Implementación de un sistema de seguridad de la información en empresa del sector salud: Caso de estudio

Implementation of an information security system in a health sector company: Case study

Jorge Andrés Llanos Cardona
Universidad Autónoma de Manizales, Colombia
Fabián Albeiro López
Universidad Autónoma de Manizales, Colombia
Mauricio Mejía-Lobo
Universidad de Manizales, Colombia
Correspondencia: jorgea.llanosc@autonoma.edu.co, fabian.lopezc@autonoma.edu.co, mmejialobo@umanizales.edu.co

RESUMEN. El presente proyecto de investigación se basó en el diseño de un conjunto de procesos para gestionar eficientemente la confidencialidad, integridad y disponibilidad de los activos de información de una entidad prestadora de servicios de salud, buscando proteger y controlar la información y asegurar por medio de la minimización de los riesgos que la entidad pueda afrontar. Para lograr el diseño, se trabajó bajo la norma ISO/IEC 27001, Alexander (2007) especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) según el conocido "Ciclo de Deming": PDCA – acrónimo de **P**lan, **D**o, **C**heck, **A**ct (Planificar, Hacer, Verificar, Actuar), siendo éste un enfoque de mejora continua. Según el decreto 1008 de 2018, la entidades oficiales en Colombia deben establecer los lineamientos generales de la política de gobierno digital y dentro de estos lineamientos, se encuentra el uso del Modelo de Seguridad y Privacidad de la Información -MSPI; el cual parte de un análisis de riesgos y la definición del Plan de Tratamiento de Riesgos que busca mitigar los riesgos identificados, evitando aquellas situaciones que impidan el logro de los objetivos de la entidad prestadora de servicios de salud y del Ministerio Tecnologías de la Información y las Comunicaciones (MINTIC). Mediante la creación y aplicación de este sistema, se logró, proteger y salvaguardar la información de la entidad, salvaguardando los atributos de disponibilidad, integridad y disponibilidad en cumplimiento de a ley y de los datos personales de los usuarios.

Palabras clave: Sistema de gestión de seguridad de la información, ISO 27001, seguridad de la información, institución hospitalaria, protección de datos.

ABSTRACT. This research project was based on the design of a set of processes to efficiently manage the confidentiality, integrity, and availability of the information assets of the health service provider, seeking to protect and control the information and ensure through the minimization of the risks that the entity may face. To achieve the design, we worked under the ISO/IEC 27001 standard, which specifies the necessary requirements to establish, implement, maintain, and improve an Information Security Management System (ISMS) according to the well-known "Deming Cycle": PDCA – acronym for **P**lan, **D**o, **C**heck, **A**ct (Plan, Do, Verify, Act), this being an approach to continuous improvement. According to Decree 1008 of 2018, official entities in Colombia must establish the general guidelines of the digital government policy and within these guidelines, there is the use of the Information Security and Privacy Model -MSPI; which is based on a risk analysis and the definition of the Risk Treatment Plan that seeks to mitigate the identified risks, avoiding those situations that prevent the achievement of the objectives of the health service provider and the Ministry of Information and Communications Technologies (MINTIC). Through the creation and application of this system, it was possible to protect and safeguard the entity's information, safeguarding the attributes of availability, integrity and availability in compliance with the law and the users' personal data.

Llanos Cardona, J. A., López, F. A. y Mejía-Lobo, M., (2023). **Implementación de un sistema de seguridad de la información en empresa del sector salud. Caso de estudio.** *SUMMA. Revista disciplinaria en ciencias económicas y sociales*, 5(2), 1-14. https://doi.org/10.47666/summa.5.2.7

Keywords: Information security management system, ISO 27001, information security, hospital, data protection.

Recibido: 09/06/2023 Aceptado: 30/11/2023

1. Introducción

El Ministerio de Tecnologías de la Información y las Comunicaciones, lidera la política de gobierno digital, a través de la Dirección de Gobierno Digital y se encarga de emitir las normas, manuales, guías y la metodología de seguimiento y evaluación para la implementación de la política de Gobierno Digital, en las entidades públicas del orden nacional y territorial.

Adicionalmente, el representante legal es el responsable Institucional de la Política de Gobierno Digital y debe coordinar, hacer seguimiento y verificación de la implementación de la Política de Gobierno Digital. Así como también, son responsables de la política de Gobierno Digital, los ministros, directores, gobernadores, alcaldes y gerentes quienes deben garantizar el desarrollo integral de la política al interior de las entidades, entendiendo que esta es un eje transversal y apalancador de su gestión interna que apoya el desarrollo de las políticas de gestión y desempeño institucional. Y de contar con sistemas de gestión integrales tal como lo presenta Atehortúa Hurtado et al., (2008).

El estado colombiano, por medio de diferentes normativas, ha establecido los lineamientos que deben cumplir las instituciones públicas, y los entes territoriales, por ejemplo, se encuentra el CONPES 3854 de 2016, el Modelo de Seguridad y Privacidad de MINTIC y lo establecido en el decreto 1008 de 14 de junio 2018, adoptando las buenas prácticas y los lineamientos de los estándares ISO 27001, recomendado por Calderón & Sánchez (2012), ISO 31000:2018 y la guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 4 emitida por el DAFP.

