UNIVERSIDAD CATÓLICA SANTO TORIBIO DE MOGROVEJO

ESCUELA DE POSGRADO

MODELO BASADO EN LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA CONTRIBUIR EN LOS PROCESOS DE LAS FARMACIAS DE LOS HOSPITALES II-I EN LA REGIÓN AMAZONAS

TESIS PARA OPTAR EL GRADO ACADÉMICO DE

MAESTRO EN INGENIERÍA DE SISTEMAS Y COMPUTACIÓN CON MENCIÓN EN DIRECCIÓN ESTRATÉGICA DE TECNOLOGÍAS DE INFORMACIÓN

AUTOR
JAIME IZQUIERDO CABRERA

ASESOR
GREGORIO MANUEL LEÓN TENORIO
https://orcid.org/0000-0002-9650-4427

Chiclayo, 2021

MODELO BASADO EN LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA CONTRIBUIR EN LOS PROCESOS DE LAS FARMACIAS DE LOS HOSPITALES II-I EN LA REGIÓN AMAZONAS

PRESENTADA POR:

JAIME IZQUIERDO CABRERA

A la Escuela de Posgrado de la

Universidad Católica Santo Toribio de Mogrovejo

para optar el grado académico de

MAESTRO EN INGENIERÍA DE SISTEMAS Y COMPUTACIÓN CON MENCIÓN EN DIRECCIÓN ESTRATÉGICA DE TECNOLOGÍAS DE INFORMACIÓN

APROBADA POR:

María Ysabel Aranguri García

PRESIDENTE

Ricardo David Imán Espinoza

SECRETARIO

Gregorio Manuel León Tenorio

VOCAL

DEDICATORIA

A la memoria de mi mamá Santos, porque verme reflejado en sus ojos el día de la graduación era la verdadera razón de continuar superándome.

A mis padres Jaime y Luisa, que me brindaron su amor, consejos, valores y enseñanzas de vida, forjando la persona que ahora soy.

ÍNDICE

LISTA DE TABLAS

RESUMEN

En esta investigación se realizó la armonización de estándares en gestión de la seguridad de la información con el propósito de elaborar un modelo adecuado a los procesos de las farmacias de los hospitales II-I en la región Amazonas. El presente modelo consta de 4 fases, 14 procesos, 6 subprocesos 15 plantillas y una herramienta de monitoreo, así mismo fue validado por expertos en el tema para evaluar su funcionalidad en base a indicadores obteniendo un 91%, los cuales fueron de gran importancia para la aplicación, implementando dicho modelo a escala real en un hospital de la muestra en la cual, se evaluó antes de la aplicación para así conocer la realidad problemática y contar con un panorama general sobre el desarrollo de procesos en los mismos. Al comparar los resultados obtenidos luego de aplicar el modelo se observa una mejora en la seguridad de la información para sus activos más relevantes, así mismo se desarrolla un plan de mejora continua para mantener y superar el estado actual de implementación de controles.

Palabras clave: ciberamenaza, sistema de gestión de seguridad de la información, activos, estándar, gestión de riesgos, controles de seguridad, procesos.

ABSTRACT

In this research, the harmonization of standards in information security management was carried out in order to develop an adequate model for the processes of the pharmacies of the II-1 hospitals in the Amazon region. This model consists of 4 phases, 14 processes, 6 sub-processes, 15 templates and a monitoring tool, it was also validated by experts on the subject to evaluate its function based on indicators, obtaining 91%, which were of great importance for the application, implementing said model on a full scale in a hospital in the sample in which it was evaluated before the application in order to know the problematic reality and have a general overview of the development of processes in them. When comparing the results obtained after applying the model, an improvement in information security is observed for its most relevant, likewise a continuous improvement plan is developed to maintain and exceed the current state of control implementation.

Keywords: cyber threat, information security management system, assets, standard, risk management, security controls, processes.

INTRODUCCIÓN

La presente investigación tiene como propósito ofrecer una alternativa de solución para los hospitales II-I, en la región Amazonas, los cuales a través de los años, ha generado un alto volumen de información que tratada adecuadamente se ha convertido en conocimiento y este conocimiento en una fuerza productiva directa, en la actualidad en [1] refiere "…para cualquier entidad es fundamental contar con información suficiente y necesaria para apoyo en la toma de decisiones" es por ello que la mayoría de las organizaciones consideran como principal activo la información.

Con el crecimiento masivo en la información digital, se enfrentan al desafío de proteger sus activos de información (por ejemplo, documentos tradicionales, correo, mensajes de texto, audio, video, etc.) dentro de un entorno complejo y cambiante de diversos sistemas o tecnologías. Esto hace necesario establecer estrategias desde el enfoque de la seguridad de la información.

Un Informe de Ciberamenazas y Tendencias 2019 realizado por el Centro Criptológico Nacional de España (CCN-CERT) da a conocer los principales sucesos de seguridad en el 2018, como el ataque entidades públicas en España donde en noviembre del 2018 instalaron y ejecutaron código dañino en los sistemas operativos de dichas entidades. Además de ello concluyen que uno de los enfoques de tendencia para el 2019 es el ciberataque a las personas, pues "los seres humanos siguen siendo el eslabón menos fuerte en todos los sistemas de seguridad de la Información" [1]. Dicho informe estima un impacto en España de 40 millones de euros al año, cifra posiblemente bajo la realidad si se tiene en cuenta que no todas las organizaciones revelan por evitar perjudicar la imagen de su marca.

Estos últimos años, los ataques contra estos datos fueron incrementando y con ello la posibilidad de compromiso de la información: disponibilidad en un 7.5%, integridad en un 10.7% y confidencialidad en un 80.5% siendo el resultado más común a los ataques, este hecho se evidencia en ataques dirigidos (APT) en vínculo con las acciones de ciberespionaje según 2020 Data Breach Investigations Report [2].

Estos no son incidentes aislados de un continente o país, informes como Eset Security Report Latinoamérica 2019 [3] reportan que el 61% de las organizaciones en

Latinoamérica ha sufrido, al menos un suceso de seguridad en el 2019, el crecimiento respecto al año anterior ha sido de un 7%, países como México reportan un 72% de incidentes de seguridad en empresas, esta información nos hace pensar en las acciones que deben tomarse para gestionar los riesgos de seguridad. ESET menciona lo importante abordar la seguridad de la información desde un enfoque por capas, las cuales no deben estar basadas exclusivamente en el uso de tecnologías, contar con políticas y planes para gestionarlo. Pero la realidad es distinta puesto que solo el 28% de las empresas en la región latinoamericana clasifica su información (física y digital).

Si bien los hospitales, así como instituciones o empresas vinculadas al sector salud desde hace algún tiempo destacan por ser uno de los principales blancos de ataques informáticos [3] al contexto de la lucha contra la pandemia COVID-19 en el año 2020, un ataque podría tener consecuencias aún más severas, en abril del 2020 la Organización Internacional de Policía Criminal (INTERPOL) [4] emitió un comunicado alertando que hospitales y otras instituciones dedicadas a la lucha contra el nuevo coronavirus están siendo blanco de ataque de cibercriminales, detectando un crecimiento significativo en el número de intento de ataques a este tipo de entidades, por lo que recomiendan el uso de una solución de seguridad de la información integral que abarque a totalidad los recursos en entidades. Por su parte El Buró Federal de Investigaciones en Estados Unidos (FBI) [5] alertó sobre los ataques dirigidos a los proveedores de servicios de salud en aquel país, así mismo la principal agencia de ciberseguridad de República Checa, [6] publicó una advertencia dando a conocer su preocupación ante algún posible ataque a gran escala en hospitales e instituciones del sector salud.

Estos incidentes llega a ser realmente preocupantes cuando se habla de datos sensibles como historias médicas; En el 2018 Bob Diachenko [7], “un experto de ciberseguridad halló una base de datos MongoDB” con acceso abierto desde internet la cual mantenía información médica de aproximadamente 2 millones de personas en México propiedad de la compañía Hova Health, una empresa de tecnología internacional que trabaja con el sector de la salud además de datos pertenecientes en el Sistema de Registro de Salud..

Nuestro país no es la excepción puesto que solo en el 2017 la actividad de amenazas marcó un máximo histórico, en aquel año un tercio de los incidentes de seguridad en Latinoamérica ocurrían en nuestro país (25%), para el 2019 el 71% de las empresas

manifestaba a menos un suceso de seguridad, de alguna manera la adopción de seguridad de estos datos no fue optima, se evidencia que ocupamos el penúltimo lugar en gestión de seguridad, puesto que solo 42% de las organizaciones afirman poseer algún Sistema de Gestión de Seguridad de la Información (SGSI) justo debajo, Ecuador (35%). Todo ello suma la implementación y desarrollo de controles en seguridad al sector salud (13.6%) ocupa el último lugar seguido del sector gobierno (14%) [3].

En la región Amazonas, los casos frecuentes en relación a seguridad de la información se encuentran relacionados a la gestión de información clínica en instituciones del estado (redes de salud y hospitales).

Por lo que nos planteamos la siguiente interrogante que indica ¿De qué manera se puede contribuir en la seguridad de la información en los procesos de las farmacias de los hospitales II-I en la región Amazonas?, lo cual nos permite proponer que, con la implementación del modelo de gestión de seguridad de la información, se contribuye en los procesos de las farmacias de los hospitales II-I en la región Amazonas.

Para alcanzar el propósito antes manifestado, se formuló desarrollar un modelo de gestión de seguridad de la información para contribuir en los procesos de las farmacias de los hospitales II-I en la región Amazonas, que es evidencia en el cumplimiento de los siguientes objetivos:

- Armonizar los estándares de gestión de seguridad de la información en base a criterios que se pueda adaptar al contexto de los procesos de farmacia y contribuir su gestión de los hospitales II-I en la región Amazonas.
- Elaborar el modelo SGSI para mejorar los procesos en farmacias de los hospitales de la región Amazonas.
- Validar la funcionalidad del modelo de SGSI en base a indicadores.
- Aplicar el modelo SGSI.

A través de esta investigación se pretende hacer uso de estándares, normativas y marcos de trabajo orientadas a la seguridad de la información adaptadas a realidades del rubro de las entidades, país y región con el objetivo de contribuir en la entidad orientada al nivel de seguridad de información. Por lo antes expuesto, se propuso que los resultados de esta

investigación sirvan de apoyo a posteriores investigaciones relacionados a seguridad de la información aplicado en hospitales de la región Amazonas. Para que desde la perspectiva económica genere una significativa reducción de costos para la gestión de procedimientos, en los hospitales proporcionando óptimos servicios y procesos en materia de manejo de la información digital y/o física, así como disminución de riesgos. Como consecuencia se proporcionó a los hospitales de la región Amazonas un nivel superior en seguridad de su información, protegiendo la integridad, disponibilidad y confidencialidad de los mismos a lo largo de todos los procesos que realiza, otorgando a los funcionarios un apoyo en la toma de decisiones y la población que utiliza los servicios de salud.

CAPÍTULO I MARCO TEÓRICO CONCEPTUAL

1.1 Antecedentes

En los últimos años, investigaciones realizadas en este campo han mostrado un panorama científico en donde se desarrollaron importantes avances. Es así que se presentan investigaciones que fueron relevantes para esta investigación, pues el aporte ha sido de valor importante.

Gonzales [8], en el 2019 comparó las normas internacionales ISO 27001:2013, COBITv5, NIST 800 53v4 y ISO 27002:2011 todas ellas con el fin de desarrollar un SGSI adecuado al sector económico, mediante del ciclo planear, hacer, verificar y actuar (PHVA) logra estructurar la comparación y adoptar un modelo para facilitar la implementación, abarcando gobierno, seguridad, identificación de activos, análisis, plan de tratamiento de riesgos y mejora continua. El análisis de los resultados obtenidos en la implementación de la metodología determinaron las ventajas de adaptar un modelo al entorno a desarrollar, y ventajas como la facilidad en la adopción de la seguridad en sus activos de información, reducción de costos relacionados a implementación de SGSI, proporcionó mecanismos para generar una cultura en temas de seguridad para la información interna en la organización, permitió ser proactivo ante la resolución de incidentes en relación a seguridad de la información. La importancia radica en la determinación de características a evaluar para determinar el grado de cumplimiento del presente modelo, el uso de diferentes estándares puede dificultar la identificación de metas, algo que Gonzales logra evitar con el uso del ciclo PHVA.

En el 2020, Ruíz et al. [9] ante el gran flujo de información que generan las instituciones educativas, la falta de uso y manejo de estos datos. Presentaron vulnerabilidades y amenazas por lo que elaboraron un modelo de seguridad de la información donde determinaron, que el conjunto de controles y procedimientos de seguridad elaborados no tienen validez en todas las organizaciones del mismo sector, adaptando así dichos controles a cada uno de las instituciones para lograr un enfoque en la gestión de riesgos de acuerdo al alcance del modelo planificado. Además, resalta la importancia de contar con un comité de seguridad de la información para ser el ente regulador en cualquier modificación interna en el sistema de gestión y responsable de la toma de decisiones en temas de seguridad. De igual manera, es necesaria la designación de un responsable de la

Seguridad de la Información, donde su función sea velar por la ejecución de las Políticas de Seguridad y notificar al Comité sobre el estado y progresos actuales del Sistema de Gestión de Seguridad tras su implementación. Este antecedente proporcionó a la presente investigación el panorama para determinar los controles y procedimientos de seguridad necesarios en la implementación del modelo, de igual forma los plazos para cada proceso que se plantea puesto que dicha implementación no es un proceso a corto plazo y el tiempo está supeditado a múltiples factores en relación a la naturaleza de sus funciones, tamaño de la empresa, recursos institucionales que se designados, estado actual relacionado a seguridad de la información, entre otros.

En el 2020, Mora et al. [10] señalaron que las organizaciones requieren un diseño de metodología que permita la identificación del estado actual en materia de seguridad informática y desarrollar procesos con el fin de implementar un SGSI alineado, es por ello que determinó características alineadas a seguridad de la información necesarias para clasificar y valorar los activos en una organización, en base a la criticidad de los activos relaciona los parámetros económicos, legal y prestigio segregado en 3 clasificaciones: confidencialidad, integridad y disponibilidad. Este modelo promedia los valores y determina la criticidad en un rango de 4 pasos (muy bajo, bajo, medio y alto) implementando un modelo practico. Así mismo desarrolla un plan de capacitación, pilar fundamental en la concientización de los colaboradores de la organización a fin de generar una cultura de seguridad de la información en donde aborda aspectos como: políticas externas, ley de protección y tratamiento de datos. El antecedente proporcionó a la presente investigación la perspectiva de un modelo de clasificación y valoración de activos tomando en consideración los pilares de seguridad de la información según ISO 27000 así mismo aportó posibles soluciones en la elaboración de un modelo para capacitaciones con enfoque a seguridad de la información.

En el 2020, Elham et al. [11] establecen que las políticas de seguridad son uno de los controles formales más importantes cuando las organizaciones trabajan para implementar un SGSI sin embargo los diseños de estas son una tarea desafiante y no se cuenta con perfiles para aliviar la carga, así mismo detectaron que los sistemas de información se vienen convirtiendo en un aspecto cada vez más integral de las organizaciones, razón por la cual mantienen una variedad de información, desde datos de productos hasta información de clientes, que a menudo posee contenido sensible que puede ser dañado,

alterado o divulgado causando pérdidas financieras, efectos negativos en la reputación y pérdida de confianza, es así como los controles de política en temas de seguridad de la información desarrollados contribuyen en la identificación de 14 temas en requisitos de alto nivel esquematizando detalles en cada uno de ellos y aplicándolo para obtener una amplia perspectiva en el éxito de cada requisito. La relevancia de este antecedente radica en ser referencia a un punto de partida para diseñar políticas de seguridad en la información adoptando una solución centrada a los objetivos de la institución, así mismo, al ser un proceso iterativo significa que tales esfuerzos desarrollados se utilizan para mejorar y refinar temas de requisitos, así como comentarios de la alta dirección y personal de la institución.

En el 2020, Safonova y Kotelnikov [12] desarrollaron un SGSI basados en la norma ISO/IEC 27000 permitiendo a instituciones médicas reunir los procesos en temas de gestión en la seguridad de la información considerando un enfoque sistemático, así mismo determinan que los sistemas de sanidad no están siendo soportados por nuevas tecnologías que brinden seguridad de la información , es por ello que el problema más urgente de la industria de la medicina es la protección de los datos, es decir, la creación de un SGSI, la cual plantean y desarrollan en base al ciclo PHVA, modelo de acuerdo a los requisitos de ISO 27001 donde estandarizan el flujo de trabajo para una mejor toma de decisión, así mismo el SGSI fue desarrollado en 6 fases incluyendo la preparación para el proceso de certificación mediante una auditoria preliminar, permitiendo a la organización alcanzar un nuevo nivel de funcionamiento, así como incrementar sus ventajas competitivas, logrando además un resultado importante como la optimización de costos, reducción de riesgos relacionado con posibles daños a activos de la empresa y asegurando el cumplimiento del nivel de seguridad de la información con los objetivos en las instituciones médicas y por último, la reducción significativa en el número de incidentes y el tiempo de respuesta a un incidente (por ejemplo, un ataque de virus). Este trabajo proporcionó a la presente investigación una guía de cómo implementar una correcta gestión de seguridad en la información, por medio del desarrollo del modelo propuesto, desde la toma de decisión y preparación de la organización para la implementación del SGSI la cual abarca la identificación de los actores, uso de estándares y su metodología, identificación de área o proceso a implementar y plan de mejora continua, hasta llegar al

proceso de certificación en donde se abala internacionalmente la implementación de controles para una gestión de seguridad en la información correcta.

En el 2019, Jara [13] a través de un framework implementó controles de seguridad en los procesos de una institución, es así como el framework basado en los controles de ISO/IEC 27000 analizó el entorno interno y externo de la entidad y reveló las fortalezas y debilidades en la seguridad de la información donde, posteriormente evaluó una implementación gradual y progresiva (por ciclos) siguiendo el contexto de la institución brindando flexibilidad, evitando así atañar a la alta dirección con requerimientos complejos ya que se carece de políticas en materia de seguridad en la información, controles o procedimientos para el manejo correcto de datos, por lo tanto existe la posibilidad de producir acciones ilícitas o incidentes como por ejemplo: violación de la privacidad , alteración de datos o interrupción de servicios que comprometan la disponibilidad, integridad y confiabilidad de la información almacenada en los sistemas de información. por medio de la implementación del framework, logró en su primera ejecución elevar a 72% el nivel de cumplimiento del dominio 16 relacionado a incidentes en la seguridad. Este antecedente contribuyó un gran aporte a esta investigación ya que logró adaptar el modelo a la institución, haciéndola flexible de implementar analizando el entorno bajo entandares internacionales mediante análisis FODA y las estrategias en cada uno de ellas, siendo de gran ayuda a la presente investigación porque demostró cómo se logró dicho análisis respectivo.

En el 2020, Bornas [14] determinó que el compromiso de la gerencia es de importancia en el proceso de implementación de un SGSI en la entidad, puesto que debe estar en constante comunicación con el gestor del proyecto para realizar coordinaciones a todo nivel, esto luego de desarrollar un modelo de SGSI adaptado al entorno de la entidad, basado en estándares como ISO 27001 conteniendo buenas prácticas, requisitos y controles, ITIL v3 como mejores prácticas para estandarizar procedimientos operativos y COBIT como framework de gobierno y control alcanzando, luego del desarrollo la validación del modelo en un proceso por medio de la implementación y proponiendo un documento de aplicabilidad SoA como documento final. La importancia de esta investigación radica en los criterios para armonización de 3 estándares, la base del modelo lleva como previo paso en análisis del sector la cual mediante procedimientos de

recolección de datos obtiene un panorama general, estas técnicas mencionadas llegan a ser un referente importante a la investigación desarrollada.

Por último, se identificó esta investigación. Tal es el caso que, en el 2020, Niño [15] en el diagnóstico de la situación actual organizacional halló debilidades en la seguridad de la información de procesos, controles, inexistencia documentación respecto al tema, ausencia de herramientas, estándares y otros. Mostrando en evidencia que las áreas de alta gerencia trabajan por separado. Para brindar una solución, Niño se basó en la definición y evaluación del proceso para el análisis, e implementó los planes de tratamiento con el respectivo seguimiento y monitoreo los activos de información usando como base la ISO/IEC 27001 e ITIL v3 logrando unificar en un proceso adaptable no solo para las áreas de alta dirección, sino también para otras áreas y empresas del mismo o diferente rubro. Este antecedente proporcionó a la presente investigación la perspectiva de un estándar global en seguridad de la información por el cual se define el contexto, que es un proceso indispensable porque se analizan los objetivos, los stakeholders, el entorno externo e interno y una gama de criterios que posibilitan el conocimiento de la complejidad así como el origen de los riesgos, además de elaborar los procesos de comunicación y consulta, la valoración del riesgo, el monitoreo y revisión, asimismo aportó posibles soluciones para asegurar de manera efectiva la mitigación de riesgos en seguridad de la información sin que los objetivos de la organización se vean afectados de manera alguna.

1.2 Definición de Modelo de Gestión

Luego de analizar la definición para MSPI [16], se define el término como un conjunto de actividades analizadas y recolectadas de metodologías y estándares reconocidos mundialmente adaptada al requerimiento de las organizaciones, con la finalidad de contribuir a los procesos y desarrollo.

1.3 Definición de Seguridad de la Información

Posterior al análisis de ISO/IEC 27000 [17] y COBIT 2019 [18] se concluye entonces, que seguridad de la información es la protección de la información que las organizaciones como los hospitales optan frente a amenazas de toda índole.

1.3.1 Definición de Información

Con respecto a las definiciones previas de ISO 27000 [17] y COBIT 5 [19], se infiere que la información es un conjunto de conocimientos que tiene relevancia para la organización la cual puede verse reflejado en bienes tangibles e intangibles, tal es el caso que las organizaciones como los hospitales cuentan con información almacenada en recetas médicas, historia clínica, análisis clínicos, reportes contables y presupuestales, así como contratos con proveedores, entre otros.

1.4 Definición de Hospitales

Luego de analizar la postura del Ministerio de Salud (MINSA) [20] concluimos, que un hospital es un establecimiento que brinda a atención de pacientes que padecen alguna enfermedad.

1.4.1 Clasificación de Hospitales

Para el Minsa [21], existen los siguientes niveles y categorías de Atención:

- Primer nivel de atención: Puestos y centros de salud
- Segundo nivel de atención: Hospitales y clínicas.
- Tercer nivel de atención: Hospitales de complejidad e institutos especializados.

1.4.2 Características de Hospitales II-I

Para el MINSA [21] los hospitales de nivel II-1 son: “Establecimientos de Salud que brinda una atención integral ambulatoria y hospitalaria en cuatro especialidades básicas: pediatría, ginecología, cirugía general y medicina interna; con actividades de promoción de salud, prevención de riesgos y daños, recuperación y rehabilitación”.

1.4.3 **Características de Farmacias en Hospitales II-I**

El MINSA [22], define una Farmacia de Nivel II-1 como una unidad básica organizada para dispensación, expendio, gestión de programación y almacenamiento especializado de producto farmacéutico, dispositivo médico y producto sanitario acuerdo a la complejidad del hospital.

La presente investigación está enfocada en hospitales de tipo II-I puesto que la región Amazonas cuenta un gran número de hospitales de esta categoría además las farmacias implementadas en estos establecimientos cuentan con autonomía presupuestal y mayor complejidad en los procesos habituales.

1.5 Estándares y Marcos de Trabajo para Gestión de Seguridad de la Información

1.5.1 Cobit 2019

"COBIT es un marco de gobierno y gestión de las tecnologías de la información" en una entidad, orientado a todo tipo de organización. Engloba la tecnología y procesamiento de información como un todo que la entidad "utiliza para el logro de sus objetivos, independientemente del lugar dentro de la entidad". En otras palabras, la información y tecnología de la entidad no se limita al área de TI de una empresa, aunque obviamente lo incluye [18].

COBIT 2019 integra a la información como un componente del sistema de gobierno, asegurando la integridad y disponibilidad de la información en la entidad, así como el nivel de capacidad que se encuentra la seguridad de la información con respecto al modelo CMMI.

1.5.2 Magerit

Es una metodología de gestión y análisis de riesgos en sistemas de información (MAGERIT), se encuentra directamente relacionada con el uso de

las tecnologías de la información, lo que beneficia a los usuarios y minimiza los riesgos mediante mecanismos de seguridad con la finalidad de generar confianza.

De interés para todos aquellos que trabajan con datos digitales y sistemas informáticos, la metodología permite conocer el riesgo a la que está sometido y ayudar a proteger; Permite la aproximación metodológica y evita improvisaciones y arbitrariedad del analista.

Los principales objetivos son:

- Concientización a los responsables y actores de los sistemas de información sobre los "riesgos y necesidad de tratamiento a tiempo".
- "Ofrecer un método sistemático para análisis de riesgos."
- Apoya en la identificación y "planeamiento de medidas" oportunas para conservar estos riesgos bajo control.
- Prepara a la entidad para evaluaciones, certificaciones, acreditaciones o auditorías. [23]

1.5.3 Iso 27000

Norma internacional, desarrollada por la Organización Internacional de Normalización (ISO), detalla cómo realizar una gestión de seguridad de la información en entidades, una versión actual de esta norma es la ISO/IEC 27001:2013.

Esta norma está pensada para ser implementada en cualquier entidad u organización, de indistinta finalidad, tamaño o estructura. También permite que la certificación de una entidad; lo que significa que garantiza y confirma que dicha entidad ha implementado un SGSI cumpliendo la norma ISO 27001.

Esta norma es una de las principales referencias a nivel mundial para seguridad de la información y por la que entidades de todo el mundo implementan esta normativa.

La norma consta de 11 secciones además del anexo A; las primeras 4 secciones opcionales al momento de implementar, mientras que las secciones restantes son obligatorias, por lo que la entidad debe implementar todos los requerimientos si desea cumplir con la norma y posteriormente certificarse. Los controles adjuntos al Anexo A pueden implementarse sólo si determina que corresponden en la Declaración de aplicabilidad. [17]

1.5.4 Itil

Es un estándar a nivel mundial, alinea la ISO 20000 y estándares como COBIT para la administración de servicios; además, contiene una amplia documentación profesional sobre la planificación, entrega y soporte a las características de los servicios de TI.

El proceso de implementación de gestión de la seguridad de la información, se encuentra dentro de la fase de Diseño del Servicio y es la encargada de “asegurar que la disponibilidad, integridad y confidencialidad de la información” al igual todas las modificaciones sean correctamente procesados. [16]

CAPÍTULO II MATERIALES Y MÉTODOS

2.1 Diseño de investigación:

Para cumplir con los objetivos de la investigación, se identificó como diseño el tipo pre test – post test; esto permite comprobar el planteamiento de la hipótesis. Para ello se midió la variable dependiente a utilizar, luego se realizó una nueva medición de esta variable, después de la ejecución de un modelo propuesto de seguridad de la Información sobre los procesos de los hospitales (post test) con la finalidad de evaluar el efecto.

G=O1 X O2

Donde:

G= Caso de estudio seleccionado

O1: Contribuir en la seguridad de la Información de los procesos de farmacia de los Hospitales II-I de la región Amazonas, antes de la aplicación del modelo de seguridad de la información.

X: Modelo de gestión de seguridad de la información basada en estándares, normas, marcos de trabajo y metodologías.

O2: Contribuir en la seguridad de la Información de los procesos de farmacia de los Hospitales II-I de la región Amazonas, después de aplicar el modelo de seguridad de la información.

2.2 Población, muestra y muestreo

La población para esta investigación, fueron funcionarios que laboran en las áreas de farmacia de los hospitales públicos de categoría II-I dentro de la región Amazonas.

Hospitales II-I dentro de la región Amazonas = 7

Funcionarios que laboran en las áreas de farmacia de cada hospital = 20

Tamaño de población = 140

El tamaño de la muestra fue obtenido luego de aplicar la siguiente formula:

$$x = \frac{Z^2 * \mathrm{P} * \mathrm{Q} * \mathrm{N}}{(\mathrm{N} - 1) * e^2 + (Z^2 * P * Q)}$$

Donde:

N = 140 Población

e = 0.08 (margen de error)

Z = 1.90 (Nivel de confianza)

P = 0.5 (probabilidad de éxito)

Q = 0.5 (probabilidad de fracaso)

El presente estudio consideró una muestra de 41 funcionarios.

Se utilizó la técnica de muestreo por conveniencia, seleccionando 3 hospitales de la región Amazonas. El criterio de selección son los hospitales que geográficamente se encuentren en una provincia diferente, ya que entre provincia existe un aproximado de 5 horas de viaje, además las regiones del norte cuentan con una idiosincrasia diferente puesto que existe un involucramiento por parte de las comunidades nativas existentes.

2.3 Técnicas e instrumentos de recolección de datos

La técnica que se utilizó fue la entrevista y el análisis documental.

Entrevista: establecer contacto con la muestra a ser evaluada, la encuesta que se utilizó fue la encuesta personal donde existió una interrelación entre el entrevistador y el entrevistado.

Análisis documental: se obtuvo datos de bibliografía y estándares en relación a seguridad de la información, proceso de farmacia en los hospitales y funciones de personal en el proceso de farmacia; sumado a ello se revisó los documentos de gestión institucional:

- Planeamiento Estratégico Institucional.
- Plan Operativo Institucional.
- Plan Operativo Informático.

- Misión, visión objetivos estratégicos y organigrama
- Cuadro de Asignación de Personal
- Reglamento de Organización de Funciones.
- Sistemas de información y proceso para la toma de decisiones.

El instrumento utilizado fue el cuestionario.

Cuestionario: conjunto de preguntas especialmente elaboradas y diseñadas para ser respondidas por una muestra de población cuya finalidad es la obtención y registro de datos.

Se aplicó una encuesta a los actores del proceso de farmacia, persona a cargo de los servicios de TI y personal jerárquico de las 4 instituciones a investigar, además se analizó los documentos de gestión institucional, a fin de diagnosticar el proceso de gestión de la seguridad de la información en las 4 instituciones.

Con la información recolectada y el diagnostico efectuado, se analizó y procesó mediante el uso de hojas de cálculo, luego se procedió con diseño y desarrollo del modelo propuesto de gestión de seguridad de la información, todo ello alineado al proceso de farmacia de los hospitales investigados.

Por último, se aplicó el modelo propuesto a una institución y se volvió a realizar la misma encuesta con la finalidad de verificar su contribución a la seguridad de la información de los procesos en las farmacias de los hospitales.

Amazonas es una de las regiones más biodiversas del Perú contando con selvas frondosas donde conviven comunidades nativas, zonas cálidas y sierra en donde se ubica la capital de la región, lo que conlleva a poseer una región multicultural. Es por ello que las entidades pertenecientes a la investigación se ubican territorialmente en 4 de las 6 provincias para abarcar culturase idiosincrasias diferentes y así obtener un diagnóstico más acorde a la región. Para más detalles de las entidades se elaboró el siguiente cuadro Informativo**.**

Tabla 1: Cuadro de información y características de hospitales

	INSTITUCIÓN 01	INSTITUCIÓN 02	INSTITUCIÓN 03	INSTITUCIÓN 04
RUBRO	Salud	Salud	Salud	Salud
CATEGORÍA	II-1	II-1	II-1	II-1
PROVINCIA	Bagua	Condorcanqui	Utcubamba	Rodríguez de Mendoza
MISIÓN	Somos un Hospital II – I, que brinda unidades que producen servicios de salud médico quirúrgico de mediana complicación basada en las personas, familia – comunidad, desarrollando un nuevo modelo de gestión hospitalaria y atenciones integrales especializadas, preventivo, promocionales, recuperativas, rehabilitación, prescripción farmacológica con énfasis en materno infantil, con una mezcla de gran humildad, mucha voluntad, alto sentido humanístico y valores éticos	Brindamos atención de salud integral, con buen trato y comprometidos con la imparcialidad e interculturalidad, tramitado y optimizando los recursos necesarios, integrando funciones con la entrada y articulado con los establecimientos de la Red de Salud.	Es una Institución del Ministerio de Salud cuyos trabajadores identificados con ella, laboran en grupo brindando una esperanza preventiva, promocional, recuperativa y de rehabilitación de la población, con profesionalismo, calaña, calidez e imparcialidad, comprometidos con la Construcción de un flamante Hospital y permanecer siendo la Institución de mayor repercusión Resolutiva de la Región	El hospital busca mejorar la calidad y calidez de atención a la persona, con compromiso social mística y respeto intercultural
VISIÓN	cubrir las expectativas de los pacientes por medio de la atención sanitaria cálida y personalizada, apoyados por los buenos ambientes de los servicios, la tecnología actualizada y el mejor trato por parte del personal	Al año 2019 aspiramos a ser un Hospital II-2, facultado para obligarse una ilusión de lozanía universal, enormemente especializada y preocupada con población de Condorcanqui con pleno compostura	En el año 2023 el Hospital estará constituido como un Hospital Acreditado en la altura III-1 del MINSA, respetado el de mayor gravedad Resolutiva de la Región. Contando con un independiente	El hospital busca convertirse en una institución especializada con autonomía financiera, innovadora en la región que brinde atención oportuna y eficiente para

	de salud, reforzando el nivel del nosocomio de complejidad mediana y del sistema de referencias y contra referencias en todas las regiones	a los tributos de sus usuarios, gestionado y optimizando los medios necesarios, con liderazgo social académico.	capacitado y registro. Que realiza funciones de encumbramiento, inmunización, recuperación y rehabilitación de enfermedades transmisibles y no transmisibles.	disminuir el gasto social
CUENTA ON ÁREA DE TI	SI	SI	SI	SI
NRO. ABAJADORES EN TI	2	1	1	1

Fuente: Elaboración propia

2.4 Técnicas de procesamiento de datos

La encuesta aplicada a los funcionarios de los hospitales II-I de la Región Amazonas fueron ingresados y procesados en una hoja de cálculo, los resultados fueron analizados e interpretados mediante gráficos estadísticos con la finalidad de diagnosticar el estado actual de la muestra respecto a la gestión de seguridad en la información.

Los resultados de la encuesta y modelo validado por los expertos fueron registrados y procesados en el programa estadístico informático SPSS con el fin de analizar la confiabilidad de la encuesta a través del Alfa de Cronbach y la validez por medio de V de Aiken, así mismo se determinó la validez del modelo propuesto mediante la concordancia a través V de Aiken.

2.5 Normas Éticas

Durante el desarrollo de la presente investigación se consideró de forma rigurosa acatar los fundamentos de ética que respalden particularidad. Así mismo, se mantuvo la consideración del caso respecto a los derechos de autor con los documentos consultados y las páginas electrónicas revisadas; igualmente la información obtenida por parte de los encuestados fue mediante el consentimiento informado, por tal motivo la información y datos presentados en el presente trabajo de investigación no son ficticios; por último, para mantener el anonimato de las instituciones y entrevistados, la investigación no presenta sus nombres.

CAPÍTULO III RESULTADOS Y DISCUSIÓN

Previo al desarrollo de esta sección se desarrolló un cuestionario de diagnóstico situacional la cual fue presentado a los responsables del área de TI de los hospitales seleccionados en la muestra.

Dicho cuestionario fue elaborado siguiendo los dominios relacionados a seguridad de la información de COBIT 2019 Framework Governance and Management Objetives, relacionando también las prácticas de gobierno y actividades de la cual se extrajo un conjunto de 10 preguntas referidas directamente a seguridad de la información para posteriormente validarlo con 03 expertos. El esquema del cuestionario en mención se encuentra en el ANEXO 01.

La aplicación de este cuestionario nos mostró los siguientes resultados:

Con respecto a definición de **naturaleza de la organización** se analiza que el 75% de las organizaciones no disponen de un plan estratégico institucional y el 25% que lo presenta en una versión desfasada de esta. Así mismo el 50% de las organizaciones no cuenta con un manual de organización y funciones o documento que haga las veces de ello, lo que demuestra que las funciones determinadas por la organización no tienen sustento documental por lo que no se encamina a un objetivo institucional. Para más detalle: el 100% de las organizaciones no cuenta con un plan estratégico en el área de Tecnologías de la Información puesto que estas áreas solo son percibidas como soporte tecnológico a las actividades que desarrolla la organización.

En cuanto al **establecimiento de gestión de la seguridad de la información (SGSI),** el 100% de las organizaciones no cuenta con una política para sí mismo, por lo que las pocas actividades para mejor la seguridad de la información en las organizaciones son realizadas de manera empírica, sin medir los resultados y sin documentar. Así mismo el 100% de las organizaciones no brinda capacitaciones a sus funcionarios sobre seguridad de la información por lo que estos funcionarios no tienen noción de las amenazas que existen y pueden realizar por desconocimiento poniendo en riesgo los activos de información de la entidad, el poco énfasis a estos temas, denota la pobre barrera de seguridad que cuentan todas las organizaciones de este sector en la región.

En relación a la **gestión de riesgos**, el 100% de las organizaciones no cuenta con una política en gestión de riesgos de Tecnologías de la Información, por lo que no identifican, ni monitorean los riesgos presentados. Asimismo, el 100% de las entidades manifiestan que no cuentan con una directiva de inventario de TI y activos de información por lo que no tienen control de los activos e imposibilita el análisis de información para el desarrollo de una gestión a estos. Además, el 75% menciona contar con una implementación parcial de un plan de copias de seguridad la cual abarca algunos sistemas informáticos con los que cuenta.

Para detalles sobre las respuestas a esta encuesta y los gráficos obtenidos consulte el **ANEXO 02** y **03.**

El proceso para validar la herramienta de diagnóstico fue mediante la aprobación de 3 expertos del tema, posteriormente estos datos son analizados mediante el coeficiente de concordancia adoptado por la prueba w de Kendall para establecer la medida de acuerdo entre los expertos.

Para determinar la concordancia entre los expertos, se presentaron 2 hipótesis:

H_0: No hay concordancia entre los expertos.

H_1: Existe una concordancia entre los expertos.

Se analizó si el valor de α sobrepasa el nivel crítico de 0.05 H_0 es rechazado. A través del programa estadístico informático SPSS se obtuvo el siguiente nivel de significancia:

Tabla 2: Resultados de W de Kendall para herramienta de diagnóstico.

	ENCUESTA
N	**3**
W de Kendall (α)	**0.333**
Chi-Cuadrado	**39**
Grado de libertad (gl)	**39**
Valor de significancia (p)	**0.47**

Fuente: SPSS

Luego de obtener los resultados proporcionados por los expertos, la hipótesis H_1 es aceptada; en conclusión, existe una coincidencia relevante entre las respuestas de los expertos para validar la encuesta desarrollada ($p < 0.05$).

De acuerdo a los resultados obtenidos por el SPSS según la tabla 18 se concluye:

- La hipótesis H_0 es rechazada.
- Existe una concordancia entre los expertos.
- La herramienta de diagnóstico cuenta con un nivel aceptable de α denotando relación en las respuestas de los 3 expertos.

De igual manera la encuesta reúne características de confiabilidad la cual se obtuvo aplicando la herramienta a un grupo de 4 hospitales dentro de la población, los resultados obtenidos fueron ingresados y procesados en SPSS para determinar el alfa de Cronbach, obteniendo un nivel de confiabilidad del 0.883.

Tabla 3: Resultados de alfa de Cronbach para herramienta de diagnóstico.

ESTADÍSTICA DE CONFIABILIDAD	
ALFA DE CRONBACH	**NÚMERO DE ÍTEMS**
0.883	10

Fuente: SPSS

Ruíz [40, p. 12] proporciona la magnitud de los coeficientes de confiabilidad mediante la siguiente escala:

Tabla 4: Interpretación de alfa de Cronbach.

ESCALAS	NIVEL DE CONFIABILIDAD
0.81 – 1.00	Muy Alta
0.61 – 0.80	Alta
0.41 – 0.60	Moderada
0.21 – 0.40	Baja
0,01 – 0.20	Muy Baja

Fuente: Ruíz – Confiablidad [40, p. 12]

Se concluye que el nivel de confiabilidad de la herramienta de diagnóstico para el Modelo de Gestión de Seguridad de la Información planteado es **Muy Alta**.

3.1 Armonizar los estándares de gestión de seguridad de la información en base a criterios que se pueda adaptar al contexto de los procesos de farmacia y contribuir su gestión de los hospitales II-I en la región Amazonas.

Con los resultados de esta encuesta se elaboró el análisis de las diferentes metodologías, estándares y marcos de trabajo relacionadas con la gestión de seguridad de la información considerando los siguientes framework:

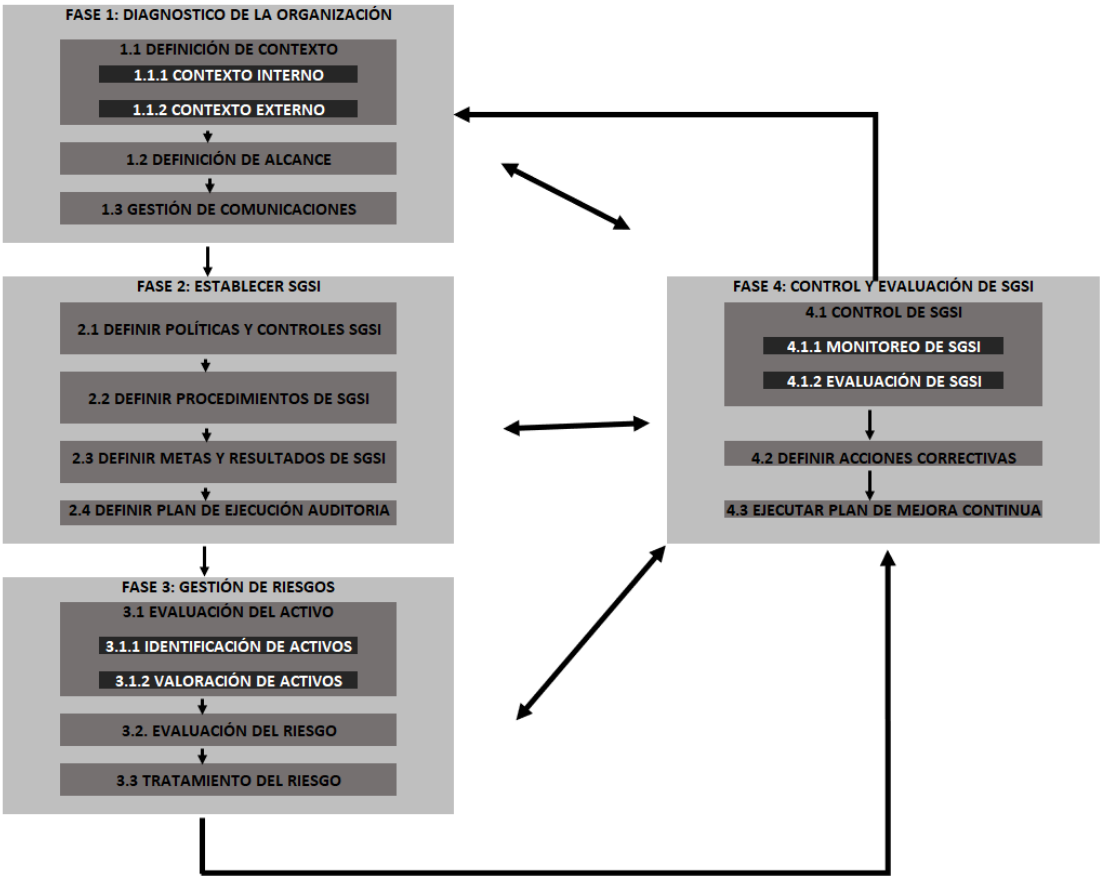
- COBIT 2019
- MAGERIT
- ISO 27000 (27001, 27002, 27003, 27004, 27005, 27006)
- Modelo de Seguridad y Privacidad de la Información (MSPI)
- ITIL v4

Para mejor precisión en los resultados comparativos, base para la propuesta consultar el **ANEXO 04.**

3.2 Elaborar el modelo de gestión de seguridad de la información para mejorar los procesos en farmacias de los hospitales de la región Amazonas.

