación en base a la valoración de activos, riesgos y vulnerabilidades que se requieren para un adecuado diseño del modelo.
c) Se revisarán diversos instrumentos, como los suministrados por el MinTIC, los cuales permitirán adquirir información sobre el estudio y las brechas de cumplimiento de los requisitos de la norma ISO 27001.

3.5. Población de estudio

Desde una perspectiva metodológica, la población de estudio está conformada por parte del universo muestral [21], no obstante, en este tipo de investigación no se trabaja con una población específica debido a que el objeto, y tipología del trabajo, se requiere que se consideren como parte de los individuos relacionados con el objeto de estudio a toda la

población de la Institución que de alguna manera tenga incidencia en los activos de información, porque potencialmente son responsables desde distintas perspectivas de la seguridad y privacidad de la información.

3.6. Plan de análisis

El plan de análisis del proyecto puede resumirse en las siguientes fases y actividades:

3.6.1. Fase 1. Diagnóstico.

Para esta fase se tienen contempladas las siguientes actividades:

- Actividad 1. Diagnostico GAP.
- Actividad 2. Informe del Diagnóstico.

3.6.2. Fase 2. Planificación.

Para esta fase se tienen contempladas las siguientes actividades:

- Actividad 1. Alcance del MSPI.
- Actividad 2. Contexto de la entidad.
- Actividad 3. Partes interesadas.
- Actividad 4. Roles y responsabilidades
- Actividad 5. Gestión de Activos de Información
- Actividad 6. Política de Seguridad aprobada por la Alta Dirección.
- Actividad 7. Manual de Políticas de Seguridad y Privacidad de la Información.

- Actividad 8. Plan de comunicación, sensibilización y capacitación.

3.6.3. Fase 3. Implementación.

Para esta fase se tienen contempladas las siguientes actividades:

Actividad 1. Identificación y valoración de los riesgos

Actividad 2. Tratamiento de riesgos.

Actividad 3. Definir indicadores.

Actividad 4. Definir la Declaración de Aplicabilidad.

CAPITULO II

4. Antecedentes

Dado que la seguridad de la información tiene un papel importante en las organizaciones, se requiere de un estándar que determine las mejores prácticas a nivel internacional en materia de gestión de la seguridad de la información.

Actualmente existen diversos estándares para el gobierno y gestión de TI que contemplan como parte de sus prácticas, la seguridad de la información, entre las que se destacan: PRINCE2, OPM3, CMMI, P-CMM, PMMM, familia de normas ISO/IEC 27000, PCIDSS, COSO, SOA, ITIL y COBIT.

Un grupo de estudiantes de la Universidad de Brunei [4], realizaron un estudio comparativo de los cinco grandes normas del sistema de gestión de seguridad de la información ISO 27001, BS 7799, PCIDSS, ITIL y COBIT, cada estándar juega su propio rol y posición en la implementación de sistemas de gestión de seguridad de la información, los estándares ISO/IEC 27001 y BS 7799 se centran en el sistema de gestión de seguridad de la información como dominio principal, mientras que PCIDSS se enfoca en la seguridad de la información relacionada con las transacciones comerciales y tarjetas inteligentes, ITIL y COBIT se centran en la seguridad de la información y su relación con la gestión de proyectos y el gobierno de TI. El estándar ISO 27001 lidera las otras cuatro normas ya que es implementado más fácilmente y es muy reconocido por las partes interesadas (alta gerencia, personal, proveedores, clientes), además tiene un nivel de usabilidad y confianza de más del 80% en el mundo, de acuerdo con el estudio en mención.

Siendo la gestión del riesgo el insumo esencial para la implementación de un adecuado sistema de gestión de seguridad de la información, existen diversas metodologías de análisis y gestión de riesgos que han sido desarrolladas y aplicadas por la comunidad académica y profesional. Algunos ejemplos de ellos son los propuestos por Tejena-Macias [5] quienes recomiendan la metodología MAGERIT por brindar un mayor cubrimiento del riesgo, en la medida que contempla un análisis de riesgos más detallado, protegiendo los datos en los tres principios de seguridad de la información: integridad, disponibilidad, confidencialidad, con algunos aspectos adicionales como su confiabilidad y que no permite arbitrariedades del analista. Así mismo, Espinosa [6] argumenta que no es suficiente gestionar el riesgo de seguridad de la información solo con la norma ISO 27005, es necesario apoyarse en otras metodologías para el análisis y gestión del riesgo, como por ejemplo OCTAVE-s, ya que la norma ISO 27005 solo describe los pasos que se deben seguir para la gestión del riesgo, pero no explica las actividades que se deben llevar a cabo específicamente, lo que OCTAVE-s si determina. Benavides Carranza [7] revisa a profundidad cada una de las guías del Modelo de Seguridad y Privacidad de la Información (MPSI) e identifica que las directrices, dominios y controles establecidos en la Norma Técnica Colombiana ISO/IEC 27001 se encuentran adoptadas cien por ciento con el Modelo de Seguridad y Privacidad de la Información. Este marco metodológico contribuye a una mayor adaptación de la norma en la creación y desarrollo de un sistema de gestión de seguridad de la información. Este modelo está siendo implementado por las entidades gubernamentales, pero dado su integración con la Norma Técnica Colombiana NTC ISO 27001 puede ser implementado por empresas del sector privado.

5. Referente Normativo y Legal

La familia de las normas ISO/IEC 27000 [8], son un marco de referencia de seguridad a nivel mundial desarrollado por la International Organization for Standardization - ISO e International Electrotechnical Commission – IEC, que proporcionan un marco, lineamientos y mejores prácticas para la debida gestión de seguridad de la información en cualquier tipo de organización. Estas normas especifican los requerimientos que deben cumplir las organizaciones para establecer, implementar, poner en funcionamiento, controlar y mejorar continuamente un Sistema de Gestión de Seguridad de la Información. En Colombia, el Instituto Colombiano de Norma Técnicas y Certificaciones, ICONTEC, es el organismo encargado de normalizar este tipo de normas.

Las siguientes son algunas de las normas que componen la familia ISO/IEC 27000, las cuales estructuran el marco normativo del presente trabajo:

Tabla 1

Marco Normativo y Legal ISO 27.000

Norma	Descripción
ISO/IEC 27000:2018	Suministra información introductoria a seguridad de la información y a la gestión de la seguridad de la información, el estado y la relación de las normas de la familia de estándares para un SGSI.
ISO/IEC 27001:2013 (antigua BS 7799-2:2002)	Es una norma que admite certificación y especifica los requerimientos para la definición, implementación, implantación, mantenimiento y mejora de un SGSI.
ISO/IEC 27002:2013 (antigua ISO 17799:2005	Proporciona la guía de implementación de los controles aplicables a la seguridad de la información. Contiene once (11) cláusulas de control de la seguridad que contienen un total de treinta y nueve (39) categorías de seguridad e igual número de

	indicaciones de objetivos de Control. Estas cláusulas, objetivos de control y controles, son incorporados en el Anexo A de la norma ISO/IEC 27001.
ISO/IEC 27003:2017	Proporciona información práctica y una guía de implementación de la norma ISO/IEC 27001, indicando las directivas generales necesarias para la correcta implementación de un SGSI. Incluye instrucciones sobre cómo lograr la implementación de un SGSI con éxito.
ISO/IEC 27004:2016	Proporciona una guía y suministra recomendaciones para el desarrollo y uso de métricas para evaluar la efectividad de un SGSI, los objetivos de control y controles utilizados para implementar y gestionar la Seguridad de la Información, según la norma ISO/IEC 27001.
ISO/IEC 27005:2018 (antigua ISO TR 13335-3:1998 e ISO TR 13335-4:2000)	Proporciona una guía metodológica para la Gestión de Riesgos de una organización, alineada con los requerimientos de la norma ISO/IEC 27001.
ISO/IEC 27006:2015	Crea los requerimientos para organismos que prestan servicios de auditoría y certificación.
ISO/IEC 27007:2017	Provee una guía para la realización de las auditorías de un SGSI y la competencia de los auditores, de acuerdo a la norma ISO/IEC 27001.
ISO/IEC TR 27008:2011	Es un reporte técnico que brinda una guía para la revisión de la implementación de los controles del SGSI.
ISO/IEC 27009:2016	Detalla los requisitos para usar la norma ISO/IEC 27001 en cualquier otro ámbito. El documento explica cómo refinar e incluir requisitos adicionales a los de la norma ISO/IEC 27001 y cómo incluir controles o conjuntos de control adicionales
ISO/IEC 27010:2015	Provee una guía para gestionar la seguridad de la información en caso la organización intercambie o comparta información importante, ya sea que pertenezca al sector público o privado, que lo haga nacional o internacionalmente, o en el mismo sector u otros sectores del mercado en el que opera.
ISO/IEC 27011:2016	Provee una guía para apoyar la implementación de un SGSI en una empresa de telecomunicaciones.
ISO/IEC 27013:2015	Brinda una guía para la implementación integrada del ISO/IEC 27001 y el ISO/IEC 20000 (gestión de servicios de TI), ya sea implementándolos al mismo tiempo o uno después de otro.
ISO/IEC 27014:2013	Brinda una guía para conocer los principios y procesos del gobierno de la seguridad de la información, que busca que las

	organizaciones puedan evaluar, dirigir y monitorear la gestión de la seguridad de la información.
ISO/IEC 27015:2012	Es una guía de SGSI orientada a organizaciones del sector financiero y de seguros.
ISO/IEC TR 27016:2014	Es un reporte técnico que brinda una metodología que permite a las organizaciones saber cómo valorar adecuadamente los activos de información identificados, los riesgos potenciales a los activos, apreciar el valor de los controles que protegen a estos activos y determinar el nivel óptimo de recursos que deben ser usados para asegurarlos.
ISO/IEC 27017:2015	Es una guía de seguridad para Cloud Computing alineada con ISO/IEC 27002 y con controles adicionales específicos de estos entornos de nube.
ISO/IEC 27018:2014	Es un código de buenas prácticas en controles de protección de datos para servicios de computación en cloud computing.
ISO/IEC TR 27019:2017	Es una guía para el proceso de sistemas de control específicos relacionados con el sector de la industria de la energía.
ISO/IEC 27031:2011	Abarca todos los eventos e incidentes que se relacionan con la seguridad que puede tener un impacto en la infraestructura y los sistemas TIC. Incluye y se extiende a las prácticas de manejo de incidentes de seguridad de la información y la gestión de la planificación y preparación para las TIC y los servicios.
ISO/IEC 27032:2012	Ofrece unas líneas generales de orientación para fortalecer el estado de la ciberseguridad en una empresa, utilizando los puntos técnicos y estratégicos más importantes para esa actividad y los que están relacionados con la seguridad en las redes, seguridad en internet, seguridad de la información y la seguridad de las aplicaciones.
ISO/IEC 27033:2015	Provee una descripción general de los controles que soportan arquitecturas técnicas de seguridad de red y controles técnicos relacionados, así como aquellos controles no-técnicos y técnicos que son aplicables no sólo a las redes.
ISO/IEC 27034:2011	Proporciona una guía de seguridad de la información dirigida a los agentes de negocio y de TI, auditores y desarrolladores y los usuarios finales de las TIC, es decir, sirve para aquellas personas que llevan a cabo el diseño, programación, adquisición y uso de los sistemas de aplicación. La finalidad de dicha norma es asegurar que las aplicaciones informáticas conceden el nivel necesario o deseado de la seguridad en apoyo del Sistema de Gestión de Seguridad de la Información de las empresas.
ISO/IEC 27035:2011	Explica un enfoque de mejores prácticas destinado a la gestión de la información de incidentes de la seguridad. Los

	controles de la seguridad de la información no son perfectos debido a que pueden fallar, pueden trabajar solo parcialmente o incluso, a veces, están ausentes, es decir, no están en funcionamiento. Debido a esto, los incidentes pasan debido que los controles preventivos no son totalmente eficaces o fiables.
ISO/IEC 27036:2014	Guía en cuatro partes de seguridad en las relaciones con proveedores.
ISO/IEC 27037:2012	Está claramente orientada al procedimiento de la actuación pericial en el escenario de la recogida, identificación y secuestro de la evidencia digital, no entra en la fase de Análisis de la evidencia.
ISO/IEC 27038:2014	Es una guía de especificación para seguridad en la redacción digital.
ISO/IEC 27039:2015	Es una guía para la selección, despliegue y operación de sistemas de detección y prevención de intrusión.
ISO/IEC 27040:2015	Es una guía para la seguridad en medios de almacenamiento.
ISO/IEC 27041:2015	Es una guía para garantizar la idoneidad y adecuación de los métodos de investigación.
ISO/IEC 27042:2015	Es una guía con directrices para el análisis e interpretación de las evidencias digitales.
ISO/IEC 27043:2015	Desarrolla principios de investigación para la recopilación de evidencias digitales.
ISO/IEC 27050:2016	Desarrolla en tres partes sobre la información almacenada en dispositivos electrónicos en relación a su identificación, preservación, recolección, procesamiento, revisión, análisis y producción.
ISO/IEC 27103:2018	Es una norma desarrollada para proporcionar orientación sobre cómo aprovechar las normas existentes en un marco de ciberseguridad.
ISO/IEC TR 27701:2019	Este documento especifica los requisitos y proporciona orientación para establecer, implementar, mantener y mejorar continuamente un Sistema de gestión de información de privacidad (PIMS) a modo de extensión de ISO/IEC 27001 e ISO/IEC 27002 para la gestión de privacidad dentro del contexto de la organización. Especifica los requisitos relacionados con PIMS y proporciona orientación para los controladores y procesadores de PII que tienen la responsabilidad y la responsabilidad del procesamiento de PII.

Nota: Elaboración propia a partir de [4]

El MinTIC establece y hace referencia a las siguientes normas por las que se debe regir las entidades públicas a la hora de diseñar e implementar el modelo de Seguridad y Privacidad de la Información MSPI.

Tabla 2

Marco Normativo y Legal

Constitución Política de Colombia. Artículos 15, 209 y 269.
Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.
Decreto 2609 de 2012. Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
Decreto 886 de 2014. Por el cual se reglamenta el Registro Nacional de Bases de Datos.
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.
Decreto 103 de 2015. Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
Decreto 1074 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.
Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Decreto 1080 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector Cultura.

Decreto 1081 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia.
Decreto 1083 de 2015 “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública”, el cual establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de “11. Gobierno Digital, antes Gobierno en Línea” y “12. Seguridad Digital”.
CONPES 3854 de 2016. Política Nacional de Seguridad digital.
Ley 1915 de 2018. Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
Decreto 612 de 2018. Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
Decreto 2106 de 2019, establece que las autoridades que realicen trámites, procesos y procedimientos por medios digitales, deberán disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.
Ley 1952 de 2019. Por medio de la cual se expide el código general disciplinario
Constitución Política de Colombia. Artículos 15, 209 y 269.
Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.
Decreto 2609 de 2012. Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
Decreto 886 de 2014. Por el cual se reglamenta el Registro Nacional de Bases de Datos.

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.
Decreto 103 de 2015. Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
Decreto 1074 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.
Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Decreto 1080 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector Cultura.
Decreto 1081 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia.
Decreto 1083 de 2015 “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública”, el cual establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de “11. Gobierno Digital, antes Gobierno en Línea” y “12. Seguridad Digital”.
CONPES 3854 de 2016. Política Nacional de Seguridad digital.
Ley 1915 de 2018. Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
Decreto 612 de 2018. Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
Decreto 2106 de 2019, establece que las autoridades que realicen trámites, procesos y procedimientos por medios digitales, deberán disponer de una estrategia de seguridad digital

siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.
Ley 1952 de 2019. Por medio de la cual se expide el código general disciplinario

Nota: articles-162621_Modelo_de_Seguridad_y_Privacidad__MSPI [5]

6. Referente Conceptual

6.1. Seguridad de la Información (SI)

Existen muchas definiciones del término Seguridad de la Información y la mayoría cubre los conceptos globalmente aceptados de confidencialidad, integridad y disponibilidad. De ellas se adopta la definición ofrecida por el estándar ISO / IEC 27000:2018 tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Descripción general y vocabulario que fue aprobado por la International Organization for Standardization (ISO) y por la International Electrotechnical Commission (IEC). “La seguridad de la información consiste en la preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, también pueden estar involucradas otras propiedades, como la autenticidad, responsabilidad, la confiabilidad y el no repudio” [8].

a. La confidencialidad significa preservar las restricciones autorizadas sobre el acceso o divulgación, incluyendo los medios para proteger la privacidad y la información propietaria. La información o los datos confidenciales deben divulgarse únicamente a usuarios autorizados. Siempre que hablamos de confidencialidad en el ámbito de la seguridad de la información nos hemos de plantear un sistema de clasificación de la información [9].

b. La integridad significa proteger contra destrucción o modificación inadecuada de la información e incluye asegurar el no repudio y autenticidad de la información. La integridad de la información se refiere a la exactitud y consistencia generales de los datos o expresado de otra forma, como la ausencia de alteración cuando se realice cualquier tipo de operación con los datos, lo que significa que los datos permanecen intactos y sin cambios [9].

c. La disponibilidad significa asegurar que se puede acceder y usar la información de manera confiable y en el momento adecuado. Cuando un sistema no funciona regularmente, la disponibilidad de la información se ve afectada y afecta significativamente a los usuarios. Además, cuando los datos no son seguros y no están fácilmente disponibles, la seguridad de la información se ve afectada. Otro factor que afecta la disponibilidad es el tiempo, si un sistema informático no puede entregar información de manera eficiente, la disponibilidad se ve comprometida. El caso es que la información debe estar disponible para en todo momento, pero solo para aquellos con autorización para acceder a ella [9].

d. La autenticidad es la seguridad de que un mensaje, una transacción u otro intercambio de información proviene de la fuente de la que afirma ser. Autenticidad implica prueba de identidad. Podemos verificar la autenticidad a través de la autenticación. El proceso de autenticación usualmente involucra más de una "prueba" de identidad (aunque una puede ser suficiente) [9].

e. La responsabilidad es el requisito que permite que puedan trazarse las acciones de una entidad de forma única. A menudo, es un requisito de la política de la organización y soporta de forma directa el no repudio, la disuasión, el aislamiento de fallos, la detección y la prevención de intrusiones y, después, la acción de recuperación y las acciones legales pertinentes sujetas al Código Penal, reflejadas en las leyes de protección de datos, de comercio electrónico y de propiedad intelectual [10].

f. La confiabilidad es la garantía en que los objetivos anteriores se han cumplido adecuadamente. Es la base de la confianza en que las medidas de seguridad, tanto

técnicas, como operacionales, funcional tal y como se idearon para proteger el sistema y la información que procesa [10].

g. El no repudio es la capacidad para demostrar la ocurrencia de un evento o acción reclamada y sus entidades de origen. El no repudio es un concepto que garantiza que alguien no puede negar algo. En el contexto de la seguridad de la información, normalmente el no rechazo se refiere a la capacidad de garantizar que una parte de un contrato o una comunicación no pueda negar la autenticidad de su firma en un documento o el envío de un mensaje enviado por un origen determinado. El no repudio es una forma de demostrar que una información fue enviada por un origen hacia un destino [10].

6.2. Sistemas de Gestión (SG)

6.2.1. Sistema de Gestión de Riesgos.

En el contexto de los sistemas de gestión de seguridad de la información, los riesgos de seguridad de la información se pueden expresar como efecto de la incertidumbre sobre los objetivos de seguridad de la información. El riesgo de seguridad de la información está asociado con la posibilidad de que las amenazas aprovechen las vulnerabilidades de un activo de información o grupo de activos de información y, por lo tanto, causen daños a una organización. Una amenaza, son circunstancias o eventos que tiene la probabilidad de ocasionar daño a un recurso de información al explotar las vulnerabilidades del sistema. Las amenazas pueden ser externas o internas, intencionales o accidentales. Pueden ser causadas por eventos naturales o factores

políticos, económicos o competitivos. La probabilidad es una medida de la frecuencia en que puede ocurrir un evento. Cuando se identifica el riesgo, la probabilidad se utiliza para calcular el nivel del riesgo en base a la cantidad de eventos combinado con el impacto que pudiera ocurrir en un determinado periodo de tiempo. Cuanto mayor es la frecuencia, mayor probabilidad y, en consecuencia, mayor el riesgo. Una vulnerabilidad, a la que muchas veces se le refiere como “debilidad”, se utiliza, generalmente, como si fuera una condición binaria. Algo “es vulnerable” o “no es vulnerable”. Una evaluación de vulnerabilidades debe considerar las debilidades del proceso y procedimiento, así como las debilidades lógicas. Si existen vulnerabilidades, existe la posibilidad de riesgo. El Impacto es el elemento fundamental para la gestión de riesgos. En definitiva, todas las actividades de gestión de riesgos están diseñadas para reducir los impactos a niveles aceptables con el fin de crear o preservar el valor para la organización. El resultado de cualquier vulnerabilidad que sea explotada por una amenaza y ocasione una pérdida se llama impacto. Las amenazas y las vulnerabilidades que no causan un impacto son, normalmente, irrelevantes y, en general, no se consideran un riesgo [11]. Todo lo anterior puede observarse en la figura 1.

Figura 1,

Análisis y Gestión de Riesgos [12]

La gestión de riesgos significa que el riesgo se gestiona de forma tal que no tenga un impacto significativo en el proceso del negocio, y que se establezcan los niveles aceptables de aseguramiento y previsibilidad sobre los resultados deseados de cualquier actividad importante de la organización. La gestión de riesgos, el desarrollo de un BIA[7], la creación de un inventario de activos de información y el análisis de riesgos son requerimientos previos fundamentales para desarrollar una estrategia de seguridad significativa. Las organizaciones que desarrollan un programa de gobierno de la seguridad de la información, incluyen la gestión de riesgos como una parte integral del programa en su conjunto, la gestión de riesgos se cumple al equilibrar la exposición al riesgo con los costos de mitigación y al implementar controles y contramedidas apropiados. Los controles se diseñan como parte del marco de gestión de riesgos de la información, que incorpora políticas, estándares, procedimientos, prácticas y estructuras organizacionales que sirve para regular una actividad que mitigue o reduzca riesgos.

