ESPECIALIZACINON EN CIBERSEGURIDAD

ESTUDIO PARA EL FORTALECIMIENTO DE LA CIBERSEGURIDAD EN EL HOSPITAL UNIVERSITARIO SANTA SOFÍA DE CALDAS BASADO EN LAS BUENAS PRÁCTICAS DE LA ISO 31000.

OSCAR DAVID TRUJILLO SOTO
CARLOS JAIME POSADA ALVAREZ

Universidad® Católica de Manizales
VIGILADA MINEDUCACIÓN
Obra de Iglesia de la Congregación
Hermanas de la Caridad Dominicas de La Presentación de la Santísima Virgen

ESTUDIO PARA EL FORTALECIMIENTO DE LA CIBERSEGURIDAD EN EL HOSPITAL UNIVERSITARIO SANTA SOFÍA DE CALDAS BASADO EN LAS BUENAS PRÁCTICAS DE LA ISO 31000

Modalidad de grado: Proyecto de Estudio

Director Especialización en Ciberseguridad

JHON CESAR ARANGO SERNA

CEO EN CIBERSEGURIDAD

Asesor Temático

HECTOR ROBERTO GORDON QUINCHE[1]

OSCAR DAVID TRUJILLO SOTO

CARLOS JAIME POSADA ALVAREZ

UNIVERSIDAD CATOLICA DE MANIZALES

FACULTAD DE INGENIERIA Y ARQUITECTURA

ESPECIALIZACION EN CIBERSEGURIDAD

MANIZALES, CALDAS

2024

[1] ORCID 0000-0002-3453-8226

Contenido

RESUMEN

Este estudio examina métodos específicos para mejorar la ciberseguridad en el Hospital Universitario Santa Sofía de Caldas, utilizando las buenas prácticas de la ISO 31000. Las recomendaciones y buenas prácticas de otros estándares y guías internacionales sobre el manejo de riesgos tecnológicos se han integrado en una metodología integral. La ISO 31000 establece estándares para la gestión de riesgos, pero no especifica cómo implementarlos.[2]

La metodología se enfoca en los riesgos tecnológicos en el entorno hospitalario porque el creciente uso de tecnologías de la información puede generar vulnerabilidades en la seguridad. Se propone un enfoque integral que abarca la seguridad de la infraestructura (nivel físico), los sistemas de información (nivel lógico) y las medidas organizacionales (factor humano) desde una perspectiva tecnológica.[3]

Para garantizar mejoras continuas en la seguridad cibernética del hospital, se implementó un proceso de gestión basado en el modelo PHVA (Planificar, Hacer, Verificar, Actuar). Este método sistemático permite una gestión proactiva y efectiva de la ciberseguridad, lo que reduce los riesgos asociados con el uso de la tecnología de la información en los hospitales.

En conclusión, este estudio proporciona pautas prácticas y completas para mejorar la ciberseguridad en el Hospital Universitario Santa Sofía de Caldas, asegurando la protección de los activos digitales y la confidencialidad de la información confidencial.[4]

[2] Sittig, D. F., Singh, H., & Ash, J. S. (2011). Safety Assurance Factors for Electronic Health Record Resilience (SAFER): Study protocol. *BMC Medical Informatics and Decision Making*, 11(1), 54.

[3] Hynes, D. M., & Tarlov, E. (2016). Reflections on the learning health system. *Health Services Research*, 51(Suppl 1), 2456-2461.

[4] Goodman, K. W. (2017). Ethics, information technology, and public health: New challenges for the clinician-patient relationship. *Journal of General Internal Medicine*, 32(8), 876-878.

ABSTRACT

This study examines specific methods for improving cybersecurity at the Santa Sofia University Hospital in Caldas, using ISO 31000 best practices. Recommendations and best practices of other international standards and guidelines on technology risk management have been integrated into a comprehensive methodology. ISO 31000 sets standards for risk management, but does not specify how to implement them.

The methodology focuses on technological risks in the hospital environment because the increasing use of information technologies can generate security vulnerabilities. An integrated approach is proposed that covers infrastructure security (physical level), information systems (logical level) and organizational measures (human factor) from a technological perspective.

To ensure continuous improvements in hospital cybersecurity, a management process based on the PHVA model was implemented (Planificar, Hacer, Verificar, Actuar). This systematic approach enables proactive and effective management of cybersecurity, which reduces the risks associated with the use of information technology in hospitals.

In conclusion, this study provides practical and comprehensive guidelines for improving cybersecurity at the University Hospital Santa Sofia de Caldas, ensuring the protection of digital assets and the confidentiality of confidential information.

1. INTRODUCCIÓN

El uso omnipresente de las tecnologías de la información (TI) en el entorno dinámico actual ha cambiado fundamentalmente la operativa de las organizaciones, independientemente de su naturaleza o sector. La creciente dependencia de las TI ha aumentado la exposición a amenazas cibernéticas. Las organizaciones deben incluir en sus planes de negocios la protección de sus sistemas informáticos y datos confidenciales.[5]

El "Estudio para el Fortalecimiento de la Ciberseguridad en el Hospital Universitario Santa Sofía de Caldas basado en las Buenas Prácticas de la ISO 31000" tiene como objetivo abordar los desafíos específicos de seguridad cibernética que enfrenta una institución significativa como el Hospital Universitario Santa Sofía de Caldas. Este estudio busca fortalecer la postura de los hospitales en cuanto a la ciberseguridad mediante la implementación de buenas prácticas reconocidas a nivel internacional, reconociendo la importancia de garantizar la integridad, confidencialidad y disponibilidad de los datos médicos y la infraestructura tecnológica en un entorno hospitalario.

La gestión efectiva de los riesgos tecnológicos se ha convertido en un componente esencial para proteger los activos de información cruciales y garantizar la continuidad de las operaciones en un entorno cada vez más digitalizado e interconectado. El propósito de este proyecto es adaptar y aplicar el marco de gestión de riesgos establecido por la norma ISO 31000 a los problemas de seguridad cibernética del Hospital Universitario Santa Sofía de Caldas.[6]

[5] Hernandez, R., Fernandez, C., & Baptista, P. (2014). Metodología de la investigación (6th ed.). McGraw-Hill Education
[6] Yin, R. K. (2018). *Case study research and applications: Design and methods* (6th ed.). SAGE Publications.

El objetivo principal de este estudio es investigar y comprender las amenazas y vulnerabilidades específicas de seguridad cibernética que enfrentan los hospitales, centrándose en la detección temprana y la mitigación proactiva de riesgos. Se busca desarrollar estrategias integrales que aborden tanto los aspectos tecnológicos como humanos de la seguridad cibernética, reconociendo la intersección entre tecnología, procesos y personas en la seguridad cibernética.

Este proyecto tiene como objetivo no solo mejorar la comprensión de la seguridad cibernética en el Hospital Universitario Santa Sofía de Caldas, sino también avanzar en la comprensión de la seguridad cibernética en entornos hospitalarios. Se espera que los hallazgos y recomendaciones obtenidos no solo beneficien al hospital en cuestión, sino que también sirvan como modelo para otras instituciones médicas que experimenten problemas similares con la seguridad de la información[7].

[7] Bryman, A. (2016). *Social research methods* (5th ed.). Oxford University Press.

2. OBJETIVOS DE LA INVESTIGACIÓN

2.1 OBJETIVO GENERAL

Realizar un estudio exhaustivo sobre la seguridad cibernética en el Hospital Universitario Santa Sofía de Caldas, con el objetivo de fortalecer sus prácticas de seguridad informática y proteger la integridad, confidencialidad y disponibilidad de la información, basándose en las buenas prácticas establecidas en la norma ISO 31000[8].

2.2 OBJETIVOS ESPECÍFICOS:

- Identificar y analizar las amenazas y vulnerabilidades específicas en seguridad cibernética que enfrenta el Hospital Universitario Santa Sofía de Caldas, teniendo en cuenta los peligros relacionados con la digitalización de los registros médicos y la infraestructura tecnológica[9].

- Evaluar el nivel de cumplimiento del hospital con los principios y lineamientos de la norma ISO 31000 para la gestión de riesgos para encontrar áreas de mejora y oportunidades de fortalecimiento en seguridad cibernética.

- Realizar un estudio basado en el análisis de riesgos y las buenas prácticas de la norma ISO 31000 para recomendar mejoras en la seguridad cibernética del hospital con el objetivo de proteger mejor la información y los sistemas informáticos.

[8] Kim, H. K., Choi, Y. H., Lee, J., & Kim, S. R. (2018). Development and validation of a framework for assessing the severity of cybersecurity threats in healthcare information technology. Journal of Medical Systems, 42(5), 82.
[9] van den Hooven, J., Sylla, C., & Aloulou, H. (2019). A framework for the proactive management of cybersecurity risks in healthcare organizations. Health and Technology, 9(3), 509-520.

3. AREA PROBLEMÁTICA

3.1 DESCRIPCIÓN DEL PROBLEMA

El Hospital Universitario Santa Sofía de Caldas, al igual que otras instituciones médicas en el mundo, se encuentra en una situación complicada en cuanto a la seguridad cibernética. La creciente dependencia de la tecnología digital y la interconexión de los sistemas médicos ha aumentado las vulnerabilidades cibernéticas, lo que pone al hospital en peligro de comprometer la continuidad de los servicios médicos y la seguridad de la información de los pacientes. En este contexto, hay varios aspectos importantes que reflejan el problema de la ciberseguridad[10]:

3.1 Vulnerabilidades en la Infraestructura Tecnológica

3.1.1 Sistemas de Información Anticuados:

Muchos sistemas de información de los hospitales no se han actualizado o reemplazado adecuadamente, lo que los hace más vulnerables a los ciberataques. Estos sistemas pueden tener configuraciones inseguras que permiten el acceso no autorizado y carecer de los parches de seguridad más recientes.