Como producto del análisis de los las diferentes metodologías, estándares y marcos de trabajo relacionadas con la gestión de seguridad de la información, así como los requerimientos y la realidad del sector, se identificaron las siguientes fases, procesos y subprocesos:

Figura 1: Modelo de Gestión de Seguridad de la Información propuesto



Fuente: Elaboración propia

Las fases, procesos y subprocesos determinados en el modelo son integrados mediante un estándar, marco de trabajo o metodología previamente analizada y su justificación basada en características relevantes orientadas a los requerimientos recolectadas en el diagnóstico. Para mayor detalle consultar el **ANEXO 05**.

A continuación, se describe el desarrollo de la propuesta:

FASE I NATURALEZA DE LA ORGANIZACIÓN

Proceso 1.1 Definición del alcance

Sub proceso 1.1.1 Contexto Interno

Luego de analizar las diferentes propuestas por parte de las metodologías que determinan el contexto interno para el proceso de SGSI se hace uso de ISO 27000 y MSPI; se asume una serie de características y pasos con el propósito de identificar y definir el contexto interno en la organización:

1. Objetivos. - Conjunto de metas establecidas para lograr el cumplimiento del proceso.

   - Reconocer y establecer los parámetros del contexto interno en la organización que influye y tiene algún impacto en el cumplimiento de los objetivos estratégicos y del SGSI.
   - Los parámetros establecidos deben contar con una revisión periódica del SGSI.
   -Si la organización lo determina, pueden agregar o eliminar objetivos que crean convenientes previo sustento.

2. Personal. - Conjunto de participantes o actores que conforman el proceso.
   -Dirección ejecutiva.
   -Administración.
   -Recursos humanos
   -Asesoría legal
   -Otros involucrados que la organización determine.

3. Documentos de entrada. - Conjunto de herramientas que son requeridas para el desarrollo de las actividades en el proceso.
   -Plan estratégico.
   -Manual de Organización y Funciones.
   -Reglamento de Organización y Funciones.
   -Organigrama.
   -Manual de Procedimientos Administrativos.
   -Otros documentos que la organización determine.

4. Proceso. - Conjunto de actividades o tareas a seguir para el cumplimiento de los objetivos.
   -Analizar los documentos de entrada a detalle
   -Definir los procesos y dependencias de la farmacia para el funcionamiento correcto.
   -Definir el personal encargado de elaborar el formato y firmarlo.
   -Definir el personal encargado de revisar el formato y firmarlo.

-Definir el personal encargado de aprobar el formato y firmarlo.

-Completar la información contenida en la plantilla.

5. Documentos de Salida. - Resultados obtenidos después de aplicar las tareas.

   -Lista de procesos *core* y críticos en la farmacia.

   -Áreas y servicios de dependencia en los procesos de las farmacias.

6. Plantilla. - Herramienta que sirve como apoyo en el desarrollo del proceso para cumplir los objetivos.

Tabla 5: Formato de definición de contexto interno.

LOGO DE LA ORGANIZACIÓN	**DEFINICIÓN DE CONTEXTO INTERNO**	
	CÓDIGO SGSI Nº _____	FECHA ELABORACIÓN: ____/____/____
		FECHA APLICACIÓN: ____/____/____
FASE: I - NATURALEZA DE LA ORGANIZACIÓN		**PROCESO: 1. DEFINICIÓN DEL CONTEXTO**
OBJETIVOS	Reconocer y establecer los parámetros del contexto interno en la organización que influye y tiene algún impacto en el cumplimiento de los objetivos estratégicos y del SGSI.	
DESCRIPCIÓN	Previo a la recolección de información se hace uso del análisis de los documentos de entrada.	

PROCESOS CRÍTICOS	**ÁREAS O SERVICIOS INVOLUCRADAS**
En esta sección se especifica los procesos críticos identificados en el análisis de los documentos de entrada	En esta sección se especifica las áreas o servicios involucradas en los procesos críticos posterior al análisis de los documentos de entrada
CONCLUSIONES	
En esta sección se define el comentario final o apreciación de lo observado posterior al llenado de la plantilla.	

HISTORIAL DE VERSIONES		
v. x.x	FECHA: **/**/****	ELABORADO POR:
	Descripción:	
…	…	…

	…

RESPONSABLES		FIRMAS
ELABORADO POR:	En esta sección se especifica el cargo o persona responsable de la elaboración de esta plantilla.	En esta sección se impregna la firma del responsable.
REVISADO POR:	En esta sección se especifica el cargo o persona responsable de la revisión de esta plantilla.	En esta sección se impregna la firma del responsable.
APROBADO POR:	En esta sección se especifica el cargo o persona responsable de la aprobación de esta plantilla.	En esta sección se impregna la firma del responsable.

Fuente: Elaboración propia

Sub proceso 1.1.2 Contexto externo

Luego de analizar las diferentes propuestas por parte de las metodologías que determinan el contexto externo para el proceso de SGSI se hace uso de ISO 27000 y MSPI; se asume una serie de características y pasos con el propósito de identificar y definir el contexto externo en la organización:

1. Objetivos. - Conjunto de metas establecidas para lograr el cumplimiento del proceso.

   - Reconocer y establecer los parámetros del contexto externo en la organización que influye y tiene algún impacto en el cumplimiento de los objetivos estratégicos y del SGSI.

   - Los parámetros establecidos deben contar con una revisión periódica del SGSI.

   -Si la organización lo determina, pueden agregar o eliminar objetivos que crean convenientes previo sustento.

2. Personal. - Conjunto de participantes o actores que conforman el proceso.

   -Dirección ejecutiva.

   -Administración.

   -Asesoría legal

-Otros involucrados que la organización determine.

3. Documentos de Entrada. - Conjunto de herramientas que son requeridas para el desarrollo de las actividades en el proceso.
   -Resoluciones ministeriales.
   -Políticas de salud.
   -Reglamentos del gobierno regional.
   -Reglamentos del gobierno central.
   -Reglamentos del MEF.

4. Proceso. - Conjunto de actividades o tareas a seguir para el cumplimiento de los objetivos.
   -Analizar los documentos de entrada a detalle
   -Definir los contextos y aspectos identificados.
   -Definir el personal encargado de elaborar el formato y firmarlo.
   -Definir el personal encargado de revisar el formato y firmarlo.
   -Definir el personal encargado de aprobar el formato y firmarlo.
   -Completar la información contenida en la plantilla Definición Contexto Externo.

5. Documentos de Salida. - Resultados obtenidos después de aplicar las tareas.
   -Lista de aspectos identificados.
   -Lista de entornos identificados.

6. Plantilla. - Herramienta que sirve como apoyo en el desarrollo del proceso para cumplir los objetivos.

Tabla 6: Formato de definición de contexto externo.

<table>
<tr><td rowspan="3">LOGO DE LA ORGANIZACIÓN</td><td colspan="2">DEFINICIÓN DE CONTEXTO EXTERNO</td></tr>
<tr><td rowspan="2">CÓDIGO SGSI Nº
_____</td><td>FECHA ELABORACIÓN:
____/____/____</td></tr>
<tr><td>FECHA APLICACIÓN: ____/____/____</td></tr>
<tr><td colspan="2"></td><td></td></tr>
</table>

FASE: I - NATURALEZA DE LA ORGANIZACIÓN	PROCESO: 1. DEFINICIÓN DEL CONTEXTO
OBJETIVOS	Reconocer y establecer los parámetros del contexto externo en la organización que influye y tiene algún impacto en el cumplimiento de los objetivos estratégicos y del SGSI.
DESCRIPCIÓN	Previo a la recolección de información se hace uso del análisis de los documentos de entrada.

ENTORNO INVOLUCRADO	ASPECTOS IDENTIFICADOS
En esta sección se especifica el entorno involucrado luego de la identificación en el análisis de los documentos de entrada	En esta sección se especifica los aspectos identificados que influye en el SGSI posterior al análisis de los documentos de entrada.
CONCLUSIONES	
En esta sección se define el comentario final o apreciación de lo observado posterior al llenado de la plantilla.	

HISTORIAL DE VERSIONES		
v. x.x	FECHA: **/**/****	ELABORADO POR:
	Descripción:	
…	…	…
	…	
RESPONSABLES		**FIRMAS**
ELABORADO POR:	En esta sección se especifica el cargo o persona responsable de la elaboración de esta plantilla.	En esta sección se impregna la firma del responsable.
REVISADO POR:	En esta sección se especifica el cargo o persona responsable de la revisión de esta plantilla.	En esta sección se impregna la firma del responsable.
APROBADO POR:	En esta sección se especifica el cargo o persona responsable de la aprobación de esta plantilla.	En esta sección se impregna la firma del responsable.

Fuente: Elaboración propia

Proceso 1.2 Definir el alcance

Luego de analizar las diferentes propuestas por parte de las metodologías que determinan el alcance para el proceso de SGSI se hace uso de COBIT 2019; se asume una serie de características y pasos con el propósito de identificar y definir el alcance del SGSI en la organización:

1. Objetivos. - Conjunto de metas establecidas para lograr el cumplimiento del proceso.
   - Reconocer y determinar los procesos, áreas y servicios que tendrán alcance en el SGSI
   - Determinar las exclusiones de los procesos que no tendrán alcance en el SGSI. - Los parámetros establecidos en la definición deben contar con una revisión periódica del SGSI.
   -Si la organización lo determina, pueden agregar o eliminar objetivos que crean convenientes previo sustento.

2. Personal. - Conjunto de participantes o actores que conforman el proceso.
   -Dirección ejecutiva.
   -Administración.
   -Asesoría legal
   -Otros involucrados que la organización determine.

3. Documentos de Entrada. - Conjunto de herramientas que son requeridas para el desarrollo de las actividades en el proceso.
   -Plantilla Definición Contexto Interno

4. Proceso. - Conjunto de actividades o tareas a seguir para el cumplimiento de los objetivos.
   -Analizar los procesos determinados en la plantilla 1.
   -Determinar los procesos que abarcará el SGSI.
   -Determinar las áreas y servicios que abarcara el SGSI.
   -Determinar las exclusiones que no abarca el SGSI.
   -Elaborar un sustento técnico sobre las exclusiones.
   -Definir el personal encargado de elaborar el formato y firmarlo.

-Definir el personal encargado de revisar el formato y firmarlo.

-Definir el personal encargado de aprobar el formato y firmarlo.

-Completar la información contenida en la plantilla.

5. Documentos de Salida. - Resultados obtenidos después de aplicar las tareas.
   -Lista de procesos, áreas y servicios que abarca el SGSI.
   -Lista de exclusiones del SGSI.
   -Sustento técnico de exclusiones.

6. Plantilla. - Herramienta que sirve como apoyo en el desarrollo del proceso para cumplir los objetivos.

Tabla 7: Formato de definición de alcance.

LOGO DE LA ORGANIZACIÓN	**DEFINICIÓN DEL ALCANCE**	
	CÓDIGO SGSI Nº _____	FECHA ELABORACIÓN: ____/____/____
		FECHA APLICACIÓN: ____/____/____
FASE: I - NATURALEZA DE LA ORGANIZACIÓN		**PROCESO: 2. DEFINICIÓN DEL ALCANCE**
OBJETIVOS	- Reconocer y determinar los procesos, áreas y servicios que tendrán alcance en el SGSI.	
DESCRIPCIÓN	La definición de alcance y exclusiones permite el desarrollo de un sistema orientado a las necesidades de la entidad.	

ALCANCE SGSI	
PROCESOS	En esta sección se especifica los procesos que abarca el SGSI.
ÁREAS O SERVICIOS	En esta sección se especifica las áreas o servicios que abarca el SGSI.
EXCLUSIONES SGSI	
PROCESOS	En esta sección se especifica los procesos que excluyen del SGSI.
CONCLUSIONES	

En esta sección se define el comentario final o apreciación de lo observado posterior al llenado de la plantilla.

HISTORIAL DE VERSIONES		
v. x.x	FECHA: **/**/****	ELABORADO POR:
	Descripción:	
…	…	…
	…	

RESPONSABLES		FIRMAS
ELABORADO POR:	En esta sección se especifica el cargo o persona responsable de la elaboración de esta plantilla.	En esta sección se impregna la firma del responsable.
REVISADO POR:	En esta sección se especifica el cargo o persona responsable de la revisión de esta plantilla.	En esta sección se impregna la firma del responsable.
APROBADO POR:	En esta sección se especifica el cargo o persona responsable de la aprobación de esta plantilla.	En esta sección se impregna la firma del responsable.

Fuente: Elaboración propia

Proceso 1.3 Gestión de las comunicaciones

Luego de analizar las diferentes propuestas por parte de las metodologías que determinan la gestión de las comunicaciones para el proceso de SGSI se hace uso de MSPI; se asume una serie de características y pasos con el propósito de desarrollar este proceso en la organización:

1. Objetivos. - Conjunto de metas establecidas para lograr el cumplimiento del proceso.

   -Definir los perfiles y responsabilidades que realizará cada miembro del SGSI en todas las fases.

   -Organizar y seleccionar el grupo de trabajo responsable de la implementación del SGSI.

- Los parámetros establecidos deben contar con una revisión periódica del SGSI.

-Si la organización lo determina, pueden agregar o eliminar responsabilidades que crean convenientes.

2. Personal. - Conjunto de participantes o actores que conforman el proceso.
   -Dirección ejecutiva.
   -Administración.
   -Asesoría legal.
   -director o jefe de TI.
   -Otros involucrados que la organización determine.

3. Documentos de Entrada. - Conjunto de herramientas que son requeridas para el desarrollo de las actividades en el proceso.
   -Plantilla Definición de Alcance

4. Proceso. - Conjunto de actividades o tareas a seguir para el cumplimiento de los objetivos.
   -Analizar los perfiles sugeridos para la implementación.
   -Analizar las responsabilidades o tareas de cada perfil.
   -Determinar los perfiles y responsabilidades a mantener.
   -Definir los responsables en cada perfil previamente determinado.
   -Definir el personal encargado de elaborar el formato y firmarlo.
   -Definir el personal encargado de revisar el formato y firmarlo.
   -Definir el personal encargado de aprobar el formato y firmarlo.
   -Completar la información contenida en la plantilla Definición de Alcance.

5. Documentos de Salida. - Resultados obtenidos después de aplicar las tareas.
   -Lista de roles y responsabilidades definidos.
   -Lista de integrantes del equipo de trabajo en el SGSI.

6. Plantilla. - Herramienta que sirve como apoyo en el desarrollo del proceso para cumplir los objetivos.

Tabla 8: Formato de gestión de las comunicaciones.

<table>
<tr><td rowspan="2">LOGO DE LA ORGANIZACIÓN</td><td colspan="2">GESTIÓN DE LAS COMUNICACIONES</td></tr>
<tr><td rowspan="2">CÓDIGO SGSI Nº
_____</td><td>FECHA ELABORACIÓN:
____/____/____</td></tr>
<tr><td>FECHA APLICACIÓN:
____/____/____</td></tr>
<tr><td colspan="2">FASE: I - NATURALEZA DE LA ORGANIZACIÓN</td><td>PROCESO: 3. GESTIÓN DE LAS COMUNICACIONES</td></tr>
<tr><td>OBJETIVOS</td><td colspan="2">-Definir los perfiles y responsabilidades que realizará cada miembro del SGSI en todas las fases.</td></tr>
<tr><td>DESCRIPCIÓN</td><td colspan="2">Los roles y perfiles determinados en esta plantilla pueden ser modificados previo acuerdo con el comité de seguridad.</td></tr>
</table>

<table>
<tr><th colspan="2">EQUIPO DE SGSI</th></tr>
<tr><td colspan="2"> 
</td></tr>
<tr><th colspan="2">INTEGRANTES</th></tr>
<tr><th>ROLES</th><th>RESPONSABLES</th></tr>
<tr><td>RESPONSABLE DE SEGURIDAD DE LA ENTIDAD</td><td>-Líder del proyecto.</td></tr>
<tr><td>EQUIPO DE PROYECTO</td><td>-Un representante de área de informática.
-Un representante del área de Control Interno.
-Un representante del área de Planeación.
-Un representante del Administración.</td></tr>
<tr><td>COMITÉ DE SEGURIDAD</td><td>-Un representante de área de informática.
-Un representante del área de Control Interno.
-Un representante del área de Planeación.</td></tr>
</table>

	-Un representante del área Jurídica. -El responsable de seguridad de la información.
CONCLUSIONES	
En esta sección se define el comentario final o apreciación de lo observado posterior al llenado de la plantilla.	

HISTORIAL DE VERSIONES		
v. x.x	FECHA: **/**/****	ELABORADO POR:
	Descripción:	
…	…	…
	…	
RESPONSABLES		**FIRMAS**
ELABORADO POR:	En esta sección se especifica el cargo o persona responsable de la elaboración de esta plantilla.	En esta sección se impregna la firma del responsable.
REVISADO POR:	En esta sección se especifica el cargo o persona responsable de la revisión de esta plantilla.	En esta sección se impregna la firma del responsable.
APROBADO POR:	En esta sección se especifica el cargo o persona responsable de la aprobación de esta plantilla.	En esta sección se impregna la firma del responsable.

Fuente: Elaboración propia

FASE II ESTABLECER SGSI

Proceso 2.1 Definir políticas y controles SGSI

Luego de analizar las diferentes propuestas por parte de las metodologías que define las políticas y controles SGSI se hace uso de ISO 27000 Y MSPI; se asume una serie de características y pasos con el propósito de desarrollar este proceso en la organización:

1. Objetivos. - Conjunto de metas establecidas para lograr el cumplimiento del proceso.

   - Identificar y determinar las políticas de acuerdo a las necesidades de la entidad

- Identificar y determinar los controles de acuerdo a las necesidades de la entidad.
- Los parámetros establecidos en la definición deben contar con una revisión periódica del SGSI.
-Si la organización lo determina, pueden agregar o eliminar políticas y controles que crean convenientes previo sustento.

2. Personal. - Conjunto de participantes o actores que conforman el proceso.
   -Responsable de seguridad.
   -Equipo de proyecto.
   -Comité de seguridad.
   -Otros involucrados que la organización determine.

3. Documentos de Entrada. - Conjunto de herramientas que son requeridas para el desarrollo de las actividades en el proceso.
   -Plantilla Definición Contexto Interno
   -Plantilla Definición Contexto Externo
   -Plantilla Definición de Alcance

4. Proceso. - Conjunto de actividades o tareas a seguir para el cumplimiento de los objetivos.
   -Identificar y determinar las políticas y controles.
   -Relacionar las políticas determinadas en MSPI con los controles identificados en ISO 27002.
   -Identificar las personas que abarca el cumplimiento de cada política.
   -Definir el personal encargado de elaborar el formato y firmarlo.
   -Definir el personal encargado de revisar el formato y firmarlo.
   -Definir el personal encargado de aprobar el formato y firmarlo.
   -Completar la información contenida en la plantilla.

5. Documentos de Salida. - Resultados obtenidos después de aplicar las tareas.
   -Relación de políticas y controles determinados de acuerdo a las necesidades de la entidad.

6. Plantilla. - Herramienta que sirve como apoyo en el desarrollo del proceso para cumplir los objetivos.

Tabla 9: Formato de definición de políticas y controles.

LOGO DE LA ORGANIZACIÓN	**DEFINICIÓN DE POLÍTICAS Y CONTROLES**	
	CÓDIGO SGSI Nº _____	FECHA ELABORACIÓN: ____/____/____
		FECHA APLICACIÓN: ____/____/____
FASE: II - ESTABLECER SGSI		**PROCESO: 2.1. DEFINIR POLÍTICAS Y CONTROLES SGSI**
OBJETIVOS	- Identificar y determinar las políticas de acuerdo a las necesidades de la entidad.	
DESCRIPCIÓN	Las políticas y controles determinados en esta plantilla pueden ser modificadas de acuerdo a la naturaleza y recursos de la entidad.	

POLÍTICA SGSI				
CÓDIGO	**EJE**	**DEFINICIÓN**	**CUMPLIMIENTO**	**CONTROL**
PS-01	GESTIÓN DE ACTIVOS	Se identificará, clasificará y gestionará los activos de información con la finalidad de garantizar la integridad de los mismos.	Todos los funcionarios que laboran en las áreas que abarca el alcance del SGSI.	8.1.1 Inventario de activos; 8.1.2 Propiedad de activos; 8.2.1 Clasificación de la información; 11.2.4 Mantenimiento de equipos.
PS-02	NO REPUDIO	Se realizará operaciones de trazabilidad, y retención de las acciones realizadas por los usuarios como creación, origen, recepción, entrega de información y otros.	Todos los funcionarios que laboran en las áreas que abarca el alcance del SGSI.	12.2.1 Controles contra códigos maliciosos
PS-03	PRIVACIDAD Y CONFIDENCIALIDAD	Conforme a lo establecido en la Ley 29733, la entidad garantizará el tratamiento de datos personales en el alcance del SGSI.	Todos los funcionarios que laboran en las áreas que abarca el alcance del SGSI.	5.1.2 Revisión de las políticas para la seguridad de la información; 6.2.1 Política de dispositivos móviles; 9.4.1 Restricción de

				acceso a la información.
PS-04	CONTROL DE ACCESO	Se determinará los procedimientos frente a la administración y responsabilidad relacionado con los accesos de la información, sin importar estos sean electrónicos o físicos.	Todos los funcionarios que laboran en las áreas que abarca el alcance del SGSI.	9.1.1 Política de control de acceso; 9.1.2 Acceso a redes y servicios de red; 9.2.1 Registro y baja de usuarios; 9.2.2 Aprovisionamiento de acceso a usuario; 9.2.5 Revisión de derechos de acceso a usuarios; Sistema de gestión de contraseñas; 11.1.2 Controles de ingreso físicos; 11.1.3 Asegurar oficinas, áreas e instalaciones.
PS-05	REGISTRO Y AUDITORIA	Velar por el mantenimiento de las evidencias de las actividades y acciones que afincan los activos de información, así como garantizar el cumplimiento del SGSI y su mejora continua.	Responsable de seguridad del SGSI	12.3.1 Respaldo de información; 12.4.1 Registro de eventos; 12.4.2 Protección de información de registros; 12.7.1 Controles de auditoría de sistemas de información; 18.2.1 Revisión independiente de la seguridad de la información.
PS-06	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	Garantiza una gestión de eventos, incidentes y vulnerabilidades de seguridad de la información.	Dirigida a todos los usuarios que tienen un acceso autorizado a cualquier sistema de información	16.1.1 Responsabilidades y procedimientos; 16.1.2 Reporte de eventos de seguridad de la información; 16.1.3 Reporte de debilidades de seguridad de la información.
PS-07	CAPACITACIÓN Y SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN	Se centra en la formación del personal en temas relacionados con la seguridad de la información, cuya finalidad es disminuir las vulnerabilidades y amenazas relacionadas con	Todos los funcionarios que laboran en la entidad.	7.2.2 Conciencia, educación y capacitación sobre la seguridad de la información.

		el recurso humano.		
…	OTROS EJES QUE LA ENTIDAD DETERMINE NECESARIO	Breve concepto de la política a determinar.	Personal involucrado en la política (ejecutor o responsable).	Control adecuado de acuerdo a la Norma ISO 27002

CONCLUSIONES
En esta sección se define el comentario final o apreciación de lo observado posterior al llenado de la plantilla.

HISTORIAL DE VERSIONES		
v. x.x	FECHA: **/**/****	ELABORADO POR:
	Descripción:	
…	…	…
	…	

RESPONSABLES		**FIRMAS**
ELABORADO POR:	En esta sección se especifica el cargo o persona responsable de la elaboración de esta plantilla.	En esta sección se impregna la firma del responsable.
REVISADO POR:	En esta sección se especifica el cargo o persona responsable de la revisión de esta plantilla.	En esta sección se impregna la firma del responsable.
APROBADO POR:	En esta sección se especifica el cargo o persona responsable de la aprobación de esta plantilla.	En esta sección se impregna la firma del responsable.

Fuente: Elaboración propia

Proceso 2.2 Definir procedimientos SGSI

Luego de analizar las diferentes propuestas por parte de las metodologías que definen los procedimientos SGSI se hace uso de COBIT 2019 E MSPI; se asume una serie de características y pasos con el propósito de desarrollar este proceso en la organización:

1. Objetivos. - Conjunto de metas establecidas para lograr el cumplimiento del proceso.

   - Identificar y determinar los dominios de acuerdo a las necesidades de la entidad

   - Identificar y determinar los procedimientos de acuerdo a las necesidades de la entidad

   - Los parámetros establecidos en la definición deben contar con una revisión periódica del SGSI.

   -Si la organización lo determina, pueden agregar o eliminar procedimientos que crean convenientes previo sustento.

2. Personal. - Conjunto de participantes o actores que conforman el proceso.

   -Responsable de seguridad.

   -Equipo de proyecto.

   -Comité de seguridad.

   -Otros involucrados que la organización determine.

3. Documentos de Entrada. - Conjunto de herramientas que son requeridas para el desarrollo de las actividades en el proceso.

   -Plantilla Definición de Alcance

4. Proceso. - Conjunto de actividades o tareas a seguir para el cumplimiento de los objetivos.

   -Identificar y determinar los dominios y sus respectivos procedimientos

   -Identificar las personas responsables de implementar cada procedimiento.

   -Determinar los puntos de control en cada procedimiento.

   -Definir el personal encargado de elaborar el formato y firmarlo.

   -Definir el personal encargado de revisar el formato y firmarlo.

   -Definir el personal encargado de aprobar el formato y firmarlo.

   -Completar la información contenida en la plantilla.

5. Documentos de Salida. - Resultados obtenidos después de aplicar las tareas.

   -Relación de procedimientos, puntos de control y responsables determinados de acuerdo a las necesidades de la entidad.

6. Plantilla. - Herramienta que sirve como apoyo en el desarrollo del proceso para cumplir los objetivos.

Tabla 10: Formato de definición de procedimientos SGSI.

LOGO DE LA ORGANIZACIÓN	**DEFINICIÓN DE PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN**	
	CÓDIGO SGSI Nº _____	FECHA ELABORACIÓN: ____/____/____
		FECHA APLICACIÓN: ____/____/____
FASE: II - ESTABLECER SGSI		**PROCESO: 2.2. DEFINIR PROCEDIMIENTOS SGSI**
OBJETIVOS	- Identificar y determinar los dominios y procedimientos de acuerdo a las necesidades de la entidad	
DESCRIPCIÓN	Los dominios son extraídos de MSPI y relacionados con los 114 controles de seguridad de la información de la ISO 27000, la entidad puede modificar los controles y dominios de acuerdo a su naturaleza y recursos.	

DOMINIO	PROCEDIMIENTO	PUNTO DE CONTROL	RESPONSABLE
Seguridad del recurso humano	Capacitación y sensibilización del personal.		
	ingreso y desvinculación del personal.		
Gestión de activos	Identificación y clasificación de activos.		
Control de acceso	Ingreso seguro a los sistemas de información.		
	gestión de usuarios y contraseñas.		
Seguridad física y del entrono	Control de acceso físico.		
	Protección de activos.		
	Mantenimiento de equipos		
Seguridad de las operaciones	Gestión de cambios.		
	Protección contra código malicioso.		

Seguridad de las comunicaciones.	Aseguramiento de servicios en la red.		
Relación con los proveedores	Tratamiento de la seguridad en los acuerdos con los proveedores.		
incidentes de seguridad de la información	Gestión de incidentes de seguridad de la información.		
Otro dominio que la entidad determine necesario	Otro procedimiento que la entidad determine necesario	…	….

*Punto de control: Requerimiento mínimo para que el procedimiento pueda ejecutarse
por ejemplo, un control de cambios, un formato o una aprobación.
*Responsable: responsable del procedimiento.

CONCLUSIONES
En esta sección se define el comentario final o apreciación de lo observado posterior al llenado de la plantilla.

HISTORIAL DE VERSIONES		
v. x.x	FECHA: **/**/****	ELABORADO POR:
	Descripción:	
…	…	…
	…	

RESPONSABLES		**FIRMAS**
ELABORADO POR:	En esta sección se especifica el cargo o persona responsable de la elaboración de esta plantilla.	En esta sección se impregna la firma del responsable.
REVISADO POR:	En esta sección se especifica el cargo o persona responsable de la revisión de esta plantilla.	En esta sección se impregna la firma del responsable.
APROBADO POR:	En esta sección se especifica el cargo o persona responsable de la aprobación de esta plantilla.	En esta sección se impregna la firma del responsable.

Fuente: Elaboración propia

Proceso 2.3 Definir metas y resultados SGSI

Luego de analizar las diferentes propuestas por parte de las metodologías que las metas y resultados SGSI se hace uso de ISO 27000; se asume una serie de características y pasos con el propósito de desarrollar este proceso en la organización:

1. Objetivos. - Conjunto de metas establecidas para lograr el cumplimiento del proceso.
   - Identificar y determinar las medidas con sus características.
   - Identificar y determinar las metas en cada medición, así como la periodicidad del misma
   - Los parámetros establecidos en la definición deben contar con una revisión periódica del SGSI.
   -Si la organización lo determina, pueden agregar o eliminar medidas que crean conveniente.

2. Personal. - Conjunto de participantes o actores que conforman el proceso.
   -Responsable de seguridad.
   -Equipo de proyecto.
   -Comité de seguridad.
   -Otros involucrados que la organización determine.

3. Documentos de Entrada. - Conjunto de herramientas que son requeridas para el desarrollo de las actividades en el proceso.
   -Plantilla Definición de Políticas y Controles SGSI
   -Plantilla Procedimiento SGSI

4. Proceso. - Conjunto de actividades o tareas a seguir para el cumplimiento de los objetivos.
   -Identificar y determinar los constructores de medición y sus características o aspectos a evaluar.
   -Identificar y determinar las metas para cada medida, la presentación de estas y la frecuencia de medición.
   -Definir el personal encargado de elaborar el formato y firmarlo.

-Definir el personal encargado de revisar el formato y firmarlo.

-Definir el personal encargado de aprobar el formato y firmarlo.

-Completar la información contenida en la plantilla Definición de Metas y Resultados SGSI.

5. Documentos de Salida. - Resultados obtenidos después de aplicar las tareas.
   -Relación de métricas sus características y aspectos.
   -Metas definidas en cada métrica de acuerdo a las necesidades de la entidad.

6. Plantilla. - Herramienta que sirve como apoyo en el desarrollo del proceso para cumplir los objetivos.

Tabla 11: Formato de definición de metas y resultados SGSI.

LOGO DE LA ORGANIZACIÓN	**DEFINICIÓN DE PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN**	
	CÓDIGO SGSI Nº _____	FECHA ELABORACIÓN: ____/____/____
		FECHA APLICACIÓN: ____/____/____
FASE: II - ESTABLECER SGSI		**PROCESO: 2.3. DEFINIR METAS Y RESULTADOS SGSI**
OBJETIVOS	- Identificar y determinar las medidas con sus características y sus metas respectivas.	
DESCRIPCIÓN	Cada métrica se relación con las políticas definidas en la Plantilla 6, la entidad puede modificar las medidas de acuerdo a su naturaleza y recursos disponibles.	

Identificación de métrica.	
Nombre de métrica.	Formación en seguridad de la información.
Código de métrica.	MS-01
Propósito de métrica.	Evaluar el cumplimiento con los requisitos de formación en concientización de seguridad de la información
Eje de política	PS-07
Objetivo de control	
Objeto de la medición y atributos	
Objeto de la medición	Base de datos de empleados

Atributo	Registros de formación		
Especificación de la medida			
Medida	Porcentaje del personal que ha recibido entrenamiento anual de concientización en seguridad de la información		
Función de medición	Número de empleados que han recibido entrenamiento anual de concientización en seguridad de la información/número de empleados que necesitan recibir entrenamiento anual de concientización en seguridad de la información * 100		
Escala	Numérico		
Unidad de medida	Empleado		
Meta	Mínima 0-60%	Satisfactoria 60-90%	Sobresaliente 90-100%
Frecuencia de Recolección y Análisis	Semestral		

Identificación de métrica.	
Nombre de métrica.	Cumplimiento con la política de concientización en seguridad de la información.
Código de métrica.	MS-02
Propósito de métrica.	Evaluar el estado del cumplimiento con la política de concientización en seguridad de la organización entre el personal relevante
Eje de política	PS-07
Objetivo de control	
Objeto de la medición y atributos	
Objeto de la medición	Plan de formación de concientización en seguridad de la información
Atributo	Personal identificado en el plan
Especificación de la medida	
Medida	Progreso hasta la fecha.
Función de medición	1. Agregar el estado a todo el personal que ha firmado, planificado y por completar hasta la fecha 2. Dividir el personal que ha firmado hasta la fecha por el personal planificado para firmar hasta la fecha
Escala	Numérico
Unidad de medida	Personal, Porcentaje

Meta	Mínima 0-60%	Satisfactoria 60-90%	Sobresaliente 90-100%
Frecuencia de Recolección y Análisis	Semestral		

Identificación de métrica.			
Nombre de métrica.	Calidad de las contraseñas		
Código de métrica.	MS-03		
Propósito de métrica.	Evaluar la calidad de las contraseñas utilizadas por los usuarios para acceder a los sistemas de TI de la organización		
Eje de política	PS-04		
Objetivo de control			
Objeto de la medición y atributos			
Objeto de la medición	Base de datos de contraseñas de usuario		
Atributo	Contraseñas individuales		
Especificación de la medida			
Medida	Total de número de contraseñas que cumplen la política de calidad de contraseñas de la organización		
Función de medición	Suma de [Total de número de contraseñas que cumplen la política de calidad de contraseñas de la organización para cada usuario]		
Escala	Ordinal		
Unidad de medida	Contraseñas		
Meta	Mínima 0-60%	Satisfactoria 60-90%	Sobresaliente 90-100%
Frecuencia de Recolección y Análisis	Semestral		

Identificación de métrica.	
Nombre de métrica.	Proceso de revisión del SGSI
Código de métrica.	MS-04
Propósito de métrica.	Evaluar el grado de realización de una revisión independiente de la seguridad de la información
Eje de política	PS-05
Objetivo de control	
Objeto de la medición y atributos	

Objeto de la medición	Informes de las revisiones		
Atributo	Revisiones de partes interesadas Informadas y planificadas		
Especificación de la medida			
Medida	Número de revisiones de partes interesadas llevadas a cabo		
Función de medición	Dividir [Número de revisiones de partes interesadas llevadas a cabo] por [Total de número de revisiones de partes interesadas planificadas].		
Escala	Ordinal		
Unidad de medida	Revisión		
Meta	Mínima 0 - 0,6	Satisfactoria 0,6 - 0,8	Sobresaliente 0,8 - 1,1
Frecuencia de Recolección y Análisis	Anual		

Identificación de métrica.			
Nombre de métrica.	Efectividad de la Gestión de Incidentes de Seguridad de la Información		
Código de métrica.	MS-05		
Propósito de métrica.	Evaluar la efectividad de la gestión de incidentes de seguridad de la información		
Eje de política	PS-06		
Objetivo de control	Posibilitar la detección temprana de eventos de seguridad y dar respuesta a los incidentes de seguridad.		
Objeto de la medición y atributos			
Objeto de la medición	SGSI		
Atributo	Incidentes individuales		
Especificación de la medida			
Medida	Incidentes que exceden el umbral		
Función de medición	Comparación del número total de incidentes con el umbral.		
Escala	Ordinal		
Unidad de medida	Revisión		
Meta	Mínima: Tendencia al alza	Satisfactoria: Tendencia se mantiene	Sobresaliente: Tendencia a baja
Frecuencia de Recolección y Análisis	Anual		

Identificación de métrica.			
Nombre de métrica.	Protección contra código malicioso		
Código de métrica.	MS-06		
Propósito de métrica.	Evaluar la eficacia del sistema de protección contra software malicioso y ataques de software.		
Eje de política	PS-03		
Objetivo de control	Proteger la integridad del software y la información. (planificado) Proteger la integridad del software y la información de software maliciosos.		
Objeto de la medición y atributos			
Objeto de la medición	Reportes de incidentes		
Atributo	Incidentes causados por software malicioso		
Especificación de la medida			
Medida	Fortaleza de la protección contra software malicioso		
Función de medición	Número de incidentes de seguridad causados por software malicioso/número de ataques detectados y bloqueados causados por software malicioso		
Escala	Enteros de cero a infinito		
Unidad de medida	Incidentes de seguridad		
Meta	Rojo > 10%	Amarillo 10%	Verde < 10%
Frecuencia de Recolección y Análisis	Mensual		

Identificación de métrica.	
Nombre de métrica.	Revisión de archivos de registro(log)
Código de métrica.	MS-07
Propósito de métrica.	Evaluar el estado de conformidad de las revisiones regulares a los archivos de registro (log) de sistemas críticos.
Eje de política	PS-02
Objetivo de control	Detectar actividades de procesamiento de información no autorizadas. (planificado) Detectar actividades de procesamiento de información no autorizadas en sistemas críticos a partir de los sistemas de registros(log)
Objeto de la medición y atributos	
Objeto de la medición	Sistema
Atributo	Archivos de Registro Individual
Especificación de la medida	
Medida	

	Porcentaje de archivos de registro de auditoría revisados cuando es requerido por período de tiempo		
Función de medición	(# de archivos de registro revisados dentro del período de tiempo especificado)/(# total de archivos de registro)*100.		
Escala	Ratio.		
Unidad de medida	Archivo de registro(log)		
Meta	Mínima 0-20%	Satisfactoria 20-70%	Sobresaliente 70-100%
Frecuencia de Recolección y Análisis	Mensual		

Identificación de métrica.			
Nombre de métrica.	Clasificación de activos de Información		
Código de métrica.	MS-08		
Propósito de métrica.	Evaluar el inventario de activos, incluyendo su administración.		
Eje de política	PS-01		
Objetivo de control	Identificar activos de información no clasificados a partir del inventario de activos.		
Objeto de la medición y atributos			
Objeto de la medición	Plan de Inventario de Activos de Información.		
Atributo	Activo de información individual.		
Especificación de la medida			
Medida	Porcentaje de activos de Información clasificados.		
Función de medición	(# de activos de información clasificados)/(# total de activos de información identificados en el plan)*100.		
Escala	Ratio.		
Unidad de medida	Activo de información.		
Meta	Mínima 0-40%	Satisfactoria 40-70%	Sobresaliente 70-100%
Frecuencia de Recolección y Análisis	Semestral		

CONCLUSIONES
En esta sección se define el comentario final o apreciación de lo observado posterior al llenado de la plantilla.

HISTORIAL DE VERSIONES

v. x.x	FECHA: **/**/****	ELABORADO POR:
	Descripción:	
…	…	…
	…	

RESPONSABLES		FIRMAS
ELABORADO POR:	En esta sección se especifica el cargo o persona responsable de la elaboración de esta plantilla.	En esta sección se impregna la firma del responsable.
REVISADO POR:	En esta sección se especifica el cargo o persona responsable de la revisión de esta plantilla.	En esta sección se impregna la firma del responsable.
APROBADO POR:	En esta sección se especifica el cargo o persona responsable de la aprobación de esta plantilla.	En esta sección se impregna la firma del responsable.

Fuente: Elaboración propia

Proceso 2.4 Definir un plan de auditoría.

Luego de analizar las diferentes propuestas por parte de las metodologías que definen un plan de auditoria se hace uso de MSPI; se asume una serie de características y pasos con el propósito de desarrollar este proceso en la organización:

1. Objetivos. - Conjunto de metas establecidas para lograr el cumplimiento del proceso.

   -Determinar aspectos importantes de la planificación en auditoria

   - Determinar características a auditar.

   - Los parámetros establecidos en la definición deben contar con una revisión periódica del SGSI.

2. Personal. - Conjunto de participantes o actores que conforman el proceso.

   -Responsable de seguridad.

   -Otros involucrados que la organización determine.

3. Documentos de Entrada. - Conjunto de herramientas que son requeridas para el desarrollo de las actividades en el proceso.
   -Plantilla Definición de Políticas y Controles SGSI

4. Proceso. - Conjunto de actividades o tareas a seguir para el cumplimiento de los objetivos.
   -Determinar duración, frecuencia y tipo de auditoría.
   -Determinar aspectos o características a evaluar en cada control determinado previamente en la plantilla Definición de Políticas y Controles SGSI
   -Definir el personal encargado de elaborar el formato y firmarlo.
   -Definir el personal encargado de revisar el formato y firmarlo.
   -Definir el personal encargado de aprobar el formato y firmarlo.
   -Completar la información contenida en la plantilla.

5. Documentos de Salida. - Resultados obtenidos después de aplicar las tareas.
   -Características de auditoria definidas de acuerdo a la capacidad de la entidad.
   -Relación de controles a auditar, así como aspectos a evaluar.

6. Plantilla. - Herramienta que sirve como apoyo en el desarrollo del proceso para cumplir los objetivos.

Tabla 12: Formato de definición de plan de auditoría.

<table>
<tr><td rowspan="2">LOGO DE LA ORGANIZACIÓN</td><td colspan="2">DEFINICIÓN DE PLAN DE AUDITORIA</td></tr>
<tr><td rowspan="2">CÓDIGO SGSI Nº _____</td><td>FECHA ELABORACIÓN: ____/____/____</td></tr>
<tr><td>FECHA APLICACIÓN: ____/____/____</td></tr>
<tr><td colspan="2">FASE: II - ESTABLECER SGSI</td><td>PROCESO: 2.4. DEFINIR PLAN DE AUDITORIA</td></tr>
<tr><td>OBJETIVOS</td><td colspan="2">-Determinar aspectos importantes de la planificación en auditoria</td></tr>
<tr><td>DESCRIPCIÓN</td><td colspan="2">Los controles a auditar deben ser los definidos por la entidad en la Plantilla 06.</td></tr>
</table>

Duración	
Frecuencia	
Tipo	

Controles Definidos	Control organizacional	Control técnico	Pruebas del sistema	Inspecciones visuales	Observaciones
5.1.2 Revisión de las políticas para la seguridad de la información					
6.2.1 Política de dispositivos móviles					
7.2.2 Conciencia, educación y capacitación sobre la seguridad de la información					
8.1.1 Inventario de activos					
8.1.2 Propiedad de activos					
8.2.1 Clasificación de la información					
9.1.1 Política de control de acceso					
9.1.2 Acceso a redes y servicios de red					
9.2.1 Registro y baja de usuarios					
9.2.2 Aprovisionamiento de acceso a usuario					
9.2.5 Revisión de derechos de acceso a usuarios					
9.4.1 Restricción de acceso a la información					
9.4.3 Sistema de gestión de contraseñas					

11.1.2 Controles de ingreso físicos					
11.1.3 Asegurar oficinas, áreas e instalaciones					
11.2.4 Mantenimiento de equipos					
12.2.1 Controles contra códigos maliciosos					
12.3.1 Respaldo de información					
12.4.1 Registro de eventos					
12.4.2 Protección de información de registros					
12.7.1 Controles de auditoría de sistemas de información					
16.1.1 Responsabilidades y procedimientos					
16.1.2 Reporte de eventos de seguridad de la información					
16.1.3 Reporte de debilidades de seguridad de la información					
18.2.1 Revisión independiente de la seguridad de la información					
Otros controles que fueron definidos en la etapa anterior					

-Control organizacional: Cuando la evidencia del control es obtenida por medio de registros en el plan, entrevistas, observación o inspección física.
-Control técnico: Cuando la evidencia del control es obtenida a través de pruebas del sistema uso de herramientas especializadas de auditoría.
-Pruebas del sistema: Cuando se obtiene información a través de configuraciones en el sistema o donde el auditor ingresa a una consola de sistema o evaluación de resultados de herramientas de sistemas.
-Inspecciones visuales: Cuando el agrupamiento de medios para la obtención de información no es suficiente, el auditor debe verificar el control insitu.
-Observaciones: Observaciones o recomendaciones del auditor en cada control auditado.

