PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

CARRERA DE INGENIERÍA EN SISTEMAS DE LA INFORMACIÓN

TEMA:

Análisis de riesgo en la seguridad de los datos médicos mediante la utilización de la norma ISO/IEC 27110:2021.

AUTOR:

Sharina Martina Bastidas Pérez

TRABAJO PREVIA A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS DE INFORMACIÓN

QUITO DM, JUNIO DE 2023

DEDICATORIA

Queridos papá y mamá:

Hoy quiero dedicarles a ustedes dos, quienes han sido mi mayor apoyo y fuente de inspiración en este largo y desafiante viaje académico, desde el colegio hasta la universidad. Su presencia constante y su amor incondicional me han dado la fuerza y la determinación necesarias para alcanzar este logro.

Mamá y Papá, quiero agradecerles por estar a mi lado en cada paso del camino. Siempre me impulsaron a seguir adelante cuando las dudas y los obstáculos amenazaban con desanimarme. Siempre creyeron en mí incluso cuando yo misma dudaba de mis propias habilidades. Gracias por siempre darme esa confianza que fue el motor que me mantuvo firme para completar este trabajo de titulación. Sin su guía y apoyo incondicional, no estaría aquí celebrando este logro.

Quiero agradecerles por brindarme momentos de alivio y felicidad en medio del estrés y la presión de este proyecto.

Y finalmente, a mí misma, quiero dedicarme este logro. Agradezco mi perseverancia y mi determinación para no rendirme cuando los obstáculos parecían insuperables. Me enorgullezco de haberme mantenido firme en mi propósito y de haber trabajado arduamente para alcanzar este hito. Este logro es un testimonio de mi capacidad y de mi dedicación, y me comprometo a seguir creciendo y alcanzando metas aún más grandes en el futuro.

A todos ustedes, mi familia amada, les dedico este logro. Su presencia y apoyo han sido el motor detrás de mi éxito. Gracias por creer en mí, por alentarme y por brindarme amor y felicidad en cada paso del camino.

AGRADECIMIENTO

Papito y mamita, su constante dedicación y amor han sido mi roca en los momentos más desafiantes. Siempre estuvieron ahí, brindándome orientación, aliento y el empuje necesario para perseguir mis sueños. Su confianza en mí me ha dado la fortaleza para superar cualquier obstáculo y me ha inspirado a ser la mejor versión de mí misma.

Natita, tu apoyo fue muy importante. Tú has estado a mi lado en cada paso, escuchándome, animándome y brindándome palabras de aliento cuando más las necesitaba. Gracias por ser ese apoyo constante y creer en mí.

Abuelita Marita y Abuelito Angelito, con cada risa y cada momento compartido, han traído luz y calma a mi vida. Su alegría inquebrantable y amor incondicional han sido un bálsamo para mi corazón en los momentos más difíciles. Agradezco profundamente el consuelo y la felicidad que siempre me han brindado.

Abuelita Anita y Pajarito, su presencia sabia y amorosa ha sido un faro en mi vida. Siempre han estado atentos a mi progreso, brindándome su apoyo y consejos valiosos. Aprecio enormemente el tiempo que han dedicado a guiarme y compartir su sabiduría conmigo.

Los amo.

RESUMEN

El objetivo de leyes y normas es proporcionar el conocimiento técnico y aumentar la comprensión de la seguridad de la información de los datos médicos.

La seguridad de los datos médicos es un riesgo compartido de todos los colaboradores de una organización del sector de la salud y de los organismos de control del estado, estos datos están expuestos a amenazas y son vulnerables debido a que pueden venderse a un muy buen precio, desde luego, es un mercado mucho más especializado que el mercado de los datos personales.

Para mitigar el riesgo y el impacto en la seguridad de los datos médicos existen leyes y normas para proteger la información, que tienen lineamientos de cumplimiento. La LOPDP – LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES para el Ecuador establece todo el criterio de cumplimiento que deben tener las organizaciones públicas y privadas y la NORMA ISO/IEC 27110:2021 que tiene la directriz para identificar, establecer controles, salvaguardas, gestionar y mitigar los riesgos asociados con la seguridad médica.

La falta de conciencia, comités de seguridad de la información, recursos financieros, capacitación, certificaciones y la brecha en la implementación son desafíos que deben abordar las organizaciones de la salud pública y privada. Se requiere actuar de forma prolija, incluir un plan integral, realizar auditorías regulares y tener el compromiso de todos para garantizar la seguridad de los datos médicos.

Las organizaciones de la salud deben promover conciencia en sus colaboradores para poder implementar protocolos de seguridad basados en la ley y en la norma, es vital realizar el proceso

interno que defina el/los protocolos de seguridad de la información de las organizaciones para evitar un expuesto legal.

Palabras Clave: Análisis de riesgo, Seguridad de datos médicos, Norma ISO/IEC 27110:2021, Ciberamenazas, Protección de información, Ciberseguridad en el sector salud, Control de riesgos

ÍNDICE

INDICE DE FIGURAS, GRÁFICOS Y TABLAS

ÍNDICE DE TABLAS

INDICE DE FIGURAS

CAPÍTULO I: INTRODUCCIÓN

1.1. Justificación

Los expertos reconocen el aumento de casos con ciber amenazas y se ha reconocido la importancia de proteger y preservar los datos médicos. Los avances tecnológicos permiten eficiencia y mejor comunicación en este campo, sin embargo, existen nuevos desafíos que ponen en riesgo la seguridad de la información de datos médicos. Este trabajo tiene como objetivo identificar los problemas relacionados con la seguridad de la información, centrándose en la especificación técnica ISO/IEC 27110:2021. Al seguir las directrices de esta norma, se busca implementar un enfoque sistemático y estructurado para gestionar y mitigar los riesgos asociados con la seguridad médica.

Usando este estándar, las organizaciones de salud podrán identificar y evaluar peligros potenciales y establecer controles y salvaguardas de seguridad apropiados. El sector de la salud fue uno de los más atacados por los piratas informáticos en 2019 (Luis Tejerina, 2021). Esta situación se debe al avance de las TIC, también aumentan las amenazas dirigidas al sector salud. Dado que este sector está estrechamente vinculado con los avances tecnológicos, los ataques de ciberseguridad representan un riesgo significativo. Muchos activos dentro del campo de la salud están conectados a través de internet o se integran con sistemas internos como los ERP (Enterprise Resource Planning), lo cual los expone a vulnerabilidades y potenciales afectaciones perjudiciales. Además, los datos que se manejan en este campo son extremadamente sensibles.

Los ciberdelincuentes buscan activamente datos personales confidenciales debido a su alto valor en el mercado negro. Además, resulta relevante destacar que el 80% de los datos afectados en estos ataques cibernéticos corresponden a información de carácter personal (Luis

Tejerina, 2021). Para el sector de la salud, el tiempo desde el momento en que se descubre un ataque exitoso hasta el momento en que una organización se da cuenta de que sus datos se han visto comprometidos es de 329 días en promedio por posible filtración de información (IBM, 2021), y cabe mencionar que la región latinoamericana tiene uno de los tiempos de detección de ataques más altos del mundo. Por consiguiente, la seguridad cibernética constituye un asunto de relevancia para toda la entidad.

La norma ISO 27110 establece cinco conceptos básicos que abordan los impactos mencionados anteriormente y a través de sus revisiones pretende llevar las medidas de protección necesarias a todas las organizaciones, especialmente al sector salud. Según la visión del "Banco Interamericano de Desarrollo (BID)", para 2025 se espera que las organizaciones, independientemente de su tamaño, consideren importante tomar correcciones para proteger la información y la hagan parte de su estrategia, ya que esto va a permitir la recuperación económica sólida y sostenible.

El estudio destaca la importancia del papel de la ciberseguridad en las transformaciones digitales y enfatiza la necesidad de dilucidar el tema de la ciberseguridad para que no sea visto como un tema exclusivo del sector TI. Las organizaciones a menudo invierten en diversas tecnologías de seguridad, como software antivirus, dispositivos de protección perimetral y más. Si bien estas tecnologías mejoran la seguridad, por sí solas no logran el objetivo deseado.

En el sector de la salud, la ciberseguridad es un tema de suma importancia que incluye proteger los datos médicos e implementar medidas de seguridad para mitigar los riesgos asociados a los ciberataques. Sin embargo, está claro que actualmente falta información detallada sobre la implementación específica de ISO/IEC 27110.

El objetivo personal de este trabajo es proporcionar una contribución y apoyo al conocimiento técnico específico que ofrece la norma ISO/IEC 27110. Mediante esta investigación, se busca aumentar la comprensión del tema y, considerando la seriedad y sensibilidad del ámbito de la salud.

1.2. Planteamiento del problema

La seguridad de los datos médicos enfrenta un desafío significativo debido a la insuficiente salvaguardia frente a las amenazas tanto internas como externas. Esta situación puede conducir a una violación de la privacidad y confidencialidad del paciente, lo que lleva al extravío y divulgación de información sensible. Asimismo, el incumplimiento de regulaciones y políticas puede tener graves repercusiones legales y financieras para las organizaciones del ámbito médico. Por lo tanto, es necesario abordar este problema tomando medidas de protección efectivas.

1.3. Objetivo General

Realizar el análisis de riesgo en la seguridad de los datos médicos mediante la utilización de la norma ISO 27110.

1.4. Objetivos Específicos

- Analizar la norma ISO 27110 y sus implicaciones en ciberseguridad de la información.
- Identificar cinco riesgos externos en la seguridad de los datos médicos mediante la aplicación del análisis de riesgo basado en la norma ISO 27110.
- Proponer parámetros de ciberseguridad para datos médicos que incluya medidas de protección y controles de seguridad adecuados para minimizar el riesgo identificado en el análisis de riesgo basado en la norma ISO 27110, en el área de salud.

1.5. Antecedentes

Debido a la creciente digitalización y los avances en las nuevas tecnologías, el sector de la salud ha experimentado una transformación significativa en la organización y almacenamiento de datos. La incorporación de la nube, procesamiento de datos masivos y la interconexión de dispositivos han producido modificaciones significativas en la manera en que se gestionan y almacenan los registros médicos. Aunque estos avances mejoran la eficiencia y la participación en el sector de la salud, también incrementan la vulnerabilidad en términos de datos y privacidad.

La incidencia de ataques cibernéticos y violaciones de seguridad de datos en el ámbito de la salud ha experimentado un notable aumento en los últimos años.(Red Seguridad, 2023). Estas amenazas pueden provenir tanto de actores externos, como piratas informáticos y ciberdelincuentes, como de amenazas internas, como malicia de los empleados o errores humanos (Kaspersky, s.f.). La protección de la privacidad y seguridad de la información del paciente es una preocupación fundamental en el ámbito de la atención médica.

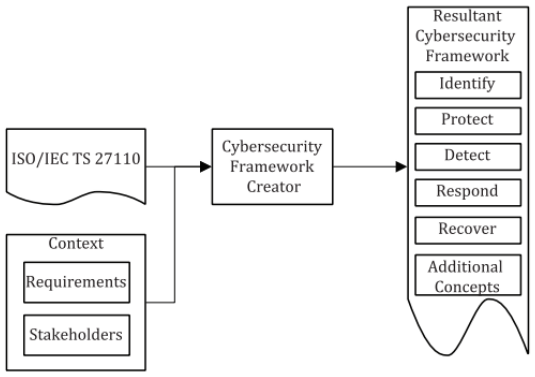
Las normas y políticas como la “Ley de portabilidad y responsabilidad del seguro médico (HIPAA) de la Unión Europea” (Office for Civil Rights (OCR), 2021) y el “Reglamento general de protección de datos (GDPR)” (European Commission, 2016) son consideraciones de privacidad y seguridad del paciente que desempeñan un papel crucial y fundamental en el enfoque de la seguridad en el ámbito de la atención médica. (Sabatino, 2021). Entre estas normas, se destaca la ISO/IEC 27110:2021, la cual ofrece directrices para establecer un marco de ciberseguridad integral y flexible. Esta norma busca lograr un equilibrio adecuado y compatible con los requisitos de las partes interesadas, al tiempo que maximiza la utilización

eficiente de los recursos. Además, promueve la interoperabilidad entre los diferentes usos del marco de ciberseguridad, facilitando su implementación y adaptación a diversas situaciones.

Se busca promover el uso y la implementación de la norma ISO 27110, ya que los creadores del marco de ciberseguridad se encuentran sujetos a los requisitos específicos de sus respectivas partes interesadas. Estos requisitos pueden ser utilizados como fundamentos para respaldar al creador del marco de seguridad informática, permitiendo una estructuración adecuada y la incorporación de conceptos de nivel inferior. A través de esta estructuración, "el marco de seguridad cibernética resultante puede consistir en estándares, pautas y prácticas para promover la gestión de riesgos de seguridad cibernética, ya que los marcos de seguridad cibernética brindan enfoques priorizados, flexibles, repetibles y rentables para ayudar a los usuarios del marco de seguridad cibernética a administrar el riesgo cibernético" (ISO/IEC 27110 , 2021, pág. 8)

Organizaciones reconocidas como Gartner (Gartner, 2020) y el "Banco Interamericano de Desarrollo" (BID, 2019) han destacado la relevancia de la ciberseguridad en el campo de la salud como un aspecto de suma importancia y se ha instado a las organizaciones del sector a tomar medidas efectivas para proteger los datos médicos. Además, se ha observado un creciente reconocimiento en el ámbito de la salud sobre la importancia de implementar marcos de ciberseguridad. La norma ISO 27110 proporciona las directrices necesarias para abordar la seguridad de datos en el sector y adoptar medidas efectivas para proteger la información sanitaria. Esta norma contiene referencias que pueden ser utilizadas de manera independiente para abordar los desafíos específicos del sector salud y salvaguardar la información de manera eficaz.

Sin embargo, la norma ISO 27110 ofrece un valioso apoyo para complementar la implementación de un análisis de riesgos enfocados en la seguridad de datos médicos, que es fundamental para las organizaciones de atención médica. Estas medidas permiten la identificación, protección, detección, respuesta y recuperación de posibles riesgos en la seguridad de los datos médicos. A través de los conceptos proporcionados por la norma ISO, se puede crear un marco de ciberseguridad comprensible, flexible, compatible e interoperable. Al establecer medidas adecuadas de protección y control, las organizaciones pueden reducir significativamente las vulnerabilidades y mejorar la protección y privacidad de información médica (BID, y otros, 2021). Esto fortalecerá su capacidad de respuesta ante amenazas y permitirá una gestión más efectiva en general.



Fuente 1: Documentación Norma ISO 27110:2021

Figura 1:Creación de un marco de ciberseguridad cibernética utilizando ISO/IEC TS 27110

La aplicabilidad de las directrices presentadas en la ISO/IEC 27110:2021 radica en la capacidad de facilitar la comunicación entre los usuarios finales de diferentes marcos de ciberseguridad. Estos conceptos desempeñan un papel fundamental en la creación de un marco

de ciberseguridad sólido y, cuando se aplican de manera integrada, ofrecen una estructura eficaz para organizarlo.

1.6. Alcance

Esta tesis se basa en la investigación y se centrará en la seguridad de los datos médicos y en la detección de posibles riesgos asociados a la información médica. Identificar el riesgo e implementar las medidas de protección y controles de seguridad apropiados para mitigarlos es competencia del comité de seguridad de la información asignado por la máxima autoridad del sector privado o público. Es importante recalcar que esta investigación es un indicador que permitirá a un cliente de salud privada o pública desarrollar un plan de gestión de riesgos con el objetivo de asegurar la protección de la información médica y deberá basar su desarrollo en la norma ISO 27110.

CAPÍTULO II: FUNDAMENTACIÓN TEÓRICA

2.1.Introducción a la Seguridad de la Información

La privacidad en los sistemas e integridad de datos en una organización es fundamental, un sector sumamente vulnerable es el de salud, debido al valor que tienen los datos recopilados. Por tanto, la seguridad de la información se enfoca en "garantizar la confidencialidad, integridad y disponibilidad de los datos, lo que implica prevenir el acceso, uso, divulgación, alteración, modificación, lectura, inspección, registro o destrucción no autorizados". (ISO/IEC 27001, 2022)

Se reconocía como responsabilidad única y exclusiva a la unidad de TIC´s, en la actualidad esta responsabilidad es compartida por todos los miembros de la organización. Es fundamental garantizar una gestión efectiva de la seguridad de la información mediante la correcta evaluación de riesgos a los activos de información de la organización, incluyendo documentos físicos como recurso humano (ISO/IEC 27001, 2022). A partir de esta evaluación, se deben aplicar políticas, procedimientos e intervenciones adecuadas para asegurar la protección de los datos.

2.2.Introducción a la Ciberseguridad de la Información

La ciberseguridad se refiere a una serie de medidas y prácticas implementadas para salvaguardar la información confidencial frente a ataques cibernéticos. También se conoce como seguridad de la tecnología de la información (TI) y se centra en controlar las amenazas que pueden afectar los N.O.S[1] y aplicaciones, tanto internas como externas a una organización

[1](Network Operating System) Sistema operativo de computadora diseñado principalmente para respaldar estaciones de trabajo, PCs y, en algunos casos, terminales más antiguos que están conectados en una red de área local (LAN).

(IBM, 2021). En esencia, la ciberseguridad protege los sistemas y los datos de una organización frente a posibles ataques digitales.

El informe de IBM reportó un costo promedio de 3.86 millones de dólares a nivel global por cada brecha de seguridad de datos, en Estados Unidos es de 8.64 millones de dólares (IBM, 2021). Este costo abarca los gastos relacionados con la detección y respuesta a la brecha, así como el tiempo de inactividad y la pérdida de ingresos, además de los daños a largo plazo en la reputación y la marca de una empresa. Los ciberdelincuentes suelen buscar información de identificación personal (PII, por sus siglas en inglés) de los clientes, como nombres, direcciones, números de identificación nacional o datos de tarjetas de crédito, para posteriormente vender estos registros en mercados digitales clandestinos. La exposición de información de identificación personal puede resultar en una respuesta adversa por parte de los clientes, sanciones regulatorias e incluso acciones legales.

Los expertos en ciberseguridad trabajan continuamente para cerrar las vulnerabilidades de seguridad, pero los atacantes buscan constantemente nuevas formas de evadir las medidas de defensa y explotar las debilidades emergentes. Las últimas tendencias en ciberseguridad se aprovechan de los entornos de trabajo remoto, las herramientas de acceso remoto y los servicios de nube nuevos. Estas tendencias incluyen programas maliciosos cada vez más difíciles de detectar, los mismos que bloquean sistemas y amenazan con divulgar información confidencial, las técnicas de phishing representan una amenaza significativa, ya que los usuarios sin la capacitación adecuada para enfrentar estas situaciones pueden verse involucrados en la revelación de información privada, amenazas internas que pueden evadir las soluciones de

seguridad tradicionales, ataques DDoS[2] que buscan saturar servidores o redes con tráfico, ataques APT[3] que permanecen ocultos durante largos períodos de tiempo, y ataques de intermediario donde un agente malintencionado intercepta y retransmite mensajes con el objetivo de robar datos confidenciales.

2.3.Norma ISO 27110

2.3.1. ¿Qué es la Norma ISO 27110?

Establece las directrices para la creación de un marco de ciberseguridad. Esta norma es "aplicable a los creadores de marcos de seguridad cibernética independientemente del tipo, tamaño o naturaleza de sus organizaciones" (ISO/IEC 27110 , 2021). La ISO 27110 tiene como objetivo proporcionar un conjunto de conceptos para definir marcos de seguridad cibernética para ayudar a aliviar la carga de los creadores y usuarios de estos marcos.

2.3.2. ¿Para qué sirve la Norma ISO 27110?

Es una guía para los creadores de marcos de seguridad cibernética, apoya a desarrollar marcos coherentes y armonizados, lo que permite la alineación de múltiples marcos de seguridad cibernética y la interoperabilidad de múltiples usos de un marco de ciberseguridad. Los principios de la normativa ISO 27110 son flexibles, compatibles e interoperables, lo que permite que existan múltiples tipos de marcos de ciberseguridad.

[2] Ataque de denegación de servicio distribuido.

[3] Una amenaza persistente avanzada (APT, por sus siglas en inglés) se refiere a técnicas de intrusión continuas, sigilosas y sofisticadas utilizadas para acceder a un sistema y mantenerse dentro de él durante un período prolongado, con posibles consecuencias destructivas.

2.3.3. Principios básicos de la normativa ISO 27110

Se fundamenta en los siguientes principios:

- **Flexibilidad:** Coexistencia de diversos enfoques con relación a modelos de ciberseguridad.
- **Compatibilidad:** Adapta diversos protocolos de ciberseguridad
- **Interoperabilidad:** Valida múltiples implementaciones de un marco de ciberseguridad.

Además, establece conceptos para definir marcos de seguridad cibernética, lo que aliviana la carga de los creadores de marcos de seguridad cibernética y a los usuarios finales.

- **Vulnerabilidad:** "Debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas" (ISO/IEC 27000:2018(E), 2018, pág. 11)
- **Amenaza:** "Potencial causa de un incidente no deseado, que puede resultar en daño a un sistema u organización" (ISO/IEC 27000:2018(E), 2018, pág. 10)
- **Impacto:** "El efecto de un evento en un activo" (ISO/IEC 27000:2018(E), 2018, pág. 3)
- **Probabilidad de ocurrencia:** "La medida de la posibilidad de que un evento ocurra". (ISO/IEC 27000:2018(E), 2018, pág. 4)
- **Riesgo:** "La combinación de la probabilidad de que ocurra un evento y su consecuencia". (ISO/IEC 27000:2018(E), 2018, pág. 8)
- **Control:** "Medida que se adopta para reducir el riesgo". (ISO/IEC 27000:2018(E), 2018, pág. 3)

- **Declaración de Aplicabilidad:** Un documento que se emplea para describir el alcance de la implementación de los controles de seguridad de la información seleccionados.(ISO/IEC 27000:2018(E), 2018, pág. 16)
- **Stakeholder:** Persona o grupo que tiene intereses en un sistema o proceso, que pueden ser afectados por el desempeño del sistema o proceso. (ISO/IEC 27000:2018(E), 2018, pág. 5)

2.4.Otras Normas ISO relevantes en Seguridad y Ciberseguridad

Además de la norma ISO 27110, hay otras normas ISO importantes que abarcan la información del sector salud a través de la seguridad y ciberseguridad. A continuación, se enumeran algunas de ellas:

- **ISO 27799:2016 – "*Informática de la salud: Gestión de la seguridad de la información en salud utilizando ISO/IEC 27002*":** Al utilizar los controles descritos en ISO/IEC 27002 y complementarlos de manera adecuada, se puede lograr una gestión efectiva de la seguridad de la información en el ámbito de la salud. (ISO 27799, 2016)
- **ISO 14971:2019- "Dispositivos médicos: Aplicación de la gestión de riesgos a los dispositivos médicos":** Proporciona ayuda a los fabricantes de dispositivos médicos (software de dispositivo) identificar los peligros asociados, valorar, evaluar los riesgos, y gestionar un control de riesgos a través del monitoreo de controles (ISO 14971, 2019)
- **ISO 15408:2022- "*Seguridad de la información, ciberseguridad y protección de la privacidad. Criterios de evaluación de la seguridad informática.*":** consta de cinco partes que abordan distintos aspectos relacionados con la evaluación y certificación.