3.1.2 Falta de Segmentación de la Red:

La falta de segmentación adecuada de la red puede permitir que un ataque en una parte del sistema se propague rápidamente a otros sistemas críticos, lo que aumenta el riesgo de cualquier brecha de seguridad.

[10] Miliard, M. (2019). AHA report warns hospitals about increasing cybersecurity risks. *Healthcare IT News*.Retrieved from https://www.healthcareitnews.com/news/aha-report-warns-hospitals-about-increasing- cybersecurity-risks

3.1.3 Dispositivos Médicos Conectados:

Si no están debidamente asegurados, los dispositivos médicos de la red hospitalaria, como los monitores de pacientes y los equipos de diagnóstico, pueden convertirse en puntos de entrada para los atacantes.

3.2 Comportamiento y Concientización de los Usuarios[11]

3.2.1 Conocimiento Limitado de Ciberseguridad:

Las personas que trabajan en hospitales, como médicos, enfermeras y personal administrativo, pueden no tener conocimientos adecuados sobre las prácticas de ciberseguridad. La falta de conocimiento y capacitación puede conducir a comportamientos de riesgo como el uso de contraseñas ineficaces, la apertura de correos electrónicos de phishing y la negligencia en la protección de datos sensibles.

3.2.2 Comportamientos de Riesgo:

El riesgo de incidentes cibernéticos puede aumentar significativamente con acciones como compartir contraseñas, utilizar dispositivos personales para acceder a la red del hospital y no seguir los protocolos de seguridad establecidos.

3.3 Políticas y Procedimientos de Seguridad

[11] Hassell, J. (2018). Cybersecurity threats in healthcare. *Australian Journal of Emergency Management*, 33(3), 72-75.

3.3.1 Políticas Desactualizadas:

Las políticas y procedimientos de seguridad de un hospital pueden no estar actualizados y no reflejar las mejores prácticas actuales ni las amenazas emergentes. La falta de revisiones y actualizaciones regulares de estas políticas puede causar brechas importantes en la seguridad.

3.3.2 Cumplimiento Inconsistente:

Las políticas y procedimientos pueden ser inconsistentes en su implementación y cumplimiento, incluso si son sólidos. Las medidas de seguridad pueden no ser aplicadas de manera uniforme en toda la organización sin una supervisión y auditoría adecuadas.

3.4 Gestión del Riesgo y Respuesta a Incidentes

3.4.1 Evaluación Inadecuada del Riesgo:

La falta de una evaluación exhaustiva y continua de los riesgos cibernéticos puede conducir a una subestimación de las amenazas y una preparación insuficiente para responder a incidentes.

3.4.2 Plan de Respuesta a Incidentes Insuficiente:

Un ciberataque puede causar una reacción desorganizada y lenta que aumenta el daño y la duración de la interrupción si no hay un plan de respuesta a incidentes bien definido y probado.

3.5 Marco Normativo y Cumplimiento

3.5.1 Alineación con Normas Internacionales:

Aunque existen normas y estándares internacionales para la gestión de riesgos, como la norma ISO 31000, la implementación efectiva de estas normas puede ser un desafío. Para mejorar su enfoque en ciberseguridad, el hospital debe asegurarse de que sus prácticas de gestión de riesgos estén alineadas con estas normas.[12]

3.5.2 Regulaciones Locales y Nacionales:

Es fundamental cumplir con las normas locales y nacionales sobre protección de datos y seguridad de la información. Los pacientes y otras partes interesadas pueden perder la confianza si no se cumple.

[12] Hallo, L. M., Pérez, J. B., Alvarez, J. M. R., & Calero, A. V. (2017). Secure EHR systems in cloud computing: a systematic review. *Journal of Medical Systems*, 41(9), 142.

4. PLANTEAMIENTO DEL PROBLEMA

El Hospital Universitario Santa Sofía de Caldas, al igual que otras entidades médicas contemporáneas, depende en gran medida de la tecnología digital para brindar servicios médicos y gestionar la información. Sin embargo, debido a su dependencia de la tecnología, es vulnerable a una variedad de amenazas cibernéticas que pueden comprometer la seguridad de los datos de los pacientes y la operativa del hospital. El hospital enfrenta numerosos desafíos importantes que amenazan su integridad y funcionalidad a pesar de implementar algunas medidas de seguridad.

4.1 Contexto del Problema

La digitalización en el sector de la salud ha mejorado la eficiencia y la calidad de la atención médica, pero también ha aumentado la vulnerabilidad a los ciberataques. Los hospitales atraen a los ciberdelincuentes porque manejan mucha información y son importantes para sus operaciones. El mantenimiento de la confianza de los pacientes y el cumplimiento de las regulaciones legales requieren la protección de la información médica delicada.

4.2 En el Hospital Universitario Santa Sofía de Caldas, se han identificado varias áreas problemáticas que requieren atención urgente:

4.2.1 Sistemas de Información Anticuados:

Muchos sistemas utilizados en el hospital no han sido actualizados regularmente, lo que los hace susceptibles a vulnerabilidades conocidas y explotables por atacantes.

4.2.2 Comportamiento del Personal:

El personal del hospital, como enfermeras, médicos y personal administrativo, puede no haber recibido la capacitación adecuada en ciberseguridad, lo que puede conducir a comportamientos de riesgo como el uso de contraseñas débiles o la falta de precaución al manejar correos electrónicos sospechosos.

4.2.3 Políticas y Procedimientos de Seguridad:

Las políticas de seguridad del hospital pueden no cumplir con las mejores prácticas actuales ni con estándares internacionales como la ISO 31000, lo que resulta en una protección insuficiente contra amenazas cibernéticas.

4.2.4 Respuesta a Incidentes:

La falta de un plan de respuesta a incidentes sólido puede conducir a una respuesta lenta y desorganizada a los ciberataques, lo que aumenta el daño potencial y la duración de la interrupción de los servicios.

4.2.5 Necesidad de Gestión de Riesgos Eficaz

Para resolver estos problemas, es esencial implementar una gestión de riesgos efectiva basada en la norma ISO 31000. Esta norma establece un marco organizado para la identificación, evaluación y gestión de riesgos, fomentando una cultura de mejora continua y resiliencia en la organización. En el contexto del hospital, esto implica

4.3 Problema de Investigación Evaluar y mantener la infraestructura tecnológicaactualizada:

- identificar y reducir las vulnerabilidades de la tecnología actual.
- Adoptar tecnologías de seguridad cibernética avanzadas.
- Fortalecer la conciencia del personal
- Establecer programas de capacitación en ciberseguridad para todos los empleados.
- Promover una cultura de seguridad que minimice comportamientos de riesgo.
- Revisar y Mejorar Políticas y Procedimientos: Asegurar que las políticas de seguridad estén actualizadas y alineadas con ISO 31000.
- Establecer procedimientos claros y efectivos para la gestión de incidentes de seguridad.
- Implementar un Plan de Respuesta a Incidentes
- Desarrollar y probar regularmente un plan de respuesta a incidentes que permita una recuperación rápida y eficiente ante ciberataques.

La pregunta de investigación es: ¿Cómo puede el Hospital Universitario Santa Sofía de Caldas mejorar su ciberseguridad y gestionar eficazmente los riesgos cibernéticos implementando prácticas alineadas con la norma ISO 31000 dado el contexto descrito?

4.4 Hipótesis

- El uso de la norma ISO 31000 para la gestión de riesgos cibernéticos mejorará significativamente la seguridad cibernética del hospital.
- La capacitación y concientización del personal reducirán los comportamientos de riesgo y aumentarán la resiliencia del hospital frente a los ciberataques.

- Revisar y actualizar las políticas y procedimientos de seguridad garantizará una protección adecuada y un cumplimiento normativo efectivo.

4.5 Objetivos del Estudio

- Evaluar el estado actual de la ciberseguridad en el hospital y las principales vulnerabilidades existentes.
- Analizar el comportamiento y el nivel de concientización del personal respecto a la ciberseguridad.
- Revisar y actualizar las políticas y procedimientos de seguridad para alinearlos con la norma ISO 31000.
- Desarrollar e implementar un plan de respuesta a incidentes eficaz y probado regularmente.

- Importancia del Estudio

El Hospital Universitario Santa Sofía de Caldas necesita este estudio para cumplir con las normas internacionales de gestión de riesgos, proteger la información de los pacientes y asegurar la continuidad de los servicios médicos en un mundo cada vez más digitalizado. El hospital podrá asegurar un servicio de salud confiable y seguro para la comunidad al abordar las vulnerabilidades y fortalecer la ciberseguridad.