También emite el decreto 1008 de 2018 se establece la Política de Gobierno Digital en Colombia, y es por medio de este acto administrativo que se evidencia la evolución del gobierno electrónico en el país, por cuanto permite que las entidades públicas mejoren su gestión, sean más eficientes en atender las necesidades y problemáticas que aquejan a los ciudadanos y como consecuencia de ello, los servicios que brindan sean óptimos, transformando de esta manera la forma en que el Estado se relaciona con las personas.

El avance en los procesos y en las tecnologías de la información ha permitido a las empresas implementar herramientas y estrategias que permiten proteger la información y los sistemas. Las Instituciones tipo empresa Social del Estado, son sujetas de esta realidad, por lo que deben implementar y adecuar sus sistemas organizacionales para cumplir con lo exigido por esta normatividad.

Estos sistemas generalmente parten del sistema de gestión de la calidad y que, en muchas organizaciones, son sistemas integrales de gestión, dentro de los que se encuentra el Sistema de Gestión de Seguridad de la Información - SGSI, Asencio (2006) definido entre otras normativas por la ISO 27001. Estas amplias gamas de sistemas se apoyan en tecnologías de software o de hardware que buscan gestionar los grandes volúmenes de información que manejan y es allí donde se debe proteger la información, pues se vuelven elementos atractivos para que los ciberdelincuentes u otros individuos logren materializar sus actos delincuenciales González (2021).

No obstante, debido al crecimiento de las tecnologías y de las constantes y nuevas amenazas, no es posible tener un sistema totalmente seguro, lo que es potencializado por la universalización y uso masivo del internet para el manejo de las comunicaciones.

Con el fin de establecer el nivel de cumplimiento de la Institución hospitalaria en la cual se diseñó y e implementó el modelo, se aplicó el instrumento MPSI de diagnóstico, de acuerdo con el trabajo de Carvajal et al., (2019), el cual permitió calcular una calificación para cada uno de los dominios, totalizando a partir de los valores registrados y promediados la cantidad de objetivos de control a establecer referenciados desde las hojas nombradas como "ADMINISTRATIVAS y TÉCNICAS" dentro de la Herramienta Instrumento MSPI. Los productos

alcanzados para la evaluación del estado actual reflejan la efectividad y los controles según la normatividad NTC/ISO 27001, Edith (2015), planteado dentro del modelo de seguridad y privacidad de la información que estableció el MINTIC direccionado a las entidades públicas de orden territorial, con el establecimiento del ciclo PHVA (Planear - Hacer -Verificar -Actuar). Con el diligenciamiento de la herramienta MSPI, se obtuvieron los siguientes resultados de los dominios para la EVALUACIÓN Y EFECTIVIDAD DE CONTROLES:

Ilustración 1. Diagnóstico de seguridad de la información

EVALUACIÓN DE EFECTIVIDAD 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	40	100	REPETIBLE
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	23	100	REPETIBLE
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	46	100	EFECTIVO
A.8	GESTIÓN DE ACTIVOS	18	100	INICIAL
A.9	CONTROL DE ACCESO	22	100	REPETIBLE
A.10	CRIPTOGRAFÍA	0	100	INEXISTENTE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	15	100	INICIAL
A.12	SEGURIDAD DE LAS OPERACIONES	1	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	60	100	EFECTIVO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	14	100	INICIAL
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	20	100	INICIAL
A.18	CUMPLIMIENTO	55	100	EFECTIVO
	PROMEDIO EVALUACIÓN DE CONTROLES	**22**	**100**	REPETIBLE

Fuente: Modelo MSPI.

De acuerdo con el análisis y los resultados obtenidos, la calificación promediada de los controles dentro de la entidad fue de 22 sobre 100, lo cual evidenció que la entidad estaba en un proceso inicial de implementación planteado por Jiménez (2009), de medidas para la seguridad y privacidad de la información, de los responsables de esta y los activos que la contienen, actualmente se encuentra en proceso de revisión y mejora de los controles existentes.

La entidad estaba en un proceso definido con respecto a los aspectos referentes a la implementación de medidas y controles destinados a la privacidad y seguridad de la información así mismo como la protección de los activos que la contienen. La brecha identificada mediante el desarrollo de esta evaluación se puede ver identificada en el siguiente gráfico (Ilustración 2).

Ilustración 2: Resultados Anexo Diagnóstico ISO/IEC 27002

Fuente: Evaluación interna frente al modelo MSPI.

Según fechas establecidas en el Decreto 1078 de 2015, para el desarrollo de las actividades correspondientes a la implementación del modelo de seguridad y privacidad de la información el cual se basa en aspectos del marco 27001, para el año 2018 todas las entidades a nivel nacional deberían cumplir con la meta propuesta la cual está entre el 80% y el 100% de ejecución del MSPI. Como se evidencia en el gráfico anterior, la entidad se encuentra en un % muy bajo en la implementación de sus controles, pero a la fecha debería estar en el 100%, para esto se han venido realizando acciones y mejoras frente a la implementación de documentos, formatos y controles al interior de la entidad, con el fin de no poner en riesgo en gran medida cada aspecto relacionado con la información y su valor.

