RECOMENDAR LAS MEJORES PRÁCTICAS EN EL SECTOR SALUD BASADAS EN FRAMEWORKS DE CIBERSEGURIDAD APLICABLES A HOSPITALES DEL SECTOR PUBLICO EN COLOMBIA

JESUS EDUARDO ROSERO CORDOBA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
PASTO
2024

RECOMENDAR LAS MEJORES PRÁCTICAS EN EL SECTOR SALUD BASADAS EN FRAMEWORKS DE CIBERSEGURIDAD APLICABLES A HOSPITALES DEL SECTOR PUBLICO EN COLOMBIA

JESUS EDUARDO ROSERO CORDOBA

Proyecto Aplicado presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMATICA

Ing. Christian Reynaldo Angulo
Asesor

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
PASTO
2024

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Pasto, mayo 2024

DEDICATORIA

Con amor dedico este trabajo en primer lugar a Dios, porque debemos agradecerle por las oportunidades y personas que pone en nuestro camino; en segundo lugar, a mi familia, quienes me inspiraron y supieron comprender que siempre hay un momento para compartir y que lo esperaron siempre con paciencia y me apoyaron en todo momento con un abrazo, un café, una mirada, una sonrisa, una llamada… Por eso éste logro es para mí madre Luisa Córdoba y para ustedes por supuesto: Lizzeth, Sara y Joaquín… Los amo.

Jesús

AGRADECIMIENTOS

Agradezco a las directivas de la Universidad Nacional Abierta y a Distancia UNAD, quienes con su trabajo continuo nos brindan la oportunidad de estudiar y laborar, por otro lado, a cada uno de los tutores y asesores que me acompañaron en el proceso, les reconozco que sin su apoyo y colaboración éste logro no hubiera sido posible. Tengo que valorar la calidad académica y el progreso de la Universidad, hace 12 años soy egresado y sin lugar a duda, se nota el cambio y ha sido para mejorar. Felicitaciones.

CONTENIDO

Pág.

1. INTRODUCCIÓN 19

2. DEFINICIÓN DEL PROBLEMA 20

2.1 ANTECEDENTES DEL PROBLEMA 20

2.2 FORMULACIÓN DEL PROBLEMA 22

3. JUSTIFICACIÓN 23

4. OBJETIVOS 25

4.1 OBJETIVO GENERAL 25

4.2 OBJETIVOS ESPECÍFICOS 25

5. MARCO REFERENCIAL 26

5.1 MARCO TEÓRICO. 26

5.1.1. Buenas Prácticas en Ciberseguridad Para Sector Salud en Colombia. 26

5.1.2. La Seguridad Informática en los Hospitales Públicos de Colombia. 39

5.1.3. Ruta para implementar la ciberseguridad en el sector salud. 42

5.2 MARCO CONCEPTUAL. 44

5.2.1. Definición de la Seguridad Informática y Ciberseguridad. 44

5.2.2. Identificación, evaluación y gestión del riesgo. 46

5.2.3. El comparativo entre los diferentes Planes de Seguridad. 47

5.2.4. Los Activos de Información. 49

5.3 MARCO CONTEXTUAL 50

5.3.1. Ciberseguridad y TICS en Hospitales Públicos de Colombia: 50

5.3.2. Retos en Ciberseguridad para sector salud. 51

5.4 ANTECEDENTES O ESTADO ACTUAL 54

5.4.1. Los Hospitales Como Infraestructura Critica. 55

5.4.2. La Ciberseguridad y la Telemedicina en Colombia. 57

5.4.3. Transformación Digital en Salud. 60

5.4.4. Enfoque en la seguridad de IoMT para el sector salud 64

5.4.5. Enfoque en amenazas específicas en el sector salud. 68

5.4.6. Colaboración Interdisciplinaria como una medida de protección. 73

5.4.7. Integración para la seguridad con las Tecnologías Emergentes. 76

5.5 MARCO LEGAL 78

5.5.1. Aspectos legales y normativos relacionados. 78

6. DISEÑO METODOLÓGICO 84

7. DESARROLLO DE LOS OBJETIVOS 85

7.1 IDENTIFICACIÓN DE AMENAZAS Y RIESGOS DE SEGURIDAD. 85

7.1.1 Identificación de activos de información. 85

7.1.2 Dependencia de activos de información. 92

7.1.3 Identificación de amenazas sobre los activos de información. 93

7.2 EVALUACION DE AMENAZAS SOBRE LOS ACTIVOS DE INFORMACION 103

7.2.1 Valoración de los activos de información. 103

7.2.2 Valoración de amenazas y nivel de riesgo frente a los activos de información. 109

7.3 MATRIZ DE SEGURIDAD DE LA INFORMACION 119

7.3.1 Identificación de controles. 120
7.3.2 Matriz de Riesgos. 122
7.4 PLAN DIRECTOR DE SEGURIDAD DIGITAL EN HOSPITALES PÚBLICOS DE COLOMBIA. 128
7.4.1 Conocer la situación actual de la organización (Fase 1). 129
7.4.2 Conocer la estrategia de la organización (Fase 2). 139
7.4.3 Definición de proyectos e iniciativas (Fase 3). 141
7.4.4 Clasificar y priorizar los proyectos a realizar (Fase 4). 144
7.4.5 Aprobar el Plan Director de Seguridad (Fase 5). 149
7.4.6 Puesta en marcha (Fase 6). 150
8. CONCLUSIONES 151
9. RECOMENDACIONES 152
10. BIBLIOGRAFÍA 153
11. ANEXOS 160

LISTA DE TABLAS

Pág.

Tabla 1 Amenazas a los Activos de Información: Esenciales 95
Tabla 2 Amenazas a los Activos de Información: Arquitectura del Sistema 96
Tabla 3 Amenazas a los Activos de Información: Datos / Información 97
Tabla 4 Amenazas a los Activos de Información: Claves Criptográficas 97
Tabla 5 Amenazas a los Activos de Información: Servicios 98
Tabla 6 Amenazas a los activos de información: Software/Aplicaciones Informáticas 98
Tabla 7 Amenazas a los activos de información: Equipos (Hardware) 99
Tabla 8 Amenazas a los activos de información: Redes de Comunicaciones 100
Tabla 9 Amenazas a los activos de información: Soportes de información 101
Tabla 10 Amenazas a los activos de información: Equipamiento Auxiliar 101
Tabla 11 Amenazas a los activos de información: Instalaciones 101
Tabla 12 Amenazas a los activos de información: Personal 102
Tabla 13 Criterios de valoración según la guía de seguridad TIC CCN STIC 803 107
Tabla 14 Criterios de Frecuencia y Degradación o Impacto. 109
Tabla 15 Escala y Valor del Riesgo 111
Tabla 16 Valoración de amenazas y riesgo asociado frente a los activos de información esenciales. 111
Tabla 17 Valor del riesgo asociado a los activos de información arquitectura del sistema 112
Tabla 18 Valor del riesgo asociado a los activos de información Datos 113
Tabla 19 Valor del riesgo asociado a los activos de información Claves Kriptográficas 114
Tabla 20 Valor del riesgo asociado a los activos de información Servicios 114
Tabla 21 Valor del riesgo asociado a los activos de información Software 115
Tabla 22 Valor del riesgo asociado a los activos de información Hardware 115
Tabla 23 Valor del riesgo asociado a los activos de información Comunicaciones 116
Tabla 24 Valor del riesgo asociado a los activos de información Soportes 117
Tabla 25 Valor del riesgo asociado a los activos de información Equipamiento Auxiliar 117
Tabla 26 Valor del riesgo asociado a los activos de información Instalaciones 117
Tabla 27 Valor del riesgo asociado a los activos de información Personal 118
Tabla 28 Controles propuestos para la muestra 120
Tabla 29 Muestra de activos de información 122
Tabla 30 Plan de tratamiento activos de información. 124
Tabla 31 Portafolio de proyectos para PDS 143

LISTA DE FIGURAS

Pág.

Ilustración 1 Fases OCTAVE 30
Ilustración 2 Pasos para análisis de riesgos MAGERIT 33
Ilustración 3 Proceso de análisis de riesgo NIST SP 800-30 36
Ilustración 4 Pasos para la Implementación de ciberseguridad 43
Ilustración 5. Histórico Afiliación y Cobertura al SGSSS en Colombia 55
Ilustración 6 Tipos de Incidente por Entidades Sector Salud 69
Ilustración 7 Tipos de amenazas en el sector salud entre 2021 y 2023 70
Ilustración 8 Activos de información más afectados en el sector salud 73
Ilustración 9 Dependencia de los Activos de Informacion 93
Ilustración 10 Criterio valoración cuantitativa de activos 104
Ilustración 11 Valoración del riesgo 127
Ilustración 12 Fases Plan director de Seguridad 128

LISTA DE CUADROS

Pág.

Cuadro 1 Sinopsis de ciberseguridad en el sector salud. 27
Cuadro 2 Versiones ISO 27005 29
Cuadro 3 Línea de tiempo OCTAVE 31
Cuadro 4 Activos de información: activos esenciales 86
Cuadro 5 Activos de información: arquitectura del sistema 86
Cuadro 6 Activos de información: datos / información 87
Cuadro 7 Activos de Información: Claves Criptográficas 87
Cuadro 8 Activos de información: Servicios 88
Cuadro 9 Activos de información: Aplicaciones Informáticas 88
Cuadro 10 Activos de información: Equipos informáticos (hardware) 89
Cuadro 11 Activos de información: redes de comunicaciones 89
Cuadro 12 Activos de información: soportes de información 90
Cuadro 13 Activos de información: equipamiento auxiliar 90
Cuadro 14 Activos de información: instalaciones 91
Cuadro 15 Activos de información: personal 91
Cuadro 16 Activos de información: valoración cuantitativa 104
Cuadro 17 Amenazas de más alto riesgo. 119
Cuadro 18Vulnerabilidades y amenazas relacionadas a los activos Software 131
Cuadro 19 Vulnerabilidades y amenazas relacionadas a los activos Hardware 132
Cuadro 20 Vulnerabilidades y amenazas relacionadas a los activos Servicios 133
Cuadro 21 Vulnerabilidades y amenazas relacionadas a los activos Soportes de Información 134
Cuadro 22 Vulnerabilidades y amenazas relacionadas a los activos Equipamiento Auxiliar 135
Cuadro 23 Vulnerabilidades y amenazas relacionadas a los activos Instalaciones y Personal 136
Cuadro 24 Vulnerabilidades y amenazas relacionadas a los activos Datos / Información 137
Cuadro 25 Vulnerabilidades y amenazas relacionadas a los activos Redes y Comunicaciones 138
Cuadro 26 Vulnerabilidades y amenazas relacionadas a los activos Base de Datos 139

LISTA DE ANEXOS

Pág.

Anexo A. Tabla para evaluación de madurez del Plan de Seguridad Conjunta (JSP). 160

GLOSARIO

ACTIVO DE INFORMACIÓN: Cualquier información o sistema relacionado con el tratamiento de esta, que tenga valor para la organización, pueden ser procesos de: negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones. Es susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización.

AMENAZA: Es una circunstancia desfavorable que puede provocar consecuencias negativas en los activos, como su indisponibilidad o pérdida de valor. Puede tener causas naturales, accidentales o intencionales y, si se produce en combinación con una vulnerabilidad en los sistemas, puede resultar en un incidente de seguridad.

CIBERATAQUE: Se refiere al intento intencional de un ciberdelincuente de acceder a un sistema informático sin autorización, utilizando diferentes técnicas y aprovechando vulnerabilidades para llevar a cabo actividades maliciosas, como robo de información, extorsión o daño al sistema.

CIBERDELINCUENTE: Persona que lleva a cabo actividades ilegales en la red, con el objetivo de causar daño a sistemas informáticos o personas, y obtener beneficios económicos de forma ilícita. Las acciones pueden incluir el robo o filtrado de información, daños al software o hardware, fraude y extorsión.

CIBERSEGURIDAD: Conjunto de prácticas y medidas destinadas a proteger los sistemas informáticos y las redes de amenazas, ataques y vulnerabilidades.

CONFIDENCIALIDAD: Propiedad de la información de ser accesible únicamente por personas autorizadas. Es una de las tres dimensiones fundamentales de la seguridad de la información, junto con la integridad y la disponibilidad. Se garantiza mediante el uso de controles de acceso y técnicas de encriptación, entre otros mecanismos de seguridad.

DISPONIBILIDAD: Capacidad de acceder a la información y a los sistemas de información necesarios en cualquier momento y lugar donde se requieran para el desarrollo normal de las actividades del negocio. Parte de las tres dimensiones fundamentales para la seguridad de la información.

DRP: (Disaster Recovery Plan) o Plan de Recuperación de Desastres, es un sistema con el cual las organizaciones se preparan contra posibles desastres de diversos índoles que puedan dañar su infraestructura tecnológica y por ende poner fin a sus actividades.

FRAMEWORK: (Marco de trabajo) es un conjunto estructurado de prácticas, políticas y procedimientos. Un framework de ciberseguridad establece una estructura de referencia para la gestión de la seguridad de la información, y puede incluir recomendaciones para la implementación de medidas de seguridad, la gestión de riesgos, la respuesta a incidentes y la evaluación de la seguridad.

GESTIÓN DEL RIESGO CIBERNÉTICO: Proceso de identificación, evaluación y mitigación de los riesgos asociados a la seguridad informática y la ciberseguridad.

GOBIERNO DIGITAL: Es la política del Gobierno Nacional que propende por la transformación digital pública. Con esta política pública se busca fortalecer la relación Ciudadano - Estado, mejorando la prestación de servicios por parte de las entidades, y generando confianza en las instituciones que conforman la administración pública y el Estado en general, a través del uso y aprovechamiento de las TIC.

IMPACTO: Medida del efecto que produce un incidente, desastre, problema o cambio en los niveles de servicio de una empresa y cómo se ven afectados en el caso de que se materialice dicha amenaza.

INFRAESTRUCTURA CRÍTICA: Activos físicos, tecnológicos, humanos o naturales cuya interrupción o destrucción tendría un impacto grave en la salud, la seguridad, la economía o el bienestar social de la población, así como en el funcionamiento normal de las instituciones del Estado o en el tejido productivo.

INTEGRIDAD: Una de las tres dimensiones clave en la seguridad de la información, junto con la disponibilidad y la confidencialidad. La integridad garantiza que la información no haya sido alterada de forma accidental o intencionada y que se mantiene exacta y completa en todo momento.

INTRUSIÓN: Acción ilegal y malintencionada que tiene como objetivo acceder a un sistema, red o dispositivo sin permiso para realizar actividades ilícitas, como el robo de información, la manipulación de datos o la instalación de software malicioso.

ISO 27002: Norma internacional que establece las pautas para la gestión de la seguridad de la información.

ISO 27005: Norma internacional que establece las pautas para la gestión de riesgos de seguridad de la información.

MAGERIT: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, un marco de trabajo desarrollado por el Gobierno de España para la gestión de riesgos de seguridad informática.

MALWARE: Software de carácter malicioso y su intención de causar daño o actuar de forma no autorizada en un sistema de información. Palabra que nace de la unión de los términos en inglés de software malintencionado: malicious software

NIST: Instituto Nacional de Estándares y Tecnología, una agencia gubernamental de Estados Unidos responsable del desarrollo de estándares y pautas para tecnologías de la información y la ciberseguridad.

NIST SP 800-30: Guía de gestión de riesgos de seguridad de la información desarrollada por el NIST.

OCTAVE: Operationally Critical Threat, Asset, and Vulnerability Evaluation, una metodología de evaluación de riesgos desarrollada por el CERT Coordination Center de la Universidad Carnegie Mellon.

PENTEST: Análisis activo de vulnerabilidades potenciales en un sistema software o hardware, incluyendo configuraciones deficientes o inadecuadas, y deficiencias en medidas de seguridad. El objetivo es determinar la viabilidad de un ataque y su posible impacto en el negocio. Tras el ataque se presenta una evaluación de seguridad del sistema con propuestas de mitigación o soluciones técnicas.

PLAN DIRECTOR DE SEGURIDAD DIGITAL: Documento que establece las políticas, procedimientos y medidas necesarias para garantizar la seguridad de los sistemas y datos informáticos de una organización.

POLÍTICA DE SEGURIDAD: Decisiones y medidas de seguridad que una empresa toma después de evaluar el valor de sus activos y los riesgos a los que están expuestos. También puede referirse al documento de nivel ejecutivo en el que se establecen las directrices de seguridad de la información de la empresa.

PSO: Plan de Seguridad del Operador. Documento fundamental para garantizar la continuidad de los servicios esenciales que prestan las organizaciones públicas o privadas, ya que establece una hoja de ruta para mitigar los riesgos y amenazas que puedan afectar su funcionamiento.

PPE: Plan de Protección Especifico. Documento de obligatorio cumplimiento en España; en el que se establecen las medidas concretas que deben ser implementadas para garantizar la seguridad física y lógica de las infraestructuras críticas.

RANSOMWARE : Malware cuya funcionalidad es “secuestrar” un dispositivo o su información, forma que, si la víctima no paga el rescate, ya no podrá acceder a ella.

REDUNDANCIA: Propiedad consistente en un determinado fichero o sistema para que en caso de caída de uno se pueda seguir proporcionando el servicio.

RESILIENCIA: Capacidad de una organización de resistir ante una situación adversa, como, por ejemplo, un incidente de ciberseguridad. La resiliencia empresarial debería ir acompañada de un plan de contingencia y continuidad para hacer frente a posibles situaciones de crisis en la empresa.

RIESGO: Es la posibilidad de que una amenaza o vulnerabilidad se convierta en un daño real para la empresa, que resulte en una pérdida o robo de información o en una detención de su actividad como consecuencia del daño ocasionado. El riesgo puede ser mitigado mediante políticas de seguridad y continuidad del negocio que suelen prever posibles ataques y proponen soluciones de actuación ante situaciones cuyo riesgo pueda ser elevado.

SECTOR SALUD: Conjunto de organizaciones y profesionales dedicados a la atención médica, la investigación y la salud pública.

SECURIZAR: Proceso de proteger los sistemas informáticos y redes contra posibles amenazas de seguridad, como ataques cibernéticos, intrusiones maliciosas, filtraciones de datos y otros riesgos relacionados con la seguridad de la información

SEGURIDAD INFORMÁTICA: (Seguridad Cibernética) Conjunto de medidas y prácticas destinadas a proteger los sistemas y datos informáticos de amenazas y riesgos de seguridad.

SGSI: Un SGSI es para una organización el diseño, implantación, mantenimiento de un conjunto de procesos 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.

VULNERABILIDAD: (Sinónimo Agujero de seguridad). Debilidad o fallo de un sistema que puede ser aprovechado con fines maliciosos (normalmente mediante un programa que se denomina exploit).

RESUMEN

Los hospitales públicos en Colombia deben reconocer la importancia de la seguridad de la información y la necesidad de contar con un Plan director de seguridad digital para proteger su información sensible y crítica. A pesar de las medidas de seguridad informática disponibles y las recomendaciones o buenas prácticas para implementar, las organizaciones que pertenecen al sector salud han sufrido un incremento en los ataques cibernéticos en los últimos 12 meses, lo que ha afectado la atención a los pacientes y la confiabilidad en las entidades afectadas a los ojos del usuario impactando directamente su reputación. Para abordar esta problemática, se propone a través de frameworks de trabajo de ciberseguridad, estándares y guías de buenas prácticas, establecer métodos para identificar las principales vulnerabilidades y amenazas que afectan al sector salud a nivel público, a fin de establecer políticas y procedimientos enfocados a la protección de la información de estas entidades. Además, se recomendarán medidas y técnicas avanzadas de seguridad, programas de concientización al personal sobre las mejores prácticas de seguridad informática. Las recomendaciones contenidas en el plan permitirán a estas organizaciones contar con estrategias sólidas y efectivas de seguridad cibernética que mitigan los riesgos y amenazas, establecen medidas de contingencia y fortalecen la seguridad de la información en cuanto a integridad, disponibilidad, confidencialidad, autenticidad y trazabilidad.

ABSTRACT

Public hospitals in Colombia must recognize the importance of information security and the need for a Digital Security Master Plan to protect their sensitive and critical information. Despite the available cybersecurity measures and recommendations or best practices for implementation, organizations within the healthcare sector have experienced an increase in cyber attacks over the past 12 months, impacting patient care and the trustworthiness of the affected entities in the eyes of users, directly affecting their reputation. To address this issue, it is proposed through cybersecurity work frameworks, standards, and best practice guides to establish methods for identifying the main vulnerabilities and threats affecting the public healthcare sector, in order to establish policies and procedures focused on protecting the information of these entities. Additionally, advanced security measures and techniques will be recommended, along with awareness programs for staff on best practices in cybersecurity. The recommendations contained in the plan will enable these organizations to have solid and effective cybersecurity strategies that mitigate risks and threats, establish contingency measures, and strengthen information security in terms of integrity, availability, confidentiality, authenticity, and traceability.

1. INTRODUCCIÓN

En la actualidad, la seguridad de la información es una prioridad para las organizaciones, especialmente para aquellas que manejan información sensible, como la correspondiente a la atención clínica de pacientes. Los hospitales públicos en Colombia, como entidades que forman parte de una infraestructura crítica necesitan fortalecer su seguridad informática y disminuir las vulnerabilidades y amenazas para garantizar la confiabilidad de la atención a los usuarios y la protección de la información tanto clínica como financiera.

A pesar de que se implementan medidas de seguridad informática, aún existen vulnerabilidades y amenazas que poner en riesgo la información y la infraestructura tecnológica de estas organizaciones, por lo que se hace necesario contar con un Plan Director de Seguridad Digital que incluya frameworks de trabajo de ciberseguridad para la gestión efectiva del riesgo cibernético.

En este proyecto de grado se plantea la formulación del problema: *¿Cómo fortalecer la seguridad de la información y disminuir las vulnerabilidades y amenazas de seguridad informática a través de un plan director de seguridad digital que incluya frameworks de trabajo de ciberseguridad para la gestión efectiva del riesgo cibernético para los hospitales públicos en Colombia?*

Para lograr este objetivo, se deben identificar las principales vulnerabilidades y amenazas, establecer políticas y procedimientos para la protección y manejo de la información sensible, recomendar técnicas avanzadas de seguridad para concientizar al personal sobre las mejores prácticas de seguridad informática. Todo ello, permitirá una gestión efectiva del riesgo cibernético y garantizará la seguridad de la información en cuanto a integridad, disponibilidad, confidencialidad, autenticidad y trazabilidad.

2. DEFINICIÓN DEL PROBLEMA

2.1 ANTECEDENTES DEL PROBLEMA

En la actualidad, la gestión efectiva de la seguridad de la información se ha convertido en una prioridad para las organizaciones, especialmente para aquellas que se catalogan como infraestructuras criticas o aquellas que manejan información sensible, como la correspondiente a la atención clínica de pacientes; este es el caso de los hospitales públicos en Colombia, que tiene a cargo la atención de mediana y alta complejidad de las poblaciones que atienden y cuya información clínica y financiera debe tener un manejo y custodia garantizada, según los lineamientos del gobierno nacional y las entidades de control.

A pesar de que se han implementado medidas de seguridad informática, aún existen vulnerabilidades y amenazas que pueden poner en riesgo la información y la infraestructura tecnológica de estas organizaciones, por cuanto en los últimos 12 meses se ha notado un incremento en ataques relacionados con el sector salud, afectando significativamente la atención a los usuarios y la confiabilidad de las organizaciones afectadas.[1]

Por lo tanto, el problema radica en cómo fortalecer la seguridad de la información y disminuir así, las vulnerabilidades y amenazas de seguridad informática en los hospitales públicos de Colombia. Para ello, se propone contar con un plan director de seguridad digital que contemple los frameworks de trabajo de ciberseguridad para la gestión efectiva del riesgo cibernético.

Es necesario identificar las principales vulnerabilidades y amenazas a las que se

[1] PORTAFOLIO. Ataques cibernéticos ponen en 'jaque' el sector de la salud. [en línea]. Bogotá: Portafolio. (11 de octubre de 2022). [Consultado: 24 de octubre de 2023]. Disponible en: https://www.portafolio.co/negocios/empresas/ataques-ciberneticos-ponen-en-jaque-el-sector-de-la-salud-572476

enfrentan estas organizaciones, así como establecer un conjunto de políticas y procedimientos para la protección y manejo de la información sensible. Además, se deben recomendar medidas y técnicas avanzadas de seguridad como: el cifrado de datos, la autenticación de doble factor, el control de acceso, copias de seguridad en la nube, plan de recuperación de desastres (DRP), la monitorización de eventos y la detección y respuesta a incidentes de seguridad, entre otras.

Para lograr una gestión efectiva del riesgo cibernético, es importante involucrar a todo el personal de estas entidades al plan director de seguridad digital y en la concientización sobre las mejores prácticas de seguridad informática. Asimismo, se debe contar con un equipo especializado en ciberseguridad que pueda monitorear y evaluar constantemente la efectividad del plan director de seguridad digital y realizar ajustes y mejoras al mismo, según sea necesario.

Finalmente, los informes de los entes de control y las oportunidades de mejora, resultado de las auditorías externas, coinciden en que un hospital público debe trabajar en la gestión integral del riesgo, precisando fortalecer la seguridad y privacidad en los sistemas de información, acatando la resolución 500 de marzo 10 de 2021[2] por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital, así como en el marco de la Política Gobierno Digital, según decreto 767 de Mayo 16 de 2022.[3]

[2] MINTIC. “Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital” [en línea]. Bogotá: MINTIC. (10 de marzo de 2021). [Consultado: 24 de octubre de 2023]. Disponible en: https://gobiernodigital.mintic.gov.co/692/articles-162625_recurso_2.pdf

[3] FUNCION PÚBLICA. “Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital” [en línea]. Bogotá: FUNCION PÚBLICA. (16 de mayo de 2022). [Consultado: 24 de octubre de 2023]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=186766

2.2 FORMULACIÓN DEL PROBLEMA

¿Cómo fortalecer la seguridad de la información y disminuir las vulnerabilidades y amenazas de seguridad informática a través de un plan director de seguridad digital que contemple frameworks de trabajo de ciberseguridad para la gestión efectiva del riesgo cibernético para los hospitales públicos en Colombia?

3. JUSTIFICACIÓN

La seguridad de la información es una de las principales preocupaciones en la actualidad para las organizaciones, en particular para aquellas que manejan información sensible y crítica, como es el caso de las instituciones de salud. Los hospitales públicos de Colombia no son la excepción, ya que manejan información clínica de los pacientes, información clave de la operación y servicios, y otros datos sensibles que requieren protección contra posibles vulnerabilidades, amenazas y riesgos que afecten la integridad, disponibilidad y confidencialidad de la información.

Por lo tanto, se hace necesario contar con un Plan director de seguridad digital que involucre un conjunto de medidas que permitan la gestión integral del riesgo, contribuir a fortalecer la seguridad de la información y prever acciones para contrarrestar ataques cibernéticos. Las recomendaciones contenidas en este plan permitirán a las organizaciones tener una estrategia de seguridad cibernética sólida y efectiva, que les permita mitigar los riesgos y amenazas a los que están expuestos.

Con lo anterior uno de los resultados esperados será la matriz para la gestión del riesgo de seguridad de la información, que permitirá a las organizaciones establecer controles necesarios y tomar las medidas de contingencia en caso de que se materialicen las amenazas, con el fin de salvaguardar la información clave de la operación y garantizar la continuidad del servicio. Esto asegurará que las instituciones tengan un plan de acción claro y efectivo en caso de un posible ataque cibernético o cualquier otro incidente que afecte la seguridad de la información.

El objetivo del proyecto es lograr una gestión integral del riesgo a través del diseño de un plan director de seguridad digital que fortalezca la seguridad de la información en términos de integridad, disponibilidad, confidencialidad, autenticidad y trazabilidad. Esto implica identificar los activos de información críticos, evaluar los riesgos, aplicar medidas de seguridad adecuadas y diseñar, supervisar y mejorar

continuamente el plan de seguridad de la información; lo anterior conforme las mejores prácticas extraídas de metodologías, framework de trabajo, guías, controles y estándares internacionales reconocidos como NIST SP 1800-30/24/8/1 – SP 800-171/53, ENISA, SANS CIS, HITRUST CSF, HIPAA, ISO-IEC 27005/27002/27799, MAGERIT, OWASP y OCTAVE, entre las más reconocidas.

4. OBJETIVOS

4.1 OBJETIVO GENERAL

Recomendar medidas de seguridad basadas en frameworks para fortalecer la gestión del riesgo cibernético para los hospitales públicos de Colombia a través de la construcción de un plan director de seguridad digital con el fin de mitigar las vulnerabilidades y amenazas que afecten la seguridad de la información.

4.2 OBJETIVOS ESPECÍFICOS

Identificar amenazas y riesgos en los sistemas y aplicaciones de los hospitales públicos de Colombia, mediante metodologías reconocidas priorizando los más críticos en un plan de seguridad digital.

Evaluar las amenazas identificadas en una matriz de seguridad de la información estableciendo controles y procedimientos de seguridad cibernética basados en estándares internacionales y recomendaciones de marcos reconocidos.

Proponer un Plan Director de Seguridad Digital que incluya capacitación en ciberseguridad para el personal de hospitales públicos en Colombia, fortaleciendo la implementación de controles y procedimientos de seguridad.

5. MARCO REFERENCIAL

5.1 MARCO TEÓRICO.

5.1.1. Buenas Prácticas en Ciberseguridad Para Sector Salud en Colombia. La seguridad de la información en el sector salud es crucial para proteger los datos sensibles de pacientes y personal médico y administrativo. Por lo tanto, implementar buenas prácticas de ciberseguridad en los hospitales públicos de Colombia es esencial para mitigar el riesgo cibernético a nivel nacional.

Para lograrlo, se propone contar con un plan director de seguridad digital basado en metodologías, frameworks, estándares, controles y guías de trabajo de ciberseguridad y privacidad. Al aplicar herramientas teóricas que permitan identificar y analizar los riesgos asociados al sector salud, se podrán adoptar medidas efectivas para diseñar políticas y estrategias que fortalezcan la gestión del riesgo y reduzcan las vulnerabilidades y amenazas.

A continuación, en el cuadro No. 1 (Sinopsis de ciberseguridad en el sector salud), se presentan algunas de las herramientas más apropiadas para implementar un plan director de seguridad digital efectivo, lo que garantizará la protección de los datos de los pacientes y del personal médico y administrativo. La intención es profundizar en cada marco de acuerdo con la necesidad o campo de aplicación en el que se quiere trabajar.

Cuadro 1 Sinopsis de ciberseguridad en el sector salud.

NOMBRE	DESCRIPCION
COBIT 5 - 2019 (GENERAL)	Marco de trabajo que tiene como objetivo asegurar una efectiva gobernanza de información y tecnologías.
ENISA - CYBER SECURITY AND RESILIENCE FOR SMART HOSPITALS (SALUD)	Investiga y hace recomendaciones sobre los "smart hospitals" y sus problemas relacionados. Define los activos y clasifica sus amenazas, planteando escenarios de ataques en donde se analizan los efectos, la recuperación y las buenas prácticas.
ENISA THREAT LANDSCAPE: HEALTH SECTOR (SALUD)	Análisis realizado por la Agencia de la Unión Europea para la Ciberseguridad (ENISA) sobre el panorama de ciber amenazas del sector sanitario en la UE
ENISA - ICT SECURITY CERTIFICATION OPPORTUNITIES IN THE HEALTHCARE SECTOR (SALUD)	Investiga las directrices y regulaciones en la tecnología de la información en la salud y IoMT.
ENISA - PROCUREMENT GUIDELINES FOR CYBERSECURITY IN HOSPITALS (SALUD)	Guía para mejorar el ciclo de compra y apoyar en el cumplimiento de los objetivos de ciberseguridad en hospitales.
ENISA - SECURITY AND RESILIENCE IN EHEALTH INFRASTRUCTURES AND SERVICES (SALUD)	Muestra el estado del arte e investiga el enfoque y los medios utilizados para proteger los sistemas de salud críticos en cada uno de los países miembros.
HIPAA (SALUD)	Este marco regulatorio establece requisitos de seguridad para la información de Salud Protegida (PHI), que incluye medidas técnicas y administrativas para proteger la información contra accesos no autorizados, alteraciones o destrucción.
HITRUST CSF (SALUD)	Marco de seguridad que proporciona una estructura para evaluar, medir y mejorar la seguridad y privacidad de la información de salud y otros datos sensibles para ayudar a las organizaciones de atención médica y sus proveedores.
ISO 27005:2022 (GLOBAL)	Norma que se centra en el proceso de gestión de riesgos y proporciona un marco para identificar, evaluar y tratar los riesgos de seguridad de la información en una organización.
ISO/IEC 27001:2022 (GLOBAL)	Norma que establece los requisitos para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) y proporciona una guía para la evaluación y tratamiento de riesgos de seguridad de la información.
ISO/IEC 27002:2022 (GLOBAL)	Proporciona una guía con buenas prácticas para mejorar el sistema de gestión de seguridad de la información de una organización a través de las categorías principales de seguridad (35) y controles específicos (114). Esta norma es una referencia para la selección e implementación de controles de seguridad de la información basados en las mejores prácticas reconocidas internacionalmente.
ISO/IEC 27799:2016 (SALUD)	Esta norma se enfoca en la gestión de la seguridad de la información en el sector de la salud y proporciona orientación sobre cómo proteger la confidencialidad, integridad y disponibilidad de los datos personales de salud
MAGERIT V3 (GLOBAL)	Metodología de trabajo para la identificación, análisis y gestión de riesgos de los sistemas de información, con un enfoque particular en la seguridad de la información y la protección de datos personales.
NIST SP 1800-1 (SALUD)	Guía para protección de registros médicos en dispositivos móviles. Muestra cómo utilizar herramientas y tecnologías disponibles comercialmente, o de código abierto, que son consistentes con los estándares de ciberseguridad, para ayudar a las organizaciones que usan dispositivos móviles a compartir registros médicos electrónicos de manera más segura.
NIST SP 1800-24 (SALUD)	Guía sobre cómo proteger el ecosistema de imagenología, centrándose en los sistemas de comunicación y archivo de imágenes (PACS) en las organizaciones de prestación de servicios de salud (HDO).
NIST SP 1800-30 (SALUD)	Guía práctica para una solución de telemedicina y monitoreo remoto de los pacientes (RPM).
NIST SP 1800-8 (SALUD)	Guía detallada sobre cómo administrar activos, protegerse contra amenazas y mitigar vulnerabilidades en bombas de infusión inalámbricas. Se utiliza un enfoque de evaluación de riesgos, contempla los estándares de ciberseguridad actualmente disponibles y la ley HIPAA. Se basa en principios como defensa en profundidad. Si bien inicialmente parece estar enfocada a bombas de infusión inalámbricas, los conceptos vertidos son útiles para todo IoMT.
NIST CSF (GLOBAL)	Marco que brinda medidas y controles a las organizaciones que suministran servicios críticos en Estados Unidos con el fin de identificar, evaluar y gestionar los riesgos de ciberseguridad.
OCTAVE (GENERAL)	Esta metodología se centra en la evaluación de los riesgos críticos de seguridad y en la implementación de controles adecuados para mitigar dichos riesgos en organizaciones y empresas
OWASP ASVS – MASVS (GENERAL)	Marco o estándar que establece los requisitos de seguridad y mejores prácticas para el desarrollo de aplicaciones Weby Móviles seguras.
CIS Controls (GENERAL)	Conjunto de mejores prácticas de seguridad cibernética que ayudan a las organizaciones a fortalecer su postura de seguridad general.

Fuente: El Autor.(2023)

El análisis de la documentación permite identificar, evaluar y gestionar eficazmente los riesgos de seguridad de la información en un hospital público de Colombia. Este

proceso contribuye a reducir las vulnerabilidades y amenazas informáticas a las que se enfrentan las instituciones de salud hoy en día. Así, se fortalecerá la ciberseguridad y la privacidad, permitiendo recomendar medidas preventivas y correctivas para proteger la información crítica y sensible en el sector de la salud. Los marcos teóricos, metodologías, guías, controles y estándares internacionales son referencias importantes en este campo, algunos específicos para el sector de la salud y otros de aplicación más general.

A continuación, se analizarán algunos de los aspectos más destacados de los estándares y marcos mencionados anteriormente.

- ISO 27005:2022.