CONCLUSIONES

En esta sección se define el comentario final o apreciación de lo observado posterior al llenado de la plantilla.

HISTORIAL DE VERSIONES		
v. x.x	FECHA: **/**/****	ELABORADO POR:
	Descripción:	
…	…	…
	…	

RESPONSABLES		FIRMAS
ELABORADO POR:	En esta sección se especifica el cargo o persona responsable de la elaboración de esta plantilla.	En esta sección se impregna la firma del responsable.
REVISADO POR:	En esta sección se especifica el cargo o persona responsable de la revisión de esta plantilla.	En esta sección se impregna la firma del responsable.
APROBADO POR:	En esta sección se especifica el cargo o persona responsable de la aprobación de esta plantilla.	En esta sección se impregna la firma del responsable.

Fuente: Elaboración propia

FASE III GESTIÓN DE RIESGOS

Proceso 3.1 Evaluación del activo

Sub proceso 3.1.1 Identificación de activos

Luego de analizar las diferentes propuestas por parte de las metodologías que determinan la identificación de activos para el proceso de SGSI se hace uso de ISO 27000 y MAGERIT; se asume una serie de características y pasos con el propósito de desarrollar este proceso en la organización:

1. Objetivos. - Conjunto de metas establecidas para lograr el cumplimiento del proceso.

   -Identificar los activos de información de la entidad de acuerdo al alcance determinado.

   -Clasificar los activos de acuerdo a su tipo según MAGERIT.

   -Los parámetros establecidos en la definición deben contar con una revisión periódica del SGSI.
2. Personal. - Conjunto de participantes o actores que conforman el proceso.

-Responsable de seguridad.

-Otros involucrados que la organización determine.

3. Documentos de Entrada. - Conjunto de herramientas que son requeridas para el desarrollo de las actividades en el proceso.
   -Plantilla Definición de Alcance
   -Catálogo de elementos MAGERITv3.

4. Proceso. - Conjunto de actividades o tareas a seguir para el cumplimiento de los objetivos.
   -Identificar y codificar los activos de ti
   -Clasificar los activos según catálogo de MAGERIT.
   -Definir el personal encargado de elaborar el formato y firmarlo.
   -Definir el personal encargado de revisar el formato y firmarlo.
   -Definir el personal encargado de aprobar el formato y firmarlo.
   -Completar la información contenida en la plantilla 009.

5. Documentos de Salida. - Resultados obtenidos después de aplicar las tareas.
   -Relación de activos de TI que cuenta la entidad.

6. Plantilla. - Herramienta que sirve como apoyo en el desarrollo del proceso para cumplir los objetivos.

Tabla 13: Formato de identificación de activos.

<table>
<tr><td rowspan="3">LOGO DE LA ORGANIZACIÓN</td><td colspan="2">IDENTIFICACIÓN DE ACTIVOS</td></tr>
<tr><td rowspan="2">CÓDIGO SGSI Nº
_____</td><td>FECHA ELABORACIÓN:
____/____/____</td></tr>
<tr><td>FECHA APLICACIÓN:
____/____/____</td></tr>
<tr><td colspan="2">FASE: III - GESTIÓN DE RIESGOS</td><td>PROCESO: 3.1. EVALUACIÓN DEL ACTIVO</td></tr>
<tr><td>OBJETIVOS</td><td colspan="2">-Identificar y clasificar los activos de información de la entidad de acuerdo al alcance determinado.</td></tr>
</table>

DESCRIPCIÓN	La clasificación de los activos se especifica en los anexos de MAGERIT e ISO 27000, la entidad puede hacer libre uso de ellos.

CÓDIGO	CLASIFICACIÓN *	ACTIVO	DESCRIPCIÓN
En esta sección se define el código del activo a identificar.	En esta sección se especifica el tipo de activo según anexo MAGERIT*.	En esta sección se determina el activo que es identificado según el nombre técnico o común que se utiliza en la entidad.	En esta sección se describe al activo identificado, el uso o rol que cumple en la entidad.
…	…	…	…

*Para la elaboración de esta plantilla, tener en cuenta el "CATALOGO DE ELEMENTOS MAGERIT v3" pág. 7-14 donde detalla todas las clasificaciones para los diferentes tipos de activos que puede haber en una entidad.

CONCLUSIONES
En esta sección se define el comentario final o apreciación de lo observado posterior al llenado de la plantilla.

HISTORIAL DE VERSIONES		
v. x.x	FECHA: **/**/****	ELABORADO POR:
	Descripción:	
…	…	…
	…	

RESPONSABLES		**FIRMAS**
ELABORADO POR:	En esta sección se especifica el cargo o persona responsable de la elaboración de esta plantilla.	En esta sección se impregna la firma del responsable.
REVISADO POR:	En esta sección se especifica el cargo o persona responsable de la revisión de esta plantilla.	En esta sección se impregna la firma del responsable.
APROBADO POR:	En esta sección se especifica el cargo o persona responsable de la aprobación de esta plantilla.	En esta sección se impregna la firma del responsable.

Fuente: Elaboración propia

Sub proceso 3.1.2 Valoración de activos

Luego de analizar las diferentes propuestas por parte de las metodologías que realizan la valoración de activos para el proceso de SGSI se hace uso de MAGERIT; se asume una serie de características y pasos con el propósito de desarrollar este proceso en la organización:

1. Objetivos. - Conjunto de metas establecidas para lograr el cumplimiento del proceso.
   -Valorar los activos de información previamente identificados según 5 dimensiones de MAGERIT (disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad) según escala determinada por MAGERIT.
   -Los parámetros establecidos en la definición deben contar con una revisión periódica del SGSI. .

2. Personal. - Conjunto de participantes o actores que conforman el proceso.
   -Responsable de seguridad.
   -Otros involucrados que la organización determine.

3. Documentos de Entrada. - Conjunto de herramientas que son requeridas para el desarrollo de las actividades en el proceso.
   -Plantilla Identificación de Activos
   -Catálogo de elementos MAGERITv3.

4. Proceso. - Conjunto de actividades o tareas a seguir para el cumplimiento de los objetivos.
   -Valorar cada activo por su capacidad de disponibilidad.
   -Valorar cada activo por su capacidad de integridad.
   -Valorar cada activo por su capacidad de confidencialidad.
   -Valorar cada activo por su capacidad de autenticidad.
   -Valorar cada activo por su capacidad de trazabilidad.
   -Hacer uso de la escala proporcionada por MAGERIT.
   -Definir el personal encargado de elaborar el Formato y firmarlo.
   -Definir el personal encargado de revisar el Formato y firmarlo.

-Definir el personal encargado de aprobar el Formato y firmarlo.

-Completar la información contenida en la Plantilla Definición Contexto Interno.

5. Documentos de Salida. - Resultados obtenidos después de aplicar las tareas.
   -Relación de activos de TI valorados la entidad.

6. Plantilla. - Herramienta que sirve como apoyo en el desarrollo del proceso para cumplir los objetivos.

Tabla 14: Formato de valoración de activos.

LOGO DE LA ORGANIZACIÓN	**VALORACIÓN DE ACTIVOS**	
	CÓDIGO SGSI Nº _____	FECHA ELABORACIÓN: ____/____/____
		FECHA APLICACIÓN: ____/____/____
FASE: III - GESTIÓN DE RIESGOS		**PROCESO: 3.1. EVALUACIÓN DEL ACTIVO**
OBJETIVOS	-Valorar los activos de información previamente identificados según 5 dimensiones (disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad) y escala determinada por MAGERIT.	
DESCRIPCIÓN	Las valoraciones de dimensiones e impacto de cada activo son elaboradas teniendo en cuenta MAGERIT, así como sus criterios para aplicación, para mejores efectos se debe evaluar todos los aspectos mencionados en esta plantilla.	

CÓDIGO	ACTIVO	DIMENSIÓN*					IMPACTO	
		DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD	AUTENTICIDAD	TRAZABILIDAD	RANGO	VALOR

En esta sección se define el código del activo a identificar.	En esta sección se determina el activo que es identificado según el nombre técnico o común que se utiliza en la entidad.	En esta sección se valoriza el activo de acuerdo a 5 dimensiones de propiedades y características estrechamente relacionados a seguridad de la información.	En esta sección se valoriza el activo de acuerdo a 5 dimensiones de propiedades y características estrechamente relacionados a seguridad de la información.	En esta sección se valoriza el activo de acuerdo a 5 dimensiones de propiedades y características estrechamente relacionados a seguridad de la información.	En esta sección se valoriza el activo de acuerdo a 5 dimensiones de propiedades y características estrechamente relacionados a seguridad de la información.	En esta sección se valoriza el activo de acuerdo a 5 dimensiones de propiedades y características estrechamente relacionados a seguridad de la información.	En esta sección de valoriza el impacto de acuerdo a la tabla proporcionada por MAGERIT	En esta sección de valoriza el impacto de acuerdo a la tabla proporcionada por MAGERIT
…	…	…	…	…	…	…	…	…

*Para la elaboración de esta plantilla, tener en cuenta el "CATALOGO DE ELEMENTOS MAGERIT v3" pág. 15-24 donde detalla las características de cada dimensión, así como los criterios de valoración para cada dimensión.

CONCLUSIONES
En esta sección se define el comentario final o apreciación de lo observado posterior al llenado de la plantilla.

HISTORIAL DE VERSIONES		
v. x.x	FECHA: **/**/****	ELABORADO POR:
	Descripción:	
…	…	…
	…	

RESPONSABLES		**FIRMAS**
ELABORADO POR:	En esta sección se especifica el cargo o persona responsable de la elaboración de esta plantilla.	En esta sección se impregna la firma del responsable.
REVISADO POR:	En esta sección se especifica el cargo o persona responsable de la revisión de esta plantilla.	En esta sección se impregna la firma del responsable.

APROBADO POR:	En esta sección se especifica el cargo o persona responsable de la aprobación de esta plantilla.	En esta sección se impregna la firma del responsable.

Fuente: Elaboración propia

Proceso 3.2 Evaluación del riesgo.

Luego de analizar las diferentes propuestas por parte de las metodologías que determinan la evaluación del riesgo de SGSI se hace uso de MAGERIT; se asume una serie de características y pasos con el propósito de desarrollar este proceso en la organización:

1. Objetivos. - Conjunto de metas establecidas para lograr el cumplimiento del proceso.

   -Identificar las amenazas y riesgos de cada activo en la entidad.

   -Los parámetros establecidos en la definición deben contar con una revisión periódica del SGSI.

2. Personal. - Conjunto de participantes o actores que conforman el proceso.

   -Responsable de seguridad.

   -Otros involucrados que la organización determine.

3. Documentos de Entrada. - Conjunto de herramientas que son requeridas para el desarrollo de las actividades en el proceso.

   -Plantilla Valoración de Activos

   -Catálogo de elementos MAGERIT v3.

4. Proceso. - Conjunto de actividades o tareas a seguir para el cumplimiento de los objetivos.

   -Identificar las amenazas de cada activo.

   -Identificar los riesgos de cada amenaza.

   -Valorar los riesgos identificados.

   -Definir el personal encargado de elaborar el formato y firmarlo.

   -Definir el personal encargado de revisar el formato y firmarlo.

-Definir el personal encargado de aprobar el formato y firmarlo.

-Completar la información contenida en la Plantilla Evaluación del Riesgo.

5. Documentos de Salida. - Resultados obtenidos después de aplicar las tareas.
   -Relación de riesgos de TI valorados en la entidad.

6. Plantilla. - Herramienta que sirve como apoyo en el desarrollo del proceso para cumplir los objetivos.

Tabla 15: Formato de evaluación de riesgos.

LOGO DE LA ORGANIZACIÓN	**IDENTIFICACIÓN DE AMENAZAS**	
	CÓDIGO SGSI Nº _____ _	FECHA ELABORACIÓN: ____/____/____
		FECHA APLICACIÓN: ____/____/____
FASE: III - GESTIÓN DE RIESGOS		**PROCESO: 3.2. EVALUACIÓN DEL RIESGO**
OBJETIVOS	-Identificar las amenazas y riesgos de cada activo en la entidad	
DESCRIPCIÓN	Previo a la recolección de información se hace uso del análisis de los documentos de entrada.	

			RIESGO				
CÓDIGO	ACTIVO	AMENAZA	ID	RIESGO	IMPACTO	FRECUENCIA	VALORACIÓN
En esta sección se define el código del activo a identificar.	En esta sección se determina el activo que es identificado según el nombre técnico o común que se utiliza	En esta sección de determina la posible amenaza del activo respectivo y su código.	En esta sección se determina el código del riesgo.	En esta sección se determina el nivel de riesgo.	En esta sección se determina el impacto de riesgo.	En esta sección se determina la frecuencia de riesgo.	En esta sección se determina la valoración de riesgo.

	en la entidad.						
…	…	…	…	…	…	…	…

*Para la elaboración de esta plantilla, tener en cuenta la tabla de frecuencia y valor de amenazas desarrollada por MAGERIT donde detalla los datos a determinar por cada amenaza identificada.

CONCLUSIONES
En esta sección se define el comentario final o apreciación de lo observado posterior al llenado de la plantilla.

HISTORIAL DE VERSIONES		
v. x.x	FECHA: **/**/****	ELABORADO POR:
	Descripción:	
…	…	…
	…	

RESPONSABLES		**FIRMAS**
ELABORADO POR:	En esta sección se especifica el cargo o persona responsable de la elaboración de esta plantilla.	En esta sección se impregna la firma del responsable.
REVISADO POR:	En esta sección se especifica el cargo o persona responsable de la revisión de esta plantilla.	En esta sección se impregna la firma del responsable.
APROBADO POR:	En esta sección se especifica el cargo o persona responsable de la	En esta sección se impregna la firma del responsable.

	aprobación de esta plantilla.	

Fuente: Elaboración propia

Proceso 3.3 Tratamiento del riesgo.

Luego de analizar las diferentes propuestas por parte de las metodologías que determinan el tratamiento de riesgos de SGSI se hace uso de MAGERIT; se asume una serie de características y pasos con el propósito de desarrollar este proceso en la organización:

1. Objetivos. - Conjunto de metas establecidas para lograr el cumplimiento del proceso.
   -Determinar el nivel de tratamiento para los riesgos de mayor capacidad.

   -Determinar las salvaguardas para la reducción de riesgos en los activos de seguridad.
   -Los parámetros establecidos en la definición deben contar con una revisión periódica del SGSI.

2. Personal. - Conjunto de participantes o actores que conforman el proceso.
   -Responsable de seguridad.
   -Otros involucrados que la organización determine.

3. Documentos de Entrada. - Conjunto de herramientas que son requeridas para el desarrollo de las actividades en el proceso.
   -Plantilla Identificación de Activos
   -Plantilla Valoración de Activos
   -Plantilla Evaluación del Riesgo

4. Proceso. - Conjunto de actividades o tareas a seguir para el cumplimiento de los objetivos.
   -Determinar el nivel de tratamiento de riesgos.
   -Determinar las salvaguardas.
   -Definir el personal encargado de elaborar el formato y firmarlo.

-Definir el personal encargado de revisar el formato y firmarlo.

-Definir el personal encargado de aprobar el formato y firmarlo.

-Completar la información contenida en la Plantilla Tratamiento del Riesgo.

5. Documentos de Salida. - Resultados obtenidos después de aplicar las tareas.
   -Relación de salvaguardas determinados en la entidad.

6. Plantilla. - Herramienta que sirve como apoyo en el desarrollo del proceso para cumplir los objetivos.

Tabla 16: Formato de tratamiento de riesgos.

LOGO DE LA ORGANIZACIÓN	**TRATAMIENTO DEL RIESGO**	
	CÓDIGO SGSI Nº _____	FECHA ELABORACIÓN: ____/____/____
		FECHA APLICACIÓN: ____/____/____
FASE: III - GESTIÓN DE RIESGOS		**PROCESO: 3.3. TRATAMIENTO DEL RIESGO**
OBJETIVOS	-Determinar el nivel de tratamiento para los riesgos de mayor capacidad. -Determinar las salvaguardas para la reducción de riesgos en los activos de seguridad. -Los parámetros establecidos en la definición deben contar con una revisión periódica del SGSI.	
DESCRIPCIÓN	Previo a la recolección de información se hace uso del análisis de los documentos de entrada.	

ACTIVO	AMENAZA	RIESGO	TRATAMIENTO	SALVAGUARDA
En esta sección se registra el activo identificado.	En esta sección de registra el código de la amenaza.	En esta sección se registra el valor de riesgo.	En esta sección se determina el nivel de tratamiento de riesgo.	En esta sección se define los salvaguardas o actividades a realizar para tratar al riesgo
…	…	…	…	…

CONCLUSIONES
En esta sección se define el comentario final o apreciación de lo observado posterior al llenado de la plantilla.

HISTORIAL DE VERSIONES		
v. x.x	FECHA: **/**/****	ELABORADO POR:
	Descripción:	
…	…	…
	…	

RESPONSABLES		FIRMAS
ELABORADO POR:	En esta sección se especifica el cargo o persona responsable de la elaboración de esta plantilla.	En esta sección se impregna la firma del responsable.
REVISADO POR:	En esta sección se especifica el cargo o persona responsable de la revisión de esta plantilla.	En esta sección se impregna la firma del responsable.
APROBADO POR:	En esta sección se especifica el cargo o persona responsable de la aprobación de esta plantilla.	En esta sección se impregna la firma del responsable.

Fuente: Elaboración propia

FASE IV CONTROL Y EVALUACIÓN DEL SGSI

Proceso 4.1 Control del SGSI

Sub proceso 4.1.1 Monitoreo y Evaluación del SGSI

Luego de analizar las diferentes propuestas por parte de las metodologías que monitorean y evalúan el SGSI se hace uso de ISO 27000 y MSPI; se asume una serie de características y pasos con el propósito de desarrollar este proceso en la organización:

1. Objetivos. - Conjunto de metas establecidas para lograr el cumplimiento del proceso.

-Solicitar documentos básicos para registrar en la hoja de levantamiento de información desarrollada en el instrumento de monitoreo y evaluación.
- Registrar el nivel de cumplimiento de las pruebas orientadas a temas de seguridad se la información que no está directamente relacionada con las áreas de ti de la entidad.
- Registrar el nivel de cumplimiento de los controles y componentes técnicos.
- Registrar el nivel de cumplimiento de acuerdo al ciclo PHVA del SGSI.

2. Personal. - Conjunto de participantes o actores que conforman el proceso.
   -Responsable de seguridad.
   -Otros involucrados que la organización determine.

3. Documentos de Entrada. - Conjunto de herramientas que son requeridas para el desarrollo de las actividades en el proceso.
   -Plantilla Definición de Políticas y Controles SGSI
   -Plantilla Definición Procedimientos SGSI
   -Plantilla Definición Metas y Resultados SGSI
   -Plantilla Identificación de Activos
   -Plantilla Valoración de Activos
   -Plantilla Evaluación del Riesgo
   -Plantilla Tratamiento del Riesgo
   -Herramienta de monitoreo y evaluación.
   -Manual de herramienta.

4. Proceso. - Conjunto de actividades o tareas a seguir para el cumplimiento de los objetivos.
   -registrar la información solicitada en la herramienta desarrollada.
   -Definir el personal encargado de elaborar el formato y firmarlo.
   -Definir el personal encargado de revisar el formato y firmarlo.
   -Definir el personal encargado de aprobar el formato y firmarlo.
   -Completar la información contenida en la plantilla 009.

5. Documentos de Salida. - Resultados obtenidos después de aplicar las tareas.

   -Monitoreo y evaluación del SGSI

6. Plantilla. - Herramienta que sirve como apoyo en el desarrollo del proceso para cumplir los objetivos.

Tabla 17: Formato de monitoreo y evaluación SGSI.

LOGO DE LA ORGANIZACIÓN	**MONITOREO Y EVALUACIÓN SGSI**	
	CÓDIGO SGSI Nº _____	FECHA ELABORACIÓN: ____/____/____
		FECHA APLICACIÓN: ____/____/____
FASE: IV - CONTROL DEL SGSI		**PROCESO: 4.1.1 MONITOREO DEL SGSI 4.1.2 EVALUACIÓN DEL SGSI**
OBJETIVOS	- Registrar el nivel de cumplimiento de las pruebas orientadas a temas de seguridad se la información que no está directamente relacionada con las áreas de ti de la entidad. - Registrar el nivel de cumplimiento de los controles y componentes técnicos. - Registrar el nivel de cumplimiento de acuerdo a las métricas del SGSI.	
DESCRIPCIÓN	Previo a la recolección de información se hace uso del análisis de los documentos de entrada.	

INSTRUMENTO DE MONITOREO
El presente modelo cuenta con una herramienta de monitoreo y evaluación la cual sirve de apoyo en la recolección de información, análisis y evaluación asistida del SGSI
EVALUACIÓN DE CONTROLES
*Luego de hacer uso de la herramienta de monitoreo y evaluación SGSI debe insertar el diagrama de evaluación de controles

EVALUACIÓN DE CICLO DE SGSI
*Luego de hacer uso de la herramienta de monitoreo y evaluación SGSI debe insertar el diagrama de evaluación de ciclo SGSI

CONCLUSIONES
En esta sección se define el comentario final o apreciación de lo observado posterior al llenado de la plantilla.

HISTORIAL DE VERSIONES		
v. x.x	FECHA: **/**/****	ELABORADO POR:
	Descripción:	
…	…	…
	…	

RESPONSABLES		**FIRMAS**
ELABORADO POR:	En esta sección se especifica el cargo o persona responsable de la elaboración de esta plantilla.	En esta sección se impregna la firma del responsable.
REVISADO POR:	En esta sección se especifica el cargo o persona responsable de la revisión de esta plantilla.	En esta sección se impregna la firma del responsable.
APROBADO POR:	En esta sección se especifica el cargo o persona responsable de la aprobación de esta plantilla.	En esta sección se impregna la firma del responsable.

Fuente: Elaboración propia

Proceso 4.2 Definir acciones correctivas.

Luego de analizar las diferentes propuestas por parte de las metodologías que definen las acciones correctivas se hace uso de MSPI; se asume una serie de características y pasos con el propósito desarrollar este proceso en la organización:

1. Objetivos. - Conjunto de metas establecidas para lograr el cumplimiento del proceso.
   -Identificar las no conformidades suscitadas en todo el ciclo del modelo.
   -Evaluar las acciones correctivas para cada conformidad.

2. Personal. - Conjunto de participantes o actores que conforman el proceso.
   -Responsable de seguridad.
   -Otros involucrados que la organización determine.

3. Documentos de Entrada. - Conjunto de herramientas que son requeridas para el desarrollo de las actividades en el proceso.
   -Plantilla Control SGSI
   -herramienta de monitoreo y evaluación.

4. Proceso. - Conjunto de actividades o tareas a seguir para el cumplimiento de los objetivos.
   -Identificar las no conformidades presentadas en el ciclo del SGSI
   -Identificar las causas de estas no conformidades.
   -Determinar el efecto de estas.
   -Determinar las acciones correctivas para cada no conformidad.
   -Definir el personal encargado de elaborar el formato y firmarlo.
   -Definir el personal encargado de revisar el formato y firmarlo.
   -Definir el personal encargado de aprobar el formato y firmarlo.
   -Completar la información contenida en la Plantilla Definición de Acciones Correctivas.

5. Documentos de Salida. - Resultados obtenidos después de aplicar las tareas.
   -Relación de acciones correctivas a ejecutar.

6. Plantilla. - Herramienta que sirve como apoyo en el desarrollo del proceso para cumplir los objetivos.

Tabla 18: Formato de definición de acciones correctivas.

LOGO DE LA ORGANIZACIÓN	**DEFINIR ACCIONES CORRECTIVAS**	
	CÓDIGO SGSI Nº _____	FECHA ELABORACIÓN: ____/____/____
		FECHA APLICACIÓN: ____/____/____
FASE: IV - CONTROL Y EVALUACIÓN DEL SGSI		**PROCESO: 4.2 DEFINIR ACCIONES CORRECTIVAS**
OBJETIVOS	-Identificar las no conformidades suscitadas en todo el ciclo del modelo. -Evaluar las acciones correctivas para cada conformidad.	
DESCRIPCIÓN	Previo a la recolección de información se hace uso del análisis de los documentos de entrada.	

NO CONFORMIDADES	CAUSA	EFECTO	ACCIÓN CORRECTIVA
En el caso de presentarse no conformidades en la auditoria o evaluación se procede a ingresar en esta tabla	Se determina la causa o raíz de la no conformidad.	Se determina el efecto según tabla en el anexo.	Se analiza y evalúa acciones correctivas para esa no conformidad.
…	…	…	…

CONCLUSIONES
En esta sección se define el comentario final o apreciación de lo observado posterior al llenado de la plantilla.

HISTORIAL DE VERSIONES		
v. x.x	FECHA: **/**/****	ELABORADO POR:
	Descripción:	
…	…	…
	…	
RESPONSABLES		**FIRMAS**
ELABORADO POR:	En esta sección se especifica el	En esta sección se impregna la firma del responsable.

	cargo o persona responsable de la elaboración de esta plantilla.	
REVISADO POR:	En esta sección se especifica el cargo o persona responsable de la revisión de esta plantilla.	En esta sección se impregna la firma del responsable.
APROBADO POR:	En esta sección se especifica el cargo o persona responsable de la aprobación de esta plantilla.	En esta sección se impregna la firma del responsable.

Fuente: Elaboración propia

Proceso 4.3 Ejecutar plan de mejora continua.

Luego de analizar las diferentes propuestas por parte de las metodologías que ejecutan el plan de mejora continua se hace uso de MSPI; se asume una serie de características y pasos con el propósito de desarrollar este proceso en la organización:

1. Objetivos. - Conjunto de metas establecidas para lograr el cumplimiento del proceso.
   -Determinar las características de cada acción correctiva.

2. Personal. - Conjunto de participantes o actores que conforman el proceso.
   -Responsable de seguridad.
   -Otros involucrados que la organización determine.

3. Documentos de Entrada. - Conjunto de herramientas que son requeridas para el desarrollo de las actividades en el proceso.
   -Plantilla Definición Acciones Correctivas

4. Proceso. - Conjunto de actividades o tareas a seguir para el cumplimiento de los objetivos.

-Determinar el costo y tiempo de cada acción correctiva.
-Determinar la prioridad de ejecución en cada acción correctiva.
-Determinar el resultado deseado para cada acción correctiva.
-Definir el personal encargado de elaborar el formato y firmarlo.
-Definir el personal encargado de revisar el formato y firmarlo.
-Definir el personal encargado de aprobar el formato y firmarlo.
-Completar la información contenida en la Plantilla Ejecución Plan de Mejora Continua.

5. Documentos de Salida. - Resultados obtenidos después de aplicar las tareas.
   -Relación de acciones correctivas a ejecutar.

6. Plantilla. - Herramienta que sirve como apoyo en el desarrollo del proceso para cumplir los objetivos.

Tabla 19: Formato de ejecución plan de mejora continua.

<table>
<tr><td rowspan="3">LOGO DE LA ORGANIZACIÓN</td><td colspan="2">PLAN DE MEJORA CONTINUA</td></tr>
<tr><td rowspan="2">CÓDIGO SGSI Nº
_____</td><td>FECHA ELABORACIÓN:
____/____/____</td></tr>
<tr><td>FECHA APLICACIÓN:
____/____/____</td></tr>
<tr><td colspan="2">FASE: IV - CONTROL Y EVALUACIÓN DEL SGSI</td><td>PROCESO: 4.3 EJECUTAR PLAN DE MEJORA CONTINUA.</td></tr>
<tr><td>OBJETIVOS</td><td colspan="2">-Determinar las características de cada acción correctiva.</td></tr>
<tr><td>DESCRIPCIÓN</td><td colspan="2">Previo a la recolección de información se hace uso del análisis de los documentos de entrada.</td></tr>
</table>

ACCIÓN CORRECTIVA	COSTO	TIEMPO	PRIORIDAD	RESULTADO
Acciones correctivas previamente identificadas	Costo de implementación.	Tiempo determinado para la implementación.	Orden de prioridad según anexo.	Se determina el resultado de la acción correctiva ejecutada.
…	…	…	…	…

CONCLUSIONES
En esta sección se define el comentario final o apreciación de lo observado posterior al llenado de la plantilla.

HISTORIAL DE VERSIONES		
v. x.x	FECHA: **/**/****	ELABORADO POR:
	Descripción:	
…	…	…
	…	

RESPONSABLES		**FIRMAS**
ELABORADO POR:	En esta sección se especifica el cargo o persona responsable de la elaboración de esta plantilla.	En esta sección se impregna la firma del responsable.
REVISADO POR:	En esta sección se especifica el cargo o persona responsable de la revisión de esta plantilla.	En esta sección se impregna la firma del responsable.
APROBADO POR:	En esta sección se especifica el cargo o persona responsable de la aprobación de esta plantilla.	En esta sección se impregna la firma del responsable.

Fuente: Elaboración propia

Además de ello para apoyo del evaluador o especialista a implementar el SGSI en los hospitales se elaboró un documento de apoyo donde aloja los elementos y características a evaluar, así como los rangos y criterios de evaluación en algunas plantillas, para mayor detalle consultar el ANEXO 06.

En la etapa de monitoreo y evaluación del SGSI se desarrolló una herramienta para facilitar la recolección de información y procesar el cumplimiento de los controles, dicha herramienta fue desarrollada en hoja de cálculo. La herramienta presenta de forma gráfica del avance y cumplimiento del SGSI en las instituciones a implementar, dicha herramienta se aloja en el ANEXO 07.

3.3 Validar la funcionalidad del modelo de sistema de gestión de seguridad de la información en base a indicadores.

Previo a la elaboración del modelo se procedió a validar la herramienta de diagnóstico la cual contaba con 10 ítems relacionando los indicadores y variables a evaluar, los criterios de evaluación fueron:

- Relación entre la variable y dimensión.
- Relación entre la dimensión y el indicador.
- Relación entre el indicador y el ítem.
- Relación entre el ítem y la opción de respuesta.

Los valores de evaluación fueron determinados en escala de Likert de mínimo 01 y máximo 05, además de recabar las observaciones y recomendaciones de cada ítem.

Dicha evaluación fue presentada a 03 magister expertos en el tema, las plantillas de evaluación de la herramienta de diagnóstico se encuentran en el ANEXO 08.

Teniendo el modelo elaborado, estructurado y con las plantillas correspondientes se procedió a verificar la validez del modelo propuesto en relación a la suficiencia, claridad, coherencia y relevancia de los procesos considerados. La evaluación se realiza mediante escala de Likert de mínimo 1 y máximo 4 especificando los indicadores en cada categoría. Además, se obtiene las observaciones del evaluador. Este modelo fue evaluado por 3 magister expertos en el tema, la evaluación obtenida se encuentra contenida en el ANEXO 09.

Posteriormente se validó el modelo desarrollado mediante la aprobación de 3 expertos del tema, estos datos fueron analizados mediante el coeficiente de concordancia adoptado por

la prueba V de Aiken para establecer la medida de acuerdo entre los expertos con respecto al modelo de Gestión de Seguridad de la Información.

Se analizó si el valor de α sobrepasa el nivel crítico de 0.80. A través del programa informático Excel se obtuvo el siguiente nivel de concordancia:

Tabla 20: Resultados de V de Aiken para modelo desarrollado.

	Suficiencia	Claridad	Coherencia	Relevancia
N	3	3	3	3
V de Aiken (α)	0.90	0.85	0.93	0.96

Fuente: Excel

Por último, de acuerdo a los resultados alcanzados en la evaluación del Coeficiente de V de Aiken se concluye:

- Existe una concordancia entre los expertos de 0.91 sobrepasando el nivel necesario para evidenciar la validez.
- El modelo de gestión de seguridad de la información SGSI cuenta con un nivel aceptable de α denotando relación en las respuestas de los 3 expertos.

3.4 Aplicar el modelo de gestión de seguridad de la información.

A raíz de la situación actual que se vive actualmente producto de la pandemia, se propuso la aplicación parcial del modelo, seleccionando la institución 01 previamente identificada solicitando el permiso respectivo contenido en el ANEXO 10, donde se designó al jefe de TI para la selección de áreas y procesos críticos, la aplicación de las 4 fases del SGSI en el Almacén Especializado de Medicamentos (AEM) del caso de estudio, por contar con procesos críticos dentro de la farmacia y contar con más del 60% de activos de información bajo responsabilidad.

Luego de aplicar el modelo, los resultados por parte de la herramienta de monitoreo fueros los siguientes:

Tabla 21: Resultados de modelo aplicado.

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	70	100	GESTIONADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	33	100	REPETIBLE
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	54	100	EFECTIVO
A.8	GESTIÓN DE ACTIVOS	32	100	REPETIBLE
A.9	CONTROL DE ACCESO	70	100	GESTIONADO
A.10	CRIPTOGRAFÍA	0	100	INEXISTENTE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	40	100	REPETIBLE
A.12	SEGURIDAD DE LAS OPERACIONES	39	100	REPETIBLE
A.13	SEGURIDAD DE LAS COMUNICACIONES	10	100	INICIAL
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	0	100	INEXISTENTE
A.15	RELACIONES CON LOS PROVEEDORES	0	100	INEXISTENTE
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	23	100	REPETIBLE
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	20	100	INICIAL
A.18	CUMPLIMIENTO	37.5	100	REPETIBLE
PROMEDIO EVALUACIÓN DE CONTROLES		31	100	REPETIBLE

Fuente: Propia

Lo que determina un importante avance al obtener un 31% de efectividad en los controles. Así mismo especificar que las políticas de seguridad de la información y controles de acceso (lógico y físicos) obtuvieron un 70% de avance.

El ANEXO 11 contiene la conformidad de la aplicación parcial.

El ANEXO 12 contiene las plantillas aplicadas para el caso de uso.

Discusión

- La presente investigación, discrepa con **Mora** en la perspectiva adoptada en su trabajo donde utiliza ISO 27000 para la clasificación de activos, dado que los criterios de selección utilizados por la norma son enfocados a activos de información independientemente del medio. El investigador emplea el modelo MAGERIT para la valoración de activos por medio de 5 factores relevantes en la seguridad de la información (disponibilidad, integridad, confidencialidad, trazabilidad y autenticidad) ya que son ligeras y sencillas de implementar en el contexto de la investigación.

- Para realizar modelo SGSI, Bornas [14] inicia realizando un análisis en la naturaleza del sector donde implementa el modelo. Asimismo, la presente investigación concuerda con dicha iniciativa del análisis realizado antes de desarrollar el modelo, sin embargo, Bornas desarrolla la herramienta de diagnóstico del sector basado en la norma ISO 27001 mientras que esta investigación lo complementa desarrollando la encuesta basada en COBIT 2019 por su adaptabilidad en organizaciones de pequeña a mediana escala.

- Lo mismo guarda similitud con investigaciones como el de **Ruíz**, en relación a los roles y perfiles del modelo contando con un comité de seguridad y responsable de la seguridad de la información. Sin embargo, esta investigación complementa los perfiles de actores en el modelo definiendo un tercer rol (equipo de proyecto) el cual tiene responsabilidades operativas en la implementación del proyecto.

- La investigación se desarrolló mediante el ciclo planear, hacer, verificar y actuar (PHVA), permitiendo una implementación ágil e iterativa, coincidiendo en este aspecto con la investigación de Safonova y Kotelnikov [12] y Gonzales [8].

CONCLUSIONES

La presente investigación permitió determinar las siguientes conclusiones:

Se armonizó los estándares de gestión de seguridad de la información basado en criterios obtenidos por la herramienta de diagnóstico situacional adaptando al contexto de los procesos de las farmacias en los hospitales II-I de la región Amazonas.

Se elaboró un modelo para la gestión de seguridad de la información adecuado a los hospitales II-I. La misma que abarca desde el diagnóstico de la organización, establecimientos del modelo, gestión de riesgos y evaluación del SGSI .

El modelo propuesto fue sometido a evaluación por parte de expertos en el tema, con el fin de determinar su aplicabilidad, contando con la aprobación y contando con un 91% de validez.

Se logró aplicar el modelo a la organización a fin de evaluar su desempeño, identificando amenazas y determinando procesos que fortalezcan la seguridad de la información en los procesos de la farmacia obteniendo un 30% de implementación de controles.

RECOMENDACIONES

- Para futuras investigaciones, se recomienda fusionar el presente modelo con estándares y normativas enfocados en continuidad del negocio. Así mismo un Sistema de Continuidad del Negocio (SGCN) alineado a los procesos del SGSI pueden brindar una amplia gama de posibilidades en la gestión de riesgos.

- En próximas investigaciones se recomienda ahondar también en riesgos no solo de Seguridad de la Información, sino también en Tecnologías de la Información puesto que este modelo es el punto de partida para lograr una gestión de riesgos completa, especificando algunos procesos enfocados a gestión de riesgos de diferente índole.

- Para obtener un mayor grado de validez en la herramienta de diagnóstico situacional se recomienda basarse estructuralmente de algún estándar o marco de trabajo además de aplicar la concordancia de expertos en la validación. De esta manera la herramienta cuenta con 2 tipos de validaciones correctamente aplicadas, como es el caso de esta investigación.

REFERENCIAS BIBLIOGRÁFICAS

[1] CCN-CERT, «Ciberamenazas y Tendencias 2019,» *CCN-CERT Resumen Ejecutivo,* vol. 13, nº 19, pp. 1-48, 2019.

[2] Verizon, «Data Breach Investigations Reports 2020,» *DBIR 2020,* vol. 20, p. 31, 2020.

[3] ESET, «Eset Security Report Latinoamerica,» *Eset Security Report Latinoamerica,* vol. 20, pp. 1-28, 2019.

[4] J. M. Harán, «We live security,» 06 04 2020. [En línea]. Available: https://www.welivesecurity.com/la-es/2020/04/06/crecen-ataques-ransomware-dirigidos-hospitales/. [Último acceso: 08 05 2020].

[5] C. Cimpanu, «Czech hospital hit by cyberattack while in the midst of a COVID-19 outbreak,» *ZDNet,* pp. 1-5, 13 03 2020.

[6] C. Cimpanu, «ZDNet,» *FBI re-sends alert about supply chain attacks for the third time in three months,* pp. 1-3, 31 03 2020.

[7] J. M. Harán, «We Live Security,» 07 08 2018. [En línea]. Available: https://www.welivesecurity.com/la-es/2018/08/07/datos-personales-pacientes-mexico-expuestos-internet/. [Último acceso: 04 06 2020].

[8] C. A. G. Durango, Metodologia integradora para simplificar la implementacion de los componentes de un sistema de gestion de la informacion (SGSI), en pequeñas y medianas empresas del sector de la informacion y comunicaciones en la ciudad de Medellin, Medellin: Instituto Tecnológico Metropolitano, 2019.

[9] C. E. E. G. M. d. l. L. S. P. Juan Alberto Ruíz Tapia, PROPUESTA DE UN MODELO DE UN SISTEMA DE GESTIÓN DE CALIDAD EN SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001 PARA

INSTITUCIONES EDUCATIVAS, Mexico: Universidad Autónoma del Estado de México, 2020.

[10] R. D. O. E. Z. M. I. E. D. K. Janeth Mora Secaira, El sistema de gestión de seguridad de la información bajo la norma NTE ISO/IEC 27001 en instituciones de Educación Superior (Ecuador)., Cuba: revista científico - educacional de la provincia Granma., 2020.

[11] F. K. ,. S. G. Elham Rostami ∗, Requirements for computerized tools to design information security policies, Sweden: ScienseDirect, 2020.

[12] N. K. O.M. Safonova, Modeling the information security management system (ISMS) of a medical organization, Irkutsk: Irkutsk National Research Technical University, 2020.

[13] J. A. Jara Arenas, FRAMEWORK DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LOS CONTROLES DE LA ISO 27002 PARA EL PROCESO ACADÉMICO DE LA UNT., Trujillo: UNIVERSIDAD PRIVADA ANTENOR ORREGO, 2019.

[14] W. M. B. RIOS, MODELO DE ANÁLISIS PARA LA IMPLANTACIÓN DE UN SGSI BASADO EN ISO 27001 y COBIT PARA UNA EMPRESA DEL SECTOR EDUCACIÓN, Arequipa: UNIVERSIDAD NACIONAL DE SAN AGUSTÍN DE AREQUIPA, 2020.

[15] N. R. N. MORANTE, MODELO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN – SGSI, PARA FORTALECER LA CONFIDENCIALIDAD, INTEGRIDAD, DISPONIBILIDAD Y MONITOREAR LOS ACTIVOS DE INFORMACIÓN PARA EL INSTITUTO NACIONAL DE ESTADÍSTICA E INFORMÁTICA - INEI FILIAL LAMBAYEQUE., Lambayeque: Universidad Nacional Pedro Ruiz Gallo, 2020.

[16] M. d. T. d. l. I. y. l. Comunicaciones, Modelo de Seguridad y Privacidad de la Información, Bogotá: MINTIC, 2016.

[17] O. I. d. Normalización, ISO/IEC 27001, Ginebra: ISO/IEC, 2016.

[18] ISACA, Guía de diseño COBIT® 2019: Diseño de una solución de Gobierno de Información y Tecnología, Schaumburg: ISACA, 2018.

[19] ISACA, ISACA Glorrary of Terms, Madrid: ISACA, 2015.

[20] M. d. Salud, INDICADORES DE GESTIÓN Y EVALUACIÓN HOSPITALARIA, PARA HOSPITALES, INSTITUTOS Y DIRESA, Lima: Minsa, 2013.

[21] M. d. Salud, NORMA TÉCNICA DE SALUD "CATEGORIAS DE ESTABLECIMIENTOS DEL SECTOR SALUD" V.02, Lima: Minsa, 2006.

[22] M. d. Salud, NORMA TÉCNICA DE SALUD "CATEGORÍAS DE ESTABLECIMIENTOS DEL SECTOR SALUD", Lima: Minsa, 2011.

[23] M. d. H. y. A. Públicas, Metodologia de Analisis y gestion de Riesgos de los Sistemas de Informacion, Madrid: administración electrónica, 2013.

[24] Andina, «Andina,» 08 2017. [En línea]. Available: https://andina.pe/Agencia/noticia-cibercriminales-hackean-diversas-paginas-lima-y-provincias-679005.aspx. [Último acceso: 13 06 2020].