  Se ofrece una descripción de las partes que conforman la norma ISO 15408:2022.

- **ISO/IEC 15408-1:2022 — *"Parte 1: Introducción y modelo general":*** La norma brinda conceptos generales para evaluar la seguridad de tecnologías de la información y especifica el modelo general de evaluación, que se utiliza de base para evaluar propiedades de seguridad de productos de tecnología de la información (ISO/IEC 15408-1:2022, 2022)
- **ISO/IEC 15408-2:2022—*"Parte 2: Componentes funcionales de seguridad":*** A través de la definición estructural y descripción de contenido de componentes funcionales de seguridad se logra el propósito de la evaluación de seguridad. Incluye un catálogo de componentes funcionales que satisface los requisitos comunes de funcionalidad de seguridad de muchos productos de tecnología de la información. (ISO/IEC 15408-2:2022)
- **ISO/IEC 15408-3:2022 — "Parte 3: Componentes de garantía de seguridad"*:*** Describe los componentes de garantía individuales que forman parte de los niveles de garantía de evaluación y otros paquetes incluidos en ISO/IEC 15408-5, así como evaluar Perfiles de Protección (PP), Configuraciones del PP, Módulos del PP y Objetivos de Seguridad (ST). (ISO/IEC 15408-3:2022)
- **ISO/IEC 15408-4:2022— *"Parte 4: Marco para la especificación de métodos y actividades de evaluación":*** Marco estandarizado para especificar métodos de evaluación y actividades de evaluación objetivas, repetibles y reproducibles. Sin embargo, la ISO /IEC 15408-4:2022 no especifica cómo evaluar, adoptar o mantener los métodos de evaluación y actividades de evaluación. Estos aspectos

corresponden a quienes desarrollan los métodos de evaluación y actividades de evaluación en su área de interés específica. (ISO/IEC 15408-4:2022)

- **ISO/IEC 15408-5:2022 — *"Parte 5: Paquetes predefinidos de requisitos de seguridad":*** Se busca establecer un marco estandarizado que permita especificar métodos de evaluación objetivos, repetibles y reproducibles, con el fin de adoptar un enfoque coherente y confiable en la evaluación de la seguridad de los productos de tecnología de la información. (ISO/IEC 15408-5, 2022)

- **ISO 19011:2018-** ***"Directrices para la auditoría de sistemas de gestión": Establece*** pautas para gestión de programas de auditoría y evaluación de la competencia de los implicados. (ISO 19011, 2018)

Aplicar estas normas en el sector salud permite resguardar la privacidad, fortalecer la integridad y garantizar la disponibilidad de datos, al mismo tiempo que se mejora la calidad de la atención brindada.

2.5.Importancia del Análisis de Riesgos en la Seguridad de los datos médicos

Es necesario entender el por qué es fundamental preservar la confidencialidad, integridad y disponibilidad en el ámbito de la salud (Domingo et al., 2008). La norma ISO 27110 resalta la importancia de detectar y reducir riesgos de seguridad cibernética y establece directrices para el desarrollo de marcos de ciberseguridad.

El análisis de riesgos implica identificar los datos médicos que requieren protección, así como reconocer las posibles amenazas y vulnerabilidades que pueden afectar dichos datos. Además, implica evaluar los posibles impactos que estas amenazas puedan tener tanto en los datos como en la organización en general. Es importante destacar que este proceso debe ser

continuo y todas las partes interesadas deben tener participación, desde proveedores de servicios de salud hasta pacientes y personal médico.

Además, el análisis de riesgos es crucial para la aplicación de regulaciones de privacidad y seguridad, tal y como se establece en la “Ley de Portabilidad y Responsabilidad del Seguro de Salud (HIPAA)” en los Estados Unidos (Sabatino, 2021) en la “Ley HIPAA”, las organizaciones de salud tienen la obligación de gestionar el análisis de riesgos de forma periódica para tener en cuenta las amenazas que pueden afectar a la organización. (Office for Civil Rights (OCR), 2021)

2.6.Análisis de los riesgos de datos médicos

2.6.1. Valoración de los riesgos de la Seguridad de la Información.

La norma ISO 31000 establece la valoración de riesgos como "el proceso integral de evaluar la probabilidad y las consecuencias de un evento perjudicial, así como seleccionar medidas de control adicionales" (ISO 31000(es), 2018).

Es fundamental identificar los recursos de información médica que necesitan ser protegidos. Estos activos abarcan una amplia gama de datos, como registros médicos electrónicos, imágenes médicas, datos de pacientes, información de facturación y otros datos médicos sensibles. Reconocer y comprender la importancia de estos activos en el área de salud permite implementar medidas de seguridad adecuadas y reducir riesgos.

Además, se debe identificar aquellas amenazas reconocidas como atacantes de organizaciones en el sector de la salud. Las amenazas pueden provenir tanto del entorno externo como interno de la organización, conocidos como riesgos de los activos de la información.

En la valoración de los riesgos de datos médicos, se debe considerar: probabilidad de ocurrencia de cada amenaza e impacto de una amenaza que llega a materializarse. Esta evaluación debe tener en cuenta los controles de seguridad existentes y su efectividad en la mitigación de los riesgos identificados.

2.6.2. Descripción de los activos de Información médica

Inicialmente, es crucial comprender los anexos establecidos en la Norma ISO 27110, ya que esto permite a la organización o al oficial de gestión de riesgos encargado entender cómo referenciar cada una de las solicitudes relacionadas con la creación de un marco de ciberseguridad. De esta manera se garantiza un adecuado levantamiento de la información y una correcta identificación del inventario de activos.

Una vez que se han establecido las referencias y se han identificado los activos existentes, se procede a analizar el estándar de referencia establecido por la norma, el estudio y valoración de riesgos considerando los tres criterios ampliamente reconocidos de la información.

El manejo de información médica es crítico para el sector médico, ya que son datos confidenciales y requieren protección especial debido a su sensibilidad y privacidad.

Tabla 1: Identificación de Activos en el contexto Hospitalario

Ítem	Tipo de activo	Modulo	Nombre de la información	Descripción

1	Activo de Información	Agenda de Citas diarias	Control de citas y agentamiento de Exámenes	Organizar y coordinar de manera eficiente las citas de los pacientes, asegurando una adecuada planificación y disponibilidad de recursos para los exámenes necesarios.
2	Activo de Información	Historia Clínica Médica	Triage	Identificar y clasificar a los pacientes según la urgencia de sus necesidades médicas, asegurando que aquellos con mayor riesgo reciban atención inmediata.
3	Activo de Información	Historia Clínica Enfermería	Escalas Pronósticas	Proporcionan indicadores objetivos para medir la gravedad de una enfermedad o condición médica, permitiendo a los enfermeros tomar decisiones informadas sobre el plan de cuidados y el tratamiento del paciente.
4	Activo de Información	Módulo Quirúrgico	Parte Operatorio	Documentación detallada que se genera durante un procedimiento quirúrgico. Incluye información sobre el tipo de cirugía realizada, los instrumentos y materiales utilizados, los hallazgos durante la operación y los pasos seguidos durante el procedimiento.
5	Activo de Información	Farmacia	Alertas, Interacciones	Las alertas e interacciones se generan a través de sistemas de gestión de medicamentos y proporcionan una capa adicional de seguridad en la dispensación y administración de medicamentos.
6	Activo de Información	Apoyo Diagnóstico	Visualización de Imágenes Diagnósticas.	Acceso y visualización de imágenes médicas relevantes para el diagnóstico de enfermedades. Estas imágenes pueden incluir radiografías, tomografías computarizadas, resonancias magnéticas, ecografías y otros estudios de diagnóstico por imágenes.

Fuente 2: Elaboración Propia

La Tabla 1 muestra los activos seleccionados de seis módulos diferentes utilizados en el contexto hospitalario. Esta Tabla permitirá identificar los activos específicos que forman parte del entorno hospitalario y su relevancia en la gestión de la información médica.

La Tabla 1 proporciona una parte del inventario de activos identificados en el contexto hospitalario. Muestra el módulo al que pertenece cada activo, su nombre y una breve descripción.

Los activos médicos tienen implicaciones directas en las personas. Existen numerosos artículos que resaltan los posibles daños inherentes a este tipo de activos, los cuales pueden afectar la reputación del hospital y de igual forma poner en riesgo a los pacientes.

Esta selección de activos es solo una muestra representativa de los muchos activos importantes que se encuentran en el entorno hospitalario.

2.6.3. Identificación de amenazas a las que se encuentra expuesta la Información médica

Según el Cyberthreat Defense Report (CDR), en el año 2022, más de un 40% de las organizaciones informaron haber experimentado seis o más incidentes de seguridad cibernética.

Para 2023, una de las principales preocupaciones reside en el riesgo de filtración de datos provenientes de dispositivos y redes civiles, un tipo de amenaza que ha sido impulsada por el resurgimiento de la era digital. Los datos médicos y otros datos personales serán especialmente buscados por los atacantes. Además del uso de estos datos para llevar a cabo ataques de phishing, smishing o ingeniería social con fines económicos, también se espera que los robos de datos se utilicen cada vez más para influir y desestabilizar.

Entre los ataques más conocidos esta: ransomware y fraude, por lo tanto, es importante anticiparse a las amenazas. La adopción de marcos de ciberseguridad desarrollados por normas ISO, así como la utilización de herramientas y metodologías específicas, junto con el intercambio de información a través de Centros de Análisis y organizaciones especializadas en la protección de datos, son maneras de mejorar la postura en seguridad. Estas acciones

permitirán en el sector privado o público identificar y abordar proactivamente los riesgos, mejorar la detección y respuesta ante incidentes, y mantener una mayor resiliencia frente a las amenazas en el entorno digital.

Como afirma Errol Weiss, director de Seguridad de Health-ISAC, el sector de salud enfrenta un gran desafío: la gestión de riesgos debe ser cuidadosamente planificada. Con medidas preventivas, que pueden parecer costosas en un principio, el sector salud puede evitar gastos mayores a largo plazo ocasionados por situaciones catastróficas. (Pomerantz, 2021)

Como expresa Deloitte en su informe titulado "Escenario de amenazas en la Industria de Salud y Ciencias de la Vida" (Deloitte, 2019), se presenta un gráfico que identifica las amenazas a la industria de la salud y describe los servicios y habilitadores utilizados para llevar a cabo este tipo de amenazas.

Figura 2: Identificación de amenazas

<table>
<tr>
<td> 
</td>
<td>SERVICIOS Y HABILITADORES
Mercados y foros clandestinos
Servicios de verificación de cuentas
Servicios de proxy y VPN criminales
Alojamiento a prueba de balas</td>
</tr>
</table>

	Kits de Maldoc y descargadores Revendedores de tráfico Servicios de spam

Fuente: (Deloitte, 2019)

En la Figura 2 se identifican diversas amenazas y se describen los servicios y herramientas para reprimirlos.

Una de las amenazas destacadas es el "Recon and Scanning" (Reconocimiento y Exploración), que implica la recopilación de información para identificar posibles vulnerabilidades en los sistemas y redes de la industria de la salud.

También se menciona la explotación de vulnerabilidades en dispositivos médicos y aplicaciones, lo cual puede comprometer la seguridad de los pacientes.

El robo de propiedad intelectual (IP) es otra amenaza relevante, donde la información y los avances médicos pueden ser objeto de robo o piratería, afectando la innovación y la competitividad de las organizaciones.

La extracción de datos de registros electrónicos de salud (EHR4/PHI5) es una preocupación importante, ya que los datos médicos y personales pueden ser extraídos de manera inapropiada o fraudulenta.

Las Amenazas Persistentes Avanzadas (APTs) se mencionan como una forma sofisticada de ataque, donde se busca obtener acceso prolongado y no autorizado a los sistemas del sector salud para obtener información confidencial o causar daño.

El "Spear Phishing" se refiere a los intentos personalizados de engañar a individuos dentro de la industria de la salud para obtener información confidencial o acceso a sistemas mediante técnicas de ingeniería social.

Por último, se hacen referencia a servicios ilícitos como mercados clandestinos, servicios de verificación de cuentas, servicios de proxy y VPN criminales, alojamiento a prueba de balas, kits de Maldoc y descargadores, revendedores de tráfico y servicios de spam. Estos servicios brindan recursos y herramientas utilizadas por ciberdelincuentes para llevar a cabo actividades maliciosas.

En la Norma ISO 27110, se destaca el concepto de "Identificar" en el contexto de la ciberseguridad. Este concepto engloba todo el panorama de la ciberseguridad que se está considerando (ISO/IEC, 2021). El concepto "Identificar" abarca diversas áreas relacionadas con actividades específicas, y selecciona únicamente las más relevantes. Estas áreas pueden incluir el “entorno empresarial, la evaluación de riesgos, la estrategia de gestión de riesgos, la

[4] Versión electrónica que incluye información como datos demográficos, notas de progreso, problemas médicos, medicamentos, signos vitales, historial médico previo, vacunas, datos de laboratorio e informes radiológicos.

[5] PHI (Información de Salud Protegida) se refiere a una amplia gama de información presente en registros médicos, ya sea en formato digital (como registros electrónicos de salud o EHR) o en papel, que puede ser utilizada para identificar a una persona.

gobernanza, la gestión de activos, el análisis del contexto empresarial y las consideraciones de la cadena de suministro" (ISO/IEC 27110 , 2021). También se deben tener en cuenta aspectos como la presencia de la organización en el ciberespacio, su "ciberpersona", las funciones e información críticas para el negocio y los recursos relacionados. Comprender este concepto de identificación proporciona una perspectiva flexible, repetible, enfocada y priorizada en la ciberseguridad.

2.6.4. Análisis comparativo de la Norma ISO 27110 vs Seguridad de la Información médica actual

Se debe fomentar la aplicación de normas, marcos de trabajo, protocolos y metodologías para establecer enfoques sistemáticos y efectivos.

Se ha realizado un análisis comparativo de la norma ISO 27110 y la seguridad de la información médica actual.

Tabla 2: Análisis comparativo de la Norma ISO 27110 vs Seguridad de la Información médica actúa

Aspectos de Seguridad	Norma ISO/IEC 27110 TS	Seguridad de la Información Médica Actual
Enfoque	Priorizado, flexible, repetible y rentable (ISO/IEC 27110 , 2021)	Enfoque integral a gestión de datos y seguridad.
Alcance	Aplicable a creadores de marcos de ciberseguridad para todo tipo de organización sin tomar en cuenta el tamaño o el giro de negocio (ISO/IEC 27110 , 2021)	Diseñar e implementar barreras de seguridad para GR.
Proceso de Gestión de Riesgos	Estructurado y consiste en estándares, pautas y prácticas documentadas (ISO/IEC 27110 , 2021)	Aplicación de SGSI.

Identificación de Activos	Identificación exhaustiva y priorización según el riesgo (ISO/IEC 27110 , 2021)	Manejo de inventario
		Falta de documentación
Evaluación de Riesgos	Evaluación de riesgos según la probabilidad e impacto del riesgo (ISO/IEC 27110 , 2021)	Evaluación de riesgos basada en experiencias anteriores
Controles de seguridad	Documentación estructurada que ayuda con el establecimiento de controles de seguridad basado en el mapeo de estándares ISO.	Enfoque en controles de seguridad específicos, no necesariamente basados en el riesgo.

Fuente: Auditoría Propia

Por lo tanto, al analizar la Tabla 2, se puede concluir que la Norma ISO 27110 ofrece un enfoque más estructurado y completo para la gestión de riesgos y seguridad de datos. La seguridad de la información médica actual se centra en la protección de la información y adopta un enfoque reactivo ante incidentes de seguridad.

La norma ISO 27110 tiene una gestión de riesgos en la identificación de activos y controles de seguridad, mientras que la seguridad de la información médica actual centra sus controles de seguridad de manera específica, sin necesariamente considerar el enfoque de riesgo.

CAPÍTULO III: METODOLOGÍA

En esta sección, se explica los pasos y enfoques utilizados para que el sector de salud pública y privada conozca como recopilar datos y analizar información.

El sector de salud pública y privada tiene la posibilidad de desarrollar el marco metodológico que describe procedimientos y técnicas para abordar y resolver el planteamiento del problema alineados a la Normas ISO 27110

Es importante que los clientes de seguridad pública y privada por medio de personal cualificado presente un borrador de propuesta del marco de ciberseguridad que contemple medidas de protección y controles necesarios de seguridad para mitigar los riesgos, basados en la Norma ISO 27110.

Ambos aspectos, el marco metodológico y el marco de ciberseguridad, se complementarán para proporcionar una base sólida en la cual se fundamentará la investigación y se brindarán recomendaciones concretas para la gestión de la ciberseguridad en el contexto de la atención médica.

Investigación Cuantitativa

El sector de la salud pública y privada puede o debe utilizar procesos organizados que permiten verificar suposiciones de manera secuencial. Dentro de esta ruta, todas las etapas preceden a la siguiente y no es posible descartar los pasos, por lo que es importante mantener un orden. Pudiéndose redefinir una etapa una vez iniciada.

Para comenzar, se parte de una idea que se delimita, se plantean los objetivos y preguntas de investigación. Se hace una lectura profunda de la literatura disponible para así lograr una base teórica sólida.

Se debe relacionar las mediciones obtenidas utilizando métodos estadísticos apropiados. (Hernández Sampieri & Mendoza Torres, 2018)

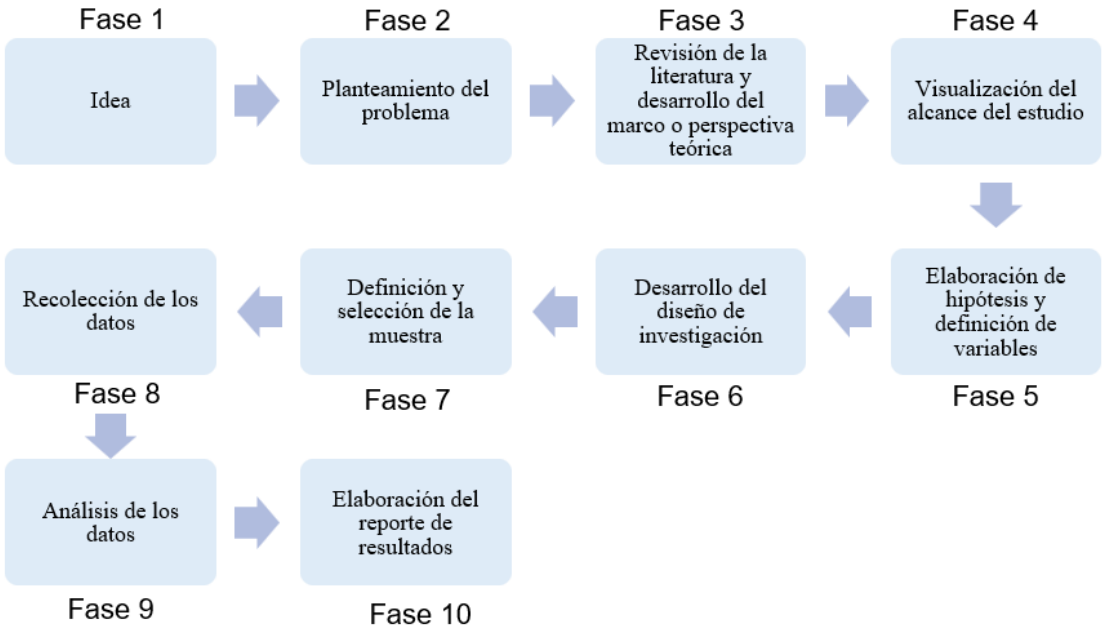


Figura 3: Proceso de Investigación Cuantitativo

Fuente: (Hernández Sampieri & Mendoza Torres, 2018)

Investigación Cualitativa

Con el estudio cualitativo el sector de la salud pública y privada pueden llegar a estudiar fenómenos de manera sistemática. Esta ruta está apoyada por los datos y los resultados, la examinación de hechos y la revisión de estudios previos.

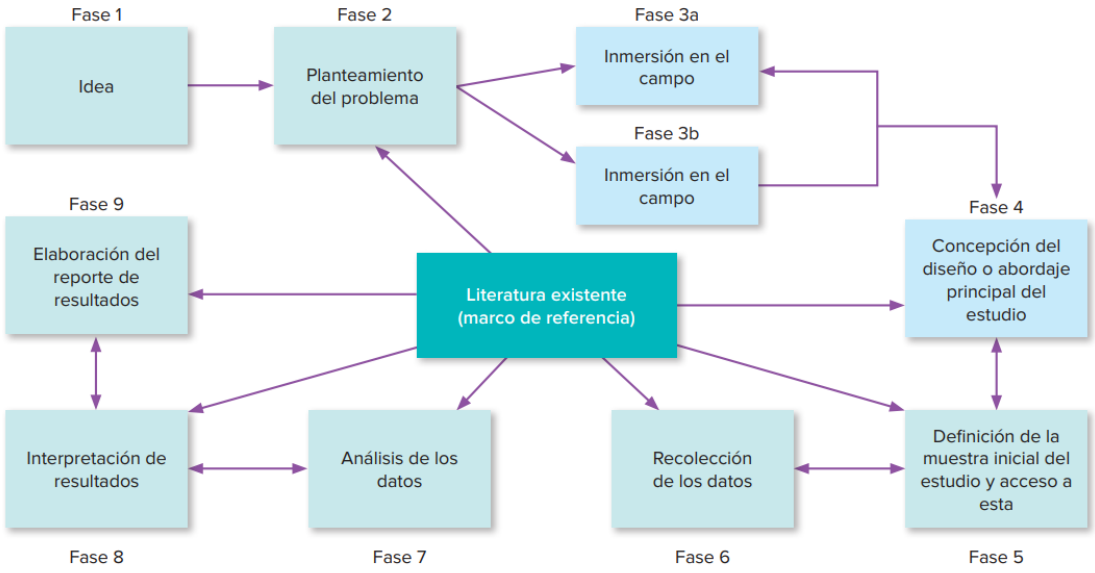


Figura 4: Proceso cualitativo

Fuente: (Hernández Sampieri & Mendoza Torres, 2018)

Investigación Mixta

Los datos médicos mediante la utilización de la norma ISO/IEC 27110:2021, tiene un enfoque metodológico mixto (cuantitativo y cualitativo). El análisis, integración y discusión de datos cuantitativos van a brindar conocimientos a la literatura de la norma ISO.