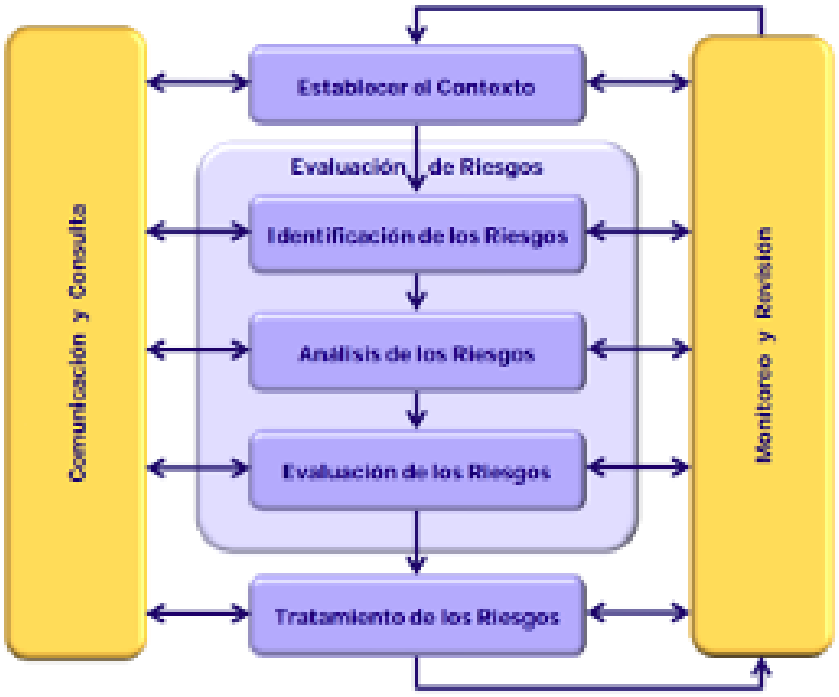
[7] Análisis de Impacto del Negocio, por su sigla en inglés (Business Impact Analysis)

Las contramedidas incluyen cualquier proceso que sirva para contrarrestar amenazas específicas y se pueda considerar como un control dirigido.

Existen múltiples metodologías para llevar a cabo el proceso de análisis, evaluación y gestión de riesgos informáticos, cada uno con su particularidad y dirigidos a ciertas situaciones. Sin embargo, todos tienen unos componentes y actividades comunes [13] como se visualiza en la figura 2.

Figura 2.

Proceso de Gestión del Riesgo [14]



a. Identificar el riesgo: La identificación del riesgo es el proceso mediante el cual se determina el tipo y la naturaleza de las amenazas visibles y se examinan las vulnerabilidades de la organización que están sujetas a esas amenazas.

- Identificar los activos: Proceso en el cual se identifican cuáles son los activos que son críticos y que tienen un impacto directo en la confidencialidad, integridad y disponibilidad de las fuentes de información para la organización.
- Identificar amenazas: Se enfoca en identificar las posibles amenazas a la seguridad de la información. Estas amenazas son los eventos, fuentes y acciones que podrían liderar a perjudicar los activos relativos a la información de la organización.
- Identificar vulnerabilidades: Se enfoca en identificar las vulnerabilidades que podrían ser explotadas por las amenazas que se han identificado. La existencia de una vulnerabilidad contribuye a calcular la probabilidad del riesgo.

b. Análisis de riesgos: El análisis de riesgos es la fase en la cual se valoran y entienden tanto el nivel del riesgo identificado como su naturaleza y las posibles consecuencias del compromiso determinado. También incluye la determinación de la efectividad de los controles existentes y el punto hasta el cual mitigan el riesgo identificado.

- Determinar el impacto: Es el proceso para medir o determinar el impacto de una amenaza sobre un activo. El impacto puede ser cuantitativo o cualitativo.
- Determinar la probabilidad: El objetivo de esta actividad es medir la posibilidad de ocurrencia de una amenaza asignándole un valor probable.
- Identificar los controles: Los controles son mecanismos que detectan o previenen las fuentes de amenazas que tratan de explotar las vulnerabilidades. Esta actividad consiste en identificar qué controles se están efectuando actualmente sobre un activo y qué efecto tendría sobre la amenaza que se está evaluando.

c. Evaluación del Riesgo: Durante la fase de evaluación del riesgo, se deben tomar decisiones con respecto a qué riesgos necesitan ser tratados y las prioridades de tratamiento basándose en el análisis correspondiente. Si el riesgo cumple con los criterios de riesgos aceptables, es probable que la opción de tratamiento sea aceptada. Si el riesgo excede el nivel aceptable y no está dentro de la variación de tolerancia, es más probable que el tratamiento consista en alguna forma de mitigación. Un riesgo anterior a la mitigación se denomina riesgo inherente. Los riesgos que permanecen después de que se han implementado controles y contramedidas son riesgos residuales. El riesgo nunca es eliminado; el riesgo residual siempre permanece [11].

d. Tratamiento de riesgos: Con el objetivo de mantener un sistema u organización lo más seguro posible, es necesario definir el tratamiento que se le dará a los riesgos analizados y valorados. Las aplicaciones de estas medidas deben estar enfocadas principalmente en aquellos riesgos que representen un impacto tan nefasto que afecte a un grupo considerable de personas o que encauce una total detención de los servicios; es decir, aquellos que sean clasificados como moderados o catastróficos. De igual forma, se encuentran los riesgos cuyas probabilidades de realización sean medios o altos. Para mitigar estos riesgos es necesario desarrollar estrategias de gestión de riesgos que permitan reducirlos a niveles aceptables. Dentro de estas se encuentran las siguientes [15]:

- Mitigar o reducir el riesgo: Este enfoque utiliza varios mecanismos de control para mitigar los riesgos identificados. Estos controles pueden ser técnicos, administrativos o físicos y el objetivo es reducir la probabilidad o impacto del riesgo.

- Asignar o transferir el riesgo: Permite transferir el riesgo de una organización a otra entidad.
- Aceptar el riesgo: En este enfoque las organizaciones conocen y están conscientes de los riesgos, pero el costo de mitigarlos supera al valor del activo que se desea proteger.
- Eliminar el riesgo: Las organizaciones definitivamente deciden no tomar el riesgo; es decir, que la pérdida potencial excede el valor de la ganancia potencial en caso de continuar con una actividad riesgosa. Se elimina la amenaza por medio del cambio de los recursos o de la infraestructura informática.

e. Monitoreo y revisión: Componentes importantes del ciclo de vida de la gestión de riesgos son el monitoreo continuo, la evaluación, la valoración y el informe de riesgos. Tanto los resultados como el estado de este análisis continuo necesitan documentarse e informarse a la alta dirección con periodicidad. A medida que ocurren los cambios en una organización, la evaluación del riesgo debe actualizarse para asegurar su precisión continuada [9].

f. Comunicación, capacitación y concientización: Las personas, normalmente, representan el mayor riesgo para cualquier organización, en general, mediante accidentes, errores, falta de conocimiento, información y, de vez en cuando, intentos maliciosos. Implementar campañas apropiadas de capacitación y concientización puede hacer una contribución positiva sustancial a la gestión del riesgo. Muchos controles son de procedimientos y requieren de conocimiento operativo y cumplimiento. Se deben configurar y operar correctamente los controles técnicos para brindar el nivel esperado de aseguramiento.

6.2.2. Metodologías de Gestión de Riesgos

Existen numerosos modelos de gestión de riesgos y enfoques de evaluación diferentes. El enfoque seleccionado se debe determinar por la mejor forma, ajuste y función. Algunas de las metodologías para el análisis, gestión y evaluación de riesgos son las siguientes:

NTC ISO/IEC 27005:2011: Es un estándar internacional desarrollado por la ISO (International Standards Organization) el cual lleva como nombre Tecnología de la Información, Técnicas de Seguridad y Gestión del Riesgo en la Seguridad de la Información (Information Technology-Security-Techniques-Information-Security Risk Management). Provee una guía sobre los procesos de gestión del riesgo de la seguridad de la información que son necesarios para la implementación efectiva de un Sistema de Gestión de la Seguridad de la Información (SGSI. ISMS, Information Security Management Systems). ISO 27005 está fuertemente alineado con NIST SP 800-30. Plantea seis etapas para gestionar la evaluación del riesgo [13]:

- Establecimiento del contexto
- Valoración del riesgo
- Tratamiento del riesgo
- Aceptación del riesgo
- Comunicación del riesgo
- Monitorización y revisión del riesgo

NTC ISO / IEC 31000:2018: Norma de Gestión del Riesgo. Principios y directrices. La norma ISO 31000 es una herramienta que proporciona los principios, el marco y un proceso para una adecuada gestión de riesgos, puede ser utilizado por cualquier organización, independientemente de su tamaño, actividad o sector. El uso de

la ISO 31000 puede ayudar a las organizaciones a incrementar la probabilidad de alcanzar los objetivos, mejorar la identificación de oportunidades y amenazas, y asignar y utilizar recursos efectivamente para el tratamiento del riesgo. Sin embargo, la ISO 31000 no puede utilizarse con fines de certificación, sólo proporciona una orientación para programas de auditoría interna o externa, por ello sus lineamientos deberían ser adaptados en las empresas en lugar de adoptados. La norma ISO 31000 tiene un enfoque de procesos, por tanto, debe seguir una serie de pasos para que sea eficaz y cumpla con los objetivos trazados. Los pasos básicos son [16]:

- Establecer el contexto estratégico
- Identificar los riesgos
- Analizar el riesgo
- Valoración de los riesgos
- Tratamiento de los riesgos
- Monitorización y revisión
- Comunicar y consultar

OCTAVE: Acrónimo de Operationally Critical Threat, Asset, and Vulnerability Evaluation. (Evaluación Crítica Operacional de Amenazas, Activos y Vulnerabilidades). Es una colección de herramientas, técnicas y métodos para la evaluación de riesgos de la seguridad de la información. Fue desarrollado por el Instituto de Ingeniería de Software (Software Engineering Institute, SEI) de Carnegie Mellon a través de su programa CERT. Actualmente presenta tres versiones: OCTAVE, OCTAVE-S y OCTAVE-Allegro. OCTAVE es usado en grandes organizaciones (más de 300 empleados) y provee los lineamientos para realizar evaluaciones de seguridad internas, este marco recomienda la participación de una amplia variedad de personas, muchas de las cuales no están directamente involucradas en la función de gestión de riesgos. OCTAVE-S fue

desarrollado para empresas pequeñas (S, Small, de menos de 100 empleados), requiere un equipo de 3 a 5 personas y asume que las personas encargadas de realizar la evaluación de riesgos conocen los activos, requerimientos de seguridad, amenazas y prácticas de seguridad de la organización, y que no requieren de la realización de entrevistas, encuestas y talleres. OCTAVE-Allegro es la versión más reciente y fue direccionado para la evaluación de los riesgos de seguridad de la información, y describe ocho pasos y provee varias hojas de cálculo y cuestionarios como guías y modelos para evaluar los riesgos de la organización o más específicamente, sus activos. Los ocho pasos de OCTAVE Allegro son [13]:

- Establecer criterios de medición de los riesgos
- Desarrollar un perfil de activos de información
- Identificar contenedores de activos de información (activos que contienen información)
- Identificar áreas de preocupación (condición o situación del mundo real que puede afectar un activo
- Identificar escenarios de amenaza
- Identificar riesgos
- Análisis de riesgos
- Selecciona el enfoque de mitigación

NIST SP800-30: Es conocido como la Guía para la Gestión del Riesgo para los Sistemas de Tecnologías de la Información (Risk Management Guide for Information Technology Systems), el cual fue desarrollado por el NIST (National Institute for Standards and Technology, Instituto Nacional para los Estándares y Tecnología). Fue diseñado para ser flexible y adoptado por organizaciones de diferentes tipos. Se descompone en nueve etapas para desglosar sus actividades, las cuales son [17]:

- Caracterización del Sistema
- Identificación de las Amenazas
- Identificación de las Vulnerabilidades
- Análisis de Control
- Determinación de Probabilidad
- Análisis del Impacto
- Determinación del Riesgo
- Recomendaciones de Control
- Documentación de Resultados

MAGERIT: Methodology for Information Systems Risk Analysis and Management Metodología de Análisis y Gestión de Riesgos de TI. MAGERIT es la metodología de análisis y gestión de riesgos elaborada por el antiguo Consejo Superior de Administración Electrónica de España (actualmente Comisión de Estrategia TIC), implementa el proceso de gestión de riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información. MAGERIT propone la realización de cuatro pasos para efectuar el análisis de riesgos [17]:

- Caracterización de los activos
- Caracterización de las amenazas
- Caracterización de las salvaguardas
- Estimación del estado del riesgo

CRAMM: CCTA Risk Analysis and Management Method. CRAMM es una metodología de análisis de riesgos desarrollada en Reino Unido por la Agencia Central de Cómputo y Telecomunicaciones (CCTA) comenzó a desarrollarse en la década de

1980. Es el método de análisis de riesgos preferente en organismos de la administración pública británica. La metodología define tres fases para la realización del análisis de riesgos [17]:

- Establecimiento del objetivo de seguridad
- Evaluación de riesgos
- Identificación y selección de contramedidas

COBIT: Objetivos De Control Para La Información y La Tecnología Relacionada. se concibe como un marco creado por ISACA para la tecnología de la información (TI) y el Gobierno de TI. Se trata de un conjunto de herramientas de apoyo que permite a los administradores cerrar la brecha entre las necesidades de control, aspectos técnicos y los riesgos de negocio. COBIT define 34 procesos genéricos para la gestión de TI. Cada proceso es definido con sus entradas y salidas, además de las actividades, sus objetivos, las medidas de rendimiento y un modelo de madurez elemental, con los siguientes componentes [18]:

- Estrategia
- Procesos
- Organización
- Tecnología
- Gestión de recursos
- Gestión de riesgos
- Medición

Metodología para la administración del riesgo y el diseño de controles en entidades públicas de Colombia. Es una metodología del Departamento Administrativo de la Función Pública –DAFP-, para hacer la administración del riesgo de gestión,

corrupción y seguridad digital más sencilla y evitar duplicidades o reprocesos. El DAFP presenta la metodología como una herramienta que permite el manejo del riesgo, así como el control en todos los niveles de la entidad pública, mediante las siguientes fases que se encuentran alineadas con la ISO 31000 [19]:

- Política de administración de riesgos
- Identificación de riesgos
- Valoración de riesgos

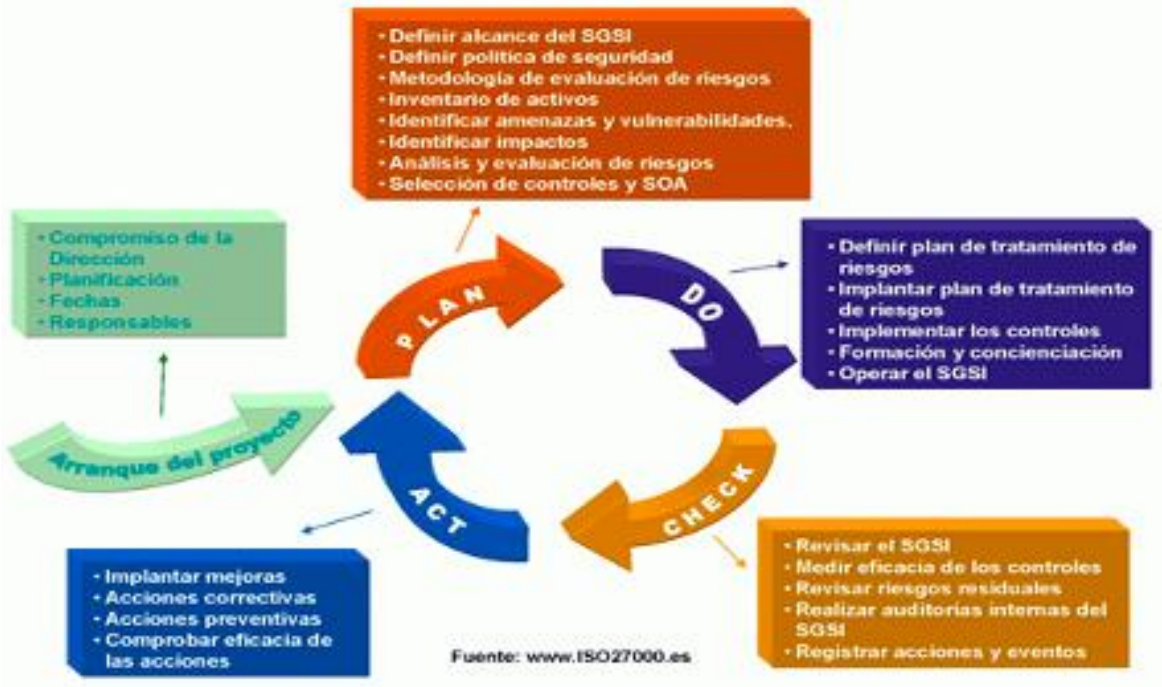
6.2.3. Sistema de Gestión Seguridad de la Información (SGSI).

Un Sistema de Gestión de Seguridad de la información (SGSI), según la norma ISO/IEC 27001 es una parte del sistema de gestión general, basada en un enfoque de riesgo empresarial, que establece para crear, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información. El modelo de gestión de la seguridad debe contemplar unos procedimientos adecuados y la planificación e implantación de controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de los mismos. Con un SGSI, la organización conoce los riesgos a los que está sometida su información y los asume, minimiza, transfiere o controla mediante una sistemática definida, documentada y conocida por todos, que se revisa y mejora constantemente [20].

Para la implantación de un Sistema de Gestión de la Seguridad de la Información, se requiere el desarrollo de actividades que marquen un orden lógico para llevar organizado todo el proceso. El modelo PDCA (Plan, Do, Check, Act) conocido como “Ciclo Deming” en su equivalencia en español es Planificar, Hacer, Verificar, Actuar (PHVA), es una estrategia de mejora continua de calidad en cuatro pasos como se indica en la figura 3.

Figura 3.

Ciclo Deming [20]



Las fases son las siguientes:

a. Planificación: Esta fase sirve para planificar la organización básica y establecer los objetivos de la seguridad de la información y para escoger los controles adecuados de seguridad (la norma contiene un catálogo de 133 posibles controles). Esta fase está formada por los siguientes pasos:

   - Determinación del alcance del SGSI;
   - Redacción de una Política de SGSI;
   - Identificación de la metodología para evaluar los riesgos y determinar los criterios para la aceptabilidad de riesgos;
   - Identificación de activos, vulnerabilidades y amenazas;
   - Evaluación de la magnitud de los riesgos;
   - Identificación y evaluación de opciones para el tratamiento de riesgos;

- Selección de controles para el tratamiento de riesgos;
- Obtención de la aprobación de la gerencia para los riesgos residuales;
- Obtención de la aprobación de la gerencia para la implementación del SGSI;
- Redacción de una declaración de aplicabilidad que detalle todos los controles aplicables, determine cuáles ya han sido implementados y cuáles no son aplicables.

b. Implementación: esta fase implica la realización de todo lo planificado en la fase anterior.

c. Revisión: el objetivo de esta fase es monitorear el funcionamiento del SGSI mediante diversos “canales” y verificar si los resultados cumplen los objetivos establecidos. Esta fase incluye los siguientes pasos como:
   - Implementación de procedimientos y demás controles de supervisión y control para determinar cualquier violación, procesamiento incorrecto de datos, si las actividades de seguridad se desarrollan de acuerdo a lo previsto, etc.;
   - Revisiones periódicas de la eficacia del SGSI;
   - Medición la eficacia de los controles;
   - Revisión periódica de la evaluación de riesgos;
   - Auditorías internas planificadas;
   - Revisiones por parte de la dirección para asegurar el funcionamiento del SGSI y para identificar oportunidades de mejoras;
   - Actualización de los planes de seguridad para tener en cuenta otras actividades de supervisión y revisión;
   - Mantenimiento de registros de actividades e incidentes que puedan afectar la eficacia del SGSI.

d. Mantenimiento y mejora: el objetivo de esta fase es mejorar todos los incumplimientos detectados en la fase anterior. Esta fase incluye los siguientes pasos como:
    - Implementación en el SGSI de las mejoras identificadas;
    - Toma de medidas correctivas y preventivas y aplicación de experiencias de seguridad propias y de terceros;
    - Comunicación de actividades y mejoras a todos los grupos de interés.
    - Asegurar que las mejoras cumplan los objetivos previstos.

6.3. Modelo de Seguridad y privacidad de la Información (MSPI).

El Ministerio de Tecnologías de la Información y Comunicaciones (TIC) a través del Marco de Referencia de Arquitectura TI soporta transversalmente los componentes de la Estrategia GEL: TIC para Servicios, TIC para Gobierno Abierto y TIC para Gestión, el Modelo Integrado de Planeación y Gestión (MIPG) y La Guía para la Administración del Riesgo y el Diseño Controles en entidades Públicas, genero el MSPI en donde especifica los lineamientos de las buenas prácticas en Seguridad y Privacidad de la Información que se deben implementar en las entidades del estado, referenciado del estándar internacional ISO 27001 y que es de cumplimiento de la Política de Gobierno Digital.

El MSPI es de estricto cumplimiento para las entidades públicas el cual debe ser integrado en los procesos, tramites, servicios, sistemas de información, infraestructura en donde su objetivo principal es preservar la confidencialidad, integridad y disponibilidad de todos los activos de información.

El diseño e implementación del MSPI se le asigna un Líder o Encargado de la Seguridad y Privacidad de la información, que velara por el cumplimento de este a través del

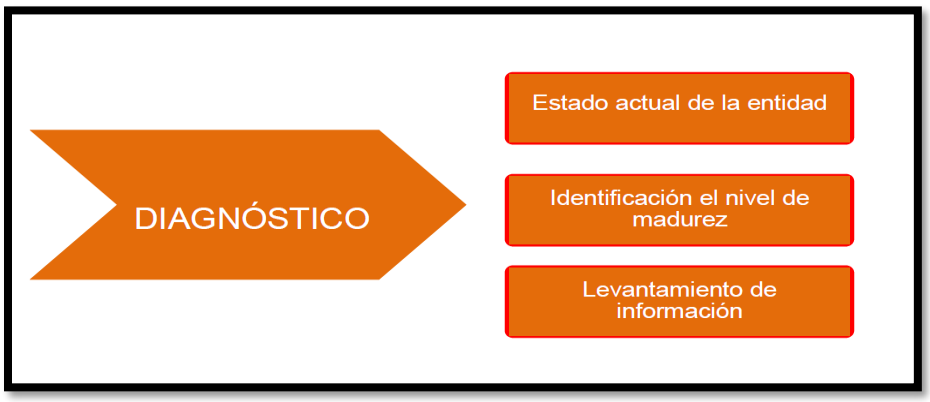
ciclo de vida PHVA (Planificar, Verificar, Hacer y Actuar) y que se desarrollara y ejecutara a través de las siguientes fases:

6.3.1. Fase de Diagnostico

Se identifica el estado actual de la organización con respecto al cumplimiento de la Seguridad y Privacidad de la Información, para esto se recomienda utilizar el Instrumento de Evaluación generado por el MinTIC.

Figura 4

MSPI - Diagnostico



En la fase de diagnóstico del MSPI se pretende alcanzar las siguientes metas:

- Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad.
- Determinar el nivel de madurez de los controles de seguridad de la información.
- Identificar el avance de la implementación del ciclo de operación al interior de la entidad.
- Identificar el nivel de cumplimiento con la legislación vigente relacionada con protección de datos personales.

- Identificación del uso de buenas prácticas en ciberseguridad.