ANEXOS

Anexo 01: Esquema de herramienta de diagnóstico.

PROCESO COBIT 2019			PREGUNTA	TIPO DE PREGUNTA
PRACTICA GESTION	PRACTICA GOBIERNO	ACTIVIDAD		
EDM01	EDM01.01	Analizar e identificar los factores ambientales internos y externos (obligaciones legales, regulatorias y contractuales), así como las tendencias en el entorno de negocio que pueden influir en el diseño del gobierno.	¿La institución cuenta con un Plan Estratégico?	CERRADA DE OPCION MULTIPLE
APO01	APO01.01	Adquirir el conocimiento de la visión, dirección y estrategia empresarial, así como el contexto empresarial actual y sus desafíos.		
APO01	APO01.04	Definir el alcance, foco, mandato y responsabilidades de cada función dentro de la organización de I&T, en línea con la dirección de gobierno.	¿La institución cuenta con un Manual Organización y Funciones donde incluya responsabilidades de información para cada trabajador?	CERRADA DE OPCION MULTIPLE
DSS06	DSS06.03	Asignar roles y responsabilidades conforme a las descripciones del cargo y las actividades aprobadas del proceso de negocio.		
EDM02	EDM02.01	Identificar las categorías generales de sistemas de información, aplicaciones, datos, servicios de TI, infraestructura, activos de I&T, recursos, habilidades, prácticas, controles y relaciones de TI necesarias para respaldar la estrategia empresarial	¿La institución cuenta con un Plan Estratégico de Tecnologías de la Información o documento similar?	CERRADA DE OPCION MULTIPLE
EDM02	EDM02.04	Recopilar datos relevantes, oportunos, completos, creíbles y precisos para informar sobre el progreso a la hora de la entrega de valor en comparación con los objetivos. Obtener una vista resumen general de 360º del rendimiento del portafolio, programa y de I&T (capacidades técnicas y operativas) que respalden la toma de decisiones. Asegurar el logro de los resultados esperados.		
APO02	APO02.03	Definir objetivos y metas de I&T de alto nivel y especificar su contribución a los objetivos empresariales.		

APO03	APO03.01	Confirmar y elaborar los principios de arquitectura, incluyendo los principios empresariales. Asegurar que todas las definiciones existentes estén actualizadas. Aclarar cualquier aspecto ambiguo.		
APO03	APO03.02	Mantener un repositorio de arquitectura, que contiene estándares, componentes reutilizables, los artefactos de modelado, las relaciones, las dependencias y las visualizaciones, para permitir la uniformidad de la organización y mantenimiento de la arquitectura.		
DSS05	DSS05.04	Identificar de forma unívoca y por roles funcionales todas las actividades de procesamiento de información. Coordinarse con las unidades de negocio para asegurarse de que todos los roles están definidos de manera consistente, incluidos los roles definidos por el propio negocio dentro de las aplicaciones de procesos del negocio.		
DSS05	DSS05.05	Registrar y monitorizar todos los puntos de entrada a las instalaciones de TI. Registrar a todos los visitantes al sitio, incluidos contratistas y proveedores.		
EDM03	EDM03.01	Conocer la organización y su contexto en relación al riesgo de I&T.	¿La institución cuenta con una Política de Gestión de Riesgos de Tecnologías de la Información o similar?	CERRADA DE OPCION MULTIPLE
EDM03	EDM03.01	Determinar los niveles de tolerancia al riesgo frente al apetito al riesgo, es decir, las desviaciones aceptables temporalmente del apetito al riesgo.		
APO12	APO12.01	Registrar datos relevantes y significativos relacionados con los riesgos de I&T en el entorno operativo interno y externo de la empresa.		
APO12	APO12.01	Estudiar y analizar los datos históricos de riesgo de I&T y de pérdidas experimentadas a partir de datos y tendencias externos disponibles, homólogos de la industria a través de logs de eventos de la industria, bases de datos, y acuerdos de la industria, para la publicación común de eventos.		
APO13	APO13.02	Formular y mantener un plan de tratamiento de riesgos de seguridad de la información alineado con objetivos estratégicos y la arquitectura empresarial. Asegurar que el plan identifique las prácticas de gestión y las soluciones de seguridad apropiadas y óptimas, con los recursos, responsabilidades y prioridades asociados para la gestión de los riesgos de seguridad de la información identificados.		
APO14	APO14.03	Desarrollar y usar los metadatos para realizar un análisis del impacto de los posibles cambios en los datos.		
BAI04	BAI04.01	Definir un plan de aseguramiento de la calidad, incluidos, por ejemplo, la especificación de los criterios de calidad, procesos de validación y verificación, definición sobre cómo se revisará la calidad, cualificaciones necesarias de los revisores de la calidad, y roles y responsabilidades para lograr la calidad.		

BAI04	BAI04.02	Determinar el impacto de los escenarios en las medidas de rendimiento del negocio (p. ej., ingresos, beneficios, servicios al cliente). Involucrar a los líderes regionales, funcionales (sobre todo de finanzas) y de la línea del negocio para entender su evaluación del impacto.		
APO01	APO01.01	Considerar el entorno interno de la empresa, incluyendo la cultura y filosofía de gestión, la tolerancia al riesgo, la política de seguridad y privacidad, los valores éticos, el código de conducta, la rendición de cuentas y los requisitos para la integridad de la gestión.	¿La institución cuenta con una política de seguridad de la información o similar?	CERRADA DE OPCION MULTIPLE
APO01	APO01.09	Crear una serie de políticas para mejorar las expectativas de control de IT en temas clave relevantes, como la calidad, la seguridad, la privacidad, los controles internos, el uso de activos de I&T, la ética y los derechos de propiedad intelectual.		
APO13	APO13.01	Definir un SGSI conforme a la política empresarial y el contexto en el que opera la empresa.		
APO13	APO13.01	Definir y comunicar los roles y responsabilidades de la gestión de seguridad de la información.		
BAI02	BAI02.01	Asegurar que los requisitos cumplan con las políticas y estándares empresariales, arquitectura empresarial, planes estratégicos y tácticos de I&T, procesos de negocios y de TI internos y externalizados, requisitos de seguridad, requisitos regulatorios, competencias del personal, estructura organizativa, caso de negocio y tecnología facilitadora.		
BAI02	BAI02.04	Asegurar que el patrocinador del negocio o dueño del producto realice la elección final de la solución, estrategia de adquisición y diseño de alto nivel, de acuerdo con el caso de negocio. Obtener las aprobaciones necesarias de las partes interesadas afectadas (p. ej. dueño del proceso de negocio, arquitecto empresarial, director de operaciones, director de seguridad de la información, director de privacidad).		
DSS01	DSS01.05	Asegurar que las instalaciones de TI cumplen con la legislación, regulaciones y, directrices de salud y seguridad y, las especificaciones de proveedores relevantes.		
DSS05	DSS05.01	Instalar y activar herramientas de protección contra software malicioso en todas las instalaciones de procesamiento, con archivos de definición de software malicioso que se actualizan según sea necesario (automáticamente o semiautomáticamente)		
APO01	APO01.07	Proporcionar las directrices para garantizar la clasificación adecuada y consistente de los elementos de información en toda la empresa.	¿La institución cuenta con una Directiva de	

APO01	APO01.07	Crear y mantener un inventario de información (sistemas y datos) que incluyan una lista de Dueños, custodios y clasificaciones. Incluir sistemas que sean externalizados y aquellos cuya propiedad debería estar dentro de la empresa.	Inventario y Gestión de Activos de Información o similar?	CERRADA DE OPCION MULTIPLE
APO01	APO01.07	Evaluar y distinguir entre datos, información y sistemas críticos (de alto valor) y no críticos. Asegurar la protección adecuada para cada categoría.		
APO12	APO12.03	Hacer un inventario de los procesos de negocio y documentar su dependencia con los procesos de gestión de servicios de I&T y los recursos de infraestructura de TI. Identificar el personal de apoyo, aplicaciones, infraestructura, instalaciones, registros manuales críticos, contratistas, proveedores, y terceros.		
APO14	APO14.01	Establecer una función de gestión de los datos con responsabilidad de gestionar las actividades que respalden los objetivos de gestión de los datos.		
APO14	APO14.01	Especificar roles y responsabilidades para respaldar la gestión de los datos y la interacción entre el gobierno y la función de gestión de datos.		
APO14	APO14.03	Desarrollar y usar los metadatos para realizar un análisis del impacto de los posibles cambios en los datos.		
APO14	APO14.04	Asegurar que la estrategia de calidad de los datos se respete en toda la organización y venga acompañada de las políticas, procesos y directrices correspondientes.		
APO14	APO14.04	Definir una estrategia de calidad de los datos en colaboración con las partes interesadas empresariales y tecnológicas, aprobada y gestionada por la dirección ejecutiva. La estrategia debería favorecer pasar del estado actual al objetivo. También debe alinearse de forma explícita con los objetivos empresariales y la estrategia de gestión de datos de la organización.		
APO14	APO14.07	Mantener un historial de cambio de datos a través de actividades de depuración.		
APO14	APO14.08	Asignar y alinear los requisitos de los consumidores y productores de datos.		
APO14	APO14.09	Usar la política y los procesos para controlar el acceso, transmisión y modificaciones a datos históricos y archivados.		
BAI03	BAI03.06	Definir un plan de aseguramiento de la calidad, incluidos, por ejemplo, la especificación de los criterios de calidad, procesos de validación y verificación, definición sobre cómo se revisará la calidad, cualificaciones necesarias de los revisores de la calidad, y roles y responsabilidades para lograr la calidad.		
BAI08	BAI08.01	Clasificar las fuentes de información con base en el esquema de clasificación de contenidos (p. ej. el modelo de arquitectura de la información). Correlacionar las fuentes de información con el esquema de clasificación.		

BAI09	BAI09.01	Identificar todos los activos adquiridos en un registro de activos que recoja el estado actual. Los activos se reportan en la hoja del balance; se compran o crean para aumentar el valor de una compañía o beneficiar las operaciones de la empresa (p. ej. hardware y software). Identificar todos los activos adquiridos y mantener el alineamiento con los procesos de gestión de la configuración y gestión de cambios, el sistema de gestión de la configuración y los datos de contabilidad financiera.		
BAI09	BAI09.02	Identificar activos que son críticos para proporcionar la capacidad de servicio mediante la referencia a los requisitos en las definiciones de servicio, los SLA y el sistema de gestión de la configuración.		
BAI09	BAI09.03	Obtener, recibir, verificar, probar y registrar todos los activos de forma controlada, incluyendo etiquetas físicas, cuando se requiera.		
DSS05	DSS05.02	Encriptar la información en tránsito de acuerdo a su clasificación.		
DSS05	DSS05.06	Establecer un inventario de documentos sensibles y dispositivos de salida y realizar reconciliaciones periódicas.		
DSS06	DSS06.06	Restringir el uso, distribución y el acceso físico a la información de acuerdo con su clasificación.		
APO07	APO07.03	Desarrollar y ofrecer programas de capacitación conforme a los requisitos del proceso y organizativos, incluidos los requisitos para el conocimiento empresarial, control interno, conducta ética, seguridad y privacidad.	¿La institución proporciona capacitaciones sobre Seguridad de la Información a los trabajadores dentro y fuera de TI?	CERRADA DE OPCION MULTIPLE
APO13	APO13.02	Implementar programas de formación y concienciación sobre seguridad de la información y privacidad.		
BAI08	BAI08.03	Transferir el conocimiento a los usuarios del conocimiento, con base en un análisis de brechas de necesidades y técnicas de aprendizaje efectivas. Crear un entorno, herramientas y artefactos que respalden el intercambio y la transferencia de conocimiento. Asegurar que se cuenta con los controles de acceso adecuados, en línea con la clasificación de conocimiento definida.		
DSS06	DSS06.06	Proporcionar una concienciación y formación adecuada sobre el uso.		
APO11	APO11.01	Obtener insumos de la dirección y las partes interesadas externas e internas sobre la definición de los requisitos de calidad y los criterios de gestión de la calidad.	¿La institución cuenta con un Plan de Gestión de la Calidad de la Información, donde detalle los requisitos	CERRADA DE OPCION MULTIPLE
BAI01	BAI01.07	Identificar las tareas y prácticas de aseguramiento requeridas para respaldar la acreditación de sistemas nuevos o modificados durante la planificación del programa e incluirlos en los planes integrados. Asegurar que las tareas proporcionen aseguramiento de que los controles internos y las soluciones de seguridad/privacidad satisfacen los requisitos definidos.		

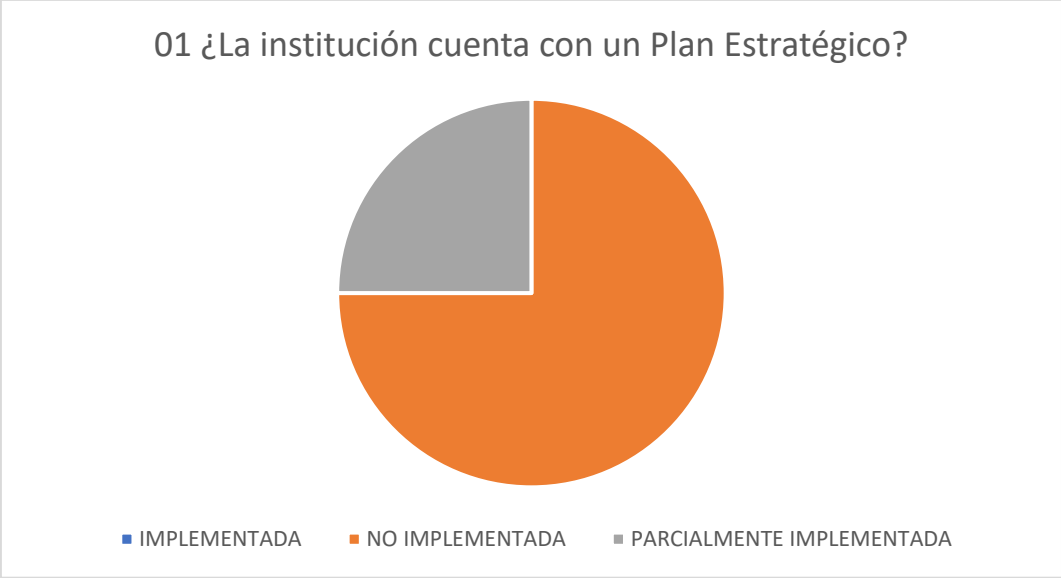
BAI11	BAI11.05	Para proporcionar el aseguramiento de la calidad de los entregables del proyecto, identificar la propiedad y las responsabilidades, procesos de revisión de la calidad, criterios de éxito y métricas de rendimiento.	mínimos y criterios de los mismos?	
APO14	APO14.10	Definir una programación para garantizar una copia de seguridad (backup) correcta de todos los datos críticos.	¿La institución cuenta con un Plan de copias de seguridad y restauración?	CERRADA DE OPCION MULTIPLE
BAI03	BAI03.02	Diseñar el almacenamiento, ubicación, recuperación y mecanismos de recuperación de los datos.		
BAI03	BAI03.02	Diseñar la redundancia, recuperación y copias de seguridad adecuadas.		
DSS04	DS04.07	Hacer una copia de seguridad de los sistemas, aplicaciones, datos y documentación conforme a un calendario definido. Considerar una frecuencia (mensual, semanal, diario, etc.), modo de copia de seguridad (p. ej., disk mirroring para copias de seguridad en tiempo real frente a DVD-ROM para retención a largo plazo), tipo de copia de seguridad (p.ej., completa vs. incremental), y tipo de medios. Considerar también copias de seguridad online automatizadas, tipos de datos (p. ej. voz, ópticos), creación de logs, datos críticos de computación de usuario final (p. ej., hojas de cálculo), ubicación física y lógica de las fuentes de datos, derechos de acceso y seguridad, y encriptación.		
APO14	APO14.10	Definir una programación para garantizar una copia de seguridad (backup) correcta de todos los datos críticos.		
DSS04	DSS04.07	Hacer una copia de seguridad de los sistemas, aplicaciones, datos y documentación conforme a un calendario definido. Considerar una frecuencia (mensual, semanal, diario, etc.), modo de copia de seguridad (p. ej., disk mirroring para copias de seguridad en tiempo real frente a DVD-ROM para retención a largo plazo), tipo de copia de seguridad (p.ej., completa vs. incremental), y tipo de medios. Considerar también copias de seguridad online automatizadas, tipos de datos (p. ej. voz, ópticos), creación de logs, datos críticos de computación de usuario final (p. ej., hojas de cálculo), ubicación física y lógica de las fuentes de datos, derechos de acceso y seguridad, y encriptación.	¿Con que frecuencia realiza copias de seguridad de la información?	ESCALA LIKERT

Anexo 02: Respuesta de cuestionario.

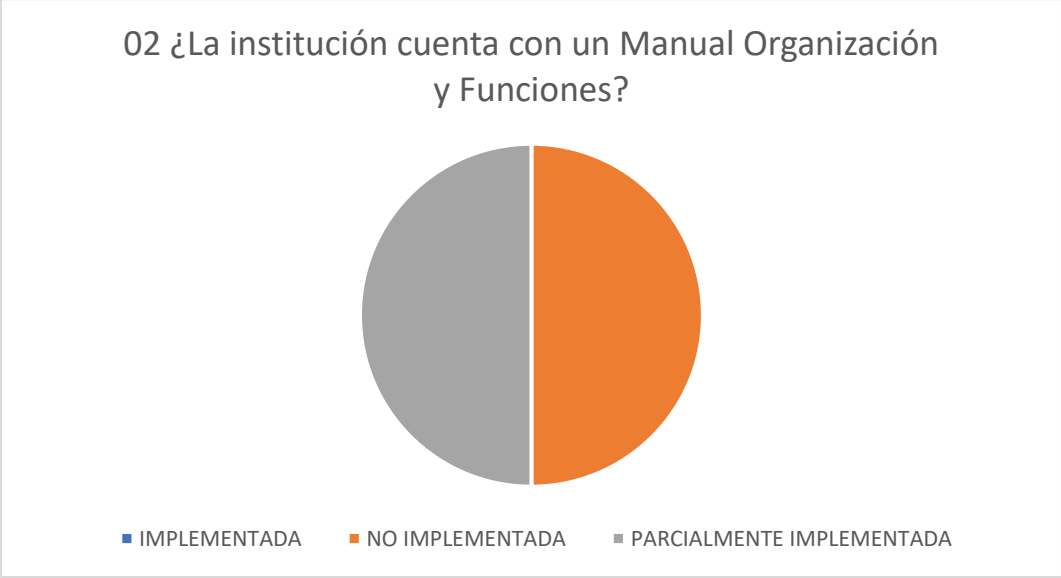
NRO	PREGUNTA	RESPUESTA			
		INSTITUCION 01	INSTITUCION 02	INSTITUCION 03	INSTITUCION 04
01	¿La institución cuenta con un Plan Estratégico?	No Implementada	No Implementada	Parcialmente Implementada	No Implementada
02	¿La institución cuenta con un Manual Organización y Funciones donde incluya responsabilidades de información para cada trabajador?	Parcialmente Implementada	No Implementada	No Implementada	Parcialmente Implementada
03	¿La institución cuenta con un Plan Estratégico de Tecnologías de la Información o documento similar?	No Implementada	No Implementada	No Implementada	No Implementada
04	¿La institución cuenta con una Política de Gestión de Riesgos de Tecnologías de la Información o similar?	No Implementada	No Implementada	No Implementada	No Implementada
05	¿La institución cuenta con una política de seguridad de la información o similar?	No Implementada	No Implementada	No Implementada	No Implementada
06	¿La institución cuenta con una Directiva de Inventario y Gestión de Activos de Información o similar?	No Implementada	No Implementada	No Implementada	No Implementada
07	¿La institución proporciona capacitaciones sobre Seguridad de la Información a los trabajadores dentro y fuera de TI?	No Implementada	No Implementada	No Implementada	No Implementada
08	¿La institución cuenta con un Plan de Gestión de la Calidad de la Información, donde detalle los requisitos mínimos y criterios de los mismos?	No Implementada	No Implementada	No Implementada	No Implementada
09	¿La institución cuenta con un Plan de copias de seguridad y restauración?	Parcialmente Implementada	No Implementada	Parcialmente Implementada	Parcialmente Implementada
10	¿Con que frecuencia realiza copias de seguridad de la información?	Casi siempre	Nunca	Casi siempre	Casi siempre

Anexo 03: Diagrama de respuestas.

NRO	PREGUNTA	RESPUESTA		
		IMPLEMENTADA	NO IMPLEMENTADA	PARCIALMENTE IMPLEMENTADA
01	¿La institución cuenta con un Plan Estratégico?	0	3	1



NRO	PREGUNTA	RESPUESTA		
		IMPLEMENTADA	NO IMPLEMENTADA	PARCIALMENTE IMPLEMENTADA
02	¿La institución cuenta con un Manual Organización y Funciones?	0	2	2

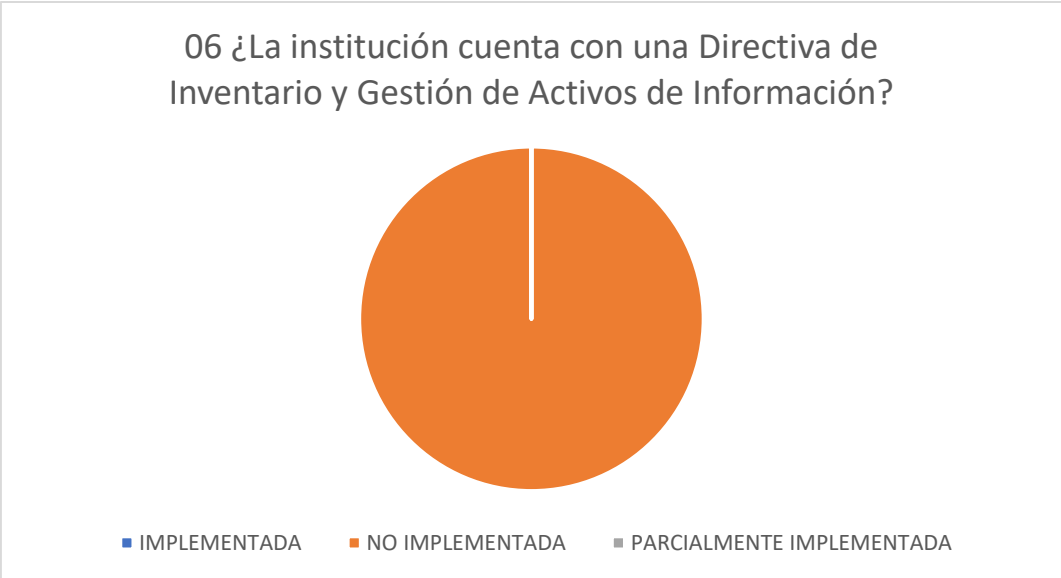


NRO	PREGUNTA	RESPUESTA		
		IMPLEMENTADA	NO IMPLEMENTADA	PARCIALMENTE IMPLEMENTADA
03	¿La institución cuenta con un Plan Estratégico de Tecnologías de la Información?	0	4	0

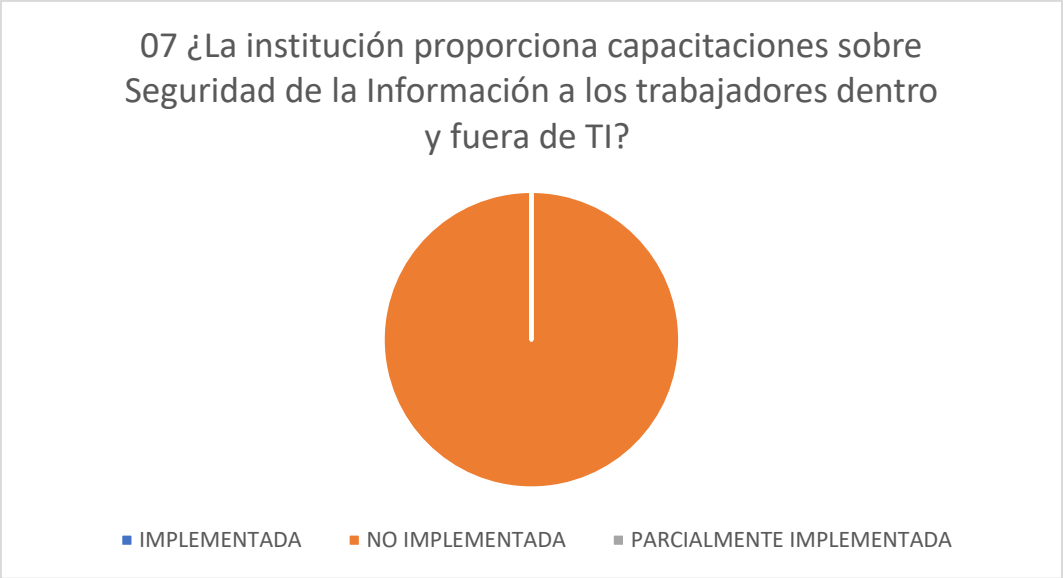
NRO	PREGUNTA	RESPUESTA		
		IMPLEMENTADA	NO IMPLEMENTADA	PARCIALMENTE IMPLEMENTADA
04	¿La institución cuenta con una Política de Gestión de Riesgos de Tecnologías de la Información?	0	4	0

NRO	PREGUNTA	RESPUESTA		
		IMPLEMENTADA	NO IMPLEMENTADA	PARCIALMENTE IMPLEMENTADA
05	¿La institución cuenta con una Política de seguridad de la información?	0	4	0

NRO	PREGUNTA	RESPUESTA		
		IMPLEMENTADA	NO IMPLEMENTADA	PARCIALMENTE IMPLEMENTADA
06	¿La institución cuenta con una Directiva de Inventario y Gestión de Activos de Información?	0	4	0



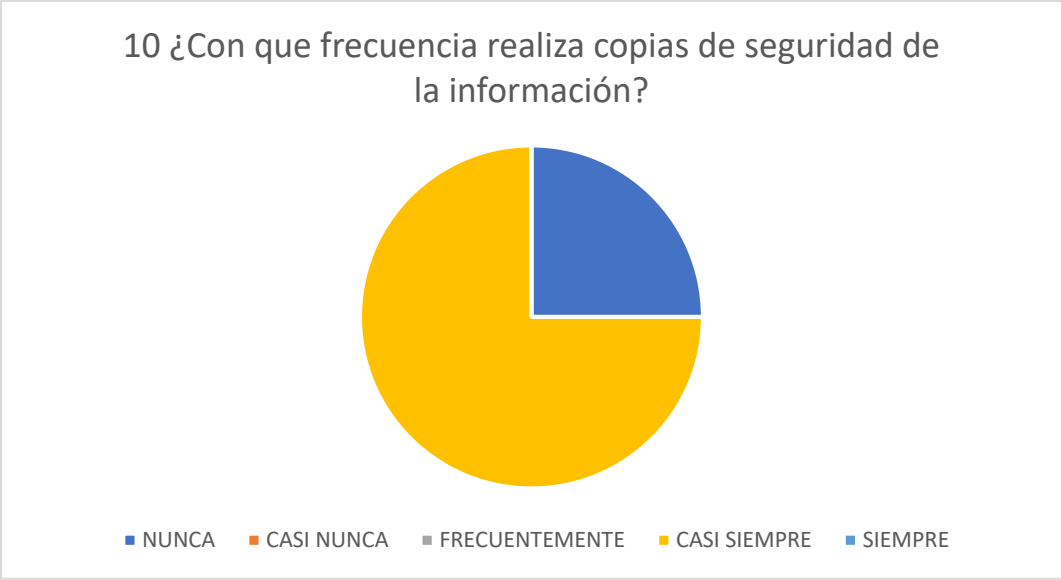
NRO	PREGUNTA	RESPUESTA		
		IMPLEMENTADA	NO IMPLEMENTADA	PARCIALMENTE IMPLEMENTADA
07	¿La institución proporciona capacitaciones sobre Seguridad de la Información a los trabajadores dentro y fuera de TI?	0	4	0



NRO	PREGUNTA	RESPUESTA		
		IMPLEMENTADA	NO IMPLEMENTADA	PARCIALMENTE IMPLEMENTADA
08	¿La institución cuenta con un Plan de Gestión de la Calidad?	0	4	0

NRO	PREGUNTA	RESPUESTA		
		IMPLEMENTADA	NO IMPLEMENTADA	PARCIALMENTE IMPLEMENTADA
09	¿La institución cuenta con un Plan de copias de seguridad y restauración?	0	1	3

NRO	PREGUNTA	RESPUESTA				
		NUNCA	CASI NUNCA	FRECUENTEMENTE	CASI SIEMPRE	SIEMPRE
10	¿Con que frecuencia realiza copias de seguridad de la información?	1	0	0	3	0



Anexo 04: Armonización de estándares.

ARMONIZACIÓN DE ESTÁNDARES DE SGSI							
FASE	PROCESO	SUB PROCESO	COBIT 2019	MAGERIT	FAMILIA ISO 27000	MSPI	ITIL
1. NATURALEZA DE LA ORGANIZACIÓN	1.1 DEFINICIÓN DEL CONTEXTO	1.1.1 CONTEXTO INTERNO	-Proporciona un enfoque articulado entre los factores ambientales internos y externos al negocio, identificando y analizando además las leyes y regulaciones externas para alinear el procesamiento de la información con los objetivos de la empresa. -Obtiene un conocimiento entre TI y su contribución a la estrategia del negocio. -Adquiere un conocimiento	-Política interna -Compromisos con los accionistas y trabajadores.	Determina los aspectos internos y externos como un todo, seleccionando por su nivel de relevancia para el SGSI y el impacto en la capacidad de lograr los resultados deseados.	Reconoce el contexto de la entidad identificando los procesos y lineamientos de la entidad e identifica los grupos de interés al interior de la entidad como control interno, calidad, líderes de procesos entre otros.	
		1.1.2 CONTEXTO EXTERNO		-Obligaciones legales -Reglamentos externos -Entorno en cuando a competencia y posicionamiento en el mercado.			

			sobre los elementos claves de gobierno para proponer un valor óptimo de acuerdo al análisis realizado.				
	1.2 DEFINIR EL ALCANCE		Determina el alcance y límites del SGSI tomando como termino el análisis del contexto del negocio incluyendo detalles y justificación de las exclusiones e integraciones del alcance.		Es la organización quien determina los limitar y la aplicabilidad del SGSI donde se considera los siguientes puntos: -Aspectos internos y externos -Requisitos de las partes interesadas relevantes en el SGSI -Interfaces y dependencias realizadas por la organización.	Alcance total de cobertura desarrollada de manera estratégica.	

	1.3 GESTIÓN DE LAS COMUNICACIONES		-Identifica roles y responsabilidades para la planificación y ejecución del SGSI. -Gestiona la comunicación para el fortalecimiento del SGSI mediante protocolos en diferentes momentos (Planificación, implementación y monitoreo).	Identifica Roles y funciones en todo el proceso: -Órganos de gobierno -Dirección ejecutiva -Dirección operacional -Responsable de la información -Responsable del servicio -Responsable de la Seguridad -Responsable del sistema -Administradores y operadores -Todos ellos integran una matriz raci donde se identifica el rol de cada uno en cada tarea del proceso de gestión.	Es la alta dirección quien asegura las responsabilidades y asigna los roles relevantes para: -Asegurar el SGSI este conforme a los requisitos solicitados. -Reportar el desempeño del SGSI a la alta dirección.	Establece e identifica 3 roles importantes, cada uno detalla sus responsabilidades y dominios que abarca: -Responsable de seguridad de la Información. -Equipo del proyecto. -Comité de seguridad.	

2. ESTABLECER SGSI	2.1 DEFINIR POLÍTICAS Y CONTROLES SGSI		Describe las características de la política a definir. -Proporciona pautas para establecer una política con relación a las políticas de riesgos y privacidad de TI.		La política a definir debe cumplir unos aspectos: -Ser apropiada para la organización. -Incluir objetivos de seguridad de la información o proporcionar el marco de referencia para fijar los objetivos de seguridad de la información. -Incluir el compromiso de satisfacer los requisitos aplicables a seguridad de la información. -Incluir un compromiso de mejora continua en el SGSI. -Esta política debe contar con 2 aspectos muy importantes: Disponible como información	Manual con políticas de seguridad y privacidad de la información, contempla la aprobación del mismo y socializadas al interior de la entidad. Cuenta con 8 fases en las políticas de seguridad de la información en donde incluye desde el desarrollo, implementación y cumplimiento del mismo.	

					documentada a las partes interesadas y Comunicada a toda la organización.		
	2.2 DEFINIR PROCEDIMIENTOS SGSI		Establece los procedimientos para el establecimiento, implementación y monitoreo del SGSI, identificando las responsabilidades y requerimientos mínimos de seguridad. -Contiene la	-Identifica los proyectos de seguridad en 3 niveles: Plan director (uno) -Plan anual (una serie de planes anuales) -Plan de proyecto (conjunto de proyectos) -Define los objetivos,	Define los procedimientos en acciones para: -Inventario de activos de Información: Proporciona un amplio catálogo para su identificación en su ámbito y valoración de cada activo mediante escalas	Presenta recomendaciones para los procedimientos del modelo brindando la capacidad de generar los documentos propios en cada entidad independientemente del contexto. -Es la entidad quien define la	

			gestión de los datos, los activos, conocimientos y calidad.	productos de entrada y salidas, estimación de coste, tiempo y estado del riesgo para cada proyecto de seguridad.	del 0 al 10 según valores CIA. -Metodología de análisis de riesgo: cuenta con un amplio catálogo para identificación de riesgos de SI.	complejidad o extensión de cada procedimiento, de acuerdo al tipo de rubro y recursos que disponga. -Contempla 11 dominios las cuales abarcan procedimientos para cada dominio identificado.	

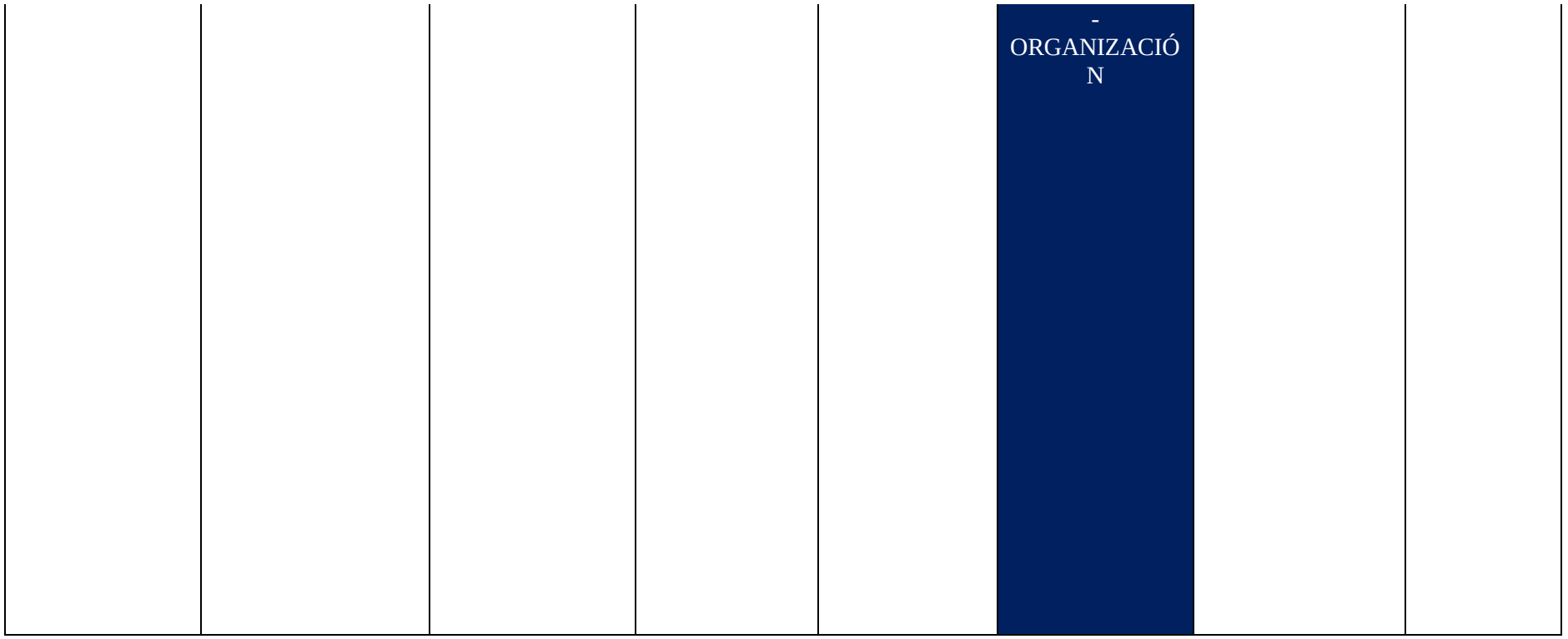
	2.3 DEFINIR METAS Y RESULTADOS SGSI		Determina la meta en relación al cumplimiento de la política y objetivos del SGSI	Define la meta en el nivel del cumplimiento de la eficacia de las salvaguardas implementadas (tratamiento de riesgos SI)	Establece parámetros para realizar una medición de metas y objetivos definidos tanto para el SGSI como para los activos. -Incluye criterios de interpretación para medir de manera correcta cada meta u objetivo. Entre las características más relevantes se encuentra: -Unidad de medida. -Indicador. -Modelo Analítico -Criterio de Decisión. -Formato de reporte. -Partes interesadas (dueño de la información o activo,	Desarrolla indicadores de gestión orientadas a medir la efectividad, eficiencia y eficacia de los componentes de implementación y gestión definidos. -Los indicadores detallan el tipo de indicador, objetivos, variables y formulas a utilizar, así como las metas y observaciones finales.	

					comunicador, cliente de la medición, revisor de la medición). -Frecuencia o periodo de recolección y análisis de datos. -Frecuencia de reporte de resultados y periodo de medición.		

	2.4 DEFINIR PLAN DE AUDITORIA		-Planifica auditorías a los programas, los proyectos y la gestión de riesgos. -Garantiza la ejecución de estos planes en la periodicidad planificada. -Define el procedimiento para la elaboración de este plan, identificando responsables y sus roles, así como los plazos de ejecución.	-Brinda consejos sobre cómo obtener un certificado mediante una auditoría externa. -Resalta la importancia de delimitar el alcance y brinda pautas sobre como dirigir la delimitación de acuerdo al contexto de la organización. -Brinda recomendaciones sobre en antes, durante y después de la auditoria con consejos claros y precisos.	Define el equipo de auditoría y otorga conocimientos de la organización, este equipo vela con que el alcance y limites definidos por el SGSI estén claramente definidos y confirma que cumpla con la clausulas definida por la organización en el SGSI. -Relaciona la complejidad de la organización en cuatro cuadrantes, así mismo puntúa los aspectos técnicos en materia del SGSI y muestra su significado para facilitar el entendimiento al auditor. -Evalúa los 114 controles	Propone un Plan de auditoria con periodicidad de 01 año donde planifican los recursos, procesos y tiempo para llevar a cabo teniendo en cuenta el desempeño de los procesos del SGSI. -Integra: -Auditoria informática -Auditoria de sistemas. -Metodologías. -Métricas de software.	Incluye proceso de gestión de revisión y auditoria de control.

					brindados por 27001 por medio de controles técnicos, pruebas del sistema o inspecciones visuales.		

3. GESTIÓN DE RIESGOS	3.1. EVALUACIÓN DEL ACTIVO	3.1.1 IDENTIFICACIÓN DE ACTIVOS	-Identifica todos los activos de TI y su ingreso a la organización (compra o creación propia) para identificar si mantienen alineamiento con los procesos de gestión posterior. -Identifica los activos críticos, la vida útil de los mismos y garantiza la contabilidad.	-Estructura los activos como: Activos esenciales, Servicios internos, equipamiento informático, entorno, servicios subcontratados a terceros, instalaciones físicas y personal. - Datos -Servicios -Aplicaciones Informáticas -Equipos informáticos -Soporte de información -Equipamiento auxiliar -Redes y comunicaciones -Instalaciones -Personas	Identifica los activos con un nivel de detalle adecuado con la SGSI para que proporciones la información suficiente. -Identifica el propietario de cada activo para su valorización -Equipo transportable -Procesamiento de periféricos -Medio Electrónico -Otros medios -SOFTWARE: -Sistema Operativo -Software de servicio, mantenimiento o administración. -Paquete de software. -APLICACIÓN DE NEGOCIOS. -RED -PERSONAL -SITIO	Define actividades para la obtención del inventario de activos: - Definición. -Revisión - Actualización -Publicación -Refleja el trabajo documental con la matriz de inventario.	Hardware -Software -Redes -Servicios de nube - Dispositivos cliente -Información -controla el ciclo de vida de los activos y datos históricos para brindar soporte.


-
ORGANIZACIÓ
N

		3.1.2 VALORACIÓN DE ACTIVOS	-Valora de acuerdo a la criticidad, vida útil, contabilidad, y su relevancia con el negocio. -Pone énfasis a los activos de información generando directrices de clasificación de datos.	- Estructura los activos según 3 dimensiones básicas y 2 secundarias: - Confidencialidad (conocer el daño) -Integridad (prejuicio típico en datos al ser manipulados) -Disponibilidad (Prejuicio al no poder hacer uso, típico en servicios) -Autenticidad (en activos de servicios y datos) -Trazabilidad (a los servicios y/o datos)	-Determina la escala y criterios para cada activo en función a su valorización. la opción de usar valores cuantitativos o cualitativos en el valor monetario de los activos es determinada por la organización. CRITERIOS: -Reducción a base común. -Escala -Dependencias -Salida	De acuerdo con la confidencialidad. -De acuerdo con la integridad. - De acuerdo con la disponibilidad. -Todas Estructurado en 03 niveles independientemente.	La valoración es económica.

	3.2. EVALUACIÓN DEL RIESGO		-Establece un método para la recolección y clasificación de riesgos relacionados a TI. -Determina el alcance adecuado para los esfuerzos en analizar el riesgo. -Desarrolla escenarios de riesgos para determinar los valores de perdida, exposición y amenazas. -Mantiene un inventario de riesgos identificados y documenta la relación con los procesos del negocio, así como los recursos y actividades de control actuales	-Identifica las amenazas en relación a 5 aspectos. -Valora las amenazas en 2 sentidos: Degradación y probabilidad. -Determina el impacto acumulado y repercutido. -Se ingresa los riesgos al mapa de calor.	Presenta una tabla con amenazas y riesgos típicos. -Daño físico -Eventos naturales -Perdida de lo esencial en servicios -Perturbación debido a radiación -Compromiso de información -Fallas técnicas -No autorizado -Compromiso de funciones -Detalla origen de amenazas de acuerdo a las causadas por personas. -Presenta una tabla con vulnerabilidades comunes en diversas áreas de seguridad para el apoyo en la evaluación de amenazas. -Cada opción de	Estructura mediante una tabla, más amenazas, tipos y origen (deliberadas, accidentales y ambientales). Recomienda tener en cuenta las fuentes de amenazas humanas, por lo que detalla una tabla para brindar una facilidad en la identificación. -Evalúa los riesgos en un mapa de calor para el posterior tratamiento.	identifica incertidumbres que afectan el logro de los objetivos.

			con los elementos del riesgo.		tratamiento cuenta con acciones, guía de implementación y salidas para evaluar de manera objetiva.		