La investigación cuantitativa no se encuentra intrínsecamente vinculada a la formulación de hipótesis. Es posible llevar a cabo un estudio cuantitativo descriptivo (encuesta), como en el caso presente, donde no se plantean hipótesis debido a la ausencia de correlaciones entre variables y la falta de una relación causa-efecto. En cambio, los estudios correlacionales, relacionales o explicativos suelen involucrar la formulación de hipótesis. En este estudio descriptivo (encuesta), se centra en la descripción de variables asociadas a la Norma ISO 27110.

Es importante destacar que la ausencia de hipótesis en un estudio descriptivo (encuesta) no implica que este carezca de enfoque cuantitativo. En el presente caso, el estudio descriptivo

(encuesta) abarca tanto aspectos cualitativos como cuantitativos. La revisión bibliográfica realizada constituye una parte del enfoque cualitativo, mientras que la parte cuantitativa se refleja en la determinación de la población objetivo para las entrevistas y en los procedimientos asociados al procesamiento de las encuestas.

En concordancia con lo anteriormente expuesto, seleccionamos el estudio descriptivo (encuesta) con el propósito de aprovechar los puntos fuertes en busca de capitalizar ventajas, para tener un análisis adecuado.

3.1. Tipo de Investigación

El tipo de investigación es descriptivo y analítico, basado en el mapeo de estándares establecidos por la norma ISO 27110 como directrices para abordar un marco de ciberseguridad. El objetivo es describir de manera precisa los activos de información médica y referenciar su nivel de exposición frente a las diversas amenazas existentes. Además, se llevará a cabo un análisis del riesgo involucrado con lo que propone la Norma ISO, aunque no se realizará una evaluación aplicando las referencias directamente. A partir de esta evaluación referencial, se propondrán medidas de protección adecuadas en respuesta a la situación identificada. Esta metodología proporciona un panorama detallado y un entendimiento profundo de la situación.

3.2. Métodos y Técnicas de Investigación

3.2.1. Métodos

Se fundamenta en los conceptos establecidos por la ISO/IEC 27110:2021 y a través de la identificación de activos de información médica, utilizando la especificación técnica que ofrece la norma se debe referenciar por Tablas los anexos que refieren la identificación, evaluación de amenazas y vulnerabilidades. Los diversos mapeos referenciales, conecta con la

evaluación de activos en función de los criterios establecidos por la norma. Este enfoque metodológico permite obtener una directriz integral para el tratamiento de riesgos y vulnerabilidades presentes en el entorno de la ciberseguridad de la información médica.

3.2.2. Técnicas

La técnica utilizada en este estudio descriptivo incluye la encuesta, para recopilar información adicional que permita conocer y tener claridad de los riesgos de los datos médicos.

3.2.3. Procedimiento

El procedimiento en el estudio descriptivo contempla tres fases principales.

- Primera Fase: Revisión bibliográfica y documental para recopilar información relevante sobre la norma ISO/IEC 27110:2021 y la seguridad de la información de datos médicos.
- Segunda Fase: Identificación de activos, categorización del impacto del activo de la información según la documentación referencial de la norma y la categorización de la evaluación del riesgo externo mediante el análisis de riesgo.
- Tercera Fase: Propuesta de medidas de protección adecuadas para minimizar los riesgos identificados utilizando únicamente las referencias que establece la norma ISO 27110:2021.

3.2.4. Elección de muestra

La unidad de análisis de este trabajo de titulación es la muestra. Roberto Hernández y Christian Paulina establecen en su libro “Metodologías de la Investigación” que “muestrear” es la acción de tomar un subconjunto de un conjunto mayor, universo o población de interés para hacer la toma de datos necesarios con el fin de lograr responder al planteamiento de problema.

3.2.5. Tipos de muestra

La selección del tipo de muestra es dirigida, debido a que no se realizan procedimientos mecánicos o se plantea fórmulas de probabilidad. La muestra en este caso es la selección cuidadosa de sujetos con características específicas.

La encuesta se realizó en el país Ecuador, provincia: Pichincha, ciudad: Quito, sector: salud, tipo: privada, ente: hospital, especialidad: tratamiento de cáncer y anomalías. En este caso, la población y la muestra serán idénticas, ya que se recolectarán datos de entre 50 y 60 personas, corresponde al 10% que trabaja en la institución. Es importante considerar que el porcentaje propuesto corresponde a colaboradores de los departamentos de Tecnología, Área Médica, Administrativa y Servicios. Quiero destacar que los colaboradores seleccionados para participar en la encuesta son aquellos que tienen personal a su cargo dentro de su unidad. Sin embargo, debido a restricciones de tiempo, se tomará a aquellos colaboradores que ocupan posiciones críticas dentro del hospital.

CAPITULO IV: DESARROLLO DE LA INVESTIGACIÓN

El Capítulo cuatro se limita a realizar las tres fases que se plantean en el capítulo III numeral 3.2.3 Procedimiento.

Primera Fase, es la recopilación de datos por medio de la encuesta para obtener información relevante que sustente el análisis de este trabajo de titulación. La encuesta comprende 34 preguntas para las cuatro áreas del hospital.

Segunda Fase, se va a realizar la identificación de activos, categorización del impacto del activo de la información según la documentación referencial de la norma y la categorización de la evaluación del riesgo externo mediante el análisis de riesgo.

Tercera Fase, concluye con una propuesta de medidas de protección adecuadas para minimizar los riesgos identificados utilizando únicamente las referencias que establece la norma ISO 27110:2021.

4.1. Primera Fase: Encuesta – Recopilación y Análisis

Una de las partes para la obtención de la titulación es la encuesta que tiene como nombre: "Encuesta *de Ciberseguridad en el Sector Salud basada en la Norma ISO/IEC 27110 TS*"- ANEXO 1, que permite la recopilación de datos para obtener información de interés para sustentar un análisis.

La encuesta tiene opción múltiple y será llenada por los responsables de departamentos mencionados en el capítulo III numeral 3.2.5 Tipos de muestra que son: Tecnología, Área Médica, Administrativa y Servicios y corresponden al 10% de colaboradores del hospital con especialidad en tratamiento de cáncer y anomalías.

4.1.1. Encuesta

Título: Encuesta de Ciberseguridad en el Sector Salud basada en la Norma ISO/IEC 27110 TS”

*Pregunta 1: ¿*Cuál *es su nivel educativo?:*

Análisis de la pregunta 1: Los valores obtenidos evidencian que el hospital con especialidad en tratamiento de cáncer y anomalías tiene un porcentaje muy alto de profesionales con titulación de tercer nivel que tienen liderazgo y tienen cierto poder de decisión.

Pregunta 2: Acorde al título que escogió en la pregunta #1, indique cuál es su área de especialización.

Análisis de la pregunta 2: Los colaboradores en un buen porcentaje pertenecen al departamento de tecnología, oportunidad para presentar un proyecto que contemple la seguridad de datos médicos, entender que la responsabilidad no solo es de TIC´s, es compartida por todos los miembros de la organización, la aprobación del proyecto puede garantizar una gestión efectiva de la seguridad de la información con políticas, procedimientos e intervenciones adecuadas para asegurar y proteger el dato médico.

Pregunta 3: ¿En qué tipo de organización relacionada con servicios de salud trabaja actualmente?

Análisis de la pregunta 3: Estos valores referencian a que la muestra es consistente, el 28.8% pertenece al sector de salud pública, podemos creer que son profesionales en medicina que pertenecen al departamento médico, especialistas que prestan su profesionalismo en ambas

organizaciones, facultados por ley, este valor, aporta y contribuye para sumar experiencia y dar estructura a un gran proyecto con responsabilidad compartida.

Pregunta 4: ¿Está familiarizado/a con el Acuerdo Ministerial No. 025-2019 relacionado con la seguridad de la información en el sector salud?

Análisis de la pregunta 4: Importante conocer que el 66.2% de los colaboradores de los departamentos de Tecnología, Área Médica, Administrativa y Servicios no conoce el Acuerdo Ministerial No. 025-2019, es decir, conocen el riesgo y las diferentes connotaciones que implica el no cumplimiento de la seguridad de la información en el sector salud.

Pregunta 5: ¿Conoce usted que es un comité de seguridad de la información?

Análisis de la pregunta 5: Este valor permite tener claro que la mayoría de los colaboradores de los departamentos de Tecnología, Área Médica, Administrativa y Servicios tienen claridad que es un comité de seguridad de la información, por lo tanto, conocen que es el ente responsable de impulsar proyectos, velar que avancen y responder por la seguridad de la información, para este estudio descriptivo, el dato médico. Adicional, acotar que es importante que este comité este estructurado antes de iniciar o implementar una estrategia de seguridad e imprescindible reforzar el conocimiento a los otros colaboradores de los departamentos.

Pregunta 6: ¿Usted sabe qué un comité de seguridad de la información es designado por la máxima autoridad de su empleador?

Análisis de la pregunta 6: Mayoría de colaboradores conocen que este comité de seguridad de información es designado por la máxima autoridad, garantiza la directriz vertical y el éxito al momento de avalar, implementar un proyecto de seguridad de la información, importante reforzar

el conocimiento del organigrama de la organización al otro grupo de colaboradores de los departamentos de Tecnología, Área Médica, Administrativa y Servicios.

Pregunta 7: ¿Usted conoce que el comité de seguridad de la información es la unidad que realiza el seguimiento del cumplimiento del acuerdo ministerial No? 025-2019?

Análisis de la pregunta 7: Se debe reforzar el conocimiento a los colaboradores en los departamentos de Tecnología, Área Médica, Administrativa y Servicios como son las funciones, acciones, deberes y cumplimiento del comité de seguridad de la información dentro de la organización que referencia este estudio descriptivo.

Pregunta 8: ¿Está familiarizado(a) con la norma ISO/IEC 27110:2021 - Tecnología de la información, ciberseguridad y protección de la privacidad — Directrices para el desarrollo del marco de ciberseguridad?

Análisis de la pregunta 8: La mayoría de los colaboradores de los departamentos de Tecnología, Área Médica, Administrativa y Servicios no conoce la norma ISO/IEC 27110:2021, la máxima autoridad debe priorizar que se imparta y socialice el conocimiento de la norma ISO/IEC 27110:2021 a sus colaboradores para que el comité de seguridad de la información realice una buena gestión.

Pregunta 9: ¿Usted considera que en el sector de la salud la ciberseguridad mencionada en la pregunta anterior es un aspecto importante para proteger la información?

Análisis de la pregunta 9: Para la gran mayoría de colaboradores de los departamentos de Tecnología, Área Médica, Administrativa y Servicios es importante la seguridad de la información, se debe canalizar e impartir conocimiento de la importancia de proteger los datos médicos a aquellos colaboradores que no dan valor a la protección de la información.

Pregunta 10: Está preocupado por la seguridad de los datos médicos de: colaboradores, pacientes, clientes pagadores, etc…en el sector de la Salud.

Análisis de la pregunta 10: Un pequeño porcentaje de la muestra considera que no existe razón para tener preocupación por la seguridad de los datos médicos, esta incredulidad abre la puerta a todo tipo de riesgo, por lo tanto, es el momento para que la organización tome acción en facilitar a estos colaboradores el conocimiento necesario para que perciban el riesgo inminente que se encuentra su lugar de trabajo.

Pregunta 11: Su empleador implementa medidas de seguridad efectivas para proteger los datos médicos?

Análisis de la pregunta 11: Desalentador que el 61.9% de colaboradores de los departamentos de Tecnología, Área Médica, Administrativa y Servicios lleguen a desconocer las medidas de seguridad que la organización implementa para proteger los datos médicos, un análisis simple, indicar que es desalentador, si analizamos un poco más, consideramos que se debe impartir, viabilizar y socializar todo lo que la organización realiza para proteger el dato médico a los colaborades que indican desconocer.

Pregunta 12: Conoce las implicaciones de pérdida, robo, ataque, amenaza, vulnerabilidad, impacto, etc…de los datos médicos de colaboradores, pacientes, clientes pagadores, etc…

Análisis de la pregunta 12: Si bien tenemos un buen porcentaje de colaboradores de los departamentos de Tecnología, Área Médica, Administrativa y Servicios que conocen las implicaciones de pérdida de los datos médicos, un 40.6% debe ser capacitado por el comité de seguridad de la información para evitar riesgos.

Pregunta 13: Considera que su empleador asigno recursos financieros suficientes para abordar los riesgos de seguridad de los datos médicos.

Análisis de la pregunta 13: La falta de socialización de parte de la organización y su comité de seguridad de la información genera incertidumbre, por lo tanto, es importante compartir información con los colaboradores de los departamentos de Tecnología, Área Médica, Administrativa y Servicios.

Pregunta 14: Su empleador realiza capacitación para la protección de datos médicos.

Análisis de la pregunta 14: Es muy importante que la organización imparta capacitación para la protección de los datos médicos, los colaboradores de los departamentos de Tecnología, Área Médica, Administrativa y Servicios están a la deriva, un 71.4% de estos colaboradores no tiene el conocimiento de cómo proteger un dato médico, puede llevar a la organización a la línea delgada de credibilidad, donde, colaboradores, pacientes, clientes pagadores, etc… se encuentran inmersos en la fuga de su información y la entidad asume un riesgo no necesario.

Pregunta 15: Considera que su empleador está comprometido en la mejora continua con la seguridad de los datos médicos.

Análisis de la pregunta 15: Un 37.5% considera que la organización está comprometida en mejorar la seguridad de los datos médicos, para aquellos colaboradores de los departamentos de Tecnología, Área Médica, Administrativa y Servicios que hacen la diferencia para llegar al 100% se debe impartir capacitación a los colaboradores, caso contrario, el comité de seguridad de la información no tendrá aceptación.

Pregunta 16: ¿Qué tan preparado está su empleador para hacer frente a posibles ataques a los datos médicos?

Análisis de la pregunta 16: La respuesta a esta pregunta causa temor, NO, simplemente se debe reforzar por parte del comité de seguridad de la información a los colaboradores de los departamentos de Tecnología, Área Médica, Administrativa y Servicios que la seguridad de los datos médicos es compartida por toda la organización y es un deber de todos proteger la información de forma transversal.

Pregunta 17: ¿Cuál de estas medidas de protección que permiten prevenir y mitigar posibles ataques a los datos médicos usted conoce que se implementó en su empleador? (Seleccione las medidas que conoce, pueden ser varias opciones)?

Análisis de la pregunta 17: Se tiene un 38.5% de colaboradores de los departamentos de Tecnología, Área Médica, Administrativa y Servicios que indican que fueron capacitados acorde a la pregunta, contradice el análisis previo?, creo que NO, considero que la capacitación no fue realizada a los usuarios clave de parte del comité de seguridad de la información.

Pregunta 18: ¿En qué parámetro considera que las medidas para proteger y prevenir de posibles ataques a los datos médicos propuestas por su empleador son satisfactorias?

Análisis de la pregunta 18: Al momento el indicador en esta respuesta no es favorable para protección y prevención de los datos médicos, por lo tanto, es indispensable que el comité de seguridad de la información capacite a los colaboradores de los departamentos de Tecnología, Área Médica, Administrativa y Servicios para mejorar la seguridad de los datos médicos en la organización.

Pregunta 19: ¿Conoce usted si su empleador cuenta con un protocolo formal establecido para responder a posibles ataques de ciberseguridad, de acuerdo, a los siguientes puntos?

Análisis de la pregunta 19: La dispersión de los resultados es una evidencia clara que no se tiene un documento y lineamientos estructurados para responder a posibles ataques de ciberseguridad, La responsabilidad es compartida y toda la organización debe avanzar para tener un protocolo documentado de forma completa. Adicional, es de vital importancia fortalecer la comunicación y generar conciencia en el impacto que puede tener la organización a un ataque a la seguridad de la información.

Pregunta 20: Los ataques de ciberseguridad afectan las transfusiones de medicamentos y el funcionamiento de las máquinas médicas. ¿Qué opción considera más aceptable?

Análisis de la pregunta 20: Los colaboradores de los departamentos de Tecnología, Área Médica, Administrativa y Servicios no tienen conciencia crítica del riesgo e impacto que puede tener la organización, todo aquel que se encuentre dentro del proceso de gestión de la información tiene responsabilidad compartida ante un ataque a la seguridad de la información. Por lo tanto, es necesario educar y concientizar a todos los miembros de la organización.

Pregunta 21: ¿Su empleador cuenta con un protocolo establecido para controlar y prevenir ataques de ciberseguridad en la transfusión de medicamentos y el uso de máquinas médicas?

Análisis de la pregunta 21: El (68,9%) responde que su empleador no cuenta con un protocolo establecido para controlar y prevenir ataques de ciberseguridad. Un indicador que la seguridad de la información no es tratada de forma adecuada. La máxima autoridad debe reforzar que la vulnerabilidad de los datos médicos son responsabilidad compartida, es el momento de

solicitar al comité de seguridad de la información el espacio y tiempo para estructurar un proyecto para proteger la información.

Pregunta 22: Si la respuesta es "No", escoja de las siguientes opciones el por qué no se implementa un protocolo:

Análisis de la pregunta 22: El conocimiento es el camino al éxito, la máxima autoridad de la organización debe fortalecer por medio del comité de seguridad de la información la capacitación en ciberseguridad de los colaboradores de los departamentos de Tecnología, Área Médica, Administrativa y Servicios.

Pregunta 23: ¿Existe un protocolo de evaluación de riesgo para controlar y prevenir ataques de ciberseguridad en la transfusión de medicamentos y el uso de máquinas médicas en su empleador?:

Análisis de la pregunta 23: Oportunidad para el cambio, todos los colaboradores de los departamentos de Tecnología, Área Médica, Administrativa y Servicios deben tener una mesa de trabajo para llevar un proyecto que permita desarrollar un protocolo de evaluación de riesgo, será el comité de seguridad de la información el aprobador, el desarrollo debe estar alineado con la norma ISO/IEC 27110.

Pregunta 24: Considera que su empleador debería aplicar la norma ISO/IEC 27110:2021 para desarrollar las directrices y obtener un marco de ciberseguridad que mejore la seguridad de los datos médicos?:

Análisis de la pregunta 24: Esta respuesta permite al comité de seguridad de la información encaminar el proyecto de seguridad en la organización, el riesgo es compartido por todos, quien

lleve la iniciativa deberá unir los esfuerzos de todos los colaboradores de los departamentos de Tecnología, Área Médica, Administrativa y Servicios.

Pregunta 25: Su empleador cuenta con alguna certificación ISO de ciberseguridad, como por ejemplo ISO 27001, ISO 27701 u otras relacionadas?:

Análisis de la pregunta 25: Los colaboradores de los departamentos de Tecnología, Área Médica, Administrativa y Servicios no conocen si la organización tiene certificación ISO, momento exacto para que el comité de seguridad de la información descubra el potencial de los colaboradores y nomine dos o tres profesionales para obtener las certificaciones que son fundamentales para establecer y alinear un sistema de gestión de seguridad de la información que garantice la protección de los datos médicos.

Pregunta 26: ¿Considera que su empleador aplica Sistemas de Gestión de Seguridad de la Información (SGSI) para el control y protección de la seguridad de los datos médicos?:

Análisis de la pregunta 26: Desconocer la realidad de la organización no necesariamente implica que se realiza algo mal, creo que el comité de seguridad de la información no informo adecuadamente a los colaboradores de los departamentos de Tecnología, Área Médica, Administrativa y Servicios el control y protección de seguridad de los datos médicos, debemos recordar que la responsabilidad es de todos.

Pregunta 27: ¿En su unidad de negocio existe uno o varios colaboradores que cuenten con certificación en seguridad de la información ISO 27001?:

Análisis de la pregunta 27: No conocer dentro de tu departamento si tienes un colaborador con certificación en seguridad de la información es un problema, esto debe ser tratado por el comité de seguridad de la información de forma urgente, si uno o varios departamentos no tiene al

colaborador certificado, es imprescindible comenzar el proceso de certificación para aplicar la norma ISO a la protección y seguridad del dato médico. La aplicabilidad del plan de certificación es responsabilidad del comité de seguridad de la información.

Pregunta 28: Es importante tener uno o varios colaboradores con certificación en Seguridad de la Información - ISO 27001 dentro de su unidad de negocio y/o empleador?:

Análisis de la pregunta 28: Para aquellos colaboradores de los departamentos de Tecnología, Área Médica, Administrativa y Servicios que no tiene claro la relevancia de tener un colaborador con certificación ISO es manejable, se debe informar y explicar el por qué es importante tener dentro del departamento un recurso con certificación ISO, es mandatorio tener colaboradores con certificaciones ISO en seguridad del dato médico, el plan de certificación es responsabilidad del comité de seguridad de la información.

Pregunta 29: ¿Conoce algún problema reciente o actual relacionado con la vulnerabilidad de la pérdida, robo, ataque, amenaza, vulnerabilidad, impacto, etc…de la seguridad de los datos médicos?:

Análisis de la pregunta 29: Ser enfáticos en la necesidad de proteger la información de los datos médicos es fundamental para evitar exponer a la organización en situaciones legales, la respuesta de los encuestados reafirma el compromiso de todos los colaboradores de los departamentos de Tecnología, Área Médica, Administrativa y Servicios para prepararse académicamente y certificarse para proteger, resguardar el dato médico ante cualquier tipo de problema que resalta la pregunta.

Pregunta 30: ¿Conoce si realizan auditorias regulares de seguridad de la información en su empleador para evaluar el cumplimiento de los estándares y normas establecidos?:

Análisis de la pregunta 30: El escenario real es el desconocimiento, debemos entender si es por falta de comunicación o socialización del comité de seguridad de la información para los colaboradores de los departamentos de Tecnología, Área Médica, Administrativa y Servicios, de ser el caso, se debe actuar y proceder inmediatamente en comunicar la importancia de las auditorías.

Pregunta 31: ¿Con qué frecuencia se realizan evaluaciones periódicas de vulnerabilidad y pruebas de penetración para identificar posibles brechas de seguridad en los sistemas y aplicaciones de su empleador?:

Análisis de la pregunta 31: El éxito del comité de seguridad de la información pasa por comunicar e informar oportunamente a los colaboradores de los departamentos de Tecnología, Área Médica, Administrativa y Servicios, por lo tanto, genera compromiso de responsabilidad para tener seguro el dato médico.