Por lo anterior, nace la pregunta: ¿Cómo asegurar la información de los procesos de apoyo tecnológico, de la institución hospitalaria en cuanto a los atributos de su confidencialidad disponibilidad e integridad?

Conforme con lo expuesto en el planteamiento del problema, es de suma importancia crear un marco de desarrollo e implementación de un sistema de gestión de la seguridad de la información basadas en la norma ISO 27001, para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información.

Aunado a lo anterior, otro hito importante a tener en cuenta en este tipo de entidades es lo relativo con la Historia clínica y la Historia clínica digital expuesto en Gerencia General de EsSalud. (2014), la cual es el registro obligatorio de las condiciones de salud del paciente y contiene los datos de los pacientes de acuerdo con la Ley 23 de 1981, por la cual se dictan normas en materia de ética médica y de acuerdo con el artículo 34 "La historia clínica es el registro obligatorio de las condiciones de salud del paciente. Es un documento privado sometido a reserva que únicamente puede ser conocido por terceros previa autorización del paciente o en los casos previstos por la Ley". Entiéndase que todos los datos de los pacientes son parte integral de la historia clínica. Atienza (2013).

La Resolución 1995 de 1999 en su artículo 18 señala, que los Prestadores de Servicios de Salud pueden utilizar medios físicos o técnicos para el registro y conservación de la historia clínica como computadoras y medios magneto ópticos, cuando así lo consideren conveniente, atendiendo lo establecido en la Circular 02 de 1997 expedida por el Archivo General de la Nación, o las normas que la modifiquen o adicionen.

De otro lado, es necesario anotar que la Ley 594 de 2000 y todos los acuerdos promulgados por el Archivo General de la Nación, debe aplicarse a efectos de las actividades inherentes a la gestión de los archivos de historias clínicas como son: la retención, conservación, disposición final y eliminación.

La Resolución 1995 de 1999, en el artículo 18, en relación con los medios técnicos de registro y conservación de la historia clínica, establece:

"Los Prestadores de Servicios de Salud pueden utilizar medios físicos o técnicos como computadoras y medios magnetoópticos, cuando así lo consideren conveniente, atendiendo lo establecido en la circular 2 de 1997 expedida por el Archivo General de la Nación, o las normas que la modifiquen o adicionen. Los programas automatizados que se diseñen y utilicen para el manejo de las Historias Clínicas, así como sus equipos y soportes documentales, deben estar provistos de mecanismos de seguridad, que imposibiliten la incorporación de modificaciones a la Historia Clínica una vez se registren y guarden los datos. En todo caso debe protegerse la reserva de la historia clínica mediante mecanismos que impidan el acceso de personal no autorizado para conocerla y adoptar las medidas tendientes a evitar la destrucción de los registros en forma accidental o provocada. (Bahos & Mora, 2014).

Los prestadores de servicios de salud (Guillen et al., 2011) deben permitir la identificación del personal responsable de los datos consignados, mediante códigos, indicadores u otros medios que reemplacen la firma y sello de las historias en medios físicos, de forma que se establezca con exactitud quien realizó los registros, la hora y fecha del registro.

La circular 02 citada, establece que podrán incorporarse tecnologías de punta en la administración de los archivos, pudiéndose utilizar cualquier soporte documental, por medio técnico, electrónico, óptico, informático, o telemático para el cumplimiento de sus funciones, siempre y cuando cumplan los debidos requisitos.

2. Metodología

El enfoque de la investigación es de enfoque metodológico mixto con aplicación cuantitativa y cualitativa para el análisis de riesgos. En el estudio se propuso un alcance descriptivo para considerar el fenómeno estudiado y sus componentes, medir los conceptos y definir las variables.

Para el desarrollo del proyecto de diseño de Sistema de Gestión de Seguridad de la Información ajustado a las necesidades, la base fue el ciclo de mejora continua PCDA (planear, hacer, verificar y actuar) de la norma ISO 27001. La siguiente tabla (tabla 1) relaciona cada una de las fases y sus actividades para la aplicación de la metodología propuesta:

Tabla 1: Fases y Actividades ciclo PCDA – SGSI

FASES CICLO PDCA	ACTIVIDADES
Planear	□ Definir el alcance del SGSI □ Definir la política de seguridad □ Metodología para la evaluación de riesgos □ Inventario de Activos □ Identificar amenazas y vulnerabilidades □ Identificar el impacto □ Análisis y evaluación de riesgos □ Selección de Controles y SOA

Hacer	□ Definir el plan de tratamiento de riesgos □ Implementar el plan de tratamiento de riesgos □ Implementar los controles □ Formar y concientizar □ Aplicar el SGSI
Verificar	□ Revisar el SGSI □ Medir la eficacia de los controles □ Revisar los riesgos residuales □ Realizar auditorías internas del SGSI □ Registrar eventos y acciones
Actuar	□ Implementar mejoras al SGSI □ Aplicar acciones correctivas □ Aplicar acciones preventivas □ Comprobar la eficacia de las acciones

Fuente: Elaboración propia.