	3.3. TRATAMIENTO DEL RIESGO		- Especifica los requisitos para implementar en las respuestas a los riesgos seleccionados. -Identifica requisitos y expectativas para controles adecuados con la finalidad de mitigar los riesgos. -Analiza el coste / beneficio en las posibles acciones de respuestas así como en la identificación de las posibles soluciones a evaluar para así buscar una respuesta optima al riesgo. -Define un portafolio de acciones para gestión de riesgos, así como	Calcula el efecto de los tratamientos (salvaguardas) de 2 formas: -Reduciendo la probabilidad de la amenaza. -Limitando el daño causado. TIPOS DE PROTECCIÓN: -Prevención -Disuasión -Eliminación -Minoración del impacto -Corrección -Recuperación -Monitorización -Detección - Concientización -Administración -Mide la eficacia del tratamiento en 6 escalas. -Calcula el impacto y riesgo residual.	Identifica 4 opciones de tratamiento de riesgos tomando en cuenta como el riesgo es percibido por las partes afectadas y las maneras más apropiadas de comunicarse con esas partes: -Modificación del riesgo -Retención del riesgo -Evitar el riesgo -Intercambio del riesgo -Las opciones de tratamiento no son excluyentes, si la organización lo determina puede hacer uso de alguna combinación de ellos.	Realiza la evaluación de controles preventivos y correctivos. - Cuantifica los controles y elige cuales son los más adecuados para obtener un nivel de riesgo aceptable. Incluye una tabla de análisis donde relaciona el riesgo y los controles implementados para evaluar su efectividad.	Recomienda de manera genera evaluar y planificar las respuestas adecuadas

			actividades de control a implementar para mitigar el riesgo.				

	3.4 MONITOREO DEL RIESGO		-Realiza un análisis periódico de eventos y factores para la identificación de nuevos riesgos o emergentes. -Realiza un monitoreo general del desempeño incluyendo la gestión de riesgo		Propone un seguimiento continuo desde la edad temprana del SGSI en determinadas situaciones: -Nuevos activos que se han incluido en el alcance de la gestión del riesgo. -Modificaciones necesarias del valor de los activos, por ejemplo, debido a los cambios en los requisitos del negocio. -Nuevas amenazas que podrían estar activas tanto fuera como dentro de la organización y que no hayan sido evaluadas; -Cambios en vulnerabilidades -Aumento del impacto o consecuencias de	Soportado en la etapa de evaluación del desempeño del MSPI	

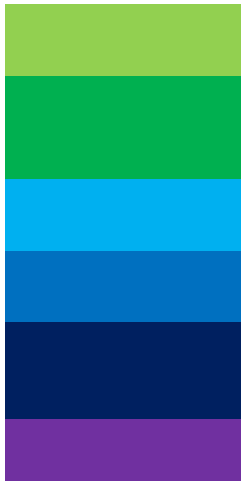
					las amenazas y riesgos evaluados que sumados resultan en un nivel inaceptable de riesgo.		
4. CONTROL Y EVALUACIÓN DE SGSI	4.1 CONTROL DEL SGSI	4.1.1 MONITOREO DE SGSI	-Realiza revisiones periódicas para el monitoreo de la eficacia y gestión del SGSI, el cumplimiento de las políticas y objetivos planificados y la revisión de las prácticas de seguridad y privacidad. -Identifica y		El enfoque de la organización para la gestión del SGSI implica revisar en intervalos planificados para asegurar la conveniencia, adecuación y eficacia continua. -Los directores son quienes debe revisar regularmente el cumplimiento del	Se programa el seguimiento de las actividades: -Programación y ejecución de auditoría. -Revisiones por parte del encargado de seguridad y privacidad. -alcance del MSPI - Planes de seguridad.	

			registra acciones o eventos que pueden obtener un impacto en el rendimiento del SGSI		procesamiento de la información, los requisitos de seguridad definidos en las políticas y/o normas. -Se considera el uso de herramientas de medición automática para una revisión periódica eficiente.		
		4.1.2 EVALUACIÓN DE SGSI	Recomienda la realización de auditorías de SGSI en los intervalos planificados.	Recomienda la evaluación con instituciones certificadas, además brinda un apéndice de pautas para preparar a la organización al momento de evaluar el SGSI implementado.	La evaluación es realizada por organismos acreditados que cumplen con la norma ISO /IEC 27001. -Se analiza el SGSI como el conocimiento de los integrantes e interesados para conocer el nivel de entendimiento. -La evaluación permite el uso de enfoque adoptado por CMMI para la	-Revisión de la eficacia del MSPI. -Medición de la efectividad de Controles. -Revisión de las valoraciones de los riesgos. -Medición de los indicadores de gestión del MSPI. -Realización de auditorías.	

					puntuación de procesos específicos, para la evaluación de controles se hace uso de checklist evaluando el origen del entregable o acreditación de cada control.		
	4.2 DEFINIR ACCIONES CORRECTIVAS				-Al evaluar y no contar con una conformidad la organización debe: -Reaccionar la no conformidad para aplicar acciones en beneficio del control u ocuparse de las consecuencias. -Evaluar la necesidad de eliminar las	Determina que, en caso de presentarse no conformidades en las auditorías realizadas, la entidad debe llevar a cabo el análisis para controlar y corregir. - Evalúa la raíz de la no conformidad con la finalidad de eliminar las causas y evitar que suceda a futuro.	

					causas revisando, determinando las causas y la ocurrencia para evitar potencialmente una ocurrencia. -Implementar cualquier acción necesaria -Revisar la efectividad de cualquier acción correctiva -Plantear cambios al SGSI	- -evidencia las no conformidades y acciones correctivas.	
	4.3 EJECUTAR PLAN DE MEJORA CONTINUA				La organización debe mejorar continuamente la conveniencia, adecuación y efectividad del SGSI ejecutando las acciones correctivas identificadas posterior a la evaluación e informar al organismo certificador para su evaluación posterior a la	-Compara las no conformidades con las acciones correctivas a tomar para evaluar su efectividad. -Es la entidad quien identificara oportunidades de mejora, de acuerdo a los criterios de calidad establecidos en el modelo a fin de preservar la disponibilidad, confidencialidad e	

					ejecución de este plan.	integridad de los activos de información.	



ISO 27001 describe cómo gestionar la seguridad de la información en una empresa.

ISO/IEC 27002 proporciona directrices para la implementación de los controles indicados en ISO 27001. ISO 27001 especifica 114 controles que pueden ser utilizados para disminuir los riesgos de seguridad, y la norma ISO 27002 puede ser bastante útil ya que proporciona más información sobre cómo implementar esos controles.

ISO/IEC 27003 focaliza su atención en los aspectos requeridos para un diseño exitoso y una buena implementación del Sistema de Gestión de Seguridad de la Información – SGSI – según el estándar ISO 27001

ISO/IEC 27004 proporciona directrices para la medición de la seguridad de la información; se acopla bien con ISO 27001 ya que explica cómo determinar si el SGSI ha alcanzado los objetivos.

ISO/IEC 27005 proporciona directrices para la gestión de riesgos de seguridad de información. Es un muy buen complemento para ISO 27001 ya que brinda más información sobre cómo llevar a cabo la evaluación y el tratamiento de riesgos, probablemente la etapa más difícil de la implementación.

ISO/IEC 27006 responde a una guía para los organismos de certificación en los procesos formales que hay que seguir al auditar SGSI.

Anexo 05: Selección de estándares.

FASE	PROCESO	SUB PROCESO	ESTÁNDAR SELECCIONADO	INTEGRACIÓN	JUSTIFICACIÓN
1. NATURALEZA DE LA ORGANIZACIÓN	1.1 DEFINICIÓN DEL CONTEXTO	1.1.1 CONTEXTO INTERNO	ISO 27000 E MSPI	COMPLEMENTACIÓN	MSPI RECONOCE LOS PROCESOS Y LINEAMIENTOS DE LA ENTIDAD; LAS ENTIDADES DEL SECTOR NO CUENTAN CON UNA DEFINICIÓN INICIAL DEL CONTEXTO POR LO QUE ES NECESARIO UN ANÁLISIS EXHAUSTIVO Y ALINEACIÓN DE OBJETIVOS QUE ISO 27000 BRINDA.
		1.1.2 CONTEXTO EXTERNO			
	1.2 DEFINIR EL ALCANCE		COBIT 2019	TOTAL	LAS ENTIDADES MANEJAN RECURSOS DE MANERA DIFERENTE ES POR ELLO QUE CADA UNO DEBE DETERMINAR EL ALCANCE CON SUSTENTO TÉCNICO SOBRE LAS EXCLUSIONES EN EL SGSI, CARACTERÍSTICA QUE SOLO COBIT BRINDA.
	1.3 GESTIÓN DE LAS COMUNICACIONES		MSPI	TOTAL	LAS ENTIDADES CUENTAN CON ESCASO RECURSO HUMANO ESPECIALISTA ES POR ELLO QUE MSPI ENGLOBA TODO EL SISTEMA EN 3 ROLES COMPLETAMENTE DEFINIDOS, ENTRE ELLOS UN COMITÉ PARA UNA MEJOR TOMA DE DECISIONES. A DIFERENCIA DE LOS DEMÁS ESTÁNDARES QUE REQUIEREN DE HASTA 16 ROLES.
2. ESTABLECER SGSI	2.1 DEFINIR POLÍTICAS Y CONTROLES SGSI		MSPI E ISO 27000	COMPLEMENTACIÓN	MSPI PROPORCIONA POLÍTICAS ESPECIFICAS ESTRUCTURADAS, ISO 27000 ASPECTOS DE SOCIALIZACIÓN EN TODA LA ENTIDAD Y ASPECTOS A CUMPLIR EN EL DESARROLLO DE CONTROLES.
	2.2 DEFINIR PROCEDIMIENTOS SGSI		COBIT 2019 E MSPI	COMPLEMENTACIÓN	MSPI CONTEMPLA DOMINIOS DENTRO DE LOS CUALES ABARCA UNA SERIE DE PROCESOS Y COBIT 2019 ESTABLECE LOS RESPONSABLES Y REQUERIMIENTOS MÍNIMOS A CADA PROCESO FACILITANDO

					LA DEFINICIÓN DE PROCESOS EN LA ENTIDAD.
	2.3 DEFINIR METAS Y RESULTADOS SGSI		ISO 27000	TOTAL	DEFINE UN CONJUNTO DE METAS Y RESULTADOS ESPECÍFICOS PARA MEDIR CADA ASPECTO, ASÍ COMO CRITERIOS DE INTERPRETACIÓN. DIGERIBLES PARA LOS ALTOS FUNCIONARIOS AL MOMENTO DE PRESENTAR.
	2.4 DEFINIR PLAN DE AUDITORIA		MSPI	TOTAL	ABARCA DESDE LA DEFINICIÓN DEL PLAN DETERMINANDO ASPECTOS A EVALUAR ORGANIZADOS EN CUADRANTES.
3. GESTIÓN DE RIESGOS	3.1. EVALUACIÓN DEL ACTIVO	3.1.1 IDENTIFICACIÓN DE ACTIVOS	27000 y MAGERIT	COMPLEMENTACIÓN	27000 OFRECE UN AMPLIO CATALOGO DE ACTIVOS DE INFORMACIÓN (NO SOLO TI) Y MAGERIT UNA ESTRUCTURA DE ASPECTOS A IDENTIFICAR EN CADA ACTIVO PARA FACILITAR AL PERSONAL DE TI DE LA ENTIDAD.
		3.1.2 VALORACIÓN DE ACTIVOS	MAGERIT	TOTAL	DETERMINA EL VALOR DE CADA ACTIVO EN 5 DIMENSIONES DE S.I., YA QUE EL VALOR MONETARIO ES UN VALOR DETERMINADO POR CADA HOSPITAL POR CUMPLIMIENTO A REGLAMENTOS NACIONALES.
	3.2. EVALUACIÓN DEL RIESGO		MAGERIT	COMPLEMENTACIÓN	AMBOS OFRECEN UN AMPLIO CATALOGO LA CUAL SERVIRÁ PARA SELECCIONAR Y ADECUAR AL CONTEXTO DE LOS HOSPITALES Y ASÍ FACILITAR SU RECONOCIMIENTO Y EVALUACIÓN.
	3.3. TRATAMIENTO DEL RIESGO		MAGERIT	TOTAL	PRESENTA UNA ESTRUCTURA MAS ESPECIFICA DEL TRATAMIENTO DE RIESGO (SALVAGUARDAS), ADEMÁS PRESENTA EN UN ANEXO LOS CÁLCULOS PARA EFICACIA, IMPACTO, ENTRE OTROS. CON LA FINALIDAD DE TENER UN AMPLIO CONOCIMIENTO DEL

					RIESGO PARA UNA MEJOR LA TOMA DE DECISIONES.
	3.4 MONITOREO DEL RIESGO		ISO 27000	PARCIAL	PROPORCIONA UN ENFOQUE DIFERENTE A LAS DEMÁS METODOLOGÍAS, REALIZA EL MONITOREO DESDE LA EDAD TEMPRANA DEL SGSI Y ANTE ALGÚN CAMBIO PARA MANTENER IDENTIFICADOS TODOS LO RIESGOS EN TIEMPO REAL.
4. CONTROL Y EVALUACIÓN DE SGSI	4.1 CONTROL DEL SGSI	4.1.1 MONITOREO DE SGSI	MSPI E ISO 27000	COMPLEMENTACIÓN	MSPI IDENTIFICA LOS PROCESOS A MONITOREAR, 27000 EL ENFOQUE Y PERSPECTIVA A TOMAR EN CUENTA.
		4.1.2 EVALUACIÓN DE SGSI	MSPI, 27000	COMPLEMENTACIÓN	MSPI IDENTIFICA LOS INDICADORES A TOMAR EN CUENTA PARA DETERMINAR EL ÉXITO DE LA SGSI Y 27000 RECOMIENDA EL ENFOQUE CMMI PARA LA PUNTUACIÓN DE PROCESOS INVOLUCRADOS ADEMÁS DEL USO DE CHECKLIST PARA LA EVALUACIÓN DE LOS CONTROLES.
	4.2 DEFINIR ACCIONES CORRECTIVAS		MSPI	TOTAL	AMBOS ESTÁNDARES DEFINEN LOS MOMENTOS PARA REALIZAR ACCIONES CORRECTIVAS, PERO MSPI EVALÚA LA RAÍZ DE LA CAUSA PARA EVITAR QUE SUCEDA A FUTURO.
	4.3 EJECUTAR PLAN DE MEJORA CONTINUA		MSPI	PARCIAL	PROVEE UN AMPLIO PANORAMA DE CASOS EN DONDE LA ORGANIZACIÓN ES QUIEN DETERMINA LAS OPORTUNIDADES DE MEJORA.

*Integración: Total, Parcial, Complementación.

Anexo 06: Elementos y características SGSI.

ELEMENTOS Y CARACTERÍSTICAS DE SGSI

Jaime Izquierdo Cabrera

ÍNDICE

ROLES Y PERFILES

El Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia [1] determina la decisión de implementar Seguridad de la Información como un sistema vivo, el primer paso es la definición de una estructura organizacional con funciones y responsabilidades para la ejecución de las actividades que esto conlleve, es por ello que el Modelo de Seguridad y Privacidad de la Información elaborado por el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia define los siguientes perfiles:

Responsable de Seguridad de la Información para la entidad:

El responsable de Seguridad de la información será el líder del proyecto, escogido dentro del equipo en cada entidad y tendrá las siguientes responsabilidades:

- Aplicar conocimientos, habilidades, herramientas, y técnicas a las actividades propias del proyecto, de manera que cumpla o exceda las necesidades y expectativas de los interesados en el mismo
- Identificar la brecha entre el SGSI y la situación de la entidad.
- Generar el cronograma de la implementación del SGSI.
- Planear, implementar y hacer seguimiento a las tareas, fechas, costos y plan de trabajo de los objetivos específicos del cronograma definido.
- Gestionar el equipo de proyecto de la entidad, definiendo roles, responsabilidades, entregables y tiempos.
- Coordinar las actividades diarias del equipo y proporcionar apoyo administrativo
- Encarrilar el proyecto hacia el cumplimiento de la implementación del SGSI para la entidad.
- Realizar un seguimiento permanente a la ejecución de los planes de trabajo, monitoreando los riesgos del proyecto para darle solución oportuna y escalar al Comité de seguridad en caso de ser necesario.
- Monitorear el estado del proyecto en términos de calidad de los productos, tiempo y los costos.
- Trabajar de manera integrada con el grupo o áreas asignadas.
- Asegurar la calidad de los entregables y del proyecto en su totalidad.
- Velar por el mantenimiento de la documentación del proyecto, su custodia y protección.
- Contribuir al enriquecimiento del esquema de gestión del conocimiento sobre el proyecto en cuanto a la documentación de las lecciones aprendidas.
- Liderar la programación de reuniones de seguimiento y velar por la actualización de los indicadores de gestión del proyecto.

Equipo del Proyecto

Teniendo en cuenta la naturaleza de la entidad, debe conformarse un equipo para el desarrollo del proyecto al cual deben pertenecer miembros directivos y representantes de las áreas misionales, con el propósito de asegurar que toda la información más relevante de la entidad esté disponible oportunamente. De esta forma se busca asegurar que sea una iniciativa de carácter transversal a la entidad, y que no dependa exclusivamente de la oficina o área de TI.

Una de las tareas principales del líder del proyecto es entregar y dar a conocer los perfiles y responsabilidades de cada personaje al grupo de trabajo e identificar las personas idóneas para tomar cada rol. De esta forma, y de manera general se pone a consideración el siguiente listado para que las entidades analicen de acuerdo a su composición orgánica cuales pueden ser los miembros del equipo de seguridad y privacidad de la información, de acuerdo a los siguientes perfiles:

- ✓ Personal de seguridad de la información.
- ✓ Un representante del área de Tecnología.
- ✓ Un representante del área de Control Interno.
- ✓ Un representante del área de Planeación.
- ✓ Un representante de sistemas de Gestión de Calidad.
- ✓ Un representante del área Jurídica.
- ✓ Funcionarios, proveedores, y ciudadanos.

Responsabilidades del equipo del proyecto:

- Apoyar al líder de proyecto al interior de la entidad.
- Oficiar como consultores de primer nivel en cuanto a las dudas técnicas y de procedimiento que se puedan suscitar en el desarrollo del proyecto.
- Ayudar al líder de proyecto designado, en la gestión de proveedores de tecnología e infraestructura.
- Asistir a las reuniones de seguimiento o de cualquier otra naturaleza planeadas por el líder de proyecto.
- Las que considere el líder del proyecto o el comité de seguridad de la entidad.

Comité de seguridad

Las funciones de este comité son:

- Coordinar la implementación del SGSI al interior de la entidad.
- Revisar los diagnósticos del estado de la seguridad de la información.
- Acompañar e impulsar el desarrollo de proyectos de seguridad.
- Coordinar y dirigir acciones específicas que ayuden a proveer un ambiente seguro y establecer los recursos de información que sean consistentes con las metas y objetivos.

- Aprobar el uso de metodologías y procesos específicos para la seguridad de la información.
- Participar en la formulación y evaluación de planes de acción para mitigar y/o eliminar riesgos.
- Realizar revisiones periódicas del SGSI (por lo menos una vez al año) y según los resultados de esta revisión definir las acciones pertinentes.
- Promover la difusión y sensibilización de la seguridad de la información dentro de la entidad.

EJES DE SEGURIDAD

El Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia [2] determina la importancia de contar con ejes de seguridad ya que son ellas quienes guiaran el comportamiento personal y profesional de los funcionarios, contratistas o terceros sobre la información obtenida, generada o procesada por la entidad, así mismo los ejes permitirán que la entidad trabaje bajo las mejores prácticas de seguridad y cumpla con los requisitos legales a los cuales esté obligada a cumplir la entidad.

Este conjunto de recomendaciones no es exhaustivo, se aconseja que cada Entidad genere sus documentaciones propias dependiendo de sus características particulares, sus activos de información, sus procesos y los servicios de información que pueda prestar. A continuación, se agruparán los ejes con el objetivo de hacer una implementación transversal de Seguridad de la Información en la Entidad.

GESTIÓN DE ACTIVOS

Este grupo de ejes deben hacer referencia a todas aquellas directrices mediante las cuales se indica a los funcionarios los límites y procedimientos frente a la identificación, uso, administración y responsabilidad frente a los activos de Información, los ejes relacionados con gestión de activos deben contemplar como mínimo:

- **Identificación de Activos**: Esta política debe determinar la periodicidad con la cual se va a realizar al interior de la Entidad la identificación y/o actualización del inventario de Activos de Información, la política debe determinar el responsable de realizar la actividad, se debe determinar bajo que instrumento se va a realizar la actividad, dicho instrumento debe permitir identificar el propietario del activo de información.
- **Clasificación de Activos**: La Entidad debe determinar la clasificación de los activos de información de acuerdo a la criticidad, sensibilidad y reserva de la

misma. En la elaboración de esta política debe tenerse en cuenta las leyes y normatividades actuales que afecten a la Entidad.

NO REPUDIO

Este eje de seguridad comprende la capacidad de no repudio con el fin de que los usuarios eviten haber realizado alguna acción.

El eje deberá incluir mínimo los siguientes aspectos:

- **Trazabilidad**: La política hará que por medio de la trazabilidad de las acciones se haga seguimiento a la creación, origen, recepción, entrega de información y otros.
- **Retención**: La política debe incluir el periodo de retención o almacenamiento de las acciones realizadas por los usuarios, el cual deberá ser informado a los funcionarios, contratistas y/o terceros de la Entidad.
- **Auditoría**: La política incluirá la realización de auditorías continuas, como procedimiento para asegurarse que las partes implicadas nieguen haber realizado una acción.

PRIVACIDAD Y CONFIDENCIALIDAD

Este eje debe contener una descripción de las políticas de tratamiento y protección de datos personales que deben ser aplicados, conforme a lo establecido en la normatividad vigente. La política de privacidad debe contener como mínimo lo siguiente:

- Ámbito de aplicación
- Excepción al ámbito de aplicación de las políticas de tratamiento de datos personales
- Principios del tratamiento de datos personales
- Principio de la Legalidad: El tratamiento de datos personales debe estar sujeto a lo establecido en la normatividad vigente.
- Principio de finalidad: Indicar la finalidad del tratamiento de datos personales, la cual debe ser informada al titular.
- Principio de veracidad o calidad: La información a tratar debe ser veraz, completa, exacta, actualizada, comprobable y comprensible.
- Principio de acceso y circulación restringida: El tratamiento sólo podrá hacerse por personas autorizadas por el titular o por personas previstas en la normatividad vigente.
- Principio de seguridad: La información sujeta a tratamiento, se debe manejar con las medidas técnicas, humanas y administrativas que sean necesarias para garantizar la seguridad evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento

- Principio de confidencialidad: Todas las personas que participen en el Tratamiento de Datos Personales deben garantizar la reserva de dicha información.

CONTROL DE ACCESO

Este grupo de ejes deben hacer referencia a todas aquellas directrices mediante las cuales la Entidad determina los mecanismos de protección, los límites y procedimientos frente a la administración y responsabilidad, relacionados con los accesos a la información, sin importar si estos accesos sean electrónicos o físicos; los ejes relacionados con el control de acceso deben contemplar como mínimo:

- **Control de acceso con usuario y contraseña**: Se debe elaborar una política sobre control de acceso a redes, aplicaciones, y/o sistemas de información de la entidad, mediante la cual se determinen los responsables y los procedimientos formales de autorización de creación, modificación, suspensión o eliminación de usuarios (ID) y contraseñas. La política debe enunciar las responsabilidades que los funcionarios, contratistas o terceros tienen al contar con un usuario o contraseña de la entidad, se debe estipular que los usuarios (ID) y contraseñas son personales e intransferibles y no deben prestarse, ni compartirse. La entidad debe establecer que por cada funcionario, contratista o tercero debe tenerse un usuario y una contraseña para el acceso.
- **Suministro del control de acceso**: Esta política debe determinar los procedimientos formales y directrices que se deben construir para la gestión de asignación, modificación, revisión o revocación de derechos y/o privilegios a cada uno de los usuarios (ID) creados, también deben tenerse en cuenta en esta política los casos especiales como lo son usuarios (ID) con privilegios superiores utilizados para la administración de infraestructura, aplicaciones y sistemas de información de la entidad.
- **Gestión de Contraseñas**: Esta política debe definir los lineamientos mínimos en cuanto a calidad que deben tener las contraseñas para ser utilizadas como mecanismo de autenticación en los accesos a la red, aplicaciones y/o sistemas de información de la entidad. Esta política debe indicar a los funcionarios, contratistas y/o terceros los parámetros mínimos para que una contraseña sea considera como fuerte, gestión de cambio de contraseña, debe determinar que los accesos a la red, las aplicaciones y sistemas de información deben requerir un usuario (ID) y una contraseña fuerte para que realice la correspondiente autenticación y acceso a la información de forma segura.
- **Perímetros de Seguridad**: La política debe definir los perímetros físicos de seguridad donde se encuentra información crítica, sensible o se realice almacenamiento y/o procesamiento de información a los cuales los funcionarios, contratistas o terceros, tienen acceso y a cuáles no, la política debe definir los responsables de autorizar o no ingresos a las áreas delimitadas como de acceso restringido.

REGISTRO Y AUDITORÍA

Este eje vela por el mantenimiento de las evidencias de las actividades y acciones que afectan los activos de información.

Este eje deberá contener:

- **Responsabilidad**: Incluir la responsabilidad de la Oficina de Control Interno y similares, acerca de la responsabilidad de llevar a cabo las auditorías periódicas a los sistemas y actividades relacionadas a la gestión de activos de información, así como la responsabilidad de dicha Oficina de informar los resultados de las auditorías.
- **Almacenamiento de registros**: La política debe incluir el almacenamiento de los registros de las copias de seguridad en la base de datos correspondiente y el correcto funcionamiento de las mismas. Los registros de auditoría deben incluir toda la información registro y monitoreo de eventos de seguridad.
- **Normatividad**: La política de auditoría debe velar porque las mismas sean realizadas acorde a la normatividad y requerimientos legales aplicables a la naturaleza de la Entidad.
- **Garantía cumplimiento**: La política de auditoría debe garantizar la evaluación de los controles, la eficiencia de los sistemas, el cumplimiento de las políticas y procedimientos de la Entidad; así como recomendar las deficiencias detectadas.
- **Periodicidad**: La política debe determinar la revisión periódica de los niveles de riesgos a los cuales está expuesta la Entidad, lo cual se logra a través de auditorías periódicas alineada a los objetivos estratégicos y gestión de procesos de la Entidad.

GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

La entidad deberá documentar una política general de gestión de eventos, incidentes y vulnerabilidades de seguridad de la información. Debe ir dirigida a todos los usuarios que tienen un acceso autorizado a cualquier sistema de información.

El eje debe contemplar para su elaboración los siguientes parámetros:

Debe estar aprobada por la alta dirección, certificando así el compromiso con el proceso.

- Visión General: ¿Qué se debe reportar? ¿A quién debe reportarse?, ¿Qué medios pueden emplearse para hacer el reporte?
- Definir responsables: Se deben mencionar de manera muy general quienes serán los responsables de gestionar los eventos.
- Actividades: Explicar de manera general en que consiste el proceso de gestión de incidentes desde el reporte hasta la resolución.
- Documentación: Se debe hacer referencia sobre la documentación del esquema de gestión y los procedimientos.

- **Descripción Del Equipo Que Manejará Los Incidentes**: Se debe indicar como está compuesta la estructura general para la gestión de incidentes y vulnerabilidades de seguridad.
- **Aspectos Legales**: Deben citarse los aspectos legales que se deben tener en cuenta o los cuales debe darse cumplimiento.

CAPACITACIÓN Y SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

Este eje se centra en la formación del personal en temas relacionados con la seguridad de la información, cuya finalidad es disminuir las vulnerabilidades y amenazas relacionadas con el recurso humano.

Dicho eje debe contener los siguientes parámetros.

- El compromiso de la alta dirección en destinar los recursos suficientes para desarrollar los programas.
- ¿Quiénes deberán ser entrenados? ¿Quiénes deberán ser sensibilizados?
- La obligación de los usuarios a asistir a los eventos o cursos de capacitación.
- Revisión periódica de resultados de capacitaciones para mejoramiento de los procesos.
- Definir los roles y responsabilidades de quienes diseñarán los programas, quienes los comunicarán.
- Documentación sobre planes de estudio y desarrollo de los programas.
- Compromisos y obligaciones por parte del personal capacitado.

CONTROLES

Dentro de la norma ISO 27001 [3], el Anexo A es el más conocido por ser normativo, lo que indica que su implementación es imprescindible. Y en cuanto a controles de seguridad en ISO 27001 se refiere, constituye una parte esencial, pues presenta una lista de dichos controles que pueden resultar fundamentales para mejorar la protección de la información en las organizaciones.

En la siguiente lista se especifica los 114 controles relacionado con los 14 dominios.

CLASIFICACIÓN DE ACTIVOS

Para ISO 27001 [4] los activos se clasifican de la siguiente manera.

CÓDIGO	CLASIFICACIÓN	DESCRIPCIÓN
[hw]	Hardware	El tipo de hardware se compone de todos los elementos físicos de apoyo a los procesos.
[epd]	Equipo de procesamiento de datos	Equipo de procesamiento automático de información, incluidos los elementos requeridos para la operación independiente.
[et]	Equipo transportable	Equipo de cómputo portátil
[ef]	Equipo fijo	Los equipos informáticos utilizados en las instalaciones de la organización
[pp]	Periféricos para procesamiento	Equipo conectado a una computadora mediante un puerto de comunicaciones (serie, paralelo, entre otros) para el ingreso, el transporte o la transmisión de datos
[md]	Medio de datos	Estos son los medios para el almacenamiento de datos o funciones.
[me]	Medio electrónico:	Un medio de información que puede ser conectado a una computadora o una red de computadoras para el almacenamiento de datos. A pesar de su tamaño compacto, estos medios pueden llegar a contener una gran cantidad de datos. Se pueden utilizar con un equipo informático estándar.
[om]	Otros medios	Estáticos, medios no electrónicos conteniendo datos.
[sf]	Software	El tipo Software está compuesto por todos los programas que contribuyen a la operación de un conjunto de procesamiento de datos.
[so]	Sistema operativo	Esto incluye todos los programas de una computadora que componen la base de operaciones a partir de la cual todos los demás programas (aplicaciones o servicios) son ejecutados. Incluye un núcleo y servicios o funciones básicas. Dependiendo de la arquitectura, un sistema

		operativo puede ser monolítico o construido a partir de un micro-núcleo y un conjunto de servicios del sistema. Los elementos principales del sistema operativo son todos los servicios de gestión del equipo (CPU, memoria, disco e interfaces de red), las tareas o servicios de gestión de procesos y los servicios de gestión de derechos de usuario.
[ss]	Software de servicios, mantenimiento o administración	Software caracterizado por el hecho de complementar los servicios del sistema operativo y no está directamente al servicio de los usuarios o aplicaciones (aunque generalmente es esencial e incluso indispensable para el funcionamiento global del sistema de información)
[ps]	Paquete de software o software estándar	Software estándar o paquete de software son los productos completos comercializados como tales (en lugar de desarrollos a medida o específicos) con soporte, liberación y mantenimiento. Proporcionan servicios a los usuarios y aplicaciones, pero no son personalizados o específicos como si lo pueden ser las aplicaciones del negocio.
[an]	Aplicaciones de negocio	Se trata de un software comercial diseñado para dar a los usuarios acceso directo a los servicios y funciones que requieren de su sistema de información en su contexto profesional. Hay una muy amplia, teóricamente ilimitada, gama de campos.
[red]	Red	El tipo red se compone de todos los dispositivos de telecomunicaciones utilizadas para interconectar varias computadoras físicamente remotas o elementos de un sistema de información.
[ms]	Medio y soporte	Los medios o equipos de comunicaciones y telecomunicaciones son caracterizados principalmente por las características físicas y técnicas de los equipos (punto a punto, broadcast) y por los protocolos de comunicación (enlace o red - niveles 2 y 3 del modelo OSI de 7 capas).

[pe]	Personal	El tipo personal se compone de todos los grupos de personas involucradas en el sistema de información.
[us]	Usuarios	Los usuarios son el personal que maneja elementos sensibles en el contexto de su actividad y que tienen una responsabilidad especial en este sentido. Ellos pueden tener derechos de acceso especiales al sistema de información para llevar a cabo sus tareas diarias.
[ub]	Ubicación	El tipo ubicación comprende todos los lugares abarcados por el alcance o parte del mismo, y los medios físicos requeridos para su operación.
[sb]	Subcontratistas/ proveedores/ fabricantes	Estas son organizaciones que proveen a la organización de un servicio o recurso y está vinculado a ella por contrato.

DIMENSIONES DE VALORACIÓN

MAGERIT [4] establece que una dimensión es una faceta o aspecto de un activo, independiente de otras facetas. Pueden hacerse análisis de riesgos centrados en una única faceta, independientemente de lo que ocurra con otros aspectos.

Las dimensiones se utilizan para valorar las consecuencias de la materialización de una amenaza. La valoración que recibe un activo en una cierta dimensión es la medida del perjuicio para la organización si el activo se ve dañado en dicha dimensión.

DISPONIBILIDAD

¿Qué importancia tendría que el activo no estuviera disponible?

Un activo tiene un gran valor desde el punto de vista de disponibilidad cuando si una amenaza afectara a su disponibilidad, las consecuencias serían graves.

Y recíprocamente, un activo carece de un valor apreciable desde el punto de vista de disponibilidad cuando puede no estar disponible frecuentemente y durante largos periodos de tiempo sin por ello causar mayor daño.

La disponibilidad es una característica que afecta a todo tipo de activos.

A menudo la disponibilidad requiere un tratamiento por escalones pues el coste de la indisponibilidad aumenta de forma no lineal con la duración de la interrupción, desde breves interrupciones sin importancia, pasando por interrupciones que causan daños considerables y llegando a interrupciones que no admiten recuperación: la organización está acabada.

Integridad de los datos

¿Qué importancia tendría que los datos fueran modificados fuera de control?

Los datos reciben una alta valoración desde el punto de vista de integridad cuando su alteración, voluntaria o intencionada, causaría graves daños a la organización.

Y, recíprocamente, los datos carecen de un valor apreciable desde el punto de vista de integridad cuando su alteración no supone preocupación alguna.

Confidencialidad de la información

¿Qué importancia tendría que el dato fuera conocido por personas no autorizadas?

Los datos reciben una alta valoración desde el punto de vista de confidencialidad cuando su revelación causaría graves daños a la organización.

Y, recíprocamente, los datos carecen de un valor apreciable desde el punto de vista de confidencialidad cuando su conocimiento por cualquiera no supone preocupación alguna.

Autenticidad

¿Qué importancia tendría que quien accede al servicio no sea realmente quien se cree?

La autenticidad de los usuarios de un servicio es lo contrario de la oportunidad de fraude o uso no autorizado de un servicio.

Así, un servicio recibe una elevada valoración desde el punto de vista de autenticidad cuando su prestación a falsos usuarios supondría un grave perjuicio para la organización.

Y, recíprocamente, un servicio carece de un valor apreciable desde el punto de vista de autenticidad cuando su acceso por cualquiera no supone preocupación alguna.

¿Qué importancia tendría que los datos no fueran realmente imputables a quien se cree?

Los datos reciben una elevada valoración desde el punto de vista de autenticidad del origen cuando un defecto de imputación causaría graves quebrantos a la organización. Típicamente, se habilita la oportunidad de repudio.

Y, recíprocamente, los datos carecen de un valor apreciable desde el punto de vista de autenticidad del origen cuando ignorar la fuente es irrelevante.

Trazabilidad

¿Qué importancia tendría que no quedara constancia fehaciente del uso del servicio?

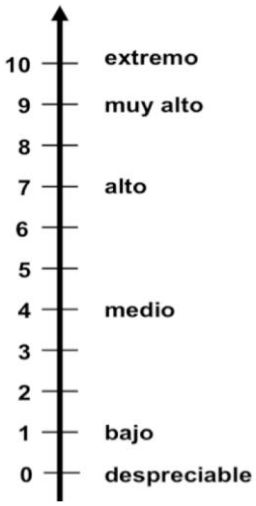
Abriría las puertas al fraude, incapacitaría a la Organización para perseguir delitos y podría suponer el incumplimiento de obligaciones legales.

¿Qué importancia tendría que no quedara constancia del acceso a los datos?

Abriría las puertas al fraude, incapacitaría a la Organización para perseguir delitos y podría suponer el incumplimiento de obligaciones legales.

Criterio de valoración

Se ha elegido una escala detallada de diez valores, dejando en valor 0 como determinante de lo que sería un valor despreciable (a efectos de riesgo). Si se realiza un análisis de riesgos de poco detalle, se puede optar por la tabla simplificada de menos niveles. Ambas escalas, detallada y simplificada se correlacionan como se indica a continuación:



VALOR		CRITERIO
10	extremo	daño extremadamente grave
9	muy alto	daño muy grave
6-8	alto	daño grave
3-5	medio	daño importante
1-2	bajo	daño menor
0	despreciable	irrelevante a efectos prácticos

[pi] Información de carácter personal		
6	6.pi1	probablemente afecte gravemente a un grupo de individuos
	6.pi2	probablemente quebrante seriamente la ley o algún reglamento de protección de información personal
5	5.pi1	probablemente afecte gravemente a un individuo
	5.pi2	probablemente quebrante seriamente leyes o regulaciones

4	4.pi1	probablemente afecte a un grupo de individuos
	4.pi2	probablemente quebrante leyes o regulaciones
3	3.pi1	probablemente afecte a un individuo
	3.pi2	probablemente suponga el incumplimiento de una ley o regulación
2	2.pi1	pudiera causar molestias a un individuo
	2.pi2	pudiera quebrantar de forma leve leyes o regulaciones
1	1.pi1	pudiera causar molestias a un individuo
[lpo] Obligaciones legales		
9	9.lro	probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación
7	7.lro	probablemente cause un incumplimiento grave de una ley o regulación
5	5.lro	probablemente sea causa de incumplimiento de una ley o regulación
3	3.lro	probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
1	1.lro	pudiera causar el incumplimiento leve o técnico de una ley o regulación
[si] Seguridad		
10	10.si	probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios
9	9.si	probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
7	7.si	probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
3	3.si	probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente
1	1.si	pudiera causar una merma en la seguridad o dificultar la investigación de un incidente
[cei] Intereses comerciales o económicos		
9	9.cei.a	de enorme interés para la competencia
	9.cei.b	de muy elevado valor comercial
	9.cei.c	causa de pérdidas económicas excepcionalmente elevadas
	9.cei.d	causa de muy significativas ganancias o ventajas para individuos u organizaciones
	9.cei.e	constituye un incumplimiento excepcionalmente grave de las obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros

7	7.cei.a	de alto interés para la competencia
	7.cei.b	de elevado valor comercial
	7.cei.c	causa de graves pérdidas económicas
	7.cei.d	proporciona ganancias o ventajas desmedidas a individuos u organizaciones
	7.cei.e	constituye un serio incumplimiento de obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros
3	3.cei.a	de cierto interés para la competencia
	3.cei.b	de cierto valor comercial
	3.cei.c	causa de pérdidas financieras o merma de ingresos
	3.cei.d	facilita ventajas desproporcionadas a individuos u organizaciones
	3.cei.e	constituye un incumplimiento leve de obligaciones contractuales para mantener la seguridad de la información proporcionada por terceros
2	2.cei.a	de bajo interés para la competencia
	2.cei.b	de bajo valor comercial
1	1.cei.a	de pequeño interés para la competencia
	1.cei.b	de pequeño valor comercial
0	0.3	supondría pérdidas económicas mínimas
[da] Interrupción del servicio		
9	9.da	Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones
	9.da2	Probablemente tenga un serio impacto en otras organizaciones
7	7.da	Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones
	9.da2	Probablemente tenga un gran impacto en otras organizaciones
5	5.da	Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones
	5.da2	Probablemente cause un cierto impacto en otras organizaciones
3	3.da	Probablemente cause la interrupción de actividades propias de la Organización
1	1.da	Pudiera causar la interrupción de actividades propias de la Organización

[po] Orden público		
9	9.po	alteración seria del orden público
6	6.po	probablemente cause manifestaciones, o presiones significativas
3	3.po	causa de protestas puntuales
1	1.po	pudiera causar protestas puntuales
[olm] Operaciones		
10	10.olm	Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística
9	9.olm	Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
7	7.olm	Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
5	5.olm	Probablemente merme la eficacia o seguridad de la misión operativa o logística más allá del ámbito local
3	3.olm	Probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local)
1	1.olm	Pudiera mermar la eficacia o seguridad de la misión operativa o logística (alcance local)
[adm] Administración y gestión		
9	9.adm	probablemente impediría seriamente la operación efectiva de la Organización, pudiendo llegar a su cierre
7	7.adm	probablemente impediría la operación efectiva de la Organización
5	5.adm	probablemente impediría la operación efectiva de más de una parte de la Organización
3	3.adm	probablemente impediría la operación efectiva de una parte de la Organización
1	1.adm	pudiera impedir la operación efectiva de una parte de la Organización
[lg] Pérdida de confianza (reputación)		
9	9.lg.a	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con otras organizaciones
	9.lg.b	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con el público en general
7	7.lg.a	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con otras organizaciones
	7.lg.b	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con el público en general
5	5.lg.a	Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con otras organizaciones
	5.lg.b	Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con el público

3	3.lg	Probablemente afecte negativamente a las relaciones internas de la Organización
2	2.lg	Probablemente cause una pérdida menor de la confianza dentro de la Organización
1	1.lg	Pudiera causar una pérdida menor de la confianza dentro de la Organización
0	0.4	no supondría daño a la reputación o buena imagen de las personas u organizaciones
[crm] Persecución de delitos		
8	8.crm	Impida la investigación de delitos graves o facilite su comisión
4	4.crm	Dificulte la investigación o facilite la comisión de delitos

AMENAZA

MAGERIT [4] presenta la categorización de amenazas de la siguiente manera:

NOMENCLATURA	TIPO DE AMENAZA	CRITERIO
[N]	**De Origen Natural**	Son aquellos acontecimientos originados por la naturaleza y suelen manifestarse sin que la intervención humana sea participe o causante de dicha manifestación.
[I]	**De Origen Industrial**	Son los acontecimientos originados industrialmente con intervención de la mano del hombre; dichos sucesos pueden ser provocados intencionalmente o de manera imprevista.
[E]	**Errores y Fallos No Intencionados**	Son aquellos acontecimientos provocados involuntariamente, donde el causal suele provenir mediante la intervención humana.
[A]	**Ataques Intencionados**	Son los acontecimientos provocados deliberadamente o mal intencionados, donde el causal suele originarse mediante la intervención humana.

IMPACTO DEL ACTIVO

NOMENCLATURA	IMPACTO	VALOR	CRITERIO
MA	**MUY ALTO**	**10**	El impacto genera repercusiones muy altas en la institución que pueden ser irreparables.
A	**ALTO**	**7 - 9**	El impacto genera repercusiones perjudiciales en la institución.
M	**MEDIO**	**4 - 6**	El impacto genera repercusiones significativas en los procesos de la institución.
B	**BAJO**	**2 - 3**	El impacto genera repercusiones menores, sin embargo, no perjudica a los procesos críticos de la institución.
MB	**MUY BAJO**	**1**	El impacto no genera repercusiones importantes en la institución.