Pregunta 32: ¿Tiene su empleador un equipo dedicado a la seguridad de la información que se encargue de gestionar, supervisar, prevenir, informar aspectos relacionados con la seguridad de la Información?:

Análisis de la pregunta 32: Un comité de seguridad de la información no tiene éxito cuando no comunica e informa a la organización. Es fundamental siempre tener el canal de comunicación abierto para dar y recibir información, de esta forma la responsabilidad es compartida y la seguridad del dato médico tendrá un equipo de profesionales dedicados a evitar vulnerabilidades.

Pregunta 33: ¿En qué nivel se implementan medidas de control de acceso físico y lógico para proteger los activos críticos y los sistemas de información de su organización?:

Análisis de la pregunta 33: Reforzar las medidas de control es una máxima en un departamento de tecnología, el costo financiero es alto, las organizaciones deben evaluar que provoca más riesgo, una inversión o una pérdida de imagen.

Pregunta 34: ¿Conoce con qué frecuencia se realizan copias de seguridad de las bases de datos de su empleador para garantizar la disponibilidad y recuperación de la información en caso de una pérdida, robo, ataque, amenaza, vulnerabilidad, impacto, etc…de la seguridad de los datos?:

Análisis de la pregunta 34: Dispersión en respuesta por desconocimiento, el comité de seguridad de la información debe regular que se tenga la misma información de los colaboradores de cada departamento de Tecnología, Área Médica, Administrativa y Servicios dentro de la organización.

Pregunta 35: Conoce en qué nivel se implementan medidas de seguridad adicionales, como: monitoreo de seguridad en tiempo real, detección de intrusos y análisis de comportamiento, para identificar y responder de manera proactiva a las amenazas pérdida, robo, ataque, amenaza, vulnerabilidad, impacto, etc… a la seguridad de los datos médicos?:

Análisis de la pregunta 35: La responsabilidad es compartida indica la norma ISO/IEC 27110, 2021, por lo tanto, todos deben reportar al comité de seguridad de la información si los niveles de seguridad no son los mejores, entonces, se debe mejorar para que la organización no se encuentre vulnerable a todo tipo de amenaza a la seguridad del dato médico e incluso temas legales.

La encuesta y el análisis de cada pregunta lleva a enfatizar que esta organización debe fomentar la comunicación e información a los colaboradores de los diferentes departamentos, no hacerlo implica poner en riesgo a la máxima autoridad y al comité de seguridad de la información.

4.2 Segunda Fase: Identificación de activos, categorización de impacto y categorización del riesgo.

4.2.1 Identificación Activos de Información

La norma ISO describe cinco conceptos fundamentales de un marco de ciberseguridad, los cuales tienen como objetivo brindar apoyo al creador del marco de seguridad cibernética. Es importante tener en cuenta que la creación de un marco cibernético involucra diferentes partes interesadas y requisitos, pero los conceptos que se enumerarán son consistentes y proporcionan una base sólida.

Ahora bien, el planteamiento de medidas y controles requiere realizar un levantamiento de activos. Los activos componen los sistemas de información y son susceptible a ataques de manera intencional o accidental que tienen consecuencias dentro de la organización. A continuación, se presenta el listado de activos identificados.

Tabla 2: Listado de activos

DEPARTAMENTO	ACTIVOS
Departamento de tecnología	Centro Datos
	Servidores
	Equipos de comunicación (Redes, Firewalls, Wifi)
	Computadoras (PC, Portables)
Departamento Médico	Agendamiento
	Nutrición-Alimentación
	Farmacia/Tecnofarmacia
	Quirófano
	Admisión
	Auditoria Médica
	Telemedicina
	LIS (PRUEBAS DE ANTIGENOS)
	RIS-PACS (IMAGENOLOGIA)

Departamento de Servicios	Mantenimiento
	Servicio de Seguridad
	Limpieza

Fuente: Auditoría Propia 1

Identificar

La identificación de activos se realizó siguiendo las pautas establecidas por la norma ISO 27110. El concepto de identificación forma parte del ecosistema de ciberseguridad que se está abordando. Dentro de las consideraciones del ecosistema, se encuentran los "activos", los cuales abarcan varias categorías, como personas, evaluación de riesgos y, en el caso específico que nos ocupa, gestión de activos. Es importante que el creador de un marco de ciberseguridad tenga en cuenta la evolución de las amenazas cibernéticas y la tecnología emergente al diseñar este concepto, para evitar que el marco resulte incompleto ante futuros requisitos (ISO/IEC 27110 , 2021).

A continuación, se presenta una sección de la Tabla 3, en la cual se menciona la Gestión de activos(ISO/IEC 27110 , 2021)

Tabla 3: Ejemplos de categorías y referencias dentro de Identificar

Categoría	Descripción	Referencias
Gestión de activos	Identificación y gestión de los sistemas, datos, dispositivos, personas e instalaciones en relación con el negocio.	ISO/CEI 27002:2013 ISO/IEC 27019:2017, cláusula 7

Como se puede observar, se realiza la identificación de activos que abarcan dispositivos, sistemas físicos, plataformas, aplicaciones de software y sistemas de información externos. Además, dentro de la identificación de recursos, se prioriza la categorización según su criticidad y valor empresarial, incluyendo hardware, dispositivos, software y datos de información. La referencia utilizada para esta subcategoría es la norma ISO/IEC 27002, la cual se enfoca

específicamente en "Seguridad de la información, ciberseguridad y protección de la privacidad: Controles de seguridad de la información" (ISO/IEC, 2022). Como se menciona en la descripción de la subcategoría, la clasificación de los datos se realiza en función de su clasificación, criticidad y valor empresarial.

En el caso del sector salud, es preocupante y relevante la vulnerabilidad ante los ataques cibernéticos, como lo indica el Informe de Ciberseguridad del 2023 elaborado por Check Point, que reporta un aumento del 74% en los ciberataques a este sector entre 2021 y 2022. Estos ataques pueden ser interpretados como intentos de obtener ventajas económicas, especialmente después del incremento de actividades relacionadas con la atención a la pandemia.

Como se ha expuesto en el desarrollo de este trabajo, el sector salud es particularmente susceptible a recibir ciberataques debido a la sensibilidad y el valor de los datos que recopila de los pacientes. Sin embargo, según el informe LATAM CISCO 2023, solo el 40% de las instituciones del sector realiza evaluaciones de seguridad, lo que muestra la necesidad de incrementar las medidas de protección y una buena categorización de activos de información.

Proteger

Este concepto ayuda a las organizaciones a abordar el desarrollo de medidas de seguridad para proteger la identidad informática, garantizar que los controles aplicados preventivos funcionen adecuadamente, lograr una buena preparación según las necesidades de la organización para ofrecer servicios críticos para conservar operaciones y la seguridad de la información de activos. De igual manera engloba diversas categorías y actividades destinadas a resguardar los activos y prevenir su uso indebido, ya sea de forma intencional o no intencional.

Tabla 4: Ejemplos de categorías y referencias dentro de Proteger

Categoría	Descripción	Referencias
Control de acceso	Limitar el acceso a las instalaciones y activos solo a las entidades autorizadas y las actividades asociadas. Incluido en la gestión de acceso está la autenticación de entidad	ISO/IEC 27002:2013, cláusula 9 ISO/IEC 29146 ISO/CEI 29115
Concienciación y formación	Garantizar que los usuarios y las partes interesadas conozcan las políticas, los procedimientos y las responsabilidades relacionadas con las responsabilidades de ciberseguridad.	ISO/IEC 27002:2013, cláusulas 6 y 7
Seguridad de datos	Responsable de la confidencialidad, integridad y disponibilidad de los datos y la información.	ISO/IEC 27002:2013, cláusula 8
Procesos y procedimientos de protección de la información	Las políticas, procesos y procedimientos de seguridad se mantienen y utilizan para gestionar la protección de los sistemas de información.	ISO/CEI 27002:2013
Mantenimiento	Procesos y procedimientos para el mantenimiento y la modernización continuos	ISO/IEC 27002:2013, cláusula 11
Tecnología de protección	Soluciones técnicas de seguridad (como registro, medios extraíbles, principios de acceso mínimo y protección de red)	ISO/CEI 27002:2013 ISO/IEC 27033 (todas las partes)

Las categorías del concepto Proteger se enfocan en la protección, mantenimiento y concienciación de activos, tanto de información como físicos. Es crucial que las organizaciones promuevan y apliquen estas categorías, especialmente considerando que el informe "LATAM CISO" revela que la región latinoamericana experimenta 1.600 ciberataques por segundo en diversas industrias. Asegurar la información y la infraestructura es un desafío complejo, pero es fundamental para las organizaciones de salud encontrar un equilibrio difícil en la gestión de la protección. Al aplicar estas categorías para abordar los incidentes significativos, se brinda una protección mejorada tanto a los pacientes como al sector de la salud en su conjunto.

Con el fin de proporcionar un mayor detalle sobre las categorías observadas en la Tabla 5, se presentan a continuación las subcategorías junto con sus referencias correspondientes, lo cual servirá como apoyo para las organizaciones en el concepto de proteger.

Tabla 5: Concepto de protección: categoría de control de acceso, subcategorías y referencias

Descripción de la subcategoría	Mapeo de estándares
Las identidades y credenciales se administran para dispositivos y usuarios autorizados	ISO/IEC 27002:2013, 9.2.1, 9.2.2, 9.2.4, 9.2.5, 9.2.6, 9.3.1, 9.4.2, 9.4.3 ISO/CEI 27019:2017, 11.1.1, 11.3.1, 11.5.2
El acceso físico y el acceso remoto están gestionados y protegidos	ISO/CEI 27002:2013, 11.1.1, 11.1.2, 6.2.2, 13.1.1
Gestionar permisos de acceso, principio mínimo y separación de funciones	ISO/CEI 27002:2013, 6.1.2, 9.1.2, 9.2.3, 9.4.1, 9.4.4 ISO/CEI 27019:2017, 8.1.1
La integridad de la red está protegida, incluida la segregación de la red según corresponda.	ISO/CEI 27002:2013, 13.1.1, 13.1.3 ISO/CEI 27033-2 ISO/CEI 27033-3 ISO/CEI 27019:2017, 10.6.3, 11.4.5, 11.4.8

La Tabla 5 proporciona información detallada sobre la categoría de control de acceso, incluyendo sus subcategorías y las referencias correspondientes para abordar este tema. Es fundamental destacar la importancia de la categoría de control de acceso, ya que según el director técnico de Bitglass, los piratas informáticos están mejorando constantemente sus habilidades y pueden adaptarse a las medidas de seguridad de autenticación de múltiples factores (Bitglass, 2020). Según el informe de ciberseguridad publicado por el "*BID*" en 2020, se destaca que, más allá de la seguridad operativa de los sistemas y redes, la ciberseguridad juega un rol fundamental y seguirá siendo crucial para garantizar la integridad (BID, OEA, 2020)

Tabla 6: Concepto de protección: categoría, subcategorías y referencias de concientización y capacitación

Descripción de la subcategoría	Mapeo de estándares
Todos los usuarios están informados y capacitados.	ISO/CEI 27002:2013, 7.2.2
Se entienden las funciones y responsabilidades de los altos ejecutivos, los usuarios privilegiados, las partes interesadas, el personal (seguridad física y de la información) y las partes interesadas de terceros (p. ej., proveedores, clientes, socios).	ISO/CEI 27002:2013, 7.2.1, 7.2.2, 6.1.1, 8.2.1

La Tabla 6 se enfoca en la subcategoría de concientización y formación es esencial en todas las organizaciones, ya que se espera que todos los miembros del personal estén informados sobre las amenazas tanto internas como externas que pueden afectar los activos de la organización. En

este sentido, la norma ISO 27002 proporciona los controles necesarios para llevar a cabo una capacitación efectiva del personal. Si bien existe cierta provisión de servicios de seguridad cibernética por parte del sector privado, parece haber una necesidad de mejora en cuanto a la conciencia y la preparación para enfrentar amenazas en este campo.

Tabla 7: Concepto de protección: categoría de seguridad de datos, subcategorías y referencias

Descripción de la subcategoría	Mapeo de estándares
Los datos en reposo están protegidos	ISO/CEI 27002:2013, 8.2.3 ISO/CEI 27033-2 ISO/CEI 27040
Los datos en tránsito están protegidos	ISO/IEC 27002:2013, 8.2.3, 13.1.1, 13.2.1, 13.2.3, 14.1.2, 14.1.3 ISO/CEI 27033-2 ISO/CEI 27033-5
Los activos se gestionan formalmente durante la remoción, transferencia y disposición	ISO/CEI 27002:2013, 8.2.3, 8.3.1, 8.3.2, 8.3.3, 11.2.7
Planificación adecuada de la capacidad para garantizar la disponibilidad	ISO/CEI 27002:2013, 12.1.3, 12.3.1
Protección contra fuga de datos	ISO/IEC 27002:2013, 6.1.2, 7.1.1, 7.1.2, 7.3.1, 8.2.2, 8.2.3, 9.1.1, 9.1.2, 9.2.3, 9.4.1, 9.4.4, 9.4.5, 13.1.3, 13.2.1, 13.2.3, 13.2.4, 14.1.2, 14.1.3
Los mecanismos de verificación de integridad se utilizan para verificar la integridad del software, el firmware y la información.	ISO/CEI 27002:2013, 12.2.1, 12.5.1, 14.1.2, 14.1.3
Los entornos de desarrollo y prueba están separados del entorno de producción.	ISO/CEI 27002:2013, 12.1.4 ISO/CEI 27019:2017, 10.1.4

La Tabla 7 se enfoca en la seguridad de los datos y establece que es importante proteger tanto los datos en reposo como los datos en tránsito. Esto garantiza que la organización cuente siempre con datos íntegros, disponibles y confiables. Asimismo, los activos pueden ser gestionados y puestos a disposición de la organización. La subcategoría de fuga de datos es una preocupación primordial para las organizaciones, por lo tanto, mediante esta subcategoría se puede manejar de manera más efectiva la información de los datos médicos. Para aplicar estas protecciones, es fundamental contar con mecanismos sólidos como software, firmware y otros recursos tecnológicos adecuados.

Tabla 8: Concepto de protección: categoría de procesos y procedimientos de protección de la información, subcategorías y referencias

Descripción de la subcategoría	Mapeo de estándares
Las configuraciones de referencia de los sistemas se crean y mantienen.	ISO/CEI 27002:2013, 12.1.2, 12.5.1, 12.6.2, 14.2.2, 14.2.3, 14.2.4 ISO/CEI 27019:2017, 12.1.1
Se implementa un ciclo de vida de desarrollo de sistemas para administrar sistemas.	ISO/CEI 27002:2013, 6.1.5, 14.1.1, 14.2.1, 14.2.5 ISO/IEC 27034 (todas las partes)
Proceso de control de cambios implementado	ISO/CEI 27002:2013, 12.1.2, 12.5.1
Las copias de seguridad se realizan, mantienen y prueban	ISO/CEI 27002:2013, 12.3.1
El entorno operativo físico cumple con la política y las reglamentaciones para los activos de la organización	ISO/CEI 27002:2013, 11.1.4, 11.2.1, 11.2.2, 11.2.3 ISO/CEI 27019:2017, 9.1.1, 9.1.2, 9.2.3, 9.1.7, 9.1.8, 9.1.9
La destrucción de datos sigue la política apropiada	ISO/CEI 27002:2013 8.2.3, 8.3.1, 8.3.2, 11.2.7
Los procesos de protección se mejoran continuamente	ISO/IEC 27001:2013, cláusulas 9 y 10
La comunicación de la eficacia de las tecnologías de protección se comparte con las partes correspondientes	ISO/CEI 27001:2013, 7.4 ISO/CEI 27002:2013, 16.1.6
Los planes de respuesta y recuperación están implementados, administrados y probados	ISO/CEI 27002:2013, 16.1.1, 17.1.1, 17.1.2 ISO/CEI 27031 ISO/CEI 27035-1 ISO/CEI 27035-2 ISO/CEI 27019:2017 14.1.1
Gestión de vulnerabilidades	ISO/CEI 27002:2013, 12.6.1, 18.2.2

La Tabla 8 detalla los lineamientos para la protección de la información. En Ecuador, se reconoce constitucionalmente la importancia de proteger los datos y la privacidad. Existen leyes y reglamentos relacionados con la protección de datos personales. Es crucial implementar mejoras constantes en estas medidas para asegurar la protección de datos, especialmente en el ámbito médico.

Tabla 9: Concepto de protección: categoría de mantenimiento, subcategorías y referencias

Descripción de la subcategoría	Mapeo de estándares
Los activos de la organización se mantienen y reparan siguiendo procesos y herramientas aprobados	ISO/CEI 27002:2013, 11.1.2, 11.2.4
El mantenimiento remoto se realiza siguiendo procesos aprobados y protegidos de accesos no autorizados.	ISO/CEI 27002:2013, 11.2.4, 15.1.1, 15.2.1

La Tabla 9 presenta dos subcategorías relacionadas con el mantenimiento y reparación de activos de la organización, así como el mantenimiento remoto. Estas subcategorías se alinean con los estándares ISO/CEI 27002:2013, que establecen los procesos y herramientas aprobados para garantizar la integridad y protección de los activos de la organización.

El mantenimiento adecuado de los activos y la realización de mantenimiento remoto de manera segura son aspectos clave en la gestión de la ciberseguridad. Los informes de ciberseguridad han resaltado la importancia de mantener y reparar los activos de manera adecuada para prevenir vulnerabilidades y ataques cibernéticos.

Al seguir los estándares mencionados, las organizaciones pueden asegurar que los procesos de mantenimiento y reparación se llevan a cabo de manera segura y protegida contra accesos no autorizados. Esto contribuye a fortalecer la ciberseguridad de la organización y reducir los riesgos asociados con posibles brechas de seguridad.

Tabla 10: Concepto de protección: categoría de tecnologías de protección, subcategorías y referencias

Descripción de la subcategoría	Mapeo de estándares
Los registros de auditoría/registro se determinan, documentan, implementan y revisan de acuerdo con la política	ISO/CEI 27002:2013, 12.4.1, 12.4.2, 12.4.3, 12.4.4, 12.7.1 ISO/CEI 27019:2017, 10.10.1
Los medios extraíbles siguen la política adecuada	ISO/CEI 27002:2013, 8.2.2, 8.3.1, 8.3.3 ISO/CEI 27040
El principio de mínima funcionalidad se aplica al acceso a sistemas y activos.	ISO/CEI 27002:2013, 9.1.2
Las redes de comunicaciones y control están protegidas	ISO/CEI 27002:2013, 13.1.1, 13.2.1 ISO/CEI 27033-2 ISO/CEI 27019:2017, 10.6.3

La Tabla 10 proporciona una visión clara de las subcategorías y su mapeo a los estándares de ciberseguridad. Estos estándares, como ISO/CEI 27002, ISO/CEI 27019 y ISO/CEI 27040, son fundamentales para establecer políticas y procedimientos que protejan la información y los activos de una organización.

Es importante destacar que la implementación de estos estándares es crucial en un contexto en el que los ciberataques están en constante aumento. Según informes de ciberseguridad, como el "Reporte de Ciberseguridad" mencionado anteriormente, la protección de la información personal y médica es de suma importancia debido al crecimiento de las amenazas cibernéticas.

Al seguir los lineamientos y recomendaciones establecidos en los estándares, las organizaciones pueden fortalecer su postura de seguridad, asegurando registros de auditoría adecuados, protección de medios extraíbles, aplicación del principio de mínima funcionalidad y salvaguarda de las redes de comunicaciones y control. Esto contribuye a la integridad, disponibilidad y confidencialidad de la información, mejorando la protección de los datos médicos y reduciendo el riesgo de posibles brechas de seguridad.

Detectar

El concepto de detección implica la implementación de actividades apropiadas para identificar eventos de seguridad cibernética. Este enfoque proporciona la capacidad de detectar de manera proactiva cambios en el comportamiento, estado, tráfico, configuración o procesamiento de los recursos. Además, este concepto abarca el monitoreo tradicional de activos. (ISO/IEC 27110 , 2021)

Tabla 11: Concepto de detección: categoría de anomalías y eventos, subcategorías y referencias

Descripción de la subcategoría	Mapeo de estándares
Se establece la línea de base de las operaciones de red y los flujos de datos.	ISO/IEC 27033 (todas las partes)
Los datos de eventos se agregan y correlacionan desde múltiples fuentes y sensores	ISO/IEC 27035 (todas las partes)

La Tabla 11 presenta dos subcategorías relevantes en el contexto de la protección de datos médicos dentro del concepto de detectar. Estas subcategorías son clave para garantizar la seguridad y confidencialidad de la información sensible de los pacientes en el ámbito de la salud.

Establecer la línea de base de las operaciones de red y los flujos de datos permite a las organizaciones detectar de manera proactiva cualquier actividad anormal o no autorizada que pueda comprometer la integridad de los datos médicos. Por otro lado, la agregación y correlación de datos de eventos provenientes de múltiples fuentes y sensores brinda una visión holística de posibles amenazas y actividades maliciosas que podrían afectar la seguridad de los datos médicos.

La protección de los datos médicos es de vital importancia debido a su carácter sensible y confidencial. Los informes de ciberseguridad destacan constantemente la necesidad de fortalecer las medidas de protección y detección en el sector de la salud, ya que los datos médicos son un objetivo atractivo para los ciberdelincuentes.

Responder

La respuesta ante las amenazas que afectan a una organización implica reconocer y gestionar los riesgos que pueden afectar sus activos. Si bien no se categorizan específicamente a los activos dentro de este concepto, es fundamental que las organizaciones adopten las medidas preventivas necesarias dentro del ecosistema cibernético.

Esto implica la adopción de medidas cautelares, como controles de seguridad, evaluaciones de riesgos y una sólida gestión de la seguridad de la información.