3. Operacionalización de variables

a) Definir el alcance y límites del SGSI en términos de las características del negocio, la entidad, su ubicación, sus activos, tecnología, e incluir los detalles y justificación de cualquier exclusión del alcance.
b) Definir una política de SGSI en términos de las características del negocio, la entidad, su ubicación, sus activos y tecnología.
c) Definir el enfoque organizacional para la valoración del riesgo.
d) Identificar los riesgos.
e) Analizar y evaluar los riesgos.
f) Identificar y evaluar las opciones para el tratamiento de los riesgos.
g) Seleccionar los objetivos de control y los controles para el tratamiento de los riesgos.
h) Obtener la aprobación de la dirección sobre los riesgos residuales propuestos.
i) Obtener autorización de la dirección para implementar y operar el SGSI.
j) Elaborar la declaración de aplicabilidad.

Para el análisis de riesgos, se usa la metodología MAGERIT, que acompaña el análisis en las escalas por los activos que se manejan en la organización, es un estándar Español de amplio uso y probada eficiencia usado en múltiples análisis como lo presentado por Mirza (2012).

Con el fin de establecer los impactos de cumplimiento de la institución frente al estándar, se realizó un cuestionario con las siguientes preguntas al personal por cada una de las dimisiones a calificar:

- Confidencialidad: ¿Cómo afectaría a la Institución que la información sea conocida por personas ajenas no autorizadas?
- Integridad: ¿Cuál sería el daño para la Institución si un activo resultara corrupto?
- Disponibilidad: ¿Cómo afectaría a la Institución que un activo no pudiera ser utilizado?

De otro lado, con el fin de establecer los procesos críticos de seguridad visualizados desde el área de TI, se aplicó la siguiente encuesta al jefe de gestión informática:

1. ¿Cuáles son los activos físicos más importantes en cada proceso de la institución?
2. Para cada uno de los activos físicos que usted considera ¿Cuál sería su valor de disponibilidad? Elija entre las siguientes opciones:

- 10 Extremo
- 9 Muy alto
- 6-8 Alto
- 3-5 Medio
- 1-2 Bajo
- Insignificante

3. Para cada uno de los activos físicos que usted considera ¿Cuál sería su valor de confidencialidad? Elija entre las siguientes opciones:
    - 10 Extremo
    - 9 Muy alto
    - 6-8 Alto
    - 3-5 Medio
    - 1-2 Bajo
    - 0 Insignificante

4. Para cada uno de los activos físicos que usted considera ¿Cuál sería su valor de integridad?
Elija entre las siguientes opciones:
    - 10 Extremo
    - 9 Muy alto
    - 6-8 Alto
    - 3-5 Medio
    - 1-2 Bajo
    - 0 Insignificante

5. Para el tipo de amenaza' x', ¿cuál sería su probabilidad de ocurrencia sobre este activo? Teniendo en cuenta:
    - 10 Muy alto
    - 9 Alto
    - 6-8 Medio
    - 3-5 Bajo
    - 1-2 Muy baja

6. Para el tipo de amenaza' x', ¿cuál sería su frecuencia de ocurrencia sobre este activo? Teniendo en cuenta:
    - A diario
    - Mensualmente
    - Más de una vez al año
    - una vez al año
    - Rara vez

7. ¿Qué tan vulnerable se encuentra expuesto el activo, para el tipo de vulnerabilidad ¿x?
Teniendo en cuenta:
    - 10 Muy alto
    - 9 Alto

- 6-8 Medio
- 3-5 Bajo
- 1-2 Muy baja

8. Para el tipo de vulnerabilidad' x', ¿cuál sería su frecuencia de ocurrencia sobre este activo? Teniendo en cuenta:
    - A diario
    - Mensualmente
    - Más de una vez al año
    - una vez al año
    - Rara vez

4. Resultados

Para entender y conocer la situación actual de la Institución, se realizó entrevista al ingeniero encargado de la gestión y el análisis de todas las herramientas de seguridad de la institución.

Entrevista sobre la gestión de seguridad informática

Tabla 3: Entrevista al analista de seguridad TI

Entrevistado: Ingeniero CISO
Cargo: Analista de Seguridad TI

PREGUNTA	RESPUESTA
1. ¿Qué problemas de seguridad informática ha tenido el hospital?	• Ataques en correos electrónicos. • Spam. • Secuestro de información.
2. ¿Cuál problema fue más perjudicial para la empresa y que aún no se ha podido controlar en su totalidad?	Pérdida de información.
3. ¿Qué acciones ha realizado la empresa en conjunto con el departamento de TI para mejorar la calidad de seguridad de la información?	El hospital optó por contratar el servicio de terceros para controlar los ataques a través de correo electrónico, forzando a cada carreo a pasar por el análisis del sophos de la institución.
4. ¿La institución cuenta con políticas de seguridad para la proteger la información?	No Existen Políticas
5. Cómo es administrada la red interna?	• La red Corporativa está distribuida por la seguridad perimetral (sophos), va al switche principal por y este distribuye en un anillo de fibra a los switches secundarios distribuidos por todos los pisos; no existen VLAN
6. ¿Cómo se encuentra la seguridad física para acceso a los servidores en la empresa?	• El acceso a los servidores se encuentra determinados solo a usuarios autorizados, en el caso de ser personas no autorizadas se deberá llenar una bitácora con sus datos.