FRECUENCIA DEL RIESGO

FRECUENCIA	PERIODO	VALOR
MA - Probabilidad muy alta	Diaria (todos los días)	5
A - Probabilidad alta	Semanal (todas las semanas)	4
M - Probabilidad media	Mensual (cada 2 meses)	3
B - Probabilidad baja	Semestral (cada 6 meses)	2
MB - Probabilidad muy baja	Anual (todos los años)	1

VALORACION DEL RIESGO

La valoración del riesgo hace uso de la metodología adoptada por MAGERIT [4].

VALORACION DE RIESGO = IMPACTO * FRECUENCIA

RIESGO		**PROBABILIDAD**				
		MB	**B**	**M**	**A**	**MA**
IMPACTO	**MA**	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Insuficiente	**Tolerable**	**Moderado**	**Importante**	**Intolerable**

TRATAMIENTO DE RIESGO

NOMENCLATURA	**DESCRIPCIÓN**	**DEFINICIÓN**
ER	Evitar el Riesgo	Se refiere al hecho de evadir acciones o escapar de aquellas situaciones donde el riesgo es concurrente. La opción de «evitar» es usada solo cuando las demás alternativas de tratamiento son las menos convenientes.

AR	Aceptar el Riesgo	Está enfocada al hecho de admitir cierta cantidad de pérdida en un rango de exposición, omitiendo las posibles respuestas hacia los riesgos (en caso de manifiesten) por lo que es aceptada la pérdida que se genere.
C/TR	Compartir/Transferir el riesgo	Esta opción de tratamiento se basa en el hecho de minimizar el impacto del riesgo mediante la transferencia de un fragmento del riesgo. Entre los procedimientos más frecuentes se encuentra la adquisición de seguros y la subcontratación.
MR	Mitigar el Riesgo	Se enfoca al hecho de escoger actividades para mitigar y disminuir el impacto y la frecuencia del riesgo.

HERRAMIENTA DE EVALUACIÓN Y CONTROL

El SGSI cuenta con una herramienta de apoyo para el monitoreo y evaluación la cual se encuentra en una hoja de cálculo. Y se divide en hojas:

Portada: Presenta la información resumida y contenida de toda la herramienta, muestra así la evaluación de efectividad de los controles, la calificación obtenida y el nivel de cumplimiento de los mismos.

Escala de evaluación: detalla la clasificación para evaluar cada uno de los aspectos a presentar.

Levantamiento de información: se registra la lista de información a recolectar de la entidad para así conocer los planes y ampliar el panorama general.

Administrativas: contiene los controles administrativos de ISO 27000 para determinar su nivel de cumplimiento, evidencia y observaciones a registrar.

Técnicas: contiene los controles técnicos de ISO 27000 para determinar su nivel de cumplimiento, evidencia y observaciones a registrar.

BIBLIOGRAFÍA

[1] Estrategia de Gobierno en Línea, «Modelo de Seguridad y Privacidad de la Información – MSPI Roles y Responsabilidades» Colombia, Ministerio de Tecnologías de la Información y las Comunicaciones, 2016.

[2] Estrategia de Gobierno en Línea, «Modelo de Seguridad y Privacidad de la Información – MSPI Política General» Colombia, Ministerio de Tecnologías de la Información y las Comunicaciones, 2016.

[3] ISO/IEC 27001 – Information technology, Suiza, Organización Internacional de Normalización.

[4] Consejo Superior de Administración Electrónica, «MAGERIT - versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (Libro II - Catálogo de Elementos),» Madrid, © Ministerio de Hacienda y Administraciones Públicas, 2012.

Anexo 07: Herramienta de monitoreo SGSI.

Logo de la entidad	**INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD HOJA PORTADA**
ENTIDAD EVALUADA	**Nombre de la Entidad**
FECHAS DE EVALUACIÓN	fecha de entrega
ELABORADO POR	Personal de la Entidad

EVALUACIÓN DE EFECTIVIDAD DE CONTROLES - ISO 27001:2013 ANEXO A

No.	Evaluación de Efectividad de controles

	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	70	100	**GESTIONADO**
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	21	100	**REPETIBLE**
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	23	100	**REPETIBLE**
A.8	GESTIÓN DE ACTIVOS	0	100	**INEXISTENTE**
A.9	CONTROL DE ACCESO	0	100	**INEXISTENTE**
A.10	CRIPTOGRAFÍA	0	100	**INEXISTENTE**
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	0	100	**INEXISTENTE**
A.12	SEGURIDAD DE LAS OPERACIONES	0	100	**INEXISTENTE**
A.13	SEGURIDAD DE LAS COMUNICACIONES	0	100	**INEXISTENTE**
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	0	100	**INEXISTENTE**
A.15	RELACIONES CON LOS PROVEEDORES	0	100	**INEXISTENTE**
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	0	100	**INEXISTENTE**
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	0	100	**INEXISTENTE**
A.18	CUMPLIMIENTO	0	100	**INEXISTENTE**
PROMEDIO EVALUACIÓN DE CONTROLES		**8**	**100**	**INICIAL**

NIVEL DE MADUREZ MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

NIVELES DE MADUREZ DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	NIVEL DE CUMPLIMIENTO
Inicial	INTERMEDIO
Repetible	CRÍTICO
Definido	CRÍTICO
Administrado	CRÍTICO

TOTAL DE REQUISITOS CON CALIFICACIONES DE CUMPLIMIENTO	
CRÍTICO	0% a 35%
INTERMEDIO	36% a 70%
SUFICIENTE	71% a 100%

Optimizado	CRÍTICO

Nivel	Descripción
Inicial	En este nivel se encuentran las entidades, que aún no cuenta con una identificación de activos y gestión de riesgos, que les permita determinar el grado de criticidad de la información, respecto a la seguridad y privacidad de la misma, por lo tanto los controles no están alineados con la preservación de la confidencialidad, integridad, disponibilidad y privacidad de la información
Repetible	En este nivel se encuentran las entidades, en las cuales existen procesos procesos básicos de gestión de la seguridad y privacidad de la información. De igual forma existen controles que permiten detectar posibles incidentes de seguridad, pero no se encuentra gestionados dentro del componente planificación del MSPI.
Definido	En este nivel se encuentran las entidades que tienen documentado, estandarizado y aprobado por la dirección, el modelo de seguridad y privacidad de la información. Todos los controles se encuentran debidamente documentados, aprobados, implementados, probados y actualizados.
Administrado	En este nivel se encuentran las entidades, que cuenten con métricas, indicadores y realizan auditorías al MSPI, recolectando información para establecer la efectividad de los controles.
Optimizado	En este nivel se encuentran las entidades, en donde existe un mejoramiento continuo del MSPI, retroalimentando cualitativamente el modelo.

LOGO DE LA ENTIDAD	INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD ADMINISTRATIVA Y TÉCNICA HOJA LEVANTAMIENTO DE INFORMACIÓN
	Nombre de la Entidad

ID. ITEM	ITEM	DESCRIPCIÓN	ISO	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN								
AD.1	**POLITICAS DE SEGURIDAD DE LA INFORMACIÓN**	**Orientación de la dirección para gestión de la seguridad de la información**	**A.5**				**70**	
AD.1.1	Documento de la política de seguridad y privacidad de la Información	Se debe definir un conjunto de políticas para la seguridad de la información aprobada por la dirección, publicada y	A.5.1.1	Solicite la política de seguridad de la información de la entidad y evalúe: a) Si se definen los			60	

		comunicada a los empleados y a las partes externas pertinentes		objetivos, alcance de la política b) Si esta se encuentra alineada con la estrategia y objetivos de la entidad c) Si fue debidamente aprobada y socializada al interior de la entidad por la alta dirección				
AD.1.2	Revisión y evaluación	Las políticas para seguridad de la información se deberían revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas.	A.5.1.2	Revise si la política: a)Define que es seguridad de la información b) La asignación de las responsabilidades generales y específicas para la gestión de la seguridad de la información, a roles definidos; c) Los procesos para manejar las desviaciones			80	

				y las excepciones. Indague sobre los responsables designados formalmente por la dirección para desarrollar, actualizar y revisar las políticas. Verifique cada cuanto o bajo qué circunstancias se revisan y actualizan, verifique la última fecha de emisión de la política frente a la fecha actual y que cambios a sufrido, por lo menos debe haber una revisión anual. **Para la calificación tenga en cuenta que:** 1) Si se empiezan a definir las				

				políticas de seguridad y privacidad de la información basada en el Modelo de Seguridad y Privacidad de la Información, están en 20. 2) Si se revisan y se aprueban las políticas de seguridad y privacidad de la información, , están en 40. 3) Si se divulgan las políticas de seguridad y privacidad de la información, están en 60.				
RESPONSABILIDADES Y ORGANIZACIÓN SEGURIDAD INFORMACIÓN								
A2	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**	**Marco de referencia de gestión para iniciar y controlar la implementación y la**	**A.6**				**21**	

		operación de la seguridad de la información dentro de la organización Garantizar la seguridad del teletrabajo y el uso de los dispositivos móviles						
AD.2.1	**Organización Interna**	**Marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización**	**A.6.1**				**12**	

AD.2.1.1	Roles y responsabilidades para la seguridad de la información	Se deben definir y asignar todas las responsabilidades de la seguridad de la información	A.6.1.1	Para revisarlo frente a la NIST verifique si 1) los roles y responsabilidades frente a la ciberseguridad han sido establecidos 2) los roles y responsabilidades de seguridad de la información han sido coordinados y alineados con los roles internos y las terceras partes externas 3) Los a) proveedores, b) clientes, c) socios, d) funcionarios, e) usuarios privilegiados, f) directores y gerentes (mandos senior), g) personal de seguridad física, h) personal de			60	

				seguridad de la información entienden sus roles y responsabilidades, i) Están claros los roles y responsabilidades para la detección de incidentes Solicite el acto administrativo a través del cual se crea o se modifica las funciones del comité gestión institucional (o e que haga sus veces), en donde se incluyan los temas de seguridad de la información en la entidad, revisado y aprobado por la alta Dirección. Revise la estructura del SGSI: 1) Tiene el				

				SGSI suficiente apoyo de la alta dirección?, esto se ve reflejado en comités donde se discutan temas como la política de SI, los riesgos o incidentes. 2) Están claramente definidos los roles y responsabilidades y asignados a personal con las competencias requeridas?, 3) Están identificadas los responsables y responsabilidades para la protección de los activos? (Una práctica común es nombrar un propietario para cada				

				activo, quien entonces se convierte en el responsable de su protección) 4)Están definidas las responsabilidades para la gestión del riesgo de SI y la aceptación de los riesgos residuales? 5) Están definidos y documentados los niveles de autorización? 6) Se cuenta con un presupuesto formalmente asignado a las actividades del SGSI (por ejemplo, campañas de sensibilización en seguridad de la información)				

AD.2.1.2	Separación de deberes / tareas	Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.	A.6.1.2	Indague como evitan que una persona pueda acceder, modificar o usar activos sin autorización ni detección. La mejor práctica dicta que el inicio de un evento deber estar separado de su autorización. Al diseñar los controles se debería considerar la posibilidad de confabulación. Tenga en cuenta que para las organizaciones pequeñas la separación de deberes puede ser difícil de lograr, en estos casos se deben considerar controles			0	

				compensatorios como revisión periódica de, los rastros de auditoría y la supervisión de cargos superiores.				
AD.2.1.3	Contacto con las autoridades.	Las organizaciones deben tener procedimientos establecidos que especifiquen cuándo y a través de que autoridades se debe contactar a las autoridades (por ejemplo, las encargadas de hacer cumplir la ley, los organismos de reglamentación y las autoridades de supervisión), y	A.6.1.3	Solicite los procedimientos establecidos que especifiquen cuándo y a través de que autoridades se debería contactar a las autoridades, verifique si de acuerdo a estos procedimientos se han reportado eventos o incidentes de SI de forma consistente.			0	

		cómo se debe reportar de una manera oportuna los incidentes de seguridad de la información identificados (por ejemplo, si se sospecha una violación de la ley).						
AD.2.1.4	Contacto con grupos de interés especiales	Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad. Por ejemplo, a través de una membresía	A.6.1.4	Pregunte sobre las membrecías en grupos o foros de interés especial en seguridad de la información en los que se encuentran inscritos las personas responsables de la SI.			0	

AD.2.1.5	Seguridad de la información en la gestión de proyectos	La seguridad de la información se debe integrar al(los) método(s) de gestión de proyectos de la organización, para asegurar que los riesgos de seguridad de la información se identifiquen y traten como parte de un proyecto. Esto se aplica generalmente a cualquier proyecto, independientemente de su naturaleza, por ejemplo, un proyecto para un proceso del negocio principal, TI, gestión de instalaciones y otros procesos de soporte.	A.6.1.5	Pregunte como la Entidad integra la seguridad de la información en el ciclo de vida de los proyectos para asegurar que para asegurar que los riesgos de seguridad de la información se identifiquen y traten como parte del proyecto. Tenga en cuenta que esto no solamente aplica para proyectos de TI, por ejemplo, puede aplicar en proyectos de traslado de activos de información, gestión de instalaciones, personal en outsourcing			0	

				que soporta procesos de la organización. Las mejores prácticas sugieren: a) Que los objetivos de la seguridad de la información se incluyan en los objetivos del proyecto; b) Que la valoración de los riesgos de seguridad de la información se lleve a cabo en una etapa temprana del proyecto, para identificar los controles necesarios; c) Que la seguridad de la información sea parte de todas las fases de la metodología				

				del proyecto aplicada.				
AD.2.2	**Dispositivos Móviles y Teletrabajo**	**Garantizar la seguridad del teletrabajo y uso de dispositivos móviles**	**A.6.2**				**30**	

AD.2.2.1	Política para dispositivos móviles	Se deberían adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	A.6.2.1	Pregunte si la entidad asigna dispositivos móviles a sus funcionarios o permite que los dispositivos de estos ingresen a la entidad. Revise si existe una política y controles para su uso, que protejan la información almacenada o procesada en estos dispositivos y el acceso a servicios te TI desde los mismos. De acuerdo a las mejores prácticas esta política debe considerar, teniendo en cuenta el uso que se le dé al dispositivo, lo siguiente:			60	

				a) el registro de los dispositivos móviles; b) los requisitos de la protección física; c) las restricciones para la instalación de software; d) los requisitos para las versiones de software de dispositivos móviles y para aplicar parches; e) la restricción de la conexión a servicios de información; f) los controles de acceso; g) técnicas criptográficas; h) protección contra software malicioso; i) des habilitación remota,				

				borrado o cierre; j) copias de respaldo; k) uso de servicios y aplicaciones web. Cuando la política de dispositivos móviles permite el uso de dispositivos móviles de propiedad personal, la política y las medidas de seguridad relacionadas también deben considerar: a) la separación entre el uso privado y de la Entidad de los dispositivos, incluido el uso del software para apoyar esta separación y proteger los datos del				

				negocio en un dispositivo privado; b) brindar acceso a la información de la Entidad solo cuando los usuarios hayan firmado un acuerdo de usuario final, en el que se reconocen sus deberes (protección física, actualización del software, etc.), desistir de la propiedad de los datos de la Entidad, permitir el borrado remoto de datos por parte de la organización en caso de robo o pérdida del dispositivo, o cuando ya no se posee autorización para usar el				

				servicio.				

AD.2.2.2	Teletrabajo	Se deberían implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	A.6.2.2	Definición de teletrabajo: El teletrabajo hace referencia a todas las formas de trabajo por fuera de la oficina, incluidos los entornos de trabajo no tradicionales, a los que se denomina "trabajo a distancia", "lugar de trabajo flexible", "trabajo remoto" y ambientes de "trabajo virtual". Indague con la entidad si el personal o terceros pueden realizar actividades de teletrabajo, si la respuesta es positiva solicite la política que			0	

				indica las condiciones y restricciones para el uso del teletrabajo. Las mejores prácticas consideran los siguientes controles: a) la seguridad física existente en el sitio del teletrabajo b) los requisitos de seguridad de las comunicaciones, teniendo en cuenta la necesidad de acceso remoto a los sistemas internos de la organización, la sensibilidad de la información a la que se tendrá acceso y que pasará a través del enlace de comunicació				

				n y la sensibilidad del sistema interno; c) el suministro de acceso al escritorio virtual, que impide el procesamiento y almacenamiento de información en equipo de propiedad privada; d) la amenaza de acceso no autorizado a información o a recursos, por parte de otras personas que usan el mismo equipo, por ejemplo, familia y amigos; e) el uso de redes domésticas y requisitos o restricciones sobre la configuració				

				n de servicios de red inalámbrica; e) acuerdos de licenciamiento de software de tal forma que las organizaciones puedan llegar a ser responsables por el licenciamiento de software de los clientes en estaciones de trabajo de propiedad de los empleados o de usuarios externos; f) requisitos de firewall y de protección contra software malicioso. Las directrices y acuerdos que se consideren deberían incluir: g) el suministro de equipo				

				adecuado y de muebles de almacenamiento para las actividades de teletrabajo, cuando no se permite el uso del equipo de propiedad privada que no está bajo el control de la organización; h) una definición del trabajo permitido, las horas de trabajo, la clasificación de la información que se puede mantener, y los sistemas y servicios internos a los que el tele trabajador está autorizado a acceder; i) el suministro de equipos de				

				comunicación adecuados, incluidos los métodos para asegurar el acceso remoto; j) la revocación de la autoridad y de los derechos de acceso, y la devolución de los equipos cuando las actividades del teletrabajo finalicen.				

SEGURIDAD DE LOS RECURSOS HUMANOS								
AD.3	**SEGURIDAD DE LOS RECURSOS HUMANOS**		**A.7**				**23**	
AD.3.1	**Antes de asumir el empleo**	**Asegurar que el personal y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que son considerados.**	**A.7.1**				**70**	

AD.3.1.1	Selección e investigación de antecedentes	Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deberían ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.	A.7.1.1	Revise el proceso de selección de los funcionarios y contratistas, verifique que se lleva a cabo una revisión de: a) Referencias satisfactorias b) Verificación de la de la hoja de vida del solicitante incluyendo certificaciones académicas y laborales; c) Confirmación de las calificaciones académicas y profesionales declaradas; d) Una verificación más detallada, como la de la información crediticia o de antecedentes			80	

				penales. Cuando un individuo es contratado para un rol de seguridad de la información específico, las organizaciones deberían asegurar que el candidato tenga la competencia necesaria para desempeñar el rol de seguridad; e) sea confiable para desempeñar el rol, especialmente si es crítico para la organización. f) Cuando un trabajo, ya sea una asignación o una promoción, implique que la persona tenga acceso a las				

				instalaciones de procesamiento de información, y en particular, si ahí se maneja información confidencial, por ejemplo, información financiera o información muy confidencial, la organización debería también considerar verificaciones adicionales más detalladas (por ejemplo estudio de seguridad, polígrafo, visita domiciliaria) g) También se debería asegurar un proceso de selección para contratistas. En estos casos, el				

				acuerdo entre la organización y el contratista debería especificar las responsabilidades por la realización de la selección, y los procedimientos de notificación que es necesario seguir si la selección no se ha finalizado, o si los resultados son motivo de duda o inquietud. h) La información sobre todos los candidatos que se consideran para cargos dentro de la organización, se debería recolectar y				

				manejar apropiadamente de acuerdo con la ley de protección de datos personales.				

AD.3.1.2	Términos y condiciones del empleo	Los acuerdos contractuales con empleados y contratistas, deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.	A.7.1.2				60	
AD.3.2	**Durante la ejecución del empleo**	**Asegurar que los funcionarios y contratistas tomen consciencia de sus responsabilidades sobre la seguridad de la información y las cumplan.**	**A.7.1.2**				**0**	

AD.3.2.1	Responsabilidades de la dirección	La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.	A.7.2.1	De acuerdo a la NIST los contratistas deben estar coordinados y alineados con los roles y responsabilidades de seguridad de la información. Indague y solicite evidencia del como la dirección se asegura de que los empleados y contratistas: a) Estén debidamente informados sobre sus roles y responsabilidades de seguridad de la información, antes de que se les otorgue el acceso a información o sistemas de información confidenciales.			0	

				b) Se les suministren las directrices que establecen las expectativas de seguridad de la información de sus roles dentro de la Entidad. c) Logren un nivel de toma de conciencia sobre seguridad de la información pertinente a sus roles y responsabilidades dentro de la organización y estén motivados para cumplir con las políticas. d) Tengan continuamente las habilidades y calificaciones apropiadas y reciban capacitación en forma regular.				

				e) Cuenten con un canal para reporte anónimo de incumplimiento de las políticas o procedimientos de seguridad de la información (“denuncias internas”).				

AD.3.2.2	Toma de conciencia, educación y formación en la seguridad de la información	Todos los empleados de la Entidad, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.	A.7.2.2	Entreviste a los líderes de los procesos y pregúnteles que saben sobre la seguridad de la información, cuáles son sus responsabilidades y como aplican la seguridad de la información en su diario trabajo. Pregunte como se asegura que los funcionarios, Directores, Gerentes y contratistas tomen conciencia en seguridad de la información, alineado con las responsabilidades, políticas y procedimientos existentes en la Entidad.			0	

				Solicite el documento con el plan de comunicación, sensibilización y capacitación, con los respectivos soportes, revisado y aprobado por la alta Dirección. Verifique que se han tenido en cuenta buenas prácticas como: a) Desarrollar campañas, elaborar folletos y boletines. b) Los planes de toma de conciencia y comunicación, de las políticas de seguridad y privacidad de la información, están aprobados y				

				documentados, por la alta Dirección c) Verifique que nuevos empleados y contratistas son objeto de sensibilización en SI. d) Indague cada cuanto o con qué criterios se actualizan los programas de toma de conciencia. e) Verifique que en las evidencias se puede establecer los asistentes al programa y el tema impartido. f) Incluir en los temas de toma de conciencia los procedimientos básicos de seguridad de la información (tales como el reporte de incidentes de				

				seguridad de la información) y los controles de línea base (tales como la seguridad de las contraseñas, los controles del software malicioso, y los escritorios limpios). g) De acuerdo a NIST verifique que los funcionarios con roles privilegiados entienden sus responsabilidades y roles. **Para la calificación tenga en cuenta que:** Si Los funcionarios de la Entidad no tienen conciencia de la seguridad y privacidad de la información.				

				Diseñar programas para los conciencia y comunicación, de las políticas de seguridad y privacidad de la información, **están en 20.** Si se observa en los funcionarios una conciencia de seguridad y privacidad de la información y los planes de toma de conciencia y comunicación, de las políticas de seguridad y privacidad de la información, deben estar aprobados y documentados, por la alta Dirección, **están en 40.** Si se han ejecutado los planes de				

				toma de conciencia, comunicación y divulgación, de las políticas de seguridad y privacidad de la información, aprobados por la alta Dirección, **están en 60.**				

AD.3.2.3	Proceso disciplinario	Se debe contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	A.7.2.3	Pregunte cual es el proceso disciplinario que se sigue cuando se verifica que ha ocurrido una violación a la seguridad de la información, quien y como se determina la sanción al infractor?			0	
AD.3.3	**Terminación y cambio de empleo**	**Proteger los intereses de la Entidad como parte del proceso de cambio o terminación de empleo.**	**A.7.3**				**0**	
AD.5.1.3	Terminación o cambio de responsabilidades de empleo	Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de contrato se deberían	A.7.3.1	Revisar los acuerdos de confidencialidad, verificando que deben acordar que después de terminada la relación laboral o contrato seguirán vigentes por			0	

		definir, comunicar al empleado o contratista y se deberían hacer cumplir.		un periodo de tiempo.				
GESTIÓN DE ACTIVOS								
AD.4	**GESTIÓN DE ACTIVOS**		**A.8**				**0**	
AD.4.1	**Responsabilidad de los activos**	**Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.**	**A.8.1**				**0**	

AD.4.1.1	Inventario de activos	Se deben identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	A.8.1.1	Solicite el inventario de activos de información, revisado y aprobado por la alta Dirección y revise: 1) Ultima vez que se actualizó 2) Que señale bajo algún criterio la importancia del activo 3) Que señale el propietario del activo Indague quien(es) el(los) encargado(s) de actualizar y revisar el inventario de activos y cada cuanto se realiza esta revisión. De acuerdo a NIST se deben considerar como activos el personal, dispositivos, sistemas e instalaciones			0	

				físicas que permiten a la entidad cumplir con su misión y objetivos, dada su importancia y riesgos estratégicos. **Tenga en cuenta para la calificación:** 1) Si Se identifican en forma general los activos de información de la Entidad, están en 40. 2) Si se cuenta con un inventario de activos de información física y lógica de toda la entidad, documentado y firmado por la alta dirección, están en 60. 3) Si se revisa y monitorean periódicamen				

				te los activos de información de la entidad, están en 80.				

AD.4.1.2	Propiedad de los activos	Los activos mantenidos en el inventario deben tener un propietario.	A.8.1.2	Solicite el procedimiento para asegurar la asignación oportuna de la propiedad de los activos. Tenga en cuenta que la propiedad se debería asignar cuando los activos se crean o cuando son entregados a la Entidad. De acuerdo a las mejores prácticas el propietario de los activos (individuo o entidad, que es responsable por el activo) tiene las siguientes responsabilidades: a) asegurarse de que los activos están inventariados; b) asegurarse			0	

				de que los activos están clasificados y protegidos apropiadamente; c) definir y revisar periódicamente las restricciones y clasificaciones de acceso a activos importantes, teniendo en cuenta las políticas de control de acceso aplicables; d) asegurarse del manejo apropiado del activo cuando es eliminado o destruido.				
AD.4.1.3	Uso aceptable de los activos	Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con	A.8.1.3	Pregunte por la política, procedimiento, directriz o lineamiento que defina el uso aceptable de los activos, verifique que es conocida			0	

		información e instalaciones de procesamiento de información.		por los empleados y usuarios de partes externas que usan activos de la Entidad o tienen acceso a ellos.				
AD.4.1.4	Devolución de activos	Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	A.8.1.4	Revisar las políticas , normas , procedimientos y directrices relativas a los controles de seguridad de la información durante la terminación de la relación laboral por ejemplo, la devolución de los activos de información (equipos, llaves, documentos , datos, sistemas) , las llaves físicas y de cifrado, la eliminación de los			0	

				derechos de acceso, etc. En caso de que un funcionario o tercero sea el dueño del activo indague como se asegura la transferencia de la información a la Entidad y el borrado seguro de la información de la Entidad. En caso en que un empleado o usuario de una parte externa posea conocimientos que son importantes para las operaciones regulares, esa información se debería documentar y transferir a la Entidad. Durante el período de notificación de la				

				terminación, la Entidad debería controlar el copiado no autorizado de la información pertinente (por ejemplo, la propiedad intelectual) por parte de los empleados o contratistas que han finalizado el empleo.				
AD.4.2	**Clasificación de información**	**Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la Entidad.**	**A.8.2**				**0**	

AD.4.2.1	Clasificación de la información	La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	A.8.2.1	Solicite el procedimiento mediante el cual se clasifican los activos de información y evalué: 1) Que las convenciones y criterios de clasificación sean claros y estén documentados 2) Que se defina cada cuanto debe revisarse la clasificación de un activo 3) La clasificación debería valorarse analizando la confidencialidad, integridad y disponibilidad. Solicite muestras de inventarios de activos de información clasificados y evalué que se			0	

				aplican las políticas y procedimientos de clasificación definidos. Evalué si los procesos seleccionados aplican de manera consistente estas políticas y procedimientos.				
AD.4.2.2	Etiquetado de la información		A.8.2.2	Solicite el procedimiento para el etiquetado de la información y evalúe: 1) Aplica a activos en formatos físicos y electrónicos (etiquetas físicas, metadatos) 2) Que refleje el esquema de clasificación establecido 3) Que las etiquetas se puedan			0	

				reconocer fácilmente 4) Que los empleados y contratistas conocen el procedimiento de etiquetado Revise en una muestra de activos el correcto etiquetado				
AD.4.2.3	Manejo de activos		A.8.2.3	Solicite los procedimientos para el manejo, procesamiento, almacenamiento y comunicación de información de conformidad con su clasificación. De acuerdo a las mejores prácticas evidencie si se han considerado los siguientes asuntos: a) Restricciones de acceso			0	

				que soportan los requisitos de protección para cada nivel de clasificación; b) Registro formal de los receptores autorizados de los activos; c) Protección de copias de información temporal o permanente a un nivel coherente con la protección de la información original; d) Almacenamiento de los activos de TI de acuerdo con las especificaciones de los fabricantes; e) Marcado claro de todas las copias de medios para la atención del receptor				

				autorizado. f) De acuerdo a NIST la información almacenada (at rest) y en tránsito debe ser protegida.				
AD.4.3	**Manejo de medios**	**Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de la información almacenada en los medios.**	**A.8.3**				**0**	

AD.4.3.1	Gestión de medios removibles		A.8.3.1	Solicite las directrices, guías, lineamientos y procedimientos para la gestión de medios removibles, que consideren: a) Si ya no se requiere, el contenido de cualquier medio reusable que se vaya a retirar de la organización se debe remover de forma que no sea recuperable; b) cuando resulte necesario y práctico, se debe solicitar autorización para retirar los medios de la organización, y se debe llevar un registro de dichos retiros			0	

				con el fin de mantener un rastro de auditoría; d) si la confidencialidad o integridad de los datos se consideran importantes, se deben usar técnicas criptográficas para proteger los datos que se encuentran en los medios removibles; f) se deben guardar varias copias de los datos valiosos en medios separados, para reducir aún más el riesgo de daño o pérdida casuales de los datos; h) sólo se deben habilitar unidades de medios removibles si hay una				

				razón de valida asociada a los procesos la Entidad para hacerlo; i) En donde hay necesidad de usar medios removibles, se debería hacer seguimiento a la transferencia de información a estos medios (Por ejemplo DLP)				
AD.4.3.2	Disposición de los medios		A.8.3.2	Solicite los procedimientos existentes para garantizar que los medios a desechar o donar, no contienen información confidencial que pueda ser consultada y copiada por			0	

				personas no autorizadas. Verifique si se ha realizado esta actividad y si existen registros de la misma.				
AD.4.3.3	Transferencia de medios físicos		A.8.3.3	Solicite las directrices definidas para la protección de medios que contienen información durante el transporte. Verifique de acuerdo a las mejores prácticas que se contemple: a) El uso de un transporte o servicios de mensajería confiables. b) Procedimientos para verificar la identificación de los servicios de mensajería. c) Indague y			0	

				evidencie como es el embalaje el cual debe proteger el contenido contra cualquier daño físico que pudiera presentarse durante el tránsito, y de acuerdo con las especificaciones de los fabricantes, por ejemplo, protección contra cualquier factor ambiental que pueda reducir la eficacia de la restauración del medio, tal como exposición al calor, humedad o campos electromagnéticos; d) Solicite los registros que dejen evidencia del				

				transporte donde se identifique el contenido de los medios, la protección aplicada, al igual que los tiempos de transferencia a los responsables durante el transporte, y el recibo en su destino.				
ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO								
AD.5	**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**		**A.17**				**0**	

AD.5.1	**Continuidad de la seguridad de la información**	**La continuidad de la seguridad de la información debe incluir en los sistemas de gestión de la continuidad del negocio de la Entidad.**	**A.17.1**				**0**	

AD.5.1.1	Planificación de la continuidad de la seguridad de la información		A.17.1.1	Indagar si la Entidad cuenta con un BCP (Bussines Continuity Plan) o DRP (Disaster Recovery Plan). Determine si aplica para procesos críticos solamente o se han incluido otros procesos o por lo menos se ha reconocido la necesidad de ampliarlo a otros procesos (para determinar el nivel de madurez) Evalúe si se ha incluido en estos planes y procedimientos los requisitos de seguridad de la información. Tenga en			0	

				cuenta que en ausencia de una planificación formal de continuidad de negocio y recuperación de desastres, la dirección de seguridad de la información debería suponer que los requisitos de seguridad de la información siguen siendo los mismos en situaciones adversas, en comparación con las condiciones operacionales normales. Como alternativa, una organización puede llevar a cabo un análisis de impacto en el negocio de los aspectos de seguridad				

				de la información, para determinar los requisitos de seguridad de la información aplicables a situaciones adversas. De acuerdo a la NIST también se deben tener planes de respuesta a incidentes y recuperación de incidentes. **Tenga en cuenta para la calificación:** 1) Si existen planes de continuidad del negocio que contemplen los procesos críticos de la Entidad que garanticen la continuidad de los mismos. Se documentan tan y protegen				

				adecuadamente los planes de continuidad del negocio de la Entidad, este de estar documentado y firmado, por la alta Dirección**, están en 40.** 2) Si se reconoce la importancia de ampliar los planes de continuidad de del negocio a otros procesos, pero aún no se pueden incluir ni trabajar con ellos, **están en 60.**				

AD.5.1.2	Implementación de la continuidad de la seguridad de la información	La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para garantizar el nivel necesario de continuidad para la seguridad de la información durante una situación adversa,	A.17.1.2	Verifique si la entidad cuenta con a) Una estructura organizacional adecuada para prepararse, mitigar y responder a un evento contingente, usando personal con la autoridad, experiencia y competencia necesarias. b) Personal formalmente asignado de respuesta a incidentes con la responsabilidad, autoridad y competencia necesarias para manejar un incidente y mantener la seguridad de la información. c) Planes aprobados, procedimientos de			0	

				respuesta y recuperación documentados, en los que se especifique en detalle como la organización gestionará un evento contingente y mantendrá su seguridad de la información en un límite predeterminado, con base en los objetivos de continuidad de seguridad de la información aprobados por la dirección. Revise si los controles de seguridad de la información que se han implementado continúan operando durante un evento				

				contingente. Si los controles de seguridad no están en capacidad de seguir brindando seguridad a la información, se la Entidad debe establecer, implementar y mantener otros controles para mantener un nivel aceptable de seguridad de la información.				

AD.5.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.		A.17.1.3	Indague y solicite evidencias de la realización de pruebas de la funcionalidad de los 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; Tenga en cuenta que la verificación de los controles de continuidad de la seguridad de la información es diferente de las			0	

				pruebas y verificación generales de seguridad de la información. Si es posible, es preferible integrar la verificación de los controles de continuidad de negocio de seguridad de la información con las pruebas de recuperación de desastres y de continuidad de negocio de la organización.				
AD.5.2	**Redundancias**	**Asegurar la disponibilidad de las instalaciones de procesamiento de la información.**	**A.17.2**				**0**	

AD.5.2.1	Disponibilidad de instalaciones de procesamiento de información		A.17.2.1	Verifique si la Entidad cuenta con arquitecturas redundantes, ya sea un centro de cómputo principal y otro alterno o componentes redundantes en el único centro de cómputo. Indague como se han definido las necesidades de los procesos para seleccionar que elementos deben ser redundantes. Solicite si aplica las pruebas aplicadas para asegurar que un componente redundante funciona de la forma prevista durante una emergencia o falla.			0	

CUMPLIMIENTO								
AD.6	**CUMPLIMIENTO**		**A.18**				**0**	
AD.6.1	**Cumplimiento de requisitos legales y contractuales**	**Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.**	**A.18.1**	**De acuerdo a la NIST: Los requerimientos legales y regulatorios respecto de la ciberseguridad, incluyendo la privacidad y las libertades y obligaciones civiles, son entendidos y gestionados.**			**0**	
AD.6.1.1	Identificación de la legislación aplicable y de los requisitos contractuales.		A.18.1.1	Solicite la relación de requisitos legales, reglamentarios, estatutarios, que le aplican a la Entidad (Normograma). Indague si existe un responsable			0	

				de identificarlos y se definen los responsables para su cumplimiento.				
AD.6.1.2	Derechos de propiedad intelectual.		A.18.1.2	1) Solicite los procedimientos para el cumplimiento de los requisitos y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados. 2) Verifique si la Entidad cuenta con una política publicada sobre el cumplimiento de derechos de propiedad intelectual que defina el uso legal del software y de productos informáticos.			0	

				Esta política debe estar orientada no solo al software, sino también a documentos gráficos, libros, etc. 3) Indague como se controla que no se instale software ilegal. 4) Indague si se tiene un inventario de software instalado y se compara con el número de licencias adquiridas para asegurar que no se incumplen los derechos de propiedad intelectual. Tenga en cuenta los controles que deben existir para asegurar que no se exceda ningún número máximo de				

				usuarios permitido dentro de la licencia.				
AD.6.1.3	Protección de registros.	Se deben proteger los registros importantes de una organización de pérdida, destrucción y falsificación, en concordancia con los requerimientos estatutarios, reguladores, contractuales y comerciales	A.18.1.3	Revise si la Entidad cuenta con tablas de retención documental que especifiquen los registros y el periodo por el cual se deberían retener, además del almacenamiento, manejo y destrucción. Posibles tipos de registros pueden ser registros			0	

				contables, registros de bases de datos, logs de transacciones, logs de auditoría y procedimientos operacionales, los medios de almacenamiento permitidos pueden ser papel, microfichas, medios magnéticos, medios ópticos etc.				
AD.6.1.4	Protección de los datos y privacidad de la información relacionada con los datos personales.	Se deben asegurar la protección y privacidad de la información personal tal como se requiere en la legislación relevante, las regulaciones y, si fuese aplicable, las cláusulas contractuales.	A.18.1.4	Indague sobre las disposiciones que ha definido la Entidad para cumplir con la legislación de privacidad de los datos personales, ley estatutaria 1581 de 2012 y decreto 1377 que reglamenta la ley de 2013.			0	

				1) Revise si existe una política para cumplir con la ley 2) Si están definidos los responsables 3) Si se tienen identificados los repositorios de datos personales 4) Si se ha solicitado consentimiento al titular para tratar los datos personales y se guarda registro de este hecho. 5) Si se adoptan las medidas técnicas necesarias para proteger las bases de datos donde reposan estos datos.				
AD.6.1.5	Reglamentación de controles criptográficos.		A.18.1.5	n/a			n/a	

AD.6.2	**Revisiones de seguridad de la información**		**A.18.2**				**0**	
AD.6.2.1	Revisión independiente de la seguridad de la información		A.18.2.1	Investigue la forma como se realizan revisiones independientes (por personas diferentes o no vinculadas a un proceso o área que se revisa), de la conveniencia, la adecuación y la eficacia continuas de la gestionar la seguridad de la información. Para esto solicite: 1) El plan de auditorías del año 2015 2) El resultado de las auditorías del año 2015 3) Las oportunidades de mejora o cambios en la seguridad de la			0	

				información identificados.				
AD.6.2.2	Cumplimiento con las políticas y normas de seguridad.	Asegurar el cumplimiento de los sistemas con las políticas y estándares de seguridad organizacional.	A.18.2.2	1) Verifique si los gerentes aseguran que todos los procedimientos de seguridad dentro de su área de responsabilidad se llevan a cabo correctamente para lograr el cumplimiento de las políticas y estándares de seguridad. 2) Verifique la revisión periódica del cumplimiento del centro de cómputo con las			0	

				políticas y normas de seguridad establecidas. 3) Verifique si los sistemas de información son revisados regularmente para asegurar el cumplimiento de las normas de seguridad de la información				
AD.6.2.3	Revisión de cumplimiento técnico.	Los sistemas de información deben chequearse regularmente para el cumplimiento con los estándares de implementación de la seguridad.	A.18.2.3	Verifique si se realizan evaluaciones de seguridad técnicas por o bajo la supervisión de personal autorizado, apoyado en herramientas automáticas o con revisiones manuales realizadas por especialistas. Solicite evidencia de las últimas pruebas			0	

				realizadas, sus resultados y seguimiento para asegurar que las brechas de seguridad fueron solucionadas.				
RELACIONES CON LOS PROVEEDORES								
AD.7	**RELACIONES CON LOS PROVEEDORES**		**A.15**				**0**	

AD.7.1	Seguridad de la información en las relaciones con los proveedores	Asegurar la protección de los activos de la entidad que sean accesibles para los proveedores	A.15.1	1) Solicite la política de seguridad de la información para las relaciones con los proveedores, que indique los requisitos de SI para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización, esta política debe reflejarse en los acuerdos con los proveedores que deben estar documentados. 2) Verifique en la muestra de proveedores con acceso a los activos de información (no necesariamen			0	

				te son proveedores de tecnología de la información, por ejemplo pueden ser proveedores que tengan por ejemplo un proceso de nómina en outsourcing), se hayan suscrito acuerdos (ANS) formales donde se establezcan y acuerden todos los requisitos de seguridad de la información pertinentes con cada proveedor. 3) Verifique para los proveedores si se tiene en cuenta los riesgos de SI asociados a la cadena de suministro, por ejemplo para los				

				proveedores en la nube es muy común que se apoyen en otros proveedores para proporcionar las instalaciones y se deben manejar los riesgos asociados a este tercero con el cual la entidad no tiene una relación comercial directa. Solicite que le indiquen como identifican para cada proveedor su cadena de suministro y obtenga evidencia de este hecho.				

AD.7.2	Gestión de la prestación de servicios de proveedores	Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores	A.15.2	1) Indague y solicite evidencia en una muestra de proveedores seleccionada, como la entidad hace seguimiento, revisa y audita con regularidad de acuerdo a la política la prestación de servicios de los proveedores y el cumplimiento de los compromisos respecto a la seguridad de la información. 2) Indague y evidencie como se gestionan los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las			0	

				políticas, procedimientos y controles de seguridad de la información existentes , teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, los incidentes de seguridad de la información y la revaloración de los riesgos. 2)				

Anexo 08: Validación expertos de herramienta.