Tabla 12: Ejemplos de categorías y referencias dentro de Responder

Categoría	Descripción	Referencias
Planificación de la respuesta	Planifique cómo responder a los eventos de manera oportuna, incluidos los procesos y procedimientos para responder a los eventos.	ISO/IEC 27002:2013, cláusula 16 ISO/ IEC 27035 (todas las partes)
Comunicaciones	Procesos y procedimientos para comunicar la información oportuna a las partes relevantes. Las empresas deben comunicarse adecuadamente con las partes relevantes, por ejemplo, divulgando información sobre medidas de seguridad o respuesta de forma regular o en momentos de emergencia.	ISO/IEC 27002:2013, cláusula 16 ISO/IEC 27035 (todas las partes) ISO/IEC 27014
Análisis	Revisión de eventos detectados, incluida la categorización y el impacto de los eventos.	ISO/IEC 27002:2013, cláusula 16 ISO/ IEC 27035 (todas las partes)
Mitigación	Actividades que limitan la expansión del evento, mitigan el evento y detienen el evento.	ISO/IEC 27002:2013, cláusula 16 ISO/ IEC 27035 (todas las partes)
Mejoras	La organización revisa el plan de respuesta y lo mejora en función de las lecciones aprendidas durante un evento.	ISO/IEC 27002:2013, cláusula 16 ISO/ IEC 27035 (todas las partes)

La Tabla 12 se desarrollará en mayor detalle en el contexto del Riesgo Externo, que forma parte de la segunda fase de este trabajo de titulación.

Recuperar

El concepto “Recuperar” proporciona a la organización las directrices necesarias para lograr una adecuada restauración de servicios. Estos servicios pueden incluir tanto procesos técnicos como de gestión. En el contexto de los activos, puede darse la situación en la que su funcionamiento se vea afectado y no se encuentre en un estado operativo o deseado. Por lo tanto, este concepto brinda la oportunidad de ofrecer orientación sobre cómo reparar dichos activos.

Tabla 13: Ejemplos de categorías y referencias dentro de Recuperar

Categoría	Descripción	Referencias
Planificación de la recuperación	Planifique cómo recuperarse de un evento y los próximos pasos después de un evento.	ISO/IEC 27002:2013, cláusula 16 ISO/ IEC 27035 (todas las partes)
Comunicaciones	Procesos y procedimientos para comunicar la información oportuna a las partes relevantes.	ISO/IEC 27002:2013, cláusula 16 ISO/ IEC 27035 (todas las partes)
Mejoras	La organización toma las lecciones aprendidas durante un evento y las retroalimenta al proceso y los procedimientos.	ISO/IEC 27002:2013, cláusula 16 ISO/ IEC 27035 (todas las partes)

La Tabla 13 proporciona categorías y referencias relevantes dentro del concepto de recuperación. En el contexto de los datos médicos, es fundamental planificar la recuperación después de un evento y establecer procesos de comunicación efectivos para mantener informadas a las partes relevantes. Además, la mejora constante basada en las lecciones aprendidas es esencial para fortalecer la capacidad de recuperación y minimizar el impacto en los datos médicos. Al seguir estas pautas y utilizar los estándares y referencias recomendados, las organizaciones del sector de la salud pueden mejorar su capacidad de respuesta y mantener la integridad de los datos médicos.

El informe de LATAM CISCO destaca la importancia de la resiliencia para las organizaciones, ya que esta les brinda la capacidad de recuperarse de los ataques o reducir el impacto que pueden causar. Además, se enfatiza que las organizaciones no deben depender exclusivamente de la prevención, sino que deben fortalecer su capacidad de recuperación para minimizar los efectos negativos en las operaciones y salvaguardar la confidencialidad de los datos médicos. (Hoffman, y otros, 2023)

Riesgo Externo

La amenaza externa se refiere al riesgo de que una persona que no mantiene relación con la organización obtenga acceso no autorizado a información confidencial mediante una serie de explotación de vulnerabilidades.

Las amenazas internas provienen en gran medida de los empleados actuales y anteriores de una organización, que, de manera intencional o accidental, pueden abusar de sus permisos de acceso para llevar a cabo ataques maliciosos.

A partir de los mismos conceptos explicados anteriormente y siguiendo la documentación de la norma ISO 27110, se llevará a cabo un análisis de los riesgos externos que pueden afectar a una organización, en este caso, dentro del sector de la salud.

Es fundamental que los marcos cibernéticos se enfoquen en prioridades claras, sea flexible, repetible y rentable, para ayudar a los usuarios finales a gestionar eficazmente el riesgo.

El diseño de un marco de ciberseguridad basado en la norma ISO 27110, en las organizaciones del sector de la salud podrán fortalecer la capacidad para enfrentar los riesgos externos en el ámbito de la ciberseguridad. Esto permite gestionar de manera efectiva los riesgos, adoptando enfoques adecuados y aplicando las mejores prácticas establecidas en la norma. Además, el sector de la salud puede gestionar de manera proactiva y efectiva los riesgos relacionados con la ciberseguridad. (ISO/IEC 27110 , 2021)

Identificar

Dentro del concepto de Identificar en el ecosistema de ciberseguridad, se analizan los riesgos cibernéticos, el entorno de amenazas y las partes interesadas relevantes. En este sentido,

se abordan aspectos como las políticas, los procesos y la tecnología que se definen dentro del alcance de las actividades de la organización. Es a través de este alcance que se pueden incluir la evaluación de riesgos, la estrategia de gestión de riesgos, la gobernanza y otros elementos relacionados.

Sergio Navarro Barreiros, Jefe de Seguridad Informática (CISO), comenta que es crucial que el sector salud reconozca que el riesgo va en aumento y también la probabilidad de impacto que pueden recaer en los sistemas, entre estos se encuentran la interrupción de servicios vitales y posibles daños personales y patrimoniales a los usuarios. Además, dado que el sector es interdependiente con otros, los incidentes se ciberseguridad pueden tener repercusiones en cascada (Redacción, 2023).

Una adecuada identificación de riesgos reduce la probabilidad de que una amenaza afecte los activos de información. Es importante identificar las amenazas que puedan aprovechar las vulnerabilidades o insuficiencias de dichos activos. Al realizar un análisis de riesgos coherente y preciso, se logra identificar de manera efectiva los elementos de información que requieren protección. Esto nos permite observar la relación entre los distintos elementos y sus debilidades, lo que a su vez nos permite determinar los posibles riesgos y llevar a cabo una evaluación exhaustiva.

La evaluación de riesgos establece y mantiene criterios para la seguridad de los datos. Esto implica la aceptación del riesgo y la realización de evaluaciones confiables, comparables y consistentes. Además, se debe identificar a los responsables de la gestión de riesgos en el entorno empresarial. El análisis de riesgos considera las consecuencias de la materialización de un riesgo y la probabilidad de que afecte un activo. La organización debe priorizar los riesgos para su tratamiento adecuado.

A continuación, se muestra el desglose por subcategoría de la Tabla 14, lo cual proporciona una comprensión más sintetizada del proceso que se debe seguir en la evaluación y gestión de riesgos. En las Tablas siguientes se detallan de manera más precisa los pasos y actividades relacionados con este proceso.

Tabla 14: Ejemplos de categorías y referencias dentro de Identificar

Categoría	Descripción	Referencias
Ambiente de negocios	Los objetivos, las partes interesadas y las actividades de la organización se entienden y utilizan para informar los roles, las responsabilidades y las decisiones de gestión de riesgos. Son necesarias medidas de seguridad integrales que abarquen a la propia empresa, a las empresas de su grupo, a los socios comerciales de su cadena de suministro y a las empresas de externalización de control de sistemas de TI.	ISO/IEC 27001:2013, cláusula 4 ISO/IEC 27001:2013, cláusula 5 ISO/IEC 27036 (todas las partes)
Evaluación de riesgos	La organización comprende los riesgos para las operaciones y los activos de la organización. Se requiere que la gerencia impulse medidas de riesgo de ciberseguridad considerando cualquier posible riesgo mientras se procede con la utilización de TI.	ISO/IEC 27001:2013, cláusula 6 ISO/IEC 27014
Estrategia de gestión de riesgos	El enfoque de una organización, los componentes de gestión y los recursos que se aplicarán a la gestión del riesgo.	ISO/CEI 27001:2013, 9.3
Gobernancia	Supervisar y gestionar los requisitos normativos, legales, ambientales y operativos de la organización. Esta información se utiliza luego para informar a los niveles apropiados de gestión.	ISO/IEC 27002:2013, cláusula 5 ISO/IEC 27002:2013, cláusula 6
Gestión de activos	Identificación y gestión de los sistemas, datos, dispositivos, personas e instalaciones en relación con el negocio.	ISO/CEI 27002:2013 ISO/IEC 27019:2017, cláusula 7

Tabla 15: Identificar el concepto: categoría de evaluación de riesgos, subcategorías y referencias

Descripción de la subcategoría	Mapeo de estándares
Las vulnerabilidades de los activos se identifican y documentan	ISO/CEI 27002:2013, 12.6.1, 18.2.3 ISO/CEI 29147 ISO/CEI 27019:2017, 7.1.1, 7.1.2
La información sobre amenazas y vulnerabilidades se recibe de foros y fuentes de intercambio de información.	ISO/CEI 27002:2013, 6.1.4
Las amenazas internas y externas se identifican y documentan	ISO/CEI 27001:2013, 6.1.2
Se identifican los posibles impactos comerciales y las probabilidades.	ISO/CEI 27001:2013, 6.1.2
Las amenazas, vulnerabilidades, probabilidades e impactos se utilizan para determinar el riesgo	ISO/CEI 27002:2013, 12.6.1
Las respuestas a los riesgos se identifican y priorizan	ISO/CEI 27001:2013, 6.1.3

Tabla 16: Identificar concepto: categoría de estrategia de gestión de riesgos, subcategorías y referencias

Descripción de la subcategoría	Mapeo de estándares
Los procesos de gestión de riesgos son establecidos, gestionados y acordados por las partes interesadas de la organización	ISO/CEI 27001:2013, 6.1.3, 8.3, 9.3
La tolerancia al riesgo organizacional está determinada y claramente expresada	ISO/CEI 27001:2013, 6.1.3, 8.3
La determinación de la tolerancia al riesgo de la organización se basa en su función en la infraestructura crítica y el análisis de riesgos específicos del sector.	ISO/CEI 27001:2013, 6.1.3, 8.3

Tabla 17: Identificar el concepto: categoría de gobernanza, subcategorías y referencias

Descripción de la subcategoría	Mapeo de estándares
Se establece la política de seguridad de la información para la organización.	ISO/CEI 27002:2013, 5.1.1
Las funciones y responsabilidades de seguridad de la información están coordinadas y alineadas con funciones internas y socios externos	ISO/CEI 27002:2013, 6.1.1, 7.2.1
Los requisitos legales y reglamentarios relacionados con la ciberseguridad, incluidas las obligaciones de privacidad y libertades civiles, se entienden y gestionan.	ISO/CEI 27002:2013, 18.1
Los procesos de gobernanza y gestión de riesgos abordan los riesgos de ciberseguridad	ISO/IEC 27001:2013, cláusula 6

Proteger

Al igual que en el concepto de proteger, donde se aborda la protección de activos de información, la Tabla 18 presenta controles, medidas de seguridad, mantenimiento y protección que una organización debe implementar para minimizar los riesgos. Sin embargo, en esta sección

se hace referencia específica a los riesgos externos. Por lo tanto, las categorías presentadas deben ser aplicadas de manera diferente y con un enfoque distinto.

Tabla 18: Ejemplos de categorías y referencias dentro de Proteger

Categoría	Descripción	Referencias
Control de acceso	Limitar el acceso a las instalaciones y activos solo a las entidades autorizadas y las actividades asociadas. Incluido en la gestión de acceso está la autenticación de entidad	ISO/IEC 27002:2013, cláusula 9 ISO/IEC 29146 ISO/CEI 29115
Concienciación y formación	Garantizar que los usuarios y las partes interesadas conozcan las políticas, los procedimientos y las responsabilidades relacionadas con las responsabilidades de ciberseguridad.	ISO/IEC 27002:2013, cláusulas 6 y 7
Seguridad de datos	Responsable de la confidencialidad, integridad y disponibilidad de los datos y la información.	ISO/IEC 27002:2013, cláusula 8
Procesos y procedimientos de protección de la información	Las políticas, procesos y procedimientos de seguridad se mantienen y utilizan para gestionar la protección de los sistemas de información.	ISO/CEI 27002:2013
Mantenimiento	Procesos y procedimientos para el mantenimiento y la modernización continuos	ISO/IEC 27002:2013, cláusula 11
Tecnología de protección	Soluciones técnicas de seguridad (como registro, medios extraíbles, principios de acceso mínimo y protección de red)	ISO/CEI 27002:2013 ISO/IEC 27033 (todas las partes)

Es importante considerar que los riesgos externos son originados por individuos o entidades que no tienen relación directa con la organización. Estos atacantes aprovechan vulnerabilidades en el sistema para llevar a cabo sus acciones. En este contexto, es fundamental aplicar las categorías establecidas con el fin de mitigar en gran medida estos riesgos externos.

En las siguientes Tablas se presentan las subcategorías de la Tabla 18. Estas descripciones se deben basar en los riesgos externos que puede sufrir una organización. Por lo tanto, dentro de las Tablas solamente se seleccionan aquellas subcategorías que van de acuerdo con el tratamiento de riesgos y su protección.

La Tabla 19 da una explicación breve de los controles de acceso que se deben de aplicar para una mejor integridad, confidencialidad y disponibilidad de la información.

Tabla 19: Concepto de protección: categoría de control de acceso, subcategorías y referencias

Descripción de la subcategoría	Mapeo de estándares
Las identidades y credenciales se administran para dispositivos y usuarios autorizados	ISO/IEC 27002:2013, 9.2.1, 9.2.2, 9.2.4, 9.2.5, 9.2.6, 9.3.1, 9.4.2, 9.4.3 ISO/CEI 27019:2017, 11.1.1, 11.3.1, 11.5.2
El acceso físico y el acceso remoto están gestionados y protegidos	ISO/CEI 27002:2013, 11.1.1, 11.1.2, 6.2.2, 13.1.1
Gestionar permisos de acceso, principio mínimo y separación de funciones	ISO/CEI 27002:2013, 6.1.2, 9.1.2, 9.2.3, 9.4.1, 9.4.4 ISO/CEI 27019:2017, 8.1.1
La integridad de la red está protegida, incluida la segregación de la red según corresponda.	ISO/CEI 27002:2013, 13.1.1, 13.1.3 ISO/CEI 27033-2 ISO/CEI 27033-3 ISO/CEI 27019:2017, 10.6.3, 11.4.5, 11.4.8

La Tabla 20, es importante por que como menciona el informe LATAM CISO 2023, se debe practicar la higiene de ciberseguridad básica, la creación de una arquitectura resistente; la capacidad de supervisar y mantener un seguimiento constante de la red de infraestructura crítica; el establecimiento de un acceso remoto seguro y un programa de gestión de vulnerabilidades basado en la evaluación de riesgos.

De acuerdo con esta subcategoría, las organizaciones, especialmente aquellas en el sector de la salud que manejan información sensible, deben anticiparse a la evolución del ciberdelito hacia la guerra cibernética y estar preparadas en caso de que esta situación se intensifique.

Por último, es importante adoptar un enfoque integral en la gestión de TI y entornos críticos, así como implementar una arquitectura basada en el principio de "confianza cero", que asegure que el acceso a la información se limite únicamente a las personas autorizadas en el momento y lugar adecuados.(Hoffman, y otros, 2023)

Tabla 20: Concepto de protección: categoría, subcategorías y referencias de concientización y capacitación

Descripción de la subcategoría	Mapeo de estándares
Todos los usuarios están informados y capacitados.	ISO/CEI 27002:2013, 7.2.2
Se entienden las funciones y responsabilidades de los altos ejecutivos, los usuarios privilegiados, las partes interesadas, el personal (seguridad física y de la información) y las partes interesadas de terceros (p. ej., proveedores, clientes, socios).	ISO/CEI 27002:2013, 7.2.1, 7.2.2, 6.1.1, 8.2.1

En la Tabla 21, se destacan las subcategorías relacionadas con la "Seguridad de datos". La protección contra la fuga de datos es especialmente relevante en el contexto de la salud, como se menciona en el informe elaborado por el BID titulado "*Protegiendo la Salud Digital - Una guía de ciberseguridad en el sector salud*". Según este informe, en el año 2020 se registró un aumento del 55% en las fugas de datos en el sector salud, y el 67% de estas fugas fue resultado de ataques cibernéticos (BID, y otros, 2021). Por lo tanto, es crucial contar con mecanismos de verificación adecuados para prevenir y detectar estos incidentes. La encuesta de ciberseguridad realizada por HIMSS en el año 2020 respalda la importancia de contar con medidas de seguridad efectivas. Aunque la implementación de firewalls empresariales, programas antivirus y plataformas EDR puede representar un costo, estas medidas son fundamentales para prevenir incidentes graves de seguridad. Por lo tanto, invertir en estas medidas de seguridad resulta una decisión prudente que puede generar ahorros significativos a largo plazo. (HIMSS, 2020)

Tabla 21: Concepto de protección: categoría de seguridad de datos, subcategorías y referencias

Descripción de la subcategoría	Mapeo de estándares
Protección contra fuga de datos	ISO/IEC 27002:2013, 6.1.2, 7.1.1, 7.1.2, 7.3.1, 8.2.2, 8.2.3, 9.1.1, 9.1.2, 9.2.3, 9.4.1, 9.4.4, 9.4.5, 13.1.3, 13.2.1, 13.2.3, 13.2.4, 14.1.2, 14.1.3
Los mecanismos de verificación de integridad se utilizan para verificar la integridad del software, el firmware y la información.	ISO/CEI 27002:2013, 12.2.1, 12.5.1, 14.1.2, 14.1.3
Los entornos de desarrollo y prueba están separados del entorno de producción.	ISO/CEI 27002:2013, 12.1.4 ISO/CEI 27019:2017, 10.1.4

La Tabla 22, abarca los procesos que las organizaciones deben seguir para garantizar la protección de la información, haciendo hincapié en el resguardo frente a ataques externos. Las subcategorías establecen configuraciones que, si se llevan a cabo de manera periódica, pueden prevenir o mitigar incidentes, ya que el control periódico y el mantenimiento son fundamentales para garantizar un correcto funcionamiento de estas categorías.

Como destaca el informe del *HIMSS* basado en su encuesta realizada en el año 2020, muchas organizaciones del área de salud que han sido víctimas de ataques han tenido que invertir grandes sumas de dinero en la restauración de datos a partir de copias de seguridad. Se subraya la importancia de implementar medidas efectivas de protección y realizar copias de seguridad regularmente para asegurar la disponibilidad y la integridad de la información ante posibles incidentes de seguridad. (HIMSS, 2020)

Tabla 22: Concepto de protección: categoría de procesos y procedimientos de protección de la información, subcategorías y referencias

Descripción de la subcategoría	Mapeo de estándares
Las configuraciones de referencia de los sistemas se crean y mantienen.	ISO/CEI 27002:2013, 12.1.2, 12.5.1, 12.6.2, 14.2.2, 14.2.3, 14.2.4 ISO/CEI 27019:2017, 12.1.1
Se implementa un ciclo de vida de desarrollo de sistemas para administrar sistemas.	ISO/CEI 27002:2013, 6.1.5, 14.1.1, 14.2.1, 14.2.5 ISO/IEC 27034 (todas las partes)
Proceso de control de cambios implementado	ISO/CEI 27002:2013, 12.1.2, 12.5.1
Las copias de seguridad se realizan, mantienen y prueban	ISO/CEI 27002:2013, 12.3.1
El entorno operativo físico cumple con la política y las reglamentaciones para los activos de la organización	ISO/CEI 27002:2013, 11.1.4, 11.2.1, 11.2.2, 11.2.3 ISO/CEI 27019:2017, 9.1.1, 9.1.2, 9.2.3, 9.1.7, 9.1.8, 9.1.9
La destrucción de datos sigue la política apropiada	ISO/CEI 27002:2013 8.2.3, 8.3.1, 8.3.2, 11.2.7
Los procesos de protección se mejoran continuamente	ISO/IEC 27001:2013, cláusulas 9 y 10
La comunicación de la eficacia de las tecnologías de protección se comparte con las partes correspondientes	ISO/CEI 27001:2013, 7.4 ISO/CEI 27002:2013, 16.1.6
Los planes de respuesta y recuperación están implementados, administrados y probados	ISO/CEI 27002:2013, 16.1.1, 17.1.1, 17.1.2 ISO/CEI 27031 ISO/CEI 27035-1 ISO/CEI 27035-2 ISO/CEI 27019:2017 14.1.1
Gestión de vulnerabilidades	ISO/CEI 27002:2013, 12.6.1, 18.2.2

Las Tablas 22, 23 y 24 están relacionadas con la implementación de principios fundamentales para garantizar una sólida gestión de ciberseguridad en una organización. Es crucial contar con una documentación clara y detallada sobre las políticas y procedimientos que deben seguirse, ya que esto facilita abordar cualquier problema relacionado con el personal y también demuestra a los clientes que su información está segura y protegida. Para las organizaciones del sector de atención médica, es fundamental adoptar y aplicar controles de seguridad de última generación, como plataformas robustas de detección y respuesta de puntos finales, puertas de enlace web seguras, herramientas de prevención de pérdida de datos, soluciones de gestión de vulnerabilidades y parches, y puertas de enlace de seguridad de correo electrónico. Las técnicas utilizadas por los actores maliciosos son cada vez más complejas y sutiles, por lo que es necesario implementar medidas avanzadas de seguridad. Reducir la superficie de ataque es crucial para dificultar la infiltración de estos actores amenazantes en las organizaciones. (HIMSS, 2020)

Tabla 23: Concepto de protección: categoría de mantenimiento, subcategorías y referencias

Descripción de la subcategoría	Mapeo de estándares
Los activos de la organización se mantienen y reparan siguiendo procesos y herramientas aprobados	ISO/CEI 27002:2013, 11.1.2, 11.2.4
El mantenimiento remoto se realiza siguiendo procesos aprobados y protegidos de accesos no autorizados.	ISO/CEI 27002:2013, 11.2.4, 15.1.1, 15.2.1

Tabla 24: Concepto de protección: categoría de tecnologías de protección, subcategorías y referencias

Descripción de la subcategoría	Mapeo de estándares
Los registros de auditoría/registro se determinan, documentan, implementan y revisan de acuerdo con la política	ISO/CEI 27002:2013, 12.4.1, 12.4.2, 12.4.3, 12.4.4, 12.7.1 ISO/CEI 27019:2017, 10.10.1
Los medios extraíbles siguen la política adecuada	ISO/CEI 27002:2013, 8.2.2, 8.3.1, 8.3.3 ISO/CEI 27040
El principio de mínima funcionalidad se aplica al acceso a sistemas y activos.	ISO/CEI 27002:2013, 9.1.2
Las redes de comunicaciones y control están protegidas	ISO/CEI 27002:2013, 13.1.1, 13.2.1 ISO/CEI 27033-2 ISO/CEI 27019:2017, 10.6.3

Detectar

Este concepto se encarga de identificar eventos inusuales. Estos eventos pueden incluir la detección de riesgos tanto internos como externos, ya sean intencionales o no intencionales. Es importante tener en cuenta que el panorama de ataques cibernéticos está en constante evolución, lo que requiere la adaptación continua de políticas para mitigar estas situaciones. Ampliar el alcance de este concepto agrega valor a un marco de ciberseguridad más completo y efectivo.