	• El espacio físico se encuentra bajo vigilados por cámaras de seguridad.

Fuente: Elaboración propia.

Entrevista al ingeniero gestor de hardware y software

Tabla 4. Gestor de hardware y software

Entrevistado: Ingeniero
Cargo: Gestor de hardware y software

PREGUNTA	RESPUESTA
1. ¿Cómo es la distribución de software y equipos informáticos para el personal?	• El personal con el cargo de Gestor de Hardware y Software es el encargado de distribuir los equipos según su cargo y su perfil tecnológico.
2. ¿Todo el software utilizado en la empresa posee licencia?	• Todo el software utilizado en la empresa posee una licencia para su uso. • Existen programas que se instalan cuando su licencia es libre o tienen versiones de prueba.
3. ¿Cuál es el procedimiento de un usuario final para realizar un requerimiento con el departamento de TI?	• El usuario final deberá ingresar al software web de requerimientos, el cual es un sistema de generación de tickets Helpdesk en el que se cargará automáticamente con su información (Equipo, usuario) y deberá describir su requerimiento de manera detallada que puede ser solo texto o enviar un archivo adjunto. • Posterior el envío de la solicitud se generará un numero de ticket para conocer el estado (Nuevo, en proceso, congelado, cancelado, en espera, cerrado,) • La solicitud llegara al personal de soporte técnico los cuales se encargarán de atender la solicitud
4.¿Cómo se maneja el acceso a la información de los servidores de archivos?	• La información se encuentra almacenada en una base de datos centralizada en un servidor Linux, a la cual los usuarios tanto administrativos como asistenciales solo podrán acceder a través del software de gestión hospitalaria Dinámica Gerencial. Los usuarios del equipo de TI tienen acceso a carpetas nombradas por área o piso de la institución, y son las únicas personas habilitadas para que mediante un ticket creado dar la autorización de acceso a la información a uno o varios usuarios y a que carpetas.
5. ¿La empresa cuenta con herramientas para realizar respaldo de información de cada empleado?	La empresa cuenta con licencias de Office en la que dispone de la nube OneDrive en la que se instala el cliente en el equipo de los empleados que requieran tener respaldado su información y de esa manera se sincronice automáticamente.

Fuente: Elaboración propia.

Inventario de activos

De acuerdo con la labor, se creó el inventario de activos, de cual se logró establecer:

- Equipo de energía: 44 UPS en estado activo y funcional.
- Equipos de seguridad Física: 5 equipos tipo DVR.
- *Servidores Virtualizados: 12 servidores.*
- *Equipo de Comunicaciones o Conmutación: 10 equipos de redes.*
- *Equipos de cómputo:* 389 equipos de cómputo.
- *Impresoras:* 88 impresoras.
- *Telefonía IP: 1 equipo controlador general.*
- *Access Point: 3 equipos.*
- *Sistemas Operativos: 5 clases de SO. De acuerdo con las seguridades que deben cumplir los sistemas libres (Perpiñan, 2011).*

De cada uno de estos equipos, adicionalmente se estableció el modelo y los años de obsolescencia de cada uno de los equipos.

Para obtener la valoración se realizaron encuestas al personal encargado de acuerdo con lo trabajado por Mora (2014), los procesos que involucran a cada activo, debido a que conocen a profundidad el significado que cada uno tienen dentro del modelo de negocio y como perjudicaría a la continuidad de la entidad si este llegara a sufrir algún daño:

- Confidencialidad: ¿Cómo afectaría a la E.S.E. que la información sea conocida por personas ajenas no autorizadas?
- Integridad: ¿Cuál sería el daño para la E.S.E. si un activo estuviera corrupto?
- Disponibilidad: ¿Cómo afectaría a la E.S.E. que un activo no pueda ser utilizado?

De acuerdo con la metodología Magerit, la valoración se realizó de manera cualitativa y cuantitativa. La Tabla 5 presenta la escala definida:

Tabla 1. Escala de valoración de activos

Valor	CID	Perspectiva
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	Insignificante	Irrelevante

Fuente: Elaboración propia.

Para la valoración de las amenazas y vulnerabilidades se realizó un check-list, el cual tuvo las siguientes columnas:

- Activo: Contienen el nombre del activo.
- Vulnerabilidad: Se describe la vulnerabilidad encontrada.
- Valoración Vulnerabilidad: Se presenta una lista con los valores de la escala definida anteriormente, que va de 0 a 10.
- Amenaza: se detalla la amenaza que puede explotar una determinada debilidad.