Anexo 3: FICHA DE VALIDACIÓN A JUICIO DE EXPERTOS

TÍTULO DE LA TESIS: MODELO BASADO EN LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA PROTEGER LOS DATOS EN LAS FARMACIAS DE LOS HOSPITALES II-1 EN LA REGIÓN AMAZONAS

N°	CRITERIO	VALORES	INSTRUCCIONES
01	RELACIÓN ENTRE LA VARIABLE Y LA DIMENSIÓN	Escala Likert Mín. 01 Máx. 05	Luego de leer y analizar cada uno de los ítems del instrumento de investigación, en forma individual, marcar con un aspa uno de los valores de la escala para cada criterio, recordando que la evaluación va de 1 hasta 5. Luego exprese su comentario sobre el ítem en el espacio correspondiente o señale que está correcto.
02	RELACIÓN ENTRE LA DIMENSIÓN Y EL INDICADOR		
03	RELACIÓN ENTRE EL INDICADOR Y EL ITEM		
04	RELACIÓN ENTRE EL ITEMS Y LA OPCIÓN DE RESPUESTA		

VARIABLE	DIMENSIÓN	INDICADOR	ÍTEMS	CRITERIOS DE EVALUACIÓN				OBSERVACIONES Y/O RECOMENDACIONES
				RELACIÓN ENTRE LA VARIABLE Y LA DIMENSIÓN	RELACIÓN ENTRE LA DIMENSIÓN Y EL INDICADOR	RELACIÓN ENTRE EL INDICADOR Y EL ÍTEM	RELACIÓN ENTRE EL ÍTEM Y LA OPCIÓN DE RESPUESTA (Ver instrumento detallado adjunto)	
Contribuir en la gestión de las farmacias de los hospitales II-I en la región Amazonas.	Gestión de seguridad de la información	Numero de Instituciones que cuentan con Plan Estratégico	¿La institución cuenta con un Plan Estratégico?	5	5	5	5	
		Numero de Instituciones que cuentan con Manual de Organización y Funciones	¿La institución cuenta con un Manual Organización y Funciones?	5	5	5	5	
		Numero de Instituciones que cuentan con Plan Estratégico de Tecnologías de la Información.	¿La institución cuenta con un Plan Estratégico de Tecnologías de la Información o similar?	5	5	5	5	
		Numero de Instituciones que cuentan con Política de Gestión de Riesgos de Tecnologías de la Información	¿La institución cuenta con una Política de Gestión de Riesgos de Tecnologías de la Información o similar?	5	5	5	5	

		Numero de Instituciones que cuentan con Política de Seguridad de la Información	¿La institución cuenta con una Política de seguridad de la información o similar?	**5**	**5**	**5**	**5**	
		Numero de Instituciones que cuentan con Directiva de Inventario y Gestión de Activos de Información.	¿La institución cuenta con una Directiva de Inventario y Gestión de Activos de Información o similar?	**5**	**5**	**5**	**5**	
		Numero de Instituciones que proporcionan capacitaciones sobre Seguridad de la Información a los trabajadores.	¿La institución proporciona capacitaciones sobre Seguridad de la Información a los trabajadores dentro y fuera de TI?	**5**	**5**	**5**	**5**	
		Numero de Instituciones que cuenten con un Plan de Gestión de la Calidad de la información.	¿La institución cuenta con un Plan de Gestión de la Calidad de la Información, donde detalle los requisitos mínimos y criterios de los mismos?	**5**	**5**	**5**	**5**	
		Numero de Instituciones que cuenten con un Plan de Copias de Seguridad y Restauración.	¿La institución cuenta con un Plan de copias de seguridad y restauración?	**5**	**5**	**5**	**5**	
		Frecuencia de Copias de Seguridad.	¿Con que frecuencia realiza copias de seguridad de la información?	**5**	**5**	**5**	**5**	

ALEX FRANKLIN CORONADO NAVARRO
INGENIERO DE SISTEMAS
Reg. CIP. 171209

Mg. Ing. Alex Coronado Navarro
DNI 42900381

USAT Posgrado

"AÑO DE LA UNIVERSALIZACIÓN DE LA SALUD"

INFORME DE VALIDACIÓN DEL INSTRUMENTO

1. TÍTULO DE LA INVESTIGACIÓN:

Modelo basado en la gestión de seguridad de la información para proteger los datos en las farmacias de los Hospitales II-1 en la región Amazonas.

2. NOMBRE DEL INSTRUMENTO:

Cuestionario de Diagnostico Situacional sobre Seguridad de la Información en Hospitales de la Región Amazonas.

3. TESISTA:

Jaime Izquierdo Cabrera.

4. DECISIÓN:

Después de haber revisado el instrumento de recolección de datos, procedió a validarlo teniendo en cuenta su forma, estructura y profundidad; por lo tanto, permitirá recoger información concreta y real de la variable en estudio, coligiendo su pertinencia y utilidad.

OBSERVACIONES: Apto para su aplicación.

APROBADO: SI [X] NO [ ]

Chiclayo, 12 de diciembre del 2020

ALEX FRANKLIN CORONADO NAVARRO
INGENIERO DE SISTEMAS
Reg. CIP. 171209

Mg. Ing. Alex Coronado Navarro
DNI N° 42900381

Anexo 3: FICHA DE VALIDACIÓN A JUICIO DE EXPERTOS

TÍTULO DE LA TESIS: MODELO BASADO EN LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA PROTEGER LOS DATOS EN LAS FARMACIAS DE LOS HOSPITALES II-1 EN LA REGIÓN AMAZONAS

N°	CRITERIO	VALORES	INSTRUCCIONES
01	RELACIÓN ENTRE LA VARIABLE Y LA DIMENSIÓN	Escala Likert Mín. 01 Máx. 05	Luego de leer y analizar cada uno de los ítems del instrumento de investigación, en forma individual, marcar con un aspa uno de los valores de la escala para cada criterio, recordando que la evaluación va de 1 hasta 5. Luego exprese su comentario sobre el ítem en el espacio correspondiente o señale que está correcto.
02	RELACIÓN ENTRE LA DIMENSIÓN Y EL INDICADOR		
03	RELACIÓN ENTRE EL INDICADOR Y EL ITEM		
04	RELACIÓN ENTRE EL ITEMS Y LA OPCIÓN DE RESPUESTA		

VARIABLE	DIMENSIÓN	INDICADOR	ÍTEMS	CRITERIOS DE EVALUACIÓN				OBSERVACIONES Y/O RECOMENDACIONES
				RELACIÓN ENTRE LA VARIABLE Y LA DIMENSIÓN	RELACIÓN ENTRE LA DIMENSIÓN Y EL INDICADOR	RELACIÓN ENTRE EL INDICADOR Y EL ÍTEM	RELACIÓN ENTRE EL ÍTEM Y LA OPCIÓN DE RESPUESTA (Ver instrumento detallado adjunto)	
Contribuir en la gestión de las farmacias de los hospitales II-I en la región Amazonas.	Gestión de seguridad de la información	Numero de Instituciones que cuentan con Plan Estratégico	¿La institución cuenta con un Plan Estratégico?	5	5	5	5	
		Numero de Instituciones que cuentan con Manual de Organización y Funciones	¿La institución cuenta con un Manual Organización y Funciones?	4	5	5	5	
		Numero de Instituciones que cuentan con Plan Estratégico de Tecnologías de la Información.	¿La institución cuenta con un Plan Estratégico de Tecnologías de la Información o similar?	5	5	5	5	
		Numero de Instituciones que cuentan con Política de Gestión de Riesgos de Tecnologías de la Información	¿La institución cuenta con una Política de Gestión de Riesgos de Tecnologías de la Información o similar?	5	5	5	5	

		Numero de Instituciones que cuentan con Política de Seguridad de la Información	¿La institución cuenta con una Política de seguridad de la información o similar?	**5**	**5**	**5**	**5**	
		Numero de Instituciones que cuentan con Directiva de Inventario y Gestión de Activos de Información.	¿La institución cuenta con una Directiva de Inventario y Gestión de Activos de Información o similar?	**5**	**5**	**5**	**5**	
		Numero de Instituciones que proporcionan capacitaciones sobre Seguridad de la Información a los trabajadores.	¿La institución proporciona capacitaciones sobre Seguridad de la Información a los trabajadores dentro y fuera de TI?	**4**	**5**	**5**	**5**	
		Numero de Instituciones que cuenten con un Plan de Gestión de la Calidad de la información.	¿La institución cuenta con un Plan de Gestión de la Calidad de la Información, donde detalle los requisitos mínimos y criterios de los mismos?	**4**	**5**	**5**	**5**	
		Numero de Instituciones que cuenten con un Plan de Copias de Seguridad y Restauración.	¿La institución cuenta con un Plan de copias de seguridad y restauración?	**5**	**5**	**5**	**5**	
		Frecuencia de Copias de Seguridad.	¿Con que frecuencia realiza copias de seguridad de la información?	**5**	**5**	**5**	**5**	

Mg. Ing. Cesar Augusto Minguillo Rubio

DNI 16787173

"AÑO DE LA UNIVERSALIZACIÓN DE LA SALUD"

INFORME DE VALIDACIÓN DEL INSTRUMENTO

1. TÍTULO DE LA INVESTIGACIÓN:

Modelo basado en la gestión de seguridad de la información para proteger los datos en las farmacias de los Hospitales II-1 en la región Amazonas.

2. NOMBRE DEL INSTRUMENTO:

Cuestionario de Diagnostico Situacional sobre Seguridad de la Información en Hospitales de la Región Amazonas.

3. TESISTA:

Jaime Izquierdo Cabrera.

4. DECISIÓN:

Después de haber revisado el instrumento de recolección de datos, procedió a validarlo teniendo en cuenta su forma, estructura y profundidad; por lo tanto, permitirá recoger información concreta y real de la variable en estudio, coligiendo su pertinencia y utilidad.

OBSERVACIONES: Apto para su aplicación.

APROBADO: SI [X] NO [ ]

Chiclayo, 18 de diciembre del 2020

Mg. Ing. Cesar Augusto Minguillo Rubio
DNI N° 16787173

Anexo 3: FICHA DE VALIDACIÓN A JUICIO DE EXPERTOS

TÍTULO DE LA TESIS: MODELO BASADO EN LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA PROTEGER LOS DATOS EN LAS FARMACIAS DE LOS HOSPITALES II-1 EN LA REGIÓN AMAZONAS

N°	CRITERIO	VALORES	INSTRUCCIONES
01	RELACIÓN ENTRE LA VARIABLE Y LA DIMENSIÓN	Escala Likert Mín. 01 Máx. 05	Luego de leer y analizar cada uno de los ítems del instrumento de investigación, en forma individual, marcar con un aspa uno de los valores de la escala para cada criterio, recordando que la evaluación va de 1 hasta 5. Luego exprese su comentario sobre el ítem en el espacio correspondiente o señale que está correcto.
02	RELACIÓN ENTRE LA DIMENSIÓN Y EL INDICADOR		
03	RELACIÓN ENTRE EL INDICADOR Y EL ITEM		
04	RELACIÓN ENTRE EL ITEMS Y LA OPCIÓN DE RESPUESTA		

VARIABLE	DIMENSIÓN	INDICADOR	ÍTEMS	CRITERIOS DE EVALUACIÓN				OBSERVACIONES Y/O RECOMENDACIONES
				RELACIÓN ENTRE LA VARIABLE Y LA DIMENSIÓN	RELACIÓN ENTRE LA DIMENSIÓN Y EL INDICADOR	RELACIÓN ENTRE EL INDICADOR Y EL ÍTEM	RELACIÓN ENTRE EL ÍTEM Y LA OPCIÓN DE RESPUESTA (Ver instrumento detallado adjunto)	
Contribuir en la gestión de las farmacias de los hospitales II-I en la región Amazonas.	Gestión de seguridad de la información	Numero de Instituciones que cuentan con Plan Estratégico	¿La institución cuenta con un Plan Estratégico?	5	5	5	5	
		Numero de Instituciones que cuentan con Manual de Organización y Funciones	¿La institución cuenta con un Manual Organización y Funciones?	5	5	5	5	
		Numero de Instituciones que cuentan con Plan Estratégico de Tecnologías de la Información.	¿La institución cuenta con un Plan Estratégico de Tecnologías de la Información o similar?	5	5	5	5	
		Numero de Instituciones que cuentan con Política de Gestión de Riesgos de Tecnologías de la Información	¿La institución cuenta con una Política de Gestión de Riesgos de Tecnologías de la Información o similar?	5	5	5	5	

		Numero de Instituciones que cuentan con Política de Seguridad de la Información	¿La institución cuenta con una Política de seguridad de la información o similar?	**5**	**5**	**5**	**5**	
		Numero de Instituciones que cuentan con Directiva de Inventario y Gestión de Activos de Información.	¿La institución cuenta con una Directiva de Inventario y Gestión de Activos de Información o similar?	**5**	**5**	**5**	**5**	
		Numero de Instituciones que proporcionan capacitaciones sobre Seguridad de la Información a los trabajadores.	¿La institución proporciona capacitaciones sobre Seguridad de la Información a los trabajadores dentro y fuera de TI?	**5**	**5**	**5**	**5**	
		Numero de Instituciones que cuenten con un Plan de Gestión de la Calidad de la información.	¿La institución cuenta con un Plan de Gestión de la Calidad de la Información, donde detalle los requisitos mínimos y criterios de los mismos?	**5**	**5**	**5**	**5**	
		Numero de Instituciones que cuenten con un Plan de Copias de Seguridad y Restauración.	¿La institución cuenta con un Plan de copias de seguridad y restauración?	**5**	**5**	**5**	**5**	
		Frecuencia de Copias de Seguridad.	¿Con que frecuencia realiza copias de seguridad de la información?	**5**	**5**	**5**	**5**	

Mg. Ing. Juan Villegas Cubas

DNI 80103991

USAT Posgrado

"AÑO DE LA UNIVERSALIZACIÓN DE LA SALUD"

INFORME DE VALIDACIÓN DEL INSTRUMENTO

1. TÍTULO DE LA INVESTIGACIÓN:

Modelo basado en la gestión de seguridad de la información para proteger los datos en las farmacias de los Hospitales II-1 en la región Amazonas.

2. NOMBRE DEL INSTRUMENTO:

Cuestionario de Diagnostico Situacional sobre Seguridad de la Información en Hospitales de la Región Amazonas.

3. TESISTA:

Jaime Izquierdo Cabrera.

4. DECISIÓN:

Después de haber revisado el instrumento de recolección de datos, procedió a validarlo teniendo en cuenta su forma, estructura y profundidad; por lo tanto, permitirá recoger información concreta y real de la variable en estudio, coligiendo su pertinencia y utilidad.

OBSERVACIONES: Apto para su aplicación.

APROBADO: SI [X] NO [ ]

Chiclayo, 18 de diciembre del 2020

Mg. Ing. Juan Villegas Cubas
DNI N° 80103991

Anexo 09: Validación de modelo

FORMATO PARA VALIDACIÓN DE EXPERTOS DEL MODELO PROPUESTO

Estimado Ingeniero:

A través de la presente me dirijo a usted con el fin de solicitarle su ayuda para la validación de la propuesta realizada en la investigación denominada MODELO BASADO EN LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA CONTRIBUIR EN LOS PROCESOS DE LAS FARMACIAS DE LOS HOSPITALES II-I EN LA REGIÓN AMAZONAS. Para tal fin, se anexa la matriz de consistencia para la validación.

Agradecemos su valiosa colaboración.

NOMBRES Y APELLIDOS : ALEX CORONADO NAVARRO

FORMACIÓN ACADÉMICA : MAGISTER INGENIERO DE SISTEMAS

ÁREAS DE EXPERIENCIA PROFESIONAL : **SEGURIDAD INFORMÁTICA**

TIEMPO DE EXPERIENCIA : 15 AÑOS

CARGO ACTUAL : JEFE DE ÁREA DE SERVIDORES

INSTITUCIÓN : **UNIVERSIDAD SEÑOR DE SIPÁN**

Objetivo de la investigación : Formular un Modelo de Gestión de Seguridad de la Información para contribuir en los procesos de las farmacias de los hospitales II-I en la región Amazonas.

Objetivo del juicio de expertos : Verificar la validez del modelo propuesto en relación a la suficiencia, claridad, coherencia y relevancia de los procesos considerados.

Objetivo de la prueba : Determinar la utilidad del modelo propuesto para los hospitales de nivel II – I de la región Amazonas.

ALEX FRANKLIN CORONADO NAVARRO
INGENIERO DE SISTEMAS
Reg. CIP. 171209

PROFESIONAL EXPERTO

De acuerdo con los siguientes indicadores califique cada uno de los procesos según corresponda.

CATEGORÍA	CLASIFICACIÓN	INDICADOR
SUFICIENCIA: Los procesos que pertenecen a una misma dimensión bastan para obtener la medición de ésta.	1. No cumple con el criterio	Los procesos no son suficientes para medir la dimensión.
	2. Bajo Nivel	Los procesos miden algún aspecto de la dimensión, pero no corresponden con la dimensión total.
	3. Moderado nivel	Se deben incrementar algunos procesos para poder evaluar la dimensión completamente.
	4. Alto nivel	Los procesos son suficientes.
CLARIDAD: El proceso se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.	1. No cumple con el criterio	El proceso no es claro.
	2. Bajo Nivel	El proceso requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de las mismas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del proceso.
	4. Alto nivel	El proceso es claro, tiene semántica y sintaxis adecuada.
COHERENCIA: El proceso tiene relación lógica con la dimensión o indicador que está midiendo.	1. No cumple con el criterio	El proceso no tiene relación lógica con la dimensión.
	2. Bajo Nivel	El proceso tiene una relación tangencial con la dimensión.
	3. Moderado nivel	El proceso tiene una relación moderada con la dimensión que está midiendo.
	4. Alto nivel	El proceso se encuentra completamente relacionado con la dimensión que está midiendo.
RELEVANCIA: El proceso es esencial o importante, es decir debe ser incluido.	1. No cumple con el criterio	El proceso puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2. Bajo Nivel	El proceso tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El proceso es relativamente importante.
	4. Alto nivel	El proceso es muy relevante y debe ser incluido.

FASE I: DIAGNOSTICO DE LA ORGANIZACIÓN						
PROCESO	**OBJETIVO**	**SUFICIENCIA**	**CLARIDAD**	**COHERENCIA**	**RELEVANCIA**	**OBSERVACIONES**
1.1 DEFINICIÓN DEL CONTEXTO	Reconocer y establecer los parámetros del contexto interno en la organización que influye y tiene algún impacto en el cumplimiento de los objetivos estratégicos y del SGSI.	4	3	4	4	Especificar documentos mininos requeridos para el desarrollo del modelo
1.2 DEFINIR EL ALCANCE	Reconocer y determinar los procesos, áreas y servicios que tendrán alcance en el SGSI.	4	3	4	4	
1.3 GESTIÓN DE LAS COMUNICACIONES	Definir los perfiles y responsabilidades que realizará cada miembro del SGSI en todas las fases.	4	4	4	4	
FASE II: ESTABLECER SGSI						
2.1 DEFINIR POLÍTICAS Y CONTROLES SGSI	Identificar y determinar las políticas de acuerdo a las necesidades de la entidad.	4	3	4	4	
2.2 DEFINIR PROCEDIMIENTOS SGSI	Identificar y determinar los dominios y procedimientos de acuerdo a las necesidades de la entidad.	3	3	4	4	
2.3 DEFINIR METAS Y RESULTADOS SGSI	Identificar y determinar las medidas con sus características y sus metas respectivas.	3	4	3	4	Metas complejas para la primera iteración del modelo.
2.4 DEFINIR PLAN DE AUDITORIA	Determinar aspectos importantes de la planificación en auditoria	4	4	4	4	
FASE III: GESTIÓN DE RIESGOS						
3.1. EVALUACIÓN DEL ACTIVO	Identificar y clasificar los activos de información de la entidad de acuerdo al alcance determinado.					

	Valorar los activos de información previamente identificados según 5 dimensiones (disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad) y escala determinada por MAGERIT.	4	4	4	4	
3.2. EVALUACIÓN DEL RIESGO	Identificar las amenazas y riesgos de cada activo en la entidad.	3	4	4	4	
3.3. TRATAMIENTO DEL RIESGO	Determinar el nivel de tratamiento para los riesgos de mayor capacidad.	4	3	3	4	
	-Determinar las salvaguardas para la reducción de riesgos en los activos de seguridad.	4	4	4	4	
3.4 MONITOREO DEL RIESGO	Evaluar el estado de aplicación de las salvaguardas en previamente identificadas	4	4	4	4	
FASE IV: CONTROL Y EVALUACIÓN DEL SGSI						
4.1 CONTROL DEL SGSI	Registrar el nivel de cumplimiento de las pruebas orientadas a temas de seguridad se la información que no está directamente relacionada con las áreas de ti de la entidad.	4	3	4	4	
4.2 DEFINIR ACCIONES CORRECTIVAS	Identificar las no conformidades suscitadas en todo el ciclo del modelo. Evaluar las acciones correctivas para cada conformidad.	2	3	3	4	Mayor detalle en la recolección de información para definir acciones correctivas.
4.3 EJECUTAR PLAN DE MEJORA CONTINUA	Determinar las características de cada acción correctiva.	4	4	4	4	

ACEPTACIÓN	**X**
OBSERVADO	
DISCONFORMIDAD	

ALEX FRANKLIN CORONADO NAVARRO
INGENIERO DE SISTEMAS
Reg. CIP. 171209

PROFESIONAL EXPERTO

FORMATO PARA VALIDACIÓN DE EXPERTOS DEL MODELO PROPUESTO

Estimado Ingeniero:

A través de la presente me dirijo a usted con el fin de solicitarle su ayuda para la validación de la propuesta realizada en la investigación denominada MODELO BASADO EN LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA CONTRIBUIR EN LOS PROCESOS DE LAS FARMACIAS DE LOS HOSPITALES II-I EN LA REGIÓN AMAZONAS. Para tal fin, se anexa la matriz de consistencia para la validación.

Agradecemos su valiosa colaboración.

NOMBRES Y APELLIDOS : Cesar Augusto Minguillo Rubio

FORMACIÓN ACADÉMICA :

ÁREAS DE EXPERIENCIA PROFESIONAL :

TIEMPO DE EXPERIENCIA :

CARGO ACTUAL :

INSTITUCIÓN :

Objetivo de la investigación : Formular un Modelo de Gestión de Seguridad de la Información para contribuir en los procesos de las farmacias de los hospitales II-I en la región Amazonas.

Objetivo del juicio de expertos : Verificar la validez del modelo propuesto en relación a la suficiencia, claridad, coherencia y relevancia de los procesos considerados.

Objetivo de la prueba : Determinar la utilidad del modelo propuesto para los hospitales de nivel II – I de la región Amazonas.

PROFESIONAL EXPERTO

De acuerdo con los siguientes indicadores califique cada uno de los procesos según corresponda.

CATEGORÍA	CLASIFICACIÓN	INDICADOR
SUFICIENCIA: Los procesos que pertenecen a una misma dimensión bastan para obtener la medición de ésta.	1. No cumple con el criterio	Los procesos no son suficientes para medir la dimensión.
	2. Bajo Nivel	Los procesos miden algún aspecto de la dimensión, pero no corresponden con la dimensión total.
	3. Moderado nivel	Se deben incrementar algunos procesos para poder evaluar la dimensión completamente.
	4. Alto nivel	Los procesos son suficientes.
CLARIDAD: El proceso se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.	1. No cumple con el criterio	El proceso no es claro.
	2. Bajo Nivel	El proceso requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de las mismas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del proceso.
	4. Alto nivel	El proceso es claro, tiene semántica y sintaxis adecuada.
COHERENCIA: El proceso tiene relación lógica con la dimensión o indicador que está midiendo.	1. No cumple con el criterio	El proceso no tiene relación lógica con la dimensión.
	2. Bajo Nivel	El proceso tiene una relación tangencial con la dimensión.
	3. Moderado nivel	El proceso tiene una relación moderada con la dimensión que está midiendo.
	4. Alto nivel	El proceso se encuentra completamente relacionado con la dimensión que está midiendo.
RELEVANCIA: El proceso es esencial o importante, es decir debe ser incluido.	1. No cumple con el criterio	El proceso puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2. Bajo Nivel	El proceso tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El proceso es relativamente importante.
	4. Alto nivel	El proceso es muy relevante y debe ser incluido.

FASE I: DIAGNOSTICO DE LA ORGANIZACIÓN						
PROCESO	**OBJETIVO**	**SUFICIENCIA**	**CLARIDAD**	**COHERENCIA**	**RELEVANCIA**	**OBSERVACIONES**
1.1 DEFINICIÓN DEL CONTEXTO	Reconocer y establecer los parámetros del contexto interno en la organización que influye y tiene algún impacto en el cumplimiento de los objetivos estratégicos y del SGSI.	4	3	4	4	
1.2 DEFINIR EL ALCANCE	Reconocer y determinar los procesos, áreas y servicios que tendrán alcance en el SGSI.	4	3	4	3	
1.3 GESTIÓN DE LAS COMUNICACIONES	Definir los perfiles y responsabilidades que realizará cada miembro del SGSI en todas las fases.	4	4	3	4	
FASE II: ESTABLECER SGSI						
2.1 DEFINIR POLÍTICAS Y CONTROLES SGSI	Identificar y determinar las políticas de acuerdo a las necesidades de la entidad.	3	4	4	4	
2.2 DEFINIR PROCEDIMIENTOS SGSI	Identificar y determinar los dominios y procedimientos de acuerdo a las necesidades de la entidad.	4	3	4	4	
2.3 DEFINIR METAS Y RESULTADOS SGSI	Identificar y determinar las medidas con sus características y sus metas respectivas.	4	4	4	4	
2.4 DEFINIR PLAN DE AUDITORIA	Determinar aspectos importantes de la planificación en auditoria	4	4	3	4	
FASE III: GESTIÓN DE RIESGOS						
3.1. EVALUACIÓN DEL ACTIVO	Identificar y clasificar los activos de información de la entidad de acuerdo al alcance determinado.					

	Valorar los activos de información previamente identificados según 5 dimensiones (disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad) y escala determinada por MAGERIT.	4	4	4	4	
3.2. EVALUACIÓN DEL RIESGO	Identificar las amenazas y riesgos de cada activo en la entidad.	4	4	4	4	
3.3. TRATAMIENTO DEL RIESGO	Determinar el nivel de tratamiento para los riesgos de mayor capacidad.	4	3	4	4	
	-Determinar las salvaguardas para la reducción de riesgos en los activos de seguridad.	4	4	4	4	
3.4 MONITOREO DEL RIESGO	Evaluar el estado de aplicación de las salvaguardas en previamente identificadas	4	3	4	4	
FASE IV: CONTROL Y EVALUACIÓN DEL SGSI						
4.1 CONTROL DEL SGSI	Registrar el nivel de cumplimiento de las pruebas orientadas a temas de seguridad se la información que no está directamente relacionada con las áreas de ti de la entidad.	4	4	4	4	Herramienta de control completa y fácil de aplicar.
4.2 DEFINIR ACCIONES CORRECTIVAS	Identificar las no conformidades suscitadas en todo el ciclo del modelo. Evaluar las acciones correctivas para cada conformidad.	3	4	4	3	
4.3 EJECUTAR PLAN DE MEJORA CONTINUA	Determinar las características de cada acción correctiva.	4	4	4	4	

ACEPTACIÓN	**X**
OBSERVADO	
DISCONFORMIDAD	

PROFESIONAL EXPERTO

FORMATO PARA VALIDACIÓN DE EXPERTOS DEL MODELO PROPUESTO

Estimado Ingeniero:

A través de la presente me dirijo a usted con el fin de solicitarle su ayuda para la validación de la propuesta realizada en la investigación denominada MODELO BASADO EN LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA CONTRIBUIR EN LOS PROCESOS DE LAS FARMACIAS DE LOS HOSPITALES II-I EN LA REGIÓN AMAZONAS. Para tal fin, se anexa la matriz de consistencia para la validación.

Agradecemos su valiosa colaboración.

NOMBRES Y APELLIDOS	: JUAN VILLEGAS CUBAS
FORMACIÓN ACADÉMICA	: MAGISTER INGENIERO DE SISTEMAS
ÁREAS DE EXPERIENCIA PROFESIONAL	: **REDES Y SEGURIDAD INFORMÁTICA**
TIEMPO DE EXPERIENCIA	: 18 AÑOS
CARGO ACTUAL	: CATEDRÁTICO
INSTITUCIÓN	: **UNPRG**
Objetivo de la investigación	: Formular un Modelo de Gestión de Seguridad de la Información para contribuir en los procesos de las farmacias de los hospitales II-I en la región Amazonas.
Objetivo del juicio de expertos	: Verificar la validez del modelo propuesto en relación a la suficiencia, claridad, coherencia y relevancia de los procesos considerados.
Objetivo de la prueba	: Determinar la utilidad del modelo propuesto para los hospitales de nivel II – I de la región Amazonas.

PROFESIONAL EXPERTO

De acuerdo con los siguientes indicadores califique cada uno de los procesos según corresponda.

CATEGORÍA	CLASIFICACIÓN	INDICADOR
SUFICIENCIA: Los procesos que pertenecen a una misma dimensión bastan para obtener la medición de ésta.	1. No cumple con el criterio	Los procesos no son suficientes para medir la dimensión.
	2. Bajo Nivel	Los procesos miden algún aspecto de la dimensión, pero no corresponden con la dimensión total.
	3. Moderado nivel	Se deben incrementar algunos procesos para poder evaluar la dimensión completamente.
	4. Alto nivel	Los procesos son suficientes.
CLARIDAD: El proceso se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.	1. No cumple con el criterio	El proceso no es claro.
	2. Bajo Nivel	El proceso requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de las mismas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del proceso.
	4. Alto nivel	El proceso es claro, tiene semántica y sintaxis adecuada.
COHERENCIA: El proceso tiene relación lógica con la dimensión o indicador que está midiendo.	1. No cumple con el criterio	El proceso no tiene relación lógica con la dimensión.
	2. Bajo Nivel	El proceso tiene una relación tangencial con la dimensión.
	3. Moderado nivel	El proceso tiene una relación moderada con la dimensión que está midiendo.
	4. Alto nivel	El proceso se encuentra completamente relacionado con la dimensión que está midiendo.
RELEVANCIA: El proceso es esencial o importante, es decir debe ser incluido.	1. No cumple con el criterio	El proceso puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2. Bajo Nivel	El proceso tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El proceso es relativamente importante.
	4. Alto nivel	El proceso es muy relevante y debe ser incluido.

FASE I: DIAGNOSTICO DE LA ORGANIZACIÓN						
PROCESO	**OBJETIVO**	**SUFICIENCIA**	**CLARIDAD**	**COHERENCIA**	**RELEVANCIA**	**OBSERVACIONES**
1.1 DEFINICIÓN DEL CONTEXTO	Reconocer y establecer los parámetros del contexto interno en la organización que influye y tiene algún impacto en el cumplimiento de los objetivos estratégicos y del SGSI.	3	3	3	4	Especificar objetivos del negocio y alinearlo al modelo.
1.2 DEFINIR EL ALCANCE	Reconocer y determinar los procesos, áreas y servicios que tendrán alcance en el SGSI.	4	4	4	3	
1.3 GESTIÓN DE LAS COMUNICACIONES	Definir los perfiles y responsabilidades que realizará cada miembro del SGSI en todas las fases.	3	4	4	4	
FASE II: ESTABLECER SGSI						
2.1 DEFINIR POLÍTICAS Y CONTROLES SGSI	Identificar y determinar las políticas de acuerdo a las necesidades de la entidad.	4	4	3	4	
2.2 DEFINIR PROCEDIMIENTOS SGSI	Identificar y determinar los dominios y procedimientos de acuerdo a las necesidades de la entidad.	4	4	3	4	
2.3 DEFINIR METAS Y RESULTADOS SGSI	Identificar y determinar las medidas con sus características y sus metas respectivas.	3	3	3	3	Ausencia de metas generales del modelo.
2.4 DEFINIR PLAN DE AUDITORIA	Determinar aspectos importantes de la planificación en auditoria	4	3	4	3	
FASE III: GESTIÓN DE RIESGOS						
3.1. EVALUACIÓN DEL ACTIVO	Identificar y clasificar los activos de información de la entidad de acuerdo al alcance determinado.					

	Valorar los activos de información previamente identificados según 5 dimensiones (disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad) y escala determinada por MAGERIT.	4	4	4	4	
3.2. EVALUACIÓN DEL RIESGO	Identificar las amenazas y riesgos de cada activo en la entidad.	4	4	4	4	
3.3. TRATAMIENTO DEL RIESGO	Determinar el nivel de tratamiento para los riesgos de mayor capacidad.	3	3	4	4	
	-Determinar las salvaguardas para la reducción de riesgos en los activos de seguridad.	4	3	4	4	
3.4 MONITOREO DEL RIESGO	Evaluar el estado de aplicación de las salvaguardas en previamente identificadas	4	3	4	4	
FASE IV: CONTROL Y EVALUACIÓN DEL SGSI						
4.1 CONTROL DEL SGSI	Registrar el nivel de cumplimiento de las pruebas orientadas a temas de seguridad se la información que no está directamente relacionada con las áreas de ti de la entidad.	4	3	3	4	
4.2 DEFINIR ACCIONES CORRECTIVAS	Identificar las no conformidades suscitadas en todo el ciclo del modelo. Evaluar las acciones correctivas para cada conformidad.	3	3	4	3	
4.3 EJECUTAR PLAN DE MEJORA CONTINUA	Determinar las características de cada acción correctiva.	4	4	4	4	

ACEPTACIÓN	**X**
OBSERVADO	
DISCONFORMIDAD	

PROFESIONAL EXPERTO

Anexo 10: Solicitud de aplicación.

Bagua, 25 de mayo del 2021

MINISTERIO DE SALUD
GOBIERNO REGIONAL AMAZONAS
HOSPITAL DE APOYO BAGUA
TRATAMITE DOCUMENTARIO
RECIBIDO
10:23 Hora 25 MAY 2021 01 Folio
Exp : ..... Doc: .....
Firma: .....

Med. Anast.
Miguel Ángel Guzmán Castañeda
DIRECTOR EJECUTIVO HOSPITAL DE APOYO BAGUA
Presente. -

De mi consideración:

Yo, **JAIME IZQUIERDO CABRERA**, identificado con **DNI 70068472**, ante Ud. respetuosamente me presento y expongo:

Que, actualmente cursando la Maestría de Ingeniera de Sistemas en la Universidad Católica Santo Toribio de Mogrovejo, solicito a Ud. De la manera mas comedida, se considere la petición de aplicar el modelo de mi investigación que lleva de nombre: "Modelo Basado en la Gestión de Seguridad de la Información Para Proteger los Datos en las Farmacias de los Hospitales II-1 en la Región Amazonas" contando con la información suficiente proporcionada por las áreas de farmacia e informática.

Con saludos cordiales y a tiempo de agradecerle su atención a esta solicitud, aprovecho la oportunidad para reiterarle mi más alta consideración y estima.

Atentamente,

Ing. Jaime Izquierdo Cabrera
DNI: 70068472

Anexo 11: Revisión y conformidad de aplicación.

Documento de revisión y conformidad

Yo DAL, en calidad de JEFE DE LA UNIDAD DE ESTADISTICA E INFORMATICA, del HAB, he verificado la información relativa al hospital incluida en la tesis que lleva como título: "MODELO BASADO EN LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA CONTRIBUIR EN LOS PROCESOS DE LAS FARMACIAS DE LOS HOSPITALES II-1 EN LA REGIÓN AMAZONAS", y con la firma de la presente doy conformidad a los valores incluidos en los formatos que se detallan a continuación, debido a que estos se ajustan a la realidad de nuestro hospital, así mismo dejo constancia de conocimiento que los datos incluidos en la tesis en mención solo serán usados con fines educativos.

Por otro lado, con la aplicación parcial desarrollada en la tesis, se han logrado identificar mas de 75% de riesgos que ponen en peligro constante a los activos de información críticos puesto que dichos activos forman parte fundamental en los procesos de la institución.

MINISTERIO DE SALUD GOBIERNO REGIONAL AMAZONAS V° B° INFORMÁTICA HOSPITAL DE APOYO BAGUA

Código	Nombre
SGSI Nº PLAN-001	Formato de definición de contexto interno.
SGSI Nº PLAN-002	Formato de definición de contexto externo.
SGSI Nº PLAN-003	Formato de definición de alcance
SGSI Nº PLAN-004	Formato de gestión de comunicaciones.
SGSI Nº PLAN-005	Formato de definición de políticas y controles SGSI.
SGSI Nº PLAN-006	Formato de definición de procedimientos SGSI.
SGSI Nº PLAN-007	Formato de definición de metas y resultados SGSI.
SGSI Nº PLAN-008	Formato de definición de plan de auditoria.
SGSI Nº PLAN-009	Formato de identificación de activos.
SGSI Nº PLAN-010	Formato de valoración de activos.
SGSI Nº PLAN-011	Formato de evaluación del riesgo.
SGSI Nº PLAN-012	Formato de tratamiento del riesgo.
SGSI Nº PLAN-0013	Formato de control del SGSI
SGSI Nº PLAN-0014	Formato de definición de acciones correctivas.

MINISTERIO DE SALUD
GOBIERNO REGIONAL AMAZONAS
HOSPITAL DE APOYO BAGUA

Téc. Comp. José Daniel Alfaro Lucero

Jefe de Unidad de Estadística e Informática

Jaime Izquierdo Cabrera

Aceptación del Modelo de Gestión de Seguridad de la Información - Jaime Izquierdo Cabrera Recibidos ×

Daniel Alfaro Lucero <jalfaro@hab.com> 13 jul 2021 13:27 (hace 6 días)
para mí

Buen dia Jaime,

Después de revisar y analizar el modelo SGSI que propones para nuestro hospital, tenemos la certeza que cumple con reforzar las debilidades relativas a la gestión de seguridad de la información que forman parte del entorno de nuestra organización, el cual servirá de gran ayuda al momento de realizar la ejecución para analizar todos los procesos de la farmacia. Estamos a la expectativa de poder llevar a cabo la implementación del 100% cuando la coyuntura actual lo permita.

Atentamente,
Daniel Alfaro Lucero
Jefe informática
Hospital de Apoyo Bagua

Anexo 12: Plantillas aplicadas en el caso de uso.

LOGO DE LA ORGANIZACIÓN	**DEFINICIÓN DE CONTEXTO INTERNO**	
	CÓDIGO SGSI Nº PLAN-001	FECHA ELABORACIÓN: __ /05/2021
		FECHA APLICACIÓN: __/05/2021
FASE: I - NATURALEZA DE LA ORGANIZACIÓN		**PROCESO: 1. DEFINICIÓN DEL CONTEXTO**
OBJETIVOS	Reconocer y establecer los parámetros del contexto interno en la organización que influye y tiene algún impacto en el cumplimiento de los objetivos estratégicos y del SGSI.	
DESCRIPCIÓN	Previo a la recolección de información se hace uso del análisis de los documentos de entrada.	

PROCESOS CRÍTICOS	**ÁREAS O SERVICIOS INVOLUCRADAS**
Mantenimiento de servidores SISMED Mantenimiento de red de datos Mantenimiento de equipos de cómputo Custodia y almacenaje de recetas expedidas hasta 5 años de antigüedad	Unidad de Informática Farmacia
CONCLUSIONES	
Los procesos críticos definidos contemplan el cumplimiento de las normas que regulan el correcto funcionamiento de las farmacias de nivel II-1	

HISTORIAL DE VERSIONES		
v. 1.0	FECHA: __/05/2021	ELABORADO POR: JIZQUIERDOC
	Descripción: ELABORACION INICIAL DE DEFINICION DE CONTEXTO (PRIMERA ITERACION)	
…	…	…
	…	
RESPONSABLES		**FIRMAS**
ELABORADO POR:	JIZQUIERDOC	
REVISADO POR:	DALFAROL	

APROBADO POR:	DALFAROL	

LOGO DE LA ORGANIZACIÓN	DEFINICIÓN DE CONTEXTO EXTERNO	
	CÓDIGO SGSI Nº PLAN-002	FECHA ELABORACIÓN: ____/05/2021
		FECHA APLICACIÓN: ____/05/2021
FASE: I - NATURALEZA DE LA ORGANIZACIÓN		PROCESO: 1. DEFINICIÓN DEL CONTEXTO
OBJETIVOS	Reconocer y establecer los parámetros del contexto externo en la organización que influye y tiene algún impacto en el cumplimiento de los objetivos estratégicos y del SGSI.	
DESCRIPCIÓN	Previo a la recolección de información se hace uso del análisis de los documentos de entrada.	

ENTORNO INVOLUCRADO	ASPECTOS IDENTIFICADOS
POLITICO, SOCIO-CULTURALES, TECNOLOGICOS, NATURALES, ECONOMICO	
CONCLUSIONES	
El entorno involucrado será de importancia para la identificación de riesgos.	

HISTORIAL DE VERSIONES		
v. 1.0	FECHA: __/05/2021	ELABORADO POR: JIZQUIERDOC
	Descripción: ELABORACION INICIAL DE DEFINICION DE CONTEXTO (PRIMERA ITERACION)	
…	…	…
	…	
RESPONSABLES		FIRMAS
ELABORADO POR:	JIZQUIERDOC	

REVISADO POR:	DALFAROL	
APROBADO POR:	DALFAROL	

LOGO DE LA ORGANIZACIÓN	**DEFINICIÓN DEL ALCANCE**	
	CÓDIGO SGSI Nº PLAN-003	FECHA ELABORACIÓN: ____/05/2021
		FECHA APLICACIÓN: ____/05/2021
FASE: I - NATURALEZA DE LA ORGANIZACIÓN		**PROCESO: 2. DEFINICIÓN DEL ALCANCE**
OBJETIVOS	- Reconocer y determinar los procesos, áreas y servicios que tendrán alcance en el SGSI.	
DESCRIPCIÓN	La definición de alcance y exclusiones permite el desarrollo de un sistema orientado a las necesidades de la entidad.	

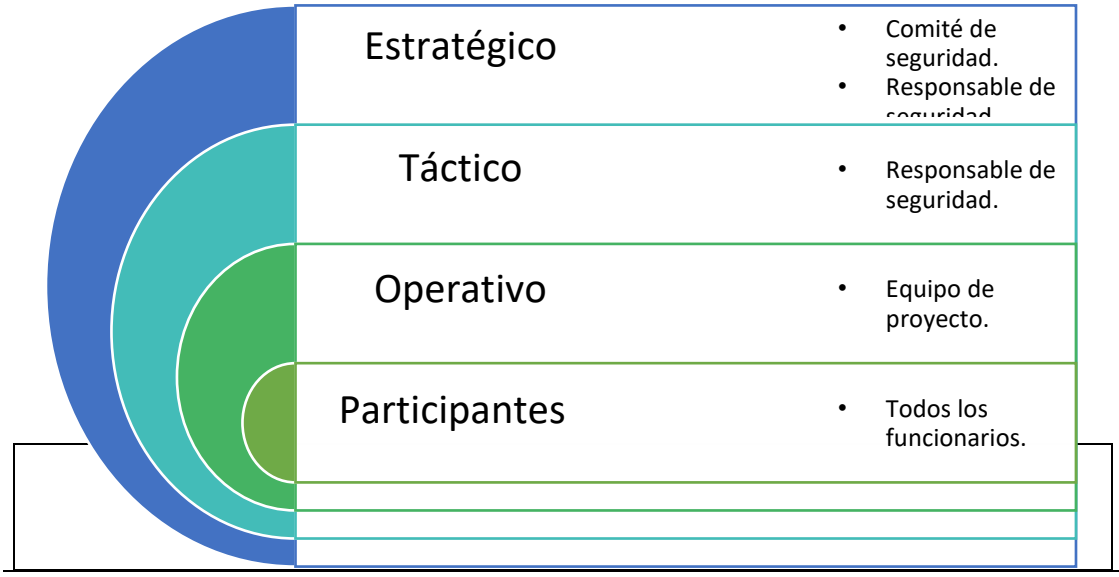
ALCANCE SGSI	
PROCESOS	ALMACEN ESPECIALIZADOS DE MEDICAMENTOS ADQUISICION DE MEDICAMENTOS
ÁREAS O SERVICIOS	UNIDAD DE INFORMATICA FARMACIA
EXCLUSIONES SGSI	
PROCESOS	NINGUNA
CONCLUSIONES	
Abarca el proceso de adquisición y almacenaje puesto que son procesos iniciales y principales en la atención de la farmacia	

HISTORIAL DE VERSIONES		
v. 1.0	FECHA: __/05/2021	ELABORADO POR: JIZQUIERDOC
	Descripción: ELABORACION INICIAL DE DEFINICION DE ALCANCE	
…	…	…

	…

RESPONSABLES		FIRMAS
ELABORADO POR:	JIZQUIERDOC	
REVISADO POR:	DALFAROL	
APROBADO POR:	DALFAROL	

LOGO DE LA ORGANIZACIÓN	GESTIÓN DE LAS COMUNICACIONES	
	CÓDIGO SGSI Nº PLAN-004	FECHA ELABORACIÓN: ____/05/2021
		FECHA APLICACIÓN: ____/05/2021
FASE: I - NATURALEZA DE LA ORGANIZACIÓN		PROCESO: 3. GESTIÓN DE LAS COMUNICACIONES
OBJETIVOS	-Definir los perfiles y responsabilidades que realizará cada miembro del SGSI en todas las fases.	
DESCRIPCIÓN	Los roles y perfiles determinados en esta plantilla pueden ser modificados previo acuerdo con el comité de seguridad.	