Para ello se recomienda utilizar los siguientes instrumentos:

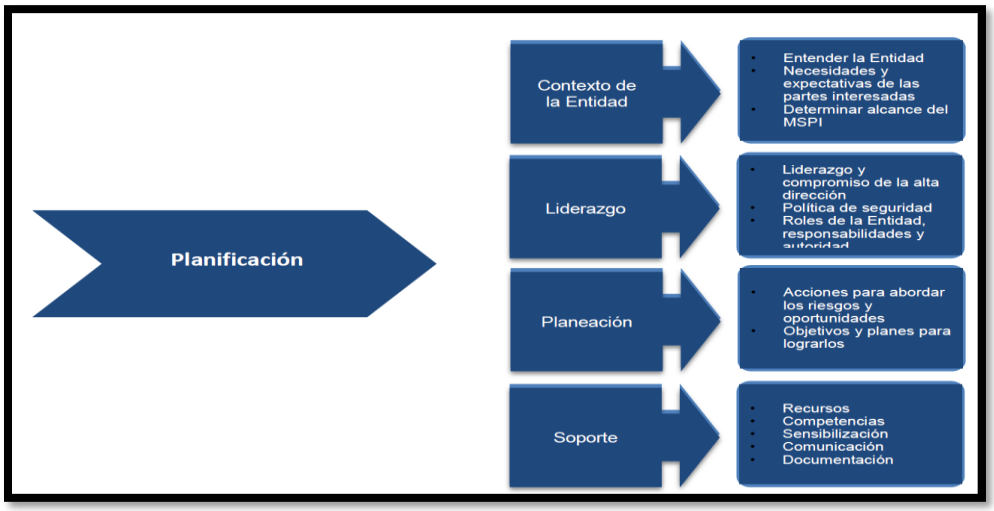
- Herramienta de diagnostico
- Instructivo para el diligenciamiento de la herramienta
- Guía No 1 - Metodología de Pruebas de Efectividad

6.3.2. Fase de Planificación

Para esta fase de debe generar El Alcance del MSPI, El Contexto de la Entidad, la Política General del MSPI, Procedimientos de Seguridad y Privacidad de la Información, Roles y Responsabilidades de Seguridad y Privacidad de la Información, Gestión de Activos, Transición Ipv4 a Ipv6, Integración del MSPI con la Gestión Documental, Gestión de Riesgos.

Figura 5

MSPI - Planificación

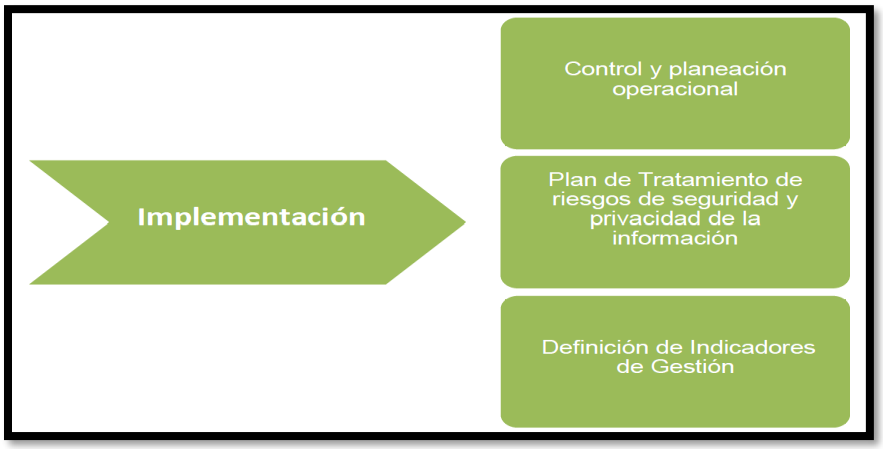


6.3.3. Fase de Implementación

En esta fase se lleva a cabo la implementación de la planificación especificada en la fase anterior y de ella se obtienen el Plan de Tratamiento de Riesgos, la Declaración de Aplicabilidad y los Indicadores de Gestión de Seguridad de la Información.

Figura 6

MSPI – Implementación

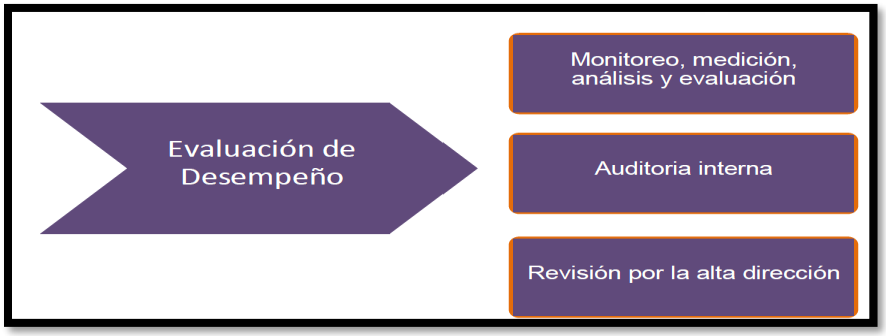


6.3.4. Fase de Evaluación de Desempeño

En esta fase se realiza seguimiento y monitoreo a los controles e indicadores especificados en la fase anterior en donde valida la eficiencia y eficacia a través de un Plan de Seguimiento y Revisión del MSPI y un Plan de Ejecución de Auditorias.

Figura 7

MSPI - Evaluación de Desempeño

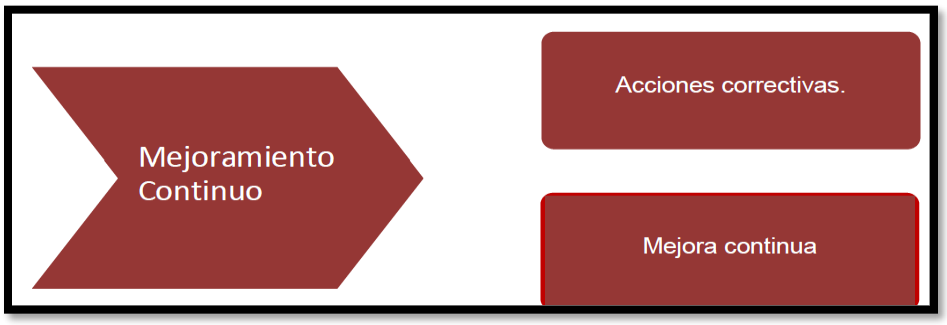


6.3.5. Fase de Mejora Continua

Acorde a las auditorias y al seguimiento por medio de los indicadores se diseña el Plan de Mejoramiento Continuo de Seguridad y Privacidad de la Información en donde se plasman las acciones que se van a implementar acorde a las debilidades encontradas y las cuales se van a mitigar.

Figura 8

MSPI – Mejora Continua.



Para el diseño y ejecución de cada una de las fases del MSPI, el MinTIC, facilita las guías que proporcionan el modelo, a continuación, se describen. Clic sitio web:

- Guía 1 - Metodología de pruebas de efectividad
- Guía 2 - Política General MSPI v1
- Guía 3 - Procedimiento de Seguridad de la Información
- Guía 4 - Roles y responsabilidades
- Guía 5 - Gestión Clasificación de Activos
- Guía 6 - Gestión Documental
- Guía 7 - Gestión de Riesgos
- Guía 8 - Controles de Seguridad de la Información
- Guía 9 - Indicadores Gestión de Seguridad de la Información
- Guía 10 - Continuidad de Negocio
- Guía 11 - Análisis de Impacto de Negocio
- Guía 12 - Seguridad en la Nube
- Guía 13 - Evidencia Digital
- Guía 14 - Plan de comunicación, sensibilización, capacitación
- Guía 15 – Auditoria
- Guía 16 - Evaluación de Desempeño
- Guía 17 - Mejora continua
- Guía 18 - Lineamientos terminales de áreas financieras de entidades públicas.
- Guía 19 - Aseguramiento de protocolo IPv4_IPv6
- Guía 20 - Transición IPv4_IPv6
- Guía 21 - Gestión de Incidentes

CAPITULO III

7. Descripción de la Organización

7.1. Misión E.S.E. HUSRT

Somos una Empresa Social del Estado de mediana y alta complejidad que ofrece los servicios de salud a los Usuarios y sus familias a través de talento humano idóneo y comprometido. Contamos con tecnología que garantiza la seguridad en la atención humanizada, contribuyendo a la gestión del conocimiento generando confianza, desarrollo, calidad de vida y responsabilidad social a nuestra comunidad.

7.2. Visión E.S.E. HUSRT

En el 2026 seremos un hospital universitario reconocido por su liderazgo en investigación, innovación y gestión clínica, generando impacto social a usuarios, colaboradores y el entorno.

7.3. Funciones E.S.E. HUSRT

- Contribuir al desarrollo social del país mejorando la calidad de vida, y reduciendo la morbilidad, la mortalidad, la incapacidad, el dolor y la angustia evitables en la población usuaria, en la medida en que esté a su alcance

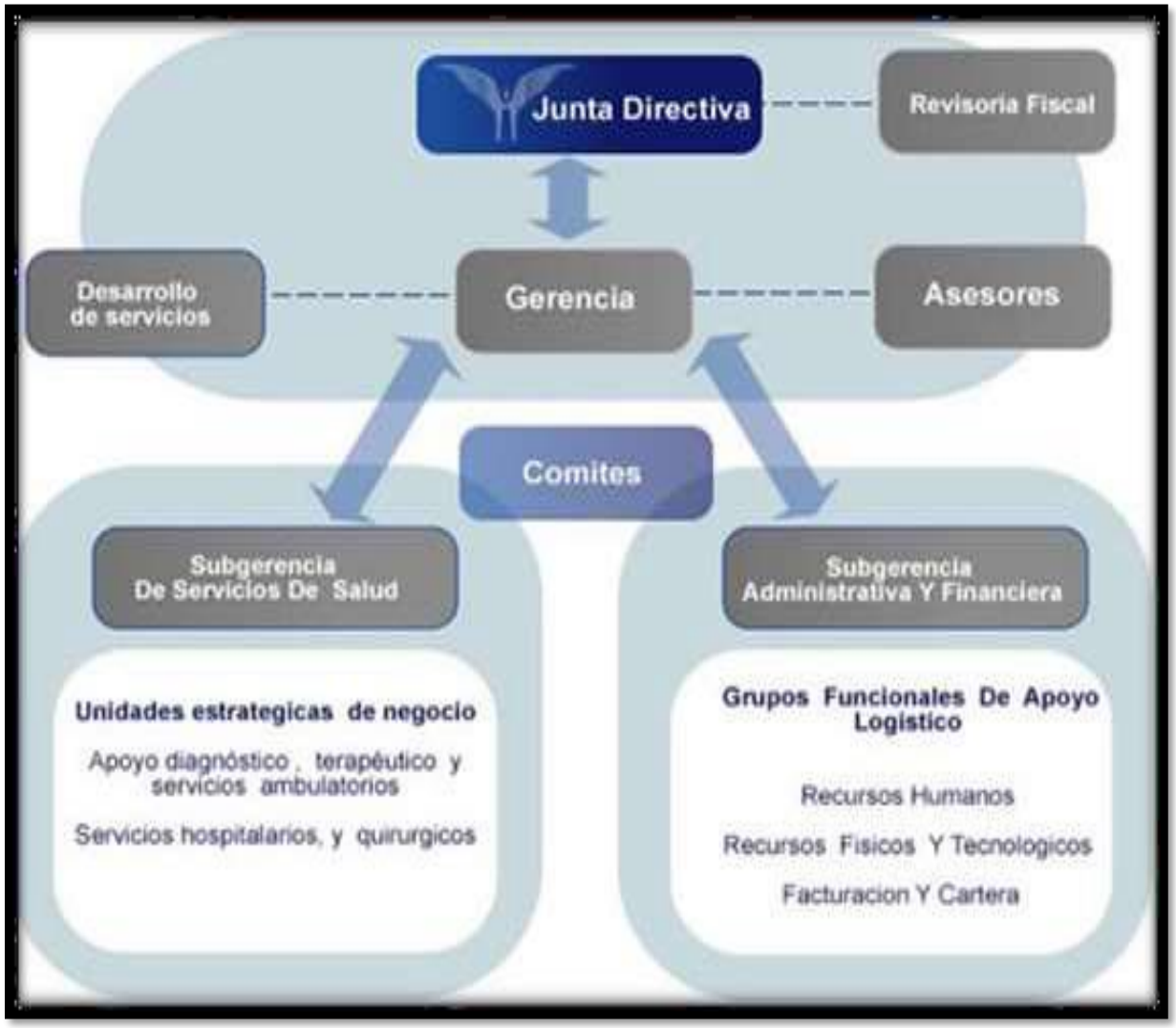
- Producir servicios de salud eficientes y efectivos, que cumplan con las normas de calidad establecidas, de acuerdo con el decreto de la reglamentación que se expida para tal propósito.
- Prestar los servicios de salud que la población requiera y que la empresa, de acuerdo con su desarrollo y recursos disponibles, pueda ofrecer.
- Garantizar, mediante un manejo gerencial adecuado, la rentabilidad social y financiera de la empresa.
- Ofrecer a las entidades promotoras de salud, Administradoras de Régimen Subsidiado, Administradoras de Riesgos Profesionales y demás personas naturales o jurídicas que lo demande, Servicios de Salud y paquetes de servicios a tarifas competitivas en el mercado.
- Satisfacer los requerimientos del entorno adecuando continuamente los servicios y funcionamiento propendiendo por prestar servicios de salud correspondientes al tercero y cuarto nivel de atención.
- Garantizar los mecanismos de participación ciudadana y comunitaria establecidos por la ley y los reglamentos.
- Prestar servicios de salud que satisfagan de manera óptima las necesidades y expectativas de la población en relación con la promoción, el fomento, y la conservación de la salud y la prevención, tratamiento y rehabilitación de la enfermedad.
- Contribuir a la satisfacción de las necesidades esenciales y secundarias de salud de los usuarios a través de acciones organizativas, técnico-científicas y técnico-administrativas.
- Desarrollar la estructura y capacidad operativa de la Empresa mediante la aplicación de principios y técnicas gerenciales que aseguren su supervivencia, crecimiento, calidad de sus recursos, capacidad de compartir en el mercado y rentabilidad social y financiera.
- Contribuir a la formación y capacitación de los directivos y funcionarios de la empresa.
- Impulsar y desarrollar proyectos de investigación para mejorar la calidad en el servicio y la gestión.

- Promover la coordinación interinstitucional e intersectorial que permita un trabajo conjunto con fines de impacto social.

7.4. Estructura Orgánica

Figura 9

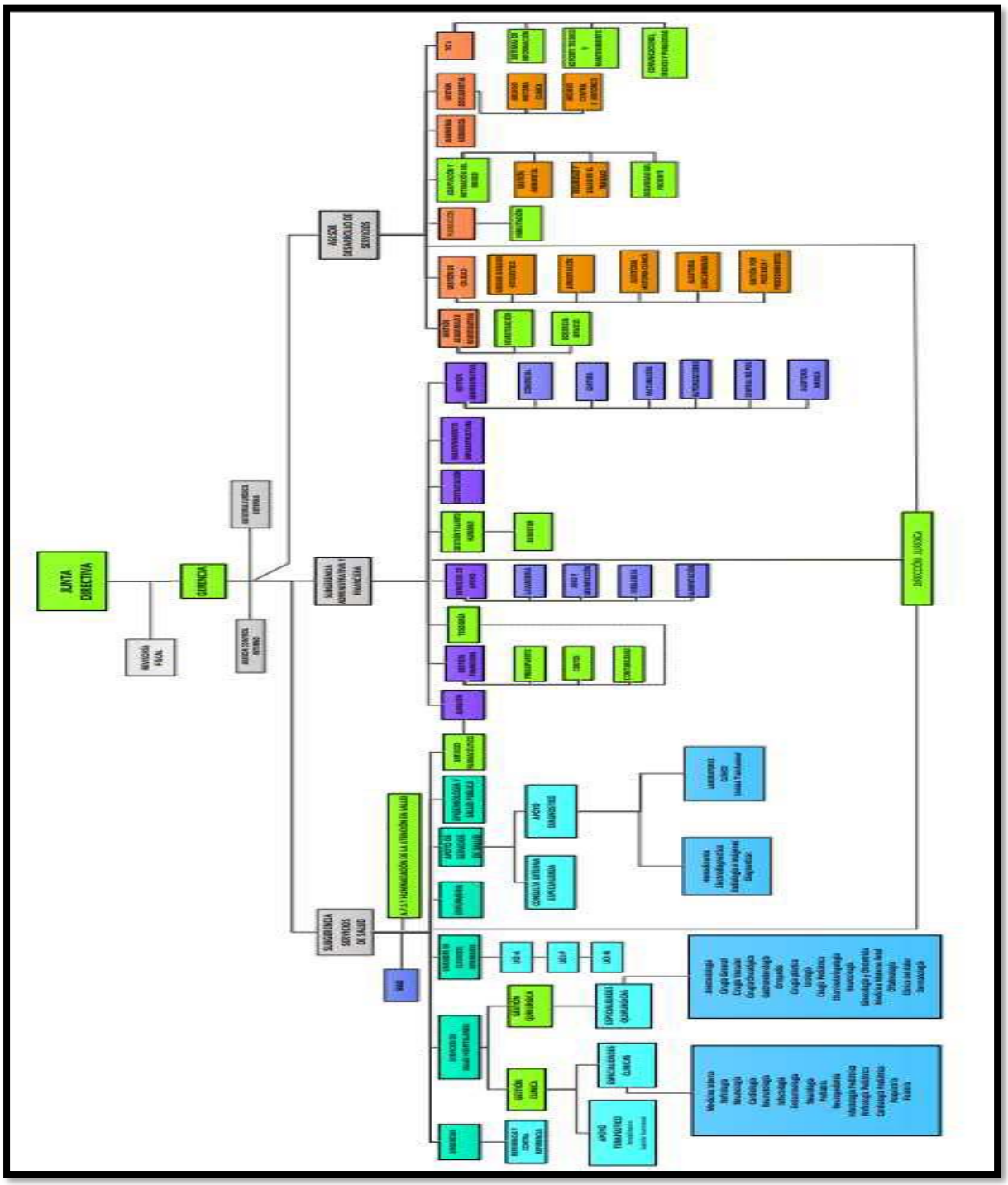
Estructura Orgánica de la E.S.E. HUSRT



7.5. Estructura Orgánica Funcional

Figura 10

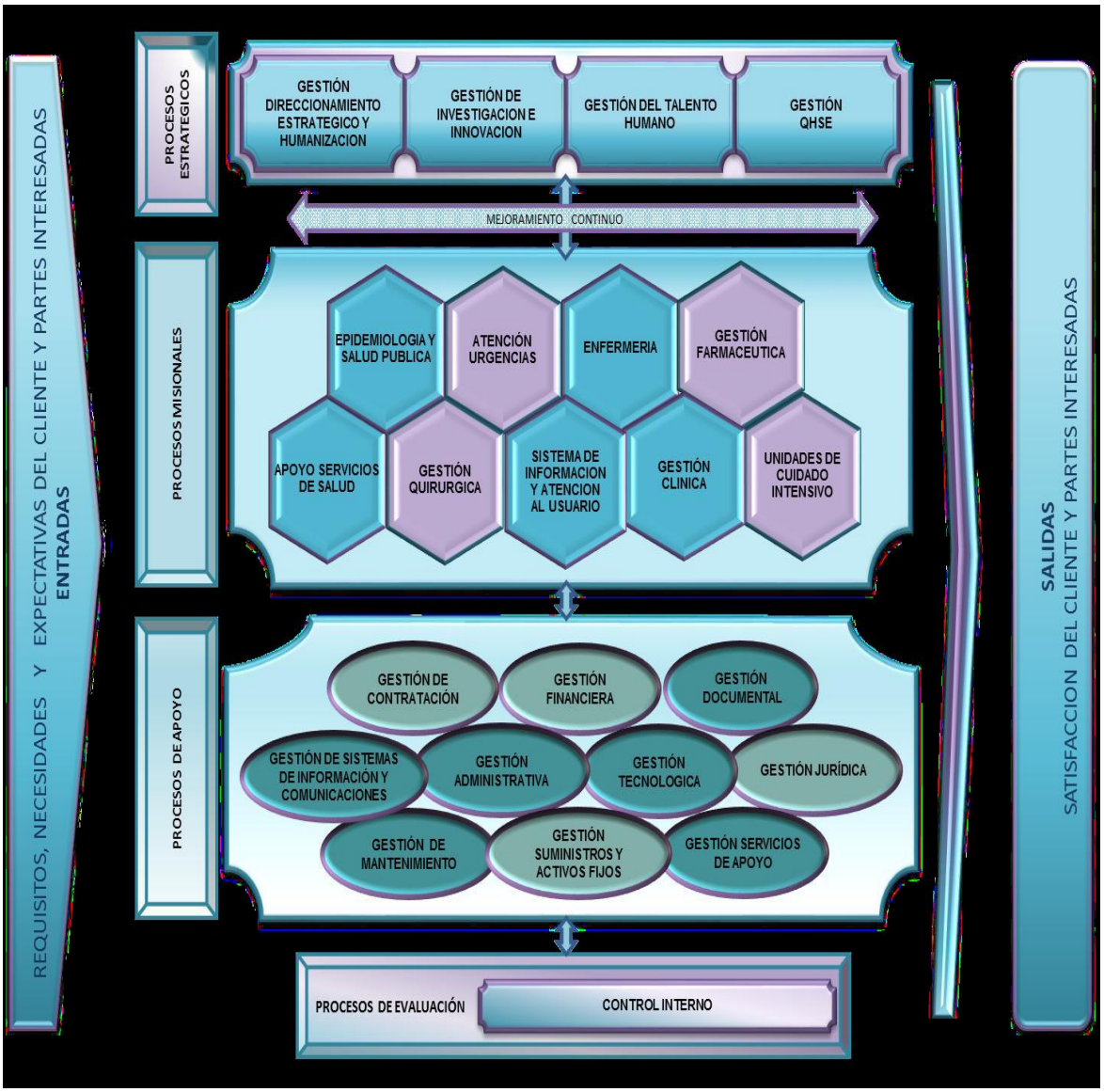
Estructura Orgánica Funcional de la E.S.E. HUSRT.



7.6. Mapa de Procesos

Figura 11

Mapa de Procesos de la E.S.E. HUSRT.



8. Alcance del MSPI de la E.S.E. HUSRT

El MSPI se diseña y aplica a todos los activos de los procesos misionales, estratégicos y de apoyo, acorde con marco legal vigente de seguridad y privacidad de la información, alineados con el plan estratégico, Derecho a la Protección de Datos Personales, Derecho de Acceso a la Información Pública y MIPG en consecución de cumplimiento de los objetivos establecidos para la entidad, el cual tendrá aplicabilidad sobre todos los usuarios de la E.S.E. HUSRT sin importar la modalidad de vinculación con la entidad, se hace extensiva a funcionarios, proveedores, personal en formación y en desarrollo de prácticas académicas, contratistas y demás terceros, sin dejar de lado los factores externos que puedan afectar los procesos o culminación de los objetivos de la entidad.