- Valoración Amenaza: Se presenta una lista con los valores de la escala definida anteriormente, que va de 0 a 10.
- Probabilidad de ocurrencia: Se presenta una lista con las opciones de selección de que son: extremo, muy bajo, bajo, medio, alto y muy alto.
- Frecuencia de ocurrencia: Se muestra una lista con las opciones de ocurrencia que son: a diario, mensualmente, una vez al año, más de una vez al año, rara vez, nunca.
- Justificación: En esta sección el personal escribió una justificación sobre la razón de sus respuestas en las columnas antes descritas.

A continuación un ejemplo sobre uno de los activos evaluados:

Tabla 6. Matriz cálculo de evaluación de Riesgos

				Tratamiento de los Riesgos											
				Impacto				Probabilidad							
Nro. Activo	Nombre Activo	Amenazas	Vulnerabilidad	Confidencialidad	Integridad	Disponibilidad	CID	Nivel de amenaza	Nivel del vulnerabilidad	Controles implementados existentes	Cáculo de Evaluación de riesgos	Nivel de riesgos	Metodo de tratamiento de riego	Tipo de control	Controles a implementar
1 A-HAR	PCs Escritorio	Incendio	Monitoreo inadecuado del sistema contra incendios o falta de mantenimiento de extintores.	4	7	9	6,67	2	2	Extintores, alarmas de humo, control interno del Dpt de seguridad, salud y ambinte	13,33	Despreciable	Mitigar	A.11. SEGURIDAD FÍSICA Y AMBIENTAL.	A.11.1.4. Protección contra amenazas externas y ambientales
		Daño por agua	Mantenimiento inadecuado de las instalaciones físicas	4	7	9	6,67	2	1	Control interno del dpt. Mantenimiento	10,00	Despreciable	Evitar	A.11. SEGURIDAD FÍSICA Y AMBIENTAL.	A.11.2.1. Ubicación y protección de los equipos
		Destrucción del equipo o los medios	Ausencia de esquemas de reemplazo periódico	7	10	10	9,00	6	2	Plan de mantenimiento Preventivo	36,00	Bajo	Aceptar	A.11. SEGURIDAD FÍSICA Y AMBIENTAL.	A.11.2.4. Mantenimiento de equipos
		Polvo o corrosión	Susceptibilidad a la humedad, el polvo y la sociedad	2	2	2	2,00	8	1	Plan de mantenimiento Preventivo. Limpieza diaria por el	9,00	Muy Bajo	Aceptar	A.11. SEGURIDAD FÍSICA Y AMBIENTAL.	A.11.2.1. Ubicación y protección de los equipos
		Perdida del suministro de energía	Susceptibilidad a variaciones y voltajes	0	0	10	3,33	6	5	Planta alterna	18,33	Despreciable	Aceptar	A.11. SEGURIDAD FÍSICA Y AMBIENTAL.	A.11.2.2. Servicios Públicos de soporte
		Error en el uso	Ausencia de un eficiente control de cambios en la configuración	9	9	9	9,00	3	7	Active directory	45,00	Medio	Evitar	A.12. SEGURIDAD DE LAS OPERACIONES.	A.12.1.2. Gestión de Cambios
		Desastres Naturales	Susceptibilidad a variaciones de temperatura	0	0	2	0,67	1	1	Alertas del equipo	0,67	Despreciable	Alerta de equipos	A.11. SEGURIDAD FÍSICA Y AMBIENTAL.	A.11.1.5. Trabajo en áreas seguras
		Robo	Falta de protección para el almacenamiento de los equipos	4	3	9	5,33	6	1	Personal mlitar	18,67	Muy Bajo	Personal	A.11. SEGURIDAD FÍSICA Y AMBIENTAL.	A.11.2.1. Ubicación y protección de los equipos

Fuente: Elaboración propia.

Una vez realizado el análisis de riesgos según lo expuesto por Mejia-Lobo (2022), obtenido el resultado de las listas de comprobación (check-list), se determinan los controles del Anexo A de la norma ISO 27001 con los que se va a trabajar, considerando los riesgos y los recursos con los que cuenta la entidad.

5. Identificación de controles aplicables

Los controles de la norma ISO 27001 permiten diseñar políticas, mismas que ayudan a mitigar la materialización de amenazas que pueden afectar a cada uno de los activos de información. De acuerdo con estos controles se pueden establecer parámetros que permitan determinar las acciones de tratamiento del riesgo o el nivel de un riesgo residual, para el cual es necesario entablar acciones que mitiguen dicha materialización. Para el caso se tienen en cuenta los dominios que permitan establecer controles de seguridad física y del entorno, seguridad de las operaciones y de las comunicaciones, controles que garanticen la adquisición, desarrollo y mantenimiento de los sistemas de información y puesta en marcha de los activos de información de la entidad hospitalaria, además de controles que permitan una adecuada gestión de incidentes de seguridad de la información (Martín-Romo et al., 2008).