EQUIPO DE SGSI


INTEGRANTES	
ROLES	**RESPONSABLES**
RESPONSABLE DE SEGURIDAD DE LA ENTIDAD	-JALFAROL
EQUIPO DE PROYECTO	-Un representante de área de informática. -Un representante del área de Control Interno. -Un representante del área de Planeación. -Un representante del Administración.
COMITÉ DE SEGURIDAD	-Un representante de área de informática. -Un representante del área de Control Interno. -Un representante del área de Planeación. -Un representante del área Jurídica. -El responsable de seguridad de la información.
CONCLUSIONES	
Los responsables del SGSI se comprometen a cumplir sus funciones para lograr el objetivo del proyecto.	

HISTORIAL DE VERSIONES		
v. 1.0	FECHA: __/05/2021	ELABORADO POR: JIZQUIERDOC
	Descripción: ELABORACION INICIAL DE DEFINICION DE ROLES	
…	…	…
	…	

RESPONSABLES		FIRMAS
ELABORADO POR:	JIZQUIERDOC	
REVISADO POR:	DALFAROL	
APROBADO POR:	DALFAROL	

	DEFINICIÓN DE POLÍTICAS Y CONTROLES

LOGO DE LA ORGANIZACIÓN		
	CÓDIGO SGSI Nº PLAN-005	FECHA ELABORACIÓN: ____/05/2021
		FECHA APLICACIÓN: ____/05/2021
FASE: II - ESTABLECER SGSI		**PROCESO: 2.1. DEFINIR POLÍTICAS Y CONTROLES SGSI**
OBJETIVOS	- Identificar y determinar las políticas de acuerdo a las necesidades de la entidad.	
DESCRIPCIÓN	Las políticas y controles determinados en esta plantilla pueden ser modificadas de acuerdo a la naturaleza y recursos de la entidad.	

POLÍTICA SGSI				
CÓDIGO	**EJE**	**DEFINICIÓN**	**CUMPLIMIENTO**	**CONTROL**
PS-01	GESTIÓN DE ACTIVOS	Se identificará, clasificará y gestionará los activos de información con la finalidad de garantizar la integridad de los mismos.	Todos los funcionarios que laboran en las áreas que abarca el alcance del SGSI.	8.1.1 Inventario de activos; 8.2.1 Clasificación de la información; 11.2.4 Mantenimiento de equipos.
PS-02	NO REPUDIO	Se realizará operaciones de trazabilidad, y retención de las acciones realizadas por los usuarios como creación, origen, recepción, entrega de información y otros.	Todos los funcionarios que laboran en las áreas que abarca el alcance del SGSI.	12.2.1 Controles contra códigos maliciosos
PS-03	PRIVACIDAD Y CONFIDENCIALIDAD	Conforme a lo establecido en la Ley 29733, la entidad garantizará el tratamiento de datos personales en el alcance del SGSI.	Todos los funcionarios que laboran en las áreas que abarca el alcance del SGSI.	5.1.2 Revisión de las políticas para la seguridad de la información; 9.4.1 Restricción de acceso a la información.
PS-04	CONTROL DE ACCESO	Se determinará los procedimientos frente a la administración y responsabilidad relacionado con los accesos de la información, sin importar estos sean	Todos los funcionarios que laboran en las áreas que abarca el alcance del SGSI.	9.1.1 Política de control de acceso; 9.2.1 Registro y baja de usuarios; Sistema de gestión de contraseñas; 11.1.2 Controles de ingreso físicos; 11.1.3

		electrónicos o físicos.		Asegurar oficinas, áreas e instalaciones.
PS-05	REGISTRO Y AUDITORIA	Velar por el mantenimiento de las evidencias de las actividades y acciones que afincan los activos de información, así como garantizar el cumplimiento del SGSI y su mejora continua.	Responsable de seguridad del SGSI	12.3.1 Respaldo de información; 12.4.1 Registro de eventos; 12.4.2 Protección de información de registros; 12.7.1 Controles de auditoría de sistemas de información.
PS-06	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	Garantiza una gestión de eventos, incidentes y vulnerabilidades de seguridad de la información.	Dirigida a todos los usuarios que tienen un acceso autorizado a cualquier sistema de información	16.1.1 Responsabilidades y procedimientos; 16.1.2 Reporte de eventos de seguridad de la información; 16.1.3 Reporte de debilidades de seguridad de la información.
PS-07	CAPACITACIÓN Y SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN	Se centra en la formación del personal en temas relacionados con la seguridad de la información, cuya finalidad es disminuir las vulnerabilidades y amenazas relacionadas con el recurso humano.	Todos los funcionarios que laboran en la entidad.	7.2.2 Conciencia, educación y capacitación sobre la seguridad de la información.

CONCLUSIONES
Las políticas de control adoptadas por la institución fueron priorizadas según la necesidad y flexibilidad en la implementación.

HISTORIAL DE VERSIONES		
v. 1.0	FECHA: __/05/2021	ELABORADO POR: JIZQUIERDOC
	Descripción: ELABORACION INICIAL DE DEFINICION DE POLITICAS Y CONTROLES	
…	…	…
	…	

RESPONSABLES		**FIRMAS**
ELABORADO POR:	JIZQUIERDOC	

REVISADO POR:	DALFAROL	
APROBADO POR:	DALFAROL	

LOGO DE LA ORGANIZACIÓN	**DEFINICIÓN DE PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN**	
	CÓDIGO SGSI Nº PLAN-006	FECHA ELABORACIÓN: ____/05/2021
		FECHA APLICACIÓN: ____/05/2021
FASE: II - ESTABLECER SGSI		**PROCESO: 2.2. DEFINIR PROCEDIMIENTOS SGSI**
OBJETIVOS	- Identificar y determinar los ejes y procedimientos de acuerdo a las necesidades de la entidad	
DESCRIPCIÓN	Los ejes son extraídos de MSPI y relacionados con los 114 controles de seguridad de la información de la ISO 27000, la entidad puede modificar los controles y dominios de acuerdo a su naturaleza y recursos.	

EJE	PROCEDIMIENTO	PUNTO DE CONTROL	RESPONSABLE
PS-07	Capacitación y sensibilización del personal.	Aprobación plan de capacitación	JALFAROL
PS-01	Identificación y clasificación de activos.	Elaboración Formato	JIZQUIERDOC
PS-03 / PS-04		Aprobaciones políticas	JALFAROL

	Ingreso seguro a los sistemas de información.		
	gestión de usuarios y contraseñas.	Aprobaciones políticas	JALFAROL
PS-01 / PS-04	Control de acceso físico.	Aprobaciones políticas	JALFAROL
	Protección de activos.	Aprobaciones políticas	JALFAROL
	Mantenimiento de equipos	Aprobación plan	JALFAROL
PS-02	Protección contra código malicioso.	Aprobaciones políticas	JALFAROL
PS-05 / PS-06	Gestión de incidentes de seguridad de la información.	Aprobaciones políticas	JALFAROL

*Punto de control: Requerimiento mínimo para que el procedimiento pueda ejecutarse

por ejemplo, un control de cambios, un formato o una aprobación.
*Responsable: responsable del
procedimiento.

CONCLUSIONES
El responsable de seguridad de la Información puede delegar las funciones correspondidas a los ejes que crea conveniente.

HISTORIAL DE VERSIONES		
v. 1.0	FECHA: __/05/2021	ELABORADO POR: JIZQUIERDOC
	Descripción: ELABORACION INICIAL DE DEFINICION DE PROCEDIMIENTOS SGSI	
…	…	…
	…	

RESPONSABLES		**FIRMAS**
ELABORADO POR:	JIZQUIERDOC	

REVISADO POR:	DALFAROL	
APROBADO POR:	DALFAROL	

LOGO DE LA ORGANIZACIÓN	**DEFINICIÓN DE PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN**	
	CÓDIGO SGSI Nº PLAN-007	FECHA ELABORACIÓN: ____/06/2021
		FECHA APLICACIÓN: ____/06/2021
FASE: II - ESTABLECER SGSI		**PROCESO: 2.3. DEFINIR METAS Y RESULTADOS SGSI**
OBJETIVOS	- Identificar y determinar las medidas con sus características y sus metas respectivas.	
DESCRIPCIÓN	Cada métrica se relaciona con las políticas definidas en la Plantilla 6, la entidad puede modificar las medidas de acuerdo a su naturaleza y recursos disponibles.	

Identificación de la métrica.	
Nombre de la métrica.	Formación en seguridad de la información.
Código de la métrica.	MS-01
Propósito de la métrica.	Evaluar el cumplimiento con los requisitos de formación en concientización de seguridad de la información
Eje de política	PS-07
Objetivo de control	
Objeto de la medición y atributos	
Objeto de la medición	Base de datos de empleados
Atributo	Registros de formación
Especificación de la medida	
Medida	Porcentaje del personal que ha recibido entrenamiento anual de concientización en seguridad de la información

Función de medición	Número de empleados que han recibido entrenamiento anual de concientización en seguridad de la información/número de empleados que necesitan recibir entrenamiento anual de concientización en seguridad de la información * 100		
Escala	Numérico		
Unidad de medida	Empleado		
Meta	Mínima 0-60%	Satisfactoria 60-90%	Sobresaliente 90-100%
Frecuencia de Recolección y Análisis	Semestral		

Identificación de la métrica.			
Nombre de la métrica.	Cumplimiento con la política de concientización en seguridad de la información.		
Código de la métrica.	MS-02		
Propósito de la métrica.	Evaluar el estado del cumplimiento con la política de concientización en seguridad de la organización entre el personal relevante		
Eje de política	PS-07		
Objetivo de control			
Objeto de la medición y atributos			
Objeto de la medición	Plan de formación de concientización en seguridad de la información		
Atributo	Personal identificado en el plan		
Especificación de la medida			
Medida	Progreso hasta la fecha.		
Función de medición	1. Agregar el estado a todo el personal que ha firmado, planificado y por completar hasta la fecha 2. Dividir el personal que ha firmado hasta la fecha por el personal planificado para firmar hasta la fecha		
Escala	Numérico		
Unidad de medida	Personal, Porcentaje		
Meta	Mínima 0-60%	Satisfactoria 60-90%	Sobresaliente 90-100%
Frecuencia de Recolección y Análisis	Semestral		

Identificación de la métrica.	
Nombre de la métrica.	Calidad de las contraseñas
Código de la métrica.	MS-03
Propósito de la métrica.	

	Evaluar la calidad de las contraseñas utilizadas por los usuarios para acceder a los sistemas de TI de la organización		
Eje de política	PS-04		
Objetivo de control			
Objeto de la medición y atributos			
Objeto de la medición	Base de datos de contraseñas de usuario		
Atributo	Contraseñas individuales		
Especificación de la medida			
Medida	Total, de número de contraseñas que cumplen la política de calidad de contraseñas de la organización		
Función de medición	Suma de [Total de número de contraseñas que cumplen la política de calidad de contraseñas de la organización para cada usuario]		
Escala	Ordinal		
Unidad de medida	Contraseñas		
Meta	Mínima 0-60%	Satisfactoria 60-90%	Sobresaliente 90-100%
Frecuencia de Recolección y Análisis	Semestral		

Identificación de la métrica.	
Nombre de la métrica.	Proceso de revisión del SGSI
Código de la métrica.	MS-04
Propósito de la métrica	Evaluar el grado de realización de una revisión independiente de la seguridad de la información
Eje de política	PS-05
Objetivo de control	
Objeto de la medición y atributos	
Objeto de la medición	Informes de las revisiones
Atributo	Revisiones de partes interesadas Informadas y planificadas
Especificación de la medida	
Medida	Número de revisiones de partes interesadas llevadas a cabo
Función de medición	Dividir [Número de revisiones de partes interesadas llevadas a cabo] por [Total de número de revisiones de partes interesadas planificadas].

Escala	Ordinal		
Unidad de medida	Revisión		
Meta	Mínima 0 - 0,6	Satisfactoria 0,6 - 0,8	Sobresaliente 0,8 - 1,1
Frecuencia de Recolección y Análisis	Anual		

Identificación de la métrica.			
Nombre de la métrica.	Efectividad de la Gestión de Incidentes de Seguridad de la Información		
Código de la métrica.	MS-05		
Propósito de la métrica.	Evaluar la efectividad de la gestión de incidentes de seguridad de la información		
Eje de política	PS-06		
Objetivo de control	Posibilitar la detección temprana de eventos de seguridad y dar respuesta a los incidentes de seguridad.		
Objeto de la medición y atributos			
Objeto de la medición	SGSI		
Atributo	Incidentes individuales		
Especificación de la medida			
Medida	Incidentes que exceden el umbral		
Función de medición	Comparación del número total de incidentes con el umbral.		
Escala	Ordinal		
Unidad de medida	Revisión		
Meta	Mínima: Tendencia al alza	Satisfactoria: Tendencia se mantiene	Sobresaliente: Tendencia a baja
Frecuencia de Recolección y Análisis	Anual		

Identificación de la métrica.	
Nombre de la métrica.	Protección contra código malicioso
Código de la métrica.	MS-06
Propósito de la métrica	Evaluar la eficacia del sistema de protección contra software malicioso y ataques de software.
Eje de política	PS-03

Objetivo de control	Proteger la integridad del software y la información. (planificado) Proteger la integridad del software y la información de software maliciosos.		
Objeto de la medición y atributos			
Objeto de la medición	Reportes de incidentes		
Atributo	Incidentes causados por software malicioso		
Especificación de la medida			
Medida	Fortaleza de la protección contra software malicioso		
Función de medición	Número de incidentes de seguridad causados por software malicioso/número de ataques detectados y bloqueados causados por software malicioso		
Escala	Enteros de cero a infinito		
Unidad de medida	Incidentes de seguridad		
Meta	Rojo > 10%	Amarillo 10%	Verde < 10%
Frecuencia de Recolección y Análisis	Mensual		

Identificación de la métrica.			
Nombre de la métrica.	Revisión de archivos de registro(log)		
Código de la métrica.	MS-07		
Propósito de la métrica.	Evaluar el estado de conformidad de las revisiones regulares a los archivos de registro (log) de sistemas críticos.		
Eje de política	PS-02		
Objetivo de control	Detectar actividades de procesamiento de información no autorizadas. (planificado) Detectar actividades de procesamiento de información no autorizadas en sistemas críticos a partir de los sistemas de registros(log)		
Objeto de la medición y atributos			
Objeto de la medición	Sistema		
Atributo	Archivos de Registro Individual		
Especificación de la medida			
Medida	Porcentaje de archivos de registro de auditoría revisados cuando es requerido por período de tiempo		
Función de medición	(# de archivos de registro revisados dentro del período de tiempo especificado) / (# total de archivos de registro) *100.		
Escala	Ratio.		
Unidad de medida	Archivo de registro(log)		
Meta	Mínima 0-20%	Satisfactoria 20-70%	Sobresaliente 70-100%

Frecuencia de Recolección y Análisis	Mensual

Identificación de la métrica			
Nombre de la métrica.	Clasificación de activos de Información		
Código de la métrica.	MS-08		
Propósito de la métrica.	Evaluar el inventario de activos, incluyendo su administración.		
Eje de política	PS-01		
Objetivo de control	Identificar activos de información no clasificados a partir del inventario de activos.		
Objeto de la medición y atributos			
Objeto de la medición	Plan de Inventario de Activos de Información.		
Atributo	Activo de información individual.		
Especificación de la medida			
Medida	Porcentaje de activos de Información clasificados.		
Función de medición	(# de activos de información clasificados) / (# total de activos de información identificados en el plan) *100.		
Escala	Ratio.		
Unidad de medida	Activo de información.		
Meta	Mínima 0-40%	Satisfactoria 40-70%	Sobresaliente 70-100%
Frecuencia de Recolección y Análisis	Semestral		

CONCLUSIONES
Los constructores de medición son concretos y contemplan una frecuencia de recolección, el responsable del SGSI puede designar algún funcionario con experiencia para la recolección de la información.

HISTORIAL DE VERSIONES		
v. 1.0	FECHA: __/06/2021	ELABORADO POR: JIZQUIERDOC
	Descripción: ELABORACION INICIAL DE DEFINICION DE METRICAS SGSI	
…	…	…
	…	

RESPONSABLES		**FIRMAS**
ELABORADO POR:	JIZQUIERDOC	

REVISADO POR:	DALFAROL	
APROBADO POR:	DALFAROL	

LOGO DE LA ORGANIZACIÓN	**DEFINICIÓN DE PLAN DE AUDITORIA**	
	CÓDIGO SGSI Nº PLAN-008	FECHA ELABORACIÓN: ____/06/2021
		FECHA APLICACIÓN: ____/06/2021
FASE: II - ESTABLECER SGSI		**PROCESO: 2.4. DEFINIR PLAN DE AUDITORIA**
OBJETIVOS	-Determinar aspectos importantes de la planificación en auditoria	
DESCRIPCIÓN	Los controles a auditar deben ser los definidos por la entidad en la Plantilla 06.	

Duración	3 días
Frecuencia	Anual
Tipo	Auditoría Interna

Controles Definidos	**Control organizacional**	**Control técnico**	**Pruebas del sistema**	**Inspecciones visuales**	**Observaciones**
5.1.2 Revisión de las políticas para la seguridad de la información	X				
7.2.2 Conciencia, educación y capacitación sobre la seguridad de la información	X				
8.1.1 Inventario de activos	X				

8.2.1 Clasificación de la información	X				
9.1.1 Política de control de acceso	X				
9.2.1 Registro y baja de usuarios		X			
9.4.1 Restricción de acceso a la información		X			
9.4.3 Sistema de gestión de contraseñas		X			
11.1.2 Controles de ingreso físicos				X	
11.1.3 Asegurar oficinas, áreas e instalaciones				X	
11.2.4 Mantenimiento de equipos	X				
12.2.1 Controles contra códigos maliciosos			X		
12.3.1 Respaldo de información		X			
12.4.1 Registro de eventos		X			
12.4.2 Protección de información de registros		X			
12.7.1 Controles de auditoría de sistemas de información	X				
16.1.1 Responsabilidades y procedimientos	X				
16.1.2 Reporte de eventos de seguridad de la información		X			
16.1.3 Reporte de debilidades de seguridad de la información		X			

-Control organizacional: Cuando la evidencia del control es obtenida por medio de registros en el plan, entrevistas, observación o inspección física.
-Control tecnico:Cuando la evidencia del control es obtenida a través de pruebas del sistema uso de herramientas especializadas de auditoría.
-Pruebas del sistema: Cuando se obtiene información a través de configuraciones en el sistema o donde el auditor ingresa a una consola de sistema o evaluación de resultados de herramientas de sistemas.
-Inspecciones visuales: Cuando el agrupamiento de medios para la obtención de información no es suficiente, el auditor debe verificar el control insitu.
-Observaciones: Observaciones o recomendaciones del auditor en cada control auditado.

CONCLUSIONES
Las observaciones serán llenadas al momento de realizar la auditoria.

HISTORIAL DE VERSIONES		
v. 1.0	FECHA: __/06/2021	ELABORADO POR: JIZQUIERDOC
	Descripción: ELABORACION INICIAL DE DEFINICION DE PLAN DE AUDITORIA	
…	…	…
	…	

RESPONSABLES		**FIRMAS**
ELABORADO POR:	JIZQUIERDOC	
REVISADO POR:	DALFAROL	
APROBADO POR:	DALFAROL	

LOGO DE LA ORGANIZACIÓN	**IDENTIFICACIÓN DE ACTIVOS**	
	CÓDIGO SGSI Nº PLAN-009	FECHA ELABORACIÓN: ____/06/2021
		FECHA APLICACIÓN: ____/06/2021
FASE: III - GESTIÓN DE RIESGOS		**PROCESO: 3.1. EVALUACIÓN DEL ACTIVO**
OBJETIVOS	-Identificar y clasificar los activos de información de la entidad de acuerdo al alcance determinado.	
DESCRIPCIÓN	La clasificación de los activos se especifica en los anexos de MAGERIT e ISO 27000, la entidad puede hacer libre uso de ellos.	

CÓDIGO	CLASIFICACIÓN*	ACTIVO	DESCRIPCIÓN

[me]	Medio Electrónico	Copias de seguridad	Archivos de respaldo de información para los distintos sistemas.
[om-1]	Otros Medios	Historias Clínicas	Información Médica de pacientes que son atendidos.
[om-2]	Otros Medios	Recetas Medicas	Información Farmacológica de pacientes que son atendidos.
[om-3]	Otros Medios	Rexportes Mensuales de Almacén	Información Mensual de movimientos en medicamentos ocurridos en AEM
[an-1]	Aplicaciones de negocio	Kardex de AEM	Información de Stock actualizado de medicamentos.
[an-2]	Aplicaciones de negocio	Base de Datos SIGA	Soporte en la Gestión administrativa del Almacén.
[an-3]	Aplicaciones de negocio	Base de Datos Sismed	Soporte en la gestión especializada de medicamentos.
[epd]	Equipo de Procesamiento de Datos	Servidor	Computador especializado para soportar los sistemas y aplicaciones que hace uso el área de Farmacia.
[ef]	Equipo Fijo	Computador	Dispositivo para realizar las tareas del personal en AEM
[om-4]	Otros Medios	Expediente de ingreso de Medicamentos	Conjunto de documentos que registra desde el requerimiento de medicamentos hasta su cotización, autorización, adquisición, almacenamiento y distribución.
[om-5]	Otros Medios	Rexportes salida de Medicamentos	Documento que registra las salidas de medicamentos hacia las diferentes áreas o servicios del hospital.
[om-6]	Otros Medios	Contratos de medicamentos con proveedores	Conjunto de documentos que almacena los contratos y pactos entre el hospital y proveedor de medicamentos.
[pp]	Periféricos Para Procesamiento	Disco Duro Externo	Dispositivo usado para almacenar las copias de seguridad en caso de falla completa del servidor.
[pe-1]	Personal	Jefe de AEM	Personal encargado de la administración dentro del AEM.
[pe-2]	Personal	Jefe de TI	Personal a cargo de la administración de las aplicaciones, comunicaciones, información, seguridad informática y soporte técnico en el hospital.
[red-1]	Red	Fibra Óptica Claro	Medio principal para proveer internet a las diferentes áreas y servicios del hospital.
[red-2]	Red	Radio Enlace	Medio de contingencia para proveer internet a las diferentes áreas y servicios del hospital.

*Para la elaboración de esta plantilla, tener en cuenta el "CATALOGO DE ELEMENTOS MAGERIT v3" pág. 7-14 donde detalla todas las clasificaciones para los diferentes tipos de activos que puede haber en una entidad.

CONCLUSIONES
Los activos identificados pertenecen al área de Almacén Especializado de Medicamentos.

HISTORIAL DE VERSIONES		
v. 1.0	FECHA: __/06/2021	ELABORADO POR: JIZQUIERDOC
	Descripción: ELABORACION INICIAL DE IDENTIFICACION DE ACTIVOS	
…	…	…
	…	

RESPONSABLES		FIRMAS
ELABORADO POR:	JIZQUIERDOC	
REVISADO POR:	DALFAROL	
APROBADO POR:	DALFAROL	

LOGO DE LA ORGANIZACIÓN	VALORACION DE ACTIVOS	
	CÓDIGO SGSI Nº PLAN-010	FECHA ELABORACION: ____/06/2021
		FECHA APLICACIÓN: ____/06/2021
FASE: III - GESTION DE RIESGOS		PROCESO: 3.1. EVALUACION DEL ACTIVO
OBJETIVOS	-Valorar los activos de información previamente identificados según 5 dimensiones (disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad) y escala determinada por MAGERIT.	
DESCRIPCION	Las valoraciones de dimensiones e impacto de cada activo son elaboradas teniendo en cuenta MAGERIT, así como su criterio para aplicación, para mejores efectos se debe evaluar todos los aspectos mencionados en esta plantilla.	

CODIGO	ACTIVO	DIMENSION*					IMPACTO	
		DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD	AUTENTICIDAD	TRAZABILIDAD	RANGO	VALOR

[me]	Copias de seguridad	5.adm	9.si	10.si			A	8
[om-1]	Historias Clínicas	1.adm	6.pi2	7.lro	6.pi2	6.pi2	A	8
[om-2]	Recetas Medicas	1.adm	6.pi2	7.lro	6.pi2	6.pi2	A	8
[om-3]	Rexportes Mensuales de Almacén	5.lro	9.si	2.pi2	3.lro	5.lro	A	7
[an-1]	Kardex de AEM	5.lro	9.si	2.pi2	3.lro	5.lro	A	7
[an-2]	Base de Datos SIGA	10.si	10.si	10.si	3.si		A	7
[an-3]	Base de Datos Sismed	10.si	10.si	10.si	3.si		A	7
[epd]	Servidor	9.da2	10.si	10.si	3.si		MA	10
[ef]	Computador	1.pi		1.si	3.si		B	3
[om-4]	Expediente de ingreso de Medicamentos	5.lro	9.si	2.pi2	3.lro	5.lro	M	5
[om-5]	Rexportes salida de Medicamentos	5.lro	9.si	2.pi2	3.lro	5.lro	M	5
[om-6]	Contratos de medicamentos con proveedores	5.lro	9.si	2.pi2	3.lro		A	7
[pp]	Disco Duro Externo	5.adm	9.si	10.si			A	7
[pe-1]	Jefe de AEM	5.adm					A	7
[pe-2]	Jefe de TI	5.adm					A	7
[red-1]	Fibra Óptica Claro	7.olm					A	8
[red-2]	Radio Enlace	7.olm					A	9

*Para la elaboración de esta plantilla, tener en cuenta el "CATALOGO DE ELEMENTOS MAGERIT v3" pág... 15-24 donde detalla las características de cada dimensión, así como los criterios de valoración para cada dimensión.

CONCLUSIONES
En esta sección se define el comentario final o apreciación de lo observado posterior al llenado de la plantilla.

HISTORIAL DE VERSIONES		
v. 1.0	FECHA: __/06/2021	ELABORADO POR: JIZQUIERDOC
	Descripción: ELABORACION INICIAL DE CLASIFICACION DE ACTIVOS	
…	…	…
	…	

RESPONSABLES		FIRMAS
ELABORADO POR:	JIZQUIERDOC	
REVISADO POR:	DALFAROL	
APROBADO POR:	DALFAROL	

LOGO DE LA ORGANIZACIÓN	IDENTIFICACIÓN DE AMENAZAS	
	CÓDIGO SGSI Nº PLAN-011	FECHA ELABORACIÓN: ____/06/2021
		FECHA APLICACIÓN: ____/06/2021
FASE: III - GESTIÓN DE RIESGOS		PROCESO: 3.2. EVALUACIÓN DEL RIESGO
OBJETIVOS	-Identificar las amenazas y riesgos de cada activo en la entidad	
DESCRIPCIÓN	Previo a la recolección de información se hace uso del análisis de los documentos de entrada.	

CÓDIGO	ACTIVO	AMENAZA	RIESGO			
			IMPACTO	FRECUENCIA	RIESGO	VALORACIÓN

[me]	Copias de seguridad	E.18 Destrucción de información	8	2	16	A
		A.15 Modificación deliberada	8	2	16	A
		A.18 Destrucción de información	8	2	16	A
		A.25 Robo	8	1	8	M
[om-1]	Historias Clínicas	N.2 Daños por agua	8	2	16	A
		I.1 Fuego	8	2	16	A
		A.11 Acceso no autorizado	8	4	32	MA
		A.18 Destrucción de información	8	3	24	A
		A.19 Divulgación de información	8	4	32	MA
[om-2]	Recetas Medicas	N.2 Daños por agua	8	1	8	M
		I.1 Fuego	8	1	8	M
		A.11 Acceso no autorizado	8	4	32	MA
		A.18 Destrucción de información	8	3	24	A
		A.19 Divulgación de información	8	3	24	A
[om-3]	Rexportes Mensuales de Almacén	N.2 Daños por agua	7	1	7	M
		I.1 Fuego	7	1	7	M
		A.11 Acceso no autorizado	7	3	21	A
		A.18 Destrucción de información	7	3	21	A
[an-1]	Kardex de AEM	N.2 Daños por agua	7	1	7	M
		I.1 Fuego	7	1	7	M
		A.11 Acceso no autorizado	7	3	21	A
		A.18 Destrucción de información	7	3	21	A
[an-2]	Base de Datos SIAF	E.2 Errores de administrador	7	2	14	A
		A.5 Suplantación de identidad	7	4	28	MA
		A.11 Acceso no autorizado	7	4	28	MA
		A.19 Divulgación de información	7	3	21	A
[an-2]		E.2 Errores de administrador	7	3	21	A

	Base de Datos SIGA	A.5 Suplantación de identidad	7	4	28	MA
		A.11 Acceso no autorizado	7	4	28	MA
		A.19 Divulgación de información	7	4	28	MA
[an-3]	Base de Datos Sismed	E.2 Errores de administrador	7	3	21	A
		A.5 Suplantación de identidad	7	4	28	MA
		A.11 Acceso no autorizado	7	3	21	A
		A.19 Divulgación de información	7	3	21	A
[epd]	Servidor	N.1 Fuego	10	1	10	A
		N.2 Daños por agua	10	1	10	A
		I.6 Corte del suministro eléctrico	10	3	30	MA
		I.7 condiciones inadecuadas de temperatura	10	2	20	MA
		I.10 Degradación de los soportes de almacenamiento	10	1	10	A
		E.8 Difusión de software dañino	10	3	30	MA
		E.20 Vulnerabilidades de los programas	10	2	20	MA
		E.21 Errores de mantenimiento / actualización de programas	10	2	20	MA
		E.22 Errores de mantenimiento / actualización de equipos	10	2	20	MA
		A.11 Acceso no autorizado	10	1	10	A
[ef]	Computador	I.6 Corte del suministro eléctrico	3	3	9	B
		A.11 Acceso no autorizado	3	2	6	B
		A.18 Destrucción de información	3	3	9	B
		A.19 Divulgación de información	3	3	9	B

[om-4]	Expediente de ingreso de Medicamentos	N.2 Daños por agua	5	1	5	B
		I.1 Fuego	5	1	5	B
		A.11 Acceso no autorizado	5	3	15	M
		A.18 Destrucción de información	5	3	15	M
		A.19 Divulgación de información	5	3	15	M
[om-5]	Rexportes salida de Medicamentos	N.2 Daños por agua	5	1	5	B
		I.1 Fuego	5	1	5	B
		A.11 Acceso no autorizado	5	3	15	M
		A.18 Destrucción de información	5	3	15	M
		A.19 Divulgación de información	5	3	15	M
[om-6]	Contratos de medicamentos con proveedores	N.2 Daños por agua	7	1	7	M
		I.1 Fuego	7	1	7	M
		A.11 Acceso no autorizado	7	3	21	A
		A.18 Destrucción de información	7	3	21	A
		A.19 Divulgación de información	7	3	21	A
[pp]	Disco Duro Externo	I.10 Degradación de los soportes de almacenamiento	7	2	14	A
		A.11 Acceso no autorizado	7	1	7	M
		A.18 Destrucción de información	7	2	14	A
		A.19 Divulgación de información	7	2	14	A
		A.25 Robo	7	3	21	A
[pe-1]	Jefe de AEM	E.7 Deficiencias en la organización	7	2	14	A
		E.28 Indisponibilidad del personal	7	2	14	A
		A.30 Ingeniería social	7	3	21	A
		E.19 Fuga de información	7	4	28	MA
[pe-2]	Jefe de TI	E.7 Deficiencias	7	2	14	A

		en la organización				
		E.28 Indisponibilidad del personal	7	2	14	A
		A.30 Ingeniería social	7	1	7	M
		E.19 Fuga de información	7	2	14	A
[red-1]	Fibra Óptica Claro	N.3 Desastres Naturales	8	2	16	A
		I.6 Corte del suministro eléctrico	8	3	24	A
		I.7 condiciones inadecuadas de temperatura	8	3	24	A
		I.1 Fuego	8	1	8	M
		I.2 Daños por agua	8	3	24	A
		A.7 Uso no previsto	8	2	16	A
[red-2]	Radio Enlace	N.3 Desastres Naturales	9	2	18	A
		I.6 Corte del suministro eléctrico	9	3	27	A
		I.7 condiciones inadecuadas de temperatura	9	3	27	A
		I.1 Fuego	9	1	9	M
		I.2 Daños por agua	9	3	27	A
		A.7 Uso no previsto	9	2	18	A

*Para la elaboración de esta plantilla, tener en cuenta la tabla de frecuencia y valor de amenazas contenida en el documento "ELEMENTOS Y CARACTERISTICAS SGSI" donde detalla los datos a determinar por cada amenaza identificada.

CONCLUSIONES

HISTORIAL DE VERSIONES		
v. 1.0	FECHA: __/06/2021	ELABORADO POR: JIZQUIERDOC
	Descripción: ELABORACION INICIAL DE EVALUACION DE RIESGOS	
…	…	…
	…	
RESPONSABLES		**FIRMAS**
	JIZQUIERDOC	

ELABORADO POR:		
REVISADO POR:	DALFAROL	
APROBADO POR:	DALFAROL	

LOGO DE LA ORGANIZACIÓN	**TRATAMIENTO DEL RIESGO**	
	CÓDIGO SGSI Nº PLAN-012	FECHA ELABORACIÓN: ____/06/2021
		FECHA APLICACIÓN: ____/06/2021
FASE: III - GESTIÓN DE RIESGOS		**PROCESO: 3.3. TRATAMIENTO DEL RIESGO**
OBJETIVOS	-Determinar el nivel de tratamiento para los riesgos de mayor capacidad. -Determinar las salvaguardas para la reducción de riesgos en los activos de seguridad. -Los parámetros establecidos en la definición deben contar con una revisión periódica del SGSI.	
DESCRIPCIÓN	Previo a la recolección de información se hace uso del análisis de los documentos de entrada.	

ACTIVO	AMENAZA	RIESGO	TRATAMIENTO	SALVAGUARDA
Historias clínicas	A.11 Acceso no autorizado	MA	MR	Implementación de controles de ingreso físicos. Asegurar las instalaciones.
	A.19 Divulgación de información	MA	MR	Capacitación al personal sobre ética y seguridad de la información.
Recetas medicas	A.11 Acceso no autorizado	MA	MR	Implementación de controles de ingreso físicos. Asegurar las instalaciones.
Base de datos SIAF	A.5 Suplantación de identidad	MA	MR	Implementación de políticas de control de acceso lógico.
	A.11 Acceso no autorizado	MA	MR	Registro y baja de usuarios.

				Sistema de gestión de contraseñas.
Base de datos SIGA	A.5 Suplantación de identidad	MA	MR	Implementación de políticas de control de acceso lógico.
	A.11 Acceso no autorizado	MA	MR	Registro y baja de usuarios. Sistema de gestión de contraseñas.
	A.19 Divulgación de información	MA	MR	Capacitación al personal sobre ética y seguridad de la información. Registro de eventos en el sistema. Restricción de acceso a la información.
Base de datos SISMED	A.5 Suplantación de identidad	MA	MR	Implementación de políticas de control de acceso lógico.
Servidor	I.6 Corte del suministro eléctrico	MA	MR	Implementación de sistema eléctrico de respaldo.
	I.7 condiciones inadecuadas de temperatura	MA	MR	Implementación de sistema de aire acondicionado
	E.8 Difusión de software dañino	MA	MR	Revisión de reportes de eventos de seguridad de la información. Implementación de controles contra código malicioso.
	E.20 Vulnerabilidades de los programas	MA	MR	Reporte de debilidades de Seguridad de la información.
	E.21 Errores de mantenimiento / actualización de programas	MA	MR	Política de actualizaciones y mantenimientos.
	E.22 Errores de mantenimiento / actualización de equipos	MA	MR	Política de actualizaciones y mantenimientos.
Jefe AEM	E.19 Fuga de información	MA	MR	Capacitación al personal sobre ética y seguridad de la información.

CONCLUSIONES
Para esta primera iteración solo se consideró el tratamiento a riesgos de grado MUY ALTO (MA)

HISTORIAL DE VERSIONES		
v. 1.0	FECHA: __/06/2021	ELABORADO POR: JIZQUIERDOC
	Descripción: ELABORACION INICIAL DE TRATAMIENTO DE RIESGOS	

…	…	…
	…	

RESPONSABLES		FIRMAS
ELABORADO POR:	JIZQUIERDOC	
REVISADO POR:	DALFAROL	
APROBADO POR:	DALFAROL	

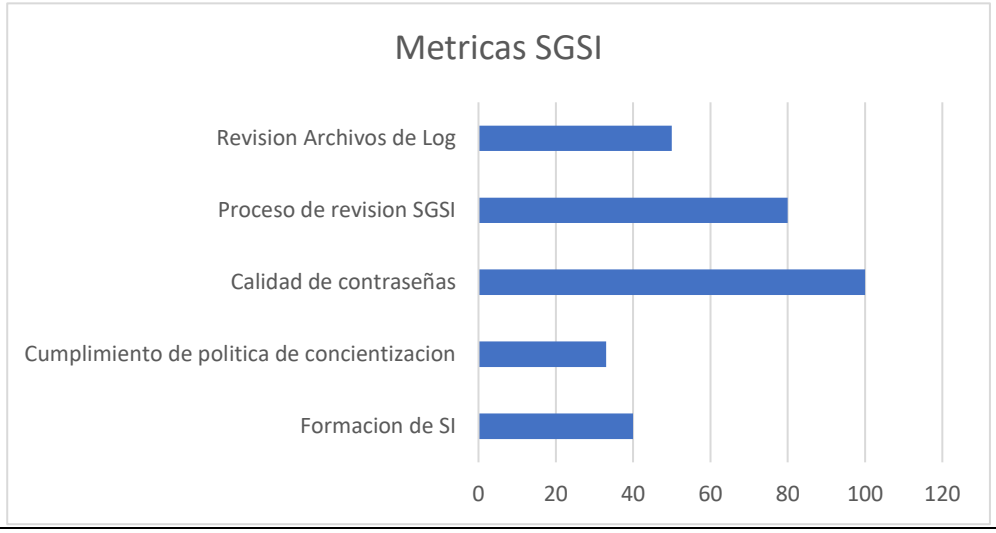
LOGO DE LA ORGANIZACIÓN	**MONITOREO Y EVALUACION SGSI**	
	CÓDIGO SGSI Nº PLAN-013	FECHA ELABORACION: ____/07/2021
		FECHA APLICACIÓN: ____/07/2021
FASE: IV - CONTROL DEL SGSI		**PROCESO: 4.1.1 MONITOREO DEL SGSI 4.1.2 EVALUACION DEL SGSI**
OBJETIVOS	- Registrar el nivel de cumplimiento de las pruebas orientadas a temas de seguridad se la información que no está directamente relacionada con las áreas de ti de la entidad. - Registrar el nivel de cumplimiento de los controles y componentes técnicos. - Registrar el nivel de cumplimiento de acuerdo a las métricas del SGSI.	
DESCRIPCION	Previo a la recolección de información se hace uso del análisis de los documentos de entrada.	

INSTRUMENTO DE MONITOREO
El presente modelo cuenta con una herramienta de monitoreo y evaluación la cual sirve de apoyo en la recolección de información, análisis y evaluación asistida del SGSI

EVALUACION DE CONTROLES

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	70	100	GESTIONADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	33	100	REPETIBLE
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	54	100	EFECTIVO
A.8	GESTIÓN DE ACTIVOS	32	100	REPETIBLE
A.9	CONTROL DE ACCESO	70	100	GESTIONADO
A.10	CRIPTOGRAFÍA	0	100	INEXISTENTE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	40	100	REPETIBLE
A.12	SEGURIDAD DE LAS OPERACIONES	39	100	REPETIBLE
A.13	SEGURIDAD DE LAS COMUNICACIONES	10	100	INICIAL
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	0	100	INEXISTENTE
A.15	RELACIONES CON LOS PROVEEDORES	0	100	INEXISTENTE
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	23	100	REPETIBLE
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	20	100	INICIAL
A.18	CUMPLIMIENTO	37.5	100	REPETIBLE
PROMEDIO EVALUACIÓN DE CONTROLES		31	100	REPETIBLE

EVALUACION DE SGSI



CONCLUSIONES

En esta sección se define el comentario final o apreciación de lo observado posterior al llenado de la plantilla.

HISTORIAL DE VERSIONES

v. 1.0	FECHA: __/07/2021	ELABORADO POR: JIZQUIERDOC
	Descripción: MONITOREO DE SGSI PRIMERA ITERACION	
…	…	…

	…

RESPONSABLES		FIRMAS
ELABORADO POR:	JIZQUIERDOC	
REVISADO POR:	DALFAROL	
APROBADO POR:	DALFAROL	

LOGO DE LA ORGANIZACIÓN	DEFINIR ACCIONES CORRECTIVAS	
	CÓDIGO SGSI Nº PLAN-014	FECHA ELABORACION: ____/07/2021
		FECHA APLICACIÓN: ____/07/2021
FASE: IV - CONTROL Y EVALUACION DEL SGSI		PROCESO: 4.2 DEFINIR ACCIONES CORRECTIVAS
OBJETIVOS	-Identificar las no conformidades suscitadas en todo el ciclo del modelo. -Evaluar las acciones correctivas para cada conformidad.	
DESCRIPCION	Previo a la recolección de información se hace uso del análisis de los documentos de entrada.	

NO CONFORMIDADES	CAUSA	EFECTO	ACCION CORRECTIVA
Unidad de almacenamiento externo para Backus y log también es usado con otros fines	No se cuenta con dispositivo de almacenamiento dedicado para almacenar Backus y log.	Alto	Solicitar adquisición de disco duro de 4tb para almacenar copias de respaldo.
Las capacitaciones sobre Seguridad de la Información no toman en cuenta a los proveedores de la entidad.	El alcance del SGSI lo contempla, pero no se realizó la invitación.	Medio	Se recomienda contemplar a todos los proveedores, invitarlos y agregar una cláusula de responsabilidad

			en los contratos.
No se guarda una copia de los registros de ingreso y salida del personal al AEM	No se tomó en cuenta.	Medio	Plan de respaldo de registro de ingreso y salida del personal al AEM

CONCLUSIONES
Las no conformidades fueron identificadas por el auditor interno y la definición de acciones correctivas por parte del equipo de SGSI

HISTORIAL DE VERSIONES		
v. 1.0	FECHA: __/07/2021	ELABORADO POR: JIZQUIERDOC
	Descripción: DEFINICION DE ACCIONES CORRECTIVAS	
…	…	…
	…	

RESPONSABLES		**FIRMAS**
ELABORADO POR:	JIZQUIERDOC	
REVISADO POR:	DALFAROL	
APROBADO POR:	DALFAROL	