Tabla 25: Categorías de ejemplo y referencia dentro de Detectar

Categoría	Descripción	Referencias
anomalías y eventos	Detección de anomalías y eventos y comprensión del impacto de esos eventos.	ISO/IEC 27002:2013, cláusula 16 ISO/ IEC 27035 (todas las partes)
Monitoreo continuo de seguridad	Los sistemas se monitorean regularmente para validar la efectividad de las medidas de seguridad implementadas.	ISO/IEC 27002:2013, cláusula 12
Proceso de detección	Procesos y procedimientos para asegurar el conocimiento y comunicación oportunos de los eventos.	ISO/IEC 27002:2013, cláusula 16 ISO/ IEC 27035 (todas las partes)

Aunque los datos de información médica no sean tangibles, su pérdida, filtración o robo pueden tener consecuencias negativas significativas. Por lo tanto, es fundamental abordar y analizar los eventos detectados relacionados con estos datos, tal como se describe en la subcategoría. Además, es necesario tomar medidas para mitigar el impacto, ya que esto es especialmente importante para las organizaciones de atención médica en términos de atención al paciente y seguridad del paciente (HIMSS, 2020)

Tabla 26: Concepto de detección: categoría de anomalías y eventos, subcategorías y referencias

Descripción de la subcategoría	Mapeo de estándares
Se establece la línea de base de las operaciones de red y los flujos de datos.	ISO/IEC 27033 (todas las partes)
Los eventos detectados se analizan para comprender los objetivos y métodos de ataque.	ISO/IEC 27002:2013, 16.1.1, 16.1.4 ISO/ IEC 27035 (todas las partes)
Los datos de eventos se agregan y correlacionan desde múltiples fuentes y sensores	ISO/IEC 27035 (todas las partes)
Determinación del impacto del evento	ISO/IEC 27035 (todas las partes)
Se establecen umbrales de alerta	ISO/IEC 27035 (todas las partes)

Tabla 27: Concepto de detección: categoría de monitoreo continuo de seguridad, subcategorías y

Descripción de la subcategoría	Mapeo de estándares
Supervisión de la red, el entorno físico, el personal y el proveedor de servicios para eventos potenciales	ISO/CEI 27002:2013, 12.4.1, 14.2.7, 15.2.1
Se detecta código malicioso	ISO/CEI 27002:2013, 12.2.1 ISO/CEI 27019:2017, 10.4.1
Se detecta código móvil no autorizado	ISO/CEI 27002:2013, 12.5.1
Se realiza el monitoreo de personal, conexiones, dispositivos y software no autorizados.	ISO/CEI 27002:2013, 12.4.1, 14.2.7, 15.2.1
La actividad del proveedor de servicios externo se monitorea para detectar posibles eventos de ciberseguridad	ISO/IEC 27036 (todas las partes)
Se realizan escaneos de vulnerabilidad	ISO/CEI 27002:2013, 14.2.9

Tabla 28: Concepto de detección: categoría de procesos de detección, subcategorías y referencias

Descripción de la subcategoría	Mapeo de estándares
Los roles y responsabilidades para la detección están bien definidos para garantizar la rendición de cuentas.	ISO/IEC 27002:2013, 6.1.1 ISO/IEC 27019:2017, 8.1.1
Las actividades de detección cumplen con todos los requisitos aplicables	ISO/CEI 27002:2013, 18.1.4
Los procesos de detección se prueban	ISO/CEI 27002:2013, 14.2.8
La información de detección de eventos se comunica a las partes correspondientes	ISO/IEC 27002:2013, 16.1.2 ISO/ IEC 27035 (todas las partes)
Los procesos de detección se mejoran continuamente	ISO/IEC 27002:2013, 16.1.6 ISO/ IEC 27035 (todas las partes)

Responder

El concepto de Responder brinda a las organizaciones la capacidad de evaluar y abordar los eventos de ciberseguridad de manera efectiva. A través de actividades como la categorización, evaluación y remediación, se puede responder adecuadamente a los eventos imprevistos teniendo en cuenta las necesidades, los recursos, las partes interesadas y los requisitos específicos.

Se debe considerar una respuesta a incidentes, interna y externa, estas respuestas pueden ser a partir de divulgaciones de vulnerabilidades, informes u otras fuentes.

La Tabla 29, proporciona directrices sobre las comunicaciones que las organizaciones deben implementar para una respuesta adecuada, efectiva y precisa ante eventos maliciosos. Es

esencial generar comunicaciones pertinentes y oportunas a todas las partes involucradas con el fin de mejorar los tiempos de respuesta.

Tabla 29: Ejemplos de categorías y referencias dentro de Responder

Categoría	Descripción	Referencias
Planificación de la respuesta	Planifique cómo responder a los eventos de manera oportuna, incluidos los procesos y procedimientos para responder a los eventos.	ISO/IEC 27002:2013, cláusula 16 ISO/ IEC 27035 (todas las partes)
Comunicaciones	Procesos y procedimientos para comunicar la información oportuna a las partes relevantes. Las empresas deben comunicarse adecuadamente con las partes relevantes, por ejemplo, divulgando información sobre medidas de seguridad o respuesta de forma regular o en momentos de emergencia.	ISO/IEC 27002:2013, cláusula 16 ISO/IEC 27035 (todas las partes) ISO/IEC 27014
Análisis	Revisión de eventos detectados, incluida la categorización y el impacto de los eventos.	ISO/IEC 27002:2013, cláusula 16 ISO/ IEC 27035 (todas las partes)
Mitigación	Actividades que limitan la expansión del evento, mitigan el evento y detienen el evento.	ISO/IEC 27002:2013, cláusula 16 ISO/ IEC 27035 (todas las partes)
Mejoras	La organización revisa el plan de respuesta y lo mejora en función de las lecciones aprendidas durante un evento.	ISO/IEC 27002:2013, cláusula 16 ISO/ IEC 27035 (todas las partes)

Con el fin de mejorar la planificación de respuesta ante eventos maliciosos, en la Tabla 30, se detalla que los planes deben ejecutarse en todo el ciclo de vida del evento desde el momento de su detección.

Tabla 30: Concepto de respuesta: categoría de planificación de respuesta, subcategorías y referencias

Descripción de la subcategoría	Mapeo de estándares
El plan de respuesta se ejecuta durante o después de un evento	ISO/IEC 27002:2013, 16.1.5 ISO/ IEC 27035 (todas las partes)

La Tabla 31, aborda la importancia de la comunicación dentro de la empresa y hacia todas sus partes relevantes. En la gestión de riesgos, es fundamental que los responsables tengan la capacidad de responder y comunicar de manera efectiva los eventos que ocurren en sus respectivas áreas.

Tabla 31: Concepto de respuesta: categoría de comunicaciones, subcategorías y referencias

Descripción de la subcategoría	Mapeo de estándares
Se investigan las notificaciones de los sistemas de detección	ISO/CEI 27002:2013, 12.4.1, 12.4.3, 16.1.5 ISO/CEI 27039
Se entiende el impacto del incidente.	ISO/CEI 27002:2013, 16.1.6 ISO/CEI 27035-2
Se realizan pericias forenses	ISO/CEI 27002:2013, 16.1.7
Los incidentes se clasifican de acuerdo con los planes de respuesta	ISO/CEI 27002:2013, 16.1.4
Los eventos se informan de acuerdo con los criterios establecidos.	ISO/IEC 27001:2013, 7.4 ISO/IEC 27002:2013, 6.1.3, 16.1.2 ISO/IEC 27035 (todas las partes)
La información se comparte de acuerdo con los planes de respuesta.	ISO/IEC 27001:2013, 7.4 ISO/IEC 27002:2013, 16.1.2 ISO/IEC 27035 (todas las partes)
La coordinación con las partes interesadas ocurre de acuerdo con los planes de respuesta	ISO/IEC 27001:2013, 7.4 ISO/IEC 27002:2013, 6.1.4, 16.1.5 ISO/IEC 27033-2 ISO/IEC 27035 (todas las partes) ISO/IEC 27019:2017, 6.1.7
El intercambio voluntario de información ocurre con las partes interesadas externas para lograr una mayor conciencia de la situación de ciberseguridad.	ISO/CEI 27001:2013, 7.4

La Tabla 32, proporciona un análisis basado en la clasificación del impacto de los incidentes, lo cual permite generar investigaciones forenses que ayudan a clasificar los riesgos en función de los planes de respuesta existentes dentro de la organización.

Tabla 32: Concepto de respuesta: categoría de análisis, subcategorías y referencias

Descripción de la subcategoría	Mapeo de estándares
Se investigan las notificaciones de los sistemas de detección	ISO/CEI 27002:2013, 12.4.1, 12.4.3, 16.1.5 ISO/CEI 27039
Se entiende el impacto del incidente.	ISO/CEI 27002:2013, 16.1.6 ISO/CEI 27035-2
Se realizan pericias forenses	ISO/CEI 27002:2013, 16.1.7
Los incidentes se clasifican de acuerdo con los planes de respuesta	ISO/CEI 27002:2013, 16.1.4

Las Tablas 33 y 34 permiten categorizar los riesgos identificados, lo que a su vez facilita su contención y mitigación, además de documentar estas vulnerabilidades y aceptarlas dentro de la organización. La aceptación se realiza para establecer un plan de respuesta que permita abordar los riesgos de manera ordenada y eficiente. Estos planes de respuesta brindan a los colaboradores

la experiencia necesaria para enfrentar estas situaciones, y el ciclo se completa cuando se actualizan las estrategias en la documentación correspondiente.

Tabla 33: — Concepto de respuesta: categoría de mitigación, subcategorías y referencias

Descripción de la subcategoría	Mapeo de estándares
Los incidentes son contenidos y mitigados	ISO/CEI 27002:2013, 12.2.1, 16.1.5 ISO/CEI 27035-1 ISO/CEI 27035-2
Las vulnerabilidades recién identificadas se mitigan o documentan como aceptadas	ISO/CEI 27002:2013, 12.6.1

Tabla 34: Concepto de respuesta: categoría de mejoras, subcategorías y referencias

Descripción de la subcategoría	Mapeo de estándares
Los planes de respuesta incorporan lecciones aprendidas	ISO/IEC 27001:2013, cláusula 10 ISO/ IEC 27002:2013, 16.1.5, 16.1.6
Las estrategias de respuesta se actualizan	ISO/IEC 27001:2013, cláusula 10 ISO/IEC 27002:2013, 16.1.6

Recuperar

El concepto recuperar se encarga de llevar a cabo las acciones necesarias para restablecer los servicios, reparar los sistemas y recuperar la reputación de la organización. Las actividades incluidas abarcan la restauración y la comunicación posterior a un evento de ciberseguridad. Además, no se limita a ser reactivo, sino que también adopta un enfoque proactivo. Mediante una planificación y ejecución eficiente de las actividades de recuperación, se busca minimizar los daños y ayudar a las organizaciones a retomar sus operaciones de manera efectiva.

Es crucial mencionar la importancia de “Recuperar”, ya que la reputación de una organización puede haber sido afectada durante un incidente cibernético. Es crucial tener en cuenta este aspecto, ya que es esencial para preservar la posición en el mercado y la confianza de los clientes. (ISO/IEC 27110 , 2021).

La Tabla 35, aborda la temática de la recuperación en situaciones de eventos adversos y presenta descripciones similares a las que se encuentran en la Tabla 29. Sin embargo, en este caso se enfoca en cómo se gestionarán las mejoras para lograr una recuperación efectiva ante posibles ataques. Es fundamental considerar y comunicar las estrategias y acciones que se implementarán para asegurar una recuperación exitosa en caso de incidentes.

Tabla 35: Ejemplos de categorías y referencias dentro de Recuperar

Categoría	Descripción	Referencias
Planificación de la recuperación	Planifique cómo recuperarse de un evento y los próximos pasos después de un evento.	ISO/IEC 27002:2013, cláusula 16 ISO/ IEC 27035 (todas las partes)
Comunicaciones	Procesos y procedimientos para comunicar la información oportuna a las partes relevantes.	ISO/IEC 27002:2013, cláusula 16 ISO/ IEC 27035 (todas las partes)
Mejoras	La organización toma las lecciones aprendidas durante un evento y las retroalimenta al proceso y los procedimientos.	ISO/IEC 27002:2013, cláusula 16 ISO/ IEC 27035 (todas las partes)

Las Tablas 35, 36 y 37 se centran en la descripción de los planes de recuperación estratégica, que son fundamentales para garantizar una recuperación activa y confiable. Como se ha mencionado anteriormente, la reputación es un aspecto crucial para las organizaciones, especialmente en el caso de las instituciones de salud, ya que se trata de un servicio sensible que involucra la vida y el bienestar de las personas. Estos planes de recuperación estratégica están diseñados para asegurar la continuidad de las operaciones y minimizar los impactos negativos en la reputación de la organización. Su implementación adecuada es esencial para garantizar una respuesta efectiva ante eventos adversos y mantener la confianza de los pacientes y la comunidad en general.

Tabla 36: Concepto de recuperación: categoría de planificación de recuperación, subcategorías y referencias

Descripción de la subcategoría	Mapeo de estándares
El plan de recuperación se ejecuta durante o después de un evento	ISO/CEI 27002:2013, 16.1.5 ISO/CEI 27031

Tabla 37: Concepto de recuperación: categoría de mejoras, subcategorías y referencias

Descripción de la subcategoría	Mapeo de estándares
Los planes de recuperación incorporan lecciones aprendidas	ISO/IEC 27001:2013, cláusula 10 ISO/IEC 27031
Las estrategias de recuperación se actualizan	ISO/IEC 27001:2013, cláusula 10 ISO/IEC 27031

Tabla 38: Concepto de recuperación: categoría de comunicaciones, subcategorías y referencias

Descripción de la subcategoría	Mapeo de estándares
Las relaciones públicas se manejan	ISO/CEI 27001:2013, 7.4 ISO/ CEI 27019:2017, 14.2.1
Reputación después de reparar un evento	ISO/CEI 27001:2013, 7.4
Las actividades de recuperación se comunican a las partes interesadas internas y a los equipos ejecutivos y de gestión.	ISO/CEI 27001:2013, 7.4

4.2.2. Categorización Impacto/Riesgo

El impacto se refiere a los incidentes que ocurren y deben ser comprendidos cuando se detectan anomalías y eventos. Esto permite realizar un análisis y una revisión de los eventos detectados. Es importante identificar la probabilidad y el impacto que pueden afectar tanto el aspecto comercial como los datos dentro de una organización.

A partir de la evaluación de amenazas, vulnerabilidades, probabilidad e impacto, se puede determinar el riesgo y establecer una respuesta priorizada a estos riesgos. La gestión de riesgos cibernéticos debe identificar las fuentes de riesgo y administrarlos a través de un buen enfoque de gestión de riesgos. Es fundamental que la gerencia impulse medidas de ciberseguridad para mitigar los riesgos.

La organización debe adoptar un enfoque adecuado para la gestión de riesgos, lo que garantiza una implementación efectiva. Es esencial que la tolerancia al riesgo de la organización esté claramente determinada y expresada a través de la documentación, lo que permite un seguimiento adecuado de los riesgos.

En resumen, aunque la norma de esta investigación no defina explícitamente los términos "impacto" y "riesgo", es posible deducir su significado a través de las Tablas y pautas proporcionadas.

Tabla 39: Categorización Impacto/Riesgo - Departamento de Tecnología

CATEGORIZACIÓN			
DEPARTAMENTO	**ACTIVOS**	**IMPACTO**	**RIESGO**
Departamento de tecnología	Centro Datos	ALTO	ALTO
	Servidores	ALTO	ALTO
	Equipos de comunicación (Redes, Firewalls, Wifi)	ALTO	ALTO
	Computadoras (PC, Portables)	MEDIO	MEDIO

Tabla 40: Categorización Impacto/Riesgo - Departamento Médico

CATEGORIZACIÓN			
DEPARTAMENTO	**ACTIVOS**	**IMPACTO**	**RIESGO**
Departamento Médico	Agendamiento	MEDIO	MEDIO
	Nutrición-Alimentación	MEDIO	MEDIO
	Farmacia/Tecnofarmacia	ALTO	MEDIO
	Quirófano	ALTO	ALTO
	Admisión	BAJO	BAJO
	Auditoria Médica	ALTO	ALTO
	Telemedicina	MEDIO	MEDIO
	LIS (PRUEBAS DE ANTIGENOS)	MEDIO	MEDIO
	RIS-PACS (IMAGENOLOGIA)	ALTO	ALTO

Tabla 41:Categorización Impacto/Riesgo - Departamento Administrativo

CATEGORIZACIÓN			
DEPARTAMENTO	**ACTIVOS**	**IMPACTO**	**RIESGO**
Departamento Administrativo	Finanzas	MEDIO	ALTO
	Comunicación	MEDIO	BAJO
	Calidad	MEDIO	MEDIO
	Mantenimiento	ALTO	ALTO
	Tesorería	MEDIO	MEDIO

	Servicio Cliente	MEDIO	MEDIO
	Legal	ALTO	ALTO
	Talento Humano	BAJO	BAJO

Tabla 42: Categorización Impacto/Riesgo - Departamento de Servicios

CATEGORIZACIÓN			
DEPARTAMENTO	**ACTIVOS**	**IMPACTO**	**RIESGO**
Departamento de Servicios	Mantenimiento	ALTO	ALTO
	Servicio de Seguridad	ALTO	ALTO
	Limpieza	ALTO	ALTO

4.3. Tercera Fase: Propuesta de medidas de protección

Comprende las medidas de protección y seguridad para reducir la categorización de impacto y riesgo identificado en el capítulo 4, numeral 4.2, además, se incluye los conceptos necesarios para proteger el dato medico basado en la norma ISO/IEC 27100:2021 para el área de salud.

4.3.1 Objeto de la propuesta

Proveer seguridad de la información a los datos médicos en el sector salud. Proponer una propuesta que contemple reducir la categorización de impacto riesgo en los departamentos de Tecnología, Área Médica, Administrativa y Servicios, esta propuesta debe garantizar la confidencialidad, integridad y disponibilidad de la información médica.

4.3.2 Acuerdo de confidencialidad

La organización debe firmar un acuerdo de confidencialidad, documento entre las partes que se comprometen a no divulgar y compartir información que son de la organización, estos acuerdos pueden ser unidireccionales o bidireccionales. Se presenta un modelo de acuerdo de confidencialidad.

Modelo acuerdo de confidencialidad

ORGANIZACIÓN manifiesta su compromiso de no utilizar con fines de difusión, publicación, protección legal por cualquier medio, licenciamiento, venta, cesión de derechos parcial o total o de proporcionar ventajas comerciales o lucrativas a terceros, con respecto al documento, materiales, datos analíticos o información de toda índole, relacionada con los intercambios de información derivados de la relación tecnológica desarrollada entre **COLABORADOR, PROVEEDOR, ETC… y ORGANIZACIÓN.**

En el caso de posibles publicaciones con fines académicos, estas se podrán realizar previa autorización escrita de la empresa **COLABORADOR, PROVEEDOR, ETC…,**

Asimismo, **ORGANIZACIÓN** y **COLABORADOR, PROVEEDOR, ETC…**asumen la responsabilidad de enterar a todas las personas que estarán relacionados con el proceso antes mencionado, de los compromisos, responsabilidades y alcances contenidos en este acuerdo, a fin de garantizar la confidencialidad aquí comprometida.

4.3.3. Levantamiento de requerimientos

Importante conocer cuáles son los departamentos involucrados en el inicio del proyecto, de esta forma podemos asignar a los usuarios claves para la toma de decisiones, estos usuarios conformarán el comité de seguridad de la información, la asignación debe realizar la máxima autoridad de la organización, este comité debe asignar un líder por departamento, el mismo que coordinará que las peticiones se cumplan para avanzar en el proyecto de seguridad de la información.

La máxima autoridad debe realizar un evento con el anuncio del comité de seguridad de la información, usuarios clave y líderes de los departamentos, este evento debe ser para toda la

organización. Esto dará el inicio y la directriz vertical para un proyecto de seguridad de la información.

4.3.4. Análisis y Diseño

- Revisión detallada de requerimientos
- Construcción de Documentos de información (protocolos)

4.3.5. Construcción

- Configuración de parámetros, cumplimiento de la norma ISO/IEC 27100:2021 para los activos de información de los departamentos asignados en el numeral 4.3.3 Levantamiento de información, estos son:
    - Identificación
    - Protección
    - Detección
    - Respuesta
    - Recuperación
    - Certificaciones
- Pruebas verticales de los protocolos de seguridad de la información, primero por departamento asignado en el numeral 4.3.3 Levantamiento de información.
- Validación de funcionalidad y cumplimiento de los documentos de protocolo de seguridad de la información.

En base a lo expuesto, se realiza la propuesta del conjunto de medidas de protección para minimizar el riesgo de los activos identificados:

Departamento de tecnología:

- **Identificación:** Realizar una evaluación exhaustiva de riesgos en el centro de datos y los servidores para identificar las vulnerabilidades y amenazas específicas.
- **Protección:** Implementar medidas de seguridad física, como control de acceso restringido y sistemas de vigilancia, en el centro de datos y la sala de servidores. Aplicar soluciones de seguridad tecnológica, como firewalls y sistemas de detección de intrusiones, para proteger los equipos de comunicación y las computadoras.
- **Detección:** Establecer sistemas de monitoreo y registro de actividad en los equipos de comunicación y las computadoras para detectar actividades sospechosas o no autorizadas.
- **Respuesta:** Desarrollar un plan de respuesta a incidentes específico para el departamento de tecnología, incluyendo procedimientos claros para reportar y manejar los incidentes de seguridad.
- **Recuperación:** Establecer planes de recuperación de desastres para el centro de datos y los servidores, incluyendo copias de seguridad regulares y procedimientos para la restauración de servicios.

Departamento Área Médica:

- **Identificación:** Identificar los activos críticos de información en el departamento médico, como los sistemas de agendamiento, nutrición-alimentación, farmacia, quirófano, entre otros.
- **Protección**: Implementar políticas y procedimientos de seguridad para proteger la confidencialidad y la integridad de los datos médicos. Establecer controles de acceso y autenticación para restringir el acceso a la información sensible.