6. Roles y Responsabilidades para el SGSI

A continuación los perfiles definidos de los funcionarios que deberían apoyar en estos cargos a la entidad para la implementación del SGSI:

- **Responsable de Seguridad:** De acuerdo con lo que dicta la norma, se sugiere que el responsable tenga línea directa con la alta gerencia, debido a que existen decisiones que son transversales para toda la entidad y que obligatoriamente necesitan ser implementadas. Para que el responsable tenga voz de mando dentro de la entidad debe contar con el respaldo de las máximas autoridades, por lo que se sugiere que este sea miembro de alguna área estratégica en función de las competencias que tengan y de su cercanía con la dirección del hospital, y en caso de que no cuente con el conocimiento necesario para asumir su cargo es obligatorio que tenga asesoría técnica de seguridad por parte de la dirección de TIC, definido por Fernández (2012). El responsable es el encargado de mantener los atributos de confidencialidad, integridad y disponibilidad de todo tipo de información, en especial de la información crítica dentro de la entidad, en el formato que esta se presente, ya sea digital o física.
- **Comité de Dirección:** Se encarga estratégicamente de todas las decisiones de seguridad que afecten a la entidad, por lo que en este comité, deben estar incluidos temas administrativo, financieros, talento humano, legales y tecnológicos, razón por la que se sugiere que mínimo una persona de estas áreas vitales para la entidad lo conformen, debido a que los temas de seguridad tienen injerencia en la parte financiera y legal específicamente cuanto se trata del incumplimiento, y sobre todo en la parte técnica. Se sugiere que lo conforme los directores de estas áreas, ya que ellos son los que las dirigen y, además, son delegados o asignados por la máxima autoridad del hospital.
- **Comité de Gestión**: Comité encargado de controlar y gestionar toda la implementación del sistema de gestión de seguridad de la información en la entidad, razón por la cual, trabajará estrechamente con el responsable de seguridad. Del mismo modo, dicho comité tendrá la capacidad de tomar decisiones de seguridad por lo que se requiere que sea conformado por personal de los diferentes departamentos involucrados directa o indirectamente en el proceso de implementación del SGSI.

7. Diseño Política de seguridad de la información

Para la Institución la protección de la información persigue la disminución del impacto generado sobre sus activos, por todos los riesgos identificados, con el propósito de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de esta, acorde con las necesidades de los diferentes grupos de interés identificados (Talavera, 2015).

De acuerdo con lo anterior, esta política aplica según el alcance, sus funcionarios y terceros, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI.

8. Alcance y usuarios

La Política de Seguridad de la Información, en lo definido por Escriva et al., (2013) es aplicable a todos los funcionarios, personal externo, en consideración a que, en todas las áreas de esta entidad, por su modelo de negocio se maneja y procesa información soportada en medios físicos, magnéticos o una combinación de estos. Dicha información podría quedar expuesta a alteraciones, daños y revelación indebida, que puede comprometer la imagen de la entidad o de terceros, de no contar con mecanismos que permitan salvaguarda las misma.

9. Diseño de estándares

Una vez seleccionados e identificados los controles a implementarse para cada activo crítico de la entidad y respondiendo a las necesidades de seguridad de información la entidad, se hace necesario elaborar estándares de seguridad que respondan a los controles establecidos según el anexo A de la norma ISO 27001 (Velásquez, 2015),

permitiendo de este modo mitigar las amenazas, que en caso de ser materializadas podrían generar un grave daño a la continuidad de las actividades de la entidad, se diseñaron los siguientes procedimientos:

- ✓ Procedimiento de elaboración y ejecución del plan de capacitación
- ✓ Procedimiento de gestión y clasificación de activos
- ✓ Proceso de control de acceso y salida de visitantes
- ✓ Procedimiento para mantenimiento de equipos informáticos
- ✓ Procedimiento gestión de cambios
- ✓ Procedimiento para el respaldo periódico de información *objetivo*
- ✓ Procedimiento de administración de redes y comunicaciones

10. Conclusiones

Durante el desarrollo, se seleccionó a la metodología Magerit para realizar la gestión de riegos debido que es muy útil para las entidades que están iniciando con el proceso gestión de la seguridad de la información. Además, esta metodología permite enfocar los esfuerzos de la institución en minimizar riesgos que le puedan resultar más críticos.

Se realizó el levantamiento de información mediante observación directa y recopilación de información proporcionada por parte del personal de la Institución hospitalaria, se utilizó como guía la norma ISO 27001 y el modelo MCPI en base a los requerimientos de la entidad, lo que permitió identificar los activos de hardware, software, información, redes de comunicación, personal y servicios. También se establecieron los procesos críticos que esta casa de salud debería implementar para minimizar sus riegos (Rodrigues et al., 2016).

En el desarrollo del proyecto también se logró identificar las vulnerabilidades y amenazas de tipo natural o ambiental, humano o accidental, técnico y organizacional que afectan a los activos que se estudiaron en el presente documento. Este objetivo se logró gracias a la información proporcionada por parte de los custodios de los activos sobre incidentes ocurridos anteriormente y apoyándose en el catálogo de amenazas y vulnerabilidades que proporciona la metodología Magerit. Lo que posibilitó minimizar riesgos y generar una cultura de autocontrol en los colaboradores internos de la institución y garantizar al usuario una adecuada gestión de riesgos lo que redunda en un impacto en la imagen reputacional y en confiabilidad.