  Esta norma es un estándar internacional que proporciona una guía para la gestión de riesgos de seguridad de la información. Establece un marco de trabajo para la identificación, evaluación, tratamiento y monitorización de riesgos de seguridad de la información en una organización. Está diseñada para ser utilizada por cualquier organización, independientemente de su tamaño, sector o ubicación geográfica. La norma proporciona una guía práctica para la gestión de riesgos de seguridad de la información que es fácil de entender y aplicar.

  Se basa en un enfoque de gestión de riesgos que se centra en la identificación de los activos de información críticos, la evaluación de los riesgos asociados con ellos, la selección y aplicación de medidas de seguridad adecuadas, y el monitoreo continuo de los riesgos de seguridad de la información.

  La implementación de la norma ISO 27005 puede ayudar a las organizaciones a identificar y mitigar los riesgos de seguridad de la

información, mejorar la eficiencia y eficacia de sus medidas de seguridad de la información, y proteger sus activos de información críticos.

La norma ISO 27005 ha tenido tres versiones, en cada versión se han realizado mejoras y actualizaciones para reflejar los cambios en las tecnologías y las amenazas de seguridad de la información.

Cuadro 2 Versiones ISO 27005

VERSIÓN	AÑO	DESCRIPCIÓN
ISO/IEC 27005:2008	**2008**	**Primera edición de la norma ISO 27005 que establece los requisitos y directrices para la gestión de riesgos de seguridad de la información en una organización.**
ISO/IEC 27005:2011	**2011**	**Edición revisada de la norma ISO 27005 que incluye una mayor orientación para la identificación y evaluación de riesgos de seguridad de la información.**
ISO/IEC 27005:2018	**2018**	**Edición actualizada de la norma ISO 27005 que proporciona una guía actualizada y ampliada para la gestión de riesgos de seguridad de la información en una organización. Se han realizado mejoras en la estructura y contenido de la norma para una mayor claridad y facilidad de uso.**

Fuente. El Autor. (2023).

Esta norma puede ayudar a identificar y mitigar los riesgos de seguridad de la información, mejorar la eficiencia y eficacia de las medidas de seguridad, y proteger la confidencialidad y privacidad de los pacientes de un hospital público. Sin embargo, es importante tener en cuenta que su implementación puede requerir una inversión significativa de tiempo y recursos, por lo que es necesario tener el aval de la alta dirección, así como evaluar cuidadosamente los costos y beneficios antes de proceder.

- OCTAVE.

  Por otro lado, está una metodología desarrollada en el 2001 en Estados Unidos por parte de la Universidad Cernegie Mellon en su Instituto de Ingeniería de Software, llamada OCTAVE (Operational Critical Threat, Asset,

and Vulnerability Evaluation) que traduce “Evaluación operacional de amenazas críticas, activos y vulnerabilidades”. Esta metodología se enfoca en la identificación y evaluación de riesgos en organizaciones y se centra en la protección de los activos críticos de las mismas.

La metodología OCTAVE se compone de tres fases:

Fase 1: Planificación y preparación: En esta fase se define el alcance del análisis de riesgos y se identifican los recursos necesarios para llevarlo a cabo.

Fase 2: Evaluación: En esta fase se identifican los activos críticos de la organización y se realizan evaluaciones de amenazas, vulnerabilidades y riesgos.

Fase 3: Implementación: En esta fase se desarrollan planes de mitigación y se implementan medidas de control para reducir los riesgos identificados.

Ilustración 1 Fases OCTAVE

Fuente: Huerta, Antonio. “Introducción al análisis de riesgos - Metodologías (II)” [imagen]. Security Art Work. 2012. [Consultado: 24 de octubre de 2023]. Disponible en: https://seguridades7a.blogspot.com/p/octave.html.

OCTAVE utiliza un enfoque basado en la gestión de riesgos que se centra en la identificación de los riesgos más críticos para la organización y en la implementación de medidas de control efectivas para reducirlos.

Según Alberts & Dorofee (2002), indica que OCTAVE es una metodología que se basa en los riesgos de la confidencialidad, integridad y disponibilidad a los que pueden estar sometidos los bienes con información crítica.[4] De este modo tenemos que OCTAVE es adaptable y puede ser implementada en organizaciones de diferentes tamaños y sectores. La siguiente tabla presenta la madurez de esta metodología, donde se observan las versiones desde su inicio.

Cuadro 3 Línea de tiempo OCTAVE

VERSIÓN	AÑO DE PUBLICACIÓN	ENFOQUE	CARACTERÍSTICAS PRINCIPALES
OCTAVE Framework, Criteria.	1999	PYMES	Enfoque en identificar y evaluar riesgos de seguridad de la información en pequeñas y medianas empresas.
OCTAVE-S V0.9	2001	General	Enfoque en identificar y evaluar riesgos de seguridad de la información en cualquier tipo de organización. Introduce el concepto de "perfil de amenazas" para analizar las amenazas específicas para cada organización.
OCTAVE Allegro v1.0	2003	General	Versión simplificada de OCTAVE-S enfocada en organizaciones con recursos limitados.
OCTAVE-CAPEC	2006	General	Incorpora la metodología de CAPEC (Common Attack Pattern Enumeration and Classification) para analizar patrones de ataque y mejorar la identificación de amenazas.
OCTAVE-IRM	2008	General	Se enfoca en la gestión integral de riesgos de seguridad de la información, incluyendo la identificación de riesgos, evaluación, tratamiento y seguimiento. Incorpora un enfoque de ciclo de vida para la gestión de riesgos.
OCTAVE-ALIRT	2010	General	Combina OCTAVE con la metodología ALIRT (Asset-Based Lightweight Risk Assessment) para identificar y evaluar riesgos de manera más eficiente y efectiva.
OCTAVE FORTE	2012	General	Enfoque en la evaluación de riesgos en sistemas de información críticos, como infraestructuras críticas o sistemas militares.
OCTAVE VULNERABILITY ASSESSMENT	2017	General	Enfoque en la identificación y evaluación de vulnerabilidades en sistemas de información. Incorpora un enfoque de pruebas de penetración y evaluación de vulnerabilidades para complementar la evaluación de riesgos.

Fuente. El Autor. (2023)

[4] Alberts, C. y Dorofee, A. (2002). Gestión de riesgos de seguridad de la información: el enfoque OCTAVE. Boston, Estados Unidos: Addison-Wesley.

Teniendo presente el cuadro anterior, de las opciones disponibles está la metodología OCTAVE-S, la cual es una versión simplificada y diseñada para organizaciones pequeñas, mientras que OCTAVE-ALLEGRO se centra solo en los activos de la organización. En contexto de un hospital público en Colombia, OCTAVE sería una opción válida para identificar y mitigar los riesgos de seguridad relacionados con los activos críticos y la información confidencial de los pacientes. La metodología OCTAVE requiere la participación de personal de varios departamentos, incluyendo operativo, tecnología, entre otros, y un especialista en seguridad para desarrollar estrategias y planes de seguridad basados en los riesgos identificados, lo que la hace una opción con un poco más de dificultad en su aplicación.

- MAGERIT v3.

  Es una metodología española de análisis de riesgos ampliamente utilizada en el ámbito de la seguridad de la información y la gestión de riesgos. Su enfoque es identificar, evaluar y tratar los riesgos asociados a la información y los sistemas de información en una organización.

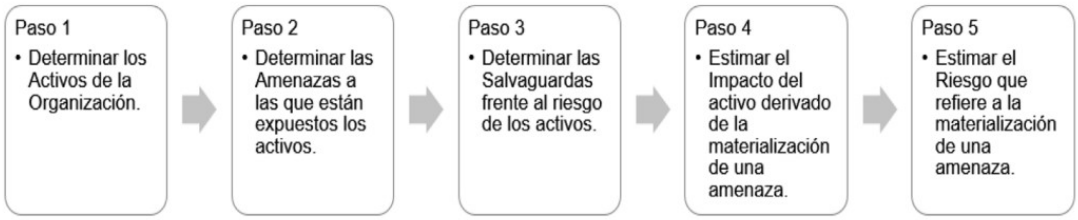
  Según Amaya C. (2013), MAGERIT está alineada con los estándares ISO lo que sirve como punto de partida para una certificación o la mejora de los sistemas de gestión.[5] Esta metodología se compone de tres fases principales: la identificación de activos, la evaluación de riesgos y la gestión de riesgos.

[5] Amaya, Camilo. “MAGERIT: metodología práctica para gestionar riesgos” [en línea]. {Consultado Marzo 2023}. Disponible en: https://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/

En la primera fase, se identifican los activos relevantes y se definen sus características, para luego evaluar las amenazas a las que están expuestos. En la segunda fase, se evalúan los riesgos asociados a los activos, considerando tanto la probabilidad de que se materialice la amenaza como el impacto que tendría en la organización en caso de ocurrir. Finalmente, en la tercera fase, se desarrollan medidas de gestión de riesgos para mitigar o eliminar los riesgos identificados.

MAGERIT se presenta como una metodología muy completa y detallada para la gestión de riesgos en la seguridad de la información y ha sido adoptada tanto por organizaciones públicas como privadas en España y en otros países. La siguiente grafica expone el método de análisis de riesgos que se manera en esta metodología, comprendido en 5 pasos:

Ilustración 2 Pasos para análisis de riesgos MAGERIT



Fuente: Fresia Holguín – Lohana Lema. Modelo para Medir la Madurez del Análisis de Riesgo de los Activos de Información en el contexto de las Empresas Naiveras [imagen]. Ecuador: risti; 2019. p. 6. [Consultado: 24 de octubre de 2023]. Disponible en: https://pdfs.semanticscholar.org/e0f8/cf42af8483db9a94996326d630888404d72d.pdf

MAGERIT persigue los siguientes objetivos directos:

- *"Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos*
- *Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC)*

- *Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control Indirectos*
- *Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso"*

Y de acuerdo con las políticas de uso y derecho de autor, establece que "*MAGERIT es una metodología de carácter público, puede ser utilizada libremente y no requiere autorización previa. En cualquier explotación de la obra se hará constar la autoría original."*[6]

Esta metodología es adaptable a diferentes contextos y sectores, incluyendo el sector de la salud y los hospitales públicos. A pesar de que su publicación y última versión data del 2012, es una metodología practica y efectiva para identificar los activos críticos de información, evaluar los riesgos asociados con ellos y desarrollar un plan de tratamiento de riesgos para garantizar que la información se proteja adecuadamente. Esto implica la evaluación de la seguridad de todos los activos de información que se utilizan en un hospital y que contribuyen directa o indirectamente a su misión. Esto incluye, por ejemplo, el proceso de gestión de la información y la gestión documental de la organización, el Sistema de Información Hospitalario (HIS), las ayudas diagnósticas (como los equipos y sistemas de imagenología, laboratorios, patología, etc.), la gestión de tecnología (que abarca equipos biomédicos, informáticos, de telecomunicaciones, y sistemas de información para la gestión de mantenimiento), los servicios farmacéuticos (como la central de gases medicinales y la central de mezclas), y cualquier otro activo que se identifique.

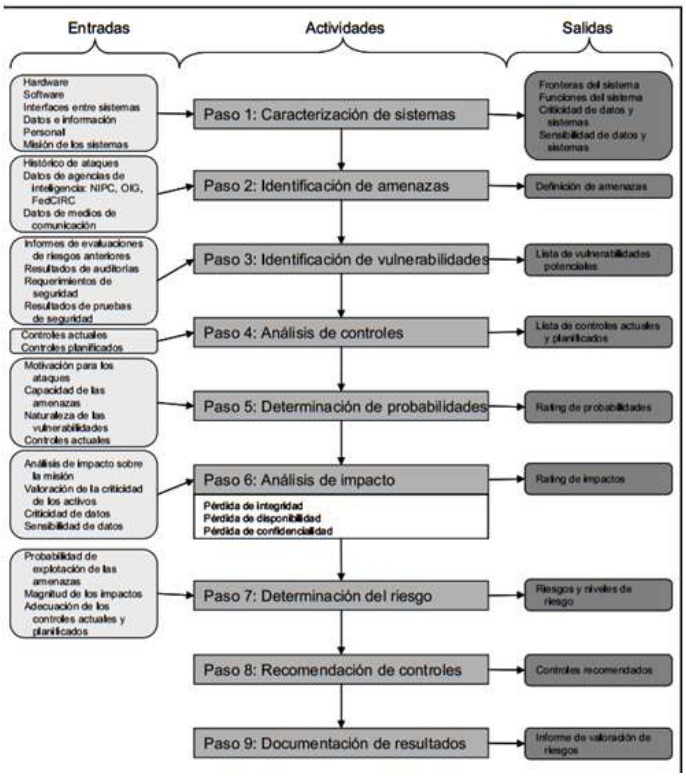
[6] Administración Electrónica. "MAGERIT: Metodología para la gestión de riesgos de seguridad de la información" [en línea]. [Consultado: 24 de octubre de 2023]. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

- NIST SP 800-30.

  Es un marco de gestión de riesgos de ciberseguridad desarrollado por el Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos, la versión original del estándar NIST 800-30 fue publicada en el año 2002 y desde entonces ha sido actualizada en varias ocasiones, su versión más reciente, NIST SP 800-30 Rev. 2 publicada en 2020, se centra en un enfoque más ágil y flexible de gestión de riesgos, con una mayor atención a la evaluación continua de los riesgos de seguridad informática en un entorno en constante evolución, además incluye nuevas secciones sobre la evaluación del riesgo de ciberseguridad y la evaluación del riesgo de privacidad. Su objetivo es evaluar y gestionar riesgos de seguridad en sistemas y organizaciones, lo que se trabaja a través de una metodología sistemática para identificar, analizar y evaluar los riesgos de seguridad en sistemas y redes, así como para seleccionar y aplicar controles adecuados para mitigar esos riesgos.

  La metodología consta de 9 pasos y pueden ser aplicados a sistemas individuales o interrelacionados.

Ilustración 3 Proceso de análisis de riesgo NIST SP 800-30



Fuente: Juan Candelario . Metodologías de Evaluación de Riesgos Informáticos. [en línea]. 2014. [Consultado: 24 de octubre de 2023]. [imagen] Disponible en: https://metodologiasevaluacionrinformaticos.blogspot.com/2014/03/

NIST SP800-30 proporciona un enfoque estructurado y sistemático para identificar y evaluar las amenazas y vulnerabilidades en el entorno hospitalario, esto permite una evaluación más completa y precisa de los riesgos, además, al establecer un ranking de las probabilidades de materialización de las amenazas, se pueden priorizar los controles necesarios para mitigar los riesgos identificados y trabajar un plan de implementación de controles. Por otro lado, NIST SP 800-30 puede requerir una inversión significativa de tiempo y recursos para llevar a cabo la evaluación de riesgos de seguridad de la información, porque no está diseñada específicamente para el sector de la salud, por lo que se pueden requerir adaptaciones para su aplicación efectiva, lo que demandara más tiempo en dar resultados.

- ISO 27799:2016

  La norma ISO 27799:2016 se enfoca en las necesidades específicas de gestión de seguridad de la información del sector salud y sus entornos operativos únicos, garantizando con especial atención la confidencialidad, integridad y disponibilidad de la información personal de salud, protegiendo la privacidad de los pacientes y asegurando la rendición de cuentas y la auditabilidad de los accesos.[7]

  En los hospitales se deben tomar medidas especiales para mantener la confidencialidad y la integridad de los datos, así como garantizar un alto nivel de disponibilidad de la información para evitar interrumpir servicios y directamente poner en peligro la vida de los pacientes.

  Este estándar ayuda a prevenir errores en la práctica médica y garantizar la continuidad de los servicios médicos, también cumple con las obligaciones legislativas en la protección de datos y mantiene las mejores prácticas de privacidad y seguridad en la informática de la salud, con un enfoque en la responsabilidad individual y organizacional. Además, busca reducir costos, mantener la confianza pública y cumplir con los estándares éticos y profesionales establecidos por organizaciones relacionadas con la salud, y facilitar la interoperabilidad entre sistemas de salud.

  La gobernanza de la información es esencial para las organizaciones de salud, ya que los sistemas de información son cada vez más importantes para apoyar la atención médica. La materialización de una amenaza puede tener un impacto clínico significativo, lo que resulta en fallas éticas y legales en el deber de cuidado, en ese sentido, los marcos de gobernanza clínica

7 ISO. (2016). ISO 27799:2016. Health Informatics: Information security management in health. [en línea] Disponible en https://www.iso.org/standard/62777.html. Consultado Noviembre 11 de 2023.

deben abordar la gestión efectiva de riesgos de seguridad de la información. Esta norma ayuda a los responsables de la gobernanza clínica, como son las juntas directivas, alta dirección o cargos con poder de decisión, a comprender la importancia de la seguridad de la información.

Dentro del alcance de la norma están las pautas para los estándares organizativos de seguridad de la información y las prácticas de gestión de seguridad de la información en el ámbito de la salud informática. Esta norma proporciona directrices para apoyar la interpretación e implementación de los controles de la norma ISO/IEC 27002 en el ámbito de la salud informática y los complementa, para que puedan ser efectivamente utilizados para la gestión de la seguridad de la información en la salud, por lo cual la familiarización entre estas dos normas es muy importante para su correcta adopción y facilitar su comprensión, ya que el documento hace referencia a cláusulas importantes de ese estándar.

Al implementar esta norma, las clínicas, hospitales y otros custodios de información de salud podrán garantizar un nivel mínimo de requisitos de seguridad adecuado a sus circunstancias organizativas, y mantendrán la confidencialidad, integridad y disponibilidad de la información personal de salud bajo su responsabilidad. La norma se aplica a la información de salud en todos sus aspectos, independientemente de la forma en que se recopile, el medio utilizado para almacenarla y el medio utilizado para transmitirla.

Esta Norma Internacional se dirige a aquellos responsables de supervisar la seguridad de la información en el cuidado de la salud y a las organizaciones encargadas de manejar información de salud, también se incluyen a los asesores de seguridad, consultores, auditores, proveedores y terceros proveedores de servicios.

Como resultado de la implementación de esta norma internacional, las organizaciones de atención médica pueden esperar ver reducido el número y la gravedad de sus incidentes de seguridad, lo que permite que los recursos se redistribuyan a actividades productivas.

5.1.2. La Seguridad Informática en los Hospitales Públicos de Colombia.

La seguridad de la información en el ámbito de la salud puede estar expuesta a una amplia variedad de amenazas y vulnerabilidades. Aunque algunos de estos riesgos son comunes a otros sectores, la atención médica presenta una serie de factores únicos que deben ser considerados al evaluar la seguridad. Por ejemplo, las organizaciones de salud operan en un entorno en el que es difícil excluir completamente a visitantes y al público en general, lo que aumenta la vulnerabilidad de los sistemas a amenazas físicas. Además, en las organizaciones de salud, es fundamental identificar correctamente a los pacientes y proteger su información personal de identificación, ya que los registros de pacientes pueden ser los repositorios más completos y con muchos datos confidenciales.

Un claro ejemplo sobre el tema de confidencialidad de la información médica lo podemos ver con la Health Insurance Portability and Accountability Act (HIPAA), que rige en Estados Unidos desde 1996, cuyo objetivo es precisamente proteger la privacidad y confidencialidad de la información de los pacientes y establece estándares para la protección de la información de salud; así como garantizar la confidencialidad, disponibilidad e integridad de toda la información médica electrónica, detectar y proteger contra amenazas a la seguridad de la información. Todo acceso a los registros médicos debe contar con el aval y la firma autorizando el uso para fines médicos, además, dicha información solo se puede compartir con

otros fines con la autorización expresa del paciente o su apoderado. Las violaciones a HIPAA acarrean sanciones civiles, monetarias o penales.[8]

Es importante tener en cuenta que muchas organizaciones de salud tienen limitaciones financieras y su personal a menudo trabaja bajo estrés, con las actividades del día a día y con sistemas antiguos, esto es más enfático en el sector público, donde la rotación de personal es alta, lo que impacta directamente la cobertura en las capacitaciones, además, las directivas no son muy amigables a la renovación tecnológica por los costos en inversión, lo que hace que no se preste la atención necesaria a temas como la actualización tanto en conocimientos al personal de TI, así como en recursos de tecnológica y mucho menos lo que tiene que ver con seguridad informática. Estos factores pueden aumentar el potencial de algunas amenazas y vulnerabilidades. Sin embargo, se rescata que los profesionales de la salud también tienen un alto nivel de formación, lo que les permite reducir la incidencia de amenazas personales, con una adecuada capacitación y concientización.

En este mismo sentido, encontramos el HITRUST CSF, que se trata de un marco de seguridad integral y certificable, diseñado para adaptarse a una amplia gama de organizaciones, incluyendo las del sector de la salud. La versión 11.2 de 2023 del CSF se alinea con estándares internacionales como ISO/IEC 27001 y 27002, y sintetiza más de 40 regulaciones y marcos de trabajo que abordan la seguridad y la privacidad de la información.[9]

Entre las ventajas que se obtienen en la implementación del marco HITRUST CSF, se encuentran:

---

[8] Sabatino, C. (2023). Confidencialidad e HIPAA. En Manual MSD versión para profesionales. [on line] Disponible en https://www.msdmanuals.com/es-co/professional/temas-especiales/cuestiones-medicolegales/confidencialidad-e-hipaa Consultado el 21 de marzo 2024.

[9] HITRUST Health Information Trust Alliance. (2023). HITRUST Cybersecurity Framework. [en linea] disponible en https://hitrustalliance.net/hitrust-framework . Consultado el 22 de marzo de 2024.

- Integración de Regulaciones y Estándares: HITRUST CSF unifica múltiples regulaciones y estándares reconocidos en un solo marco, simplificando el cumplimiento normativo como HIPAA, HITECH, ISO/IEC 27001 y PCI-DSS.

- Cumplimiento Robusto de Seguridad y Privacidad: asegura una mejor protección de los datos sensibles de los pacientes al cumplir con requisitos rigurosos de seguridad y privacidad.

- Enfoque Basado en Riesgos: permite a las organizaciones personalizar sus controles de seguridad y privacidad según sus necesidades específicas, adoptando un enfoque adaptado a los riesgos.

- Certificación de Cumplimiento: ofrece una certificación que valida el cumplimiento, agregando una capa adicional de confianza para las organizaciones certificadas por HITRUST, lo que fortalece la confianza entre proveedores, socios comerciales y pacientes.

- Mejora de la Seguridad: ayuda a cumplir con la gestión de riesgos y el cumplimiento regulatorio al proteger los datos sensibles y regulados contra ciberataques.

- Reconocimiento en la Industria: la certificación HITRUST es reconocida en la industria, demostrando un compromiso firme con la seguridad y la privacidad.

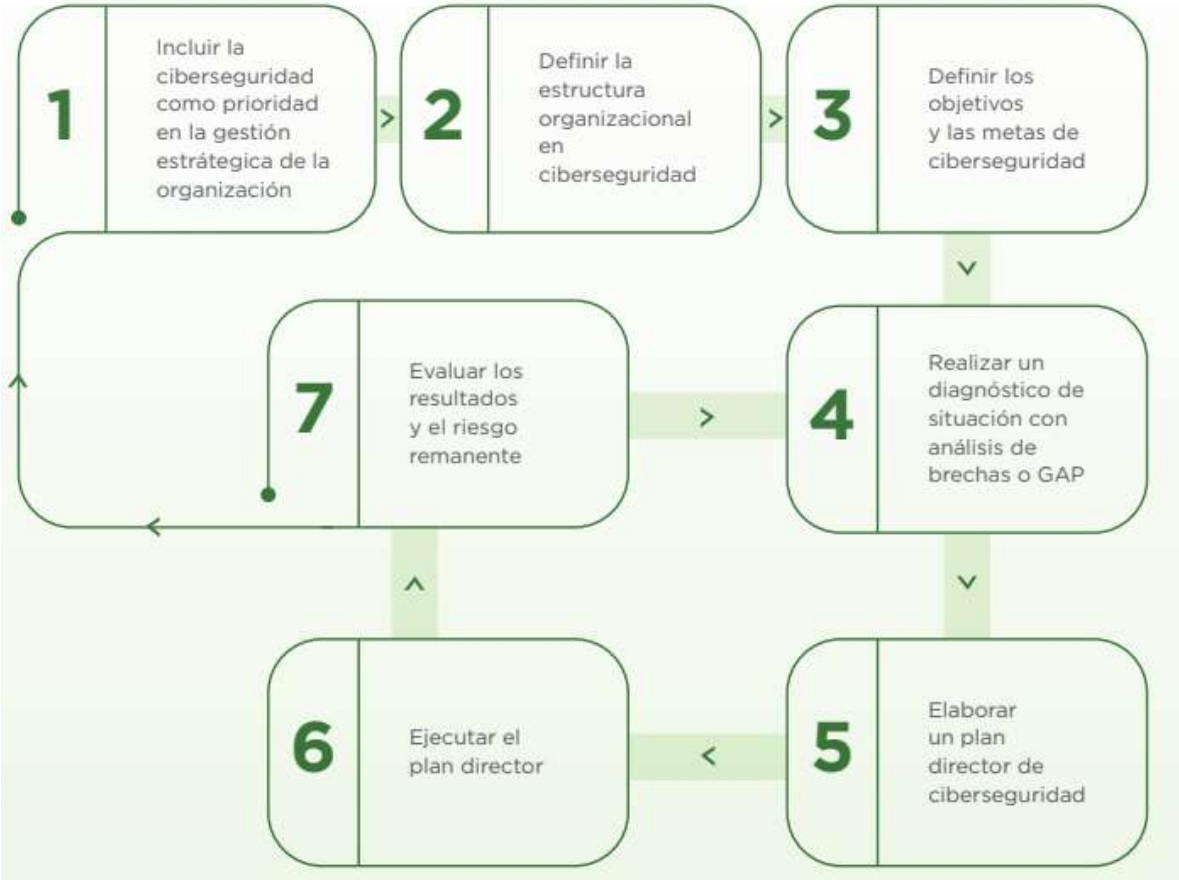
En Colombia, donde la protección de datos en el sector de la salud es necesaria, el reconocer y aplicar marcos como el HITRUST CSF es muy importante. Esto no solo mejora la seguridad y la gestión de riesgos, sino que también posiciona a las entidades de salud para una colaboración más segura y eficiente a nivel nacional e internacional, lo cual es vital en un mundo cada vez más interconectado y digitalizado.

Con esto se resalta que el entorno de la atención médica tiene riesgos únicos y particulares, que deben ser evaluados cuidadosamente al considerar la seguridad de la información. El nivel de protección necesario para la confidencialidad, integridad y disponibilidad depende de la naturaleza de la información, los usos para los que se emplea y los riesgos a los que se expone. Por ejemplo, los datos estadísticos pueden no requerir confidencialidad, pero sí es importante proteger su integridad. De igual manera, los datos de auditoría de seguimiento pueden no requerir alta disponibilidad, pero su contenido podría ser altamente confidencial. La evaluación del riesgo puede determinar adecuadamente el nivel de esfuerzo necesario para proteger la confidencialidad, integridad y disponibilidad de la información de un hospital o clínica, dependiendo de su contexto y factores como la gobernanza y gobierno TI.

5.1.3. Ruta para implementar la ciberseguridad en el sector salud.

En el contexto de los hospitales públicos en Colombia, es crucial establecer una cultura de ciberseguridad para proteger los datos de los pacientes y garantizar la integridad de la información. Para ello, es importante seguir los 7 pasos para la implementación de la ciberseguridad, como lo muestra ilustración 4 de este documento.

Ilustración 4 Pasos para la Implementación de ciberseguridad



Fuente: Alzuri, P., Cabral Berenfus, F., Paz, S., Nowersztern, A. y Libedinsky, P. (2021). Protegiendo la salud digital - Una guía de ciberseguridad en el sector de salud [PDF]. Recuperado de https://publications.iadb.org/publications/spanish/document/protegiendo-la-salud-digital-una-guia-de-ciberseguridad-en-el-sector-de-salud.pdf Consultado octubre 29 de 2023.

En primer lugar, la alta dirección debe incluir la ciberseguridad como una prioridad en su plan estratégico, para garantizar que se le dé la importancia que merece. Luego, se debe definir la estructura organizacional en ciberseguridad, designando roles y responsabilidades claras para garantizar la implementación adecuada de medidas de seguridad.

Posteriormente, se deben definir los objetivos y metas de ciberseguridad, en función de las necesidades y requisitos específicos del hospital. Es fundamental realizar un diagnóstico de situación con análisis de brechas o también conocido como análisis

GAP (donde estamos y donde queremos llegar), lo que implica comparar controles, políticas, procedimientos o practicas existentes para identificar las vulnerabilidades y deficiencias en la seguridad de la información. A partir de los resultados del diagnóstico, se debe elaborar un plan director de ciberseguridad, con objetivos y estrategias claras para mejorar la seguridad de la información y mitigar los riesgos identificados. La implementación del plan director es el siguiente paso y debe realizarse de manera rigurosa y estructurada para garantizar su efectividad.

Finalmente, se debe evaluar los resultados y el riesgo remanente, monitoreando continuamente la efectividad de las medidas implementadas y actualizando el plan director según sea necesario. De esta manera, se puede garantizar una cultura de ciberseguridad sólida y eficiente para proteger los datos y la privacidad de los pacientes, del personal médico y del ejercicio en general.

5.2 MARCO CONCEPTUAL.

5.2.1. Definición de la Seguridad Informática y Ciberseguridad.

Tanto la ciberseguridad como la seguridad informática son términos que se utilizan comúnmente para referirse a la protección de los sistemas informáticos y de la información que estos manejan. Sin embargo, es importante destacar que mientras la ciberseguridad se enfoca en la protección en el ámbito de lo digital contra ataques maliciosos llevados a cabo por cibercriminales; la seguridad informática se encarga de la gestión integral de los riesgos relacionados con el uso y procesamiento de información en los sistemas informáticos.

CISCO define la ciberseguridad como *la práctica de proteger sistemas, redes y programas de ataques digitales*.[10] En otras palabras, la ciberseguridad se centra en la defensa de los sistemas y la información contra los ataques cibernéticos.
Por otro lado, IBM indica que la seguridad informática *se caracteriza por la protección de datos y de comunicaciones, asegurando los tres principios básicos: la integridad de los datos, la disponibilidad del sistema y la confidencialidad.*[11] Explicado de otra manera, se enfoca en la gestión de los riesgos inherentes al uso de los sistemas informáticos, incluyendo la identificación, evaluación y mitigación de dichos riesgos.

Ambas disciplinas son importantes para garantizar la protección de la información y de los sistemas informáticos, y deben ser implementadas de manera integrada y coordinada para lograr una gestión eficaz de los riesgos y amenazas cibernéticas. Para lograr una estrategia de seguridad informática efectiva, se debe tener en cuenta la integración de marcos de referencia y los pilares fundamentales de la seguridad informática, que son la confidencialidad, la integridad y la disponibilidad.

La confidencialidad asegura que la información sea accesible solo para aquellos que tengan la autorización correspondiente, y se logra mediante el uso de sistemas de cifrado. La integridad garantiza que la información sea precisa, completa y confiable, y es importante contar con sistemas que permitan detectar y prevenir cualquier intento de alteración de la información. La disponibilidad implica la capacidad de acceder a la información en el momento que se necesite, lo que requiere que los canales de intercomunicación y los dispositivos tecnológicos estén en óptimas condiciones.

---

[10] Cisco. (s.f.). ¿Qué es la ciberseguridad?. [en línea] [Consultado: 22 Noviembre 2023]. Disponible en https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html
[11] IBM. (s.f.). Seguridad informática. [en línea] [Consultado: 22 Noviembre 2023]. Disponible en https://www.ibm.com/mx-es/topics/it-security

La integración de los modelos, marcos, guías y estándares de gestión de riesgos de seguridad de la información, con los tres pilares de la seguridad informática permite una mayor protección y seguridad de la información. Esto se logra mediante el análisis y la evaluación de los riesgos de seguridad de la información en cada uno de estos pilares, y la implementación de controles y medidas de seguridad para prevenir y mitigar estos riesgos, lo que permite una gestión integral de la seguridad de la información en cualquier organización.

5.2.2. Identificación, evaluación y gestión del riesgo.

El tratamiento de riesgos de seguridad de la información es un proceso fundamental para garantizar la protección de los activos de información de una organización. En esta línea, el estándar ISO 27001 enmarca el paso a paso del proceso general que permite identificar los riesgos y establecer los controles adecuados para mitigarlos y reducir el impacto en caso de que se materialicen. Esta evaluación es fundamental para el diseño e implementación de medidas efectivas de seguridad de la información y se compone de 4 etapas o fases, tales como:

- La primera fase de la evaluación de riesgos es la identificación de todos los activos de información relevantes para la organización, como datos, sistemas, equipos, instalaciones y personal. También se deben identificar las vulnerabilidades asociadas a cada activo, es decir, las debilidades o puntos débiles que podrían ser explotados por una amenaza para acceder, modificar o destruir información crítica.

- La segunda fase es la identificación de las amenazas, donde están las posibles fuentes de riesgo, tanto internas como externas, que podrían explotar las vulnerabilidades encontradas en la fase anterior, esto puede incluir ataques cibernéticos, robos, errores humanos, desastres naturales, entre muchas otras.

- La tercera fase implica la evaluación de la probabilidad de ocurrencia y el impacto de cada amenaza. La probabilidad se refiere a la posibilidad de que una amenaza se materialice, mientras que el impacto se refiere a las consecuencias que tendría esa amenaza en caso de que se produjera.

- Finalmente, en la cuarta fase se determinan los controles adecuados para tratar el riesgo, esto puede incluir medidas técnicas como la encriptación, la segmentación de redes o la implementación de sistemas de detección de intrusiones, así como medidas organizativas como políticas de seguridad, capacitación de empleados y protocolos de respuesta a incidentes, entre otras.

5.2.3. El comparativo entre los diferentes Planes de Seguridad.

Aquí se presenta un análisis comparativo de los planes de seguridad más reconocidos y con posibilidad de adaptación a diferentes entornos. Cada uno de estos planes convergen en la finalidad y objetivos, aunque difieren un poco en el alcance, por lo que resulta interesante compararlos para entenderlos mejor y comprender su importancia en el ámbito de la ciberseguridad.

5.2.3.1. Plan Director de Seguridad Digital.

Tiene como objetivo establecer políticas, procedimientos y medidas necesarias para garantizar la seguridad de los sistemas y datos informáticos de una organización. Este plan busca proteger la confidencialidad, integridad y disponibilidad de la información, así como también garantizar la continuidad de los servicios que dependen de dicha información. El Plan director de seguridad digital es un documento que debe ser elaborado por los responsables de la seguridad de la información en una organización y debe ser actualizado regularmente para mantenerse vigente frente a las nuevas amenazas y riesgos que puedan surgir.

5.2.3.2. Plan de Seguridad del Operador (PSO).

Se trata de un documento fundamental para garantizar la continuidad de los servicios esenciales que prestan las organizaciones públicas o privadas. Este plan establece una hoja de ruta para mitigar los riesgos y amenazas que puedan afectar el funcionamiento de la organización. El PSO debe incluir una evaluación de los riesgos y amenazas a los que está expuesta la organización, así como también un plan de contingencia y respuesta ante incidentes. Además, el PSO debe ser actualizado regularmente y contar con la aprobación de los responsables de la organización.

5.2.3.3. Plan de Protección Específico (PPE).

Se puede resumir como un documento de obligatorio cumplimiento en España, en el que se establecen las medidas concretas que deben ser implementadas para garantizar la seguridad física y lógica de las infraestructuras críticas. El objetivo principal del PPE es proteger a la sociedad de las posibles consecuencias negativas que pueden derivarse de la interrupción de los servicios esenciales. El PPE debe incluir una evaluación de los riesgos y amenazas que pueden afectar las infraestructuras críticas, así como también un plan de contingencia y respuesta ante incidentes. Además, el PPE debe ser actualizado regularmente y contar con la aprobación de las autoridades competentes.

5.2.3.4. Plan de Continuidad del Negocio (BCP).

La planificación de la continuidad del negocio (Business Continuity Plan o BCP) establece procesos y procedimientos de gestión de riesgos que tienen como objetivo evitar interrupciones en los servicios de misión crítica y restablecer la función completa de la organización de la forma más rápida y sencilla posible. El BCP debe incluir una evaluación de los riesgos y amenazas a los que está expuesta la organización, así como también un plan de contingencia y respuesta ante incidentes. Además, el BCP como los demás debe ser actualizado regularmente y contar con la aprobación de los responsables de la organización.