El diseño y ejecución del MSPI se realizará acorde a los lineamientos que contienen las guías que proporciona el MinTIC y que se describen en el apartado de este archivo del Referente Conceptual del MSPI; pero que se encuentren relacionadas también con el apartado de este documento en donde se especifica el Plan de Análisis, el cual describe las actividades a desarrollar de las fases de Diagnostico, Planificación e Implementación, finalizando con la actividad de la Declaración de Aplicabilidad, ya que para el desarrollo y aprobación de las siguientes fases, la entidad, debe gestionar los recursos físicos, tecnológicos, humanos y económicos.

9. Contexto de la Entidad

9.1. Marco Contextual del Hospital Universitario San Rafael de Tunja

La E.S.E. Hospital Universitario San Rafael de Tunja fue fundado en 1553 en el departamento de Boyacá de la ciudad de Tunja, el cual presta servicios de salud de mediana y alta complejidad, donde el Sistema Obligatorio de Garantía de Calidad enfoca su objetivo en proveer los servicios a usuarios individuales y colectivos de una forma asequible y equitativa.

Los servicios son de nivel III y IV son ofrecidos a la SUBRED 4 Integrada por 26 municipios, centro de referencia de todos los municipios de Boyacá, y de algunos de Santander, Casanare y Cundinamarca.

Se denomina y restructura como "EMPRESA SOCIAL DEL ESTADO HOSPITAL SAN RAFAEL TUNJA", Establecimiento Público del Orden Departamental el 27 de diciembre de 1995 mediante Decreto 001528 de la Gobernación de Boyacá, lo que hace que sea una empresa dotada de personería jurídica, patrimonio propio y autonomía administrativa, adscrita a la Secretaría de Salud de Boyacá e integrante del Sistema General de Seguridad Social en Salud.

Debido a la complejidad de los servicios que presta la HUSRT tiene relación constante con diferentes entes municipales, departamentales, nacionales e internacionales, así como con proveedores, clientes, EPS, IPS, usuarios, empleados y demás terceros, con los cuales debe garantizar la calidad de sus servicios.

Acorde a lo anterior la E.S.E. HUSRT genera, administra, procesa, almacena, custodia y transfiere información muy valiosa lo esto hace que esta sea uno de los activos más importantes ya que contiene información personal, empresarial, investigativa y clasificada, por ende, debe ser protegida, confidencial, integral y debe estar disponible para el personal autorizado.

El Gobierno Nacional a través de la estrategia de Gobierno Digital y con apoyo del Ministerio de las TIC genero lineamientos que deben seguir o cumplir las entidades públicas a través del MSPI (Modelo de Seguridad y Privacidad de la Información) que permite cumplir con la confidencialidad, integridad y disponibilidad, es por todo lo anterior y debido a que el E.S.E. HUSRT es una entidad pública se encuentra en el proceso de diseño, desarrollo e implementación del MSPI. “Informe completo del Contexto del HUSRT”. Clic AQUÍ.

10. Partes Interesadas

10.1. Objetivo

Determinar las partes interesadas, sus necesidades, expectativas y requisitos que son pertinentes al Sistema de Gestión de Seguridad de la Información en la ESE Hospital Universitario San Rafael de Tunja

10.2. Alcance Partes Interesadas

Está implementado para todas las partes interesadas en cumplimiento con los requisitos técnicos y legales de la organización, debe establecer los límites y la aplicabilidad del Sistema de Gestión de Seguridad de la Información para determinar su ámbito de aplicación. Al determinar este ámbito, la organización debe considerar los problemas externos e internos, los requisitos e interfaces y las dependencias entre las actividades llevadas a cabo por la organización.

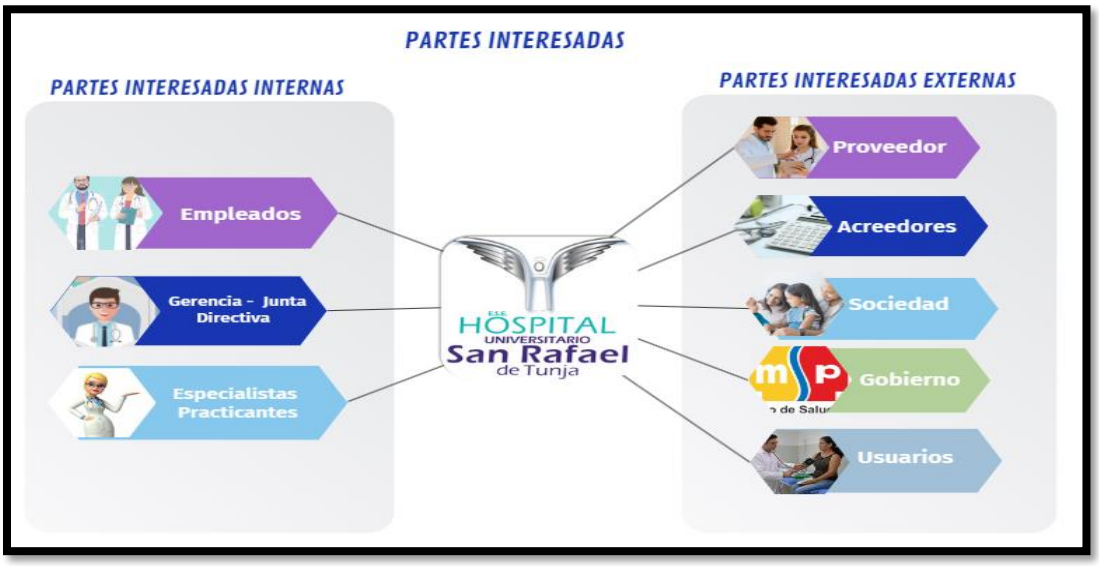
10.3. Partes Interesadas

Mediante este documento, la E.S.E. Hospital Universitario san Rafael de Tunja identifica las partes interesadas, sus necesidades y requisitos, pertinentes al Sistema de Gestión de Seguridad de la Información, tener en cuenta aquellos con los que la empresa tiene una responsabilidad legal, operativa o fiscal, no olvidando aquellas partes interesadas con las que se tienen establecidos contratos, personas y empresas que se encuentren en las zonas donde

la empresa interactúa ya que pueden ser afectadas por la actividad de la empresa y, a su vez influyen en la buena marcha de esta.

Figura 12

Partes Interesadas de la E.S.E. HUSRT.



Partiendo del análisis de contexto interno y externo realizado y teniendo en cuenta lo definido en el numeral 4 de la norma ISO 27001 se establece la prioridad de identificar y definir las necesidades de las partes interesadas con relación a la seguridad de la información y las expectativas creadas por el Sistema de Gestión de Seguridad de la Información, ya que esto determinará las políticas de Seguridad de la Información y los objetivos a seguir para el proceso de gestión de riesgos. De acuerdo con lo anterior se definieron las siguientes partes interesadas para el hospital:

Tabla 3

Partes Interesadas

Parte Interesada	Definición por Grupo de Valor
Usuarios	Niños, niñas, adolescentes, pueblos indígenas, pueblos y comunidades indígenas, ROM y negras, afrocolombianas, raizales y palenqueras (definidos según el artículo 6 de la Ley 1751 de febrero 16 de 2015) y lo definido en el artículo 11. Entendiéndose como usuario a quien hace uso del servicio y/o de los programas del hospital. La clasificación por grupo de valor para esta parte interesada es: Prevalencia de Derechos por ciclos vitales: Prenatal hasta seis (6) años, de los (7) a los catorce (14) años, y de los quince (15) a los dieciocho (18) años. Pueblos y comunidades indígenas, ROM y negras, afrocolombianas, raizales y palenqueras. (niñas, niños y mujeres en estado de embarazo y personas de escasos recursos, grupos vulnerables y sujetos de especial protección). Sujetos de especial protección: La atención de niños, niñas y adolescentes, mujeres en estado de embarazo, desplazados, víctimas de violencia y del conflicto armado, la población adulta mayor, personas que sufren de enfermedades huérfanas y personas en condición de discapacidad.

Parte Interesada	Definición por Grupo de Valor
Gobierno	LEY 489 DE 1.998.- ARTÍCULO 38. INTEGRACIÓN DE LA RAMA EJECUTIVA DEL PODER PÚBLICO EN EL ORDEN NACIONAL y por los Órganos de Control (Procuraduría General de la Nación, Defensoría del Pueblo, Contraloría General de la República, secretaria de Salud).
Empleados	Son colaboradores de la E.S.E Hospital Universitario San Rafael de Tunja quienes estén vinculados a la institución: servidores públicos: Personas naturales vinculadas a la administración pública por una relación legal y reglamentaria para el cumplimiento de funciones administrativas en el marco de una planta de personal aprobada para la entidad – Contratistas: personas naturales que apoyan actividades relacionadas con la administración y funcionamiento del hospital mediante contrato de prestación de servicios – en misión: personas vinculadas – Sindicatos.
Especialistas – Practicantes	Este Grupo de Interés considera a todos aquellos profesionales que desarrollan su labor, tanto a nivel Asistencial como de Gestión y Servicio, en el Hospital, incluyendo a todas las categorías profesionales. Además, en este Grupo de Interés se considera a las instituciones docentes e investigadoras que mantienen una relación con el Hospital, definida mediante convenios de colaboración y conciertos entre instituciones, para llevar a cabo actividades ligadas a su práctica asistencial, investigadora y formadora y

Parte Interesada	Definición por Grupo de Valor
	a sus integrantes: personal docente, investigador, administrativo y de servicios, así como los alumnos que en ellos toman parte.
Proveedores	Toda persona natural, jurídica u organización que tiene una relación contractual con el hospital, para suministrar bienes, obras o servicios, el hospital mediante estos vínculos contractuales cumple con los objetivos y planes institucionales y con sus proyectos de funcionamiento, se establecen los siguientes subgrupos: Comodatos, Sistematización, Mantenimientos, Soportes, y otros proveedores de bienes, obras, servicios (relacionados con el funcionamiento de la Entidad).
Acreedores	Toda persona natural, jurídica u organización que tiene una relación contractual con el hospital, para suministrar bienes, obras o servicios, el hospital, es acreedora de otra si está autorizada legítimamente para exigirle el pago o cumplimiento de una obligación contraída con anterioridad. Es decir, que a pesar de que una de las partes se quede sin medios para cumplir con su obligación, esta persiste.
Sociedad	Este Grupo de Interés considera a toda la Ciudadanía, tanto a los usuarios, pacientes, familiares, acompañantes, cuidadores, etc., que mantienen relación con el Hospital, como a los que están representados por las asociaciones de pacientes y usuarios.

Parte Interesada	Definición por Grupo de Valor
Gerencia – Junta Directiva	Este Grupo de Interés tiene la responsabilidad general sobre toda la compañía, incluyendo la aprobación y la supervisión de la implementación que haga la alta gerencia de los objetivos estratégicos, la estructura de gobierno y la cultura corporativa

10.4. Identificación de Necesidades y Expectativas de las Partes Interesadas

En la E.S.E Hospital Universitario de San Rafael de Tunja se han realizado acciones de implementación de controles con el objeto de proteger la seguridad y privacidad de la información para satisfacer las necesidades y expectativas de las partes interesadas con relación al Sistema de Gestión de la Seguridad de la Información – SGSI, resultados que a continuación se anuncian.

Tabla 4

Grupos de Interés

GRUPOS DE VALOR / GRUPOS DE INTERÉS	NECESIDADES A SATISFACER	EXPECTATIVAS
USUARIOS	Proteger la integridad, confidencialidad, disponibilidad y autenticidad de la información de los usuarios, que se encuentra en custodia de la E.S.E	Garantizar que la información suministrada sea confidencial, integra y esté disponible cuando se requiera, para la

GRUPOS DE VALOR / GRUPOS DE INTERÉS	NECESIDADES A SATISFACER	EXPECTATIVAS
	Hospital Universitario San Rafael de Tunja Realizar campañas de sensibilización sobre el uso de tecnologías.	oportuna prestación de servicios de salud.
GOBIERNO	Sensibilización en temas de delitos informáticos y riesgos de Seguridad Digital. Brindar información sobre la ejecución de los planes, servicios, marco estratégico de TI y Gobierno Digital. Cumplir con los lineamientos y procedimientos en la normativa legal vigente correspondiente a seguridad y privacidad de la información. Generar informes de los incidentes de seguridad y privacidad de la información, seguridad digital	Acompañamiento en el análisis de la infraestructura con el fin de identificar vulnerabilidades en la implementación del MPSI. Fortalecer canales de comunicación con entes externos para que la E.S.E HUSRT se mantenga informada de los diferentes ataques cibernéticos con el propósito de mitigar los riesgos y prevenir incidentes. Aplicar los controles de seguridad digital y seguridad

GRUPOS DE VALOR / GRUPOS DE INTERÉS	NECESIDADES A SATISFACER	EXPECTATIVAS
	presentado en la entidad cuando se considere necesario.	de la Información, establecidos para la mitigación de los riesgos en los procesos. Cumplimiento de la normatividad legal vigente para el aseguramiento de la infraestructura tecnológica y prestación de los servicios de la Entidad.

GRUPOS DE VALOR / GRUPOS DE INTERÉS	NECESIDADES A SATISFACER	EXPECTATIVAS
COLABORADORES	Socializar políticas, procedimientos y documentación del SGSI. Disponer de las herramientas tecnológicas que faciliten la realización de actividades y que la información registrada a través de esta sea resguardada y custodiada bajo los criterios de la seguridad de la información. Fortalecer el acompañamiento frente a la implementación y sostenimiento del MPSI. Fortalecer el Plan de Cultura Uso de TI para brindar un mayor nivel de apropiación en los temas a los colaboradores. Asignación de recursos para el cumplimiento de los requisitos legales	Fortalecer el nivel de apropiación y aplicación de las buenas prácticas digitales establecidas en la política de seguridad de la información vigente, que permitan asegurar la confidencialidad, seguridad y acceso a la información por parte de los colaboradores. Reducir los riesgos por perdida, o uso indebido de la información cumpliendo con la normatividad vigente establecida por la E.S.E HUSRT. Asegurar que la información gestionada sea almacenada de forma segura en los sistemas de información y/o

GRUPOS DE VALOR / GRUPOS DE INTERÉS	NECESIDADES A SATISFACER	EXPECTATIVAS
	asociados a las necesidades del eje de seguridad de la información. Actualizar el parque computacional (hardware) en los procesos de la E.S.E. HUSRT. Asignación de recursos para actividades y/o eventos del eje de seguridad de la Información.	equipos de la E.S.E HUSRT acorde a las políticas establecidas por la entidad.
PROVEEDORES	Realizar acompañamiento y apoyo frente al cumplimiento de las cláusulas establecidas en los contratos en el marco de la prestación de los servicios de la E.S.E HSRT.	Prestación calificada de servicios y cumplimiento eficiente de las obligaciones contractuales de seguridad digital y del SGSI.

11. Diagnostico

A nivel mundial y nacional se ha identificado que las empresas, entidades, industrias, etc. sufren de un problema en común, que es la Seguridad de la Información a través de sus activos en cualquier tipo de formato, por ende, conllevó a que implementaran un Sistema de Gestión de la Seguridad de la Información (SGSI), el Gobierno Nacional a través del Ministerio de Tecnologías de la Información y Comunicaciones (MinTIC), genero el modelo de Seguridad y Privacidad de la Información (MSPI), sustraído del SGSI - ISO 27000 y el cual está compuesto de 5 fases (Diagnostico, Planificación, Implementación, Evaluación y Mejora Continua) en donde su misión es salvaguarda los tres pilares de la seguridad de la información (Confidencialidad, Integridad y Disponibilidad), que es implantado o va dirigido principalmente a las entidades gubernamentales o públicas; pero que también pueden implementar las entidades privadas si lo desean.

Para generar el diseño e implementación del MSPI se debe iniciar con la fase de Diagnostico, en esta fase lo que se recolecta es información de la entidad en donde inicialmente se obtienen los siguientes resultados:

- Determina el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad.
- Determinar el nivel de madurez de los controles de seguridad de la información.
- Identificar el avance de la implementación del ciclo de operación al interior de la entidad.
- Identificar el nivel de cumplimiento con la Normatividades vigente relacionada con protección de datos personales e identificación del uso de buenas prácticas en seguridad de la información.

Al finalizar de diligenciar el diagnostico se identifican también cuales son las posibles vulnerabilidades acorde a los controles técnicos y administrativos evaluados que permiten realizar por último unas recomendaciones y que sirve como insumo para las siguientes fases del MSPI.

11.1. Objetivo del Diagnostico

Determinar el estado actual de Seguridad de la Información del HUSRT a través de la Implementación de la herramienta de Diagnostico GAP propuesta por el MSPI.

11.2. Objetivos Específicos del Diagnostico

- Detallar la efectividad de los controles que se están implementando actualmente en la entidad e identificar la brecha de estos.
- Determinar y concluir el avance del ciclo de funcionamiento del modelo de operación PHVA.
- Determinar el nivel de madurez de seguridad de la información.
- Plantear recomendaciones acordes a la identificación de la brecha y el nivel de madurez de la entidad.

11.3. Alcance del Diagnostico

Actualmente la entidad no cuenta con un área o personal especialista de seguridad de la información; pero las actividades a nivel general que tienen que ver con seguridad de la información son asignadas al área de TIC y 1 funcionario de Calidad, esto no quiere decir que

las otras áreas no tengan que estar o estén involucradas en pro de la seguridad de la información, por ende, los funcionarios o contratistas de estas áreas son los que tienen el conocimiento a nivel general de cómo se encuentra la seguridad de la información. A acorde a lo anterior y para verificar en gran medida el estado actual de la seguridad de información en la entidad se utilizará como herramienta una encuesta a estos funcionarios o contratistas para validar en que porcentaje se ha efectuado el diseño e implementación del MSPI (Modelo de Seguridad y Privacidad de la Información).

Realizada la encuesta y para tener un porcentaje y certeza más amplio en cuanto al estado actual de la seguridad de la información la siguiente actividad que se desarrollara es utilizar la herramienta del GAP y diligenciarla con el apoyo de las dos áreas, allí se validara el diseño e implementación de Seguridad de la Información en todas las áreas y procesos de la Entidad, evaluando los controles administrativos, técnicos y se evidenciara la implementación del ciclo PHVA(Planificar-Hacer-Verificar-Actuar), ciberseguridad y su madurez.

11.4. Herramientas del Diagnostico

Para realizar el Diagnostico en donde los resultados evidencien un porcentaje con un alto grado de confiabilidad y certeza, se seleccionó, implementar dos herramientas. Para este informe se concretó implementar la metodología cualitativa con la implementación de la herramienta de la encuesta, en donde se toma como población el personal de la entidad y se implementa la muestra estratificada a priori ya que el personal que tiene un conocimiento más confiable es el del área de TIC junto con el personal que se relaciona del área de Calidad en las actividades generales de seguridad de la información y segundo utilizar la herramienta GAP suministrada por el MSPI.

11.4.1. Diseño Encuesta de Diagnostico.

La encuesta se le realizo a 6 funcionarios y contratista del área de TIC y 1 funcionario del área de calidad. Los objetivos de esta encuesta son:

- Identificar el nivel de madurez perceptivo de seguridad de la información de la entidad.
- Valorar la Gestión del Conocimiento de los funcionarios y contratistas con respecto a la seguridad de la información en la entidad.
- Calcular el porcentaje perceptivo del diseño e implementación de cada una de las fases de MSPI.

La encuesta está compuesta de 26 preguntas, 6 que son información del encuestado y 20 que van dirigidas a la seguridad de la información de las cuales 18 son las que se evalúan para obtener el nivel de seguridad perceptivo por los funcionarios y contratistas.

Las 18 preguntas que se evalúan tienen las siguientes respuestas y cada una de estas se les asigna el siguiente puntaje para realizar las respectivas mediciones y cumplir con los objetivos.

SI = 10

No =1

No Sabe= 0

Acorde a lo anterior el puntaje máximo por encuestado es de 180 puntos. El puntaje máximo de todos los encuestados es de 1260 puntos. Los niveles de madurez en el MSPI son 5, por lo tanto, la tabla para validar el nivel de madurez en que se encuentra la entidad es la siguiente:

Tabla 5.

Puntaje Nivel de Madures de la Seguridad de la Información.

Puntaje Individual	Puntaje Grupal	Nivel de Madurez
180	1260	Optimizado
144	1008	Administrado
108	756	Definido
72	504	Repetible
36	252	Inicial
0	0	Inexistente

Se formula el siguiente indicador para obtener el nivel de madurez:

NM=Nivel de Madurez

PPN=Puntaje Pregunta Numero

PE=Puntaje Encuestado= Sumatoria (PPN1+PPN2+…)

NM= Sumatoria (PE1+PE2+…)

Para valorar la Gestión del Conocimiento de los funcionarios y contratistas de la entidad con respecto a la seguridad de la información (SI), se toma como base la opción las respuestas que el encuestado selecciono que “NO SABE”, para esta respuesta va tener un puntaje de 1(uno). Se formula el siguiente indicador para obtener la Gestión del Conocimiento (GC) en Seguridad de la Información (SI).

PPN=Puntaje Pregunta Número.

PE= Puntaje Encuestado= Sumatoria (PN1+PN2+…)

PG=Puntaje Grupal = Sumatoria (PE1+PE2+…)

Acorde a lo anterior, cada vez que el encuestado tome como opción de respuesta “NO SABE” obtendrá 1(un) punto, por lo tanto, tendría un puntaje máximo de 18 puntos y grupalmente tendría un puntaje de 126 puntos. A continuación, se relaciona la tabla con la que se identifica cual es el conocimiento que tienen los funcionarios o contratistas con respecto al diseño e implementación de la SI.

Tabla 6.

Valoración de la Gestión del Conocimiento de Seguridad de la Información.

Puntaje Individual	Puntaje grupal	Gestión del Conocimiento (GC) en Seguridad de la Información (SI)
18	126	Baja GC en Seguridad de Información (SI)
12	84	Básica GC en Seguridad de Información (SI)
6	42	Alta GC en Seguridad de Información (SI)
0	0	Superior GC en Seguridad de Información (SI)

Para calcular el porcentaje perceptivo del diseño e implementación de cada una de las fases de MSPI, se define un indicador que calcula el promedio de la siguiente pregunta a todos los encuestados, el puntaje a obtener por la respuesta de cada fase es de 0 a 100.

¿Según todo lo que acaba de responder en que porcentaje se encuentra cada una de las fases del MSPI?

Encuesta Diligenciada. Clic AQUÍ.