Finalmente, debido a que la institución hospitalaria no disponía de un SGSI que le permitiera resguardar de manera adecuadas sus activos de información, se realizó el establecimiento del diseño de un SGSI basado en la norma ISO/IEC 27001, con el fin de asegurar el cumplimiento normativo y legal y ante todo para proteger la integridad, disponibilidad y confidencialidad de la información de los usuarios.

Referencias bibliográficas

Alexander, A. G. (2007). Diseño de un Sistema de Gestión de Seguridad de Información. Óptica ISO 27001:2005. Alfaomega ed. ISBN: 9789586827133

Asencio, Gonzalo. (2006). Seguridad en Internet. Madrid: Ediciones.

Atehortúa Hurtado, F. A., Bustamante Vélez, R. E., & Valencia de los Ríos, J. A. (2008). Sistema de Gestión Integral: Una sola gestión, un solo equipo. Medellín: Universidad de Antioquia. De Pablos Heredero, C., López-Hermoso Agius, J. J.

Atienza, O. A. (2013). Historia Clínica informática única una herramienta en la mejora de procesos en salud pública. Córdoba, Argentina: Universidad Nacional de Córdoba.

Bahos, M., & Mora Bahos, A. (2014). La seguridad informática en el sistema de seguridad social de la salud colombiana, presentada en la clínica Miocardio. Bogotá: Universidad Piloto de Colombia.

Calderón Merchán, D. O., & Sánchez Meza, D. A. (2012). Desarrollo de un Sistema de Gestión de Seguridad de la Información (SGSI) para la Empresa Comware S.A. en la Ciudad de Quito, Aplicando la Norma ISO/IEC 27001. Quito, Ecuador: Universidad Politécnica Salesiana.

Carvajal, D. L., Cardona, A., & Valencia, F. J.. (2019). Una propuesta de gestión de la seguridad de la información aplicado a una entidad pública colombiana. *Entre Ciencia e Ingeniería*, *13*(25), 68-76. https://doi.org/10.31908/19098367.4016

Edith, A. T. (2015). Guía para Implantar un Sistema de Gestión de Seguridad de Información: Basada en la Norma ISO/IEC 27001. EAE.

Escriva, Gema; Romero, Rosa y Ramada, David. (2013). Seguridad informática. Madrid, ES: Macmillan Iberia, S.A. Retrieved from http://www.ebrary.com

Fernández, V. D. (2012). Sistema de Gestión de Seguridad de la Información. EAE.

Guillen Pinto, E. P., Ramírez López, L. J., & Estupiñán Cuesta, E. P. (2011). Análisis de seguridad para el manejo de la información médica en telemedicina. *Ciencia e Ingeniería Neogranadina*, P.57.

Gerencia General de EsSalud. (2014). Directiva de Gerencia General Nº 001-GG-ESSALUD2014. *Gestión de la Historia Clínica en los Centros Asistenciales del Seguro Social de Salud - ESSALUD*. Lima.

Gonzáles, Jacobo Cortés. 2021. El hack-back como modalidad de legítima ciberdefensa.

Jiménez, J. A. (2009). Evaluación: seguridad de un sistema de información, s.l. : El Cid Editor apuntes, 2009.

Mejía-Lobo, M. (2022). Software para la gestión de riesgos en las prácticas forenses de derecho basado en los principios de la norma ISO 31000 e ISO 27005 . Encuentros. Revista De Ciencias Humanas, Teoría Social Y Pensamiento Crítico., (Extra), 243–257. https://doi.org/10.5281/zenodo.6551136

Martín-Romo Romero, S., Medina Salgado, S., Montero Navarro, A., & Nájera Sánchez, J. J. (2008). Dirección y gestión de los sistemas de información en la empresa: una visión integradora. Madrid: ESIC.

Mirza B, M. (2012). Risk Management For Health Information Security And Privacy. *American Journal of Health Sciences*, 10.

Mora Bahos, A. (2014) La seguridad informática en el sistema de seguridad social de la salud colombiana, presentada en la clínica Miocardio. Universidad piloto de Colombia.

Perpiñan, Antonio. (2011). Seguridad de sistemas GNU/Linux. Fundación código libre dominicano. Recuperado de: http://highsec.es/wp-content/uploads/2013/10/LibroSeguridad-GNULinux-Antonio-Perpinan-2011.pdf

Rodrigues Martinez Basile, F., Cezar Amate, F., & Ramirez López, L. J. (2016). Desarrollo colaborativo en Telemedicina y Telesalud para la Educación, la atención y la investigación: Estudio de caso Lab.Sh-Brasil - Tigum-Colombia. Academia Y Virtualidad, 9(1), 123–141. https://doi.org/10.18359/ravi.1708

Talavera Álvarez, V. R. (2015). Diseño de un Sistema de Gestión de Seguridad de la Información para una Entidad Estatal de Salud de Acuerdo a la ISO/IEC 27001:2013. Lima, Perú: Pontificia Universidad Católica del Perú.

Velásquez Isaza, J. (2015). Modelamiento de los procesos de auditoría en seguridad de la información asociados a los dominios 6, 8, 13 Y 14 del anexo A de La norma ISO 27001 mediante una herramienta de flujo de trabajo. Tesis, Universidad Tecnológica de Pereira.