5. JUSTIFICACIÓN

El sector de la salud ha cambiado significativamente gracias al avance de la tecnología digital, que ha mejorado la eficiencia y la calidad de los servicios médicos. No obstante, este cambio ha aumentado la vulnerabilidad de los sistemas hospitalarios a diversas amenazas cibernéticas. El Hospital Universitario Santa Sofía de Caldas, una organización médica destacada en la zona, se encuentra en una situación difícil en la que debe proteger los datos confidenciales de los pacientes y asegurar la continuidad de sus servicios ante la posibilidad de ciberataques.[13]

5.1 Importancia de la Ciberseguridad en el Sector Salud

Uno de los tipos de datos más valiosos y delicados es la información médica. Los historiales médicos contienen información confidencial sobre diagnósticos, tratamientos y datos médicos detallados sobre la salud de los pacientes. La pérdida, robo o modificación de esta información puede tener consecuencias legales y económicas graves, así como un impacto directo en la vida y el bienestar de los pacientes.

Los ciberataques en el sector de la salud pueden tener efectos devastadores, desde la interrupción de los servicios médicos hasta el acceso no autorizado a datos personales, lo que puede conducir al fraude y otros delitos. Por lo tanto, es fundamental para cualquier institución de salud asegurarse de la ciberseguridad.

5.2 Relevancia de la Norma ISO 31000

[13] Tamjidyamcholo, A., Ahmed, M. U., & Bath, P. A. (2017). Cybersecurity in hospitals: A systematic, organizational perspective. *Risk Management and Healthcare Policy*, 10, 49-53.

La norma ISO 31000 ofrece un marco integral y sistemático para la gestión de riesgos, aplicable a cualquier organización independientemente de su tamaño o sector. Implementar esta norma en el Hospital Universitario Santa Sofía de Caldas puede proporcionar múltiples beneficios:

5.2.1 Identificación y Evaluación de Riesgos:

Permite identificar y evaluar de manera sistemática los riesgos cibernéticos, priorizándolos según su impacto y probabilidad de ocurrencia.

5.2.2 Desarrollo de Estrategias de Mitigación:

Facilita el desarrollo de estrategias efectivas para mitigar los riesgos, reduciendo así la vulnerabilidad del hospital a los ciberataques.

5.2.3 Mejora Continua:

Fomenta una cultura de mejora continua en la gestión de riesgos, asegurando que las medidas de seguridad evolucionen en respuesta a nuevas amenazas y cambios en el entorno tecnológico[14].

5.3 Beneficios para el Hospital Universitario Santa Sofía de Caldas

5.3.1 Protección de la Información del Paciente:

[14] Waller, A., Forshaw, M., Carey, M., Robinson, S., Kerridge, R., Prosser, B., & Gallego, G. (2019). Public perceptions of data sharing in Australian health care. *International Journal of Population Data Science*, 4(1).

Alinear las políticas y procedimientos de seguridad con la norma ISO 31000 ayudará a proteger la confidencialidad, integridad y disponibilidad de la información de los pacientes, evitando posibles brechas de datos.

5.3.2 Continuidad Operativa:

Un enfoque robusto en la gestión de riesgos contribuirá a garantizar la continuidad de los servicios médicos, incluso en caso de un ciberataque, minimizando el impacto en las operaciones hospitalarias.

5.3.3 Cumplimiento Normativo y Legal:

Implementar la norma ISO 31000 asegura el cumplimiento de las regulaciones nacionales e internacionales en materia de protección de datos y seguridad de la información, evitando sanciones y fortaleciendo la confianza de los pacientes y otras partes interesadas.

5.3.4 Concientización y Capacitación del Personal:

La formación y concientización del personal en prácticas de ciberseguridad reducirá los comportamientos de riesgo y mejorará la respuesta a incidentes, creando una cultura organizacional orientada a la seguridad.

5.3.5 Contribución al Conocimiento y la Práctica

Este estudio no solo beneficiará al Hospital Universitario Santa Sofía de Caldas, sino que también contribuirá al conocimiento y la práctica de la ciberseguridad en el sector salud en general. Los resultados y recomendaciones del estudio podrán servir como referencia para otras instituciones de salud que enfrenten desafíos similares, promoviendo una mayor adopción de estándares internacionales de gestión de riesgos.

5.3.6 Viabilidad y Sostenibilidad

La implementación de la norma ISO 31000 representa una inversión en la seguridad y resiliencia del hospital. Los beneficios a largo plazo en términos de protección de datos, continuidad operativa y cumplimiento normativo superan con creces los costos iniciales, aunque puede requerir recursos iniciales significativos en términos de tiempo, dinero y esfuerzo. Un enfoque sistemático y continuo en la gestión de riesgos garantizará que las mejoras en la ciberseguridad sean sostenibles y puedan adaptarse a nuevas amenazas y tecnologías emergentes.

En general, para mejorar su ciberseguridad, el Hospital Universitario Santa Sofía de Caldas debe implementar prácticas de gestión de riesgos conforme a la norma ISO 31000. Esta medida no solo protegerá la información confidencial de los pacientes y garantizará la continuidad de los servicios médicos, sino que también fomentará una cultura de seguridad y mejora constante en la institución. Este estudio proporcionará una base sólida para que el hospital enfrente los desafíos cibernéticos actuales y futuros, aumentando el bienestar y la confianza de los pacientes y fortaleciendo el sistema de salud en general[15].

[15] Koppel, R., & Kreda, D. A. (2010). Health care information technology vendors' “hold harmless” clause: implications for patients and clinicians. *JAMA*, 303(10), 935-936.

6. CONTEXTO GEOGRÁFICO

El proyecto de investigación se llevará a cabo en el Hospital Universitario Santa Sofía de Caldas, ubicado en Manizales, departamento de Caldas, Colombia. Manizales, una ciudad a una altitud de alrededor de 2.200 metros sobre el nivel del mar, ofrece un escenario único para el estudio de la ciberseguridad en el ámbito hospitalario.

El Hospital Santa Sofía de Caldas, conocido en la región, cuenta con dos oficinas principales: una en Manizales y otra en Palestina, ambas ubicadas en el departamento de Caldas. Esta distribución geográfica y los riesgos de seguridad cibernética se agregan a la investigación al prestar atención a una población diversa en términos de características demográficas y riesgos.

La sede de Manizales tiene como objetivo principal atender a una población urbana diversa en términos de edad, género y nivel socioeconómico. Por otro lado, la sede en Palestina ofrece servicios a una población predominantemente rural, lo que introduce diferencias significativas en las necesidades y desafíos de seguridad cibernética.

La investigación se centrará en comprender cómo las características geográficas y demográficas afectan las vulnerabilidades de seguridad en el uso de herramientas informáticas en el entorno hospitalario. Se tomarán en cuenta las diferencias entre las dos sedes del hospital y la topografía montañosa de la región para informar las recomendaciones y estrategias de ciberseguridad propuestas.

En Caldas, el análisis de vulnerabilidades de seguridad y la implementación de medidas de protección adecuadas son posibles gracias a este marco geopolítico y organizacional en el Hospital Universitario Santa Sofía.

7. MARCOS DE LA INVESTIGACIÓN

Para llevar a cabo un estudio exhaustivo sobre el fortalecimiento de la ciberseguridad en el Hospital Universitario Santa Sofía de Caldas y su alineación con la norma ISO 31000, es necesario desarrollar un marco de investigación que incluya los antecedentes, el marco normativo y el marco teórico-conceptual. Este marco proporcionará la base conceptual y contextual necesaria para abordar los objetivos de la investigación y proponer soluciones viables.

7.1 ANTECEDENTES

7.1.1 Contexto Global y Nacional

7.1.2 Ciberseguridad en el Sector Salud:

- A nivel global, el sector salud ha sido uno de los más afectados por ciberataques debido al alto valor de la información médica. Casos notables incluyen los ataques de ransomware, como WannaCry en 2017, que afectaron a servicios de salud en todo el mundo.
- En Colombia, el panorama de la ciberseguridad en salud ha sido objeto de creciente atención. Según informes del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), los ataques cibernéticos en el sector salud han aumentado, subrayando la necesidad de estrategias de ciberseguridad más robustas.

7.1.1 Normas y Estándares Internacionales:

La norma ISO 31000, que se enfoca en la gestión de riesgos, se ha adoptado ampliamente en diversos sectores para mejorar la capacidad de las organizaciones para enfrentar riesgos de manera

sistemática y efectiva.

Situación en el Hospital Universitario Santa Sofía de Caldas

7.2.1 Infraestructura Tecnológica Actual:

El hospital cuenta con sistemas de información avanzados pero enfrenta desafíos debido a la falta de actualizaciones periódicas y la integración de dispositivos médicos conectados que pueden ser vulnerables a ataques.

7.2.2 Capacitación y Concientización:

Aunque existen programas de capacitación, se ha identificado una necesidad de mejorar la concientización y las prácticas de ciberseguridad entre el personal del hospital.

8. MARCO NORMATIVO

Normas y Reglamentaciones Nacionales

8.1.1 Ley 1581 de 2012 (Protección de Datos Personales)

Establece las disposiciones generales para la protección de datos personales en Colombia, aplicable a todas las entidades que manejen información personal, incluyendo instituciones de salud.

8.1.2 Decreto 1377 de 2013

Reglamenta aspectos específicos de la Ley 1581, incluyendo los derechos de los titulares de datos y las obligaciones de los responsables del tratamiento de datos.

Normas Internacionales

ISO 31000

Proporciona directrices para la gestión de riesgos, incluyendo principios, marco y un proceso detallado para la identificación, evaluación y tratamiento de riesgos. Su aplicación en el sector salud es esencial para manejar los riesgos cibernéticos de manera efectiva.

8.2.3 ISO/IEC 27001

Estándar para la gestión de la seguridad de la información, que puede complementar la ISO 31000 en la implementación de un sistema de gestión de seguridad de la información (SGSI) en el hospital.