- **Detección:** Implementar soluciones de monitoreo y detección de actividad sospechosa en los sistemas médicos, como telemedicina y registros de imágenes.
- **Respuesta:** Desarrollar un plan de respuesta a incidentes específico para el departamento médico, incluyendo la notificación de incidentes y la coordinación con otras áreas de la organización.
- **Recuperación:** Establecer planes de recuperación de desastres para los sistemas médicos, incluyendo la restauración de datos y la continuidad de la atención médica.

Departamento Administrativo:

- **Identificación:** Identificar los activos críticos de información en el departamento administrativo, como los sistemas de finanzas, comunicación, calidad, mantenimiento, entre otros.
- **Protección**: Implementar políticas y procedimientos de seguridad para proteger la confidencialidad y la integridad de la información administrativa. Establecer controles de acceso y cifrado de datos para proteger la información sensible.
- **Detección:** Implementar soluciones de monitoreo y detección de actividad sospechosa en los sistemas administrativos, como detección de intrusos y análisis de registros.
- **Respuesta:** Desarrollar un plan de respuesta a incidentes específico para el departamento administrativo, incluyendo la notificación de incidentes y la coordinación con otras áreas de la organización.
- **Recuperación**: Establecer planes de recuperación de desastres para los sistemas administrativos, incluyendo la restauración de datos y la continuidad de las operaciones administrativas.

Departamento de Servicios:

- **Identificación:** Identificar los activos críticos de información en el departamento de servicios, como los sistemas de mantenimiento, servicio de seguridad y limpieza.
- **Protección:** Implementar políticas y procedimientos de seguridad para proteger la confidencialidad y la integridad de la información de servicios. Establecer controles de acceso y supervisión para proteger los activos físicos.
- **Detección:** Implementar soluciones de monitoreo y detección de actividad sospechosa en los sistemas de servicios, como sistemas de videovigilancia y sistemas de alarma.
- **Respuesta:** Desarrollar un plan de respuesta a incidentes específico para el departamento de servicios, incluyendo la notificación de incidentes y la coordinación con otras áreas de la organización.
- **Recuperación:** Establecer planes de recuperación de desastres para los sistemas de servicios, incluyendo la restauración de datos y la continuidad de los servicios.

4.3.6. Transición

- Capacitación a Usuario Final.
- Pruebas horizontales del cumplimento de protocolos de seguridad de la información creados, se debe ejecutar por departamento asignado en el numeral 4.3.3 Levantamiento de información.
- Validación de Funcionalidad Integrada de los protocolos de seguridad de la información en la organización, ejecutarlo transversalmente.

4.3.7. Producción

- Entrega de información a la máxima autoridad avalada por el comité de seguridad de la información.
- Pruebas de cumplimiento de protocolos de seguridad de la información a la máxima autoridad por el comité de seguridad de la información
- Ejecutar la salida a vivo.

4.3.8. Cronograma de implementación

El cronograma es flexible y puede estar sujeto a cambios por parte del comité de seguridad de la información, es importante ir con el cronograma para cumplir con los tiempos asignados y comprometidos a la máxima autoridad.

Tabla 43: Cronograma Propuesta

CRONOGRAMA

ACTIVIDAD	Mes 1 -Mes 2	Mes 3 - Mes 5	Mes 6 - Mes 11	Mes 12	RESPONSABLE	GERENTE DE PROYECTO	HORARIO
Levantamiento de Requerimientos					Máxima Autoridad Comité de Seguridad de la información Usuarios Clave Colaboradores Organización	Asignado por Comité de Seguridad de la Información	08:00 - 12:00
Análisis y Diseño					Comité Seguridad de la Información Usuarios Clave Colaboradores Organización	Asignado por usuario Clave	09:00 - 15:00
Construcción			Certificaciones		Comité Seguridad de la Información Usuarios Clave Colaboradores Organización	Asignado por usuario Clave	09:00 - 15:00
Transición					Comité Seguridad de la Información Usuarios Clave Colaboradores Organización	Asignado por usuario Clave	11:00 - 17:00
Producción					Comité Seguridad de la Información Usuarios Clave	Asignado por usuario Clave	08:00 - 17:00

												Colaboradores Organización			

CAPITULO V: IMPLEMENTACIÓN

Es fundamental para una organización del sector salud público o privado que la seguridad es un todo, por lo tanto, la directriz vertical debe ser de la máxima autoridad para toda la organización, entonces, la seguridad de la información de un dato médico es compartida por todos.

Toda implementación debe tener un cronograma de actividades, responsables y tiempos para poder dar forma a un marco de seguridad de la información a la organización.

No todas las organizaciones necesariamente pueden tomar este modelo como factual para proceder e implementar, pero si como una base fundamentada.

5.1 Levantamiento de información

La máxima autoridad debe designar un comité de seguridad de la información, la designación se realiza en base al perfil académico de los profesionales que tiene la organización.

El comité es responsable de la valoración de los diferentes departamentos de la organización, el maco de este modelo descriptivo son los siguientes: Departamento de Tecnología, departamento de área médica, departamento administrativo, departamento de servicios.

El comité debe asignar a los usuarios claves y los lideres de cada departamento, usuarios claves son aquellos que tienen decisión y lo lideres son los que llevan adelante la recopilación de toda la información relevante de los diferentes usuarios de cada departamento.

Los usuarios claves definirán los activos de información que se tiene por cada departamento, los lideres llevaran un control de esos activos de información.

El comité debe definir con los usuarios clave cuales son los profesionales que tomarán las certificaciones de seguridad de la información.

5.2 Análisis y Diseño

Se realiza una revisión detallada obtenida del levantamiento de información, a cada documento se le debe asignar nombre y responsable.

Todos los documentos son almacenados en repositorio de datos para poder revisarlo y ejecutar el cambio respectivo, es importante que los documentos se encuentren con firma de responsabilidad

Con los documentos, como base, los usuarios clave deben analizar y diseñar acorde a la norma ISO/IEC 27100:2021 los protocolos, estos serán la primera versión para revisión en una mesa de trabajo.

La socialización de estos documentos con la organización es fundamental para lo toma de decisión del comité de seguridad de la información.

En esta etapa es importante analizar y diseñar el documento de capacitación y certificación, este debe tener los responsables, certificaciones a tomar y los tiempos de preparación para presentar el examen.

Se debe realizar reuniones de trabajo para revisión de cada documento, antes de llegar a la etapa de construcción, con esta revisión se dará la aprobación de los documentos analizados y diseñados, insumo fundamental para la siguiente etapa, siempre puede haber un cambio, debe estar fundamentado con un control de cambios, tendrá firma de responsabilidad.

Los controles de cambio de los documentos deben ser nuevamente revisados, analizados y de ser el caso diseñados, al obtener una nueva versión del documento, se debe realizar una mesa de trabajo para la socialización y aprobación de parte del comité de la seguridad de la información.

Si el documento que tiene un control de cambio no es aprobado, se deberá realizar nuevamente el levantamiento de información en el departamento e iniciar el proceso nuevamente, son tareas que se pueden realizar en paralelo, esto puede llegar a afectar el cronograma.

5.3 Construcción

En esta etapa se tiene documentos analizados, diseñados con firma de responsabilidad y aprobados por el comité de seguridad de la información, a cada documento con su respectiva versión se realizará lo siguiente:

Configuración de parámetros, cumplimiento de la norma ISO/IEC 27100:2021 para los activos de información:

- Identificación
- Protección
- Detección
- Respuesta
- Recuperación
- Certificaciones

Departamento de tecnología:

- **Identificación:** Realizar una evaluación exhaustiva de riesgos en el centro de datos para identificar las vulnerabilidades y amenazas específicas.

- **Protección:** Implementar medidas de seguridad física, como control de acceso restringido y sistemas de vigilancia, en el centro de datos. Aplicar soluciones de seguridad tecnológica, como firewalls y sistemas de detección de intrusiones, para proteger los equipos de comunicación y las computadoras.
- **Detección:** Establecer sistemas de monitoreo y registro de actividad en los equipos de comunicación y las computadoras para detectar actividades sospechosas o no autorizadas.
- **Respuesta:** Desarrollar un plan de respuesta a incidentes específico para el departamento de tecnología, incluyendo procedimientos claros para reportar y manejar los incidentes de seguridad.
- **Recuperación:** Establecer planes de recuperación de desastres para el centro de datos y los servidores, incluyendo copias de seguridad regulares y procedimientos para la restauración de servicios.

Departamento Área Médica:

- **Identificación:** Identificar los activos críticos de información en el departamento médico, como los sistemas de agendamiento, nutrición-alimentación, farmacia, quirófano, entre otros.
- **Protección**: Implementar políticas y procedimientos de seguridad para proteger la confidencialidad y la integridad de los datos médicos. Establecer controles de acceso y autenticación para restringir el acceso a la información sensible.
- **Detección:** Implementar soluciones de monitoreo y detección de actividad sospechosa en los sistemas médicos, como telemedicina y registros de imágenes.

- **Respuesta:** Desarrollar un plan de respuesta a incidentes específico para el departamento médico, incluyendo la notificación de incidentes y la coordinación con otras áreas de la organización.
- **Recuperación:** Establecer planes de recuperación de desastres para los sistemas médicos, incluyendo la restauración de datos y la continuidad de la atención médica.

Departamento Administrativo:

- **Identificación:** Identificar los activos críticos de información en el departamento administrativo, como los sistemas de finanzas, comunicación, calidad, mantenimiento, entre otros.
- **Protección:** Implementar políticas y procedimientos de seguridad para proteger la confidencialidad y la integridad de la información administrativa. Establecer controles de acceso y cifrado de datos para proteger la información sensible.
- **Detección:** Implementar soluciones de monitoreo y detección de actividad sospechosa en los sistemas administrativos, como detección de intrusos y análisis de registros.
- **Respuesta:** Desarrollar un plan de respuesta a incidentes específico para el departamento administrativo, incluyendo la notificación de incidentes y la coordinación con otras áreas de la organización.
- **Recuperación:** Establecer planes de recuperación de desastres para los sistemas administrativos, incluyendo la restauración de datos y la continuidad de las operaciones administrativas.

Departamento de Servicios:

- **Identificación:** Identificar los activos críticos de información en el departamento de servicios, como los sistemas de mantenimiento, servicio de seguridad y limpieza.
- **Protección:** Implementar políticas y procedimientos de seguridad para proteger la confidencialidad y la integridad de la información de servicios. Establecer controles de acceso y supervisión para proteger los activos físicos.
- **Detección:** Implementar soluciones de monitoreo y detección de actividad sospechosa en los sistemas de servicios, como sistemas de videovigilancia y sistemas de alarma.
- **Respuesta:** Desarrollar un plan de respuesta a incidentes específico para el departamento de servicios, incluyendo la notificación de incidentes y la coordinación con otras áreas de la organización.
- **Recuperación:** Establecer planes de recuperación de desastres para los sistemas de servicios, incluyendo la restauración de datos y la continuidad de los servicios.

Las certificaciones son un punto importante y debe ser para todas los departamentos que previamente fueron asignados, además, los profesionales por departamento que tomarán la certificación en seguridad de la información.

Certificaciones: El plan de certificaciones debe estar alineado a la normativa ISO, de cumplimiento mandatorio para los profesionales asignados en el análisis y diseño y se sujetará a cada departamento.

Se debe realizar las pruebas verticales con los documentos de seguridad de la información (protocolos), se inicia por cada departamento para probar que está cumpliendo su objetivo.

Se debe validar la funcionalidad y cumplimiento de los documentos de protocolo de seguridad de la información, regresamos a la etapa anterior si estos documentos no pasaron la

funcionalidad y cumplimiento, siempre con un control de cambio, con la respectiva socialización en la mesa de trabajo.

5.4 Transición

Estamos en el mes 6 y se realizan en paralelo las etapas de construcción y transición, es el momento de capacitar a los usuarios finales de la organización en el uso de los documentos de seguridad de la información, en este punto se indica que los documentos son protocolos de estricto cumplimiento obligatorio, no cumplirlo será un llamado de atención que la unidad de talento humano hará conocer.

Se realizan las pruebas horizontales en toda la organización de los protocolos de seguridad de la información, se comprueba y documenta cada prueba. La socialización a toda la organización es fundamental para evitar riesgo de conocimiento de cualquier miembro de la organización.

La validación de funcionalidad es integral para toda la organización de todos los protocolos de seguridad de la información, el aprobar la funcionalidad indica compromiso y credibilidad en tiempo y forma. No hacerlo implica regresar a las etapas anteriores con el control de cambio respectivo.

5.5 Producción

Momento para poner en marcha todo el modelo de seguridad de la información de la organización, previo, se debe entregar toda la documentación de respaldo con firmas de responsabilidad de todos los responsables que participaron en la elaboración de los protocolos a la máxima autoridad, la entrega la realiza el comité de seguridad de la información en reunión formal.

Con todos los protocolos de la seguridad de la información aprobados, probados vertical y horizontalmente, profesionales certificados en las normas ISO, podemos garantizar que la organización manejará la información del dato médico de forma responsable.

CAPITULO VI: CONCLUSIONES Y RECOMENDACIONES

6.1.Conclusiones

- Es de vital importancia protocolos de seguridad de la información basados en la Norma ISO 27110:2021 para evitar expuestos legales a la organización.
- En las últimas décadas, las organizaciones de salud han sufrido numerosos ataques que han afectado la disponibilidad de sus servicios y la confidencialidad de los datos personales y clínicos de toda la organización. Por este motivo, las organizaciones se han visto en la necesidad de priorizar y abordar los problemas de ciberseguridad.
- La industria de la salud presenta una falta de conciencia y capacitación en materia de seguridad de la información. Existe un desconocimiento generalizado sobre normativas, protocolos y medidas de protección, lo que pone en riesgo la confidencialidad, integridad y disponibilidad de los datos médicos.
- Las organizaciones del sector de la salud no tienen comités de seguridad de la información, genera un problema estructural dentro de la organización debido que no existe un manejo adecuado de la información a nivel vertical.
- La falta de comunicación y socialización por parte del comité de seguridad de la información ha generado una brecha en la implementación efectiva de medidas de protección. Existe una necesidad urgente de fortalecer la comunicación, impartir capacitaciones adecuadas y generar conciencia en todos los colaboradores.
- Es mandatorio una acción inmediata por parte de la máxima autoridad y el comité de seguridad de la información para desarrollar e implementar un plan integral de seguridad de la información. Esto incluye establecer protocolos, realizar evaluaciones de riesgo, promover la certificación de profesionales,

- Es mandatorio que la organización refleje auditorias regulares del cumplimiento de los protocolos de seguridad de la información, informes que deben ser presentados a la máxima autoridad.
- La seguridad de los datos médicos debe ser una prioridad en la organización y debe contar con el compromiso de todos los colaboradores, el riesgo es compartido.

6.2.Recomendaciones

- Incorporar protocolos de seguridad de la información como una prioridad estratégica en la gestión de las organizaciones del sector de salud, que garanticen la protección de los datos médicos.
- Establecer una estructura organizativa sólida, con directriz vertical que incluya un comité de seguridad de la información, encargados de definir políticas, metas y objetivos, así como de supervisar y apoyar los proyectos relacionados con la seguridad de la información.
- Asignar los recursos financieros necesarios para garantizar el éxito de los proyectos de seguridad de la información, permitiendo la implementación de medidas adecuadas de identificación, protección, detección, recuperación, respuesta y certificación a posibles ataques y amenazas.
- Realizar evaluaciones periódicas de la situación actual de la seguridad de la información, identificando brechas, vulnerabilidades y riesgos.
- Establecer planes de acción con objetivos claros, métricas e indicadores para medir el progreso y tomar medidas correctivas cuando sea necesario.
- Implementar programas de capacitación y socialización en seguridad de la información dirigidos a toda la organización, con el objetivo de involucrar a todos los colaboradores en la protección de los datos médicos y fomentar una cultura de seguridad.

- Proporcionar información clara sobre los riesgos y amenazas existentes, las políticas y procedimientos de seguridad, así como las mejores prácticas en el manejo de la información sensible.
- Promover mesas de trabajo para los colaboradores puedan expresar sus inquietudes y contribuir ideas y soluciones en materia de seguridad de la información.

BIBLIOGRAFÍA

Alzuri, P., Cabral, F., Paz, S., Nowersztern, A., & Libedinsky, P. (2020). Proteguiendo la salud digital - Una guía de ciberseguridad en el sector salud.

BID, Alzuri, P., Cabral, F., Paz, S., Nowersztern, A., & Libedinsky, P. (2021). *Protegiendo la salud digital. Una Guía de ciberseguridad en el sector de salud.* BID.

BID, OEA. (2020). *Reporte Ciberseguridad 2020.*

Bitglass. (2020). *Informe 2020 de brechas de datos en el sector sanitario.*

Deloitte. (2019). Escenario de amenazas en la Industria de Salud y Ciencias de la Vida. *Deloitte Threat Intelligence & Analytics*, 28.

European Commission. (27 de 04 de 2016). General Data Protection Regulation. Europa.

Fonseca, T. H. (2018). ANÁLISIS Y EVALUACIÓN DE RIESGOS, DE LOS ACTIVOS DE INFORMACIÓN DE LA DIRECCIÓN EJECUTIVA SECCIONAL DE ADMINISTRACIÓN JUDICIAL DE TUNJA . DESAJT, ADOPTANDO UNA METODOLOGÍA DE GESTIÓN DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN. CEAD, TUNJA.

Hernández Sampieri, R., & Mendoza Torres, C. P. (2018). *Metodología de la investigación: las rutas: cuantitativa ,cualitativa y mixta.* Mc Graw Hill educación.

HIMSS. (2020). *La seguridad cibernética.*

Hoffman, D., Professor, S. F., Duke, U., Kotz, A., Researcher, Contreras, B., . . . Digi, A. A. (2023). *LATAM CISO - Report 2023.*

IBM. (2021). *IBM Security.* Obtenido de Informe sobre el coste de una brecha de datos: https://www.ibm.com/downloads/cas/2YW7GWO1

IBM. (s.f.). *IBM Security.* Obtenido de Elimine las dificultades del cumplimiento normativo con las herramientas adecuadas, la conformidad puede ser un activo valioso y no solo un costo necesario: https://www.ibm.com/downloads/cas/VM8RZ87Y

Ignacio Alamillo i Domingo, Ó. B. (2008). *Seguridad de la Información en Entornos Sanitarios.* España: SEIS, Navarra de Gestión para la Administración, S.A. .

ISO 14971. (2019). Medical devices — Application of risk management to medical devices. Obtenido de Medical devices — Application of risk management to medical devices: https://www.iso.org/standard/72704.html

ISO 19011. (2018). *Guidelines for auditing management systems*. Obtenido de Guidelines for auditing management systems: https://www.iso.org/standard/70017.html

ISO. (2021). *Tecnología de la información, ciberseguridad y protección de la privacidad - Directrices para el desarrollo del marco de ciberseguridad.* ISO.

ISO 27799. (2016). Health informatics — Information security management in health using ISO/IEC 27002. Obtenido de Health informatics — Information security management in health using ISO/IEC 27002: https://www.iso.org/standard/62777.html

ISO 31000(es). (2018). *Gestión del riesgo — Directrices*. Obtenido de Gestión del riesgo — Directrices: https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es

ISO/IEC 15408-1:2022. (2022). *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 1: Introduction and general model*. Obtenido de

Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 1: Introduction and general model: https://www.iso.org/standard/72891.html

ISO/IEC 15408-2:2022. (s.f.). Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 2: Security functional components. Obtenido de ISO: https://www.iso.org/standard/72892.html

ISO/IEC 15408-3:2022. (s.f.). Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 3: Security assurance components. Obtenido de ISO: https://www.iso.org/standard/72906.html

ISO/IEC 15408-4:2022. (s.f.). *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 4: Framework for the specification of evaluation methods and activities*. Obtenido de Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 4: Framework for the specification of evaluation methods and activities: https://www.iso.org/standard/72913.html

ISO/IEC 15408-5. (2022). *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 5: Pre-defined packages of security requirements*. Obtenido de Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 5: Pre-defined packages of security requirements: https://www.iso.org/standard/72917.html

ISO/IEC. (02 de 2022). Information security, cybersecurity and privacy protection - Information security controls.

ISO/IEC 27000:2018(E). (02 de 2018). Information technology — Security techniques — Information security management systems — Overview and vocabulary.

ISO/IEC 27001. (2022). Information security, cybersecurity and privacy protection - Information security management systems - Requirements. ISO.

ISO/IEC 27110 . (02 de 2021). TÉCNICO ESPECIFICACIÓN. *Tecnología de la información, ciberseguridad y protección de la privacidad — Directrices para el desarrollo del marco de ciberseguridad*.

Kaspersky. (s.f.). *Kaspersky*. Obtenido de Piratas informáticos de sombrero negro, sombrero blanco y sombrero gris: definición y explicación: https://www.kaspersky.es/resource-center/definitions/hacker-hat-types

Luis Tejerina, S. P. (22 de 02 de 2021). *BID*. Obtenido de El sector salud es el más atractivo para los ciberataques. ¿Estamos preparados para protegerlo?: https://blogs.iadb.org/salud/es/el-sector-salud-es-el-mas-atractivo-para-los-ciberataques/

MINISTERIO DE TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACIÓN. (2020). Acuerdo Ministerial No. 025-2019. *Registro Oficial*, (pág. 123). Quito.

Office for Civil Rights (OCR). (17 de 05 de 2021). HIPAA for Professionals. United States. Obtenido de https://www.hhs.gov/hipaa/index.html

Pomerantz, D. (16 de 03 de 2021). *Mastercard*. Obtenido de Surgen más amenazas cibernéticas en el área de la salud - ¿es un efecto secundario de la pandemia? 4 razones explican el por qué: https://www.mastercard.com/news/latin-america/es/perspectivas/blog-posts/blog-es/2021/surgen-mas-amenazas-ciberneticas-en-el-area-de-la-salud/

Red Seguridad. (11 de 04 de 2023). *Red Seguridad*. Obtenido de Los ciberataques al sector sanitario crecen un 650% en el último año:

https://www.redseguridad.com/actualidad/cibercrimen/los-ciberataques-al-sector-sanitario-crecen-un-650-en-el-ultimo-ano_20230411.html#:~:text=Los%20ciberataques%20al%20sector%20sanitario%20crecen%20un%20650%25%20en%20el%20%C3%BAltimo%20a%C3%B1o&text=Los%2

Redacción. (04 de 05 de 2023). *consumoTIC*. Obtenido de Sector salud, vulnerable ante la ciberdelincuencia : https://consumotic.mx/tecnologia/sector-salud-vulnerable-ante-la-ciberdelincuencia/

Sabatino, C. (mayo de 2021). *Manual MSD*. Obtenido de La confidencialidad y la HIPAA (Ley de Portabilidad y Responsabilidad de Seguros de Salud en Estados Unidos): https://www.msdmanuals.com/es-ec/hogar/fundamentos/asuntos-legales-y-%C3%A9ticos/la-confidencialidad-y-la-hipaa-ley-de-portabilidad-y-responsabilidad-de-seguros-de-salud-en-estados-unidos

ANEXOS

ANEXO A. PREGUNTAS DE ENCUESTA

Encuesta Ciberseguridad - Norma ISO/IEC 27110 TS - Sector Salud

Estimado profesional del sector de la atención médica:

Nos complace invitarlo a participar en esta encuesta cuyo objetivo principal es analizar la situación actual de la seguridad de los datos médicos en el ámbito de la ciberseguridad. Esta investigación forma parte del proyecto de titulación titulado "Análisis de riesgo en la seguridad de los datos médicos mediante la utilización de la norma ISO/IEC 27110:2021".