5.2.3.5. Plan de Recuperación de Desastres (DRP).

Es un documento fundamental para cualquier organización que dependa de la tecnología y de los sistemas informáticos para llevar a cabo sus operaciones diarias. El objetivo principal del DRP es establecer los procedimientos necesarios para garantizar la continuidad del negocio en caso de que se produzca un desastre natural o un incidente no planificado que afecte el funcionamiento normal de la organización y amerite activar una contingencia. En este sentido, el DRP debe contemplar todas las medidas necesarias para recuperar la operatividad del sistema informático de la organización de forma rápida y efectiva. Entre las medidas que se pueden incluir en un DRP se encuentran la realización de copias de seguridad periódicas, la definición de roles y responsabilidades en caso de emergencia, la implementación de medidas de seguridad física y lógica para proteger la infraestructura y los datos, la definición de un protocolo de comunicación para mantener informados a los empleados y clientes de la situación, entre otras.

Estos planes citados anteriormente son los más reconocidos, sin embargo no son los únicos. Cada país según su legislación y nivel normativo tendrá un plan similar con el objetivo de ejecutar en caso de incidentes de seguridad, destacando que cada uno de ellos coincide en la necesidad de estar en actualización permanente para asegurar la efectividad ante nuevos riesgos o amenazas que puedan surgir.

5.2.4. Los Activos de Información.

Es importante destacar que los activos de información de una organización pueden ser muy diversos y variados, por ejemplo, encontramos activos identificados como procesos de negocio, otros como personal, y de igual manera equipos informáticos o instalaciones físicas. Cada uno de estos activos puede contener información sensible o crítica para el funcionamiento de la organización, por lo que deben ser protegidos adecuadamente, además, es importante recalcar que los riesgos de seguridad pueden ser tanto internos como externos, es decir, pueden provenir de

amenazas externas como hackers o ciberdelincuentes, pero también de errores o negligencias internas de los propios empleados o colaboradores de la institución.

Actualmente a nivel de Colombia el MINTIC establece una guía para la gestión e identificación de los activos de información disponible en su página web oficial, por otro lado, metodologías como MAGERIT v3 en su libro 2 también presenta la clasificación de los activos de información de acuerdo con la Integridad, confidencialidad y disponibilidad; este último fue el método que se acoge en esta investigación.

Es fundamental considerar todos los activos de información que estén directa o indirectamente relacionados con el sistema de información. La correcta identificación de estos activos es la materia prima para establecer controles efectivos y mitigar el riesgo de forma significativa.

5.3 MARCO CONTEXTUAL.

5.3.1. Ciberseguridad y TICS en Hospitales Públicos de Colombia:

La ciberseguridad en el sector de la salud es un tema de creciente importancia. La transformación digital ha revolucionado numerosos sectores, incluido el de la salud. La digitalización y la tecnología ofrece eficiencia y precisión en los tratamientos y diagnósticos, pero también ha abierto la puerta a un nuevo conjunto de riesgos, entre ellos los ciberataques.[12]

Los sistemas actuales muestran una falta de robustez en sus protocolos de

[12] El Economista. (2023). El estado de la ciberseguridad en el sector de la salud. Consultado el 26 de octubre de 2023, [On line] Disponible en www.eleconomista.es/opinion/noticias/12499014/10/23/el-estado-de-la-ciberseguridad-en-el-sector-de-la-salud.html

seguridad. Muchos establecimientos todavía utilizan sistemas operativos obsoletos y carecen de políticas de seguridad informática actualizadas. Además, el personal médico y administrativo a menudo carece de formación en buenas prácticas de ciberseguridad, lo que incrementa la posibilidad de brechas por error humano.
En cuanto a Colombia específicamente, es importante mencionar que muchos servicios del sector público son susceptibles a amenazas cibernéticas, y los hospitales públicos no son una excepción.[13]

Es necesario que los hospitales públicos inviertan en ciberseguridad y tomen medidas para proteger sus sistemas y datos. Esto incluye la formación del personal en ciberseguridad, la actualización de políticas, reconocimiento de las normativas de gobierno dadas para trabajar en pro de un gobierno digital seguro, establecer mecanismos que permitan evaluar y fortalecer la infraestructura existente, adoptar marcos dados para aplicar las mejores prácticas con el objetivo de mitigar riesgos y blindar estas instituciones.

5.3.2. Retos en Ciberseguridad para sector salud.

La ciberseguridad en las instituciones de salud pública en Colombia es un tema de gran importancia, especialmente en el contexto de los recientes ciberataques, como el de Ransomware del que en 2023 fue víctima la multinacional IFX Network, proveedor de servicios de entidades del orden nacional del sector salud en Colombia.[14] Este ataque afectó a varias instituciones del Estado, incluyendo el Ministerio de Salud, la Superintendencia de Salud, entre otras, cuyas plataformas fueron afectadas por no disponibilidad del servicio, dejando afectaciones a procesos misionales como Mipres (prescripciones en línea de medicamentos NoPBS),

---

[13] Ciberseguridad.com. (2022). Guías: Sector público. [en línea]. Disponible en https://ciberseguridad.com/guias/sector-publico/ Consultado el 16 de octubre de 2023
[14] CNN en Español. (2023). Colombia: ciberataque a IFX Networks. [en línea]. Disponible en https://cnnespanol.cnn.com/2023/09/14/colombia-ciberataque-ifx-networks-orix/ . Consultado el 16 de octubre 2023.

RETHUS (Registro único Nacional de talento humano en Salud) RUAF (Registro en línea de nacimientos y defunciones en el país), SISPRO (Reportes de informes para entes de control y registros de personal médico asistencial), BDUA (Consulta de derechos de afiliados al sistema de salud), ADRES (Administradora de recursos del sistema general de seguridad social en salud).[15]

Estos son solo algunos ejemplos de las más de 700 organizaciones cuyos sistemas se afectaron, lo que resultó en retrasos en los servicios y procesos de las Instituciones Prestadoras de Salud (IPS) y las Entidades Promotoras de Salud (EPS) a nivel nacional e Internacional. Teniendo presente el anterior incidente, es importante considerar los retos en ciberseguridad para el sector salud, entre los que se pueden destacar los siguientes:

- Exposición y vulnerabilidad de sistemas y dispositivos conectados (IoMT): Es un llamado de atención a la creciente cantidad de dispositivos IoT interconectados en redes de salud, combinada con la dificultad de mantenerlos actualizados, controles de acceso débiles, la diversidad de las redes y la dependencia de sistemas heredados no preparados para ciberataques aumenta la vulnerabilidad de estos dispositivos a ser comprometidos en ataques cibernéticos. El reto en este aspecto es trabajar de la mano con los desarrolladores, con los representantes de las marcas y los fabricantes, para que de primera mano brinden pautas para tener en cuenta en el control de este tipo de equipos y capacitación directamente al usuario final.

- Necesidad de implementar buenas prácticas y un protocolo de recuperación de desastres (DRP): Cada entidad en el sector de la salud debe establecer

[15] CONSULTORSALUD SAS. (2023). Sector salud afectado en ciberataque a entidades del Estado. Recuperado el [octubre 2023], de https://consultorsalud.com/ciberataques-entidades-del-estado/

medidas de protección preventiva y proporcionar a su personal las herramientas necesarias para reaccionar de manera rápida y efectiva ante posibles ciberataques.

- Preservación de aspectos fundamentales de la seguridad de la información: La confidencialidad, integridad, disponibilidad, autenticidad y privacidad de los datos son aspectos cruciales que deben ser salvaguardados en el entorno de la salud.

- Generar confianza y seguridad en los servicios para pacientes y ciudadanos: Dado que se manejan datos altamente sensibles en el sector de la salud, es esencial generar confianza y seguridad en los pacientes y ciudadanos que utilizan los servicios de atención médica.

- Falta de formación específica: La falta de profesionales con conocimientos especializados en tecnologías de la información en el contexto de la salud representa un desafío significativo que requiere atención. Además, la rotación constante de personal en las entidades públicas plantea un riesgo notable, ya que puede dar lugar a la fuga de talentos y la exposición de información confidencial.

- Ausencia de la figura del CISO: La falta de un Chief Information Security Officer (CISO) o responsable de la seguridad de la información puede obstaculizar la implementación y seguimiento efectivo a las medidas de ciberseguridad en la institución.

- Es esencial que la Resolución 3100 de 2019 para la habilitación de prestación de servicios de las entidades de salud en Colombia, incluya requisitos específicos y más estrictos en materia de seguridad de la información. Estos

requisitos deben garantizar medidas mínimas de protección, como el uso de cifrado, acceso restringido a datos y evaluaciones de seguridad periódicas. Esto no solo asegura el cumplimiento normativo, sino que también protege la confidencialidad de los datos de los pacientes y mitiga riesgos cibernéticos en el sector de la salud, haciéndolos de obligatorio cumplimiento y vigilancia continua por parte de los entes de control.[16]

Estos retos son críticos para garantizar la seguridad de la información en el sector de la salud y requieren una atención constante y esfuerzos coordinados para abordarlos de manera efectiva.

5.4 ANTECEDENTES O ESTADO ACTUAL

Este apartado demuestra como la ciberseguridad en el sector de la salud, un área que ha evolucionado y requiere atención continua. Aunque existen marcos y literatura avanzados, principalmente en países desarrollados, la falta de inversión en ciberseguridad hace que el sector de la salud sea un objetivo atractivo para los ciberdelincuentes. Se enfatiza la necesidad de mejorar las defensas, minimizar el impacto de los ataques y eliminar las fuentes de ingresos de los criminales. Se discuten también las barreras institucionales para la seguridad de los dispositivos médicos, como la ambigüedad en la propiedad de la seguridad de los dispositivos. Finalmente, se subraya la necesidad de una infraestructura de ciberseguridad estratégica para combatir los ataques en todos los frentes, que incluya dispositivos médicos, sistemas de información, personal de TI preparado y la misma administración de las organizaciones.

[16] Resolución 3100 de 2019 Nueva Habilitación de Servicios de Salud y reps. MINSALUD. (2019, November 28). https://consultorsalud.com/resolucion-3100-de-2019-nueva-habilitacion-de-servicios-de-salud-y-reps/#TELEMEDICINA_INTERACTIVA

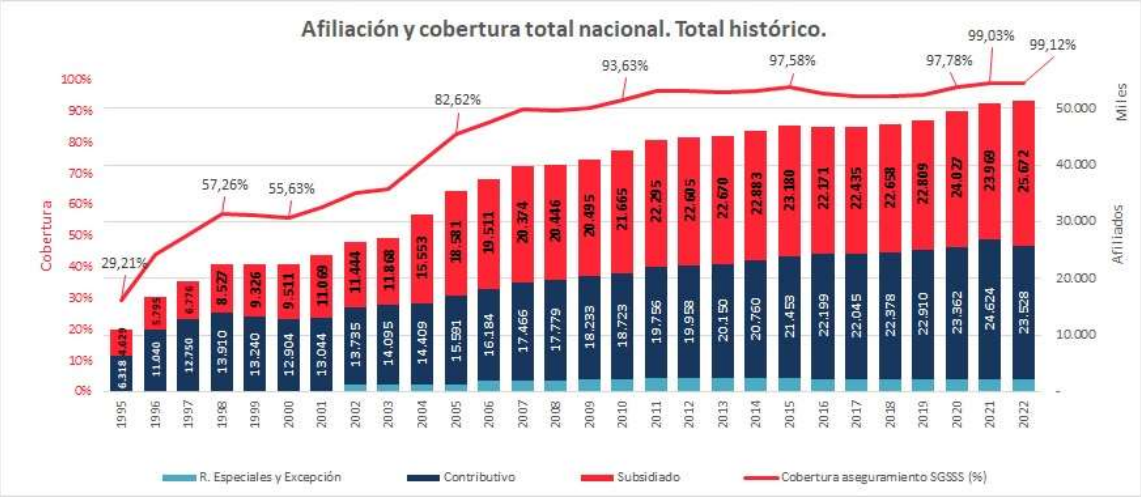
5.4.1. Los Hospitales Como Infraestructura Critica.

En Colombia, el sector salud ha experimentado un notable crecimiento en los últimos años en el nivel de cobertura y afiliación, como lo muestra la ilustración 5 (Histórico Afiliación y Cobertura al SGSSS en Colombia), esto según las estadísticas que entrega MinSalud y el DANE con corte al año 2022.

La cantidad de afiliados tanto al régimen subsidiado como al régimen contributivo y régimen especial cubren un alto porcentaje de la población total del país lo que es directamente proporcional a la información que se procesa.

Esta información abarca desde la afiliación de los usuarios hasta el registro de las atenciones médicas recibidas en las instituciones prestadoras de servicios de salud, así como los procesos administrativos y de facturación.

Ilustración 5. Histórico Afiliación y Cobertura al SGSSS en Colombia



Fuente: MINISTERIO DE SALUD Y PROTECCIÓN SOCIAL. Régimen subsidiado. Grafica de Barars. [en línea]. Disponible en https://www.minsalud.gov.co/proteccionsocial/Regimensubsidiado/Paginas/coberturas-del-regimen-subsidiado.aspx . Consultado: octubre 2023].

Dicha cobertura, se traduce en información y datos sensibles de ciudadanos, que se procesan día a día en los sistemas de información de estas entidades motivo por

el cual se contemplan en el marco denominado “infraestructuras críticas”, según la Directiva del Concejo de la Unión Europea 2008/114/CE, donde se define a la infraestructura critica como: “…*el elemento, sistema o parte de este situado de los Estados miembros, que es esencial para el mantenimiento de funcionares sociales vitales, la salud, la integridad física, la seguridad y el bienestar social y económico de la población y cuya perturbación o destrucción afectaría gravemente a un estado miembro…*” . Motivo por el cual las instituciones de salud deben estar catalogadas por su actividad misional y esencial como infraestructura crítica del sector salud, que prestan sus servicios 7/24 los 365 días del año, procesando información de poblaciones significativamente numerosas y garantizando un derecho fundamental, con lo que se quiere hacer comprender, que deben contar con unos sistemas de información robustos y seguros, lo que ha representado unos desafíos históricos, particularmente en términos de seguridad de la información y ciberseguridad, con dificultades particulares en el sector público.

El sector salud en Colombia se ha convertido en un objetivo importante para los ciberataques debido a la gran cantidad de información sensible que maneja, lo que incluye registros médicos, información financiera y personal del paciente. Para el año 2022 de las 34 empresas colombianas que reportaron afectación por ciberataques durante ese año, 7 pertenecen al sector salud[17]. La falta de medidas de seguridad adecuadas para mitigar los riesgos puede comprometer gravemente la privacidad y la seguridad de los pacientes, así como la integridad de los datos, riesgo financiero por la interrupción de los servicios médicos en hospitales y clínicas, afectando de manera directa la reputación de estas instituciones victimas de incidentes de este tipo.

El reconocimiento de los hospitales y organizaciones de salud como infraestructuras

[17]Infobae. (2023). Las 34 empresas que fueron hackeadas en Colombia durante 2022. Recuperado el 26 de octubre de 2023, de www.infobae.com/america/tecno/2023/01/02/las-34-empresas-que-fueron-hackeadas-en-colombia-durante-2022/

críticas en Colombia es el primer paso hacia una protección más efectiva. Sin embargo, este reconocimiento debe ir acompañado de leyes y regulaciones puntuales, como el proyecto de ley 245/19, que busca crear el Sistema Nacional de Protección de las Infraestructuras Criticas (SNINC), para exhortar a estas instituciones a tomar medidas proactivas para proteger sus sistemas y la información que contienen.

5.4.2. La Ciberseguridad y la Telemedicina en Colombia.

En el contexto de los hospitales públicos de Colombia, la Resolución 3100 del 25 de noviembre de 2019 establece las condiciones, estándares y criterios mínimos que deben cumplir todas las entidades de salud que ofrecen servicios en el país. Esta resolución también define los procedimientos y condiciones mínimas para la inscripción y habilitación de los proveedores de servicios de salud. Además, establece el proceso para la habilitación de servicios en la modalidad de Telemedicina. Como resultado, se han abierto oportunidades para que los sistemas de información de los hospitales públicos sean accesibles y utilizados por profesionales de la salud desde ubicaciones externas a la institución, con el objetivo de ampliar la cobertura del servicio.

Para habilitar este tipo de modalidades, es obligatorio garantizar la conectividad, por lo que es necesario realizar configuraciones específicas en cuanto a medios de acceso, alta disponibilidad en la conexión y considerar la seguridad perimetral. Estas medidas se implementan con el propósito de garantizar estabilidad y seguridad hacia los sistemas de historias clínicas, apoyo diagnostico y otras aplicaciones necesarias para la prestación de servicios de salud en la modalidad de telemedicina.

En el transcurso del año 2020, Colombia, al igual que el resto del mundo, se vio afectada por la pandemia de COVID-19. Esta situación de emergencia sanitaria

global puso a prueba la capacidad de respuesta de los sistemas de salud y acelero la adopción de nuevas modalidades de atención médica para garantizar la continuidad de los servicios de salud. En este contexto, la teleconsulta emergió como una solución viable y fue adoptada masivamente por los hospitales públicos del país.

Este cambio en la modalidad de atención no solo permitió mantener la prestación de servicios de salud en un momento crítico, sino que también resultó en un aumento significativo en el número de conexiones externas a los sistemas de información de los hospitales. Estas conexiones incluían a personal médico, administrativo, auditores médicos, entes de control y otros actores autorizados, quienes accedían de manera remota a los sistemas de información de los hospitales.

Sin embargo, este aumento en las conexiones remotas también representa un desafío en términos de seguridad de la información. El riesgo de posibles ataques informáticos se incrementó considerablemente, lo que pone de manifiesto la necesidad de implementar medidas de control de seguridad más robustas para proteger la integridad y confidencialidad de la información de los pacientes y garantizar la continuidad de los servicios de salud en el país.

En la actualidad, el acceso externo a los sistemas de información en los hospitales públicos de Colombia ya es una práctica común y ampliamente utilizada. Sin embargo, este aumento en la plataforma de conexiones y accesos remotos ha expandido la superficie de ataques, comprometiendo la seguridad de la información. En esta misma línea, la información es uno de los activos más valiosos en cualquier organización, y su importancia se magnifica cuando se trata de datos confidenciales o críticos.

Existen marcos de referencia específicos para la ciberseguridad en telemedicina,

como el NIST SP 1800-30. Este marco aborda la seguridad en el monitoreo remoto de pacientes, proporcionando un diseño de referencia basado en estándares y guías prácticas para implementar medidas de ciberseguridad y privacidad. Analiza los factores de riesgo del ecosistema de monitoreo remoto y destaca que las soluciones tecnológicas por sí solas pueden no ser suficientes. Enfatiza la importancia de combinar personas, procesos y tecnología para una estrategia de mitigación de riesgos holística. Al hacerlo, ayuda a las organizaciones a asegurar la confidencialidad, integridad y disponibilidad de las soluciones de monitoreo remoto de pacientes, mejorando la privacidad del paciente y limitando el riesgo para las organizaciones de atención médica al implementar dichas soluciones.[18]

En el sector de la salud, las Instituciones Prestadoras de Salud (IPS) y las Entidades Promotoras de Salud (EPS) manejan información extremadamente sensible, como las historias clínicas de los pacientes, lo que es esencial, motivo por el cual este sector forma parte de las infraestructuras críticas en países como los de la UE. Estas instituciones se han convertido en un objetivo muy atractivo para los ciberdelincuentes, quienes buscan apoderarse de esta información, cifrándola y denegando su acceso, para luego extorsionar a sus víctimas. Este tipo de ataque, conocido como Ransomware, es un malware muy común y que afecta a organizaciones en todo el mundo, Colombia no es la excepción.

Es necesario entender que la protección de estos datos no solo es una cuestión de privacidad, sino que también es una cuestión de seguridad nacional. Por lo tanto, es imperativo que el estado defina leyes y normas claras en este sentido y las organizaciones las implementen con medidas de seguridad robustas para protegerse contra estos ataques y garantizar la integridad y confidencialidad de la información de los pacientes.

---

[18] National Institute of Technical Standards (NIST), 2021: “SP1800-30. Securing Telehealth Remote Patient Monitoring Ecosystem (2nd Versión)”, disponible en https://csrc.nist.gov/publications/detail/sp/1800-30/draft consultado: 29 marzo 2024.

Este método extorsivo ha sido un problema creciente en los últimos años, como se ha documentado en diversos estudios y artículos a nivel internacional, como por ejemplo, un artículo de la revista latinoamericana Salud Digital destaca que "e*n una comparación realizada entre sectores como educación, atención médica, finanzas y servicios profesionales en general, el porcentaje de ataques dirigidos a entidades de atención médica representó el 41%, siendo el más alto entre los sectores* " (Salud Digital, 2019)[19].

Igualmente, un informe de Gery Coronel, director de Check Point Software para Chile, revela que 1 de cada 42 empresas del sector salud es objetivo de ataques con ransomware[20], lo anterior porque pueden ejercer una fuerte presión sobre estas entidades, por cuanto atentar contra la disponibilidad de la información clínica retrasa atenciones como cirugías, consultas, seguimientos, exámenes y demás atenciones que son el eje de una entidad prestadora de servicios de salud y un derecho fundamental de toda persona.

5.4.3. Transformación Digital en Salud.

El sector salud en Colombia está en un proceso de transformación digital que implica el uso de tecnologías de la información y la comunicación (TIC) para mejorar la calidad, la eficiencia y la accesibilidad de los servicios de salud. Entre los aspectos que se abordan en este proceso se encuentran:

- La interoperabilidad de la historia clínica electrónica, que permite el intercambio de información clínica entre los diferentes actores del sistema de

[19] Revista Salud Digital Latino América. HOSPITALES: Uno de los principales blancos de ciberataques. En: Salud Digital [en línea]. Bogotá: Salud Digital, 2019. [Consultado: octubre 2023]. Disponible en: https://www.revistasaluddigital.com/es/noticia/hospitales-uno-de-los-principales-blancos-de-ciberataques

[20] CHECK POINT RESEARCH. 1 de cada 42 organizaciones del sector salud es víctima de ransomware [en línea]. IT Sitio. (26 de octubre de 2022). [Consultado: octubre 2023]. Disponible en: https://www.itsitio.com/us/1-de-cada-42-organizaciones-del-sector-salud-es-victima-de-ransomware

salud, facilitando la continuidad de la atención, la prevención de errores y la toma de decisiones basada en la evidencia.

- La analítica de datos en salud, que consiste en el uso de técnicas estadísticas y de inteligencia artificial para extraer conocimiento a partir de los datos generados por el sistema de salud, con el fin de mejorar la gestión, la planificación, la investigación y la innovación en salud.

- La integración de los sistemas de información de las instituciones prestadoras de servicios de salud (IPS) a las plataformas de servicio de seguridad social del Ministerio de Salud y Protección Social, que busca optimizar los procesos administrativos, financieros y de control de calidad de los servicios de salud.

Estas iniciativas requieren de un alto nivel de ciberseguridad, que garantice la confidencialidad, la integridad y la disponibilidad de la información y los sistemas de salud, frente a posibles amenazas internas o externas. Además, la transformación digital en salud también implica el uso de tecnologías de apoyo al diagnóstico, como los equipos biomédicos, que se conectan a las redes y a los sistemas de información para transmitir y procesar datos. Estos equipos se convierten en activos de información con riesgos y amenazas asociados, que deben ser considerados y mitigados mediante medidas de seguridad adecuadas.

Según el Plan Conjunto de Seguridad de TI para Salud y Dispositivos Médicos[21], la ciberseguridad es una responsabilidad compartida entre los fabricantes, los proveedores y los usuarios finales de los dispositivos médicos y la tecnología de la información de salud. El Medical Device and Health IT Joint Security Plan fue creado como resultado de un grupo de trabajo establecido en respuesta a una

[21]HEALTH SECTOR COORDINATING COUNCIL. The joint security plan (JSP) [en línea]. Health Sector Council. (10 de junio de 2019). [Consultado: octubre 2023]. Disponible en: https://healthsectorcouncil.org/the-joint-security-plan

recomendación importante del informe del Health Care Industry Cybersecurity Task Force, publicado en junio de 2017. Este plan aborda la necesidad de una estrategia intersectorial para fortalecer la ciberseguridad en los dispositivos médicos y la tecnología de la salud. El plan fue elaborado por un grupo de trabajo compuesto por organizaciones de tecnología médica, tecnología de la salud y proveedores de servicios de salud, junto con la Administración de Alimentos y Medicamentos (FDA).

El plan establece que:

- Los fabricantes deben diseñar, desarrollar y gestionar la seguridad de sus productos, así como proporcionar documentación, divulgación y actualización de las vulnerabilidades y los parches de seguridad.

- Los proveedores deben hacer lo mismo con la tecnología de la información de salud que ofrecen a los usuarios finales.

- Los usuarios finales deben implementar medidas de seguridad para proteger los dispositivos médicos y la tecnología de la información de salud que utilizan.

Entre las recomendaciones que se dan en el plan para mejorar la ciberseguridad se encuentran:

- Establecer un programa de gestión de riesgos de seguridad cibernética para dispositivos médicos y tecnología de la información de salud.

- Implementar medidas de seguridad desde el diseño, desarrollo y manejo de quejas para dispositivos médicos y tecnología de la información de salud.

- Proporcionar documentación de seguridad del producto, divulgaciones de

vulnerabilidades y parches de seguridad.

- Realizar pruebas de penetración y evaluaciones de vulnerabilidades en dispositivos médicos y tecnología de la información de salud.
- Establecer un proceso de gestión de incidentes de seguridad cibernética para dispositivos médicos y tecnología de la información de salud.
- Proporcionar capacitación en seguridad cibernética para el personal que trabaja con dispositivos médicos y tecnología de la información de salud.
- Realizar evaluaciones de riesgos de seguridad cibernética para dispositivos médicos y tecnología de la información de salud.
- Establecer un proceso de gestión de parches de seguridad para dispositivos médicos y tecnología de la información de salud.
- Implementar medidas de seguridad para proteger los datos de pacientes y la privacidad de la información de salud.
- Incorporar prácticas de seguridad en el diseño y desarrollo de productos de tecnología médica.
- Gestionar quejas de productos relacionadas con incidentes y vulnerabilidades de ciberseguridad.
- Gestionar el riesgo de seguridad a lo largo del ciclo de vida de la tecnología médica.
- Evaluar la madurez de un programa de ciberseguridad de productos

En el marco de este proyecto, se ha incorporado un ejemplo detallado para evaluar la madurez del Plan de Seguridad Conjunta (JSP) que puede ser implementado en el contexto de los hospitales públicos de Colombia (véase anexo A). Este anexo propone una guía práctica y sistemática que sigue las recomendaciones y enfoques presentados en el documento citado, con el propósito de ayudar a las instituciones de salud a hacer un primer acercamiento y evaluación inicial, a fin de fortalecer su seguridad digital y proteger la información crítica de manera efectiva, en el contexto de los activos de información que en estas entidades existen, como es el caso de los equipos biomédicos con acceso a red, así como de las aplicaciones de software de desarrollo propio o tecnologías IoMT, entre otros.

5.4.4. Enfoque en la seguridad de IoMT para el sector salud.

El Internet de las Cosas (IoT) ha surgido como un actor principal en los últimos años, mostrando un crecimiento acelerado. Esta tecnología se ha implementado en una variedad de campos, desde el agrario y hotelero hasta el industrial, comercial, educativo y, por supuesto, el sector salud. Los datos generados por estos dispositivos constituyen la materia prima para Big Data, lo que permite la toma de decisiones, la mejora de procesos y, en el sector salud, la mejora de la calidad de vida de los pacientes.

Es importante considerar los dispositivos médicos conectados a internet (IoMT). La falta de capacitación y la configuración inadecuada de servicios por parte de casas comerciales, combinada con la masificación de la historia clínica digital, ha generado la necesidad de que los resultados, imágenes diagnósticas y exámenes viajen por la red y se incluyan en los registros médicos. Esto intensifica la interacción de estos dispositivos biomédicos con servidores y sistemas críticos de un hospital, aumentando la posibilidad de ataques. En muchas instituciones, estos dispositivos no se consideran activos de información y se segregan del inventario de seguridad, lo que puede crear posibles riesgos que afecten la seguridad de la información.

En el sector salud, el Internet de las Cosas Médicas (IoMT, por sus siglas en inglés) juega un papel crucial en la recopilación, transmisión y almacenamiento de datos de salud. Los equipos médicos de diagnóstico están conectados a internet, lo que permite transmitir la información del paciente sin intervención humana. Esto facilita el monitoreo remoto y un seguimiento efectivo de la salud, sirviendo como una herramienta valiosa para el personal médico. Sin embargo, esta tecnología no está exenta de riesgos de ciberdelincuencia, por lo que existen documentos y guías con recursos de ciberseguridad para dispositivos IoMT.

Por ejemplo, la Agencia Europea para la Ciberseguridad (ENISA) aborda varios aspectos relacionados con la IoMT en su documento “Oportunidades de Certificación de Seguridad en el Sector de la Salud” (ICT Security Certification Opportunities in the Healthcare Sector). Este documento evidencia una fragmentación del mercado y una baja interoperabilidad en los sistemas de información, lo que dificulta los posibles esquemas de certificación. Por lo tanto, propone las siguientes recomendaciones para mejorar la seguridad de las soluciones digitales en el ámbito de la atención médica:

- Implementar el concepto de seguridad por diseño y privacidad por diseño en el desarrollo de soluciones digitales de salud.
- Adoptar medidas operativas y técnicas para abordar los desafíos de seguridad en el sector de la salud.
- Cerrar las brechas en la estandarización y armonización de los sistemas de TIC en el sector de la salud para facilitar la interoperabilidad y el intercambio de datos médicos.
- Establecer requisitos de seguridad básicos para la Internet de las Cosas Médicas (IoMT) que cubran aspectos como la autenticación, autorización y otros controles de seguridad.

- Adaptar los marcos de prueba de interoperabilidad y seguridad a los nuevos requisitos relacionados con el sector de la salud.

Este documento tiene un alcance que va desde dispositivos médicos básicos conectados a la red hasta equipos más grandes como los de rayos X y de resonancia magnética, e incluso semiconductores utilizados en estos equipos. Entre las ventajas de la IoMT se incluyen el acceso inmediato a los resultados de imágenes diagnósticas, el acceso en tiempo real a datos médicos como signos vitales, temperatura, presión y glucemia, así como la correlación automática de estos datos obtenidos de diversas fuentes. Todo esto contribuye a un diagnóstico más preciso, una gestión más adecuada de las prescripciones y, con impacto directo en la reducción de costos en el sector salud.[22]

El aporte de ENISA busca promover la confianza y la seguridad en las soluciones digitales para el sector, así como fomentar prácticas seguras en el desarrollo y la implementación de tecnología de la información en el ámbito de la atención médica.

Según los datos consultados, el valor de mercado de la IoMT sigue en aumento y se proyecta alcanzar los 140 mil millones de euros para el año 2022, según un estudio de Deloitte[23].

El tema de la seguridad en los IoMT y los equipos médicos se ha tomado con gran seriedad por parte de instituciones reconocidas. En diciembre de 2020, el Centro Nacional de Excelencia en Ciberseguridad del NIST (NCCoE) reunió a expertos y representantes de diversas áreas involucradas, como fabricantes, operadores, empresas de software comerciales, empresas de seguridad y universidades. El

[22] ENISA. ICT security certification opportunities in the healthcare sector [en línea]. ENISA. (Diciembre de 2018). Disponible en: https://www.enisa.europa.eu/publications/healthcare-certification . Consultado: noviembre 13 2023

[23] DELOITTE. Medtech and the Internet of Medical Things [en línea]. Deloitte. (s.f.). Disponible en: https://www2.deloitte.com/global/en/pages/life-sciences-and-healthcare/articles/medtech-internet-of-medical-things.htm . Consultado marzo 10 2024

objetivo de esta colaboración fue desarrollar una guía denominada NIST SP 1800-24 para mejorar el ecosistema de imágenes médicas.[24]

El sistema que gestiona estas imágenes médicas se conoce como Sistema de Comunicación y Archivo de Imágenes (PACS, por sus siglas en inglés). El PACS es prácticamente omnipresente en entornos de atención médica, puesto que centraliza las funciones relacionadas con los flujos de trabajo de imágenes médicas y sirve como un repositorio autorizado de información de imágenes médicas.

Dentro de un entorno de organización de prestación de servicios de salud como los hospitales, el PACS interactúa con una variedad de sistemas interconectados. Puede conectarse con sistemas de información clínica, dispositivos médicos y profesionales de la salud internos y externos. La complejidad de esta interacción puede exponer oportunidades para que actores maliciosos comprometan la confidencialidad, integridad y disponibilidad del ecosistema del PACS.

El NCCoE analizó los factores de riesgo relacionados con el ecosistema del PACS utilizando un enfoque de evaluación de riesgos basado en el Marco de Gestión de Riesgos del NIST. Además, se utilizaron el Marco de Ciberseguridad del NIST y otros estándares relevantes para identificar medidas que protejan el ecosistema. Como resultado, se desarrolló una implementación de ejemplo que demuestra cómo las organizaciones de prestación de atención médica pueden utilizar tecnologías de ciberseguridad disponibles comercialmente y basadas en estándares para proteger mejor el ecosistema del PACS. Esta guía práctica ayuda a los hospitales a implementar estándares y mejores prácticas de ciberseguridad, reduciendo así su

[24] Cawthra, J., Wang, S., Hodges, B., Zheng, K., Williams, R., Kuruvilla, J., Peloquin, C., Littlefield, K. y Neimeyer, B. (2020). Securing Picture Archiving and Communication System (PACS): Cybersecurity for the Healthcare Sector. Special Publication (NIST SP). National Institute of Standards and Technology, Gaithersburg, MD. [En línea] https://doi.org/10.6028/NIST.SP.1800-24. Consultado el 22 de marzo de 2024.

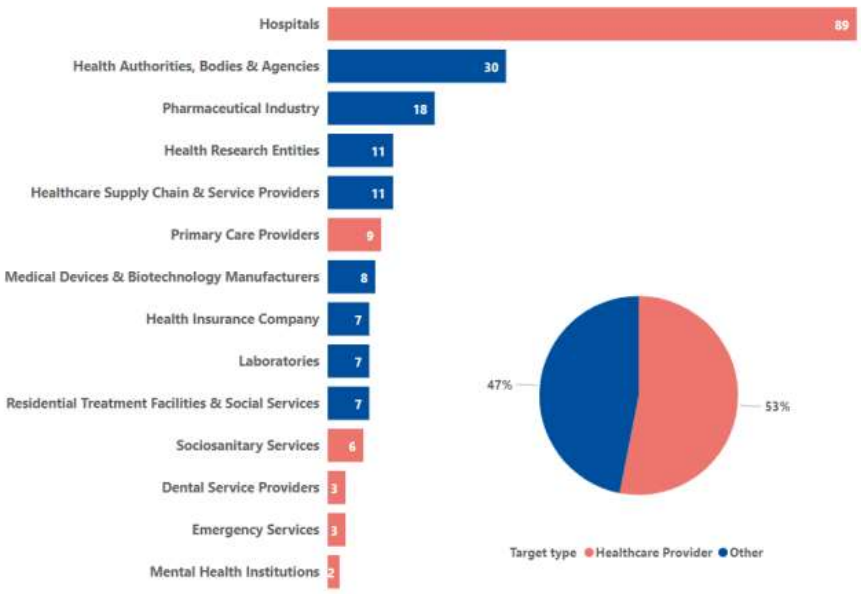
riesgo y protegiendo la privacidad de los pacientes sin comprometer el rendimiento y la usabilidad del PACS.

5.4.5. Enfoque en amenazas específicas en el sector salud.

Si bien es importante considerar las amenazas generales de ciberseguridad, se busca profundizar en las amenazas específicas que enfrentan los hospitales públicos en Colombia. La investigación revela una amplia brecha normativa entre países como la Unión Europea y Suramérica, particularmente Colombia. Por ejemplo, la UE cuenta con estadísticas claras y de fuentes confiables sobre los tipos de ataques y las consecuencias en el sector salud, lo que le permite tener políticas específicas respaldadas por leyes bien articuladas para cubrir las necesidades sin dejar vacíos legislativos, situación que contrasta con la realidad en Suramérica.