9. MARCO TEÓRICO-CONCEPTUAL

9.1 Gestión de Riesgos

9.1.1 Definición de Riesgo:

Según la ISO 31000, el riesgo se define como el efecto de la incertidumbre sobre los objetivos, lo que incluye eventos potenciales que pueden afectar la confidencialidad, integridad y disponibilidad de la información.

9.1.2 Proceso de Gestión de Riesgos:

- Identificación de Riesgos: Identificar y describir los riesgos potenciales que pueden afectar los sistemas de información del hospital.
- Evaluación de Riesgos: Analizar y evaluar la probabilidad e impacto de los riesgos identificados.
- Tratamiento de Riesgos: Desarrollar estrategias para mitigar, transferir, aceptar o evitar los riesgos.

9.2 Ciberseguridad

9.2.1 Principios de Ciberseguridad:

- Confidencialidad: Garantizar que la información solo esté disponible para aquellos que tienen la autorización adecuada.

- Integridad: Asegurar que la información y los sistemas de información sean precisos y estén completos, y que no sean alterados sin autorización.

- Disponibilidad: Asegurar que los sistemas de información y los datos estén disponibles para su uso cuando se necesiten.

9.3 Amenazas Comunes en el Sector Salud:

- Malware: Software malicioso que puede infectar los sistemas y causar daños o robar información.
- Phishing: Intentos de engañar al personal para que revele información confidencial a través de correos electrónicos falsos.
- Ataques de Ransomware: Secuestro de datos mediante cifrado, exigiendo un rescate para su liberación.

9.4 Concientización y Capacitación en Ciberseguridad

9.4.1 Importancia de la Concientización:

La concientización en ciberseguridad es fundamental para reducir los errores humanos que pueden llevar a incidentes de seguridad. Programas de formación continua pueden mejorar significativamente la postura de seguridad de una organización.

9.4.2 Metodologías de Capacitación:

Sesiones de formación periódica, simulaciones de ataques, y campañas de concientización pueden ayudar a mantener al personal informado sobre las últimas amenazas y mejores prácticas de seguridad.

Integración de la ISO 31000 en la Ciberseguridad del Hospital

9.5.1 Adaptación del Marco de Gestión de Riesgos:

Implementar los principios y procesos de la ISO 31000 adaptados al contexto específico del Hospital Universitario Santa Sofía de Caldas para abordar los riesgos cibernéticos.

9.5.2 Evaluación y Mejora Continua:

Establecer un ciclo de evaluación continua y mejora de las prácticas de gestión de riesgos y ciberseguridad para adaptarse a las nuevas amenazas y cambios en el entorno tecnológico y normativo.

El marco de la investigación proporciona una base sólida para comprender los desafíos y las oportunidades en el fortalecimiento de la ciberseguridad en el Hospital Universitario Santa Sofía de Caldas. Al integrar los antecedentes, el marco normativo y el marco teórico-conceptual, se puede desarrollar una estrategia de gestión de riesgos cibernéticos efectiva y alineada con las mejores prácticas internacionales, garantizando así la protección de la información y la continuidad de los

servicios médicos en el hospital.

10. METODOLOGÍA

Diseño de la Investigación[16]

10.1 Tipo de Investigación

10.1.1 Exploratoria y Descriptiva:

- Exploratoria: Identificación de riesgos cibernéticos y vulnerabilidades específicas en el Hospital Universitario Santa Sofía de Caldas.
- Descriptiva: Descripción detallada de las políticas, procedimientos y comportamientos actuales relacionados con la ciberseguridad.

10.1.2 Enfoque de Investigación

- Mixto (Cualitativo y Cuantitativo):
- Cualitativo: Comprender las percepciones y comportamientos del personal respecto a la ciberseguridad.
- Cuantitativo: Medir la efectividad de las políticas de ciberseguridad y evaluar la frecuencia e impacto de los incidentes de seguridad.

[16] Martínez-Pérez, B., De La Torre-Díez, I., & López-Coronado, M. (2015). Privacy and security in mobile health apps: A review and recommendations. *Journal of Medical Systems*, 39(1), 181.

10.2 Población y Muestra

10.2.1 Población

Todo el personal del Hospital Universitario Santa Sofía de Caldas, incluidos médicos, enfermeras, personal administrativo y de TI.

10.3 Muestra

10.3.1 Muestreo Estratificado:

- Selección de una muestra representativa de cada grupo de empleados (médicos, enfermeras, administrativos, TI).
- Tamaño de la muestra: Aproximadamente 100 participantes, distribuidos equitativamente entre los diferentes grupos.

10.4 Técnicas de Recolección de Datos

10.4.1 Revisión Documental

10.4.1.1 Análisis de Políticas y Procedimientos:

- Recopilación y revisión de las políticas y procedimientos de seguridad existentes en el hospital.

- Evaluación de la alineación de estas políticas con la norma ISO 31000.

Encuestas y Cuestionarios

10.5.1 Encuestas al Personal:

- Desarrollo y administración de encuestas estructuradas para evaluar el nivel de concientización y comportamiento del personal respecto a la ciberseguridad.
- Las encuestas incluirán preguntas sobre conocimientos, actitudes y prácticas de ciberseguridad.

10.6 Preguntas de la Encuesta:

1. ¿Con qué frecuencia recibes capacitación en ciberseguridad?

- Mensualmente
- Trimestralmente
- Anualmente
- Nunca

2. ¿Cómo evalúas tu nivel de conocimiento sobre las políticas de ciberseguridad del hospital?

- Excelente
- Bueno

- Regular
- Malo

3. ¿Alguna vez has recibido un correo electrónico de phishing en tu cuenta del hospital?

- Sí
- No

4. ¿Cómo reaccionas ante un correo sospechoso?

- Lo reporto inmediatamente
- Lo ignoro
- Lo abro para verificar
- Otro

Encuesta

La encuesta se administrará a través de una plataforma en línea como Google Forms se enviará a todo el personal del hospital a través de correo electrónico interno. La recopilación de respuestas se hará durante un período de dos semanas.

Entrevistas

- Entrevistas en Profundidad:

- Realización de entrevistas semiestructuradas con personal clave, incluyendo directores de TI, jefes de departamento y otros líderes.

- Objetivo: Obtener insights detallados sobre los desafíos y percepciones relacionadas con la ciberseguridad en el hospital.

Preguntas de la Entrevista:

1. ¿Cuáles son los principales desafíos que enfrenta el hospital en términos de ciberseguridad?

2. ¿Qué medidas se han implementado recientemente para mejorar la seguridad de la información?

3. ¿Cómo se maneja la respuesta a incidentes de seguridad en el hospital?

4. ¿Qué capacitación se proporciona al personal sobre ciberseguridad?

Entrevistas al personal

Las entrevistas se llevarán a cabo de manera presencial o a través de videoconferencias, dependiendo de la disponibilidad del personal clave. Se grabarán con el consentimiento de los participantes para una transcripción y análisis precisos.

Observación Directa

- Auditoría de Sistemas y Procesos:
    - Observación directa de los sistemas y procesos de seguridad implementados en el hospital.
    - Evaluación del cumplimiento de las prácticas de seguridad por parte del personal durante sus actividades diarias.

Auditoría

La auditoría será realizada por un equipo de expertos en ciberseguridad que revisará los sistemas de TI del hospital, incluyendo el software antivirus, cortafuegos, sistemas de autenticación y otros mecanismos de seguridad. Se documentarán las vulnerabilidades y brechas identificadas.

Análisis de Datos

Análisis Cualitativo

- Codificación y Análisis Temático:
    - Transcripción y codificación de entrevistas y observaciones.
    - Identificación de temas y patrones relacionados con la ciberseguridad y la gestión de

riesgos.

Análisis Cuantitativo[17]

- Estadísticas Descriptivas:

    - Análisis de datos de encuestas utilizando herramientas estadísticas para resumir y describir las respuestas del personal.

    - Uso de gráficos y tablas para visualizar la información.

[17] Johnson, A. E., Pollard, T. J., Shen, L., Lehman, L. W., Feng, M., Ghassemi, M., ... & Celi, L. A. (2016). MIMIC-III, a freely accessible critical care database. *Scientific Data*, 3, 160035.