11.4.2. Herramienta GAP del MSPI

La herramienta del GAP del MSPI se diligencio con las mismas 7 personas que participaron en la encuesta y en ella se evalúa los controles de seguridad de la

información administrativos y técnicos. Los objetivos de esta herramienta conllevan a que se vea con más claridad cómo se encuentra la seguridad de la información en la entidad, a nivel general estos son:

- Evaluar el diseño e implementación de los controles administrativos y técnicos.
- Identificar la brecha o lo que falta realizar para cambiar el estado en que se encuentra la entidad a un estado ideal.
- Identificar el avance del PHVA con respecto al ideal.
- Definir el nivel de madurez en el que se encuentra la entidad.
- Identificar qué porcentaje cumple del modelo de ciberseguridad NIST con respecto al ideal.

11.5. Diagnóstico del MSPI

Para realizar el diagnostico se utilizaron 2 herramientas, una encuesta y el diligenciamiento de la herramienta GAP del MinTIC. La entidad cuenta con 29 áreas, 2 de las cueles tienen a cargo la Seguridad de la Información a nivel general, están son el área de TIC y calidad. Identificadas las áreas se procedió a realizar una reunión en donde el Área TIC junto con su Coordinador de Sistemas y 5 de sus ingenieros se comprometieron apoyar las actividades para el desarrollo de la encuesta y diligenciamiento de la herramienta GAP, de igual forma el área de Calidad asigno a un ingeniero y también al asesor del MSPI asignado por la Universidad de Manizales.

El propósito de la encuesta es verificar de una forma muy rápida el nivel de madurez, el porcentaje de diseño e implementación de las fases del MSPI y la gestión del conocimiento de los funcionarios o contratistas con respecto a la seguridad de la información.

El diligenciamiento de la herramienta GAP, permite evaluar e identificar los posibles controles administrativos y técnicos de seguridad de la información que se están o no aplicando en la entidad, para verificar y validar con la encuesta el nivel de madurez, de igual forma se identifica la brecha, el avance del ciclo PHVA y el avance en ciberseguridad.

Para concluir se generan unas recomendaciones acordes a los resultados obtenidos que mejoran la seguridad de la información, a continuación, se evidencian los resultados.

11.5.1. Resultados Encuesta Seguridad de la Información (SI).

11.5.1.1. Nivel de madurez perceptivo de la Encuesta de SI.

Para obtener el resultado del nivel de madurez se aplica el indicador NM= Sumatoria (PE1+PE2+…) definido anteriormente, lo primero que realiza es sumar el puntaje obtenido en las 18 preguntas por encuestado y por último se realiza una suma con el puntaje obtenido de todos los encuestados, la siguiente tabla muestra los resultados.

Tabla 7.

Resultado de Nivel de Madurez de Seguridad de la Información.

No Encuestado	NIVEL DE MADURAZ POR ENCUESTADO
Encuestado 1	49
Encuestado 2	62
Encuestado 3	20
Encuestado 4	15
Encuestado 5	106
Encuestado 6	16

Encuestado 7	19
TOTAL, NIVEL DE MADUREZ GRUPAL	287

Acorde a la Tabla 5. “Puntaje Nivel de Madures de la Seguridad de la Información” y la Tabla 7. “Resultado de Nivel de Madurez de Seguridad de la Información”, se evidencia que el puntaje final es de **287**, por lo tanto, la entidad se encuentra en un **Nivel de Madurez Repetible**.

11.5.1.2. Cálculo de la Gestión de Conocimiento de funcionarios y contratistas de la SI en la Entidad.

La Gestión de Conocimiento se calcula por medio del siguiente indicador que se definió con anticipación PG=Puntaje Grupal = Sumatoria (PE1+PE2+…), la información que toma el indicador es la sumatoria de todas las respuestas que los encuestados tomaron como opción “No Sabe”. La siguiente tabla muestra los resultados.

Tabla 8.

Resultado Gestión del Conocimiento de Seguridad de la Información.

No de encuestado	Puntaje GC Individual
Encuestado 1	5
Encuestado 2	1
Encuestado 3	7
Encuestado 4	3
Encuestado 5	2

Encuestado 6	11
Encuestado 7	8
Puntaje GC Grupal	37

Como se observa en la Tabla 8. “Resultado de Gestión del Conocimiento de Seguridad de la Información”, el puntaje obtenido es 37 y comparándolo con la Tabla 2. “Valoración de la Gestión del Conocimiento de Seguridad de la Información”, se define que los funcionarios y contratistas que realizaron la encuesta tienen una **Alta Gestión del Conocimiento GC en Seguridad de Información (SI)**.

11.5.1.3. Porcentaje perceptivo del diseño e implementación de las fases de MSPI.

Para calcular el porcentaje perceptivo cada uno de los encuestados realizo una valoración a cada fase del MSPI y posterior se obtuvo el promedio de los porcentajes de todos los encuestados por fase.

Tabla 9.

Porcentaje Perceptivo Fases del MSPI.

No de Encuestado	Diagnostico	Planeación	Implementación	Evaluación	Mejora continua
Encuestado 1	85	50	25	20	15
Encuestado 2	90	40	45	35	50
Encuestado 3	30	15	10	5	0
Encuestado 4	10	5	0	15	20
Encuestado 5	95	40	20	10	5

Encuestado 6	0	5	10	15	20
Encuestado 7	40	35	30	25	20
Puntaje Encuestados	350	190	140	125	130
Porcentaje Total	50 %	27 %	20 %	18 %	19 %

Observando la Tabla 9. “Porcentaje Perceptivo Fases del MSPI” se obtuvo que la Fase de Diagnostico cumple el 50 %, la fase de Planeación un 27 %, la fase de Implementación un 20 %, la fase de Evaluación un 18 % y la fase de Mejora Continua un 19 %. Encuestas con su análisis. Clic AQUÍ.

11.5.2. Evaluación del Estado Actual

A través de la encuesta se obtuvo un resultado a nivel general de cómo se encuentra la Seguridad de la Información en la entidad; pero para que este resultado sea un porcentaje más completo y sea verificado se diligencia la herramienta GAP, que es más específica y detallada. A continuación, se evidencian los resultados de la herramienta GAP. Herramienta de Diagnostico GAP. Clic AQUÍ.

11.5.2.1. Evaluación de Efectividad de Controles

La herramienta GAP evalúa los controles que se definen en la pestaña administrativas y técnicas con base en el Anexo “A” de la Norma ISO 27001 del 2013, eligiendo 14 dominios que van desde el A.5 al A.18, compuesto por 114 controles, la

calificación de estos controles se basa en la siguiente tabla de Nivel de Madurez del MSPI.

Tabla 10.

Nivel de madurez – MSPI.

Nivel	Porcentaje	Criterios
Inexistente	0%	No se cuenta con la cláusula o control. No se reconoce la información como un activo importante para el logro de la misión y visión de la entidad.
Inicial	1-20%	El control esta implementado no obstante el modelo de seguridad de políticas, procedimientos y estándares de configuración, no existe.
Repetible	21-40%	El control esta implementado y además es soportado por un documento que contiene una política de alto nivel y otras políticas operativas debidamente aprobadas.
Definido - Efectivo	41-60%	El control esta implementado y soportado por políticas, procedimientos y estándares de configuración debidamente publicados y socializados.
Administrado - Gestionado	61-80%	En este nivel se realizan mediciones sobre la efectividad de los controles.
Optimizado	81-100%	En este nivel se encuentran las entidades en las cuales se mide la efectividad de los controles con el fin de mejorarlos y optimizarlos.

Nota: Modelo de seguridad y privacidad de la información (MSPI)

A continuación, se plasma los resultados obtenidos por dominio.

Tabla 11.

Resultados Evaluación de efectividad de Controles - ISO 27001:2013

No.	Evaluación de Efectividad de controles			
	DOMINIO	**Calificación Actual**	**Calificación Objetivo**	**EVALUACIÓN DE EFECTIVIDAD DE CONTROL**
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	30	100	**REPETIBLE**
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	2	100	**INICIAL**
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	41	100	**EFECTIVO**
A.8	GESTIÓN DE ACTIVOS	27	100	**REPETIBLE**
A.9	CONTROL DE ACCESO	52	100	**EFECTIVO**
A.10	CRIPTOGRAFÍA	0	100	**INEXISTENTE**
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	64	100	**GESTIONADO**
A.12	SEGURIDAD DE LAS OPERACIONES	55	100	**EFECTIVO**
A.13	SEGURIDAD DE LAS COMUNICACIONES	58	100	**EFECTIVO**
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	58	100	**EFECTIVO**
A.15	RELACIONES CON LOS PROVEEDORES	30	100	**REPETIBLE**
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	29	100	**REPETIBLE**
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA	24	100	**REPETIBLE**

	GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO			
A.18	CUMPLIMIENTO	54	100	**EFECTIVO**
PROMEDIO EVALUACIÓN DE CONTROLES		**37**	**100**	**REPETIBLE**

Nota: Herramienta-Instrumento de Evaluación MSPI-Portada

Como se puede detallar en la tabla anterior la entidad en la evaluación de efectividad tiene un promedio de 37 % lo que significa que se encuentra en un nivel repetible, según las recomendaciones de Gobierno Digital y MinTIC el promedio para que una entidad logre una gestión de seguridad de la información aceptable el porcentaje en que se debe encontrar es un 70 % o más.

Se debe tener en cuenta que los siguientes dominios se encuentran por debajo del promedio del nivel de madurez identificado y se organizan de menor a mayor porcentaje obtenido, los cuales se deben tratar en una primera etapa:

- Criptografía – 0 %
- Organización de la seguridad de la información – 2%
- Gestión de la continuidad del negocio – 24 %
- Gestión de activos – 27 %
- Gestión de incidentes de seguridad de la información – 29 %
- Políticas de seguridad de la información – 30 %
- Relaciones con los proveedores – 30 %

En la segunda etapa se deben tratar los controles que se encuentre en un estado Repetible para avanzar al nivel Efectivo. Se debe tener en cuenta que para subir

de niveles las entidades deben contar con los recursos y debe aprobar que estos sean asignados para poder efectuarlos y ejecutarlos.

En la tercera etapa, tratar los controles que se encuentren en el nivel efectivo para escalar a un nivel Gestionado, otro aspecto que se debe tener en cuenta es que la entidad puede contar con algunos recursos que se pueden implementar en cualquiera de los niveles (ej. personal especializado), para que no dependa de la aprobación de estos mismos por parte de la dirección. Al culminar esta etapa la entidad cumpliría con el 70 %, por lo tanto, tendría una seguridad de la información aceptable y estaría cumpliendo con las directrices de gobierno digital.

En la cuarta y última etapa se tratan los controles que se encuentren en el nivel efectivo para subirlos al nivel optimizado. Se debe tener en cuenta que con el transcurso del tiempo se generan nuevos activos, amenazas, vulnerabilidades, riesgos y controles, lo que hace que siempre exista un mejoramiento continuo.

11.5.2.2. Brecha Anexo A ISO 27001:2013

La brecha que proyecta la herramienta GAP resume cada uno de los dominios en donde se identifica el porcentaje en el que se encuentran actualmente y se refleja la diferencia que falta para obtener el estado ideal. En la siguiente ilustración se detallan los resultados.

Figura 13

Brecha Anexo a ISO 27001:2013

Nota: Instrumento de Evaluación MSPI de la E.S.E HUSRT – Portada.

En la figura se especifica que ninguno de los controles sobrepasa el 64 % por lo que se concreta que ninguno cumple con un estado aceptable, lo que concluye que la entidad se encuentra en un estado de riesgo en seguridad de la información.

11.5.2.3. Avance Del Ciclo PHVA (Planear-Hacer-Verificar-Actuar)

En el diagnostico también se evalúa los componentes del avance de la metodología PHVA que también es una directriz de Gobierno Digital. En la siguiente tabla se plasman los resultados o avance obtenido.

Tabla 12.

Avance del Ciclo PHVA

Año	AVANCE PHVA		
	COMPONENTE	**% de Avance Actual Entidad**	**% Avance Esperado**
2022	Planificación	14%	40%
2022	Implementación	2%	20%
2022	Evaluación de desempeño	5%	20%
2022	Mejora continua	4%	20%
TOTAL		**25%**	**100%**

Nota: Instrumento de Evaluación MSPI de la E.S.E HUSRT – Portada.

Acorde a los resultados de la tabla anterior se evidencia que se está cumpliendo un 25% del avance del PHVA; pero el porcentaje más alto se encuentra en el componente de Planificación que es un 14% y que tiene como un estado ideal un 40%. El componente Implementación cuenta con un 2 % de un avance esperado del 20%, el componente de Evaluación de Desempeño tiene un 5% de un “20% por obtener y componente de Mejora Continua tiene un 4% de un 20% por lograr. Se concluye que el avance del PHVA se encuentra en un porcentaje muy bajo y por ende se debe realizar una planificación para avanzar y conseguir el avance esperado.

11.5.2.4. Nivel De Madurez

El nivel de madurez se obtuvo del diligenciamiento de la herramienta GAP, en donde se evalúan los controles administrativos y técnicos, que identifican lo que se cumple de cada control y que le falta a cada uno. Acorde a lo anterior se verifico que el

nivel de madurez en el que se encuentra la entidad es “Repetible”, por lo tanto, la entidad debe crear estrategias, planes y controles para que escale al nivel “Administrado”, que es el nivel en el que la entidad estaría tolerable con la seguridad de la información. En el nivel repetible, los procesos son básicos en cuanto a gestión de la seguridad y privacidad de la información, se tienen controles que permiten detectar posibles incidentes de seguridad; pero que no tienen definida una gestión de riesgos y controles acorde con unas métricas e indicadores que permitan evaluarlos y realizar una mejora continua.

Verificando el GAP se obtuvo una calificación de 300 puntos, acorde a la siguiente tabla se deduce el nivel en el que se encuentra la entidad.

Tabla 13.

Nivel de Madurez. HUSRT

NIVEL	ID. REQUISITO	PUNTAJE OBTENIDO	PUNTAJE ESPERADO
OPTIMIZADO	R55		1100
ADMINISTRADO	R41 a R53		880
DEFINIDO	R20 a R40		660
REPETIBLE	R9 a R19	300	460
INICIAL	R1 a R8		260

Nota: Instrumento de Evaluación MSPI de la E.S.E HUSRT – Portada.

11.5.2.5. Resultados Avance Ciberseguridad NIST

Los resultados en las funciones de ciberseguridad reflejan que no obtuvieron un avance del más del 50 %, por lo tanto, se concluye que no alcanzaron el nivel ideal y

por ende se debe planear que controles se deben ejecutar para conseguir un mejor nivel. A continuación, se detallan los resultados.

Tabla 14.

Avance del Modelo Ciberseguridad NIST

MODELO FRAMEWORK CIBERSEGURIDAD NIST		
Etiquetas de fila	**CALIFICACIÓN ENTIDAD**	**NIVEL IDEAL CSF**
IDENTIFICAR	48	100
DETECTAR	41	100
RESPONDER	47	100
RECUPERAR	20	100
PROTEGER	47	100

Nota: Instrumento de Evaluación MSPI de la E.S.E HUSRT – Portada.

11.5.3. Recomendaciones Generadas GAP

A continuación, se plasman los dominios con sus brechas y recomendaciones.

Tabla 15.

Políticas de Seguridad de la Información

ITEM	ISO	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	A.5		30	
Documento de la política de seguridad y privacidad de la Información	A.5.1.1	B. Alinear con plan de desarrollo institucional. C. se debe actualizar la Política acorde a los lineamientos, se realiza acto administrativo y socializar mediante correo, integrar con la vinculación de personal de inducción y reinducción. Definir periodicidad de revisión y actualización de políticas.	40	Realizar desde el inicio la definición de la política y sus dominios, definiendo la periodicidad de revisión y actualización junto con el rol encargado.
Revisión y evaluación	A.5.1.2	Actualizar la política, con roles y responsabilidades.2	20	Revisar la política de seguridad de la información, según ocurra un incidente de seguridad, cambios normativos, cambios sugeridos en reuniones del grupo de seguridad

Tabla 16.

Organización de la Seguridad de la Información

ITEM	ISO	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	**A.6**		**2**	
Organización Interna	**A.6.1**		**4**	
Roles y responsabilidades para la seguridad de la información	A.6.1.1	Los roles y responsabilidades no estan claramente definidos, no se cuenta con un cronograma en donde en las reuniones de la dirección se toquen temas puntuales de la seguridad de la información y tampoco tienen definido un presupuesto para actividades de seguridad de la información.	0	Roles definidos en la resolución 221 de 2018, definir claramente las responsabilidades, una vez se defina el equipos de seguridad. Generar cronograma de las reuniones con las directivas para tratar temas de SI.
Separación de deberes / tareas	A.6.1.2	Definir en el PETI roles y responsabilidades de usuarios en los sistemas de información	20	Definir en el PETI roles y responsabilidades de usuarios en los sistemas de información
Contacto con las autoridades.	A.6.1.3	Elaborar procedimiento para escalar a la autoridad competente (jurídica o talento humano) incidentes o eventos relacionados con violaciones de ley de seguridad de la información	0	Elaborar procedimientos para reportes de incidentes ante las autoridades legales junto con las posibles sanciones.
Contacto con grupos de interés especiales	A.6.1.4	informar a los roles de seguridad que participe e informe en que foros o grupos en seguridad se encuentra inscrito.	0	Los roles inscribirse en capacitaciones y foros de SI
Seguridad de la información en la gestión de proyectos	A.6.1.5	No se encuentra un procedimiento para la integración de los proyectos con la SI y el área desarrollo y servicios encargadas Integrar la seguridad de la información como parte integral de cualquier proyecto que realice la institución	0	Definir los procedimiento para la integración de los proyectos con la SI.

ITEM	ISO	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
Dispositivos Móviles y Teletrabajo	**A.6.2**		**0**	
Política para dispositivos móviles	A.6.2.1	Crear política, procesos, procedimientos para dispositivos móviles	0	Actualizar la política, procesos, procedimientos, manuales, guías para dispositivos móviles
Teletrabajo	A.6.2.2	Definir política, crear manuales, procedimientos.	0	Actualizar la política, procesos, procedimientos, manuales, guías para el teletrabajo.

Tabla 17.

Seguridad de los Recursos Humanos

ITEM	ISO	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
SEGURIDAD DE LOS RECURSOS HUMANOS	**A.7**		**41**	
Antes de asumir el empleo	**A.7.1**		**70**	
Selección e investigación de antecedentes	A.7.1.1		100	
Términos y condiciones del empleo	A.7.1.2		40	verificar cumplimiento en los empleados de planta y de trabajo asociado. Pendiente documento de confidencialidad para otros vinculados como los médicos internos, auditores y docentes externos. Verificar acuerdo en los contratistas
Durante la ejecución del empleo	**A.7.1.2**		**13**	
Responsabilidades de la dirección	A.7.2.1	Es muy mínima la alineación de los contratistas con los roles y responsabilidades de SI. Es muy baja la toma de conciencia en SI para los contratistas porque no tienen las habilidades y no se reciben capacitación, mucho menos cuentan con un canal de reportes anónimos.	20	Crear procedimientos, contratos, manuales, capacitaciones, guías que alineen los contratistas con los roles y responsabilidades de SI. Crear un canal de reportes anónimos.
Toma de conciencia, educación y formación en la seguridad de la información	A.7.2.2	No se evidencia campañas, folletos ni boletines en el plan de comunicaciones. No se evidencia la sensibilización a los nuevos contratistas y empleados. No se evidencia cada cuanto se actualizan los programas de sensibilización.	20	Elaborar campañas, folletos, boletines en el plan de comunicaciones. Crear procedimientos y cronograma para la sensibilización a los nuevos contratistas y empleados.
Proceso disciplinario	A.7.2.3		0	Crear el proceso disciplinario que determine la sanción cuando se viola la seguridad de la información.

ITEM	ISO	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
SEGURIDAD DE LOS RECURSOS HUMANOS	**A.7**		**41**	
Terminación y cambio de empleo	**A.7.3**		**40**	
Terminación o cambio de responsabilidades de empleo	A.7.3.1	Solo existe acuerdo de confidencialidad para los empleados.	40	Crear acuerdo de confidencialidad para contratista, proveedores, terceros. Definir clausulas de SI para contratistas. Procedimientos para finalización y cambio de empleo en donde se refleje la SI.

Tabla 18.

Gestión de Activos

ITEM	ISO	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
GESTIÓN DE ACTIVOS	**A.8**		**27**	
Responsabilidad de los activos	**A.8.1**		**35**	
Inventario de activos	A.8.1.1	No esta actualizas los activos y la información es incoherente. La ultima vez que se recolectaron los activos fue en el 2018, No cumple con todos los criterios del MSPI.	20	Recolectar nuevamente los activos con un formato que contenga todos los lineamientos acorde al MSPI
Propiedad de los activos	A.8.1.2	No se cuenta con un procedimiento completo y claro para asegurar la propiedad de cualquier tipo de activo.	40	Actualizar formato conforme a Guía 5 para la Gestión y Clasificación de Activos de Información. Actualizar registro de activos incluyendo activos como los sistemas de información o bases de datos a proteger bajo un responsable.
Uso aceptable de los activos	A.8.1.3	No se evidencia el conocimiento del uso aceptable de los activos por parte de todos los empleados y usuarios.	40	Crear estrategia para sensibilizar a los empleados del uso aceptable de los activos.
Devolución de activos	A.8.1.4	No se evidencia un procedimiento adecuado o cumplimiento de este cuando se termina o finaliza un contrato con todos los activos que involucren SI.	40	Crear procedimiento para la adecuada finalización o entrega de un contrato validando los posibles cambios y entrega de información.

ITEM	ISO	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
GESTIÓN DE ACTIVOS	**A.8**		**27**	
Clasificación de información	**A.8.2**		**20**	
Clasificación de la información	A.8.2.1		20	Actualizar formato conforme a Guía 5 para la Gestión y Clasificación de Activos de Información. Realizar proceso de actualización de identificación y clasificación de activos de información.
Etiquetado de la información	A.8.2.2	No se encuentran identificados todos los activos.	20	realizar procedimiento
Manejo de activos	A.8.2.3		20	Adjuntar otros procedimientos conforme el criterio en el manejo, procesamiento, almacenamiento y comunicación de información de conformidad con su clasificación.
Manejo de medios	**A.8.3**		**27**	
Gestión de medios removibles	A.8.3.1		0	Definir procedimientos de respaldo de Información de equipos de funcionarios y uso de medios removibles
Disposición de los medios	A.8.3.2	En Comité de Sostenibilidad se Aprueba la baja del Equipo de Computo, falta documentar procedimiento de medios a desechar o donar.	40	Crear procedimiento para desechar o donar activos o medios de información.
Transferencia de medios físicos	A.8.3.3	Se verifica que se gestiona y administra la mensajería electrónicamente por Orfeo; pero no se evidencian los procedimientos ni directrices en medios físicos.	40	Documentar Directrices y procedimientos definidos para la protección de medios que contienen información durante el transporte.

Tabla 19.