En este contexto, según el documento sobre el Panorama de amenazas en el sector salud emitido por la Agencia Europea de Ciberseguridad ENISA en julio de 2023, el cual toma una muestra desde enero 2021 hasta marzo 2023, el sector salud en la EU fue víctima del 53% del total de incidentes, donde resultaron afectados particularmente los hospitales. Se reportan perdidas en el sector por un 7% debido a este tipo de incidentes, sin embargo, aunque es difícil de cuantificar con exactitud, se estima que el costo económico por un incidente de seguridad está en una media de 300.000 euros, además de las sanciones, demandas por parte de las autoridades de protección de datos, así como la perdida reputacional que conlleva por lo general este tipo de situaciones, entre otros aspectos relacionados.

Ilustración 6 Tipos de Incidente por Entidades Sector Salud

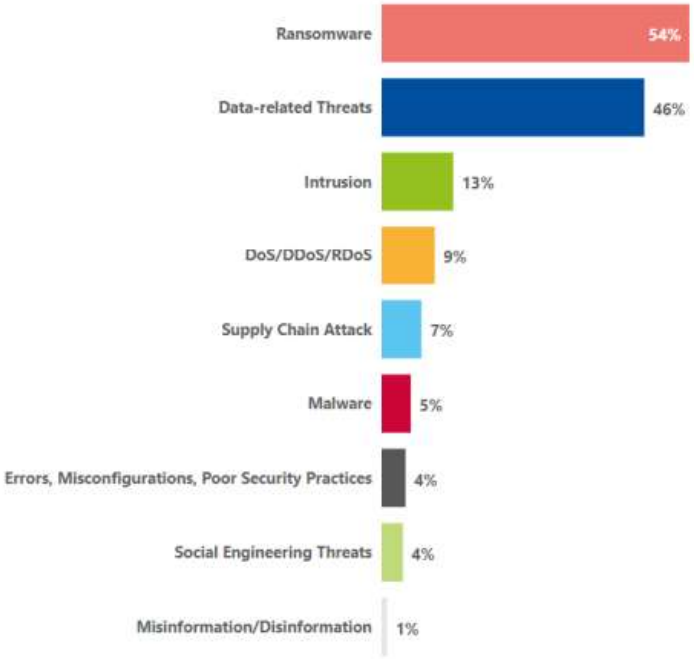


Fuente: (2023) ENISA THREAT LANDSCAPE: HEALTH SECTOR [Diagrama de barras]. En: ENISA THREAT LANDSCAPE: HEALTH SECTOR. Pag. 11. [Consultado: 25 de marzo de 2024]. Disponible en: https://www.enisa.europa.eu/publications/health-threat-landscape

La seguridad del paciente es una de las consecuencias de estos incidentes, puesto que se afecta directamente, en vista de que se retrasa su tratamiento, causa demoras en su clasificación y diagnóstico.

En este escenario el Ransomware se clasifica como el principal método de ataque, ocasionando filtración de información, indisponibilidad de servicios, violación de datos, y no solo en Europa sino a nivel global.

Ilustración 7 Tipos de amenazas en el sector salud entre 2021 y 2023



Fuente: (2023) ENISA THREAT LANDSCAPE: HEALTH SECTOR [Diagrama de barras]. En: ENISA THREAT LANDSCAPE: HEALTH SECTOR. Pag. 12. [Consultado: 25 de marzo de 2024]. Disponible en: https://www.enisa.europa.eu/publications/health-threat-landscape

Las amenazas relacionadas con los datos ocupan el segundo lugar en términos de frecuencia en el sector de la salud. La información sanitaria, por su naturaleza confidencial, se ve claramente comprometida por estas amenazas, con atacantes que buscan acceder a ella sin autorización para su manipulación y divulgación sin consentimiento. Esta fuga de datos puede ser el resultado de configuraciones incorrectas, vulnerabilidades en los sistemas de seguridad y errores humanos. Los atacantes suelen utilizar esta información robada para varios fines malintencionados. Estos incluyen la venta de la información en la DeepWeb, la obtención no autorizada de datos personales como la identificación o el número de seguridad social, llegando hasta la extorsión o chantaje de las victimas con el objetivo de obtener ganancias financieras a cambio de no divulgar su información medico-diagnostica.

En el mismo informe se puede observar los vectores de ataque o las puertas de entrada más comunes en este sector, entre los que están en primer lugar la Mala Configuración (68%), errores humanos en la operación (16%), Ingeniería Social/Phishing (4%).

La Directiva (UE) 2022/2555NIS2, conocida como NIS2 la cual impulsa las medidas legales en materia de ciberseguridad en Europa, que se promulga desde el 2016 y se actualizo en 2023, refuerza la importancia de la responsabilidad y el compromiso por parte de la dirección de las entidades, subrayando que la seguridad cibernética no es solo una cuestión técnica, sino también una de liderazgo y gestión.[25]
Aunque Colombia ha hecho avances a nivel normativo en el campo de la ciberseguridad, se observa que en muchas organizaciones este tema aún se relega al área de TI, sin contar con un respaldo significativo y las garantías necesarias por parte de la alta dirección. Es esencial compartir la responsabilidad y asegurar la inversión necesaria que este campo requiere. Es importante que normativas como la NIS2 sean adoptadas en Colombia con el objetivo de transferir el riesgo a las directivas y la administración de las entidades de salud. Esto permitirá contar con apoyo y trabajar conjuntamente para mitigar los riesgos, siguiendo las recomendaciones y mejores prácticas del sector.

El sector salud colombiano, particularmente los hospitales, se enfocan en la prestación del servicio médico, lo que a veces resulta en el descuido de otros factores importantes, convirtiéndolos en un blanco fácil para los delincuentes. De acuerdo con Jaime Ríos, socio de Digital y Cyber-Advisory de BDO en Colombia, los dispositivos médicos pueden ser un método fácil de entrada para los atacantes, así como los constantes accesos remotos a los sistemas que el personal médico requiere para sus tareas diarias. Además, Ríos resalta la necesidad de renovar

[25] Parlamento Europeo y Consejo de la Unión Europea. (2022). Directiva (UE) 2022/2555.[en línea]. Consultado el 25 de marzo de 2024. Recuperado de https://www2.deloitte.com/es/es/pages/risk/articles/directiva-nis-2.html

elementos obsoletos en el sector salud, como los sistemas de aplicación y las infraestructuras sin soporte de los fabricantes. Coincide en recomendaciones como el levantamiento de activos de información, la actualización frecuente de procedimientos, el fortalecimiento de controles y la capacitación como medidas efectivas ante este tipo de situaciones.[26]

Por otro lado, se destaca el artículo escrito por la periodista Laura Lesmes Díaz de la Casa Editorial El Tiempo. En su publicación, añade a las recomendaciones ya conocidas, la importancia de realizar simulacros de crisis para que el personal esté preparado y sepa cómo actuar en situaciones de emergencia. Asimismo, enfatiza la necesidad de elaborar planes de respuesta a incidentes, que facilitan una rápida reacción en caso de un ataque cibernético, disminuyendo directamente el impacto y las pérdidas. Confirma que el sector salud se cataloga como infraestructura crítica y, por lo tanto, se convierte en objetivo para los ciberdelincuentes. Este argumento subraya la necesidad de un plan de seguridad digital para los hospitales, que puede ser utilizado como herramienta de análisis y consulta continua, enfocándose en el uso adecuado de los recursos por parte de las directivas, y con las garantías de tener una dirección clara en caso de sufrir un incidente de seguridad.[27]

Como conclusión de este apartado, se destaca que la ausencia de programas de defensa específicos contra el ransomware y la falta de concienciación sobre seguridad cibernética entre el personal no técnico, ponen a estas organizaciones en riesgo de sufrir ataques cibernéticos. Estos ataques pueden tener consecuencias devastadoras, especialmente en un sector tan crítico como el de la salud. Entre los activos más afectados están la historia clínica del paciente, los dispositivos inteligentes para seguimiento y control de pacientes, redes y sistemas no médicos

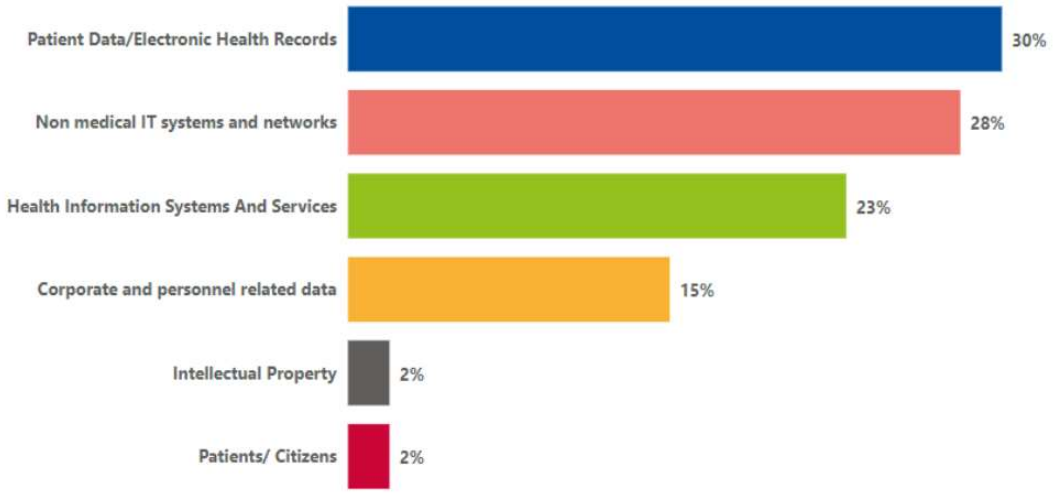
---

[26] Vanguardia. (2024). Así Puede prevenir los riesgos cibernéticos en el sector salud. [en linea] disponible en: www.vanguardia.com. https://www.vanguardia.com/mundo/tecnologia/2024/03/20/asi-puede-prevenir-los-riesgos-ciberneticos-en-el-sector-salud/ Consultado el 23 de marzo de 2024.

[27] Díaz, L. L. (2023). ¿Qué pasa con la ciberseguridad en las plataformas de salud de colombia?. El Tiempo. [en linea] disponible en https://www.eltiempo.com/tecnosfera/novedades-tecnologia/ciberseguridad-en-las-plataformas-de-salud-de-colombia-736510 . Consultado el 24 de marzo de 2024.

como página web institucional o aplicativos administrativos, datos corporativos expuestos y propiedad intelectual relacionada a temas de investigación científica.

Ilustración 8 Activos de información más afectados en el sector salud



Fuente: (2023) ENISA THREAT LANDSCAPE: HEALTH SECTOR [Diagrama de barras]. En: ENISA THREAT LANDSCAPE: HEALTH SECTOR. Pag. 26. [Consultado: 25 de marzo de 2024]. Disponible en: https://www.enisa.europa.eu/publications/health-threat-landscape

El análisis y evaluación de riesgos es fundamental para identificar y mitigar posibles amenazas. Las prácticas recomendadas, como la realización de copias de seguridad cifradas y la formación continua del personal, son medidas básicas y esenciales para fortalecer la resiliencia de las organizaciones frente a los ciberataques.

5.4.6. Colaboración Interdisciplinaria como una medida de protección.

La colaboración interdisciplinaria es una solución efectiva a varios retos en todos los niveles. Es necesario compartir el conocimiento y la experiencia, así como aprender de los demás. Cada profesión tiene una profundización del conocimiento

específica, lo que hace necesaria la interrelación de procesos y disciplinas para converger y tener un conocimiento holístico y colectivo.

En el campo de la ciberseguridad, el objetivo común es mitigar los riesgos y mantener el nivel de riesgo residual en niveles mínimos. Esta es una tarea difícil de realizar si no se trabaja en conjunto. Se requiere de la colaboración interdisciplinaria para que cada uno tenga presente su rol y se articule el trabajo para obtener buenos resultados. Esto involucra desde el apoyo de la administración, el personal de TI, el área de planeación, los usuarios internos y todo el personal que interactúa con los sistemas de información.

En el campo de la salud, particularmente en los hospitales públicos, se presenta el mismo concepto. Hay varios profesionales involucrados que deben aportar al objetivo de reducir el riesgo y velar por mantener la información disponible, confidencial e íntegra.

En una entidad de salud encontramos:

- Al personal médico como operario de los equipos y sistemas de información clínica.
- Al personal de ingeniería clínica quienes tienen a cargo el mantenimiento de los equipos e interactúan con los fabricantes para obtener los manuales de servicio y solicitar las actualizaciones y demás necesidades técnicas a nivel operativo de los equipos biomédicos.
- Al personal de TI quienes deben suministrar el canal de comunicación entre los dispositivos, a través de una red de datos correctamente administrada y habilitada de acuerdo con los requerimientos del fabricante o proveedor. Además de liderar la Gestión de la Información que incluye activos de información como el archivo clínico, gestión documental y la administración del software como aplicaciones de desarrollo propio así como los que se

adquieren para el funcionamiento de la organización, entre los más importantes el HIS (Sistema de Información Hospitalario).

- Al área jurídica, en donde se establecen las necesidades contractuales y se puede definir hasta qué nivel debe tener responsabilidad el proveedor del equipo o del servicio. En este espacio es importante definir soporte, vida útil, seguridad y acompañamiento técnico y demás objetivos del contrato.
- A la administración, que es quien define si se llevan a cabo o no los contratos y las negociaciones y en qué términos se dan. Es importante y necesario que se tenga presente temas como seguridad y se den las garantías necesarias para tener esta área presente dentro de toda negociación.

Todos estos profesionales deben actuar dentro de la ética para lograr un bien común. La colaboración interdisciplinaria es, por lo tanto, una medida de protección esencial en este campo y según lo confirma Hernández Armas, en el boletín No. 37 de Hospitecnica[28], la mejor manera de colaborar para mejorar la ciberseguridad en el sector es implementar acciones clave como:

- Implementar medidas de seguridad en dispositivos médicos, incluyendo antivirus, cortafuegos y sistemas de detección de intrusos.
- Cumplir con normativas legales y el reglamento sobre productos sanitarios para garantizar la confidencialidad de los datos médicos.
- Colaborar en la segmentación de la red y utilizar tecnologías como VLAN y cifrado para mejorar la seguridad de la red.
- Mantener actualizados los sistemas y software para prevenir ataques de malware y vulnerabilidades.

[28] Hernández Armas, J. A. (2020). Ciberseguridad en el entorno sanitario. Hospitecnia, Boletín 37, 09/11/2020, p.p 1-8. [On line] Disponible en https://hospitecnia.com/sites/default/files/inline-files/JAHernandez-seeic-ciberseguridad-entorno-sanitario.pdf Consultado 23 marzo de 2024.

- Incorporar inteligencia a las redes y controlar las comunicaciones para proteger equipos y sistemas médicos de manera más eficaz.
- Realizar estudios de riesgos y aplicar medidas de seguridad en todas las etapas del ciclo de vida de un dispositivo o sistema médico.

5.4.7. Integración para la seguridad con las Tecnologías Emergentes.

Es fundamental tener presente el enfoque futurista, explorando las últimas tendencias en seguridad, especialmente en el sector salud. Esto implica fomentar una mentalidad de investigación e innovación para desarrollar nuevos métodos y alternativas que combatan las crecientes amenazas de ataques cibernéticos. Esta orientación permite estar un paso adelante en la protección de la información, asegurando su disponibilidad, integridad, confidencialidad, trazabilidad y autenticidad. Al implementar estas tecnologías emergentes en los hospitales públicos de Colombia, se puede elevar significativamente el nivel de seguridad de los datos médicos, lo que se traduce en una atención médica más segura y confiable para los pacientes.

5.4.7.1. Inteligencia Artificial (IA): A través del análisis de grandes volúmenes de datos, como los que se manejan en registros o logs de eventos, la IA puede de manera automatizada identificar patrones anómalos en la red por ejemplo, de modo que no permita intrusiones y de esta manera proteja los sistemas de información médica de accesos no autorizados, aislando las terminales sospechosas para una confirmación del evento por parte del personal de seguridad, actuando de manera preventiva y temprana ante posibles incidentes de seguridad. Pero la cara opuesta a estas ventajas la encontramos en los riesgos asociados que esta tecnología representa para el sistema de salud, si no se aplican los principios rectores que menciona la OMS en su primer informe sobre IA denominado Ética y Gobernanza de la Inteligencia Artificial para la Salud, publicación en la cual menciona el riesgo ético por parte de los desarrolladores de la IA para optimizar resultados financieros u ocultar prácticas, así como el riesgo de la explotación de vulnerabilidades a los desarrolladores de la IA.[29]

5.4.7.2. Blockchain (Cadena de bloques): Se trabaja enfocando esta tecnología para garantizar la confidencialidad, integridad, autenticidad y trazabilidad de los datos médicos, reduciendo el riesgo de alteraciones maliciosas o accesos no autorizados a la información de los pacientes. El blockchain garantiza la confidencialidad al proteger los datos mediante la criptografía, asegura la autenticidad al utilizar firmas digitales y registros inmutables, y proporciona trazabilidad al mantener un registro transparente y verificable de todas las transacciones. Esto evita alteraciones o modificaciones no autorizadas en la información almacenada en la red blockchain. [30]

---

[29] OMS Organización Mundial de la Salud. (2021) Ethics and Governance of Artificial Intelligence for Health: WHO guidance. Pp. 57. [on line] Disponible en https://iris.who.int/bitstream/handle/10665/341996/9789240029200-eng.pdf?sequence=1 Consultado el 27 de marzo de 2024.

[30] Rodríguez, N. (2022) Blockchain en la Atención Médica: Casos de uso Y aplicaciones, 101 Blockchains. [on line] Disponible en https://101blockchains.com/es/blockchain-atencion-medica/ Consultado el 27 de marzo de 2024.

5.4.7.3. Machine Learning (Aprendizaje Automático): El aprendizaje automático, dentro del campo de la seguridad informática, se emplea para reforzar las defensas contra ataques cibernéticos. Mediante algoritmos especializados, es posible detectar y prever patrones de comportamiento malicioso, lo que potencia la capacidad de los sistemas de seguridad para adaptarse y responder eficazmente ante nuevas amenazas. En la actualidad, diversas aplicaciones de seguridad automatizan tareas como la gestión de actualizaciones y parches de seguridad, así como la orquestación de múltiples actividades de seguridad simultáneamente. Esto, en conjunto con el aprendizaje automático, reduce la carga laboral del personal de TI, permitiéndoles concentrarse en actividades más estratégicas y de mayor relevancia.

5.5 MARCO LEGAL.

En este documento se analiza la importancia de varios aspectos legales relacionados con la seguridad informática en una entidad de salud pública, centrándose en la protección de la información crítica y sensible de los pacientes, en particular, la historia clínica. Para ello, se examinan diversos decretos y leyes en el contexto de la investigación.

5.5.1. Aspectos legales y normativos relacionados.

El Decreto 338 del 8 de marzo de 2022,[31] "*Por el cual se adiciona el Titulo 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones*", exhorta la necesidad de

[31] COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Decreto 338 (8, marzo, 2022). Crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones [en línea]. Bogotá, D.C.: Diario Oficial. 2022. nro. 51.667. p. 1-32. [Consultado: octubre 2023]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=181866

garantizar la gobernanza de la seguridad digital, como es el caso en la prestación de servicios de salud, dado que la información médica es considerada información sensible y privada. Este decreto establece lineamientos para fortalecer la seguridad digital en el país, impulsar la gestión integral de riesgos, proveer mecanismos para coordinar la gestión y respuesta a incidentes de seguridad digital, promover la confianza en el intercambio de información y la gestión del conocimiento sobre seguridad digital y generar capacidades de seguridad digital de manera eficiente y colaborativa. A través de este decreto los hospitales públicos adoptaran las medidas para garantizar la seguridad digital en la información médica y el intercambio de información con otras entidades, así como la gestión de riesgos y respuesta a incidentes de seguridad digital. Además, de promover la generación de capacidades de seguridad digital en el personal médico y administrativo, lo que permitirá fortalecer la seguridad de los datos personales de los pacientes y mejorar la calidad de los servicios de salud.

La Ley 1273 de 2009[32] establece medidas para la protección de la información y los datos, así como la preservación integral de los sistemas que utilizan tecnologías de la información y las comunicaciones. Esta ley es de gran importancia para los hospitales públicos, ya que estos manejan información confidencial y sensible de los pacientes, como sus historias clínicas y datos personales. La ley establece penas para aquellos que accedan de manera ilegal a los sistemas informáticos, obstaculicen su funcionamiento, intercepten datos o utilicen software malicioso para dañar los sistemas. También sanciona la violación de datos personales y la suplantación de sitios web para capturar información personal.

Los hospitales públicos deben garantizar la seguridad y confidencialidad de la información de sus pacientes y empleados, por lo que deben implementar medidas

[32] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273 (5, enero, 2009). Por medio de la cual se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones [en línea]. Bogotá, D.C.: Diario Oficial. 2009. nro. 47.223. p. 1-4. [Consultado: octubre 2023]. Disponible en: http://secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

de seguridad informática y cumplir con las disposiciones establecidas en esta ley. Además, deben capacitar a su personal en el manejo de la información y los riesgos asociados a la tecnología, y establecer protocolos de respuesta en caso de una eventualidad.

Por otro lado, dentro de las regulaciones y normas en el marco del actual proyecto aplicado, tenemos la Ley 23 de 1981[33], que trata la ética médica y entre sus apartes, de la reserva de la historia clínica, tema de importancia para la seguridad de la información de una entidad de salud, porque establece claramente que la historia clínica de un paciente es un documento privado sometido a reserva y únicamente puede ser conocido por terceros previa autorización del paciente o en los casos previstos por la Ley. Esto significa que la información médica y personal de los pacientes debe ser protegida y tratada con confidencialidad por los profesionales de la salud y el personal del hospital.

Esta ley es fundamental para garantizar la privacidad y seguridad de la información de los pacientes, ya que los datos médicos y personales son sensibles y confidenciales. Si se produjera una violación de la seguridad de la información en un hospital y se revelara información confidencial sin autorización, se estaría violando esta ley y se podrían producir consecuencias legales graves. Por lo tanto, es importante que estas entidades tomen medidas adecuadas para proteger la información médica de sus pacientes y asegurar que solo se comparta la información de manera autorizada y segura.

Otra norma importante es la Resolución 1995 de 1999[34], la que decreta lineamientos técnicos y de seguridad para el manejo de la información contenida en la historia

---

[33] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 23 (11, febrero, 1981). Por la cual se dictan normas en materia de ética médica. Ley 23 de 1981. Bogotá, D.C.: Diario Oficial. 1981. nro. 35.657. p. 1-5. [Consultado: octubre 2023]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0023_1981.html

[34] COLOMBIA. MINISTERIO DE SALUD. Por la cual se establecen normas para el manejo de la historia clínica. Resolución 1995 de 1999. (8, julio, 1999). Bogotá, D.C.: Diario Oficial. [Consultado: octubre 2023]. Disponible en: https://www.minsalud.gov.co/sites/rid/Lists/BibliotecaDigital/RIDE/DE/DIJ/Resoluci%C3%B3n_1995_de_1999.pdf

clínica. Establece que la historia clínica es un documento privado y confidencial que contiene información sensible sobre la salud de los pacientes y su uso indebido puede tener graves consecuencias para la privacidad y la seguridad de la información. Por esta ley todos los prestadores de servicios de salud pueden utilizar medios técnicos como computadoras y medios magneto - ópticos para el registro y conservación de la historia clínica, siempre y cuando se adopten mecanismos de seguridad que impidan la incorporación de modificaciones no autorizadas y se proteja la reserva de la historia clínica mediante mecanismos que impidan el acceso de personal no autorizado.

Ley 1581 de 2012 de Protección de Datos Personales[35] reconoce y protege el derecho que tienen todas las personas a conocer, actualizar y rectificar la información que se hayan recogido sobre ellas en bases de datos o en archivos y que sean susceptibles de tratamiento por entidades de naturaleza pública o privada. Su principal objetivo de esta es "garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas y especialmente de su honor e intimidad personal y familiar". Esta ley establece los principios, derechos, deberes y procedimientos para garantizar el derecho constitucional al hábeas data, así como las funciones y sanciones de la Superintendencia de Industria y Comercio como autoridad de protección de datos

La Resolución 500 de 2021[36] es también relevante ya que establece los lineamientos y estándares para la estrategia de seguridad digital en el país y adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno

[35] COLOMBIA. CONGRESO DE LA REPÚBLICA. (2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Ley 1581 de 2012. Bogotá, D.C.: Diario Oficial. [Consultado: octubre 2023]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

[36] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. (2021). Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital. Resolución 500 de 2021. Bogotá, D.C.: Diario Oficial. [Consultado: octubre 2023]. Disponible en: https://normograma.mintic.gov.co/docs/pdf/resolucion_mintic_0500_2021.pdf

Digital. En conjunto, estas medidas contribuyen a fortalecer la capacidad del sector salud para prevenir y responder a amenazas y riesgos, garantizando la confidencialidad y la integridad de la información y los servicios digitales en este ámbito.

La Directiva Presidencial 03 de 2021[37] es de rescatar en toda entidad publica, ya que establece los lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital, gestión de datos y lineamientos de la directiva en los territorios. Garantizaría la calidad, integridad, disponibilidad, confidencialidad y accesibilidad de los datos que se generan, almacenan, procesan y transmiten en la entidad, aplicando los principios y estándares de gobierno digital y seguridad digital, implementando una estrategia de gobierno de datos y promoviendo el uso y el aprovechamiento de los datos para la toma de decisiones y la generación de valor público.

Por último, La Resolución 1519 de 2020[38] tiene como objetivo definir los estándares y directrices para publicar la información señalada en la Ley 1712 de 2014, que regula el derecho de acceso a la información pública, y establecer los requisitos en materia de accesibilidad web, seguridad digital y datos abiertos, que son aspectos clave para facilitar el acceso, la consulta y el uso de la información por parte de los ciudadanos, las entidades públicas y los demás interesados. La resolución busca impulsar la transformación digital de las entidades públicas, garantizar el derecho de acceso a la información, promover la transparencia y la participación ciudadana, y proteger la privacidad y la seguridad de los datos. En cuanto a seguridad digital, la resolución dispone medidas para fortalecer la seguridad de la información y los

[37] COLOMBIA. PRESIDENCIA DE LA REPÚBLICA. Directiva Presidencial 03 (15, marzo, 2021). Por la cual se establecen lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos por parte de las entidades públicas de la rama ejecutiva del orden nacional [en línea]. Bogotá, D.C.: Diario Oficial. 2021. nro. 51.637. p. 1-8. [Consultado: octubre de 2023]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=160326

[38] COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Resolución 1519 (24, agosto, 2020). Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos [en línea]. Bogotá, D.C.: El Ministerio. 2020. 8 p. [Consultado: octubre de 2023]. Disponible en: https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Resolucion/30044657

servicios digitales de las entidades públicas, tales como definir políticas de infraestructura, evitar la instalación de programas o extensiones desconocidas, no exponer información personal o reservada en enlaces públicos, usar aplicaciones de mensajería con encriptación extremo a extremo, contar con capa de conexión segura (SSL) y cambiar las contraseñas periódicamente. Esto es fundamental para garantizar la transparencia y el acceso a información en el sector salud, al mismo tiempo que se protege la privacidad y seguridad de los datos de los pacientes.

Por lo tanto, el cumplimiento de las disposiciones establecidas en las resoluciones, decretos y demás normativas legales es esencial para garantizar la integridad, confidencialidad y disponibilidad de la información en el sector de la salud. La seguridad informática en las entidades de salud pública es un componente crítico para salvaguardar la privacidad de los pacientes y el adecuado funcionamiento de los sistemas. La implementación de las mejores prácticas en ciberseguridad no solo es un requisito legal, sino una responsabilidad fundamental para preservar la confianza de los pacientes y asegurar la calidad de los servicios de salud. La interacción entre estas regulaciones contribuye a un entorno seguro y transparente en el manejo de datos en el sector de la salud, lo que beneficia tanto a pacientes como a profesionales de la salud, así como la información financiera y contable para la continuidad del negocio en este sector.

6. DISEÑO METODOLÓGICO

Los métodos aplicados a esta investigación serán tanto cuantitativos como cualitativos, lo que resulta en un enfoque mixto, combinando estos dos métodos para abordar cada uno de los objetivos específicos, permite una comprensión profunda de los riesgos y amenazas de seguridad cibernética que enfrentan los hospitales públicos en Colombia y la elaboración de políticas y procedimientos de seguridad efectivos.

En primer lugar, se aplica un enfoque cuantitativo al identificar las amenazas y riesgos de seguridad cibernética en los sistemas misionales y aplicaciones utilizados, por medio de metodologías y marcos reconocidos para identificar los riesgos críticos que deben ser abordados en el plan director de seguridad digital. Este enfoque cuantitativo podría involucrar la recopilación de datos a través de encuestas, análisis de datos y estadísticas.

En segundo lugar, se aplica un enfoque cualitativo al evaluar las amenazas identificadas en el análisis de riesgos y estableciendo así la matriz de seguridad de la información como estrategia integral de seguridad que deriva en el desarrollo de políticas y procedimientos de seguridad cibernética basados en las recomendaciones dadas en los marcos, metodologías y estándares internacionales. Este enfoque cualitativo podría involucrar entrevistas, grupos focales y análisis de documentos.

Finalmente, se propone construir un Plan director de seguridad digital que contemple capacitación y entrenamiento en ciberseguridad al personal administrativo y asistencial de estas instituciones, que fortalezca la adopción de las políticas y procedimientos de seguridad cibernética establecidos. Este plan se basaría en los resultados de la investigación cuantitativa y cualitativa previas.

7. DESARROLLO DE LOS OBJETIVOS

Este proyecto busca mejorar la seguridad digital en los sistemas misionales y aplicaciones utilizados por los hospitales públicos en Colombia. Para lograrlo, se plantean varios objetivos específicos, que incluyen la identificación de amenazas y riesgos de seguridad, la evaluación detallada de estas amenazas y la creación de una matriz de seguridad de la información como estrategia integral. Además, se propone un plan detallado que contempla la capacitación en ciberseguridad para el personal administrativo y asistencial de los hospitales públicos en Colombia, con el fin de fortalecer la adopción de controles y procedimientos de seguridad cibernética.

7.1 IDENTIFICACIÓN DE AMENAZAS Y RIESGOS DE SEGURIDAD.

La metodología MAGERIT v3 reconocido como un marco estructurado que permite la identificación, evaluación y tratamiento de los riesgos de seguridad de la información, es una herramienta practica en la identificación de los activos de información, que son el punto de partida para la gestión integral del riesgo.

A partir de los activos, se determinan las amenazas, las vulnerabilidades, los controles y el impacto que podrían afectar la confidencialidad, la integridad y la disponibilidad de la información. Así que se puede aplicar esta metodología para analizar y gestionar los riesgos de seguridad de la información de forma sistemática y eficiente.

7.1.1 Identificación de activos de información.

En este apartado se trabaja con la Metodología Magerit v3, donde se confirma que los activos de información son elementos valiosos para una organización y requieren protección contra posibles amenazas y los define como: ”los recursos que usa el sistema de información o que se relacionan con este para que la organización

cumpla con sus objetivos". Esta clasificación permite a las organizaciones identificar y priorizar los activos de información más críticos, asignando así mayores recursos y esfuerzos a su protección y seguridad.

A continuación, se presenta el inventario de activos de información de un hospital público de tercer nivel de complejidad. Siguiendo la clasificación establecida por esta metodología, los activos se han agrupado en doce categorías y se han relacionado según su descripción y propósito correspondiente.

Cuadro 4 Activos de información: activos esenciales

MAGERIT	HOSPITAL
[info] información	HIS (SISTEMA DE INFORMACION HOSPITALARIO) BASE DE DATOS DEL HIS INFRAESTRUCTURA DE RED: SEGURIDAD PERIMETRAL, SWITCH CORE – SERVICIO DHCP/DNS – CONTROLADORAS WiFi SOFTWARE MISIONAL: RESULTADO A PROCEDIMIENTOS, LABORATORIOS, IMÁGENES DIAGNOSTICAS ARCHIVOS DE USUARIO: RESOLUCIONES, ACTAS, ACUERDOS. ACCESO A INTERNET
[adm] datos de interés para la administración pública	
[vr] datos vitales (registros de la organización) (1)	
[per] datos de carácter personal (2)	
[A] nivel alto	
[M] nivel medio	
[B] nivel bajo	
[classified] datos clasificados (3)	
[C] nivel confidencial	
[R] difusión limitada	
[UC] sin clasificar	
[pub] de carácter público	
[service] servicio	

Fuente: El Autor (2023).

Cuadro 5 Activos de información: arquitectura del sistema

MAGERIT	HOSPITAL
[sap] punto de [acceso al] servicio (1)	HIS SERVIDORES RED DE VOZ Y DATOS APLICATIVOS MISIONALES PLATAFORMAS ENTES DE CONTROL PLATAFORMAS MINSALUD PLATAFORMAS EPS INTERNET – TELEVISION – TELEFONIA RED ELECTRICA SERVICIOS DE MANTENIMIENTO TERCERIZADOS SERVICIOS DE SALUD ESPECIALIZADOS TERCERIZADOS
[ip] punto de interconexión (2)	
[ext] proporcionado por terceros (3)	

Fuente: El Autor (2023).

Cuadro 6 Activos de información: datos / información

MAGERIT	HOSPITAL
[files] ficheros	COPIAS DE SEGURIDAD APLICATIVOS MISIONALES COPIAS DE SEGURIDAD DISPOSITIVOS DE RED COPIA DE SEGURIDAD DISPOSITIVOS PERIMETRALES COPIA SEGURIDAD HIS COPIA DE SEGURIDAD GESTION DOCUMENTAL COPIA DE SEGURIDAD CORREO ELECTRONICO COPIA DE SEGURIDAD INTRANET COPIA DE SEGURIDAD PAGINA WEB COPIA DE SEGURIDAD CENTRAL TELEFONICA COPIA SEGURIDAD PROYECTOS INVESTIGACION COPIA DE SEGURIDAD ARCHIVOS ALTA DIRECCION CREDENCIALES PLATAFORMAS EXTERNAS MISIONALES CÓDIGO FUENTE DE APLICATIVOS
[backup] copias de respaldo	
[conf] datos de configuración (1)	
[int] datos de gestión interna	
[password] credenciales (ej. contraseñas)	
[auth] datos de validación de credenciales	
[acl] datos de control de acceso	
[log] registro de actividad (2)	
[source] código fuente	
[exe] código ejecutable	
[test] datos de prueba	
[D] Datos / Información	

Fuente. El Autor (2023).

Cuadro 7 Activos de Información: Claves Criptográficas

MAGERIT	HOSPITAL
[info] protección de la información	FIRMA DIGITAL TOKEN DIGITAL CERTIFICADOS TLS/SSL PARA EL DOMINIO
[encrypt] claves de cifra	
[shared_secret] secreto compartido (clave simétrica) (1)	
[public_encryption] clave pública de cifra (2)	
[public_decryption] clave privada de descifrado (2)	
[sign] claves de firma	
[shared_secret] secreto compartido (clave simétrica)	
[public_signature] clave privada de firma (2)	
[public_verification] clave pública de verificación de firma (2)	
[com] protección de las comunicaciones	
[channel] claves de cifrado del canal	
[authentication] claves de autenticación	
[verification] claves de verificación de autenticación	
[disk] cifrado de soportes de información	
[encrypt] claves de cifra	
[x509] certificados de clave pública	

Fuente: El Autor (2023).

Cuadro 8 Activos de información: Servicios

MAGERIT	HOSPITAL
[anon] anónimo (sin requerir identificación del usuario)	CORREO ELECTRÓNICO INSTITUCIONAL CARPETAS COMPARTIDAS PÁGINA WEB INSTITUCIONAL GESTIÓN DE ROLES Y RESTRICCIÓN DE PRIVILEGIOS EN HIS Y APLICATIVOS INSTITUCIONALES
[pub] al público en general (sin relación contractual)	
[ext] a usuarios externos (bajo una relación contractual)	
[int] interno (a usuarios de la propia organización)	
[www] world wide web	
[telnet] acceso remoto a cuenta local	
[email] correo electrónico	
[file] almacenamiento de ficheros	
[ftp] transferencia de ficheros	
[edi] intercambio electrónico de datos	
[dir] servicio de directorio (1)	
[ipm] gestión de privilegios	
[idm] gestión de identidades (2)	
[pki] PKI - infraestructura de clave pública (3)	

Fuente. El Autor (2023).