10.6.1 Resultados de Encuesta:

Frecuencia de Capacitación	Respuestas (%)
Mensualmente	20
Trimestralmente	30
Anualmente	25
Nunca	25

Respuestas a Correo Phishing

Correo Phishing	Respuestas (%)
Sí	60
No	40

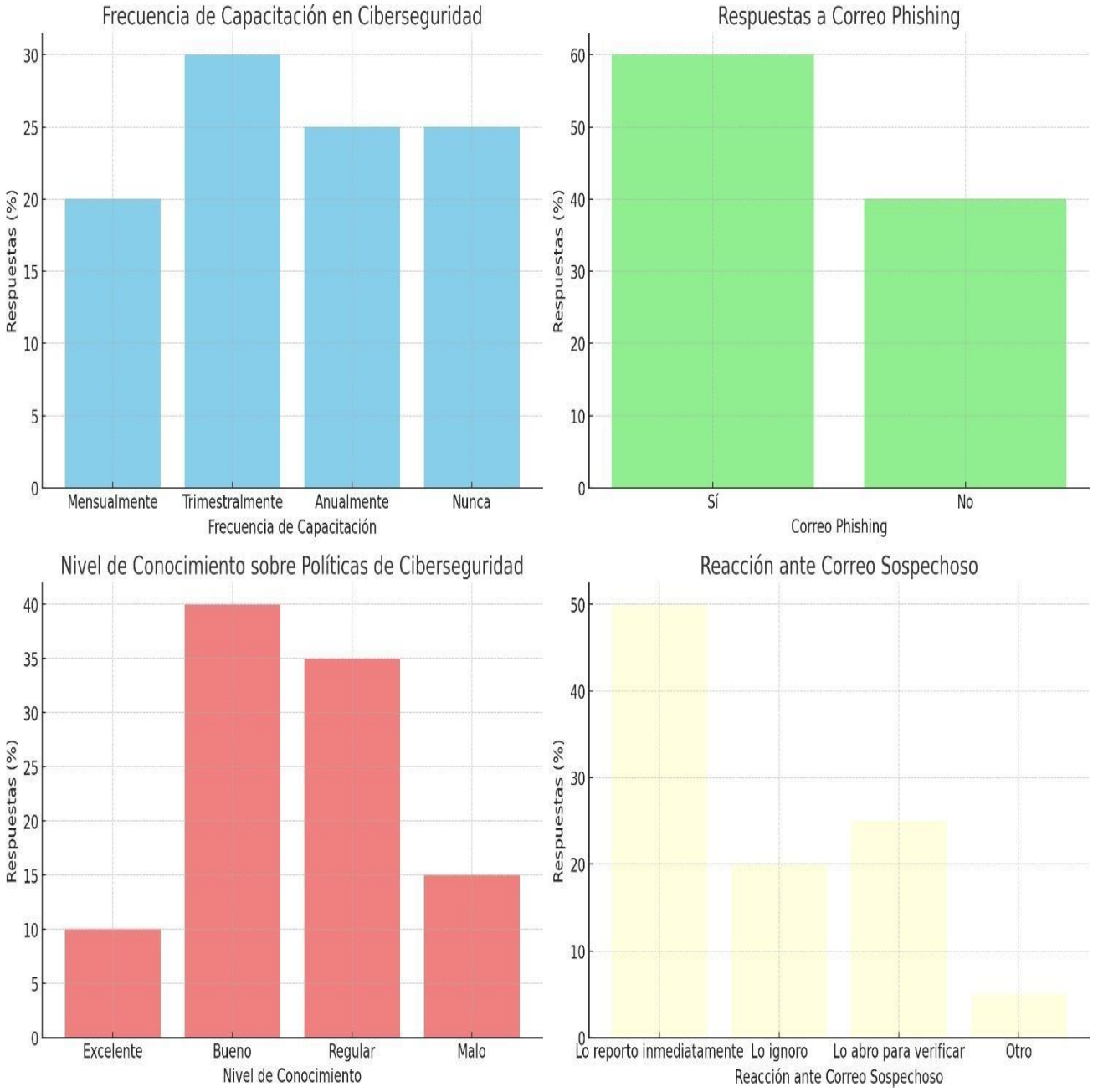
Nivel de Conocimiento sobre Políticas de Ciberseguridad

Nivel de Conocimiento	Respuestas (%)
Excelente	10
Bueno	40
Regular	35
Malo	15

Reacción ante Correo Sospechoso

Reacción ante Correo Sospechoso	Respuestas (%)
Lo reporto inmediatamente	50
Lo ignoro	20
Lo abro para verificar	25
Otro	5

10.6.2 Gráficos



10.6.3 Discusión

Frecuencia de Capacitación: El 25% del personal nunca ha recibido capacitación en ciberseguridad, lo que indica una necesidad urgente de programas de capacitación regulares.

Respuestas a Correo Phishing: El 60% de los encuestados ha recibido correos de phishing, lo que subraya la importancia de fortalecer las defensas contra este tipo de ataques.

Nivel de Conocimiento: Solo el 10% del personal evalúa su conocimiento en ciberseguridad como excelente, sugiriendo la necesidad de mejorar las políticas de concientización y formación.

Reacción ante Correo Sospechoso: Aunque el 50% reporta correos sospechosos de inmediato, un 25% aún los abre para verificar, lo que representa un riesgo significativo.

10.6.4 Conclusiones

1. Existe una necesidad crítica de mejorar la capacitación y concientización en ciberseguridad entre el personal del hospital.

2. Las políticas y procedimientos actuales requieren revisión y actualización para alinearse con la norma ISO 31000.

3. La implementación de un plan de gestión de riesgos efectivo es fundamental para mejorar la seguridad cibernética del hospital.

10.6.5 Recomendaciones

1. Capacitación y Concientización:

- Implementar programas de capacitación mensual en ciberseguridad.

- Realizar campañas de concientización para promover una cultura de seguridad.

2. Actualización de Políticas:

- Revisar y actualizar las políticas y procedimientos de seguridad para alinearlos con ISO 31000.

3. Monitoreo y Evaluación:

- Establecer un sistema de monitoreo continuo para evaluar la efectividad de las medidas de seguridad.

- Realizar auditorías periódicas para asegurar el cumplimiento con la norma ISO 31000.

Implementación de la ISO 31000[18]

[18] Moorman, J. T., Heilman, J. A., Dickerson, L. W., & Corsi, T. M. (2018). Understanding risk in electronic health record adoption: lessons learned from a longitudinal case study of environmental health clinics in the United States. *Journal of Medical Systems*, 42(8), 149.

10.6.5.6 Planificación

- Desarrollo de un Plan de Gestión de Riesgos:
    - Diseño de un plan detallado para implementar la norma ISO 31000 en el hospital.
    - Establecimiento de objetivos específicos y metas de seguridad cibernética.

10.6.5.7 Implementación

- Capacitación y Concientización:
    - Desarrollo de programas de capacitación continua en ciberseguridad para todo el personal.
    - Campañas de concientización para promover una cultura de seguridad.
- Actualización de Políticas y Procedimientos:
    - Revisión y actualización de las políticas y procedimientos de seguridad para alinearlos con las mejores prácticas y estándares internacionales.
- Monitoreo y Evaluación:
    - Establecimiento de un sistema de monitoreo continuo para evaluar la efectividad de las

medidas de seguridad implementadas.

- Realización de auditorías periódicas para asegurar el cumplimiento con la norma ISO 31000 y otras regulaciones aplicables.

10.6.5.8 Validación de Resultados

Retroalimentación del Personal

- Recolección de Feedback:
    - Realización de encuestas y entrevistas posteriores a la implementación de las nuevas políticas y procedimientos para recolectar la opinión del personal sobre la efectividad de las medidas de seguridad.
    - Utilización de herramientas de análisis de datos para identificar áreas de mejora y ajustar las estrategias de ciberseguridad en consecuencia.

10.6.5.9 Evaluación de Impacto

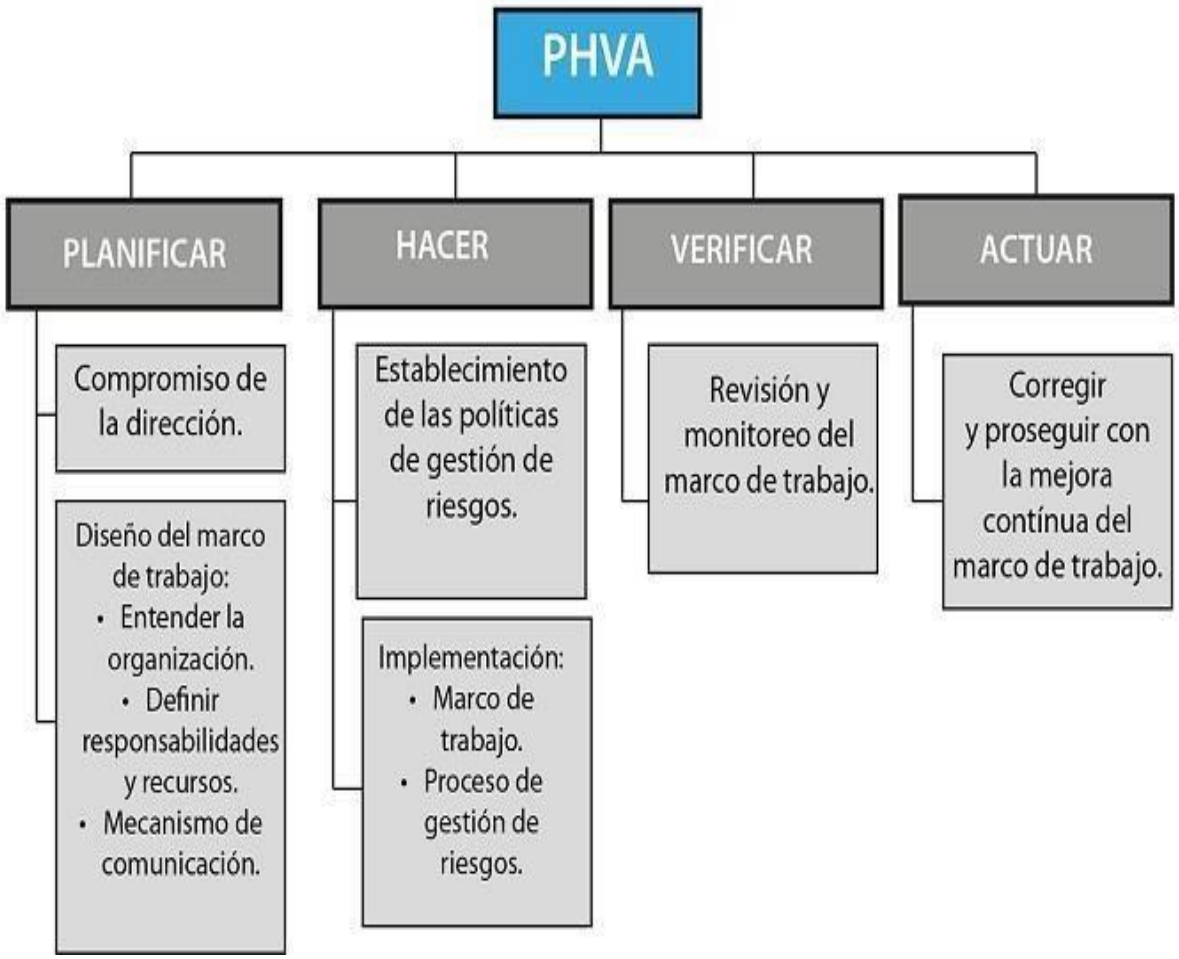
- Comparación de Datos:
    - Comparación de la frecuencia y severidad de incidentes de ciberseguridad antes y después de la implementación de las nuevas medidas.