Control de Acceso

ITEM	ISO	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
CONTROL DE ACCESO	**A.9**		**52**	
REQUISITOS DEL NEGOCIO PARA CONTROL DE ACCESO	**A.9.1**		**50**	
Política de control de acceso	A.9.1.1	No se evidencia en la política la revisión periódica de los derechos de acceso, el retiro de los derechos de acceso, el ingreso de los registros de todos los eventos significativos concernientes al uso y gestión de los usuarios y los roles de acceso privilegiado.	60	Actualizar Manual de políticas
Acceso a redes y a servicios en red	A.9.1.2	En la política no se evidencia los procedimientos de autorización para determinar a quién se permite el acceso a qué redes y servicios de red, tampoco se evidencia los requisitos de autenticación de usuarios para acceder a diversos servicios de red; y el seguimiento del uso de servicios de red.	40	Actualizar Manual de políticas
GESTIÓN DE ACCESO DE USUARIOS	**A.9.2**		**47**	
Registro y cancelación del registro de usuarios	A.9.2.1	Se cumple con el proceso pero no se encuentra bien documentado.	60	Documentar el proceso y realizar los formatos y manuales pertinentes para el desarrollo de este.
Suministro de acceso de usuarios	A.9.2.2	Se cumple con el proceso pero no se encuentra bien documentado.	60	Documentar el proceso y realizar los formatos y manuales pertinentes para el desarrollo de este.
Gestión de derechos de acceso privilegiado	A.9.2.3	Se cumple con el proceso pero no se encuentra bien documentado.	60	Documentar el proceso y realizar los formatos y manuales pertinentes para el desarrollo de este.
Gestión de información de autenticación secreta de usuarios	A.9.2.4		0	Elaborar procedimiento para autenticación secreta de usuarios
Revisión de los derechos de acceso de usuarios	A.9.2.5		40	Documentar el proceso y realizar los formatos y manuales pertinentes para el desarrollo de este.
Retiro o ajuste de los derechos de acceso	A.9.2.6		60	Documentar el proceso y realizar los formatos y manuales pertinentes para el desarrollo de este.

ITEM	ISO	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
CONTROL DE ACCESO	**A.9**		**52**	
RESPONSABILIDADES DE LOS USUARIOS	**A.9.3**		**60**	
Uso de información de autenticación secreta	A.9.3.1		60	Fortalecer el proceso de autenticación secreta (Divulgar estándares de seguridad en las contraseñas)
CONTROL DE ACCESO A SISTEMAS Y APLICACIONES	**A.9.4**		**52**	
Restricción de acceso a la información	A.9.4.1		100	
Procedimiento de ingreso seguro	A.9.4.2		20	Crear documento con los procedimientos para realizar pruebas de vulnerabilidad y documentar las fallas de Seguridad
Sistema de gestión de contraseñas	A.9.4.3		60	Realizar pruebas de la complejidad de las contraseñas y si estas pueden ser vulnerables acordes a cada sistema de información con el que cuenta la entidad.
Uso de programas utilitarios privilegiados	A.9.4.4		40	Documentar proceso (Capitulo en Manual S-M-02)
Control de acceso a códigos fuente de programas	A.9.4.5		40	Documentar proceso

Tabla 20.

Criptografía

ITEM	ISO	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
CRIPTOGRAFÍA	**A.10**		**0**	
CONTROLES CRIPTOGRÁFICOS	**A.10.1**		**0**	
Política sobre el uso de controles criptográficos	A.10.1.1		0	Incluir en manual de políticas lo referente a criptografía
Gestión de llaves	A.10.1.2		0	Incluir en manual de políticas lo referente a llaves criptografía

Tabla 21.

Seguridad Física y del Entorno

ITEM	ISO	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
SEGURIDAD FÍSICA Y DEL ENTORNO	**A.11**		64	
ÁREAS SEGURAS	**A.11.1**		70	
Perímetro de seguridad física	A.11.1.1		60	Revisar los controles de acceso a las Áreas Seguras, para verificar los perímetros de seguridad.
Controles físicos de entrada	A.11.1.2		60	Revisar los controles de acceso a las Áreas Seguras. Restringir el ingreso de personal particular y no autorizado a las áreas mas susceptibles de la entidad como son el área financiera, el centro de computo, etc., a través de controles o generando nuevas estrategias.
Seguridad de oficinas, recintos e instalaciones	A.11.1.3		80	Fortalecer controles de acceso a las áreas seguras
Protección contra amenazas externas y ambientales	A.11.1.4	No se cuenta con una eficiente y eficaz protección física contra desastres naturales, ataques maliciosos o accidentes.	60	Implementar los controles de respaldo en lugares externos a la institución
Trabajo en áreas seguras	A.11.1.5		60	Documentar lineamientos de acceso a áreas seguras
Áreas de despacho y carga	A.11.1.6		100	

ITEM	ISO	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
SEGURIDAD FÍSICA Y DEL ENTORNO	A.11		64	
EQUIPOS	A.11.2		58	
Ubicación y protección de los equipos	A.11.2.1	No se evidencia pruebas de vulnerabilidad para la protección de los equipos.	60	Definir procedimientos para probar los controles que se tienen para la ubicación y protección de los equipos y activos físicos.
Servicios de suministro	A.11.2.2	No se evidencia pruebas a los controles de fallas de energía y otras interrupciones.	60	Definir procedimientos para probar los controles que se tienen para las fallas de energía y otras interrupciones de los servicios de suministro(internet)
Seguridad del cableado	A.11.2.3	No se cuenta con los procedimientos para la seguridad del cableado	40	Crear documento con los procedimientos, diseños para la seguridad del cableado y cumplir o ejecutar sus directrices.
Mantenimiento de equipos	A.11.2.4		100	
Retiro de activos	A.11.2.5		80	Realizar pruebas a los controles de retiro de equipos para validar si se encuentran vulnerabilidades.
Seguridad de equipos y activos fuera de las instalaciones	A.11.2.6	No se evidencia una política especifica para los activos de información externos y un procedimiento.	40	Actualizar Manual de políticas y crear los procedimientos para los activos externos.
Disposición segura o reutilización de equipos	A.11.2.7		0	Documentar proceso de borrado de Discos y la encriptación de la información que contienen.
Equipos de usuario desatendidos	A.11.2.8		100	
Política de escritorio limpio y pantalla limpia	A.11.2.9		40	Documentar y publicar directrices para escritorio limpio

Tabla 22.

Seguridad de las Operaciones

ITEM	ISO	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
SEGURIDAD DE LAS OPERACIONES	**A.12**		55	
PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES	**A.12.1**		**50**	
Procedimientos de operación documentados	A.12.1.1	No se evidencia la gestión de la información del log del sistema.	80	Crear procedimientos y controles en donde se evidencia la gestión de la información del log del sistema;
Gestión de cambios	A.12.1.2		40	Definir procedimientos para controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
Gestión de capacidad	A.12.1.3		0	Implementar Seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura a través de procedimientos.
Separación de los ambientes de desarrollo, pruebas y operación	A.12.1.4		80	

ITEM	ISO	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
SEGURIDAD DE LAS OPERACIONES	**A.12**		55	
PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS	**A.12.2**		80	
Controles contra códigos maliciosos	A.12.2.1	No se evidencian pruebas para los controles de códigos maliciosos; pero si cuentan con los controles.	80	Realizar pruebas a los controles de códigos maliciosos.
COPIAS DE RESPALDO	**A.12.3**		0	
Respaldo de la información	A.12.3.1		0	Crear procedimientos y realizar pruebas a las copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.
REGISTRO Y SEGUIMIENTO	**A.12.4**		55	
Registro de eventos	A.12.4.1		60	Crear procedimientos y pruebas para los siguientes eventos que falten: a) identificar los usuarios; b) establecer las actividades del sistema; c) definir las fechas, horas y detalles de los eventos clave, (entrada y salida); d) identificar el dispositivo o ubicación, si es posible, e identificador del sistema; e) tener registros de intentos de acceso al sistema exitosos y rechazados; e) definir registros de datos exitosos y rechazados y otros intentos de acceso a recursos; g) establecer los cambios a la configuración del sistema; h) definir el uso de privilegios; i) establecer el uso de utilitarios y aplicaciones del sistema; j) definir los archivos a los que se tuvo acceso, y el tipo de acceso; k) establecer las direcciones y protocolos de red; l) definir las alarmas accionadas por el sistema de control de acceso; m) activar y desactivar los sistemas de protección, tales como sistemas antivirus y sistemas de detección de intrusión; n) registrar las transacciones ejecutadas por los usuarios en las aplicaciones.
Protección de la información de registro	A.12.4.2		0	Definir los procedimientos de como se protege contra registro y protección, alteración y acceso no autorizado
Registros del administrador y del operador	A.12.4.3		60	Realizar Backup a los registros.
Sincronización de relojes	A.12.4.4		100	

ITEM	ISO	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
SEGURIDAD DE LAS OPERACIONES	**A.12**		55	
CONTROL DE SOFTWARE OPERACIONAL	**A.12.5**		60	
Instalación de software en sistemas operativos	A.12.5.1		60	
GESTIÓN DE LA VULNERABILIDAD TÉCNICA	**A.12.6**		80	
Gestión de las vulnerabilidades técnicas	A.12.6.1		60	Documentar directrices para vulnerabilidades técnicas
Restricciones sobre la instalación de software	A.12.6.2		100	
CONSIDERACIONES SOBRE AUDITORÍAS DE SISTEMAS DE INFORMACIÓN	**A.12.7**		60	
Controles sobre auditorías de sistemas de información	A.12.7.1		60	Documentar procesos de auditorias enfocados en la seguridad de la información.

Tabla 23.

Seguridad de las Comunicaciones

ITEM	ISO	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
SEGURIDAD DE LAS COMUNICACIONES	**A.13**		58	
GESTIÓN DE LA SEGURIDAD DE LAS REDES	**A.13.1**		60	
Controles de redes	A.13.1.1		60	Documentar directrices para la gestión de seguridad de redes
Seguridad de los servicios de red	A.13.1.2		60	Documentar directrices para la seguridad de los servicios de red
Separación en las redes	A.13.1.3		60	Documentar integridad de las redes incorporando segregación donde se requiera
TRANSFERENCIA DE INFORMACIÓN	**A.13.2**		55	
Políticas y procedimientos de transferencia de información	A.13.2.1		60	Documentar y mapear los flujos de comunicaciones y datos
Acuerdos sobre transferencia de información	A.13.2.2		0	Validar en todas las áreas con que entidades externas(Proveedores, clientes etc.) se realiza transferencia de información y de acuerdo a esto generar procedimientos y acuerdos bajo las directrices para la transferencia de información.
Mensajería electrónica	A.13.2.3		60	Crear o validar procedimientos acorde a las directrices para mensajería electrónica
Acuerdos de confidencialidad o de no divulgación	A.13.2.4		100	

Tabla 24.

Adquisición, Desarrollo y Mantenimiento de Sistemas

ITEM	ISO	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	**A.14**		58	
REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN	**A.14.1**		**40**	
Análisis y especificación de requisitos de seguridad de la información	A.14.1.1		80	Revisar los procedimientos y controles establecidos para la adquisición de nuevos sistemas de información.
Seguridad de servicios de las aplicaciones en redes públicas	A.14.1.2		0	Realizar procedimientos en donde se evidencie las pruebas a los controles de los sistemas de información adquiridos por proveedores en las redes publicas y acorde a cronogramas.
Protección de transacciones de los servicios de las aplicaciones	A.14.1.3		0	Revisar los procedimientos para la protección de las transacciones de los de los servicios de las aplicaciones y realizar pruebas a los controles, acorde a las directrices.

ITEM	ISO	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	**A.14**		58	
SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y DE SOPORTE	**A.14.2**		53	
Política de desarrollo seguro	A.14.2.1		80	Realizar procedimientos para verificar que los proveedores de los sistemas de información implementen las directrices para el desarrollo de software.
Procedimientos de control de cambios en sistemas	A.14.2.2		60	Documentar directrices procedimientos control de cambio en sistemas
Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	A.14.2.3		60	Documentar directrices revisión técnica de las aplicaciones después de cambios en la plataforma de operación
Restricciones en los cambios a los paquetes de software	A.14.2.4		60	Documentar directrices restricciones en los cambios a los paquetes de software
Principios de construcción de sistemas seguros	A.14.2.5		0	Documentar principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información
Ambiente de desarrollo seguro	A.14.2.6		0	Documentar directrices para ambiente de desarrollo seguro
Desarrollo contratado externamente	A.14.2.7		60	Documentar directrices desarrollo contratado externamente
Pruebas de seguridad de sistemas	A.14.2.8		80	
Prueba de aceptación de sistemas	A.14.2.9		80	

ITEM	ISO	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	**A.14**		58	
DATOS DE PRUEBA	**A.14.3**		**80**	
Protección de datos de prueba	A.14.3.1		80	

Tabla 25.

Relaciones con los Proveedores

ITEM	ISO	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
RELACIONES CON LOS PROVEEDORES	**A.15**		**30**	
Seguridad de la información en las relaciones con los proveedores	A.15.1	No se evidencia procedimientos para las relaciones con los nuevos proveedores en donde se alienan a la SI.	60	Establecer acuerdos de normas de seguridad con proveedores
Gestión de la prestación de servicios de proveedores	A.15.2	No se evidencia como se realiza el seguimiento con los proveedores acorde a las políticas de seguridad de la información. No se evidencia como se gestionan los cambios en el suministro de servicios por parte de los proveedores relacionada con la política de SI.	0	Establecer acuerdos de normas de seguridad con proveedores para poder realizar medición del criterio

Tabla 26.

Gestión de Incidentes de Seguridad de la Información

ITEM	ISO	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	A.16		29	
GESTIÓN DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN	A.16.1		29	
Responsabilidades y procedimientos	A.16.1.1		40	Documentar responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.
Reporte de eventos de seguridad de la información	A.16.1.2		40	Documentar eventos de seguridad de la información
Reporte de debilidades de seguridad de la información	A.16.1.3		40	Documentar Reporte de debilidades de seguridad de la información
Evaluación de eventos de seguridad de la información y decisiones sobre ellos	A.16.1.4		0	Documentar eventos de seguridad de la información y decisiones sobre ellos
Respuesta a incidentes de seguridad de la información	A.16.1.5		40	Documentar los planes de respuesta a incidentes
Aprendizaje obtenido de los incidentes de seguridad de la información	A.16.1.6		20	Documentar el impacto de los incidentes de acuerdo al modelo de madurez
Recolección de evidencia	A.16.1.7		20	Documentar las directrices de cadena de custodia

Tabla 27.

Aspectos de Seguridad de la Información de la Gestión de la Continuidad del Negocio

ITEM	ISO	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	**A.17**		**23,5**	
Continuidad de la seguridad de la información	**A.17.1**		**27**	
Planificación de la continuidad de la seguridad de la información	A.17.1.1	Dado que la recolección de activos no contiene la información coherente y acorde al MSPI no se tiene definido en el plan de continuidad todos los aspectos.	40	Generar un nuevo documento en donde se evidencia el plan de continuidad acorde a los activos actuales y con las directrices del MSPI.
Implementación de la continuidad de la seguridad de la información	A.17.1.2	No se cuenta con todo el personal idóneo para responder a una contingencia de eventos de gran impacto y no se cuenta con procedimientos ni evidencia en donde se realicen pruebas a los controles para eventos de gran magnitud.	20	Falta procedimientos de respuesta y recuperación documentados. Contratar personal idóneo que mitigue, evite y controle los ataques de SI.
Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	A.17.1.3	No se evidencia la verificación, revisión y evaluación de la continuidad de la seguridad de la información.	20	Documentar procesos, procedimientos y controles de continuidad de la seguridad de la información, para asegurar que son coherentes con los objetivos de continuidad de la seguridad de la información.
Redundancias	**A.17.2**		**20**	
Disponibilidad de instalaciones de procesamiento de información	A.17.2.1	Tiene componentes redundantes en el mismo centro de computo. No se evidencia pruebas redundantes.	20	No se cuenta con centro de computo alterno. Realizar pruebas redundantes.

Tabla 28.

Cumplimiento

ITEM	ISO	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
CUMPLIMIENTO	**A.18**		54	
Cumplimiento de requisitos legales y contractuales	**A.18.1**		75	
Identificación de la legislación aplicable y de los requisitos contractuales.	A.18.1.1	No se encuentran las ultimas normas, leyes, etc. de la SI.	60	Actualizar Normograma acorde a las ultimas leyes, normas, etc. nacionales e internacionales de SI.
Derechos de propiedad intelectual.	A.18.1.2		100	
Protección de registros.	A.18.1.3	Se evidencia que hay documentos de apoyo que pueden ser definidos en las TRD	80	Validar y verificar que documentos pueden agregarse a las TRD e ingresarlos.
Protección de los datos y privacidad de la información relacionada con los datos personales.	A.18.1.4		60	Actualizar el documento y procedimientos de privacidad de datos personales.
Reglamentación de controles criptográficos.	A.18.1.5		n/a	
Revisiones de seguridad de la información	**A.18.2**		33	
Revisión independiente de la seguridad de la información	A.18.2.1		100	
Cumplimiento con las políticas y normas de seguridad.	A.18.2.2	No se evidencia que se realice una revisión periódica al cumplimiento de las políticas por parte del centro de computo y los sistemas de información.	0	Definir procedimientos para la revisión periódica del cumplimiento de las políticas por parte del centro de computo y los sistemas de información.
Revisión de cumplimiento técnico.	A.18.2.3	No se cuenta con evidencia de la realización de evaluaciones de seguridad con las pruebas realizadas y el seguimiento.	0	Establecer procedimientos y cronogramas para las pruebas de seguridad de la información.

11.5.4. Conclusiones Diagnostico

Los resultados que se obtuvieron al aplicar las 2 herramientas concluyo que el nivel de madurez en seguridad de la información en la entidad se encuentra en un Nivel Repetible, indicando que no se está cumpliendo con un Nivel Aceptable y puede materializarse un ataque en alguno de los 3 pilares de la seguridad de la información.

En gestión del conocimiento se identifica que los funcionarios y contratistas tienen una **Alta Gestión del Conocimiento GC en Seguridad de Información (SI)**, lo que conlleva a que tengan claro cuáles son las debilidades, amenazas, oportunidades y fortalezas de la entidad con respecto a la seguridad de la información; pero así mismo se evidencia que no tienen una total claridad del porcentaje implementado en cada una de las fases de MSPI, ya que en la encuesta obtuvieron un puntaje más bajo.

Según los componentes del ciclo PHVA con la identificación del avance de cada uno, se concluye que, se debe definir un nuevo alcance del MSPI, el manual de políticas es muy básico debido a que no se encuentran relacionadas la mayoría de las políticas acorde al MSPI, porque los activos hasta la fecha no se encuentran identificados completamente en cada área y tampoco están relacionadas todas las áreas, aparte de lo anterior, la información que se encuentra en el documento de activos es incoherente, ósea, no está clara o no es comprensible, por ende se recomienda realizar un formato nuevo de activos y realizar las actividades pertinentes para recolectar una lista nueva, así como actualizar el manual de políticas. Se realiza un cálculo considerando las 29 áreas de la entidad y en donde cada una tiene un promedio de 5 funcionarios o contratistas, lo que deduce, que hay un mínimo de 4 a 5 activos por área, para un total

de 580 activos, y en el documento de activos que tiene la entidad se relacionan 222 activos, por ende, la entidad tiene registrado un mínimo del 35 % a 40 % de sus activos.

Se evidencia que no hay un documento completo o resolución con el comité de seguridad de la información, con la identificación de los roles y responsabilidades en seguridad de la información y tampoco tienen contratado un especialista en seguridad de la información para que lidere el desarrollo de los procesos, actividades, procedimientos, manuales, etc. enfocados en seguridad de la información

Se verifica que existe un documento de gestión de riesgos; pero como se menciona anteriormente los activos no están totalmente definidos y claros, por ende, estos documentos se deben realizar acorde a las nuevas actualizaciones.

No se evidencia un documento con los controles y las pruebas que se le ejecutan, en donde se les realice un seguimiento, identifiquen indicadores y los posibles procedimientos que se desarrollaron si se encuentra alguna vulnerabilidad o amenaza que afecten a la entidad, para que posteriormente se evidencie una mejora continua y por último no se tiene y cumple un cronograma de un plan de capacitaciones en seguridad de la información. Informe General del Diagnostico GAP. Clic AQUÍ.

12. Procedimientos MSPI de la E.S.E. HUSRT

El MinTIC a través de los lineamientos que genera por medio del MSPI en la Guía No 3 - Procedimiento de Seguridad de la Información, especifica los procedimientos que normalmente deben crear las entidades públicas con respecto a la Seguridad y Privacidad de la Información. Este control no se cumple a cabalidad y se debe proyectar en la Declaración de Aplicabilidad, debe ser evaluado en las fases de Evaluación de Desempeño y Mejora Continua, fases que no se ejecutaran en este proyecto y por lo tanto son actividades pendientes para la entidad.

Acorde a lo anterior, se validó, ¿qué procesos tiene ya la entidad?, ¿cuáles no?, ¿quiénes deberían ser los responsables de crearlos y gestionarlos? Lo anterior se especifica en la Matriz de responsables de Procedimientos del MSPI. Clic Aquí.

13. Roles y Responsabilidades

Para diseñar y posteriormente implementar el Modelo de Seguridad y Privacidad de la Información en primer lugar, se deben definir claramente unos roles y responsabilidades de los usuarios involucrados con la información en general, para ello tenemos la tarea de crear de nuevas estructuras TI, que no están definidas actualmente y no atiende a criterios estándar. Lo que este documento pretende, es establecer la definición de roles y responsabilidades en materia de seguridad de la información. Por esto los roles de una organización no deberían sufrir cambios significativos después de su creación, salvo que se produzcan cambios drásticos en la tecnología o estructura de la entidad. En todo caso, los roles pueden sufrir modificaciones en el alcance de sus responsabilidades. Por tanto, la acogida y aplicación de estas responsabilidades es obligatoria para todo el personal de la E.S.E. Hospital Universitario San Rafael de Tunja., cualquiera sea su situación contractual, la dependencia o proceso al cual se encuentre adscrito y el nivel de las tareas que desempeñe.

13.1. Objetivo Roles y Responsabilidades

Identificar los roles y responsabilidades a través de formular lineamientos y actividades para la prevención, detección, contención y recuperación de los activos de información como resultado de eventos e incidentes adversos que afecten la seguridad de la información de la E.S.E. Hospital Universitario San Rafael de Tunja.

13.2. Objetivos Específicos Roles y Responsabilidades

- Establecer un marco de referencia que defina las responsabilidades generales en la gestión de la seguridad de los sistemas de información.
- Definir roles y responsabilidades para la atención de incidentes de seguridad de la información.
- Gestionar de manera oportuna los eventos de seguridad de la información que puedan comprometer la seguridad de la información.