Cuadro 9 Activos de información: Aplicaciones Informáticas

MAGERIT	HOSPITAL
[prp] desarrollo propio (in house)	HIS, HIPERVISORES, SERVIDOR Y CLIENTE DE CORREO, MOTORES DE BASES DE DATOS, SISTEMAS OPERATIVOS, ANTIVIRUS, OFIMÁTICA, APLICATIVOS MISIONALES, PLATAFORMAS MISIONALES, VISORES IMAGENOLOGIA, INTRANET, MESA DE AYUDA, PLATAFORMAS GESTION EQUIPAMENTO DE RED, DOMOTICA, APLICACIONES WEB, PLATAFORMAS IDRAC DELL, PLATAFORMAS ILO HP, SOFTWARE EQUIPOS BIOMEDICOS Y DE LABORATORIO, SOFTWARE PLATAFORMAS CARGUE DE INFORMACIÓN A EPS, SOFTWARE DE GESTIÓN DOCUMENTAL.
[sub] desarrollo a medida (subcontratado)	
[std] estándar (off the shelf)	
[browser] navegador web	
[www] servidor de presentación	
[app] servidor de aplicaciones	
[email_client] cliente de correo electrónico	
[email_server] servidor de correo electrónico	
[file] servidor de ficheros	
[dbms] sistema de gestión de bases de datos	
[tm] monitor transaccional	
[office] ofimática	
[av] anti virus	
[os] sistema operativo	
[hypervisor] gestor de máquinas virtuales	
[ts] servidor de terminales	
[backup] sistema de backup	

Fuente. El Autor (2023).

Cuadro 10 Activos de información: Equipos informáticos (hardware)

MAGERIT	HOSPITAL
[host] grandes equipos (1)	SERVIDORES, WORKSTATION, DESKTOP, LAPTOP, SMARTPHONES, TABLETAS, NAS, SAN, IMPRESORAS, SCANNER, LECTORES CÓDIGO BARRAS, HUELLEROS, SWITCH CORE, MODEM INTERNET, PLANTA TELEFÓNICA, GATEWAY TELEFONÍA IP, TELÉFONOS IP, FIREWALL, AP, DOMOTICA, CÁMARAS IP, DVR-IP CCTV, SMART TV, SISTEMAS RFID, EQUIPOS BIOMÉDICOS, LLAMADOS ENFERMERIA, DIGITURNOS, IoT, IoMT.
[mid] equipos medios (2)	
[pc] informática personal (3)	
[mobile] informática móvil (4)	
[pda] agendas electrónicas	
[vhost] equipo virtual	
[backup] equipamiento de respaldo (5)	
[peripheral] periféricos	
[print] medios de impresión (6)	
[scan] escáneres	
[crypto] dispositivos criptográficos	
[bp] dispositivo de frontera (7)	
[network] soporte de la red (8)	
[modem] módems	
[hub] concentradores	
[switch] conmutadores	
[router] encaminadores	
[bridge] pasarelas	
[firewall] cortafuegos	
[wap] punto de acceso inalámbrico	
[pabx] centralita telefónica	
[ipphone] teléfono IP	

Fuente. El Autor (2023).

Cuadro 11 Activos de información: redes de comunicaciones

MAGERIT	HOSPITAL
[PSTN] red telefónica	CANAL E1 DE VOZ CANAL DEDICADO INTERNET FIBRA ÓPTICA PRINCIPAL Y RESPALDO (WAN) ANTENAS DE COMUNICACIONES DE RADIO (AMBULANCIAS Y RADIOS) RED DE DATOS Y VOZ TELEFONÍA MÓVIL, RADIO ENLACE
[ISDN] rdsi (red digital)	
[X25] X25 (red de datos)	
[ADSL] ADSL	
[pp] punto a punto	
[radio] comunicaciones radio	
[wifi] red inalámbrica	
[mobile] telefonía móvil	
[sat] por satélite	
[LAN] red local	
[MAN] red metropolitana	
[Internet] Internet	

Fuente: El Autor (2023).

Cuadro 12 Activos de información: soportes de información

MAGERIT	HOSPITAL
[electronic] electrónicos	CLOUD, DISCOS DUROS FÍSICOS, DISCOS DUROS VIRTUALES, NAS, SAN, DISCOS DUROS EXTERNOS, MEMORIAS USB, ALMACENAMIENTO EN RED, DVD, TARJETAS DE MEMORIA, TARJETAS INTELIGENTES, MATERIAL IMPRESO.
[disk] discos	
[vdisk] discos virtuales	
[san] almacenamiento en red	
[disquette] disquetes	
[cd] cederrón (CD-ROM)	
[usb] memorias USB	
[dvd] DVD	
[tape] cinta magnética	
[mc] tarjetas de memoria	
[ic] tarjetas inteligentes	
[non_electronic] no electrónicos	
[printed] material impreso	
[tape] cinta de papel	
[film] microfilm	
[cards] tarjetas perforadas	

Fuente. El Autor (2023).

Cuadro 13 Activos de información: equipamiento auxiliar

MAGERIT	HOSPITAL
[power] fuentes de alimentación	RED ELECTRICA REGULADA, UPS, PLANTA ELECTRICA, AIRES ACONDICIONADOS, CABLEADO DE AREA PARA DATOS Y RED ELECTRICA, BACKBONE FIBRA, RACKS DE COMUNICACIONES,
[ups] sistemas de alimentación ininterrumpida	
[gen] generadores eléctricos	
[ac] equipos de climatización	
[cabling] cableado	
[wire] cable eléctrico	
[fiber] fibra óptica	
[robot] robots	
[tape] ... de cintas	
[disk] ... de discos	
[supply] suministros esenciales	
[destroy] equipos de destrucción de soportes de información	
[furniture] mobiliario: armarios, etc	
[safe] cajas fuertes	

Fuente. El Autor (2023).

Cuadro 14 Activos de información: instalaciones

MAGERIT	HOSPITAL
[site] recinto	DATA CENTER CENTROS DE CABLEADO Y DATOS CUARTOS ELECTRICOS CENTRAL ELECTROGENA CENTRAL TELEFONICA
[building] edificio	
[local] cuarto	
[mobile] plataformas móviles	
[L] Instalaciones	
[car] vehículo terrestre: coche, camión, etc.	
[plane] vehículo aéreo: avión, etc.	
[ship] vehículo marítimo: buque, lancha, etc.	
[shelter] contenedores	
[channel] canalización	
[backup] instalaciones de respaldo	

Fuente: El Autor (2023).

Cuadro 15 Activos de información: personal

MAGERIT	HOSPITAL
[ue] usuarios externos	USUARIOS INTERNOS: FUNCIONARIOS. COORDINACIÓN TI, DBA, PROFESIONALES CONTRATISTAS TICS, TÉCNICOS OPERATIVOS. PROVEEDORES DE SERVICIOS TECNOLOGICOS TERCERIZADOS
[ui] usuarios internos	
[op] operadores	
[P] Personal	
[adm] administradores de sistemas	
[com] administradores de comunicaciones	
[dba] administradores de BBDD	
[sec] administradores de seguridad	
[des] desarrolladores / programadores	
[sub] subcontratas	
[prov] proveedores	

Fuente: El Autor (2023).

La relación anterior abarca todos los activos de información que están directa o indirectamente relacionados con los sistemas de información misionales de los hospitales. Esta inclusión de todos los activos es crucial para obtener una visión completa y poder realizar una valoración individual de cada uno de ellos. Esta valoración se realiza considerando un criterio que abarca desde activos que poseen un valor muy alto hasta aquellos que tienen un valor despreciable.

De esta manera, se puede asignar la debida importancia y prioridad en términos de la protección a la Confidencialidad, Integridad y Disponibilidad.

7.1.2 Dependencia de activos de información.

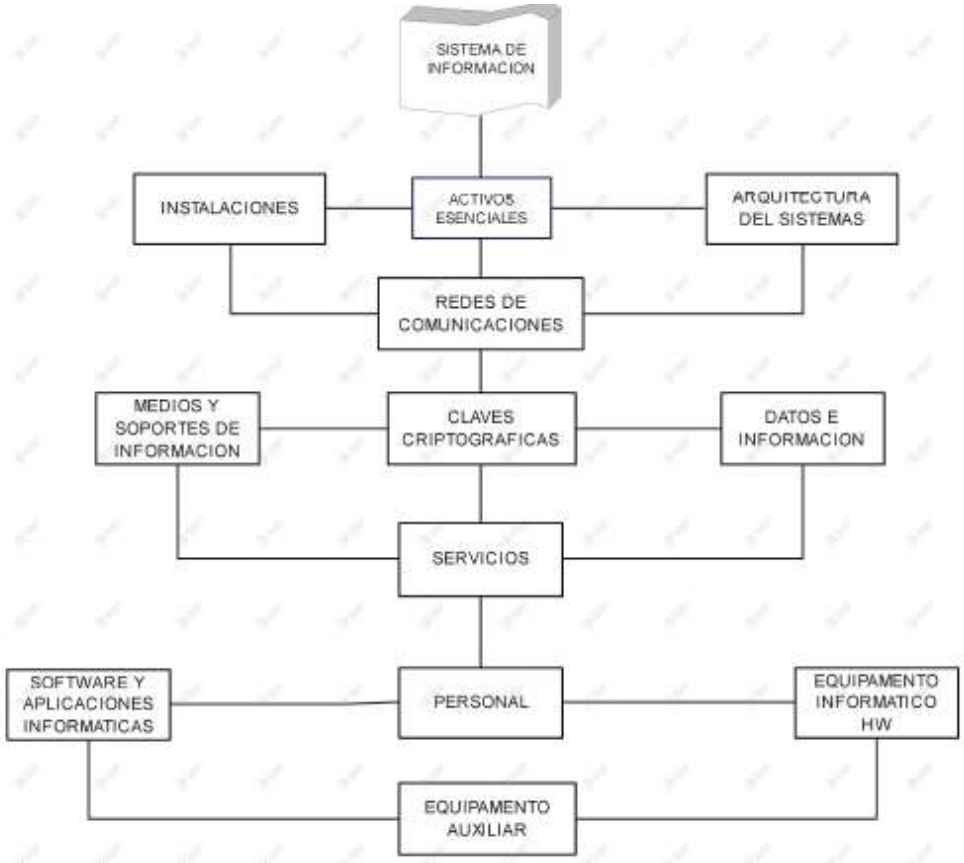
La identificación de las amenazas y riesgos de seguridad en los sistemas misionales y aplicaciones en hospitales públicos de Colombia requiere una comprensión de las dependencias entre los activos de información. Estas dependencias muestran cómo las amenazas pueden afectar indirectamente los activos de mayor valor o impacto, cuando directamente afectan un activo de menor valor.

Al atender las necesidades de seguridad de los activos de menor nivel, se puede proteger eficazmente toda la cadena de dependencias y reducir los riesgos críticos definidos en el plan director de seguridad digital. Magerit en su libro I nos explica la dependencia de activos y la define como : " *dependencias entre activos, es la medida en que un activo de orden superior se puede ver perjudicado por una amenaza materializada sobre un activo de orden inferior* ." [39]

La ilustración 9 (Dependencia de los Activos de Información) representa un ejemplo de la estructura en la dependencia de los activos para una entidad de salud pública.

[39] Ministerio de Hacienda y Administraciones Públicas. (2012). MAGERIT versión 3 (versión española): Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I: Método [PDF]. NIPO: 630-12-171-8. P.p. 39 Disponible en https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Ilustración 9 Dependencia de los Activos de Informacion



Fuente: El Autor (2023).

7.1.3 Identificación de amenazas sobre los activos de información.

Las amenazas son eventos o situaciones que pueden ocurrir y representar un riesgo para los activos, causándoles daño. Es importante tener en cuenta los diferentes tipos de amenazas que pueden afectar los sistemas y activos, según el Libro 2 de Magerit, los tipos de amenazas se clasifican así:

Amenazas de origen natural: Estas amenazas están relacionadas con eventos naturales como incendios, terremotos, inundaciones, volcánicos y otros desastres similares. Aunque el sistema de información es una víctima pasiva en estos casos,

es necesario tener en cuenta las posibles consecuencias que estos eventos pueden tener en los activos.

Amenazas del entorno industrial: Estas amenazas están vinculadas a desastres de origen industrial, como la contaminación, fugas, fallas eléctricas, siniestros mayores, vibraciones, polvo, suciedad, contaminación electromagnética, falla hardware, climatización, falla de medios de telecomunicaciones; para estos casos se deben tomar las medidas de protección adecuadas.

Defectos de las aplicaciones: Estas amenazas surgen directamente de posibles fallos o defectos en el diseño o implementación de las aplicaciones utilizadas. Errores de usuarios, de administración, de monitorización, de configuración, de organización, de malware, de integridad, de disponibilidad, de confidencialidad, de actualizaciones, de recursos, de personal. Estas vulnerabilidades técnicas pueden tener consecuencias negativas en el sistema y deben ser identificadas y mitigadas.

Amenazas causadas por personas de forma accidental: Las personas que tienen acceso al sistema de información pueden ser la causa de problemas no intencionados, ya sea por error o por omisión. Errores de usuarios, de administración, de monitorización, de configuración, de organización, de malware, de integridad, de disponibilidad, de confidencialidad, de actualizaciones, de recursos, de personal. Es importante considerar estas amenazas accidentales y establecer medidas para prevenirlas o mitigar su impacto.

Amenazas causadas por personas de forma deliberada: En ocasiones, las personas con acceso al sistema de información pueden actuar de manera intencionada para llevar a cabo ataques o acciones perjudiciales. Suplantación, manipulación, abuso de privilegios, uso no previsto, malware, integridad, confidencialidad, análisis de tráfico, repudio, interceptación, modificación, destrucción, robo, ocupación enemiga, indisponibilidad de personal, extorsión, ingeniería social. Estos ataques deliberados

pueden tener como objetivo obtener beneficios indebidos o causar daños y perjuicios a los legítimos propietarios.

La evaluación de las amenazas identificadas en un análisis de riesgos es importante para comprender los posibles escenarios de seguridad a los que se enfrentan los hospitales públicos, con el fin de proyectarlos en la matriz de seguridad de la información y obtener una visión clara de las amenazas en relación con los activos críticos y de esta manera, asignar los controles adecuados.

La selección y valoración de las amenazas se basa en los criterios establecidos en Magerit, específicamente en el capítulo 5 del libro 2. En este capítulo, se proporciona un catálogo de amenazas con descripciones detalladas de cada una, así como la dimensión de seguridad que afectan y los activos involucrados.

Siguiendo esta metodología, a continuación, se presenta la información referente a la valoración de las amenazas en relación con los activos críticos en hospitales públicos de Colombia.

Tabla 1 Amenazas a los Activos de Información: Esenciales

AMENAZAS A LOS ACTIVOS DE INFORMACION ESENCIALES				
TIPO DE ACTIVO	DESCRIPCION	AMENAZAS	FRECUENCIA	DEGRADACION E IMPACTO
ACTIVOS ESENCIALES	HIS (SISTEMA DE INFORMACION HOSPITALARIO) BASE DE DATOS DEL HIS INFRAESTRUCTURA DE RED: SEGURIDAD PERIMETRAL, SWITCH CORE – SERVICIO DHCP/DNS – CONTROLADORAS WiFi	[A.11] Acceso no autorizado	1	5

Tabla 1 (Continuacion)

ACTIVOS ESENCIALES	SOFTWARE MISIONAL: RESULTADO A PROCEDIMIENTOS, LABORATORIOS, IMÁGENES DIAGNOSTICAS ARCHIVOS DE USUARIO: RESOLUCIONES, ACTAS, ACUERDOS. ACCESO A INTERNET	[A.15] Modificación deliberada de la información	1	5
		[A.18] Destrucción de información	1	5
		[A.19] Revelación de información	1	4
		[E.14] Escapes de información	2	3
		[E.15] Alteración accidental de la información	1	4
		[E.18] Destrucción de información	1	5
		[E.21] Errores de mantenimiento / actualización de programas (software)	2	3

Fuente: El Autor (2023)

Tabla 2 Amenazas a los Activos de Información: Arquitectura del Sistema

AMENAZAS A LOS ACTIVOS DE INFORMACION ARQUITECTURA DEL SISTEMA				
TIPO DE ACTIVO	DESCRIPCION	AMENAZAS	FRECUENCIA	DEGRADACION E IMPACTO
ARQUITECTURA DEL SISTEMA	HIS SERVIDORES RED DE VOZ Y DATOS APLICATIVOS MISIONALES PLATAFORMAS ENTES DE CONTROL PLATAFORMAS MINSALUD PLATAFORMAS EPS INTERNET – TELEVISION – TELEFONIA RED ELECTRICA SERVICIOS DE MANTENIMIENTO TERCERIZADOS SERVICIOS DE SALUD ESPECIALIZADOS TERCERIZADOS	[A.11] Acceso no autorizado	1	4
		[A.23] Manipulación de los equipos	1	4
		[A.24] Denegación de servicio	1	5
		[A.25] Robo	2	4
		[A.26] Ataque destructivo	1	5
		[A.5] Suplantación de la identidad del usuario	1	4
		[A.6] Abuso de privilegios de acceso	1	4
		[A.7] Uso no previsto	1	5
		[E.2] Errores del administrador	2	3
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	3
		[E.24] Caída del sistema por agotamiento de recursos	3	3
		[E.25] Perdida de Equipos	2	4
		[E.4] Errores de configuración	3	3
		[I.*] Desastres industriales	1	5

Tabla 2 (continuacion)

ARQUITECTURA DEL SISTEMA		[I.11] Emanaciones electromagnéticas	1	4
		[I.3] Contaminación mecánica	2	3
		[I.4] Contaminación electromagnética	2	2
		[I.5] Avería de origen físico o lógico	2	4
		[I.6] Corte del suministro eléctrico	2	3
		[I.7] Condiciones inadecuadas de temperatura y/o humedad	2	3
		[I.8] Fallo de servicios de comunicaciones	3	3
		[I.9] Interrupción de otros servicios y suministros esenciales	1	5
		[N.*] Desastres naturales	1	5
		[N.1] Fuego	1	5
		[N.2] Daños por agua	2	4

Fuente: El Autor (2023)

Tabla 3 Amenazas a los Activos de Información: Datos / Información

AMENAZAS A LOS ACTIVOS DE INFORMACION DATOS/INFORMACION				
TIPO DE ACTIVO	DESCRIPCION	AMENAZAS	FRECUENCIA	DEGRADACION E IMPACTO
DATOS / INFORMACION	COPIAS DE SEGURIDAD APLICATIVOS MISIONALES COPIAS DE SEGURIDAD DISPOSITIVOS DE RED COPIA DE SEGURIDAD DISPOSITIVOS PERIMETRALES COPIA SEGURIDAD HIS COPIA DE SEGURIDAD GESTION DOCUMENTAL COPIA DE SEGURIDAD CORREO ELECTRONICO COPIA DE SEGURIDAD INTRANET COPIA DE SEGURIDAD PAGINA WEB COPIA DE SEGURIDAD CENTRAL TELEFONICA COPIA SEGURIDAD PROYECTOS INVESTIGACION COPIA DE SEGURIDAD ARCHIVOS ALTA DIRECCION CREDENCIALES PLATAFORMAS EXTERNAS MISIONALES CÓDIGO FUENTE DE APLICATIVOS	[A.11] Acceso no autorizado	1	4
		[A.15] Modificación deliberada de la información	1	5
		[A.18] Destrucción de información	1	5
		[A.19] Revelación de información	1	4
		[E.1] Errores de los usuarios	3	2
		[E.14] Escapes de información	2	3
		[E.15] Alteración accidental de la información	1	4
		[E.18] Destrucción de información	1	5
		[E.19] Fugas de información	2	3
		[E.2] Errores del administrador	2	3
		[E.4] Errores de configuración	2	4
		[E.8] Difusión de software dañino	2	3

Fuente: El Autor (2023)

Tabla 4 Amenazas a los Activos de Información: Claves Criptográficas

AMENAZAS A LOS ACTIVOS DE INFORMACION CLAVES KRIPTOGAFICAS				
TIPO DE ACTIVO	DESCRIPCION	AMENAZAS	FRECUENCIA	DEGRADACION E IMPACTO
CLAVES KRIPTOGRAFICAS	FIRMA DIGITAL TOKEN DIGITAL CERTIFICADOS TLS/SSL PARA EL DOMINIO	[A.11] Acceso no autorizado	1	4
		[A.15] Modificación deliberada de la información	1	4
		[A.18] Destrucción de información	1	4
		[A.19] Revelación de información	1	4
		[A.6] Abuso de privilegios de acceso	1	4
		[E.1] Errores de los usuarios	2	4
		[E.15] Alteración accidental de la información	1	4
		[E.18] Destrucción de información	1	4
		[E.19] Fugas de información	1	4
		[E.2] Errores del administrador	2	3

Fuente: El Autor (2023)

Tabla 5 Amenazas a los Activos de Información: Servicios

AMENAZAS A LOS ACTIVOS DE INFORMACION SERVICIOS				
TIPO DE ACTIVO	DESCRIPCION	AMENAZAS	FRECUENCIA	DEGRADACION E IMPACTO
SERVICIOS	CORREO ELECTRÓNICO INSTITUCIONAL CARPETAS COMPARTIDAS PÁGINA WEB INSTITUCIONAL GESTIÓN DE ROLES Y RESTRICCIÓN DE PRIVILEGIOS EN HIS Y APLICATIVOS INSTITUCIONALES	[A.11] Acceso no autorizado	2	4
		[A.12] Análisis de tráfico	2	4
		[A.14] Interceptación de información (escucha)	1	4
		[A.15] Modificación deliberada de la información	2	4
		[A.19] Revelación de información	1	4
		[A.24] Denegación de servicio	2	4
		[A.6] Abuso de privilegios de acceso	1	4
		[A.7] Uso no previsto	2	2
		[E.1] Errores de los usuarios	3	1
		[E.19] Fugas de información	2	3
		[E.2] Errores del administrador	2	3
		[E.9] Errores de [re-]encaminamiento	1	2
		[I.8] Fallo de servicios de comunicaciones	3	3

Fuente: El Autor (2023)

Tabla 6 Amenazas a los activos de información: Software/Aplicaciones Informáticas

AMENAZAS A LOS ACTIVOS DE INFORMACION SOFTWARE APLICACIONES INFORMATICAS				
TIPO DE ACTIVO	DESCRIPCION	AMENAZAS	FRECUENCIA	DEGRADACION E IMPACTO
SOFTWARE APLICACIÓNES INFORMATICAS	HIS, HIPERVISORES, SERVIDOR Y CLIENTE DE CORREO, MOTORES DE BASES DE DATOS, SISTEMAS OPERATIVOS, ANTIVIRUS, OFIMÁTICA, APLICATIVOS MISIONALES, PLATAFORMAS MISIONALES, VISORES IMAGENOLOGIA, INTRANET, MESA DE AYUDA, PLATAFORMAS GESTION EQUIPAMENTO DE RED, DOMOTICA, APLICACIONES WEB, SOFTWARE EQUIPOS BIOMEDICOS Y DE LABORATORIO, SOFTWARE PLATAFORMAS CARGUE DE INFORMACIÓN A EPS, SOFTWARE DE GESTIÓN DOCUMENTAL.	[A.11] Acceso no autorizado	1	5
		[A.18] Destrucción de información	1	5
		[A.19] Revelación de información	1	4
		[A.22] Manipulación de programas	1	4
		[A.4] Manipulación de la configuración	1	4
		[A.5] Suplantación de la identidad del usuario	1	4
		[A.6] Abuso de privilegios de acceso	1	4
		[A.7] Uso no previsto	2	4
		[A.8] Difusión de software dañino	1	4
		[E.1] Errores de los usuarios	3	3
		[E.18] Destrucción de información	1	5
		[E.19] Fugas de información	2	4
		[E.2] Errores del administrador	3	3
		[E.20] Vulnerabilidades de los programas (software)	3	3
		[E.4] Errores de configuración	3	3
		[E.8] Difusión de software dañino	3	3
		[I.5] Avería de origen físico o lógico	3	4

Fuente: El Autor (2023)

Tabla 7 Amenazas a los activos de información: Equipos (Hardware)

AMENAZAS A LOS ACTIVOS DE INFORMACION: EQUIPOS INFORMATICOS (HARDWARE)				
TIPO DE ACTIVO	DESCRIPCION	AMENAZAS	FRECUENCIA	DEGRADACION E IMPACTO
EQUIPOS INFORMATICOS (HARDWARE)	SERVIDORES, WORKSTATION, DESKTOP, LAPTOP, SMARTPHONES, TABLETAS, NAS, SAN, IMPRESORAS, SCANNER, LECTORES CÓDIGO BARRAS, HUELLEROS, SWITCH CORE, MODEM INTERNET,	[A.11] Acceso no autorizado	1	4
		[A.23] Manipulación de los equipos	1	4
		[A.24] Denegación de servicio	1	5
		[A.25] Robo	2	4
		[A.26] Ataque destructivo	1	5
		[A.5] Suplantación de la identidad del usuario	1	4
		[A.6] Abuso de privilegios de acceso	1	4
		[A.7] Uso no previsto	1	5

Tabla 7 (Continuación)

EQUIPOS INFORMATICOS (HARDWARE)	, PLANTA TELEFÓNICA, GATEWAY TELEFONÍA IP, TELÉFONOS IP, FIREWALL, AP, DOMOTICA, CÁMARAS IP, DVR-IP CCTV, SMART TV, SISTEMAS RFID, EQUIPOS BIOMÉDICOS, LLAMADOS ENFERMERIA, DIGITURNOS, IoT, IoMT.	[A.11] Acceso no autorizado	1	4
		[A.23] Manipulación de los equipos	1	4
		[A.24] Denegación de servicio	1	5
		[A.25] Robo	2	4
		[A.26] Ataque destructivo	1	5
		[A.5] Suplantación de la identidad del usuario	1	4
		[A.6] Abuso de privilegios de acceso	1	4
		[A.7] Uso no previsto	1	5
		[E.2] Errores del administrador	2	3
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	3
		[E.24] Caída del sistema por agotamiento de recursos	3	3
		[E.25] Perdida de Equipos	2	4
		[E.4] Errores de configuración	3	3
		[I.*] Desastres industriales	1	5
		[I.11] Emanaciones electromagnéticas	1	4
		[I.3] Contaminación mecánica	2	3
		[I.4] Contaminación electromagnética	2	2
		[I.5] Avería de origen físico o lógico	2	4
		[I.6] Corte del suministro eléctrico	2	3
		[I.7] Condiciones inadecuadas de temperatura y/o humedad	2	3
		[I.8] Fallo de servicios de comunicaciones	3	3
		[I.9] Interrupción de otros servicios y suministros esenciales	1	5
		[N.*] Desastres naturales	1	5
		[N.1] Fuego	1	5
		[N.2] Daños por agua	2	4

Fuente: El Autor. (2023)

Tabla 8 Amenazas a los activos de información: Redes de Comunicaciones

AMENAZAS A LOS ACTIVOS DE INFORMACION: REDES DE COMUNICACIONES				
TIPO DE ACTIVO	DESCRIPCION	AMENAZAS	FRECUENCIA	DEGRADACION E IMPACTO
REDES DE COMUNICACIONES	CANAL E1 DE VOZ CANAL DEDICADO INTERNET FIBRA ÓPTICA PRINCIPAL Y RESPALDO (WAN) ANTENAS DE COMUNICACIONES DE RADIO (AMBULANCIAS Y RADIOS)	[A.11] Acceso no autorizado	1	4
		[A.23] Manipulación de los equipos	1	4
		[A.24] Denegación de servicio	1	5
		[A.26] Ataque destructivo	1	5
		[A.5] Suplantación de la identidad del usuario	1	4
		[A.6] Abuso de privilegios de acceso	1	4

Tabla 8 (Continuación)

REDES DE COMUNICACIONES	RED DE DATOS Y VOZ TELEFONÍA MÓVIL, RADIO ENLACE	[A.7] Uso no previsto	1	5
		[I.*] Desastres industriales	1	5
		[I.4] Contaminación electromagnética	1	4

Fuente. El Autor (2023)

Tabla 9 Amenazas a los activos de información: Soportes de información

AMENAZAS A LOS ACTIVOS DE INFORMACION: SOPORTES DE INFORMACION				
TIPO DE ACTIVO	DESCRIPCION	AMENAZAS	FRECUENCIA	DEGRADACION E IMPACTO
SOPORTES DE INFORMACION	CLOUD, DISCOS DUROS FÍSICOS, DISCOS DUROS VIRTUALES, NAS, SAN, DISCOS DUROS EXTERNOS, MEMORIAS USB, ALMACENAMIENTO EN RED, DVD, TARJETAS DE MEMORIA, TARJETAS INTELIGENTES, MATERIAL IMPRESO.	[A.11] Acceso no autorizado	1	4
		[A.23] Manipulación de los equipos	1	4
		[A.24] Denegación de servicio	1	5
		[A.26] Ataque destructivo	1	5
		[A.5] Suplantación de la identidad del usuario	1	4
		[A.6] Abuso de privilegios de acceso	1	4
		[A.7] Uso no previsto	1	5
		[I.5] Avería de origen físico o lógico	2	4
		[A.25] Robo	2	4

Fuente: El Autor (2023)

Tabla 10 Amenazas a los activos de información: Equipamiento Auxiliar

AMENAZAS A LOS ACTIVOS DE INFORMACION: EQUIPAMENTO AUXILIAR				
TIPO DE ACTIVO	DESCRIPCION	AMENAZAS	FRECUENCIA	DEGRADACION E IMPACTO
EQUIPAMENTO AUXILIAR	RED ELECTRICA REGULADA, UPS, PLANTA ELECTRICA, AIRES ACONDICIONADOS, CABLEADO DE AREA PARA DATOS Y RED ELECTRICA, BACKBONE FIBRA, RACKS DE COMUNICACIONES	[A.11] Acceso no autorizado	1	5
		[A.24] Denegación de servicio	1	5
		[A.26] Ataque destructivo	1	5
		[A.7] Uso no previsto	1	5
		[I.*] Desastres industriales	1	5
		[I.9] Interrupción de otros servicios y suministros esenciales	1	5
		[N.*] Desastres naturales	1	5
		[N.1] Fuego	1	5

Fuente: El Autor (2023)

Tabla 11 Amenazas a los activos de información: Instalaciones

AMENAZAS A LOS ACTIVOS DE INFORMACION: INSTALACIONES				
TIPO DE ACTIVO	DESCRIPCION	AMENAZAS	FRECUENCIA	DEGRADACION E IMPACTO
INSTALACIONES	DATA CENTER CENTROS DE CABLEADO Y DATOS CUARTOS ELECTRICOS CENTRAL ELECTROGENA CENTRAL TELEFONICA	[A.26] Ataque destructivo	1	5
		[I.*] Desastres industriales	1	5
		[I.9] Interrupción de otros servicios y suministros esenciales	1	5
		[N.*] Desastres naturales	1	5
		[N.1] Fuego	1	5

Fuente: El Autor (2023)

Tabla 12 Amenazas a los activos de información: Personal

AMENAZAS A LOS ACTIVOS DE INFORMACION: PERSONAL				
TIPO DE ACTIVO	DESCRIPCION	AMENAZAS	FRECUENCIA	DEGRADACION E IMPACTO
PERSONAL	USUARIOS INTERNOS: FUNCIONARIOS. COORDINACIÓN TI, DBA, PROFESIONALES CONTRATISTAS TICS, TÉCNICOS OPERATIVOS. PROVEEDORES DE SERVICIOS TECNOLOGICOS TERCERIZADOS	[A.28] Indisponibilidad del personal	3	2
		[A.29] Extorsión	1	4
		[A.30] Ingeniería social	3	2
		[A.6] Abuso de privilegios de acceso	3	2
		[A.7] Uso no previsto	3	2
		[E.19] Fugas de información	3	3
		[E.21] Errores de mantenimiento / actualización de programas (software)	3	4
		[E.28] Indisponibilidad del personal	2	2
		[E.7] Deficiencias en la organización	4	4

Fuente: El Autor (2023)

Al hacer la evaluación de las amenazas que puedan afectar a un activo, se consideraron dos aspectos importantes: la degradación o impacto que sufriría el activo en caso de que ocurra un incidente, y la probabilidad o frecuencia de que la amenaza se materialice.

Para efectos de este proyecto, se realizó esta evaluación teniendo en cuenta la frecuencia, definida como cada cuanto se materializa un incidente y la degradación o impacto, lo que se entiende como que tanto resultaría degradado el activo, si la amenaza se materializa.

7.2 EVALUACION DE AMENAZAS SOBRE LOS ACTIVOS DE INFORMACION

Este capítulo proporciona una visión integral de cómo se analizan, cuantifican y enfrentan las amenazas para proteger los activos de información más relevantes de los hospitales públicos en Colombia.

Este aparte del proyecto se centra en la evaluación de las amenazas que afectan los activos de información críticos. Este proceso implica una valoración tanto cualitativa como cuantitativa de dichos activos, así como la identificación de las amenazas que podrían impactarlos, lo que es fundamental para determinar los riesgos más significativos que enfrentan estos activos. Igualmente se aborda la identificación de controles destinados a mitigar los riesgos con mayor impacto. Estos controles se diseñan y aplican estratégicamente para reducir la probabilidad de ocurrencia de las amenazas y minimizar su impacto en los activos de información crítica.

7.2.1 Valoración de los activos de información.

La valoración cuantitativa de los activos de información se realiza utilizando una escala numérica del 0 al 10, lo que proporciona un método claro y objetivo para evaluar el riesgo asociado a la pérdida de dichos activos.

Esta valoración se basa en las dimensiones fundamentales de confidencialidad, integridad y disponibilidad, asignando un valor a criterio del daño según sea la afectación del activo en cada una de las dimensiones.

Al seguir estas pautas de valoración, se puede mantener el enfoque en los activos más críticos y de mayor valor para las instituciones. En este caso específico, se ha establecido que los activos que califican con un valor total igual o superior a 25 puntos son considerados para la muestra que se trabaja en este proyecto aplicado.

Para una mejor comprensión, se ilustra a continuación los rangos de valoración y el criterio correspondiente para la clasificación de los activos, según la metodología Magerit:

Ilustración 10 Criterio valoración cuantitativa de activos

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

Fuente: Magerit V3 (2012). Libro 2. p. 75

De esta manera se propone como alternativa, esta valoración cuantitativa de los activos de información, con el fin de identificar y priorizar los activos más críticos, enfocando los esfuerzos y recursos en proteger aquellos que representan mayor riesgo para la institución.

El siguiente cuadro representa la valoración cuantitativa de los activos de información de acuerdo con lo establecido en la teoría anterior.