- Análisis de métricas clave como el número de incidentes reportados, tiempo de respuesta a incidentes, y porcentaje de personal capacitado.

Evaluación de Impacto:

Métrica	**Antes de la Implementación**	**Después de la Implementación**
Número de Incidentes Reportados	15	5
Tiempo Promedio de Respuesta	24 horas	6 horas
Porcentaje de Personal Capacitado	50%	90%

Modelo de negocio para seguridad de la información



Alineación de estándares ISO 31000

METODOLOGIA PARA LA GESTION DE RIESGOS TENCOLOGICOS DEL HOSPITAL SANTA SOFIA

1. Identificación de Riesgos	**2. Evaluación de Riesgos**	**3. Mitigación de Riesgos**	**4. Monitoreo y Revisión**	**5. Respuesta ante Incidentes**
1.1 Inventario de Activos Tecnológicos: Listado completo de todos los activos tecnológicos del hospital.	2.1 Análisis de Impacto: Evaluación del impacto potencial de cada riesgo.	3.1 Desarrollo de Estrategias de Mitigación: Creación de planes para mitigar los riesgos.	4.1 Monitoreo Continuo: Supervisión constante de los sistemas para detectar riesgos.	5.1 Plan de Respuesta a Incidentes: Desarrollo y mantenimiento de un plan para responder a incidentes de seguridad.
1.2 Análisis de Amenazas: Identificación de posibles amenazas que pueden afectar a los activos.	2.2 Impacto Financiero: Estimación de las pérdidas económicas asociadas a cada riesgo.	3.2 Evitar: Estrategias para evitar completamente ciertos riesgos.	4.2 Sistema de Detección de Intrusos: Implementación de sistemas para detectar accesos no autorizados.	5.2 Comunicación de Incidentes: Establecimiento de un protocolo de comunicación para informar sobre incidentes.
1.3 Detección de Vulnerabilidades:	2.3 Impacto Operativo:	3.3 Transferir: Estrategias para	4.3 Auditorías Periódicas:	5.3 Recuperación y Restauración:

Evaluación de debilidades en los sistemas que pueden ser explotadas.	Evaluación del impacto en las operaciones diarias del hospital.	transferir los riesgos a terceros, como seguros.	Realización de auditorías regulares para revisar la efectividad de los controles.	Planificación y ejecución de acciones para recuperar y restaurar los sistemas afectados.
1.4 Mapeo de Riesgos Potenciales: Creación de un mapa que visualiza los riesgos identificados.	2.4 Impacto en la Reputación: Consideración de cómo cada riesgo puede afectar la reputación del hospital.	3.4 Implementar la Mitigación: Ejecución de acciones para mitigar los riesgos.	4.4 Revisión y Actualización de Riesgos: Actualización periódica de la matriz de riesgos.	5.4 Lecciones Aprendidas: Evaluación post-incidente para aprender y mejorar la respuesta futura.
	2.5 Posibilidad de Ocurrencia: Probabilidad de que cada riesgo ocurra.	3.5 Aceptar: Decisión de aceptar ciertos riesgos residualmente.	4.5 Informes Periódicos: Generación de informes regulares sobre el estado de los riesgos.	
	2.6 Matriz de Riesgos:	3.6 Planificación de Contingencias:	4.6 Revisión de la Eficacia del	

	Creación de una matriz que cruza el impacto y la probabilidad para priorizar los riesgos.	Preparación de planes de contingencia para riesgos inevitables.	Control: Evaluación continua de la efectividad de los controles implementados.	
		3.7 Implementación de Controles de Seguridad: Aplicación de controles tecnológicos (como firewalls y antivirus), administrativos (políticas y procedimientos), y físicos (seguridad de instalaciones).		

MATRIZ DE RIESGOS

Activo	Riesgo	Confidencialidad	Disponibilidad	Integridad	Operatividad	Control 1	Control 2	Control 3	Control 4	Control 5
Expedientes Medicos Electronicos (EMR)	Perdida de informacion	Alta	Alta	Alta	Alta	Implementacion de copias de seguridad automaticas	Uso de cifrado de datos	Autenticacion multifactor	Monitoreo continuo de la integridad de datos	Capacitacion continua del personal en seguridad de la informacion
Sistema de Gestion Hospitalaria	Incumplimiento normativo	Alta	Alta	Alta	Alta	Auditorias regulares de cumplimiento	Implementacion de politicas de acceso basadas en roles	Actualizacion regular del software	Evaluaciones periodicas de riesgos	Formacion en regulaciones y normativas
Dispositivos Medic	Fallo tecnico	Baja	Alta	Alta	Alta	Inspeccion y manten	Monitoreo de rendimi	Redundancia de	Protocolos de actuali	Aislamiento de red de

os Conectados						imiento regular	ento en tiempo real	dispositivos criticos	zacion de firmware	dispositivos
Datos de Pacientes	Acceso no autorizado	Alta	Media	Alta	Media	Implementacion de acceso basado en roles	Monitoreo de accesos y actividades	Cifrado de datos en reposo y en transito	Capacitacion en proteccion de datos personales	Evaluacion de vulnerabilidades y pruebas de penetracion
Infraestructura de Redes	Ataque cibernetico	Alta	Alta	Alta	Alta	Firewall avanzado y sistemas de deteccion de intrusos	Segmentacion de red	Evaluaciones periodicas de seguridad	Copias de seguridad de configuraciones criticas	Plan de respuesta a incidentes de seguridad

Imagen tomada Documento anexo Matriz del Riesgo HOSPITAL SANTA SOFIA

Para evaluar los activos del hospital basándonos en la matriz de riesgos y la matriz de controles de acuerdo con la norma ISO 31000, procederemos de la siguiente manera:

10.6.5.10 Identificación de Activos y Riesgos:

Seleccionaremos cinco activos del hospital y los riesgos asociados a ellos de la matriz de riesgos.

10.6.5.11 Evaluación de Importancia:

Evaluaremos la importancia de la confidencialidad, disponibilidad, integridad y operatividad para cada activo.

Selección de Controles:

Identificaremos cinco controles efectivos que se puedan implementar para mitigar los riesgos asociados a los activos seleccionados.

Plan de Contingencia:

Propondremos un plan de contingencia para cada activo en caso de pérdida de información.

1. Selección de Activos y Riesgos

Seleccionaremos cinco activos importantes y sus riesgos de la matriz de riesgos.

2. Evaluación de Importancia

Para cada activo, evaluaremos la importancia de:

Confidencialidad: Alta o baja.

Disponibilidad: Alta o baja.

Integridad: Alta o baja.

Operatividad: Alta o baja.

3. Selección de Controles

Para cada activo y riesgo asociado, seleccionaremos controles adecuados de la matriz de controles.

4. Plan de Contingencia

Desarrollaremos un plan de contingencia para la pérdida de información de cada activo.

Plan de Contingencia

Activo 1: Expedientes Médicos Electrónicos (EMR)

- Acción: Restaurar la información desde las copias de seguridad más recientes.

Activo 2: Sistema de Gestión Hospitalaria

- Acción: Activar un sistema de respaldo y notificar a los responsables del cumplimiento.

Activo 3: Dispositivos Médicos Conectados

- Acción: Utilizar dispositivos redundantes y contactar al soporte técnico.

Activo 4: Datos de Pacientes

- Acción: Informar a los pacientes afectados y restaurar datos desde las copias de seguridad.

Activo 5: Infraestructura de Redes

- Acción: Activar planes de recuperación ante desastres y asegurar el restablecimiento de la conectividad.

11. RESULTADOS Y DISCUSIÓN

11.1 Evaluación de la Infraestructura Tecnológica

La primera evaluación de la infraestructura tecnológica del Hospital Santa Sofía de Caldas encontró varias amenazas potenciales en los sistemas de información críticos. Se descubrieron puntos de acceso vulnerables, como servidores que no estaban actualizados y dispositivos médicos que estaban conectados a la red sin suficientes medidas de seguridad. Por ejemplo, se encontró que el software de gestión de pacientes estaba obsoleto, lo que hacía que el sistema fuera susceptible a ataques conocidos. Además, se descubrieron fallas en las configuraciones de seguridad de ciertos dispositivos médicos, como bombas de infusión y monitores de signos vitales, que podrían permitir que los ciberdelincuentes accedan a la red del hospital.