13.3. Alcance de Roles y Responsabilidades

El presente documento describe los roles y responsabilidades de los encargados de la Seguridad de la información de los diferentes procesos de la E.S.E. Hospital Universitario San Rafael de Tunja, conservando la confidencialidad, integridad y disponibilidad de los activos de Información de la entidad. Por lo anterior, todos los colaboradores serán responsables de la identificación, evaluación y control de los riesgos de seguridad de la información.

13.4. Definición de Roles y Responsabilidades

La identificación de los roles y responsabilidades en la E.S.E. Hospital Universitario San Rafael de Tunja permite establecer al interior de la entidad las acciones correspondientes para proteger los activos de información, reduciendo posibles eventos y/o incidentes de seguridad de la información. De esta manera los colaboradores de la entidad adquieren el compromiso de protegerlos y se hacen partícipe de las actividades e iniciativas encaminadas al aseguramiento de los recursos que se encuentran bajo su custodia.

13.5. Identificación de los responsables

Para lograr el buen funcionamiento del Modelo de Seguridad y Privacidad de la Información, la Entidad se establecerá los roles y responsabilidades de los colaboradores de la entidad que se van a encargar de establecer y desarrollar cada una de estas actividades asociadas a los sistemas.

Para la asignación de los responsables, la E.S.E. Hospital Universitario San Rafael de Tunja, analizará las funciones de cada rol relacionándolas con las actividades que realiza el personal de la entidad, por lo anterior, es necesario que las responsabilidades asignadas en el desarrollo del Sistema de Gestión de Seguridad de la Información y el Modelo de Seguridad y Privacidad de la Información, para cada perfil, sean incorporadas a los manuales de funciones y/o en las obligaciones de los contratos por prestación de servicios de acuerdo con el cargo que desempeñan.

A continuación, se definen algunos roles y responsabilidades que se deben tener en cuenta en la implantación y seguimiento del Sistema de Gestión de Seguridad de la Información y el Modelo de Seguridad y Privacidad de la Información.

Tabla 29.

Roles y Responsabilidades.

RECURSO HUMANO	ROL	RESPONSABILIDADES
COMITÉ DE SEGURIDAD DE INFORMACIÓN	➢ Alta Dirección	Apoyo implementación MSPI
SECRETARIA DEL COMITÉ DE SEGURIDAD DE INFORMACIÓN	➢ Coordinar Actividades del Comité.	Desarrollar todas las actividades pertinentes para que los comités se ejecuten efectivamente.
LIDER DE SEGURIDAD DE INFORMACIÓN	➢ Toma de decisiones.	Toma de decisiones frente a la seguridad de la Información
EQUIPO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	➢ Oficial de seguridad ➢ Oficial de tratamiento de datos personales ➢ Analista de seguridad de la información – gestor de riesgo ➢ Gestor de controles ➢ Analista forense ➢ Analista de datos	Gestión operativa y apoyo al líder de Seguridad de la Información o quien haga sus veces
EQUIPO PROCESOS GESTIÓN DE SISTEMAS DE INFORMACIÓN Y COMUNICACIONES	➢ Coordinador de TIC ➢ Administrador de Servidores ➢ Administrador de Base de Datos ➢ Administrador de Aplicaciones ➢ Administrador de Redes	Gestión operativa para la configuración, monitoreo y seguimiento de controles, así como apoyo del equipo de Seguridad de la Información y Ciberseguridad.

ROLES RELEVANTES	➢ Propietarios de activos ➢ Custodio de activos de información ➢ Usuarios de activos de información ➢ Auditor de seguridad de la información	Gestión operativa y apoyo al Líder de Seguridad de la Información o quien haga sus veces y Oficial de Tratamiento de Datos.

Nota: Elaboración Propia

13.5.1. Comité de Seguridad de la Información

El Comité de Seguridad de la Información, es creado en E.S.E. Hospital Universitario San Rafael de Tunja, mediante Resolución 051 de 2022; en el cual tiene dentro de sus funciones:

- Definir y aprobar las directrices, políticas y mecanismos de control y seguimiento de la Información de la Entidad de conformidad con el marco normativo vigente.
- Aprobar los objetivos de seguridad de la información, los cuales estarán alineados con los objetivos estratégicos de la entidad.
- Aprobar anualmente o cuando se requiera la Política de Seguridad y Privacidad de la Información de la entidad.
- Asignar y aprobar el presupuesto necesario para la implantación y posteriormente el normal funcionamiento y/o puesta en marcha del Sistema de Gestión de Seguridad de la Información, Sistema de Gestión de Continuidad de Negocio y Modelo de Seguridad y Privacidad de la Información.
- Garantizar que los requisitos del Sistema de Gestión de Seguridad de la Información, Sistema de Gestión de Continuidad de Negocio y Modelo de

Seguridad y Privacidad de la Información, se encuentran integrados en todos los procesos críticos de la entidad.

- Proporcionar los recursos necesarios para la implementación y desarrollo de las actividades del Sistema de Gestión de Seguridad de la Información, Sistema de Gestión de Continuidad de Negocio y Modelo de Seguridad y Privacidad de la Información de la entidad.
- Velar por la ejecución y desarrollo de las actividades del Sistema de Gestión de Seguridad de la Información, Sistema de Gestión de Continuidad de Negocio y Modelo de Seguridad y Privacidad de la Información.
- Promover activamente una cultura de seguridad y privacidad de la información basada en riesgos para la entidad.
- Aprobar los roles y responsabilidades relacionados con la seguridad de la información en todos los niveles de la entidad.
- Postular y nombrar la Secretaria del Comité de Seguridad de la Información.

13.5.2. Secretaria del Comité De Seguridad De Información

Las funciones de la Secretaría Técnica serán las siguientes:

- Elaborar las actas de las reuniones del Comité y verificar su formalización por parte de sus miembros.
- Citar a los integrantes del Comité a las sesiones ordinarias o extraordinarias.
- Remitir oportunamente a los miembros la agenda de cada comité.
- Llevar la custodia y archivo de las actas y demás documentos soportes.
- Servir de interlocutor entre terceros y el Comité.
- Realizar seguimiento a los compromisos y tareas pendientes del Comité.

- Presentar los informes que requiera el Comité.
- Las demás que le sean asignadas por el Comité.

13.5.3. Líder de Seguridad de la Información.

Responsable de Seguridad Digital que, a su vez, también es el responsable de la Seguridad de la Información en la entidad, el cual debe pertenecer a un área que haga parte de la Alta Dirección. Así mismo, el cual asistirá en forma oportuna y garantizará el mejoramiento continuo de cualquier necesidad de mejora respecto a la seguridad y privacidad de la información de la entidad. Sus principales funciones son:

- Emitir conceptos referentes a riesgos y seguridad de la información de la entidad, para la toma de decisiones por parte del comité de Seguridad y Privacidad de la Información.
- Coordinar la implementación, despliegue y sostenibilidad del Sistema de Gestión de Seguridad de la Información y Modelo de Seguridad y Privacidad de la Información.
- Mantener una comunicación clara, oportuna, completa y permanente con los integrantes del comité de Seguridad y Privacidad de la Información.
- Definir las herramientas, metodologías y lineamientos necesarios para la implementación del Modelo de Seguridad y Privacidad de la Información.
- Realizar seguimiento a los objetivos planteados frente al Sistema de Gestión de Seguridad de la Información y Modelo de Seguridad y Privacidad de la Información, para detectar desviaciones y tomar las acciones correctivas necesarias.
- Verificar el cumplimiento de la implementación de los objetivos y tareas asignadas al Comité de Seguridad y Privacidad de la Información.

- Verificar que se incluyan los temas asociados al Modelo de Seguridad y Privacidad de la Información, dentro del plan de capacitaciones de la entidad.
- Asegurar que se definan e implementen actividades de sensibilización y concienciación frente a la seguridad de la información a la Alta Dirección y demás partes interesadas.
- Guiar a la Alta dirección de la entidad, ante incidentes de seguridad mediante el plan de respuesta de incidentes.
- Responsable de la elaboración y desarrollo del Plan de Seguridad de la Información.
- Mantener contacto con grupos de interés.
- Mantener y promover la actualización de las políticas de seguridad de la información.
- Debe responder por la revisión de problemas de seguridad de la información existentes y aquellos que se consideren potenciales.

13.5.4. Equipo de Seguridad y Privacidad de la Información.

Es el equipo que se encarga por velar que se implemente el MSPI y que la seguridad y privacidad de la información este en términos aceptables en sus tres pilares (Confidencialidad, Integridad y Disponibilidad), para que la entidad cumpla con su objeto social, debe generar mecanismos proactivos y reactivos para que no se materialicen los riesgos o subsanar los incidentes que se presenten.

13.5.4.1. Oficial de Seguridad de la Información

Oficial de Seguridad de la Información: Se encarga de implementar, controlar y mantener las políticas, normas, estándares, procedimientos, necesarios para preservar y proteger la confidencialidad, disponibilidad e integridad de la información.

- Responsable por la correcta ejecución de los procedimientos relacionados con el manejo de Incidentes, en todas sus etapas.
- Liderar al grupo de investigación de incidentes aportando sus conocimientos específicos en el área de Seguridad y realizar el proceso de documentación general del proceso de investigación y de la evidencia recopilada.
- Responsable por la ejecución del procedimiento de tratamiento de evidencia y su adecuado manejo durante la investigación del incidente correspondiente (Cadena de Custodia).
- Evaluar la definición de perfiles de usuarios en las diferentes plataformas y sistemas de acuerdo con las necesidades de recursos establecidas y las funciones de los diferentes cargos.
- Contar con mecanismos de monitoreo con el fin de detectar oportunamente procedimientos inseguros para los Sistemas Operacionales, Aplicativos, Datos y Redes.
- Evaluar la definición de los requerimientos de respaldo y backups de la información almacenada en servidores y medios magnéticos requerida para garantizar la continuidad del negocio.
- Definir, configurar y mantener la base de datos de conocimiento de Seguridad de la Información y el archivo Físico de Seguridad de la Información

- Identificar el detalle de los requerimientos de inscripción de la información y definir la solución.
- Realizar las evaluaciones de riesgo de seguridad de la información con el apoyo del Coordinador.

13.5.4.2. Oficial de Tratamiento de datos personales

Promover la elaboración e implementación de un sistema que permita administrar los riesgos del tratamiento de datos personales.

- Coordinar la definición e implementación de los controles del Programa Integral de Gestión de Datos Personales.
- Servir de enlace y coordinador con las demás áreas de la organización para asegurar una implementación transversal del Programa Integral de Gestión de Datos Personales.
- Impulsar una cultura de protección de datos dentro de la organización.
- Mantener un inventario de las bases de datos personales en poder de la Organización y clasificarlas según su tipo.
- Realizar un entrenamiento general en protección de datos personales para todos los empleados de la E.S.E. Hospital Universitario San Rafael de Tunja.
- Realizar el entrenamiento necesario a los nuevos empleados, que tengan acceso por las condiciones de su empleo, a datos personales gestionados por la organización.

- Integrar las políticas de datos dentro de las actividades de las demás áreas de la organización (talento humano, seguridad, call centers y gestión de proveedores, etc.).
- Medir la participación, y calificar el desempeño de los empleados, se encuentre haber completado satisfactoriamente el entrenamiento sobre protección de datos personales.

13.5.4.3. Analista de seguridad de la Información

Es el encargado de identificar, desarrollar, implementar y mantener los procesos en la organización para reducir los riesgos en los activos de la información y en la plataforma tecnológica, también debe responder a los incidentes, establecer normas y políticas apropiadas y velar por que estas se cumplan adecuadamente. Las responsabilidades y funciones son las siguientes:

- Salvaguardar los activos de información de la empresa, el cumplimiento normativo y los sistemas informáticos.
- Administrar el desarrollo y la aplicación de las políticas de seguridad, normas y procedimientos para garantizar el mantenimiento continuo de la seguridad de la información y la protección de activos.
- Definir la arquitectura de seguridad de red, acceso a la red y las políticas de monitoreo.
- Capacitación y sensibilización de los empleados frente a la cultura de seguridad en toda la organización.
- Desarrollar e implantar un sistema de gestión de la seguridad que permita identificar y dar respuesta a los nuevos riesgos de la organización.

- Estar a cargo de la planificación de respuesta de incidentes, así como la investigación de vulneración de la seguridad.
- Trabajar con consultores o terceros según sea apropiado para las auditorías de seguridad externas.
- Desarrollar el plan operativo anual del área de seguridad de la información.
- Aprobar las principales iniciativas para el incremento del nivel de seguridad de la información.
- Supervisar los cambios significativos en la exposición de los recursos de información frente a las amenazas más importantes.
- Supervisar los incidentes relativos a la seguridad.
- Garantizar que la seguridad sea parte del proceso de planificación de la información y un requisito más del negocio.
- Coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios.
- Crear y definir los aspectos para la conformación de un grupo de respuesta a incidentes de seguridad, para atender los problemas relacionados a la seguridad informática dentro de la organización

13.5.4.4. Gestor de Controles

Las funciones de este rol son las siguientes:

- Apoyar al oficial de seguridad y a los líderes del proceso en la identificación de activos de información.
- Apoyar al oficial de seguridad a los líderes de proceso en la aplicación de la metodología de valoración de riesgos.

- Apoyar la medición de indicadores del SGSI.
- Alimentar la herramienta dispuesta para la documentación del SGSI.
- Proponer al Oficial de seguridad de la información actualización a la documentación del SGSI existente.
- Gestionar las campañas de sensibilización o divulgación del SGSI.
- Apoyar la mejora continua del SGSI

13.5.4.5. Analista forense

Las funciones de este rol son las siguientes:

- Debe estar disponible en caso de que ocurra un incidente de impacto alto (o uno que amerite acciones disciplinarias o legales o investigación profunda) que requieran la recopilación de evidencia digital.
- Debe ser un apoyo para los demás roles en caso de dudas sobre los procedimientos o acciones a seguir con respecto a la gestión de incidentes y debe ejercer un liderazgo técnico en el proceso de atención de incidentes de seguridad de la información.

Se recomienda que el primer respondiente cuente con habilidades y experiencia en recolección de evidencia digital de diferente tipo y sobre diferentes tipos de activos. Adicionalmente se recomienda que conozca y maneje los fundamentos jurídicos que exigen la intervención de un perito en informática forense y que tenga conocimientos sobre la ejecución de procedimientos de gestión de vulnerabilidades y test de penetración sobre plataforma tecnológica.

13.5.4.6. Analista de Datos

- Reconocer y solucionar problemas específicos gracias al análisis de datos.
- Gestionar y analizar toda la información nueva que se recabe detectando así posibles ataques en tiempo real.
- Análisis Big Data para identificar irregularidades y posibles violaciones de seguridad.
- Procesar datos y analizarlos para identificar quien pretende transgredir los datos de la entidad.
- Interpretar datos, analizar resultados utilizando técnicas estadísticas y enviar informes.
- Desarrollar e implementar bases de datos, sistemas de recopilación de datos, analítica de datos y otras estrategias que optimicen la eficiencia estadística y la calidad.
- Captar datos de fuentes de datos primarias o secundarias y mantener las bases de datos y los sistemas de datos.
- Identificar, analizar e interpretar tendencias o patrones en conjuntos complejos de datos.
- Filtrar y «limpiar» los datos mediante la revisión de informes informáticos, impresos e indicadores de rendimiento para localizar y corregir problemas de código.
- Trabajar con la dirección para priorizar las necesidades de información y de la empresa.
- Localizar y definir nuevas oportunidades de mejora de procesos.

13.5.5. Equipo Proceso Gestión de Sistemas de Información y Comunicaciones

13.5.5.1. Coordinador de TIC

- Dirigir, planear, organizar y controlar, los procesos del área.
- Elaborar y actualizar el Plan Estratégico de Tecnología de la Información.
- Gestionar la implementación de normas y procedimientos del uso de hardware y software alineados por la seguridad de la información.
- Coordinar y gestionar la integración de las Tecnologías de la Información, la Comunicación en el centro, la Seguridad de la Información y la Gestión de Datos Personales.
- Coordina y supervisa la producción de manuales, instructivos y formularios para hardware y software.
- Analizar las necesidades del centro relacionadas con las Tecnologías de la Información y la Comunicación integradas con Seguridad de la Información y para posteriormente elaborar propuestas y proyectos presentadas a la Alta Dirección.
- Conocer las distintas amenazas y riesgos asociados al uso de las tecnologías y la Red para gestionar la aplicación de medidas de protección y seguridad.
- Identificar y promover las conductas apropiadas en el contorno digital para proteger la información y datos personales.
- Conocer y aplicar los principios legales, éticos y sociales incorporados con el uso de información digital, los derechos de propiedad intelectual y las licencias de uso.
- Identificar y gestionar la aplicación de medidas de seguridad y prevención de riesgos en la operación de equipos tecnológicos.
- Velar por el desempeño de indicadores, flujo de documentos, agilización, racionalización de trámites y la aplicación del gobierno en línea

- Gestionar y administrar el buen funcionamiento de los sistemas de información, infraestructura y red tecnológica.
- Supervisa el trabajo del personal a su cargo.
- Gestionar las pruebas de vulnerabilidad y de auditoría de sistemas para evidenciar las vulnerabilidades y riesgos que tiene el área para posteriormente implementar los controles aprobados por la Alta Dirección.

13.5.5.2. Administrador de Servidores

- Administrar, operar y gestionar las plataformas de sistemas operativos, almacenamiento y centro de datos.
- Instaurar y operar los mecanismos de respaldos en los sistemas operativos de los servidores físicos y virtuales.
- Implantar y operar los mecanismos de monitoreo de los sistemas operativos de los servidores físicos y virtuales.
- Detectar y corregir errores en los servidores.
- Realizar las actualizaciones a los sistemas operativos, aplicaciones, controladores, etc. que mejoren y mitiguen la seguridad de la información.
- Configurar, administrar y gestionar los servidores de Directorio Activo, DNS, DHCP.
- Administrar y gestionar roles, perfiles, usuarios, permisos, políticas de los usuarios del directorio activo, de la red y de los sistemas operativos.
- Programar scripts a los servidores para la ejecución de tareas programadas automatizadas.
- Administrar, gestionar la instalación y mantenimiento del antivirus en los equipos de la red.
- Configurar, administrar y gestionar el correo Exchange.

- Administrar, configurar y gestionar los periféricos como escáneres, impresoras, etc.
- Configurar, administrar y gestionar las copias de seguridad de los servidores.
- Administrar y gestionar el Firewall de la entidad.

13.5.5.3. Administrador de Base de Datos

- Implementar, mantener, optimizar y administrar estructuras de bases de datos para la entidad.
- Conceder permisos y privilegios a los usuarios.
- Realizar actividades en conjunto con los Gerentes de Proyecto de TI, Desarrolladores, Diseñadores multimedia y Administradores de aplicaciones.
- Supervisar las actividades de las bases de datos.
- Solucionar incidencias y perdidas de datos.
- Planificar y conservar un sistema de respaldo.
- Realizar copias de seguridad y recuperación.
- Proyectar la capacidad para que no se presenten inconvenientes futuros.
- Gestionar la seguridad de las bases de datos.

13.5.5.4. Administrador de Aplicaciones

- Configurar, administrar y gestionar el Servidor de Aplicaciones.
- Supervisar, actualizar y realizar mantenimiento a las aplicaciones de software.
- Monitorear la red de aplicaciones para prevenir ataques de virus e incidentes de seguridad.
- Generar un sistema de respaldo de las aplicaciones.

- Asignar niveles de acceso, roles, perfiles, permisos, usuarios, contraseñas para los que interactúan con las aplicaciones de escritorio o web.
- Capacitar al personal que accede a las aplicaciones.
- Diagnosticar y solucionar problemas que presentan las aplicaciones.

13.5.5.5. Administrador de Redes

- Diseñar, instalar y configurar las redes de la entidad que garanticen una seguridad aceptable.
- Gestionar y administrar la red.
- Detectar y corregir fallas de la red.
- Generar y supervisar las posibles actualizaciones y migraciones.
- Configurar y realizar mantenimiento a el Router y los Switch de la red.
- Gestionar los proyectos para la adquisición e instalación de nuevos equipos de red acorde a una planeación presupuesto.
- Gestionar, administrar, configurar las redes wifi y los procedimientos necesarios para que accedan.

13.5.6. Otros Roles Relevantes para la Seguridad de la Información y Ciberseguridad

Todos los servidores públicos, estudiantes, contratistas, practicantes o terceros y demás personas jurídicas o naturales que hagan uso de la información y de las tecnologías que la soportan, tienen un rol de seguridad de la información, según el nivel

de involucramiento con la información con la que trabajan. Los roles descritos en esta sección son: propietarios, custodios y usuarios de la información.

13.5.6.1. Propietarios de Activos de Información

Rol, proceso o área con la capacidad de tomar decisiones sobre activos de información. Por ejemplo: cambiar, eliminar, conceder acceso, o compartir; sus responsabilidades incluyen:

- Autorizar y/o denegar acceso a los activos de información que se encuentren bajo su responsabilidad. Participar en los procesos de gestión del riesgo de seguridad de la información.
- Validar que los activos de información bajo su responsabilidad se encuentren dentro del inventario de activos de información.
- Velar por la existencia de custodios de los activos de información bajo su responsabilidad.
- Apoyar la realización de actividades de gestión del riesgo sobre los activos bajo su responsabilidad; lo que incluye, por ejemplo, la entrega oportuna de información y la asistencia a sesiones de trabajo celebradas para tal fin.

13.5.6.2. Custodio de Activo de Información

Rol con mandato de aplicar y mantener controles para proteger la seguridad de activos de información. Los administradores de sistemas de información, por ejemplo, son custodios de los sistemas que administran. Sus responsabilidades incluyen:

- Aplicar, operar y mantener los controles para la protección de los activos de información.
- Participar en las actividades de mitigación o tratamiento de riesgos en las que sea requerido.
- Rendir cuentas sobre la eficacia de los controles aplicados a los activos de información bajo su responsabilidad.

13.5.6.3. Usuarios de Activos de Información

Corresponde a todos los usuarios de la información de la E.S.E. Hospital Universitario San Rafael de Tunja y de otros activos que la soportan, por ejemplo, los sistemas de información. Sus responsabilidades incluyen:

- Apoyar, asesorar y cuando sea requerido coordinar las actividades de gestión del riesgo de información.
- Reportar cambios en procesos, estrategias, o activos de información al comité de dirección de seguridad de la información.
- Cumplir las políticas de seguridad de la información de la entidad.
- Atender las iniciativas de cultura en seguridad de la información en las que se requiera de su participación.
- Reportar cualquier anomalía que puede desencadenar en incidentes de seguridad.

13.5.6.4. Auditor de Seguridad de la Información

El auditor de seguridad informática comprueba que las medidas de seguridad y control de los sistemas informáticos se adecúan a la normativa que se ha desarrollado para la protección de los datos; identifica las deficiencias, y propone medidas correctoras o complementarias. Este debe ser un rol con objetividad e independencia del área que supervisa, responsabilidades incluyen:

- Validar el cumplimiento de la normativa “MSPI” emitida por Min Tic.
- Reportar hallazgos y sugerencias al comité de dirección de seguridad de la información.
- Cumplir las políticas de seguridad de la información de la entidad.
- Reportar cualquier anomalía que puede desencadenar en incidentes de seguridad.
- Generar reportes, observaciones y recomendaciones para mejorar la infraestructura tecnológica y la seguridad de la información.