Cuadro 16 Activos de información: valoración cuantitativa

VALORACION DE ACTIVOS DE INFORMACION						
TIPO DE ACTIVO MAGERIT	**ACTIVO**	**DESCRIPCION**	**VALORACION**			**VALORACION TOTAL DEL ACTIVO**
			C	**I**	**D**	
ACTIVOS ESENCIALES	BASES DE DATOS	DB HISTORIA CLINICA – BD IMAGENES DIAGNOSTICAS – BD CONFIGURACION EQUIPOS DE RED Y SEGURIDAD PERIMETRAL -BD INFORMACION FINANCIERA	10	10	10	30
	DATOS DE ACCESO	CREDENCIALES DE ACCESO A SERVIDORES Y EQUIPAMIENTO.	10	10	10	30
ARQUITECTURA DEL SISTEMA	SERVIDORES WEB PLATAFORMAS EXTERNAS SISTEMA DE INFORMACION MINSALUD HIS SERVIDORES RED DE VOZ Y DATOS APLICATIVOS MISIONALES PLATAFORMAS ENTES DE CONTROL PLATAFORMAS EPS INTERNET – TELEVISION – TELEFONIA RED ELECTRICA SERVICIOS DE MANTENIMIENTO TERCERIZADOS SERVICIOS DE SALUD ESPECIALIZADOS TERCERIZADOS	SISTEMAS DE INFORMACION DEL MINISTERIO DE SALUD (MIPRES, RUAF, SISPRO, etc) SISTEMA DE INFORMACION HOSPITALARIA INFRAESTRUCTURA DE RED Y SERVIDORES TELECOMUNICACIONES MANTENIMIENTO	8	8	9	25
DATOS / INFORMACION	COPIAS DE SEGURIDAD ARCHIVOS DE USUARIO	COPIA BASE DE DATOS MISIONALES (HIS) - CONFIGURACION DE DISPOSITIVOS DE ACCESO A RED - PROYECTOS DE INVESTIGACION - ARCHIVOS DE USUARIO ALTA DIRECCION Y GESTION FINANCIERA - GESTION DOCUMENTAL - IMAGENES DIAGNOSTICAS -CODIGO FUENTE - CONTRASEÑAS	9	9	10	28
CLAVES KRIPTOGRAFICAS	Certificados SSL TOKEN	SSL PARA DOMINIO Y SUB DOMINIOS. TOKEN DE ACCESO A PORTALES MISIONALES O APLICACIONES FINANCIERAS	7	7	7	21
SERVICIOS	NAS Pagina Web	DIRECTORIOS COMPARTIDOS - REPOSITORIOS DE ALMACENAMIENTO - NUBE LOCAL - PAGINA WEB INSTITUCIONAL - INTRANET - CORREO ELECTRONICO	7	9	9	25

Cuadro 16 (Continuación)

SOFTWARE APLICACIÓNES INFORMATICAS	LICENCIAS DE SOFTWARE COMERCIALES, APLICACIONES DE TERCEROS Y DESARROLLOS PROPIOS	APLICACIONES MISIONALES: PROPIAS Y DE TERCEROS. APLICACIONES PARA DIAGNOSTICOS PLATAFORMAS MinSALUD SOFTWARE DE GESTION Y MANTENIMIENTO. HYPERVISORES MOTORES DE BASES DE DATOS OFIMATICA ANTIVIRUS CLOUD BACKUPS SISTEMAS OPERATIVOS SOFTWARE PARA COPIAS DE SEGURIDAD	6	8	8	22
EQUIPOS INFORMATICOS HARDWARE	INFORMATICA PERSONAL INFORMATICA MOVIL SERVIDORES PERIFERICOS DISPOSITIVOS DE RED TELEFONIA IP ALMACENAMIENTO EQUIPOS BIOMEDICOS CCTV SISTEMA CONTROL DE ACCESO FIREWALL	COMPUTADORES CORPORATIVOS DE ESCRITORIO Y PORTATILES SERVIDORES FISICOS Y VIRTUALIZADOS SAN DE ALMACENAMIENTO IMPRESORAS Y ESCANER EN RED TABLETS SMARTPHONES SMART TV SWITCH CORE, AP, CONTROLADORAS TOMOGRAFO, RESONADOR, ACELERADOR LINEAL, EQUIPOS DE RX, BOMBAS DE INFUSION, EQUIPOS DE LABORATORIO, PACS PLANTA TELEFONICA IP DVR-IP RFID SEGURIDAD PERIMETRAL	7	7	9	23
REDES DE COMUNICACIONES	CANAL E1 DE VOZ TELEFONIA CELULAR CANAL INTERNET PRINCIPAL Y RESPALDO	RED DE VOZ INTERNA COMUNICACIÓN CELUAR ACCESO A INTERNET EN ALTA DISPONIBILIDAD	9	7	9	25
SOPORTES DE INFORMACION	ALMACENAMIENTO DE INFORMACION DIGITAL O FISICA	DISCOS DUROS - MEMORIAS USB - NAS ARCHIVO DOCUMENTAL FISICO	8	8	9	25
EQUIPAMENTO AUXILIAR	FUENTES DE ALIMENTACION ELECTRICA - CABLEADO ESTRUCTURADO VOZ Y DATOS -	UPS - PLANTAS ELECTRICAS - SISTEMAS DE AIRE ACONDICIONADO - RED DE DATOZ Y DE VOZ - BACKBONE DE FIBRA - RED ELECTRICA REGULADA	6	7	10	23
INSTALACIONES	CUARTO TECNICO	DATACENTER - RACK DE COMUNICACIONES	8	8	8	24
PERSONAL	PERSONAL RELACIONADO CON LOS SISTEMAS DE INFORMACION	PERSONAL DE SOPORTE TECNICO PERSONAL DE DESARROLLO DE SOFTWARE ADMINISTRADOR BASE DE DATOS PROVEEDORES O TERCEROS DE SEGURIDAD	9	8	9	26

Fuente: El Autor (2023).

Por otro lado, se propone una herramienta para quienes opten por una valoración cualitativa de los activos de información, que se basa en los criterios: No Aplica, Bajo, Medio y Alto, para efectos de proporcionar una explicación más detallada del criterio de valoración en términos de Confidencialidad, Integridad y Disponibilidad. Con este entendido, se propone una valoración dada en la versión 2022 de la Guía de Seguridad de las TIC CCN-STIC 803, elaborada por el Ministerio de Defensa y el Centro Criptológico Nacional del Gobierno Español[40]. Esta guía establece criterios comunes que pueden aplicarse a diversas entidades, independientemente de su naturaleza, tamaño o características específicas.

El objetivo es adaptar estos criterios al entorno específico de una entidad de salud pública de nivel territorial. Al recurrir a esta guía, se garantiza un enfoque sólido y adaptado a las necesidades de seguridad de las instituciones de salud objeto de este proyecto aplicado.

La siguiente tabla presenta los criterios de valoración cualitativa para los activos de información, dados en la Guía de Seguridad de las TIC CCN-STIC 803.

Tabla 13 Criterios de valoración según la guía de seguridad TIC CCN STIC 803

CRITERIOS COMUNES APLICABLES A TODAS LAS DIMENSIONES DE TIPOS DE INFORMACIÓN Y SERVICIOS				
	No Adscrito (N/A)	**BAJO**	**MEDIO**	**ALTO**
Pérdidas económicas	COM.ECO.N No implica pérdidas económicas.	COM.ECO.B Pérdidas económicas apreciables (no superiores al 4% del presupuesto anual de la organización).	COM.ECO.M Pérdidas económicas importantes (superiores al 4% e inferiores al 10% del presupuesto anual de la organización).	COM.ECO.A Pérdidas económicas o alteraciones financieras significativas (superiores al 10% del presupuesto anual de la organización).
Reputación	COM.REP.N No implica daño reputacional.	COM.REP.B Daño reputacional moderado con los ciudadanos o con otras organizaciones.	COM.REP.M Daño reputacional significativo con los ciudadanos o con otras organizaciones.	COM.REP.A Daño reputacional grave con los ciudadanos o con otras organizaciones.

[40] CENTRO CRIPTOLÓGICO NACIONAL. CCN STIC 803: Valoración de sistemas en el ENS. Madrid. (2020). 48 p. Guía del Esquema Nacional de Seguridad, n. 803. Disponible en: https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/682-ccn-stic-803-valoracion-de-sistemas-en-el-ens-1/file.html . Consultado octubre 2023.

Tabla 13 (Continuación)

Protestas	COM.PRO.N No se prevé que pueda desembocar en protestas.	COM.PRO.B Múltiples protestas individuales.	COM.PRO.M Protestas públicas (alteración del orden público).	COM.PRO.A Protestas masivas (alteración seria del orden público).
Delitos	COM.DEL.N No facilitaría la comisión de delitos ni dificultaría su investigación.	COM.DEL.B Favorecería la comisión de delitos.	COM.DEL.M Favorecería significativamente la comisión de delitos o dificultaría su investigación.	COM.DEL.A Podría incitar a la comisión de delitos, constituiría en sí un delito, o dificultaría enormemente su investigación.
Disposición legal o administrativa	COM.DIS.N No existe ninguna disposición legal o administrativa que condicione su nivel.	COM.DIS.B Por disposición legal o administrativa: ley, decreto, orden, resolución…	COM.DIS.M Por disposición legal o administrativa: ley, decreto, orden, resolución…	COM.DIS.A Por disposición legal o administrativa: ley, decreto, orden, resolución…
Perjuicio Directo al ciudadano (de cualquier índole)	COM.PER.N No supone ningún perjuicio directo al ciudadano.	COM.PER.B Algún perjuicio.	COM.PER.M Daño importante, aunque subsanable.	COM.PER.A Grave daño, de difícil o imposible reparación.
Incumplimiento de una Norma Legal o administrativa	COM.LEG.N No implica incumplimiento de una norma jurídica.	COM.LEG.B Incumplimiento formal leve de una norma jurídica, de carácter subsanable.	COM.LEG.M Incumplimiento material de una norma jurídica, o incumplimiento formal no subsanable.	COM.LEG.A Incumplimiento formal y material grave de una norma jurídica.
Incumplimiento de una Norma Regulatoria	COM.REG.N No implica incumplimiento de normativa de un regulador.	COM.REG.B Implica incumplimiento de normativa de un regulador.	COM.REG.M Implica sanción significativa de un regulador.	COM.REG.A Implica sanción grave de un regulador y/o pérdida de licencia de operar.
Incumplimiento de una Norma Contractual	COM.CON.N No implica incumplimiento de una obligación contractual.	COM.CON.B Incumplimiento formal leve de una obligación contractual.	COM.CON.M Incumplimiento material o formal de una obligación contractual.	COM.CON.A Incumplimiento formal o material grave de una obligación contractual.
Incumplimiento de una Norma Interna	COM.INT.N No implica incumplimiento de normativa interna.	COM.INT.B Incumplimiento formal leve de una norma interna.	COM.INT.M Incumplimiento material o formal de una norma interna.	COM.INT.A Incumplimiento formal o material grave de una norma interna.

Fuente: CENTRO CRIPTOLÓGICO NACIONAL. CCN STIC 803: Valoración de sistemas en el ENS [en línea]. Madrid: Centro Criptológico Nacional. 2020. p. 10. Disponible en: https://www.ccn-cert.cni.es/ . Consultado: noviembre de 2023.

Teniendo claras las anteriores propuestas para la valoración de los activos de información, regresamos al enfoque principal de este proyecto, que está dirigido hacia los activos que han sido calificados con más de 25 puntos, priorizando su protección debido a su alta valoración del riesgo asociado.

7.2.2 Valoración de amenazas y nivel de riesgo frente a los activos de información.

Siguiendo la metodología Magerit, a continuación se presenta el proceso de valoración de amenazas asociado a estos activos, identificando y evaluando su impacto potencial, implementando medidas de seguridad y mitigación de riesgos específicos para garantizar su protección. Sin embargo, es importante destacar que esto no significa descuidar los demás activos, ya que todos ellos son relevantes y requerirán una valoración y protección acorde a su importancia relativa y los recursos disponibles a futuro; esto se lograría realizando un seguimiento anual y actualizando del inventario de activos de información, dando nuevas calificaciones a los mismos, teniendo en cuenta los riesgos ya mitigados con los controles propuestos y los resultados obtenidos.

Para la evaluación de cada amenaza se propone apoyarse en la siguiente tabla, donde se encuentra un comparativo entre la valoración cualitativa y cuantitativa, en términos de frecuencia y degradación o impacto. Entiéndase por Frecuencia la cantidad de incidentes ocurridos en una línea de tiempo y por degradación o impacto, el nivel de daño que puede sufrir el activo de información evaluado si la amenaza llega a materializarse.

Tabla 14 Criterios de Frecuencia y Degradación o Impacto.

FRECUENCIA	DESCRIPCION	IMPACTO O DEGRADACION	DESCRIPCION
5	A Diario	5	Totalmente Degradado
4	Mensual	4	Altamente Degradado
3	Una vez al año	3	Medianamente Degradado
2	Cada Varios años	2	Mínimamente Degradado
1	Nunca hasta el momento	1	No Degradado

Fuente: El Autor (2023)

Con estos criterios se proporciona la base para calificar el nivel de riesgo asociado a cada amenaza evaluada, tema que se tratara a continuación.

7.2.2.1 Determinación del riesgo**.** La norma ISO/IEC 27000 define el riesgo como la combinación de la probabilidad de ocurrencia de un evento y sus consecuencias[41]. En el contexto de la seguridad de la información, el riesgo se refiere a la posibilidad de que se produzcan incidentes que afecten la confidencialidad, integridad y disponibilidad de los activos de información.

El riesgo informático tiene un impacto significativo en todos los aspectos de una institución, especialmente en el contexto de la sensibilidad de la información manejada por una institución de salud. Las consecuencias de no mitigar este riesgo pueden ser graves por lo que es fundamental abordar este riesgo de manera proactiva.

Se propone hacer un análisis cuantitativo con el fin de facilitar el cálculo, cuya formula la compone:

$$Riesgo = Vr.Frecuencia\ Amenaza * Vr.Degradacion\ o\ Impacto$$

De esta manera se obtiene el valor del riesgo y se lo puede clasificar en una escala, donde su nivel estará acorde al tratamiento correspondiente, como se indica en la tabla No. 15 (Escala y Valor del Riesgo), así:

[41] ISO27000. Glosario: Lista de términos relacionados con la serie ISO 27000 y la seguridad de la información [en linea]. Madrid: ISO27000. 2020. Disponible en: https://www.iso27000.es/glosario.html . Consultado: noviembre de 2023.

Tabla 15 Escala y Valor del Riesgo

VALOR DEL RIESGO	NIVEL		TRATAMIENTO
16-25	1	Riesgos muy probables y de muy alto impacto	La gestión del riesgo implica tomar medidas preventivas, de protección y la posibilidad de compartir o transferir el riesgo mediante pólizas de seguros. Es importante priorizar la acción de sacar los riesgos de la zona de mayor peligro.
10-15	2	Situaciones improbables y de impacto medio, hasta situaciones muy probables, pero de impacto bajo o muy bajo	La organización tiene diversas opciones para gestionar el riesgo, como reducirlo, compartirlo o transferirlo. Es importante que se diseñen planes de contingencia para protegerse en caso de que los riesgos se materialicen.
6-9	3	Riesgos improbables y de bajo impacto	La gestión del riesgo implica tomar decisiones entre dejar los riesgos como están o permitir que aumenten si eso proporciona alguna ventaja o beneficio en otra área. Para tomar la decisión de aceptar el riesgo, es necesario realizar un análisis de costo-beneficio que permita decidir entre asumir el riesgo o compartirlo.
0-5	4	Riesgos improbables, pero de muy alto impacto	El desafío en estos casos es la toma de decisiones, ya que la baja probabilidad de ocurrencia no justifica la implementación de medidas preventivas. Sin embargo, dado el alto impacto potencial, es necesario contar con planes de acción para reaccionar y limitar el daño en caso de que ocurra el riesgo. En este sentido, es importante enfocarse en medidas de respuesta y recuperación ante posibles desastres.

Fuente. El Autor. (2023).

Teniendo en cuenta la escala dada en la tabla anterior, se presenta un consolidado con los valores más altos, según el resultado de la calificación del riesgo de los activos de información en el presente proyecto. Esta información será fundamental, para tomar decisiones informadas sobre las medidas de seguridad a implementar y así garantizar la protección efectiva de los activos de información que más alto riesgo asociado tienen.

Tabla 16 Valoración de amenazas y riesgo asociado frente a los activos de información esenciales.

VALORACION DE AMENAZAS EN LOS ACTIVOS DE INFORMACION ESENCIALES					
TIPO DE ACTIVO	DESCRIPCION	AMENAZAS	FRECUENCIA	DEGRADACION E IMPACTO	VALOR DEL RIESGO
ACTIVOS ESENCIALES	HIS (SISTEMA DE INFORMACION HOSPITALARIO) BASE DE DATOS DEL HIS INFRAESTRUCTURA DE RED: SEGURIDAD	[A.11] Acceso no autorizado	1	5	5
		[A.15] Modificación deliberada de la información	1	5	5
		[A.18] Destrucción de información	1	5	5
		[A.19] Revelación de información	1	4	4
		[E.14] Escapes de información	2	3	6

Tabla 16 (Continuación)

ACTIVOS ESENCIALES	PERIMETRAL, SWITCH CORE – SERVICIO DHCP/DNS – CONTROLADORAS WiFi SOFTWARE MISIONAL: RESULTADO A PROCEDIMIENTOS, LABORATORIOS, IMÁGENES DIAGNOSTICAS ARCHIVOS DE USUARIO: RESOLUCIONES, ACTAS, ACUERDOS. ACCESO A INTERNET	[E.15] Alteración accidental de la información	1	4	4
		[E.18] Destrucción de información	1	5	5
		[E.21] Errores de mantenimiento / actualización de programas (software)	2	3	6

Fuente: El Autor (2023)

Tabla 17 Valor del riesgo asociado a los activos de información arquitectura del sistema

VALOR DEL RIESGO EN LOS ACTIVOS DE INFORMACION ARQUITECTURA DEL SISTEMA					VALOR DEL RIESGO
TIPO DE ACTIVO	DESCRIPCION	AMENAZAS	FRECUENCIA	DEGRADACION E IMPACTO	
ARQUITECTURA DEL SISTEMA	HIS SERVIDORES RED DE VOZ Y DATOS APLICATIVOS MISIONALES PLATAFORMAS ENTES DE CONTROL PLATAFORMAS MINSALUD PLATAFORMAS EPS INTERNET – TELEVISION – TELEFONIA RED ELECTRICA SERVICIOS DE MANTENIMIENTO TERCERIZADOS SERVICIOS DE SALUD ESPECIALIZADOS TERCERIZADOS	[A.11] Acceso no autorizado	1	4	4
		[A.23] Manipulación de los equipos	1	4	4
		[A.24] Denegación de servicio	1	5	5
		[A.25] Robo	2	4	8
		[A.26] Ataque destructivo	1	5	5
		[A.5] Suplantación de la identidad del usuario	1	4	4
		[A.6] Abuso de privilegios de acceso	1	4	4
		[A.7] Uso no previsto	1	5	5
		[E.2] Errores del administrador	2	3	6
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	3	9
		[E.24] Caída del sistema por agotamiento de recursos	3	3	9
		[E.25] Perdida de Equipos	2	4	8
		[E.4] Errores de configuración	3	3	9
		[I.*] Desastres industriales	1	5	5
		[I.11] Emanaciones electromagnéticas	1	4	4
		[I.3] Contaminación mecánica	2	3	6

Tabla 17 (Continuación)

ARQUITECTURA DEL SISTEMA		[I.4] Contaminación electromagnética	2	2	4
		[I.5] Avería de origen físico o lógico	2	4	8
		[I.6] Corte del suministro eléctrico	2	3	6
		[I.7] Condiciones inadecuadas de temperatura y/o humedad	2	3	6
		[I.8] Fallo de servicios de comunicaciones	3	3	9
		[I.9] Interrupción de otros servicios y suministros esenciales	1	5	5
		[N.*] Desastres naturales	1	5	5
		[N.1] Fuego	1	5	5
		[N.2] Daños por agua	2	4	8

Fuente: El Autor (2023)

Tabla 18 Valor del riesgo asociado a los activos de información Datos

VALOR DEL RIESGO EN LOS ACTIVOS DE INFORMACION DATOS/INFORMACION					VALOR DEL RIESGO
TIPO DE ACTIVO	DESCRIPCION	AMENAZAS	FRECUENCIA	DEGRADACION E IMPACTO	
DATOS / INFORMACION	COPIAS DE SEGURIDAD APLICATIVOS MISIONALES COPIAS DE SEGURIDAD DISPOSITIVOS DE RED COPIA DE SEGURIDAD DISPOSITIVOS PERIMETRALES COPIA SEGURIDAD HIS COPIA DE SEGURIDAD GESTION DOCUMENTAL COPIA DE SEGURIDAD CORREO ELECTRONICO COPIA DE SEGURIDAD INTRANET COPIA DE SEGURIDAD PAGINA WEB COPIA DE SEGURIDAD CENTRAL TELEFONICA COPIA SEGURIDAD PROYECTOS INVESTIGACION COPIA DE SEGURIDAD ARCHIVOS ALTA DIRECCION CREDENCIALES PLATAFORMAS EXTERNAS MISIONALES CÓDIGO FUENTE DE APLICATIVOS	[A.11] Acceso no autorizado	1	4	4
		[A.15] Modificación deliberada de la información	1	5	5
		[A.18] Destrucción de información	1	5	5
		[A.19] Revelación de información	1	4	4
		[E.1] Errores de los usuarios	3	2	6
		[E.14] Escapes de información	2	3	6
		[E.15] Alteración accidental de la información	1	4	4
		[E.18] Destrucción de información	1	5	5
		[E.19] Fugas de información	2	3	6
		[E.2] Errores del administrador	2	3	6
		[E.4] Errores de configuración	2	4	8
		[E.8] Difusión de software dañino	2	3	6

Fuente: El Autor (2023)

Tabla 19 Valor del riesgo asociado a los activos de información Claves Kriptográficas

VALOR DEL RIESGO EN LOS ACTIVOS DE INFORMACION CLAVES KRIPTOGAFICAS					VALOR DEL RIESGO
TIPO DE ACTIVO	DESCRIPCION	AMENAZAS	FRECUENCIA	DEGRADACION E IMPACTO	
CLAVES KRIPTOGRAFICAS	FIRMA DIGITAL TOKEN DIGITAL CERTIFICADOS TLS/SSL PARA EL DOMINIO	[A.11] Acceso no autorizado	1	4	4
		[A.15] Modificación deliberada de la información	1	4	4
		[A.18] Destrucción de información	1	4	4
		[A.19] Revelación de información	1	4	4
		[A.6] Abuso de privilegios de acceso	1	4	4
		[E.1] Errores de los usuarios	2	4	8
		[E.15] Alteración accidental de la información	1	4	4
		[E.18] Destrucción de información	1	4	4
		[E.19] Fugas de información	1	4	4
		[E.2] Errores del administrador	2	3	6

Fuente: El Autor (2023)

Tabla 20 Valor del riesgo asociado a los activos de información Servicios

VALOR DEL RIESGO EN LOS ACTIVOS DE INFORMACION SERVICIOS					VALOR DEL RIESGO
TIPO DE ACTIVO	DESCRIPCION	AMENAZAS	FRECUENCIA	DEGRADACION E IMPACTO	
SERVICIOS	CORREO ELECTRÓNICO INSTITUCIONAL CARPETAS COMPARTIDAS PÁGINA WEB INSTITUCIONAL GESTIÓN DE ROLES Y RESTRICCIÓN DE PRIVILEGIOS EN HIS Y APLICATIVOS INSTITUCIONALES	[A.11] Acceso no autorizado	2	4	8
		[A.12] Análisis de tráfico	2	4	8
		[A.14] Interceptación de información (escucha)	1	4	4
		[A.15] Modificación deliberada de la información	2	4	8
		[A.19] Revelación de información	1	4	4
		[A.24] Denegación de servicio	2	4	8
		[A.6] Abuso de privilegios de acceso	1	4	4
		[A.7] Uso no previsto	2	2	4
		[E.1] Errores de los usuarios	3	1	3
		[E.19] Fugas de información	2	3	6
		[E.2] Errores del administrador	2	3	6
		[E.9] Errores de [re-]encaminamiento	1	2	2
		[I.8] Fallo de servicios de comunicaciones	3	3	9

Fuente: El Autor (2023)

Tabla 21 Valor del riesgo asociado a los activos de información Software

VALOR DEL RIESGO EN LOS ACTIVOS DE INFORMACION SOFTWARE APLICACIONES INFORMATICAS					VALOR DEL RIESGO
TIPO DE ACTIVO	DESCRIPCION	AMENAZAS	FRECUENCIA	DEGRADACION E IMPACTO	
SOFTWARE APLICACIÓNES INFORMATICAS	HIS, HIPERVISORES, SERVIDOR Y CLIENTE DE CORREO, MOTORES DE BASES DE DATOS, SISTEMAS OPERATIVOS, ANTIVIRUS, OFIMÁTICA, APLICATIVOS MISIONALES, PLATAFORMAS MISIONALES, VISORES IMAGENOLOGIA, INTRANET, MESA DE AYUDA, PLATAFORMAS GESTION EQUIPAMENTO DE RED, DOMOTICA, APLICACIONES WEB, SOFTWARE EQUIPOS BIOMEDICOS Y DE LABORATORIO, SOFTWARE PLATAFORMAS CARGUE DE INFORMACIÓN A EPS, SOFTWARE DE GESTIÓN DOCUMENTAL.	[A.11] Acceso no autorizado	1	5	5
		[A.18] Destrucción de información	1	5	5
		[A.19] Revelación de información	1	4	4
		[A.22] Manipulación de programas	1	4	4
		[A.4] Manipulación de la configuración	1	4	4
		[A.5] Suplantación de la identidad del usuario	1	4	4
		[A.6] Abuso de privilegios de acceso	1	4	4
		[A.7] Uso no previsto	2	4	8
		[A.8] Difusión de software dañino	1	4	4
		[E.1] Errores de los usuarios	3	3	9
		[E.18] Destrucción de información	1	5	5
		[E.19] Fugas de información	2	4	8
		[E.2] Errores del administrador	3	3	9
		[E.20] Vulnerabilidades de los programas (software)	3	3	9
		[E.4] Errores de configuración	3	3	9
		[E.8] Difusión de software dañino	3	3	9
		[I.5] Avería de origen físico o lógico	3	4	12

Fuente: El Autor (2023)

Tabla 22 Valor del riesgo asociado a los activos de información Hardware

VALOR DEL RIESGO EN LOS ACTIVOS DE INFORMACION EQUIPOS INFORMATICOS (HARDWARE)					VALOR DEL RIESGO
TIPO DE ACTIVO	DESCRIPCION	AMENAZAS	FRECUENCIA	DEGRADACION E IMPACTO	
EQUIPOS INFORMATICOS (HARDWARE)	SERVIDORES, WORKSTATION, DESKTOP, LAPTOP, SMARTPHONES, TABLETAS, NAS, SAN, IMPRESORAS, SCANNER, LECTORES CÓDIGO BARRAS, HUELLEROS, SWITCH CORE,	[A.11] Acceso no autorizado	1	4	4
		[A.23] Manipulación de los equipos	1	4	4
		[A.24] Denegación de servicio	1	5	5
		[A.25] Robo	2	4	8
		[A.26] Ataque destructivo	1	5	5
		[A.5] Suplantación de la identidad del usuario	1	4	4
		[A.6] Abuso de privilegios de acceso	1	4	4

Tabla 22 (continuación)

EQUIPOS INFORMATICOS (HARDWARE)	MODEM INTERNET, PLANTA TELEFÓNICA, GATEWAY TELEFONÍA IP, TELÉFONOS IP, FIREWALL, AP, DOMOTICA, CÁMARAS IP, DVR-IP CCTV, SMART TV, SISTEMAS RFID, EQUIPOS BIOMÉDICOS, LLAMADOS ENFERMERIA, DIGITURNOS, IoT, IoMT.	[A.7] Uso no previsto	1	5	5
		[E.2] Errores del administrador	2	3	6
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	3	9
		[E.24] Caída del sistema por agotamiento de recursos	3	3	9
		[E.25] Perdida de Equipos	2	4	8
		[E.4] Errores de configuración	3	3	9
		[I.*] Desastres industriales	1	5	5
		[I.11] Emanaciones electromagnéticas	1	4	4
		[I.3] Contaminación mecánica	2	3	6
		[I.4] Contaminación electromagnética	2	2	4
		[I.5] Avería de origen físico o lógico	2	4	8
		[I.6] Corte del suministro eléctrico	2	3	6
		[I.7] Condiciones inadecuadas de temperatura y/o humedad	2	3	6
		[I.8] Fallo de servicios de comunicaciones	3	3	9
		[I.9] Interrupción de otros servicios y suministros esenciales	1	5	5
		[N.*] Desastres naturales	1	5	5
		[N.1] Fuego	1	5	5
		[N.2] Daños por agua	2	4	8

Fuente: El Autor (2023)

Tabla 23 Valor del riesgo asociado a los activos de información Comunicaciones

VALOR DEL RIESGO EN LOS ACTIVOS DE INFORMACION: REDES DE COMUNICACIONES					VALOR DEL RIESGO
TIPO DE ACTIVO	DESCRIPCION	AMENAZAS	FRECUENCIA	DEGRADACION E IMPACTO	
REDES DE COMUNICACIONES	CANAL E1 DE VOZ CANAL DEDICADO INTERNET FIBRA ÓPTICA PRINCIPAL Y RESPALDO (WAN) ANTENAS DE COMUNICACIONES DE RADIO (AMBULANCIAS Y RADIOS) RED DE DATOS Y VOZ TELEFONÍA MÓVIL, RADIO ENLACE	[A.11] Acceso no autorizado	1	4	4
		[A.23] Manipulación de los equipos	1	4	4
		[A.24] Denegación de servicio	1	5	5
		[A.26] Ataque destructivo	1	5	5
		[A.5] Suplantación de la identidad del usuario	1	4	4
		[A.6] Abuso de privilegios de acceso	1	4	4
		[A.7] Uso no previsto	1	5	5
		[I.*] Desastres industriales	1	5	5
		[I.4] Contaminación electromagnética	1	4	4

Fuente: El Autor (2023)

Tabla 24 Valor del riesgo asociado a los activos de información Soportes

VALOR DEL RIESGO EN LOS ACTIVOS DE INFORMACION: SOPORTES DE INFORMACION					VALOR DEL RIESGO
TIPO DE ACTIVO	DESCRIPCION	AMENAZAS	FRECUENCIA	DEGRADACION E IMPACTO	
SOPORTES DE INFORMACION	CLOUD, DISCOS DUROS FÍSICOS, DISCOS DUROS VIRTUALES, NAS, SAN, DISCOS DUROS EXTERNOS, MEMORIAS USB, ALMACENAMIENTO EN RED, DVD, TARJETAS DE MEMORIA, TARJETAS INTELIGENTES, MATERIAL IMPRESO.	[A.11] Acceso no autorizado	1	4	4
		[A.23] Manipulación de los equipos	1	4	4
		[A.24] Denegación de servicio	1	5	5
		[A.26] Ataque destructivo	1	5	5
		[A.5] Suplantación de la identidad del usuario	1	4	4
		[A.6] Abuso de privilegios de acceso	1	4	4
		[A.7] Uso no previsto	1	5	5
		[I.5] Avería de origen físico o lógico	2	4	8
		[A.25] Robo	2	4	8

Fuente: El Autor (2023)

Tabla 25 Valor del riesgo asociado a los activos de información Equipamiento Auxiliar

VALOR DEL RIESGO EN LOS ACTIVOS DE INFORMACION: EQUIPAMENTO AUXILIAR					VALOR DEL RIESGO
TIPO DE ACTIVO	DESCRIPCION	AMENAZAS	FRECUENCIA	DEGRADACION E IMPACTO	
EQUIPAMENTO AUXILIAR	RED ELECTRICA REGULADA, UPS, PLANTA ELECTRICA, AIRES ACONDICIONADOS, CABLEADO DE AREA PARA DATOS Y RED ELECTRICA, BACKBONE FIBRA, RACKS DE COMUNICACIONES	[A.11] Acceso no autorizado	1	5	5
		[A.24] Denegación de servicio	1	5	5
		[A.26] Ataque destructivo	1	5	5
		[A.7] Uso no previsto	1	5	5
		[I.*] Desastres industriales	1	5	5
		[I.9] Interrupción de otros servicios y suministros esenciales	1	5	5
		[N.*] Desastres naturales	1	5	5
		[N.1] Fuego	1	5	5

Fuente: El Autor (2023)

Tabla 26 Valor del riesgo asociado a los activos de información Instalaciones

VALOR DEL RIESGO EN LOS ACTIVOS DE INFORMACION: INSTALACIONES					VALOR DEL RIESGO
TIPO DE ACTIVO	DESCRIPCION	AMENAZAS	FRECUENCIA	DEGRADACION E IMPACTO	
INSTALACIONES	DATA CENTER CENTROS DE CABLEADO Y DATOS CUARTOS ELECTRICOS CENTRAL ELECTROGENA CENTRAL TELEFONICA	[A.26] Ataque destructivo	1	5	5
		[I.*] Desastres industriales	1	5	5
		[I.9] Interrupción de otros servicios y suministros esenciales	1	5	5
		[N.*] Desastres naturales	1	5	5
		[N.1] Fuego	1	5	5

Fuente: El Autor (2023)

Tabla 27 Valor del riesgo asociado a los activos de información Personal

VALOR DEL RIESGO EN LOS ACTIVOS DE INFORMACION: PERSONAL					VALOR DEL RIESGO
TIPO DE ACTIVO	DESCRIPCION	AMENAZAS	FRECUENCIA	DEGRADACION E IMPACTO	
PERSONAL	USUARIOS INTERNOS: FUNCIONARIOS. COORDINACIÓN TI, DBA, PROFESIONALES CONTRATISTAS TICS, TÉCNICOS OPERATIVOS. PROVEEDORES DE SERVICIOS TECNOLOGICOS TERCERIZADOS	[A.28] Indisponibilidad del personal	3	2	6
		[A.29] Extorsión	1	4	4
		[A.30] Ingeniería social	3	2	6
		[A.6] Abuso de privilegios de acceso	3	2	6
		[A.7] Uso no previsto	3	2	6
		[E.19] Fugas de información	3	3	9
		[E.21] Errores de mantenimiento / actualización de programas (software)	3	4	12
		[E.28] Indisponibilidad del personal	2	2	4
		[E.7] Deficiencias en la organización	4	4	16

Fuente: El Autor (2023).

Una vez evaluadas las amenazas y valorado riesgo de los activos de información, el siguiente paso en la metodología MAGERIT es la identificación de controles. Para este proyecto, se definen controles para los riesgos evaluados con valores entre 9 y 25 puntos, cuya finalidad es priorizar aquellos de mayor urgencia. Es importante resaltar que los riesgos fuera de este rango no se descuidarán; todas las amenazas identificadas deberán ser analizadas, actualizadas y monitoreadas continuamente por el personal encargado de la gestión del riesgo en las instituciones.

Se debe establecer una ruta clara y procedimientos definidos para asegurar la continuidad de estas prácticas. De esta manera, se garantiza que cada amenaza identificada sea mitigada, dando lugar a la aplicación de tratamientos necesarios. Este enfoque permitirá abordar proactivamente cada nueva amenaza que surja, manteniendo así la seguridad de los activos de información de manera constante.

Cuadro 17 Amenazas de más alto riesgo.

TIPO DE ACTIVO	AMENAZAS	VALOR DEL RIESGO
ARQUITECTURA DEL SISTEMA	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	9
	[E.24] Caída del sistema por agotamiento de recursos	9
	[E.4] Errores de configuración	9
	[I.8] Fallo de servicios de comunicaciones	9
SERVICIOS	[I.8] Fallo de servicios de comunicaciones	9
SOFTWARE APLICACIÓNES INFORMATICAS	[E.1] Errores de los usuarios	9
	[E.2] Errores del administrador	9
	[E.20] Vulnerabilidades de los programas (software)	9
	[E.4] Errores de configuración	9
	[E.8] Difusión de software dañino	9
	[I.5] Avería de origen físico o lógico	12
EQUIPOS INFORMATICOS (HARDWARE)	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	9
	[E.24] Caída del sistema por agotamiento de recursos	9
	[E.4] Errores de configuración	9
	[I.8] Fallo de servicios de comunicaciones	9
PERSONAL	[E.19] Fugas de información	9
	[E.21] Errores de mantenimiento / actualización de programas (software)	12
	[E.7] Deficiencias en la organización	16

Fuente: El Autor (2023)

El cuadro anterior representa el resultado de la muestra con los activos de información y las amenazas asociadas y calificadas con una valoración entre 9-25 puntos como se estableció para efectos del proyecto.

7.3 MATRIZ DE SEGURIDAD DE LA INFORMACION

En esta parte del proyecto se trabajará con siete de los activos de información más críticos identificados en el entorno de los hospitales públicos en Colombia. Se propone una matriz de seguridad que se basa en MAGERIT v3 y los controles de ISO 27002:2013 para el análisis de riesgos. En la matriz se identifica amenazas y

se propone controles de seguridad según los estándares mencionados. El objetivo es obtener un mapa de calor con los riesgos identificados y clasificados según el impacto vrs. la probabilidad, el plan de tratamiento, la valoración cuantitativa y cualitativa, así como un resumen ejecutivo a manera de ejemplo para tener una perspectiva clara de la muestra tomada para el ejercicio.

7.3.1 Identificación de controles.

Evaluar amenazas y riesgos para establecer controles en una matriz de seguridad es una práctica muy común y respaldada por estándares internacionales. Esta evaluación permite elegir medidas efectivas y adaptables a las mejores prácticas, protegiendo los activos de información de manera puntual. Identificar controles correctamente es decisivo para proteger activos mediante medidas de seguridad. Esto implica explorar y evaluar opciones disponibles para mitigar los riesgos y reducirlos a un nivel óptimo. Es esencial considerar enfoques técnicos, organizativos y de gestión para una protección integral.