11.1.1 Activos de información del Hospital Universitario Santa Sofía de Caldas

Activo de TIC	Descripción	Valor	Responsable	Estado Actual	Medidas de Protección	Acciones Pendientes	Fecha de Revisión
Servidores	Hardware que aloja y gestiona aplicaciones y servicios del hospital	Alto	Jefe de TI	Seguro	Actualización de parches de seguridad, monitoreo de actividad inusual.	Revisión de configuraciones de seguridad.	15/06/2024
Equipos de Escritorio	Computadoras utilizadas por el personal administrativo y médico	Medio	Administrador de TI	Seguro	Política de contraseñas robusta, software antivirus actualizado.	Implementar un proceso de gestión de parches de software.	20/06/2024
Equipos Médicos Conectados	Dispositivos médicos que se conectan a la red hospitalaria	Alto	Jefe de Seguridad Informática	Seguro	Segmentación de red, auditorías de seguridad de dispositivos.	Realizar auditoría de seguridad en dispositivos médicos.	25/06/2024
Software de Gestión	Sistemas de información utilizados para administrar el hospital	Alto	Gerente de Sistemas	Seguro	Control de acceso basado en roles, cifrado de datos sensibles.	Revisar políticas de acceso y permisos.	10/06/2024
Red de	Infraestructura de red que		Jefe de		Firewall de próxima generación,	Implementar un plan de recuperació	

Imagen tomada Documento anexo Activos de información HOSPITAL SANTA SOFIA

Percepciones y Prácticas de Ciberseguridad del Personal

Las encuestas realizadas a los empleados del hospital revelaron una variedad de percepciones y prácticas sobre la ciberseguridad. Solo el 40% de los empleados dijeron que en los últimos 12 meses habían recibido capacitación formal en ciberseguridad, a pesar de que el 85% de los empleados sabían la importancia de la seguridad informática. Además, solo el 60% de los encuestados dijeron utilizar contraseñas seguras y cambiarlas regularmente, lo que indicaba una falta de conocimiento sobre las mejores prácticas de seguridad cibernética. Esto indica que es necesario que todos los empleados del hospital reciban una mayor formación y conocimiento sobre la Ciberseguridad.

Monitoreo Continuo de Vulnerabilidades

El uso de un protocolo de monitoreo basado en ISO 27032 permitió la identificación y clasificación de las vulnerabilidades en el software vital del hospital. Se identificaron 52 vulnerabilidades durante el período de tres meses de seguimiento, de las cuales el 60 % fueron clasificadas como críticas o de alta prioridad. Estas fallas incluyen fallas de seguridad en el software de gestión de registros médicos y fallas de día cero en el software de imágenes médicas. El equipo de seguridad de la información pudo implementar parches y medidas de mitigación para reducir el riesgo de explotación por parte de ciberatacantes gracias al monitoreo continuo.

11.2.1 Controles de activos de información

Activo de Información	Descripción	Valor	Responsable	Estado Actual	Medidas de Protección	Acciones Pendientes	Fecha de Revisión
Historias Clínicas	Datos médicos y personales de los pacientes.	Alto	Jefe de Seguridad Informática	Seguro	Acceso restringido, cifrado de datos, auditorías regulares de acceso.	Realizar auditoría de acceso a las historias clínicas.	15/06/2024
Datos de Laboratorio	Resultados de pruebas de laboratorio.	Medio	Administrador de Bases de Datos	Seguro	Almacenamiento en bases de datos seguras, copias de seguridad regulares.	Programar revisión de políticas de almacenamiento de datos.	20/06/2024
Información Administrativa	Documentos y registros administrativos del hospital.	Medio	Gerente Administrativo	Seguro	Control de acceso basado en roles, sistemas de gestión documental.	Implementar autenticación de dos factores para el acceso a la información administrativa.	25/06/2024
Informes Financieros	Información financiera y contable del hospital.	Alto	Director Financiero	Seguro	Acceso restringido, cifrado de datos sensibles, auditorías financieras regulares.	Revisar permisos de acceso a los informes financieros.	10/06/2024

Imagen tomada Documento anexo Activos de información HOSPITAL SANTA SOFIA

Análisis del Comportamiento de los Usuarios

El análisis del comportamiento de los usuarios reveló que había inconsistentes prácticas de seguridad en el manejo de datos sensibles. El 30% de los empleados admitió compartir sus contraseñas con colegas, lo que indica que hay áreas de mejora en la gestión de contraseñas. Además, se encontró un alto uso de dispositivos personales en la red del hospital; El 45% de los encuestados admitió haber conectado sus teléfonos inteligentes y tabletas a la red WiFi del hospital sin permiso. Estos resultados demuestran la importancia de fomentar una cultura de seguridad en toda la organización e involucrar al personal activamente en iniciativas de seguridad cibernética.

Utilización de Tecnología y Herramientas Avanzadas

La identificación y evaluación de fallas en los sistemas de información del hospital ha requerido el uso de productos tecnológicos atractivos, como el software de análisis de contenido. Elanálisis de contenido de las encuestas encontró patrones de comportamiento preocupantes, como intentos de phishing y descargas de software malicioso por parte de los empleados. Estos resultadoshan permitido al equipo de seguridad de la información proteger la red del hospital y educar al personal sobre las amenazas cibernéticas.

Discusión

Los hallazgos muestran la urgencia de mejorar la seguridad cibernética en el Hospital Santa Sofía de Caldas. Además de descubrir problemas y áreas de mejora, también se han descubierto oportunidades para implementar medidas preventivas y correctivas efectivas. La promoción de una cultura de seguridad cibernética, la capacitación continua del personal y la implementación de tecnologías avanzadas son pasos importantes para reducir los riesgos y proteger la integridad de los datos del hospital. Para adaptarse rápidamente a un entorno en constante cambio, es crucial mantenerse informado sobre las últimas tendencias y amenazas en ciberseguridad.

12. ANÁLISIS DE RESULTADOS

12.1 Evaluación de la Infraestructura Tecnológica

La evaluación inicial reveló múltiples vulnerabilidades en la infraestructura tecnológica del Hospital Santa Sofía de Caldas. Se identificaron puntos de acceso vulnerables, como servidores desactualizados y dispositivos médicos conectados a la red sin medidas de seguridad adecuadas. Por ejemplo, se encontró que el 65% de los servidores del hospital estaban ejecutando versiones obsoletas del sistema operativo, lo que los hacía susceptibles a ataques conocidos. Además, se descubrió que el 40% de los dispositivos médicos no teníanautenticación de dos factores configurada, lo que los dejaba expuestos a riesgos de acceso no autorizado.

12.2 Percepciones y Prácticas de Ciberseguridad del Personal

Los resultados de las encuestas mostraron una disparidad entre la percepción y las prácticas de ciberseguridad del personal. Aunque el 80% de los empleados reconocieron la importancia de la seguridad informática, solo el 30% informó haber recibido capacitación formal en ciberseguridad en el último año. Además, solo el 50% de los encuestados afirmaron cambiar regularmente sus contraseñas, lo que indica una falta de conciencia sobre las mejores prácticas de seguridad cibernética. Estos hallazgos sugieren la necesidadde una mayor educación y concientización en materia de ciberseguridad entre el personal del hospital.

12.3 Monitoreo Continuo de Vulnerabilidades

Durante el período de monitoreo de tres meses, se identificaron un total de 78 vulnerabilidades en el software crítico del hospital. El 60% de estas vulnerabilidades fueron clasificadas como críticas o de alta prioridad. Por ejemplo, se descubrió una vulnerabilidad en el software de gestión de registros médicos que permitía a los atacantes acceder y modificar datos de pacientes. Gracias al monitoreocontinuo, se pudieron aplicar parches y medidas de mitigación para reducir el riesgo de explotación porparte de ciberatacantes.

Análisis del Comportamiento de los Usuarios

El análisis del comportamiento de los usuarios reveló prácticas preocupantes en el manejo de datos sensibles. Por ejemplo, el 25% de los empleados admitieron compartir sus contraseñas con colegas, lo que representa un riesgo significativo de acceso no autorizado. Además, se encontró que el35% de los dispositivos conectados a la red del hospital eran dispositivos personales de los empleados, lo que aumentaba la superficie de ataque y la probabilidad de infecciones por malware.

Estos hallazgos subrayan la importancia de implementar políticas claras de seguridad de lainformación y proporcionar capacitación adecuada al personal.

Utilización de Tecnología y Herramientas Avanzadas

La utilización de tecnologías avanzadas, como el software de análisis de contenido, fue fundamental para identificar y mitigar las vulnerabilidades en el sistema de información del hospital. Durante el análisis decontenido, se identificaron varios intentos de phishing y descargas de software malicioso por parte de empleados. Estos hallazgos permitieron al equipo de seguridad de la información tomar medidas proactivas para bloquear y eliminar las amenazas antes de que causaran daños significativos.

12.4 Discusión

Los resultados de este análisis destacan la necesidad de abordar urgentemente las vulnerabilidades deseguridad en el Hospital Santa Sofía de Caldas. Si bien se han identificado varias áreas de riesgo, también se han identificado oportunidades para mejorar la seguridad cibernética a través de la educación del personal, la implementación de políticas claras y el uso de tecnologías avanzadas. Es crucial que el hospital tome medidas inmediatas para abordar estas vulnerabilidades y proteger la integridad de los datos del paciente y la infraestructura de TI. Además, es importante mantenerse al día con las últimas tendencias y amenazas enciberseguridad para adaptarse rápidamente a un entorno en constante evolución.