Informe General de Roles y Responsabilidades. Clic AQUÍ.

14. Gestión de Activos

Esta Metodología brinda los lineamientos para la identificación y clasificación de los activos de la información que son manejados en el Hospital Universitario San Rafael de Tunja, los cuales hacen parte fundamental para el desarrollo del Modelo de Seguridad y Privacidad de la Información (MSPI), en el marco de la Estrategia de Gobierno en Línea.

El levantamiento de estos activos de información se elabora haciendo uso de las mejoras prácticas Nacionales e Internacionales para suministrar a la entidad requisitos de diagnóstico, planificación, implementación, gestión y mejora continua.

Manual General de Levantamiento de Activos. Clic AQUÍ.

Matriz de Levantamiento de Activos. Clic AQUÍ.

15. Manual de Políticas de Seguridad y Privacidad de la Información

El activo más importante para las entidades es la información en sus diferentes presentaciones, por ende, a nivel internacional y nacional se generaron modelos gestión de seguridad de la información (MGSI), que tienen como objeto mitigar los riesgos de seguridad de la información para preservar la confidencialidad, integridad y disponibilidad de la información.

La E.S.E Hospital Universitario San Rafael Tunja (HUSRT) basada en el criterio anterior y en que cuenta con talento humano comprometido, motivado e idóneo, con el apoyo de tecnología avanzada, genera confianza, desarrollo, calidad de vida y responsabilidad social a nuestra sociedad, por ende, diseña e implementa el Modelo de Seguridad y Privacidad de la Información (MSPI), que acorde a uno de sus lineamientos se debe generar un Manual de Políticas de Seguridad de la información.

El manual de Seguridad de la Información de la E.S.E. Hospital San Rafael Tunja, es un documento que contiene los objetivos, alcance, definiciones, la política general de seguridad y las políticas específicas, que soportan el Modelo de Seguridad y Privacidad de la Información, que orientan y apoyan la gestión y administración en materia de seguridad de la información.

Manual de Políticas de Seguridad y Privacidad de la Información. Clic AQUÏ.

Resolución 238 del 2022 Política General de Seguridad. Clic AQUÏ.

16. Plan de Sensibilización, Capacitación y Comunicación del MSPI

En la última década, las tecnologías de información y comunicaciones se han convertido en la herramienta por excelencia para la optimización de los procesos y el funcionamiento eficaz de las empresas. Con el uso de la tecnología, surgen a su vez amenazas y vulnerabilidades asociadas, que pueden llegar a afectar la disponibilidad, privacidad, confidencialidad e integridad de la información que se encuentra en las diferentes plataformas, afectando de esta manera el desempeño normal de la Entidad. Para esto, el modelo de seguridad y privacidad indica pautas específicas para guiar a las instituciones a mejorar sus plataformas y mitigar amenazas que pueden llegar a traer consigo las tecnologías implementadas, sin embargo, un programa robusto de seguridad y privacidad de la información, no se basa únicamente en el aseguramiento de plataformas y procesos, sino que también debe involucrar los factores humanos, que en muchos casos, son la principal causa de los incidentes de seguridad dentro de un sistema determinado, esto debido a que no conocen sobre seguridad de la información y su rol dentro de la Entidad. Muchas instituciones no prestan la suficiente atención a su recurso humano, que puede llegar a ser el eslabón más débil en la cadena de la seguridad de la información, por lo que es necesario sensibilizarlos o capacitarlos sobre la importancia de la preservación de la información.

Plan de Sensibilización, Capacitación y Comunicación del MSPI. Clic AQUÏ.

CAPITULO IV

17. Gestión de Riesgos

Los activos de información del Hospital Universitario San Rafael Tunja son indispensables para su correcto desempeño dentro de la Política de Gobierno Digital y la prestación efectiva y eficiente de los servicios a los usuarios, generando el cumplimiento de sus objetivos estratégicos, por lo tanto, se debe generar una correcta Gestión de Riesgos de Seguridad y Privacidad de la Información para evitar perdida de confidencialidad, integridad y disponibilidad de los activos de información, acorde a lo anterior, se debe generar una cultura de carácter preventiva.

El hospital es una empresa social del estado y teniendo en cuenta que se va a desarrollar el contexto organizacional de esta guía, se rige por la normativa establecida por el estado colombiano, CONPES 3995 de 2020, Modelo de Seguridad y Privacidad de MINTIC y lo establecido en el decreto 1008 de 14 de junio 2018, a la Resolución 500 de 2021, por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital adoptando las buenas prácticas y los lineamientos de los estándares ISO 27001, ISO 31000:2018 y la guía para la administración del riesgo y el diseño de controles en entidades públicas (DAFP), Riesgos de gestión, corrupción y seguridad digital, establecidos en el Modelo Integrado de Planeación y Gestión que están enfocados en las entidades del estado.

Para iniciar con la GRSPI se tiene como insumo la clasificación de activos de información, para posteriormente identificar o plantear acciones que mitiguen la materialización de riesgos, posteriormente se implementa la Guía No 7 Gestión del Riesgo del MSPI con la

Guía de Riesgos del DAFP que formulan la planeación para la identificación, análisis, evaluación, tratamiento y monitoreo de los Riesgos de Seguridad y Privacidad de la Información.

Informe General de Gestión de Riesgos. Clic AQUÏ.

Matriz de Gestión de Riesgos. Clic AQUÏ.

18. Declaración de Aplicabilidad

La E.S.E. HUSRT define los controles de seguridad de la información aplicados y por aplicar, acorde a los lineamientos especificados por el MinTIC a través del Anexo A del MSPI que es tomado del Anexo A de la Norma ISO/IEC 27001:2013.

Esta declaración es revisada y aceptada por el Comité de Seguridad y Privacidad de Información de la entidad y se basa en los controles identificados en la herramienta GAP y en la Gestión del Riesgo.

La declaración se revisará trimestralmente para validar qué controles se han ejecutado, cuáles quedan por ejecutar, para posteriormente realizar un feedback, así mismo, se actualizará cada año acorde a los nuevos activos, vulnerabilidades, riesgos, amenazas y a los nuevos controles identificados por implementar. Declaración de Aplicabilidad, Clic AQUÏ.

18.1. Objetivo General Declaración de Aplicabilidad

Fortalecer la Seguridad y Privacidad de la Información, definiendo y aplicando los controles especificados por el MinTIC a través del Anexo A del MSPI, de igual forma explicando las exclusiones de estos, para proteger la información de la entidad, buscando mantener su integridad, confidencialidad y disponibilidad.

18.2. Convenciones

A continuación, se describen las convenciones o justificaciones del porque la selección o excepción de los controles seleccionados.

RL: Requerimientos Legales

OC: Obligaciones Contractuales

RN/MP: Requerimientos del Negocio/Mejores Prácticas adoptadas,

RVR: Resultado de la Valoración de Riesgos

19. Indicadores de Seguridad y Privacidad de la Información

La E.S.E Hospital Universitario San Rafael Tunja, es una Entidad que cuenta con talento humano comprometido, motivado e idóneo, con el apoyo de tecnología avanzada, que entienden la importancia de una adecuada gestión de la información; acorde a lo anterior busca crear condiciones de uso confiable de todos los activos de información, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información.

Conforme a la gestión de riesgos se plantean unos tratamientos o controles, los cuales tiene unos responsables de ejecución y de seguimiento, generando las condiciones de uso confiable en donde se evalúa o aplican unos indicadores de gestión que miden la eficacia, eficiencia y efectividad.

El presente documento relaciona todos los indicadores propuestos y que se aprobaron para realizar un seguimiento al tratamiento o controles de seguridad de la información a partir de abril del 2023, estos se basan en los indicadores propuestos por el MSPI; pero se complementan acorde al tratamiento de riesgos. Lo principal que se identifica en cada uno de los indicadores es su objetivo y la formula con sus variables para validar que se está cumpliendo con las metas.

Indicadores de Seguridad y Privacidad de la Información. Clic AQUÏ.

CAPITULO V

20. Resultados Esperados

Los resultados esperados y sus productos se especifican en la siguiente tabla:

Tabla 30.

Resultados Esperados

Objetivo Específico	Resultado Esperado	Medio de Verificación	Supuestos
Determinar e identificar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad y su nivel de madurez.	Nivel de madurez de Seguridad y Privacidad de la Información de la E.S.E. HUSRT.	Herramienta de Diagnostico MSPI. Link.	Reporte de Incidentes de seguridad y el no cumplir con la Política de Gobierno Digital.
Realizar el diseño e implementar la identificación de los Activos de Información con Criticidad Alta, la Gestión de los Riesgos y establecer los Controles de Seguridad y Privacidad de la Información.	Identificación de los activos de información con criticidad alta analizando sus amenazas, vulnerabilidades, riesgos y controles.	*Matriz de Activos de Información. Link. *Matriz de Gestión del Riesgo. Link.	No tener el MSPI estipulado en los lineamientos de la Política de Gobierno Digital.
Generar la Declaración de Aplicabilidad que la entidad aprueba	Informe en donde se pasa al Comité de Seguridad y Privacidad de la	Matriz de Declaración de Aplicabilidad. Link.	No se tiene identificado que controles se deben aplicar y el

para la gestión de los Riesgos de Seguridad y Privacidad de la Información.	Información de la Entidad identificando los controles o tratamientos a implementar y que deben ser aprobados.		responsable para mitigar los ataques y riesgos de seguridad y privacidad de la Información.

Nota: Elaboración propia

21. Impactos Esperados

Los impactos esperados y sus plazos se especifican en la siguiente tabla:

Tabla 31:

Impactos esperados del proyecto

Tipo Impacto	Impacto Esperado	Plazo (Corto: 1-4 años, Mediano: 5-9 años, Largo: más de 10 años)
Capacidades científico tecnológicas	Mejoramiento del servicio tecnológico, sistemas de información, red y gestión documental de la Entidad.	1 año
Sociales /Económicos/Ambientales	*Información de los usuarios, funcionarios, contratistas, entidad y terceros mucho menos vulnerable.	1 año
Productividad y competitividad	Atención a los ciudadanos eficiente y eficaz.	1 año

Nota: Elaboración propia

22. Cronograma

La tabla a continuación relaciona el tiempo empleado en meses para el desarrollo de cada una de las actividades del proyecto. Tiene como supuesto una dedicación semanal de 15 horas.

Tabla 32.

Cronograma de actividades

Fase / Actividad	2022									2023								
Mes	Ab	My	Jn	JL	Ag	Sp	O	N	D	E	F	M	Ab	My	Jn	JL	Ag	Sp
Fase 1																		
Diagnostico GAP.																		
Informe Diagnostico																		
Fase 2																		
Alcance MSPI - Descripción y actualización del contexto de la entidad																		
Descripción de las expectativas de las partes interesadas																		
Seleccionar el comité – roles y definir responsabilidades																		
Recolección y clasificación de los activos																		
Definir la política de seguridad de información con su Manual																		
Plan de Comunicación, Sensibilización y Capacitación																		
Fase 3																		
Identificación de Riesgos																		
Tratamiento de Riesgos																		

Definir indicadores																		
Declaración de Aplicabilidad																		
Resultados, Impactos y Conclusiones																		

Nota: Elaboración propia

23. Presupuesto

La tabla a continuación contiene todos los rubros asociados a la ejecución del presente proyecto.

Tabla 33.

Presupuesto del proyecto

Ítem	Unidad	Cantidad	Meses	Valor unitario (en pesos)	Valor Total (en pesos)	Aporte (en pesos)	
						Personal	UM
Recursos Humanos							
Autor	hora	50	18	$20,000	$18,000,000	$18,000,000	$ -
Asesoría	hora	4	18	$62,500	$4,500,000	$ -	$ 4,500,000
Recursos Técnicos							
Software[8]	-	-	18	$ -	$ -	$ -	$ -
PC	-	1	18	$ -	$ 3,200,000	$3,200,000	$ -
Internet	hora	1	18	$40,000	$ 720,000	$ 720,000	$ -
Subtotal						$21,920,000	$4,500,000
Imprevistos (5%)						$1,096,000	$200,000
Totales						$23,016,000	$4,700,000
Total, Proyecto							**$ 27,716,000**

Nota: Elaboración propia

[8] El software que se usará en el proyecto es de libre acceso y uso, por lo que no genera rubro en el presupuesto.

24. Conclusiones

El diseño y ejecución del proyecto conlleva a concluir que el no implementar un Sistema de Gestión de Gestión de Seguridad de la Información (SGSI) hace que la entidad ejecute sus procesos y cumplimiento de metas de una forma inadecuada y le pueda generar pérdidas de confidencialidad, integridad, disponibilidad de la información, económicas, sociales, ambientales, etc. por ende, se formuló, diseño y ejecuto el Modelo de Seguridad y Privacidad de la Información (MSPI) hasta el lineamiento de la Declaración de Aplicabilidad, el cual la entidad posteriormente valorara e implementara acorde a sus recursos. Para llegar hasta este punto fue fundamental ejecutar los siguientes lineamientos del MSPI donde se concluye lo siguiente:

En el diagnóstico realizado por medio de la entrevista a los funcionarios, contratistas y con el diligenciamiento de la herramienta de diagnóstico del MSPI se verifico que el nivel de madurez en seguridad de la información en la entidad se encuentra como Repetible, por ende, se concluye, que no se está cumpliendo con un nivel aceptable. Con respecto a la gestión del conocimiento valorado en los funcionarios y contratistas se obtiene una Alta Gestión del Conocimiento (GC) en Seguridad de Información (SI), lo que indica que tienen claro cuáles son las debilidades, amenazas, oportunidades y fortalezas de la entidad con respecto a la seguridad de la información; pero no tienen una total claridad del porcentaje implementado en cada una de las fases de MSPI, ya que en la encuesta obtuvieron un puntaje bajo.

Para continuar con la gestión del MSPI y el desarrollo del proyecto en la entidad se establece el Comité de Seguridad y Privacidad de la Información, quien aprobara y validara todos los documentos, procesos, procedimientos, políticas, matrices, diseños, recursos, personal y responsabilidades, este comité queda aprobado mediante Resolución 051 de 2022.

Como segunda medida se desarrolla el manual de Roles y Responsabilidades, que es aprobado por el comité, en donde se identifica los equipos con los profesionales que estarán a cargo de las funciones de acuerdo a los roles especificados.

En la recolección de los activos de información de la entidad se evidencio que el 8 de junio del 2022 cuenta con 572 activos aprobados en la Resolución 239 de 2022 y que a la fecha aumento a 616 activos de información, de los cuales, 185 son de criticidad alta, que corresponden al tipo de activo Hardware, Software, Servicios, Personas, Instalaciones e Información física o digital y 13 activos son de infraestructura critica cibernética. Es de aclarar que en la matriz se identificaron los propietarios y custodios de cada uno de los activos con la clasificación de la información.

Acorde a la identificación de los activos se realiza el Manual de Políticas de Seguridad y Privacidad de la Información en el cual se plasma la Política General de Seguridad y Privacidad de la Información con sus dominios, acorde a los lineamientos del MSPI en donde se plasman las políticas que se identificaron al realizar la evaluación del estado actual de la entidad en la herramienta de diagnóstico del MSPI. Las políticas son aprobadas mediante la Resolución 238 de 2022 y se dan a conocer para que sean implementadas por los funcionarios, contratistas, proveedores y demás terceros que tengan de una u otra forma relación con la entidad.

Los activos con criticidad alta se plasman en la Matriz de Gestión del Riesgo, para identificar por cada activo cada uno de sus riesgos, a los que posteriormente se le realiza un análisis del riesgo el cual arroja un riesgo inherente, a este se le realiza una valoración del riesgo acorde a los controles que se están implementando actualmente en la entidad, del cual se obtiene un riesgo residual y al que se le aplica un tratamiento para reducir, trasferir, compartir, asumir y evitar el riesgo. En esta misma matriz se definió el responsable de ejecutar y realizar seguimiento

al control, así como los indicadores que se ejecutaran para realizar el seguimiento. Para el caso del proyecto se deben aplicar 34 tratamientos enfocados en el Anexo A del MSPI y se aplicaran 18 indicadores para el seguimiento de estos.

En la Matriz de Declaración de aplicabilidad se plasman los 114 controles del Anexo A, de los cuales se valida que se está cumpliendo con 14 controles, 66 controles a los cuales ya se les había realizado tratamiento; pero a los cuales se les debe realizar uno más tratamientos más para poder cumplir y 34 a los cuales no se le había ejecutado ningún tipo de tratamiento. En la matriz queda especificado el tratamiento propuesto y si se ha implementado alguno a la fecha, así como la evidencia que se generó o se debe generar para el cumplimento de este y por último se plasma el responsable de la ejecución o el que ejecuto esos tratamientos.

En el transcurso del desarrollo del proyecto se implementaron los siguientes tratamientos que hacen que la entidad cumpla con un porcentaje más de la política de gestión digital.

- Diagnostico e informe de la Seguridad y Privacidad de la Información de la entidad.
- Recolección de los activos de Información con su resolución de aprobación.
- Se establece el Comité de Seguridad y Privacidad de la Información con su resolución de aprobación.
- Manual de Roles y Responsabilidades.
- Identificación de Activos de Información actualizado a la fecha con su resolución de aprobación.
- Manual de Política General con sus Dominios y resolución de aprobación.
- Propuesta del nuevo mapa de procesos y organigrama de la entidad.
- Identificación de los procedimientos de Seguridad y Privacidad de la Información y quien debe documentarlos.

- Identificación de los riesgos acorde a los activos de información con Criticidad Alta.
- Análisis de los Riesgos con la criticidad del Riesgo Inherente.
- Valoración de los Riesgo Inherente con la criticidad del Riesgo Residual.
- Tratamiento del Riesgo Residual con el responsable de su ejecución y seguimiento.
- Identificación de los indicadores acorde a los tratamientos propuestos.
- Declaración de Aplicabilidad acorde al Anexo A del MSPI, con el responsable de cada tratamiento.

Como ultima conclusión, se cumple con el ultimo objetivo específico, que es la Declaración de Aplicabilidad y que la E.S.E HUSRT debe analizar y aprobar que controles implementar acorde a los recursos con los que cuenta y un cronograma que genere para su cumplimento.

Por último, el conocimiento que adquirí en la Universidad de Manizales y el poder plasmarlo en la E.S.E HUSRT mediante este proyecto y con el apoyo de mi asesor, me genera satisfacción, ya que cumplí con lo que propuse, pero sobre todo con la experiencia y conocimientos adquiridos sobre lo débiles que podemos llegar a ser, ya sea, una persona, entidad pública o privada si dejamos a la derive la Información, el entender que se puede generar estrategias y aplicar metodologías que mitigan esas debilidades hace que mi inconsciente o consciente siempre este alerta y en función de solucionar y mejorar cada día esas debilidades que puedo llegar a identificar.

25. Referencias bibliográficas

[1] Cámara Colombiana de Informática y Telecomunicaciones, CCIT. “Informe de las Tendencias del Cibercrimen en Colombia 2019 - 2020,” 2019.

[2] Comparitech, "Which countries have the worst (and best) cybersecurity?", Comparitech, 2020. [En Línea]. Disponible: https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/. [Consultado: 12- Mar- 2021].

[3] Sophos, "The State of Cloud Security 2020 Report", Sophos, 2020. [En Línea]. Disponible: https://secure2.sophos.com/en-us/content/state-of-cloud-security.aspx. [Consultado: 12- Mar- 2021].

[4] H. Susanto, M. Almunawar, and Y. Tuan, “Information security management system standards: A comparative study of the big five,” Int. J. Electr. Comput. Sci. IJECS-IJENS, vol. 11, no. 5, pp. 23–29, 2011.

[5] M. A. Tejena-Macías, “Análisis de riesgos en seguridad de la información,” Polo del Conoc., vol. 3, no. 4, pp. 230–244, 2018.

[6] D. Espinosa, J. Martínez, and S. Amador, “Gestión del riesgo en la seguridad de la información con base en la Norma ISO/IEC 27005 de 2011, proponiendo una adaptación de la Metodología OCTAVE-S. Caso de estudio: proceso de inscripciones y admisiones en la división de admisión registro y control AC,” Ing. USBMed, vol. 5, no. 2, pp. 33–43, 2014.

[7] J. C. Benavides Carranza, “Integración de la NTC ISO/IEC 27001:2013 con el Modelo de Seguridad y privacidad de la Información-MSPI del MinTIC,” 2019.

[8] ISO 27000, “Sistema de Gestión de la Seguridad de la Información,” 2012.

[9] “NORMA ISO 27001.” [En Línea]. Disponible: https://normaiso27001.es/.

[10] J. A. Bertolín, Seguridad de la información. Redes, informática y sistemas de información. Editorial Paraninfo, 2008.

[11] ISACA, Manual de Preparación para el Examen CISM 15° edición. 2016.

[12] ISO 27000, “ISO27000.es - El portal de ISO 27001 en español. Gestión de Seguridad de la Información,” 13 de enero de 2018 21:03:23, 2018. .

[13] M. Talabis and J. Martin, Information Security Risk Assessment Toolkit: Practical assessments through data collection and data analysis. Newnes, 2012.

[14] ISOTools Excellence, “La norma,” 2003.

[15] B. Sambana, FUNDAMENTALS OF INFORMATION SECURITY. 2018.

[16] E. R. Lizarzaburu Bolaños, G. Barriga, K. Burneo, and E. Noriega, “Gestión Integral de Riesgos y Antisoborno: Un enfoque operacional desde la perspectiva ISO 31000 e ISO 37001,” Rev. Univ. y Empres., vol. 21, no. 36, pp. 79–118, 2019.

[17] H. Alemán Novoa and C. Rodríguez Barrera, “Metodologías para el análisis de riesgos en los sgsi,” Publicaciones e Investig. Vol. 9 (2015)DO - 10.22490/25394088.1435, Oct. 2015.

[18] D. N. L. Armendáriz, “Modelo de gestión de los servicios de tecnología de información basado en COBIT, ITIL e ISO/IEC 27000,” Rev. Tecnológica-ESPOL, vol. 30, no. 1, 2017.

[19] Departamento Administrativo de la Función Pública, “Guía para la administración del riesgo y el diseño de controles en entidades públicas: Riesgos de Gestión, Corrupción y Seguridad Digital,” pp. 1–93, 2018.

[20] ISO 27000, “ISO27000.es - El portal de ISO 27001 en español. Gestión de Seguridad de la Información,” Consultado: 13 de enero de 2018.

[21] P. Hernandez Sampieri, Roberto, Fernandez Collado, Carlos, Baptista Lucio, Metodología de la Investigación, Sexta. 2014.