Tanto en Magerit como en la norma ISO 27002, se proponen controles específicos para cada tipo de activo. Estos son seleccionados cuidadosamente por su aplicabilidad y efectividad para mitigar el riesgo asociado, como lo podemos ver en la siguiente tabla, con una muestra de cinco activos de información.

Tabla 28 Controles propuestos para la muestra

TIPO DE ACTIVO	AMENAZAS	CONTROL MAGERIT	CONTROL ISO 27002
ARQUITECTURA DEL SISTEMA	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	HW.CM Cambios (actualizaciones y mantenimiento)	11.2.4 Mantenimiento del equipamiento
	[E.24] Caída del sistema por agotamiento de recursos	Plan de estimación de recursos	17.2.1 Disponibilidad de las instalaciones de procesamiento de la información
	[E.4] Errores de configuración	H.tools.CC Herramienta de chequeo de configuración H.tools.VA Herramienta de análisis de vulnerabilidades	12.1.4 Separación de los ambientes de desarrollo, prueba y operacionales
	[I.8] Fallo de servicios de comunicaciones	COM Protección de las Comunicaciones	A13.1.3 Segregación en redes

Tabla 28 (Continuacion)

SERVICIOS	[I.8] Fallo de servicios de comunicaciones	COM.A Aseguramiento de la disponibilidad	A13.1.2 Seguridad de los servicios de red
SOFTWARE APLICACIONES INFORMATICAS	[E.1] Errores de los usuarios	PS.AT Formación y concienciación	9.2.5 Revisión de los derechos de acceso de usuario
	[E.2] Errores del administrador	SW.A Copias de seguridad (backup)	12.3.1 Respaldo de la información
	[E.20] Vulnerabilidades de los programas (software)	SW Protección de las Aplicaciones Informáticas	12.6.2 Restricciones sobre la instalación de software
	[E.4] Errores de configuración	H.tools.CC Herramienta de chequeo de configuración H.tools.VA Herramienta de análisis de vulnerabilidades	14.2.4 Restricciones en los cambios a los paquetes de software
	[E.8] Difusión de software dañino	H.tools.AV Herramienta contra código dañino	12.2.1 Controles contra códigos maliciosos
	[I.5] Avería de origen físico o lógico	SW.CM Cambios (actualizaciones y mantenimiento)	14.2.3 Revisión técnica de las aplicaciones después de los cambios en la plataforma de operación
EQUIPOS INFORMATICOS HARDWARE	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	HW.CM Cambios (actualizaciones y mantenimiento)	11.2.4 Mantenimiento del equipamiento
	[E.24] Caída del sistema por agotamiento de recursos	HW.A Aseguramiento de la disponibilidad	17.2.1 Disponibilidad de las instalaciones de procesamiento de la información
	[E.4] Errores de configuración	H.tools.CC Herramienta de chequeo de configuración	12.1.4 Separación de los ambientes de desarrollo, prueba y operacionales
	[I.8] Fallo de servicios de comunicaciones	COM Protección de las Comunicaciones	13.1 Gestión de la seguridad de red
PERSONAL	[E.19] Fugas de información	PS.AT Formación y concienciación	7.1 Previo al empleo
	[E.21] Errores de mantenimiento / actualización de programas (software)	PS.A Aseguramiento de la disponibilidad	7.2.2 Concientización, educación y formación en seguridad de la información
	[E.7] Deficiencias en la organización	PS Gestión del Personal	7.2.3 Proceso disciplinario

Fuente: El Autor (2023)

Es esencial comprender que la identificación de controles no solo se limita a una lista predefinida, sino que también implica una evaluación continua y adaptativa, considerando las necesidades y particularidades de cada entorno organizativo. Por ejemplo, se pueden considerar controles como el cifrado de datos, la autenticación de dos factores, sistemas de monitoreo en tiempo real, protocolos de acceso seguro, entre otros, dependiendo de las características y riesgos específicos de los activos de información en cuestión.

La selección de controles adecuados no solo se basa en su disponibilidad, sino en su idoneidad para reducir los riesgos identificados. Por ende, se requiere una cuidadosa evaluación y análisis para garantizar la implementación de medidas que proporcionen una protección integral y efectiva a los activos de información, pero que a la vez no se desborde en la necesidad de recursos o que la aplicación del control supere el valor del activo de información a proteger.

7.3.2 Matriz de Riesgos.

La matriz de riesgos se emplea como herramienta fundamental para visualizar y evaluar los distintos riesgos a los que se enfrenta una organización. Su objetivo primordial consiste en identificar, analizar y priorizar estos riesgos, permitiendo así la toma de decisiones informadas.

A continuación, se presenta la siguiente tabla, la cual resume la valoración de una muestra de activos de información pertenecientes a una institución de salud pública. Estos activos que se presentan han sido clasificados como de Riesgo Extremo, lo que demanda una gestión inmediata y prioritaria.

Tabla 29 Muestra de activos de información

Resumen de Valoración de los activos					
Nombre del Activo	**Riesgo**	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Valor**
HIS SISTEMA DE INFORMACION HOSPITALARIO	EXTREMO	9	9	9	9
BASE DE DATOS HIS	EXTREMO	9	9	9	9
SERVIDOR RIS PACS IMAGENOLOGIA	EXTREMO	9	9	9	9
SAN ALMACENAMIENTO PACS	EXTREMO	9	9	9	9
VISOR IMÁGENES DIAGNOSTICAS	EXTREMO	9	9	9	9
ESTACIONES DE TRABAJO	EXTREMO	9	9	9	9
NAS ALMACENAMIENTO ARCHIVOS	EXTREMO	9	6	9	8
COPIAS DE SEGURIDAD BASES DE DATOS MISIONALES	EXTREMO	9	9	6	8

Fuente: El Autor (2023)

En la tabla anterior, se identifican ocho activos de información clasificados como de Riesgo Extremo. Para cada uno de ellos, se lleva a cabo un análisis exhaustivo y se establece un tratamiento específico. El propósito es obtener una planificación estratégica y diseñar medidas preventivas y correctivas que aseguren la protección de la información dentro de la organización

Procedemos entonces a listar cada activo para identificar las amenazas asociadas y las vulnerabilidades. Para abordar estos aspectos, se asignan controles específicos y se describe detalladamente cómo se aplicarán. Además, se puede clasificar el origen del riesgo para darle una clasificación extra a fin de priorizar el tratamiento, que puede variar entre:

- Requerimiento legal: Incumplimiento de leyes o normativas.
- Análisis de Riesgo: Identificación durante el análisis.
- Requerimiento de Negocio: Crucial para actividades del objeto social.
- Obligación contractual: Definido en acuerdos.
- Exclusión: Riesgo no considerado para tratamiento.

Tabla 30 Plan de tratamiento activos de información.

Plan de Tratamiento de Activos de Información				Control ISO 27001:2013			
Activos de Información	Nombre del activo de información	Amenazas Metodología Magerit	Vulnerabilidades	DOMINIO	OBJETIVO	CONTROL	Descripción de la aplicación del control
SOFTWARE	HIS SISTEMA DE INFORMACION HOSPITALARIO	[I5] Avería de origen físico o lógico	Falta de actualizaciones de seguridad que podrían llevar a la vulnerabilidad del sistema. Falta de redundancia en los servidores que hospedan el sistema, aumentando el riesgo de interrupciones debido a fallos físicos.	DOMINIO_A17	OBJETIVO_A17_2	A17.2.1 Disponibilidad de instalaciones de procesamiento de información --Control: Las instalaciones de procesamientos de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.
DATOS	BASE DE DATOS HIS	[E18] Destrucción de información	Falta de copias de seguridad regulares y pruebas de recuperación de datos. Falta de políticas de acceso y control de datos adecuadas que podrían llevar a la eliminación accidental o maliciosa de información crítica.	DOMINIO_A12	OBJETIVO_A12_3	A12.3.1 Respaldo de la información --Control: Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas
HARDWARE	SERVIDOR RIS PACS IMAGENOLOGIA	[E24] Caída del sistema por agotamiento de recursos	No monitorear activamente el uso de recursos (CPU, memoria, almacenamiento) puede llevar a una carga excesiva y, finalmente, a una caída del sistema. Falta de redundancia o balanceo de carga en servidores críticos puede aumentar la probabilidad de agotamiento de recursos.	DOMINIO_A17	OBJETIVO_A17_2	A17.2.1 Disponibilidad de instalaciones de procesamiento de información --Control: Las instalaciones de procesamientos de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.
HARDWARE	SAN ALMACENAMIENTO PACS	[E23] Errores de mantenimiento / actualización de equipos (hardware)	Actualizaciones de firmware o software sin realizar pruebas previas adecuadas pueden llevar a interrupciones no deseadas en el sistema de almacenamiento. Falta de supervisión activa de la integridad de los dispositivos de almacenamiento.	DOMINIO_A11	OBJETIVO_A11_2	A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.

Tabla 30 (Continuación)

SOFTWARE	VISOR IMÁGENES DIAGNOSTICAS	[E20] Vulnerabilidades de los programas (software)	Falta de actualizaciones de seguridad del software, dejando posibles brechas que podrían ser explotadas por atacantes. Configuraciones predeterminadas inseguras o puertos abiertos que podrían ser puntos de acceso para amenazas externas.	DOMINIO_A12	OBJETIVO_A12_6	A12.6.2 Restricciones sobre la instalación de software --Control: Se deben establecer e implementar las reglas para la instalación de software por parte de los usuarios.	Se deben establecer e implementar reglas para la instalación de software por parte de los usuarios.
HARDWARE	ESTACIONES DE TRABAJO	[A23] Manipulación de los equipos	Falta de controles de acceso físico a las estaciones de trabajo. Uso de contraseñas débiles o compartidas, lo que facilita el acceso no autorizado a los dispositivos.	DOMINIO_A9	OBJETIVO_A9_4	A9.4.3 Sistema de gestión de contraseñas --Control: Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.
DATOS	COPIAS DE SEGURIDAD BASES DE DATOS MISIONALES	[E18] Destrucción de información	Falta de procedimientos y políticas de respaldo y almacenamiento seguro de las copias de seguridad. No realizar pruebas regulares de restauración de las copias de seguridad para verificar su integridad y disponibilidad.	DOMINIO_A12	OBJETIVO_A12_3	A12.3.1 Respaldo de la información --Control: Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.

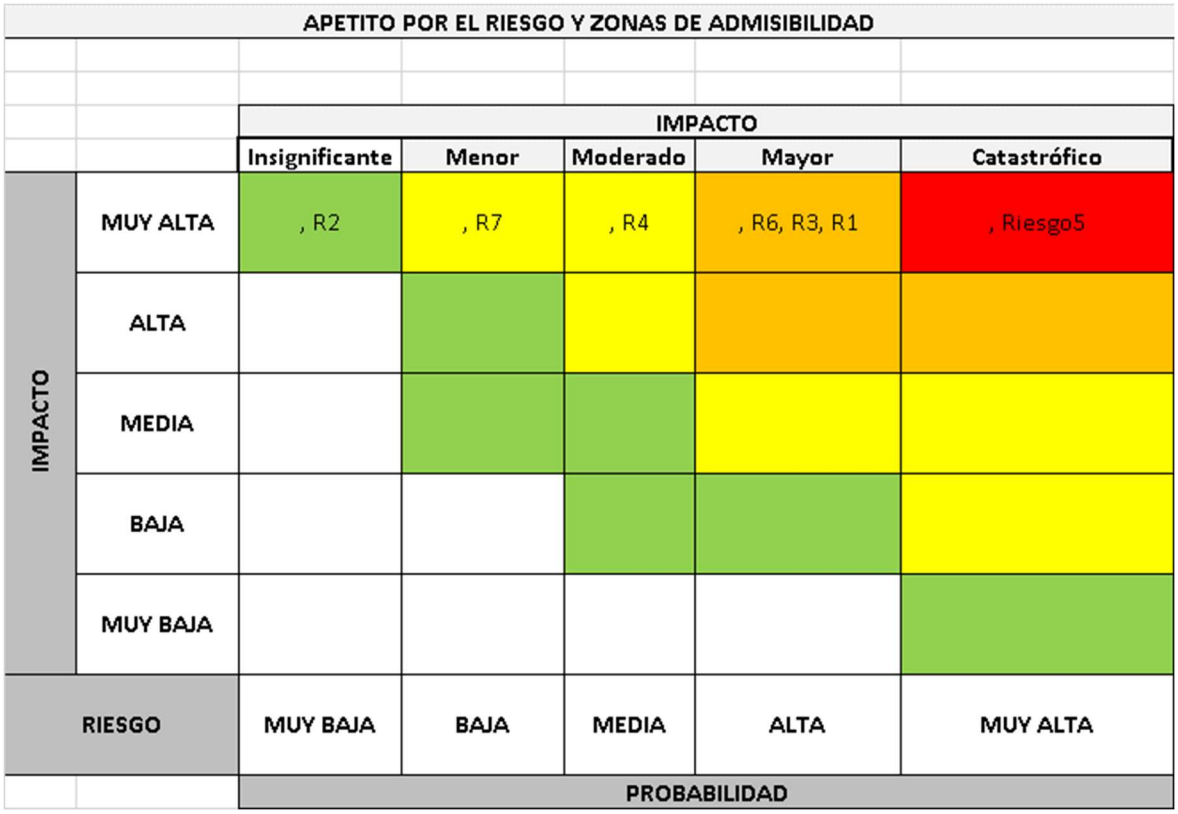
Fuente: El Autor (2023)

Dada la clasificación de riesgo extremo para los activos de la tabla anterior, todos serán sometidos al proceso de Mitigación. No obstante, esta medida no es obligatoria en todos los casos, ya que se puede elegir entre diferentes enfoques, entre los cuales se proponen:

- Mitigar: Reducir el riesgo con controles adecuados.
- Transferir: Delegar riesgos a terceros o cubrirlos con seguros.
- Aceptar: Reconocer riesgos manejables.
- Eliminar: Descartar riesgos insignificantes.

Finalmente, como uno de los resultados, la matriz nos proporciona un mapa de calor que presenta la ubicación de los riesgos en diferentes niveles según su impacto y probabilidad. Este cálculo se deriva de la validación tanto cualitativa como cuantitativa de los activos, así como de la evaluación de la gestión actual, los controles existentes y la documentación de los procedimientos o políticas con que se cuenta. Además, considera la probabilidad actual de materialización del riesgo y la calificación basada en las dimensiones y atributos particulares asignados a cada activo. Todo lo anterior forma parte del resultado que se presenta en el mapa de calor, a continuación se ilustra con la muestra de los activos del caso planteado.

Ilustración 11 Valoración del riesgo



APETITO POR EL RIESGO Y ZONAS DE ADMISIBILIDAD						
		IMPACTO				
		Insignificante	Menor	Moderado	Mayor	Catastrófico
IMPACTO	MUY ALTA	, R2	, R7	, R4	, R6, R3, R1	, Riesgo5
	ALTA					
	MEDIA					
	BAJA					
	MUY BAJA					
RIESGO		MUY BAJA	BAJA	MEDIA	ALTA	MUY ALTA
		PROBABILIDAD				

Fuente: El Autor (2023)

De esta manera se clasifican los riesgos en el Mapa de Calor, donde se destaca el Riesgo 5 con una probabilidad muy alta y un posible impacto catastrófico para la organización si se materializa. Este riesgo se vincula a un activo de tipo SOFTWARE, específicamente un Visor de Imágenes Diagnósticas, con un valor de riesgo asociado de 23 en la escala critica dada entre 21 a 25 puntos. La aplicación del control en este caso se plantea como la implementación de reglas para la instalación de software en la institución, donde en el procedimiento se deberá establecer la condición de actualizar las versiones de los programas, parches y control de estado de puertos, de manera que se realice periódicamente y ejercer controles según cronogramas definidos.

7.4 PLAN DIRECTOR DE SEGURIDAD DIGITAL EN HOSPITALES PÚBLICOS DE COLOMBIA.

El Plan Director de Seguridad (PDS) para hospitales públicos en Colombia tiene como objetivo principal mitigar los riesgos asociados con la seguridad de la información y proteger los activos críticos de datos médicos y la infraestructura tecnológica. Este documento establece un marco integral que se debe alienar con los objetivos estratégicos de los hospitales públicos como los definidos en el Plan Estratégico de Tecnologías de la Información PETI de estas instituciones y abordar las amenazas emergentes en el entorno digital.

El esquema general que maneja un PDS consta de 6 fases, como se representa en la siguiente ilustración:

Ilustración 12 Fases Plan director de

Fuente: INCIBE. Plan director de Seguridad, página 5. [Gráfico]. Disponible en: https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_plan-director-seguridad.pdf. Consultado diciembre 2023.

Para la propuesta del PDS se deben considerar cada una de las fases, las que se propone desarrollar de la siguiente manera:

7.4.1 Conocer la situación actual de la organización (Fase 1).

Esta fase implica llevar a cabo distintos análisis considerando aspectos técnicos, organizativos, regulatorios y normativos, entre otros. Es fundamental contar con el apoyo de la Dirección.

7.4.1.1. **Actividades Previas al análisis.**

- Acotar y establecer el alcance: se debe definir qué áreas del hospital se incluirán en el análisis de seguridad y que activos de información se relacionan directamente con el proceso, por ejemplo el sistema de historia clínica, bases de datos misionales, plataformas de terceros, equipos de diagnóstico, equipamiento de red, etc. Para este proyecto se propone trabajar este aspecto con la metodología MAGERIT v3 el proceso para llevar a cabo el alcance se puede ver en el numeral 6.1.1. Identificación de activos de información.

- Responsables de la gestión de los activos: Identificar a las personas o equipos responsables de la gestión de los activos de información en el hospital. Para este punto cada organización según sus procesos internos define los responsables de los activos.

- Valoración inicial: Realizar una evaluación inicial de la situación de seguridad en el hospital, incluyendo la identificación de activos de información y su clasificación en términos de confidencialidad, integridad y disponibilidad. Como ejemplo se plantea la estructura del Cuadro 16 Activos de información: valoración cuantitativa, de este documento.

- Análisis de cumplimiento: Verificar el cumplimiento de las normativas y regulaciones aplicables en el sector de la salud en Colombia, que corresponden descrito en el capitulo 4.5 Marco Legal de este documento.

- Establecer los objetivos: Definir los objetivos de seguridad que se quieren alcanzar con la implementación del Plan de Seguridad. El objetivo del Plan Director de Seguridad en hospitales públicos en Colombia es garantizar la confidencialidad, integridad y disponibilidad de los datos médicos de los pacientes, reducir los riesgos de ciberseguridad y proteger la infraestructura tecnológica del hospital, cumplir con las regulaciones de protección de datos y estándares de seguridad en el sector de la salud, y promover una cultura de seguridad entre el personal hospitalario

7.4.1.2. Análisis Técnico de Seguridad.

Realizar un análisis detallado de los sistemas de información y tecnologías utilizadas en el hospital, identificando posibles vulnerabilidades y amenazas, relacionadas con cada tipo de activos de información. Para ello se propone diseñar una tabla donde se precise esta información, de la siguiente manera:

Cuadro 18Vulnerabilidades y amenazas relacionadas a los activos Software

Categoría Activo de Información	AMENAZAS	VULNERABILIDADES
SOFTWARE / APLICACIONES INFORMÁTICAS [SW]	[A01] Acceso no autorizado [A02] Negación de las acciones realizadas [A03] Interceptación de datos o información [A04] Alteración o modificación no autorizada [A05] Destrucción e eliminación no autorizada [A06] Divulgación no autorizada de datos o información [A07] Sabotaje o daño intencional [A10] Abuso de privilegios de acceso [A12] Usos no previstos o inadecuados [A14] Errores en el uso [A17] Errores en mantenimiento o actualización [A20] Alteración de funcionalidades [A21] Infecciones por software dañino o malicioso [A22] Fallas o mal funcionamiento [A23] Fallas o Errores en instalación, administración o custodia [A25] Comportamientos inesperados o anormales [A27] Cambios o ajustes no controlados [A29] Errores o fallas en el monitoreo [A32] Suplantación de la identidad del usuario	Ausencia o insuficiencia de pruebas de calidad de software Aceptación de Defectos conocidos en el software Ausencia o debilidad en el manejo de las sesiones de acceso Errores de programación en el sistema Ausencia de registros de auditoria Ausencia de soporte, mantenimiento o actualización Interfaz de usuario compleja Ausencia de manuales de uso y configuración Instalación y/o configuración incorrecta o por defecto Ausencia de validaciones para el registro de información Ausencia de mecanismos de identificación y autenticación de usuario Ausencia de pruebas de seguridad Software nuevo o inmaduro Especificaciones de desarrollo incompletas o incorrectas Ausencia de control de cambios o versionamiento adecuado Ausencia de manejo de roles y perfiles Falta de implementación de políticas de desarrollo seguro Ausencia de copias de respaldo de las configuraciones

Fuente: El Autor (2023)

Cuadro 19 Vulnerabilidades y amenazas relacionadas a los activos Hardware

Categoría Activo de Información	AMENAZAS	VULNERABILIDADES
HARDWARE/ INFRAESTRUCTURA [HW]	[A01] Acceso no autorizado [A04] Alteración o modificación no autorizada [A05] Destrucción e eliminación no autorizada [A07] Sabotaje o daño intencional [A08] Hurtos, Robos o Pérdidas [A09] Vandalismo o Ataque destructivo [A12] Usos no previstos o inadecuados [A13] Condiciones ambientales inadecuadas [A14] Errores en el uso [A17] Errores en mantenimiento o actualización [A18] Agotamiento de recursos [A19] Degradación o deterioro [A21] Infecciones por software dañino o malicioso [A22] Fallas o mal funcionamiento [A23] Fallas o Errores en instalación, administración o custodia [A25] Comportamientos inesperados o anormales [A27] Cambios o ajustes no controlados [A29] Errores o fallas en el monitoreo [A31] Desastres naturales	Ausencia o debilidades en los controles de acceso Ausencia de procedimientos para el transporte o traslado de equipos Ausencia de esquemas de reemplazo o actualización Ausencia de esquemas de monitoreo y control Uso o manejo inadecuado de los equipos Mantenimientos Insuficientes Instalaciones o configuraciones fallidas o por defecto Ausencia de controles de cambios en las configuraciones Ubicación o almacenamiento en lugares inseguros Falta de controles para la disposición final Ausencia de mecanismos de monitoreo y control ambiental Fallas en los servicios de suministros Desconocimiento de los procedimientos de control y cambio Ausencia de mecanismos de continuidad Ausencia de planes y pruebas de continuidad

Fuente: El Autor (2023)

Cuadro 20 Vulnerabilidades y amenazas relacionadas a los activos Servicios

Categoría Activo de Información	AMENAZAS	VULNERABILIDADES
SERVICIOS [SI]	[A01] Acceso no autorizado [A02] Negación de las acciones realizadas [A03] Interceptación de datos o información [A04] Alteración o modificación no autorizada [A07] Sabotaje o daño intencional [A10] Abuso de privilegios de acceso [A12] Usos no previstos o inadecuados [A14] Errores en el uso [A16] Fugas o tráfico de información [A17] Errores en mantenimiento o actualización [A18] Agotamiento de recursos [A19] Degradación o deterioro [A20] Alteración de funcionalidades [A21] Infecciones por software dañino o malicioso [A22] Fallas o mal funcionamiento [A24] Denegación o inaccesibilidad [A25] Comportamientos inesperados o anormales [A27] Cambios o ajustes no controlados [A28] Redireccionamiento a destinos no autorizados [A29] Errores o fallas en el monitoreo [A32] Suplantación de la identidad del usuario	Ausencia de pruebas de envío o recepción de mensajes Líneas de comunicación sin protección Tráfico sensible sin protección Conexión deficiente de los cables. Punto único de falla Ausencia de identificación y autentificación de emisor y receptor Arquitectura insegura del servicio Transferencia de contraseñas en claro Gestión inadecuada del servicio (Tolerancia a fallas en el enrutamiento) Conexiones de red públicas o sin protección Falta de separación de Redes Utilización de Protocolos inseguros de comunicación Ausencia de sistemas de monitoreo y control Falta de conciencia acerca de la seguridad Ausencia de pruebas funcionales o de stress

Fuente: El Autor (2023)

Cuadro 21 Vulnerabilidades y amenazas relacionadas a los activos Soportes de Información

Categoría Activo de Información	AMENAZAS	VULNERABILIDADES
SOPORTES DE INFORMACIÓN [SA]	[A01] Acceso no autorizado [A04] Alteración o modificación no autorizada [A05] Destrucción e eliminación no autorizada [A06] Divulgación no autorizada de datos o información [A07] Sabotaje o daño intencional [A08] Hurtos, Robos o Pérdidas [A11] Daños provocados por fuego, agua, polvo, vibraciones, suciedad, etc. [A12] Usos no previstos o inadecuados [A13] Condiciones ambientales inadecuadas [A14] Errores en el uso [A17] Errores en mantenimiento o actualización [A19] Degradación o deterioro [A20] Alteración de funcionalidades [A21] Infecciones por software dañino o malicioso [A22] Fallas o mal funcionamiento [A23] Fallas o Errores en instalación, administración o custodia [A25] Comportamientos inesperados o anormales	Ausencia de esquemas de reemplazo periódico. Susceptibilidad a la humedad, el polvo y la suciedad. Almacenamiento sin protección Falta de cuidado en la disposición final Almacenamiento desprotegido de datos o información Ausencia de controles contra códigos maliciosos Ausencia de copias de respaldos Falta de estándares y controles para el uso dispositivos Ubicación o almacenamiento en lugares inseguros Desconocimiento de las recomendaciones o guías de uso Falta de conciencia acerca de la seguridad

Fuente: El Autor (2023)

Cuadro 22 Vulnerabilidades y amenazas relacionadas a los activos Equipamiento Auxiliar

Categoría Activo de Información	AMENAZAS	VULNERABILIDADES
EQUIPOS AUXILIARES [EA]	[A01] Acceso no autorizado [A04] Alteración o modificación no autorizada [A05] Destrucción e eliminación no autorizada [A07] Sabotaje o daño intencional [A08] Hurtos, Robos o Pérdidas [A09] Vandalismo o Ataque destructivo [A11] Daños provocados por fuego, agua, polvo, vibraciones, suciedad, etc. [A12] Usos no previstos o inadecuados [A13] Condiciones ambientales inadecuadas [A14] Errores en el uso [A17] Errores en mantenimiento o actualización [A18] Agotamiento de recursos [A19] Degradación o deterioro [A20] Alteración de funcionalidades [A22] Fallas o mal funcionamiento [A23] Fallas o Errores en instalación, administración o custodia [A25] Comportamientos inesperados o anormales [A27] Cambios o ajustes no controlados	Ausencia de esquemas de reemplazo periódico. Susceptibilidad a la humedad, el polvo y la suciedad. Almacenamiento sin protección Falta de estándares y controles para el uso de elementos Ubicación o almacenamiento en lugares inseguros Ausencia de pruebas de funcionamiento Falta de conciencia acerca de la seguridad Obsolescencia de los equipos o las tecnologías

Fuente: El Autor (2023)

Cuadro 23 Vulnerabilidades y amenazas relacionadas a los activos Instalaciones y Personal

Categoría Activo de Información	AMENAZAS	VULNERABILIDADES
INSTALACIONES Y PERSONAL [IP]	[A01] Acceso no autorizado [A02] Negación de las acciones realizadas [A03] Interceptación de datos o información [A07] Sabotaje o daño intencional [A08] Hurtos, Robos o Pérdidas [A09] Vandalismo o Ataque destructivo [A11] Daños provocados por fuego, agua, polvo, vibraciones, suciedad, etc. [A12] Usos no previstos o inadecuados [A13] Condiciones ambientales inadecuadas [A15] Ingeniería social [A25] Comportamientos inesperados o anormales [A26] Ocupación o invasión de espacios [A29] Errores o fallas en el monitoreo [A30] Extorsión o amenazas [A31] Desastres naturales [A32] Suplantación de la identidad del usuario [A33] Cortes del suministro eléctrico [A34] Interrupción de suministros esenciales [A35] Indisponibilidad del personal	Uso inadecuado o descuidado de las instalaciones o recintos Ubicación en un área susceptible a inundaciones, suciedad Red energética inestable Ausencia de protección física de la edificación, puertas y ventanas Ausencia o indisponibilidad del personal Debilidades en los procedimientos de contratación Entrenamiento insuficiente en seguridad Trabajo no supervisado del personal externo o de limpieza Ausencia de mecanismos de monitoreo y control Falta de conciencia acerca de la seguridad Falta de segregación de funciones Ausencia de implementación de perímetros de seguridad Ausencia de procesos disciplinarios Ausencia de control de acceso físico en las instalaciones o recintos

Fuente: El Autor (2023)

Cuadro 24 Vulnerabilidades y amenazas relacionadas a los activos Datos / Información

Categoría Activo de Información	AMENAZAS	VULNERABILIDADES
DATOS O INFORMACIÓN [DI]	[A01] Acceso no autorizado [A02] Negación de las acciones realizadas [A03] Interceptación de datos o información [A04] Alteración o modificación no autorizada [A05] Destrucción e eliminación no autorizada [A06] Divulgación no autorizada de datos o información [A07] Sabotaje o daño intencional [A08] Hurtos, Robos o Pérdidas [A09] Vandalismo o Ataque destructivo [A10] Abuso de privilegios de acceso [A11] Daños provocados por fuego, agua, polvo, vibraciones, suciedad, etc. [A12] Usos no previstos o inadecuados [A13] Condiciones ambientales inadecuadas [A14] Errores en el uso [A19] Degradación o deterioro [A24] Denegación o inaccesibilidad [A26] Ocupación o invasión de espacios [A31] Desastres naturales [A35] Indisponibilidad del personal	Ausencia de requisitos de seguridad con terceros Ausencia de acuerdos o cláusulas de confidencialidad Disposición insegura de datos o información Ausencia de copias de respaldo Falta de revisión periódica de las medidas de seguridad Tratamiento inadecuado de datos o información Ausencia de lecciones aprendidas sobre incidentes de seguridad No corrección de vulnerabilidades conocidas Ausencia de mecanismos de monitoreo y control Copias no controladas ni autorizadas de datos o información Ausencia de métodos de cifrado Ausencia de Controles de acceso Habilitación de servicios o accesos innecesarios Almacenamiento sin protección Desconocimiento de políticas y procedimientos Clasificación inadecuada de la información Entrenamiento insuficiente en seguridad Falta de conciencia acerca de la seguridad

Fuente: El Autor (2023)

Cuadro 25 Vulnerabilidades y amenazas relacionadas a los activos Redes y Comunicaciones

Categoría Activo de Información	AMENAZAS	VULNERABILIDADES
REDES DE COMUNICACIÓN [RC]	[A01] Acceso no autorizado [A04] Alteración o modificación no autorizada [A05] Destrucción e eliminación no autorizada [A07] Sabotaje o daño intencional [A08] Hurtos, Robos o Pérdidas [A09] Vandalismo o Ataque destructivo [A12] Usos no previstos o inadecuados [A13] Condiciones ambientales inadecuadas [A14] Errores en el uso [A17] Errores en mantenimiento o actualización [A18] Agotamiento de recursos [A19] Degradación o deterioro [A21] Infecciones por software dañino o malicioso [A22] Fallas o mal funcionamiento [A23] Fallas o Errores en instalación, administración o custodia [A25] Comportamientos inesperados o anormales [A27] Cambios o ajustes no controlados [A29] Errores o fallas en el monitoreo [A31] Desastres naturales	Ausencia de requisitos de seguridad con terceros Ausencia de acuerdos o cláusulas de confidencialidad Disposición insegura de datos o información Ausencia de copias de respaldo Falta de revisión periódica de las medidas de seguridad Tratamiento inadecuado de datos o información Ausencia de lecciones aprendidas sobre incidentes de seguridad No corrección de vulnerabilidades conocidas Ausencia de mecanismos de monitoreo y control Copias no controladas ni autorizadas de datos o información Ausencia de métodos de cifrado Ausencia de Controles de acceso Habilitación de servicios o accesos innecesarios Almacenamiento sin protección Desconocimiento de políticas y procedimientos Clasificación inadecuada de la información Entrenamiento insuficiente en seguridad Falta de conciencia acerca de la seguridad

Fuente: El Autor (2023)

Cuadro 26 Vulnerabilidades y amenazas relacionadas a los activos Base de Datos

Categoría Activo de Información	AMENAZAS	VULNERABILIDADES
BASES DE DATOS [BD]	[A01] Acceso no autorizado [A02] Negación de las acciones realizadas [A03] Interceptación de datos o información [A04] Alteración o modificación no autorizada [A05] Destrucción e eliminación no autorizada [A06] Divulgación no autorizada de datos o información [A07] Sabotaje o daño intencional [A10] Abuso de privilegios de acceso [A12] Usos no previstos o inadecuados [A14] Errores en el uso [A17] Errores en mantenimiento o actualización [A20] Alteración de funcionalidades [A21] Infecciones por software dañino o malicioso [A22] Fallas o mal funcionamiento [A23] Fallas o Errores en instalación, administración o custodia [A25] Comportamientos inesperados o anormales [A27] Cambios o ajustes no controlados [A29] Errores o fallas en el monitoreo [A32] Suplantación de la identidad del usuario	Ausencia o debilidades en los controles de acceso Ausencia de procedimientos para el transporte o traslado de equipos Ausencia de esquemas de reemplazo o actualización Ausencia de esquemas de monitoreo y control Uso o manejo inadecuado de los equipos Mantenimientos Insuficientes Instalaciones o configuraciones fallidas o por defecto Ausencia de controles de cambios en las configuraciones Ubicación o almacenamiento en lugares inseguros Falta de controles para la disposición final Ausencia de mecanismos de monitoreo y control ambiental Fallas en los servicios de suministros Desconocimiento de los procedimientos de control y cambio Ausencia de mecanismos de continuidad

Fuente: El Autor (2023)

7.4.1.3. Análisis de Riesgos.

Nivel de riesgo aceptable: Definir el nivel de riesgo que la organización está dispuesta a aceptar. Para este propósito se propone analizar la tabla 15 Escala y Valor del Riesgo, dentro de este documento, donde se explican el valor del riesgo, el nivel y su tratamiento.

7.4.2 Conocer la estrategia de la organización (Fase 2).

Esta fase del Plan Director de Seguridad (PDS) se enfoca en comprender la estrategia corporativa de los hospitales públicos en Colombia, teniendo en cuenta su situación particular y las limitaciones derivadas de la crisis económica y la

pandemia de COVID-19. Las actividades que se pueden contemplar para esta fase son:

7.4.2.1. Proyectos en curso y futuros:

Es crucial tener en cuenta los proyectos actuales y futuros del hospital. Esto puede incluir la implementación de nuevos sistemas de información médica, la expansión de la infraestructura del hospital, la adquisición de nuevas tecnologías, la actualización normativa, entre otros.

Se debe buscar alinear la estrategia de seguridad TIC con los objetivos estratégicos de los hospitales. Esto permitirá implantar medidas de seguridad acordes a la naturaleza de la organización y conseguir una visión objetiva y global de la estrategia de negocio. Es fundamental involucrar a los directivos responsables de los departamentos implicados y la alta gerencia en la toma de decisiones que este paso requiere, ya que de ello depende el nivel de éxito del proceso.

7.4.2.2. Aumento de la Capacidad instalada:

Es importante analizar las previsiones de crecimiento del hospital. Esto puede implicar el aumento de la capacidad de atención al paciente, la expansión geográfica, la habilitación de nuevos servicios, entre otros aspectos.

7.4.2.3. Cambios en la organización:

Se deben considerar los posibles cambios en la organización debido a reestructuración. Esto puede incluir la fusión con otros hospitales, cambios en la administración, reasignación de funciones, entre otros.

7.4.2.4. Estrategia de Centralización o tercerización de Servicios:

Es necesario evaluar si el hospital planea centralizar servicios, especialmente en sistemas de información, servicios en la nube, tareas de mantenimiento, SaaS,

IaaS. Esta decisión puede tener un impacto significativo en la estrategia de seguridad y en la gestión de riesgos.

7.4.3 Definición de proyectos e iniciativas (Fase 3).

La Fase 3 del Plan director de Seguridad (PDS) se enfoca en la definición y elaboración de proyectos e iniciativas específicas para fortalecer la seguridad en los hospitales públicos de Colombia.

Esta fase se basa en la información recopilada en las fases anteriores y considera diferentes ámbitos como Recursos Humanos, Tecnología, Procesos y Gestión. El objetivo principal es abordar las deficiencias identificadas y mejorar el nivel de seguridad de la institución.