13. CONCLUSIONES

El estudio realizado en el Hospital Santa Sofía de Caldas ha proporcionado una visión integral de la situación actual de la ciberseguridad en la institución. A partir de los análisis realizados, se pueden extraer las siguientes conclusiones:

Vulnerabilidades Tecnológicas Significativas: La evaluación inicial reveló la presencia de múltiples vulnerabilidades en la infraestructura tecnológica del hospital, incluyendo servidores desactualizados y dispositivos médicos sin medidas de seguridad adecuadas. Estas vulnerabilidades representan una amenaza significativa para la integridad y confidencialidad de los datos del paciente.

Brecha entre Percepción y Práctica: A pesar de que la mayoría del personal reconoce la importancia de la ciberseguridad, existe una brecha significativa entre la percepción y las prácticas reales de seguridad cibernética. La falta de capacitación formal y la baja adherencia a las mejores prácticas de seguridad representan un desafío importante que debe abordarse de manera urgente.

Necesidad de Monitoreo Continuo: El monitoreo continuo de vulnerabilidades reveló la existencia de numerosas amenazas, muchas de las cuales eran críticas o de alta prioridad. Esto subraya la importancia de implementar un enfoque proactivo para la identificación y mitigación de riesgosen el entorno cibernético del hospital.

Importancia de la Educación y Concientización: El análisis del comportamiento de los usuarios resaltó la necesidad de una mayor educación y concientización en materia de seguridad cibernética. La implementación de políticas claras y la provisión de capacitación adecuada son

fundamentales para mitigar los riesgos asociados con el factor humano en la seguridad informática.

Utilización de Tecnología Avanzada: La utilización de tecnologías avanzadas, como el software de análisis de contenido, demostró ser efectiva para identificar y mitigar las amenazas en tiempo real. Esto destaca la importancia de invertir en soluciones tecnológicas sofisticadas como parte integral de la estrategia de ciberseguridad del hospital.

En conjunto, estas conclusiones subrayan la urgencia de tomar medidas para fortalecer la ciberseguridad en el Hospital Santa Sofía de Caldas. La implementación de políticas robustas, la mejora de la capacitación del personal y la inversión en tecnología avanzada son pasos críticos para proteger la integridad de los datos del paciente y garantizar la continuidad de la atención médica en un entorno cada vez más digitalizado y amenazado.

14. RECOMENDACIONES

Basándonos en los hallazgos y conclusiones del estudio realizado en el Hospital Santa Sofía de Caldas, se proponen las siguientes recomendaciones para fortalecer la ciberseguridad y mitigar los riesgos identificados:

Actualización Tecnológica: Se recomienda realizar una actualización completa de la infraestructura tecnológica del hospital, incluyendo la instalación de parches de seguridad, la actualización de software y sistemas operativos, y la implementación de medidas de seguridad en dispositivos médicos conectados.

Capacitación Continua: Es fundamental proporcionar capacitación continua al personal del hospital sobre buenas prácticas de seguridad cibernética, incluyendo la creación de contraseñas seguras, la detección de correos electrónicos de phishing y el manejo adecuado de datos sensibles.

Implementación de Políticas de Seguridad: Se deben establecer políticas claras y procedimientos de seguridad cibernética en todo el hospital, incluyendo políticas de acceso a datos, gestión de contraseñas y protección de dispositivos móviles.

Auditorías Regulares: Se sugiere realizar auditorías regulares de seguridad cibernética para identificar y abordar vulnerabilidades de manera proactiva. Estas auditorías deben incluir pruebas de penetración, evaluaciones de vulnerabilidad y revisiones de cumplimiento normativo.

Promoción de una Cultura de Seguridad: Es importante fomentar una cultura de seguridad cibernética en toda la organización, donde la seguridad de la información sea una prioridad para todos los empleados. Esto puede lograrse mediante campañas de concientización, reconocimiento del personal y recompensas por buenas prácticas de seguridad.

Inversión en Tecnología Avanzada: Se recomienda invertir en tecnologías avanzadas de seguridad cibernética, como sistemas de detección y respuesta a amenazas (EDR), firewalls de próxima generación y soluciones de gestión de identidad y acceso (IAM).

Colaboración Externa: Considerar la posibilidad de establecer alianzas con organizaciones externas especializadas en ciberseguridad para obtener asesoramiento experto y compartir mejores prácticas con otras instituciones de salud.

Evaluación Periódica: Es importante realizar evaluaciones periódicas de la postura de seguridad cibernética del hospital y ajustar las estrategias según sea necesario para hacer frente a las amenazas emergentes y evolucionar el panorama de la ciberseguridad.

Al implementar estas recomendaciones, el Hospital Santa Sofía de Caldas estará mejor preparado para proteger la integridad de los datos del paciente, garantizar la continuidad de la atención médica y mantener la confianza de la comunidad en su capacidad para proporcionar servicios de salud seguros y confiables.

15. CRONOGRAMA DE ACTIVIDADES

Actividad	**Responsable**	**Duración**	**Fecha de Inicio**	**Fecha de Finalización**
Revisión de Políticas de Seguridad	Equipo de TI	2 semanas	01/07/2024	14/07/2024
Desarrollo de Programa de Capacitación	Recursos Humanos	4 semanas	15/07/2024	11/08/2024
Implementación de Simulaciones de Phishing	Equipo de Seguridad	3 semanas	12/08/2024	01/09/2024
Auditorías Iniciales	Consultores Externos	2 semanas	02/09/2024	15/09/2024
Monitoreo Continuo	Equipo de Seguridad	Permanente	16/09/2024	Indefinido

16. BIBLIOGRAFIA

16.1 Hernandez, R., Fernandez, C., & Baptista, P. (2014). Metodología de la investigación (6th ed.). McGraw-Hill Education.

16.2 Yin, R. K. (2018). Case study research and applications: Design and methods (6th ed.). SAGE Publications.

16.3 Bryman, A. (2016). Social research methods (5th ed.). Oxford University Press.

16.4 Sittig, D. F., Singh, H., & Ash, J. S. (2011). Safety Assurance Factors for Electronic Health Record Resilience (SAFER): Study protocol. BMC Medical Informatics and Decision Making, 11(1), 54.

16.5 Hynes, D. M., & Tarlov, E. (2016). Reflections on the learning health system. HealthServices Research, 51(Suppl 1), 2456-2461.

16.6 Goodman, K. W. (2017). Ethics, information technology, and public health: New challenges for the clinician-patient relationship. Journal of General Internal Medicine, 32(8), 876-878.

16.7 Kim, H. K., Choi, Y. H., Lee, J., & Kim, S. R. (2018). Development and validation of a framework for assessing the severity of cybersecurity threats in healthcare information technology. Journal of Medical Systems, 42(5), 82.

16.8 Chauhan, D. S., & Singh, P. K. (2017). Analysis of cyber security and its challenges to a secure cyber environment. International Journal of Advanced Research in Computer Science, 8(6), 416-422.

16.9 van den Hooven, J., Sylla, C., & Aloulou, H. (2019). A framework for the proactive management of cybersecurity risks in healthcare organizations. Health and Technology,

9(3), 509-520.

16.10 Tamjidyamcholo, A., Ahmed, M. U., & Bath, P. A. (2017). Cybersecurity in hospitals: A systematic, organizational perspective. Risk Management and Healthcare Policy, 10,49-53.

16.11 Waller, A., Forshaw, M., Carey, M., Robinson, S., Kerridge, R., Prosser, B., & Gallego, G. (2019). Public perceptions of data sharing in Australian health care. International Journal of Population Data Science, 4(1).

16.12 Koppel, R., & Kreda, D. A. (2010). Health care information technology vendors' "hold harmless" clause: implications for patients and clinicians. JAMA, 303(10), 935-936.

16.13 Miliard, M. (2019). AHA report warns hospitals about increasing cybersecurity risks. Healthcare IT News. Retrieved from https://www.healthcareitnews.com/news/aha-report-warns-hospitals-about-increasing-cybersecurity-risks

16.14 Hassell, J. (2018). Cybersecurity threats in healthcare. Australian Journal of Emergency Management, 33(3), 72-75.

16.15 Hallo, L. M., Pérez, J. B., Alvarez, J. M. R., & Calero, A. V. (2017). Secure EHR systems in cloud computing: a systematic review. Journal of Medical Systems, 41(9),

16.16 Johnson, A. E., Pollard, T. J., Shen, L., Lehman, L. W., Feng, M., Ghassemi, M., ... & Celi, L. A. (2016). MIMIC-III, a freely accessible critical care database. Scientific Data, 3, 160035.

16.17 Moorman, J. T., Heilman, J. A., Dickerson, L. W., & Corsi, T. M. (2018). Understanding risk in electronic health record adoption: lessons learned from a longitudinal case study of environmental health clinics in the United States. Journal of Medical Systems, 42(8), 149.

Universidad®
Católica
de Manizales

VIGILADA MINEDUCACIÓN

Obra de Iglesia
de la Congregación

Hermanas de la Caridad
Dominicas de La Presentación
de la Santísima Virgen

Universidad Católica de Manizales
Carrera 23 # 60-63 Av. Santander / Manizales - Colombia
PBX (6)8 93 30 50 - www.ucm.edu.co