Esto se logra a través de la evaluación de deficiencias, el diseño de iniciativas para mejorar los métodos de trabajo, la implementación de controles técnicos y físicos, la definición de estrategias de gestión de riesgos, el desarrollo de proyectos específicos, la estimación de costos y recursos, y el establecimiento de cronogramas y prioridades. Se debe garantizar una comunicación y participación efectiva a todos los niveles de la organización.

Cada una de las etapas contempla:

- Evaluación de Deficiencias Identificadas: Revisar exhaustivamente las deficiencias detectadas en las fases previas para determinar sus causas y prioridades. Para este caso se plantea la tabla 16 Valoración de amenazas y riesgo asociado frente a los activos de información, donde se identifican los activos con mayor nivel de riesgo relacionado a las amenazas.

- Diseño de Iniciativas para Mejora de Métodos de Trabajo: Desarrollar planes de acción para mejorar los métodos de trabajo actuales, asegurando que cumplan con los controles y estándares regulatorios pertinentes en seguridad de la información. Si la entidad cuenta con un Sistema de Gestión de Calidad, puede abordar esta etapa con los formatos para planes de acción que se manejen para trabajarlas como oportunidades de mejora.

- Implementación de Controles Técnicos y Físicos: Establecer e implementar medidas técnicas y físicas para fortalecer la seguridad, abordando las deficiencias encontradas en la infraestructura y en los sistemas tecnológicos. Se puede apoyar con la tabla 17 Controles propuestos para la muestra, de este documento, donde se trabaja con una muestra de 5 activos de información, proponiendo los controles dados según ISO 27003 y Magerit V3.

- Definición de Estrategias de Gestión de Riesgos: Identificar y establecer estrategias específicas para gestionar los riesgos que exceden el nivel aceptable de la institución, priorizando aquellos de mayor impacto. Se propone como estrategia el numeral 6.3.2. Matriz de Riesgos, de este documento, cuyo resultado es un mapa de calor con los riesgos identificados según su impacto y probabilidad.

- Desarrollo de Proyectos Específicos: Crear proyectos con objetivos claros, plazos definidos y recursos asignados para abordar áreas críticas, como la protección de datos, la gestión de acceso a los sistemas y la continuidad del negocio. Se propone implementar una tabla como la siguiente, contemplado los aspectos citados.

Tabla 31 Portafolio de proyectos para PDS

ID	NOMBRE DEL PROYECTO	DESCRIPCON	MESES			
			3	6	9	12
1	Creación del Comité de Seguridad de la Información CSI	Este comité estaría compuesto por representantes de diferentes departamentos del hospital, incluyendo personal administrativo y asistencial. Su objetivo sería supervisar la implementación del PDS y asegurar que se cumplan los controles y procedimientos de seguridad cibernética establecidos.	x			
2	Implementación de la metodología de Gestión de Riesgos	Se llevarían a cabo sesiones de formación para el personal del hospital sobre cómo identificar y gestionar los riesgos de seguridad de la información en cada proceso al que pertenecen, socializando la metodología y los formatos establecidos.	x			
3	Contratación de Pentesting	Adquisición de herramientas o servicios, que permitan identificar y corregir vulnerabilidades en los sistemas de información del hospital para fortalecer la seguridad. Realizar esta actividad una vez al año y establecer planes de acción según el resultado de los informes.				x
4	Implementación del Programa de Recuperación ante Desastres	Desarrollo de un programa formativo para el personal en respuesta a desastres informáticos, garantizando una adecuada recuperación de sistemas afectados por eventos imprevistos. Teniendo claridad en la ruta que cada funcionario debe seguir y que plan de choque se debe seleccionar.			x	
5	Desarrollar y/o Actualizar la Política de Seguridad de la Información	Mantenimiento de una política integral de seguridad, incluyendo capacitación en aspectos clave uso seguro de herramientas digitales y protección de datos. Conformar un plan semestral de reinducción al personal, donde se socialice la política. La misma que deberá estar actualizada anualmente.		x		
6	Despliegue de Plan de Concienciación en Seguridad	Realización de sesiones de formación para todo el personal, incluyendo la Dirección, para aumentar la conciencia y comprensión sobre ciberseguridad y la importancia de las medidas preventivas. Hacer uso de incentivos para fomentar participación.			x	
7	Mejorar Coordinación entre RRHH y Departamento TIC	Sesiones de formación obligatorias para personal nuevo. Incluir en los requisitos del cargo formación básica en informática y ciberseguridad.	x			
8	Política de copias de seguridad	Análisis e implementación de una política de copias de seguridad y restauraciones periódicas para salvaguardar la información corporativa crítica ante posibles pérdidas o ataques.				x
9	Regulación de los servicios TIC prestado por terceros	Revisión y estandarización de contratos con proveedores externos, asegurando que se ajusten a las necesidades del hospital y estableciendo acuerdos de nivel de servicio para servicios críticos. Exigir en pliegos certificaciones y personal con experiencia especifica según el servicio prestado.				x

Fuente: El Autor (2023)

- Estimación de Costos y Recursos: Evaluar los recursos necesarios, tanto económicos como humanos, para cada iniciativa y proyecto, considerando aspectos internos y, si es necesario, la posibilidad de colaboración externa.

- Establecimiento de Cronogramas y Prioridades: Crear un cronograma detallado que establezca plazos realistas para la implementación de las iniciativas, priorizando aquellas que aborden riesgos de mayor relevancia o urgencia.

- Comunicación y Participación: Involucrar a los diferentes niveles de la organización en el proceso, comunicando de manera clara los objetivos, beneficios y responsabilidades de cada proyecto o iniciativa.

Al finalizar esta fase se tendrá una estructura clara y detallada para la ejecución de acciones concretas, asegurando una mejora continua en la seguridad de la información en los hospitales públicos de Colombia.

7.4.4 Clasificar y priorizar los proyectos a realizar (Fase 4).

La Fase 4 del Plan Director de Seguridad se refiere a la "Clasificación y Priorización" de los proyectos a realizar. En esta fase, se lleva a cabo la identificación y clasificación de los proyectos e iniciativas relacionados con la seguridad, así como la priorización de estos. Implica evaluar la importancia y el impacto de cada proyecto en función de los riesgos y necesidades de seguridad de la organización. La priorización de los proyectos es crucial para asignar recursos de manera efectiva y garantizar que se aborden primero los aspectos de seguridad más críticos.

Se tiene entonces la siguiente propuesta para la clasificación y priorización de los proyectos dados:

PRIORIDAD ALTA: Proyecto 4.

- Implementación del Programa de Recuperación ante Desastres

Importancia: Garantiza la recuperación efectiva de sistemas ante eventos imprevistos, fundamental para la continuidad operativa.

Impacto: Crítico en la seguridad y disponibilidad de datos.

Plazo: 6 meses.

Objetivo: Desarrollar un programa formativo para el personal en respuesta a desastres informáticos para garantizar una adecuada recuperación de sistemas afectados por eventos imprevistos.

Acciones Clave: Definir una ruta para la recuperación, capacitar al personal en ella y establecer planes de acción específicos.

PRIORIDAD ALTA: Proyecto 5.

- Desarrollar y/o Actualizar la Política de Seguridad de la Información.

Importancia: Fundamenta la seguridad, incluyendo aspectos clave como el uso seguro de herramientas digitales y protección de datos.

Impacto: Afecta la cultura de seguridad y prácticas diarias del personal.

Plazo: 9 meses.

Objetivo: Mantener una política integral de seguridad que incluya capacitación en aspectos clave, como el uso seguro de herramientas digitales y la protección de datos.

Acciones Clave: Conformar un plan semestral de reinducción al personal, donde se socialice la política actualizada anualmente.

PRIORIDAD MEDIA: Proyecto 3

- Contratación de Pentesting.

Importancia: Identificar y corregir vulnerabilidades en sistemas.
Impacto: Mejora la robustez de la seguridad.
Plazo: 12 meses.
Objetivo: Identificar y corregir vulnerabilidades en los sistemas de información del hospital para fortalecer la seguridad.
Acciones Clave: Realizar análisis periódicos y establecer planes de acción basados en informes de pentesting.

PRIORIDAD MEDIA: Proyecto 6

- Despliegue de Plan de Concienciación en Seguridad.

Importancia: Aumentar la conciencia y comprensión sobre ciberseguridad en todo el personal.
Impacto: Cultural, mejorando la comprensión de la importancia de medidas preventivas.
Plazo: 9 meses.
Objetivo: Aumentar la conciencia y comprensión sobre ciberseguridad en todo el personal.
Acciones Clave: Realizar sesiones de formación y uso de incentivos para fomentar la participación.

PRIORIDAD BAJA: Proyecto 2

- Implementación de la metodología de Gestión de Riesgos

Importancia: Capacitar al personal en la identificación y gestión de riesgos.
Impacto: Fortalece la cultura de seguridad.
Plazo: 6 meses.
Objetivo: Capacitar al personal en la identificación y gestión de riesgos relacionados con la seguridad de la información en sus procesos.
Acciones Clave: Sesiones de formación centradas en la metodología y formatos establecidos.

PRIORIDAD BAJA: Proyecto 1

- Creación del Comité de Seguridad de la Información CSI

Importancia: Supervisar la implementación del PDS.
Impacto: Coordinación y cumplimiento de controles y procedimientos.
Plazo: 6 meses.
Objetivo: Supervisar la implementación del PDS y asegurar el cumplimiento de los controles y procedimientos de seguridad.
Acciones Clave: Formar un comité multidisciplinario y definir responsabilidades.

PRIORIDAD BAJA: Proyecto 8

- Política de copias de seguridad

Importancia: Salvaguarda de información corporativa crítica.
Impacto: Mitigación de pérdida de datos.
Plazo: 12 meses.
Objetivo: Salvaguardar información crítica ante posibles pérdidas o ataques.
Acciones Clave: Análisis e implementación de políticas y restauraciones periódicas.

PRIORIDAD MÍNIMA: Proyecto 7

- Mejorar Coordinación entre RRHH y Departamento TIC

Importancia: Coordinación entre áreas clave.
Impacto: Mejora en la respuesta ante contingencias y apego a TICS
Plazo: 3 meses.
Objetivo: Mejorar la coordinación entre áreas clave para una mejor respuesta ante contingencias y manejo correcto de TICS dispuestas.
Acciones Clave: Sesiones de formación para personal nuevo y requisitos específicos para los cargos.

PRIORIDAD MÍNIMA: Proyecto 9

- Regulación de los servicios TIC prestado por terceros.

Importancia: Establecer acuerdos con proveedores externos.
Impacto: Garantizar servicios adecuados a necesidades hospitalarias.
Plazo: 12 meses.

Objetivo: Asegurar acuerdos con proveedores externos que se ajusten a las necesidades del hospital.
Acciones Clave: Revisión y estandarización de contratos y pliegos, exigiendo certificaciones y experiencia específica.

7.4.5 Aprobar el Plan Director de Seguridad (Fase 5).

La Fase 5 del Plan Director de Seguridad para hospitales públicos en Colombia corresponde a la "Aprobación del Plan Director de Seguridad". En esta etapa, después de identificar, clasificar y priorizar las acciones y proyectos de seguridad, se lleva a cabo la revisión y aprobación del plan por parte de la Dirección de la institución hospitalaria o la Gerencia de TICs. Se realiza una evaluación detallada del plan, permitiendo ajustes en su alcance, duración o prioridad de proyectos si es necesario. Este proceso de revisión puede repetirse hasta obtener una versión final formalmente aprobada por la alta dirección.

Una vez aprobado, se debe socializar a todo el personal, subrayando la importancia de su colaboración para la implementación efectiva del mismo en la institución.

7.4.6 Puesta en marcha (Fase 6).

La Fase 6 del Plan Director de Seguridad se enfoca en la "Puesta en Marcha" del plan. Tras la aprobación por parte de la alta dirección, esta etapa implica la implementación del plan aprobado. Se asignan responsables o coordinadores para cada proyecto, se les proporcionan los recursos necesarios y se puede crear un Comité de Gestión para supervisar su desarrollo. Se establece la periodicidad para el seguimiento de los proyectos y del Plan Director de Seguridad en su conjunto. Además, se enfoca en el seguimiento a las oportunidades de mejora identificadas en auditorías o análisis de riesgos a medida que se cumplen los objetivos planificados.

Esta fase busca asegurar que las acciones propuestas se ejecuten de manera efectiva para mejorar la seguridad de la institución hospitalaria

8. CONCLUSIONES

Se ha identificado un conjunto de amenazas y riesgos de seguridad relevantes para los sistemas misionales y aplicaciones de los hospitales públicos en Colombia. Estas amenazas incluyen la exposición a ataques cibernéticos, la pérdida de datos críticos y la interrupción de servicios esenciales.

La aplicación de metodologías y marcos reconocidos ha permitido un enfoque sistemático y completo para la identificación de riesgos críticos, proporcionando una base sólida para el desarrollo del plan director de seguridad digital.

La evaluación de las amenazas identificadas en el análisis de riesgos ha permitido establecer una matriz de seguridad de la información sólida y eficaz que sirve como fundamento para el desarrollo de controles y procedimientos de seguridad cibernética.

La adopción de recomendaciones de marcos y estándares internacionales mejora la consistencia y la robustez de los controles y procedimientos de seguridad cibernética, lo que fortalece la postura de seguridad de los hospitales públicos en Colombia.

La propuesta de un Plan director de seguridad digital que incluye capacitación en ciberseguridad para el personal administrativo y asistencial es un paso esencial para fortalecer la seguridad en los hospitales públicos. Esta capacitación continua es fundamental para garantizar que el personal sea consciente de los riesgos y sepa cómo contribuir a la protección de la información.

La adopción de controles, procedimientos y políticas en seguridad cibernética constituyen una guía clara y eficaz para la protección de la información y los activos de los hospitales públicos en Colombia, así como para mitigar los riesgos identificados, al aplicar esta estrategia integral, las instituciones se encuentran en una posición más sólida para enfrentar los desafíos de seguridad.

9. RECOMENDACIONES

Continuar actualizando regularmente el análisis de riesgos de seguridad para mantenerse al día con las amenazas en constante evolución. Esto implica la revisión periódica de las amenazas y la evaluación de nuevos riesgos emergentes.

Fomentar la colaboración con organizaciones de salud referentes y compartir las mejores prácticas en la identificación de amenazas y riesgos de seguridad. Esto puede ayudar a mejorar la eficacia de los esfuerzos de seguridad digital.

Continuar monitoreando y actualizando regularmente la matriz de seguridad de la información a medida que evolucionen las amenazas y cambien las circunstancias operativas. Esto asegurará que los controles sean pertinentes y efectivos en todo momento.

Fomentar la capacitación del personal encargado de implementar y mantener los controles y procedimientos de seguridad cibernética, garantizando que estén plenamente conscientes de las mejores prácticas y los estándares internacionales para su correcta implementación.

Implementar programas de capacitación continuos en ciberseguridad para el personal, adaptados a diferentes niveles de conocimiento y responsabilidades. Esto garantizará que todos estén equipados con las habilidades necesarias para proteger la información.

Establecer una cultura de seguridad cibernética en la que se promueva la responsabilidad individual y colectiva en la protección de la información. Esto puede lograrse a través de campañas de concientización y la inclusión de la seguridad cibernética en la evaluación del desempeño del personal.

10. BIBLIOGRAFÍA

ALBERTS, C. y DOROFEE, A. (2002). "Gestión de riesgos de seguridad de la información: el enfoque OCTAVE". Boston, Estados Unidos: Addison-Wesley.

ALZURI, P. (ed.) (2021) “Protegiendo la Salud digital - Una guía de ciberseguridad en el sector salud”. {En línea}. {14 Mayo 2023} disponible en: (https://publications.iadb.org/es/publications/spanish/viewer/protegiendo-la-salud-digital-una-guia-de-ciberseguridad-en-el-sector-de-salud.pdf)

AMAYA, Camilo. (2013). "MAGERIT: metodología práctica para gestionar riesgos" {en línea}. {15 marzo 2023} disponible en: (https://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/)

CAWTHRA, J., WANG, S., HODGES, B., ZHENG, K., WILLIAMS, R., KURUVILLA, J., PELOQUIN, C., LITTLEFIELD, K. y NEIMEYER, B. (2020). "Securing Picture Archiving and Communication System (PACS): Cybersecurity for the Healthcare Sector". Special Publication (NIST SP). National Institute of Standards and Technology, Gaithersburg, MD. {en línea}. {22 de marzo de 2024} disponible en: (https://doi.org/10.6028/NIST.SP.1800-24).

CENTRO CRIPTOLÓGICO NACIONAL. (2020). "CCN STIC 803: Valoración de sistemas en el ENS". Madrid: Guía del Esquema Nacional de Seguridad, n. 803. {en línea}. { 22 octubre de 2023} disponible en: (https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/682-ccn-stic-803-valoracion-de-sistemas-en-el-ens-1/file.html).

CHECK POINT RESEARCH. (26 de octubre de 2022). "1 de cada 42 organizaciones del sector salud es víctima de ransomware" {en línea}. {15 octubre de 2023} disponible en: (https://www.itsitio.com/us/1-de-cada-42-organizaciones-del-sector-salud-es-victima-de-ransomware)

CIBERSEGURIDAD EN EL SECTOR PÚBLICO. (2022). Guías: Sector público. {en línea}. {16 octubre de 2023.} disponible en: (https://ciberseguridad.com/guias/sector-publico/)

CISCO. (s.f.). "¿Qué es la ciberseguridad?". {en línea} { 22 noviembre de 2023} disponible en (https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html)

CNN en Español. (2023). "Colombia: ciberataque a IFX Networks" {en línea}. {22 noviembre de 2023} disponible en (https://cnnespanol.cnn.com/2023/09/14/colombia-ciberataque-ifx-networks-orix/)

COLOMBIA. CONGRESO DE LA REPÚBLICA. (2012). "Por la cual se dictan disposiciones generales para la protección de datos personales. Ley 1581 de 2012". Bogotá, D.C.: Diario Oficial. {en línea}. {octubre de 2023} disponible en: (https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981)

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273 (5 de enero de 2009). "Por medio de la cual se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones". Bogotá, D.C.: Diario Oficial. 2009. nro. 47.223. p. 1-4. {en línea}. {12 octubre de 2023} disponible en: (http://secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html)

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 23 (11 de febrero de 1981). "Por la cual se dictan normas en materia de ética médica. Ley 23 de 1981". Bogotá, D.C.: Diario Oficial. 1981. nro. 35.657. p. 1-5. {en línea}. {12 octubre de 2023} disponible en: (http://www.secretariasenado.gov.co/senado/basedoc/ley_0023_1981.html)

COLOMBIA. MINISTERIO DE SALUD. (8 de julio de 1999) "Por la cual se establecen normas para el manejo de la historia clínica. Resolución 1995 de 1999". Bogotá, D.C.: Diario Oficial. {en línea}. {10 octubre de 2023} disponible en: (https://www.minsalud.gov.co/sites/rid/Lists/BibliotecaDigital/RIDE/DE/DIJ/Resoluci%C3%B3n_1995_de_1999.pdf)

COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Decreto 338 (8 de marzo de 2022). "Crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones. Bogotá, D.C.: Diario Oficial. 2022. nro. 51.667. p. 1-32. " {en línea} {18 octubre de 2023} disponible en: (https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=181866)

COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Resolución 1519 (24 de agosto de 2020). "Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos". {en línea}. {18 octubre de 2023} disponible en: (https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Resolucion/30044657)

COLOMBIA. PRESIDENCIA DE LA REPÚBLICA. Directiva Presidencial 03 (15 de marzo de 2021). "Por la cual se establecen lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos por parte de las entidades públicas de la rama ejecutiva del orden nacional". Bogotá, D.C.: Diario Oficial. 2021. nro. 51.637. p. 1-8. {en línea}. {20 octubre de 2023} disponible en: (https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=160326).

CONSULTORSALUD SAS. (2023). "Sector salud afectado en ciberataque a entidades del Estado". {en línea}. {20 octubre de 2023} disponible en: (https://consultorsalud.com/ciberataques-entidades-del-estado/)

DELOITTE. (s.f.). "Medtech and the Internet of Medical Things" Deloitte. {en línea}. {20 marzo de 2023} disponible en: (https://www2.deloitte.com/global/en/pages/life-sciences-and-healthcare/articles/medtech-internet-of-medical-things.htm).

DÍAZ, L. L. (2023). "¿Qué pasa con la ciberseguridad en las plataformas de salud de Colombia?". El Tiempo. {en línea}. {24 marzo de 2023} disponible en (https://www.eltiempo.com/tecnosfera/novedades-tecnologia/ciberseguridad-en-las-plataformas-de-salud-de-colombia-736510)

EL ECONOMISTA. (2023). "El estado de la ciberseguridad en el sector de la salud". {en línea}. {26 octubre de 2023} disponible en: (www.eleconomista.es/opinion/noticias/12499014/10/23/el-estado-de-la-ciberseguridad-en-el-sector-de-la-salud.html)

ENISA. (Diciembre de 2018). "ICT security certification opportunities in the healthcare sector" {en línea}. { noviembre 13 de 2023} disponible en: (https://www.enisa.europa.eu/publications/healthcare-certification)

FUNCION PÚBLICA. (16 de mayo de 2022). "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital" Bogotá: FUNCION PÚBLICA. {en línea}. {24 de octubre de 2023} disponible en: (https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=186766)

HEALTH SECTOR COORDINATING COUNCIL. (10 de junio de 2019). "The joint security plan (JSP)" {en línea}. {23 de noviembre de 2023}. Health Sector Council. disponible en: (https://healthsectorcouncil.org/the-joint-security-plan)

HERNÁNDEZ ARMAS, J. A. (2020). "Ciberseguridad en el entorno sanitario". Hospitecnia, Boletín 37, 09/11/2020, p.p 1-8. {En línea}. {23 de marzo de 2024} disponible en: (https://hospitecnia.com/sites/default/files/inline-files/JAHernandez-seeic-ciberseguridad-entorno-sanitario.pdf).

HITRUST - Health Information Trust Alliance. (2023). "HITRUST Cybersecurity Framework". {en línea}. {22 de marzo de 2024} disponible en: (https://hitrustalliance.net/hitrust-framework)

HUERTA, A. (2012, April 2). Introducción al Análisis de Riesgos – Metodologías . Security Art Work. {en línea}. {22 de marzo de 2024} disponible en: (https://www.securityartwork.es/2012/04/02/introduccion-al-analisis-de-riesgos-%E2%80%93-metodologias-ii/)

IBM. (s.f.). "Seguridad informática". {en línea}. {22 de noviembre de 2023} disponible en: (https://www.ibm.com/mx-es/topics/it-security)

INFOBAE. (2023). "Las 34 empresas que fueron hackeadas en Colombia durante 2022". {en línea}. {26 de octubre de 20} disponible en: (www.infobae.com/america/tecno/2023/01/02/las-34-empresas-que-fueron-hackeadas-en-colombia-durante-2022/)

ISO. (2016). "ISO 27799:2016. Health Informatics: Information security management in health". {en línea} {noviembre 11 de 2023} disponible en (https://www.iso.org/standard/62777.html)

ISO27000. (2020). "Glosario: Lista de términos relacionados con la serie ISO 27000 y la seguridad de la información". {en línea}. {noviembre de 2023} disponible en: (https://www.iso27000.es/glosario.html)

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. (2012). "MAGERIT: Metodología para la gestión de riesgos de seguridad de la información". {En línea}. {24 octubre de 2023} disponible en: (https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html)

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. (2012). "MAGERIT versión 3 (versión española): Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I: Método". NIPO: 630-12-171-8. P.p. 39. {en línea}. {24 octubre de 2023} disponible en: (https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html)

MINISTERIO DE HACIENDAS Y ADMINISTRACIÓN PÚBLICA DE GOB. ESPAÑA. (2012). “Magerit v.3 : Metodología de Análisis y gestión de riesgos de los sistemas de información. PAe”. {en línea}. {24 octubre de 2023} disponible en: (http://imagenesbibliotecacentral.minhap.gob.es/pdfpublicaciones/Publicaciones%20gratuitas%20pendientes%20Millennium/completo.pdf)

MINISTERIO DE HACIENDAS Y ADMINISTRACIÓN PÚBLICA DE GOB. ESPAÑA. (2012). “Magerit Versión 3.0: Catalogo de Elementos Libro 2”. {en línea}. {24 octubre de 2023} disponible en: (https://pilar.ccn-cert.cni.es/index.php/docman/documentos/2-magerit-v3-libro-ii-catalogo-de-elementos)

MINISTERIO DE SALUD Y PROTECCIÓN SOCIAL DE COLOMBIA. (2022). “Comportamiento del aseguramiento en salud”. {en línea}. {14 marzo de 2023} disponible en: (https://www.minsalud.gov.co/proteccionsocial/Regimensubsidiado/Paginas/coberturas-del-regimen-subsidiado.aspx)

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. (2021). "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital. Resolución 500 de 2021". Bogotá, D.C.: Diario Oficial. {en línea}. {3 octubre de 2023} disponible en: (https://normograma.mintic.gov.co/docs/pdf/resolucion_mintic_0500_2021.pdf)

MINTIC. (10 de marzo de 2021). "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital" Bogotá: MINTIC. {en línea}. {24 de octubre de 2023} disponible en: (https://gobiernodigital.mintic.gov.co/692/articles-162625_recurso_2.pdf)

MINSALUD - Resolución 3100 de 2019 “Habilitación de Servicios de Salud y reps”. (2019, November 28). {en línea}. {25 de marzo de 2024} disponible en: (https://consultorsalud.com/resolucion-3100-de-2019-nueva-habilitacion-de-servicios-de-salud-y-reps/#TELEMEDICINA_INTERACTIVA)

NIST - National Institute of Technical Standards, (2021). "SP1800-30. Securing Telehealth Remote Patient Monitoring Ecosystem (2nd Versión)". {en línea}. {29 de marzo de 2024} disponible en: (https://csrc.nist.gov/publications/detail/sp/1800-30/draft).

OMS Organización Mundial de la Salud. (2021). "Ethics and Governance of Artificial Intelligence for Health: WHO guidance". Pp. 57. {en línea}. {27 de marzo de 2024} disponible en: (https://iris.who.int/bitstream/handle/10665/341996/9789240029200-eng.pdf?sequence=1)

PARLAMENTO EUROPEO Y CONSEJO DE LA UNIÓN EUROPEA. (2022). "Directiva (UE) 2022/2555". {en línea}. {25 de marzo de 2024} disponible en: (https://www2.deloitte.com/es/es/pages/risk/articles/directiva-nis-2.html)

PORTAFOLIO. (11 de octubre de 2022). "Ataques cibernéticos ponen en ‘jaque’ el sector de la salud". Bogotá: Portafolio. {en línea}. {23 de noviembre de 2023} disponible en: (https://www.portafolio.co/negocios/empresas/ataques-ciberneticos-ponen-en-jaque-el-sector-de-la-salud-572476)

REVISTA SALUD DIGITAL LATINO AMÉRICA. (2019). "HOSPITALES: Uno de los principales blancos de ciberataques". Bogotá: Salud Digital. {en línea}. {3 octubre de 2023} disponible en: (https://www.revistasaluddigital.com/es/noticia/hospitales-uno-de-los-principales-blancos-de-ciberataques)

RODRÍGUEZ, N. (2022) "Blockchain en la Atención Médica: Casos de uso Y aplicaciones", 101 Blockchains. {en línea}. {27 de marzo de 2024} disponible en (https://101blockchains.com/es/blockchain-atencion-medica/).

SABATINO, C. (2023). "Confidencialidad e HIPAA". En Manual MSD versión para profesionales. {en línea}. {21 de marzo 2024}. Disponible en (https://www.msdmanuals.com/es-co/professional/temas-especiales/cuestiones-medicolegales/confidencialidad-e-hipaa).

VANGUARDIA. (2024). "Así Puede prevenir los riesgos cibernéticos en el sector salud". {en línea} {23 de marzo de 2024} disponible en: www.vanguardia.com. (https://www.vanguardia.com/mundo/tecnologia/2024/03/20/asi-puede-prevenir-los-riesgos-ciberneticos-en-el-sector-salud/)

11. ANEXOS

Anexo A. Tabla para evaluación de madurez del Plan de Seguridad Conjunta (JSP).

COMPONENTE DEL PLAN	DESCRIPCION	NIVEL DE MADUREZ ACTUAL	NIVEL DE MADUREZ OBJETIVO	HITOS
ORGANIZACIÓN				
ESTRUCTURA	¿La organización cuenta con un director de seguridad CISO? ¿Tiene la organización una función de seguridad del producto? ¿Están claramente definidas las funciones y responsabilidades de las funciones de seguridad del producto? ¿La función de seguridad del producto cuenta con el personal adecuado?	[1-5]	[1-5]	[AAAA/MM]
GOBERNANZA	¿Existen políticas y/o procedimientos que cubran la seguridad del producto? ¿El liderazgo organizacional ha aprobado la política y los procedimientos de seguridad del producto? ¿Se audita la organización según las políticas/procedimientos de seguridad del producto? ¿Con que frecuencia? ¿La función de seguridad? ¿Se informan las métricas de seguridad del producto a los lideres como el Director de Calidad, El Director de Seguridad Medica, el líder de I+D, etc? Si es así, ¿Con que frecuencia?			
GESTION DE RIESGOS				
REGISTRO DE RIESGOS	¿Se ha creado un inventario de productos para productos comercializados y productos en desarrollo? ¿Se rastrean los riesgos de seguridad en los sistemas de seguimiento de defectos de I+D, en los archivos de historial de diseño o en los archivos de gestión de riesgos? ¿Se rastrean los riesgos de seguridad en los sistemas de manejo de quejas de servicio o en los archivos de gestión de riesgos?	[1-5]	[1-5]	[AAAA/MM]
EVALUACION DE RIESGOS	¿Se ha establecido un método utilizado para la evaluación de riesgos de seguridad? ¿Se han actualizado las políticas y procedimientos para incorporar la evaluación de riesgos de seguridad y la derivación a otros tipos de evaluación de riesgos?			
CADENA DE SUMINISTRO	¿Se evalúan y gestionan los entornos de desarrollo y fabricación para garantizar el cumplimiento de la política de seguridad de la información?	[1-5]	[1-5]	[AAAA/MM]
ENTIDADES DE TERCEROS	¿Se han evaluado a terceros en función de los componentes de este marco? ¿Se realizan evaluaciones periódicas de seguridad a terceros? ¿La organización tiene requisitos de seguridad en el lenguaje del contrato para proveedores y terceros?			
EXCEPCIONES	¿Se documentan las excepciones a los componentes del marco en el historial de diseño y/o en los archivos de gestión de riesgos? ¿Se proporcionan controles compensatorios relacionados con las excepciones en la documentación de seguridad del cliente?			
DISEÑO Y CONTROL				

REQUISITOS DE SEGURIDAD PARA DISEÑO DE ENTRADA	¿Se incorporan los requisitos de ciberseguridad en diseños de entrada para los productos en desarrollo?	[1-5]	[1-5]	[AAAA/MM]
NORMAS Y PRUEBAS (TEST)	¿Se incorporan estándares de endurecimiento del sistema, parches del sistema y escaneo de vulnerabilidades en las prácticas de desarrollo de productos? ¿Se incorporan estándares de codificación segura y análisis de código en las prácticas de desarrollo de productos? ¿Se realiza pruebas de seguridad, como pruebas de penetración, realizadas por profesionales de ciberseguridad capacitados durante el control de diseño? ¿Se realiza pruebas de robustez durante el desarrollo de productos?			
GESTION DE VULNERABILIDADES Y GESTION DE PARCHES	¿Se han establecido procesos para monitorear, identificar, evaluar, remediar y validar parches de seguridad para el software del producto y componentes de terceros? ¿Se despliegan los parches validados utilizando un método establecido? ¿Es posible generar informes que muestren fallos en la aplicación de parches? ¿Existe una página web pública a la que los clientes puedan acudir para identificar nuevos parches?			
REQUISITOS DEL CLIENTE	¿El personal de servicio y soporte tiene procedimientos para solicitar acceso a los sistemas del cliente y restaurar medidas de seguridad? ¿Existen controles para que el personal de servicio se autentique de manera única en los sistemas del cliente? ¿Se han establecido políticas y procedimientos en torno al uso de medios extraíbles con productos y al manejo de los datos del cliente?			
PLAN DE GESTION DE CIBERSEGURIDAD	¿Se han establecido planes para mantener la seguridad a lo largo del ciclo de vida de un producto? ¿Los productos tienen fechas previstas de fin de vida y/o fin de soporte establecidas teniendo en cuenta el soporte de productos y componentes de terceros?			
MANEJO DE QUEJAS				
ESCALAMIENTO DE QUEJAS DE CLIENTES	¿Las procedimientos de escalación definen señales de ciberseguridad? ¿Se documentan los problemas de ciberseguridad informados por los clientes en los sistemas de manejo de quejas? ¿Se han establecido procesos para garantizar la revisión de quejas informadas relacionadas con la ciberseguridad?	[1-5]	[1-5]	[AAAA/MM]
CONSIDERACION DE INFORMES	¿Se han establecido procesos para notificar a un CERT (Equipo de Respuesta a Incidentes de Seguridad Cibernética), ISAO (Organización de Compartición de Información de Seguridad en la Industria) y/o regulador, según corresponda, sobre problemas de ciberseguridad informados?			
GESTION DE INCIDENTES DE SEGURIDAD, RESPUESTA Y COMUNICACIÓN	¿Los equipos internos se involucran en un plazo de 30 días a partir de un incidente de seguridad informado y se actualizan cada 60 días a partir de entonces? ¿Se practican regularmente los procesos de respuesta a incidentes? ¿Existe una página web pública donde se puedan publicar boletines o avisos relacionados con vulnerabilidades o incidentes?			
PLANIFICACION DE LA REMEDIACION	¿Existen criterios claramente definidos para la remedición de riesgos de seguridad en productos en desarrollo? ¿Existen criterios claramente definidos para la remedición de riesgos de seguridad en productos comercializados? ¿Se comunican vulnerabilidades de nivel medio a crítico			

	a los clientes en un plazo de 30 días? ¿Se remedian vulnerabilidades de nivel medio a crítico en un plazo de 60 días?			

NIVELES DE MADUREZ

Nivel 1: Inicial - Se han presentado uno o varios componentes del marco a las partes internas y se han elaborado planes, pero no existe un proceso probado o formalizado ni personas responsables.
Nivel 2: Gestionado - Los componentes del marco se han planificado y la ejecución está en marcha. Los planes establecidos aseguran que los componentes del marco se realicen, midan y controlen con visibilidad rutinaria proporcionada a la dirección.
Nivel 3: Definido - Se han logrado todos los componentes del marco. Se han establecido políticas y procedimientos formales, así como se han incorporado en los sistemas de gestión de calidad. Se ha proporcionado a las partes internas una descripción clara de las actividades y se les ha proporcionado capacitación. Los entregables para el componente del marco están bien documentados y se revisan periódicamente entre las partes internas.
Nivel 4: Cuantitativamente Gestionado - Se han logrado todos los aspectos de un componente del marco y se recopilan diversas métricas de rendimiento para determinar áreas de mejora. Las métricas de rendimiento que se pueden considerar incluyen el número de quejas de seguridad informadas, el tiempo promedio de respuesta a los clientes, el tiempo promedio de cierre de las quejas de seguridad, el tiempo promedio de comunicación con el cliente, el número de defectos de ciberseguridad fuera de control de diseño, el tiempo promedio de remedio, el porcentaje de parches aplicados con éxito de forma remota a productos desplegados, el porcentaje de parches aplicados con éxito por los clientes a productos desplegados, y el porcentaje de parches aplicados con éxito por el servicio a productos desplegados.
Nivel 5: Optimización - Las métricas recopiladas sobre un componente del marco se revisan periódicamente y se establecen planes de mejora del proceso. Se establecen objetivos cuantitativos de mejora del proceso y se revisan continuamente para reflejar los cambios en los estándares de la industria y en el Plan de Seguridad Conjunta (JSP). La revisión del análisis cuantitativo produce resultados predecibles. Se comprende la variación del proceso en múltiples productos y, cuando la variación produce un rendimiento deficiente, se aborda mediante la creación de planes de mejora del proceso con propiedad interfuncional. El proceso de mejora continua es intrínseco para todos los involucrados en el diseño, desarrollo, producción, implementación, servicio y soporte de dispositivos médicos y tecnología de la información en salud.