El propósito de esta encuesta es recopilar información valiosa sobre las prácticas existentes en materia de seguridad y ciberseguridad de los datos médicos. La norma ISO/IEC 27110:2021 proporciona directrices técnicas para el desarrollo de un marco de ciberseguridad, bajo el título "Seguridad de la información, ciberseguridad y protección de la privacidad - Líneas directrices para el desarrollo de un marco de ciberseguridad".

Agradecemos sinceramente su participación y compromiso en este estudio. Sus respuestas serán tratadas de manera confidencial y anónima, y la información recopilada se utilizará únicamente con fines académicos e investigativos. Sus aportes serán de gran valor para fortalecer la seguridad de los datos médicos y garantizar la confidencialidad, integridad y disponibilidad de la información en el sector de la atención médica.

Le invitamos a responder con sinceridad y precisión a las preguntas que se presentan a continuación. La encuesta consta de preguntas cerradas, preguntas abiertas y una escala de calificación. Estimamos que tomará aproximadamente 5 minutos completarla.

Agradecemos de antemano su colaboración y el tiempo dedicado a esta importante investigación. Sus respuestas contribuirán al avance de la ciberseguridad en el ámbito de la atención médica y al cumplimiento de los objetivos del proyecto de titulación. Si tiene alguna pregunta o inquietud, no dude en comunicarse.

¡Muchas gracias por su participación y apoyo!

Sharina Bastidas

Estudiante de Ingeniería de Sistemas de la Información – PUCE

Preguntas

1. **¿Cuál es su nivel educativo?**

a) Tercer Nivel

b) Cuarto Nivel

c) Phd

2. **Acorde al título que escogió en la pregunta #1, indique cuál es su área de especialización.**

a) Tecnología

b) Área Médica

c) Administrativo

d) Servicios

3. **¿En qué tipo de organización relacionada con servicios de salud trabaja actualmente?**

a) Público

b) Privado

4. ¿Está familiarizado/a con el Acuerdo Ministerial No. 025-2019 relacionado con la seguridad de la información en el sector salud?

a) Si

b) No

5. ¿Conoce usted que es un comité de seguridad de la información?

a) Si

b) No

6. ¿Usted sabe qué un comité de seguridad de la información es designado por la máxima autoridad de su empleador?

a) Si

b) No

7. Usted conoce que el comité de seguridad de la Información es la unidad que realiza el seguimiento del cumplimiento del acuerdo ministerial No. 025-2019?

a) Si

b) No

8. ¿Está familiarizado(a) con la norma ISO/IEC 27110:2021 - Tecnología de la información, ciberseguridad y protección de la privacidad — Directrices para el desarrollo del marco de ciberseguridad?

a) Si

b) No

9. **¿Usted considera que en el sector de la salud la ciberseguridad mencionada en la pregunta anterior es un aspecto importante para proteger la información?**

a) Si

b) No

10. **Está preocupado por la seguridad de los datos médicos de: colaboradores, pacientes, clientes pagadores, etc…en el sector de la Salud?**

a) Si

b) No

11. **Su empleador implementa medidas de seguridad efectivas para proteger los datos médicos?**

a) Si

b) No

c) Desconozco

12. **Conoce las implicaciones de pérdida, robo, ataque, amenaza, vulnerabilidad, impacto, etc…de los datos médicos de colaboradores, pacientes, clientes pagadores, etc…**

a) Si

b) No

13. **Considera que su empleador asigno recursos financieros suficientes para abordar los riesgos de seguridad de los datos médicos.**

a) Si

b) No

c) Desconozco

14. Su empleador realiza capacitación para la protección de datos médicos

a) Si

b) No

15. Considera que su empleador está comprometido en la mejora continua con la seguridad de los datos médicos

a) Si

b) No

c) Desconozco

16. **¿Qué tan preparado está su empleador para hacer frente a posibles ataques a los datos médicos?**

a) Bajo

b) Medio

c) Alto

17. ¿Cuál de estas medidas de protección que permiten prevenir y mitigar posibles ataques a los datos médicos usted conoce que se implementó en su empleador? (Seleccione las medidas que conoce, pueden ser varias opciones)

a) Uso de firewalls y sistemas de detección de intrusos

b) Implementación de políticas de acceso y autenticación robustas

c) Encriptación de datos sensibles

d) Realización regular de pruebas de vulnerabilidad y penetración

e) Capacitación y concientización de los empleados sobre buenas prácticas de seguridad

f) Contratación de servicios de seguridad gestionada

g) Monitoreo constante de la red y registros de actividad

h) Implementación de respaldos regulares y políticas de recuperación de datos

i) Colaboración con proveedores externos especializados en seguridad de la información

18. ¿En qué parámetro considera que las medidas para proteger y prevenir de posibles ataques de los datos médicos propuestas por su empleador son satisfactorias?

a) Bajo

b) Medio

c) Alto

19. ¿Conoce usted si su empleador cuenta con un protocolo formal establecido para responder a posibles ataques de ciberseguridad, de acuerdo, a los siguientes puntos?

a) Contamos con un protocolo detallado y documentado.

b) Contamos con un protocolo básico, pero no está completamente desarrollado y documentado.

c) No contamos con un protocolo establecido, pero estamos en proceso de desarrollarlo.

d) No contamos con un protocolo establecido en nuestra organización.

20. Los ataques de ciberseguridad afectan las transfusiones de medicamentos y el funcionamiento de las máquinas médicas. ¿Qué opción considera más aceptable?

a) Soy consciente de los riesgos en la transfusión de medicamentos y el uso de máquinas médicas.

b) Conozco los riesgos, pero no tengo un conocimiento profundo sobre el tema.

c) Desconozco los riesgos en estos contextos.

21. ¿Su empleador cuenta con un protocolo establecido para controlar y prevenir ataques de ciberseguridad en la transfusión de medicamentos y el uso de máquinas médicas?

a) Si

b) No

Si la respuesta es "No", escoja de las siguientes opciones el por qué no se implementa un protocolo:

a) Falta de recursos financieros

b) Falta de conocimiento sobre los riesgos de ciberseguridad en estos contextos.

c) Consideramos que los riesgos de ciberseguridad en estos contextos son insignificantes.

22. ¿Existe un protocolo de evaluación de riesgo para controlar y prevenir ataques de ciberseguridad en la transfusión de medicamentos y el uso de máquinas médicas en su empleador?

a) Contamos con un protocolo detallado y documentado.

b) Nos basamos en las experiencias y asumimos un riesgo

c) Conocemos el riesgo y el impacto que puede ocasionar

d) Desconozco si existe o no un protocolo

23. Considera que su empleador debería aplicar la norma ISO/IEC 27110:2021 para desarrollar las directrices y obtener un marco de ciberseguridad que mejore la seguridad de los datos médicos?

a) Definitivamente sí.

b) Probablemente sí.

c) No estoy seguro/a.

d) Probablemente no.

e) Definitivamente no.

24. ¿Su empleador cuenta con alguna certificación ISO de ciberseguridad, como por ejemplo ISO 27001, ISO 27701 u otras relacionadas?

a) Sí

b) No

c) En proceso

d) Desconozco

25. ¿Considera que su empleador aplica Sistemas de Gestión de Seguridad de la Información (SGSI) para el control y protección de la seguridad de los datos médicos?

a) Sí

b) No

c) Desconozco

26. ¿En su unidad de negocio existe uno o varios colaboradores que cuenten con certificación en seguridad de la información ISO 27001?

a) Al menos uno.

b) Más de uno

c) No tenemos

d) Desconozco

27. Es importante tener uno o varios colaboradores con certificación en Seguridad de la Información - ISO 27001 dentro de su unidad de negocio y/o empleador?

a) Mandatorio

b) De vital importancia

c) Considero no es necesario

d) No estoy seguro/a de su relevancia en nuestra unidad de negocio

28. ¿Conoce algún problema reciente o actual relacionado con la vulnerabilidad de la pérdida, robo, ataque, amenaza, vulnerabilidad, impacto, etc…de la seguridad de los datos médicos?

a) Sí

b) No

29. ¿Conoce si realizan auditorias regulares de seguridad de la información en su empleador para evaluar el cumplimiento de los estándares y normas establecidos?

a) Nunca

b) Ocasionalmente

c) Siempre, semestral, anual

d) Desconozco

30. ¿Con qué frecuencia se realizan evaluaciones periódicas de vulnerabilidad y pruebas de penetración para identificar posibles brechas de seguridad en los sistemas y aplicaciones de su empleador?

a) Nunca

b) Ocasionalmente

c) Siempre

d) Desconozco

31. ¿Tiene su empleador un equipo dedicado a la seguridad de la información que se encargue de gestionar, supervisar, prevenir, informar aspectos relacionados con la seguridad de la Información?

a) Si

b) No

c) Desconozco

32. ¿En qué nivel se implementan medidas de control de acceso físico y lógico para proteger los activos críticos y los sistemas de información de su organización?

a) Bajo

b) Medio

c) Alto

33. ¿Conoce con qué frecuencia se realizan copias de seguridad de las bases de datos de su empleador para garantizar la disponibilidad y recuperación de la información en caso de una pérdida, robo, ataque, amenaza, vulnerabilidad, impacto, etc…de la seguridad de los datos?…

a) Diario

b) Semanal

c) Mensual

d) Trimestral

e) Semestral

f) Anual

34. Conoce en qué nivel se implementan medidas de seguridad adicionales, como: monitoreo de seguridad en tiempo real, detección de intrusos y análisis de comportamiento, para identificar y responder de manera proactiva a las amenazas pérdida, robo, ataque, amenaza, vulnerabilidad, impacto,etc… a la seguridad de los datos médicos?

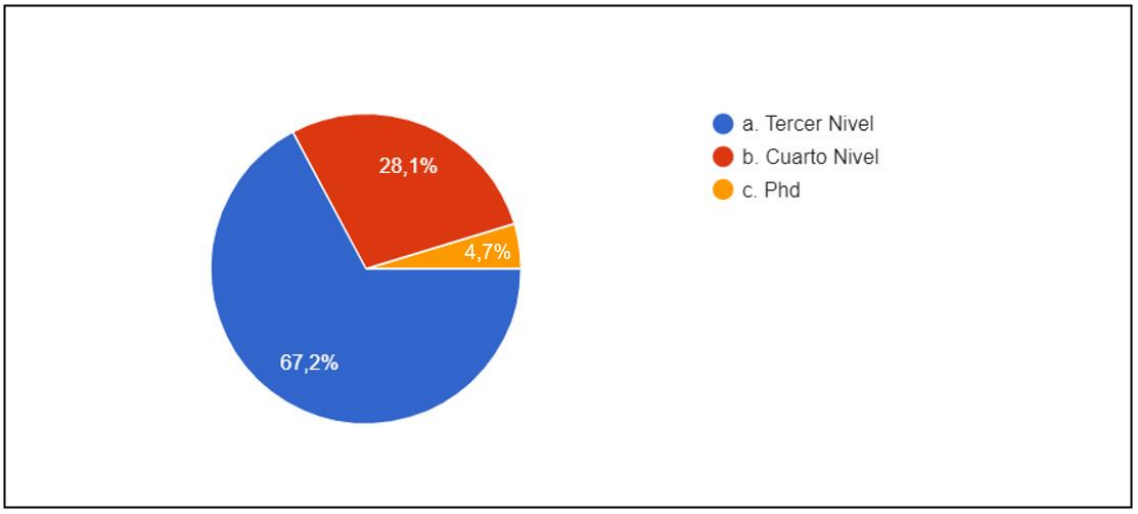
a) Bajo

b) Medio

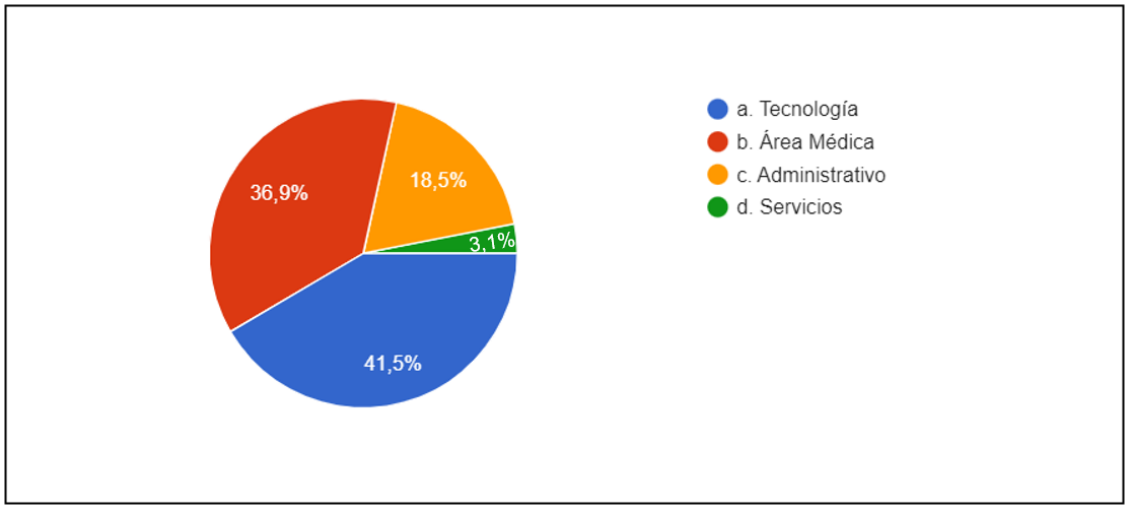
c) Alto

ANEXO B. GRÁFICOS DE RESPUESTAS (ENCUESTA)

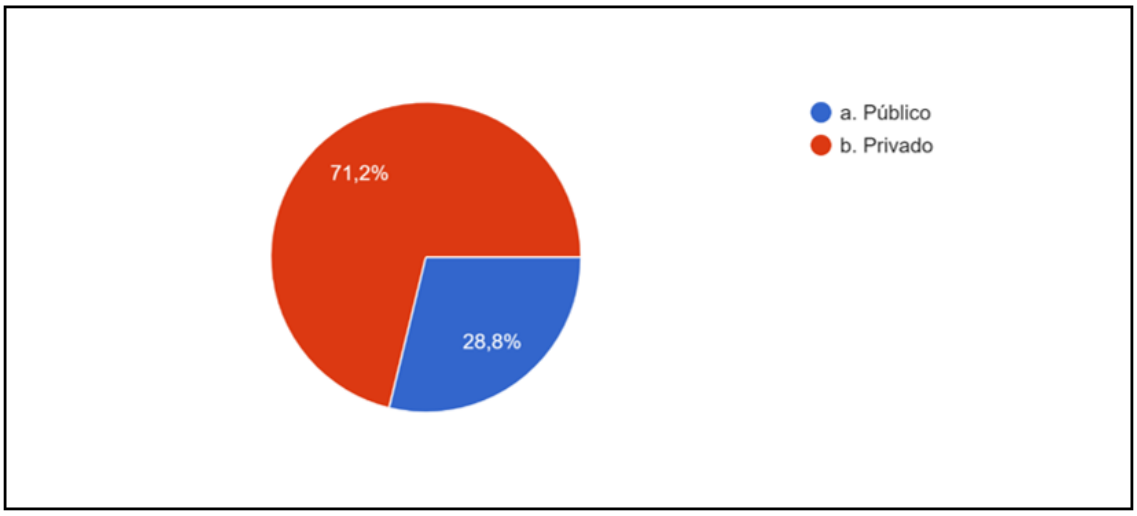
Pregunta 1: ¿Cuál es su nivel educativo?:



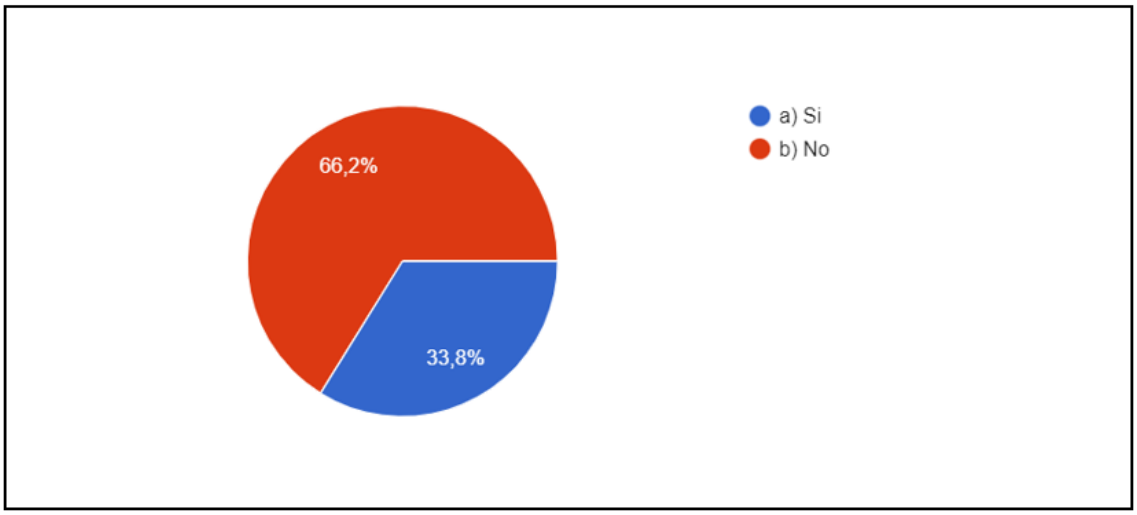
Pregunta 2: Acorde al título que escogió en la pregunta #1, indique cuál es su área de especialización.



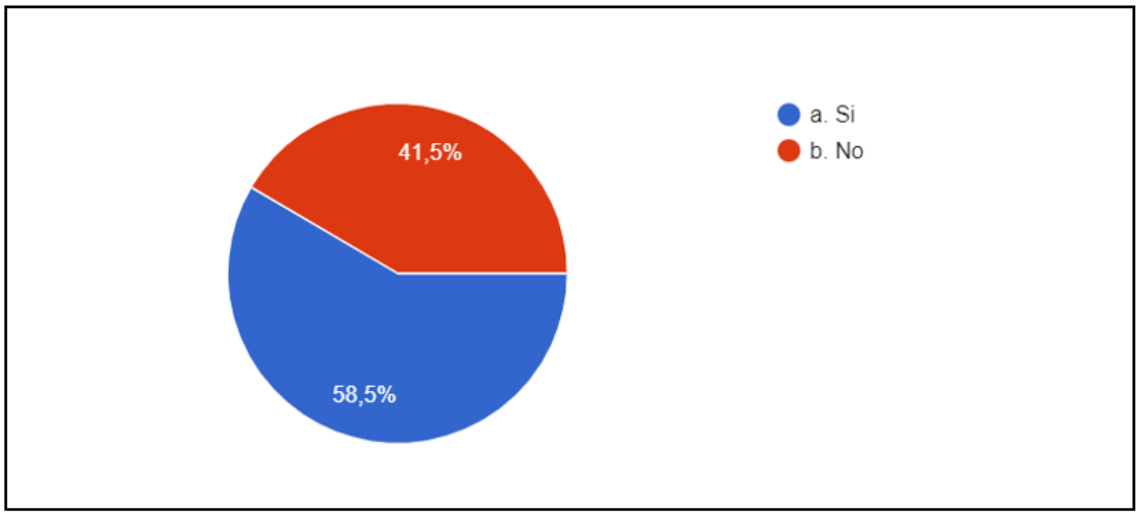
Pregunta 3: ¿En qué tipo de organización relacionada con servicios de salud trabaja actualmente?



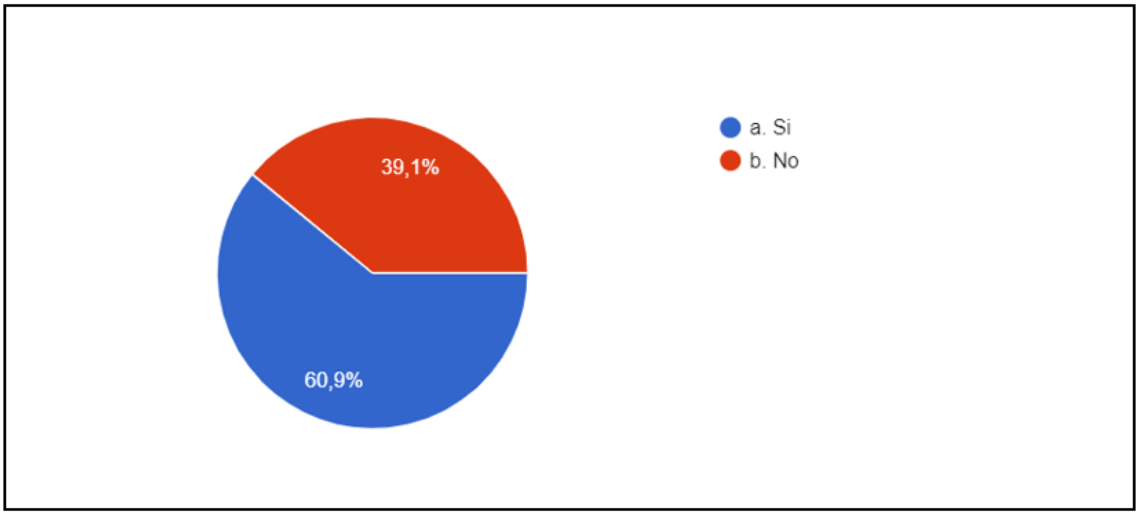
Pregunta 4: ¿Está familiarizado/a con el Acuerdo Ministerial No. 025-2019 relacionado con la seguridad de la información en el sector salud?



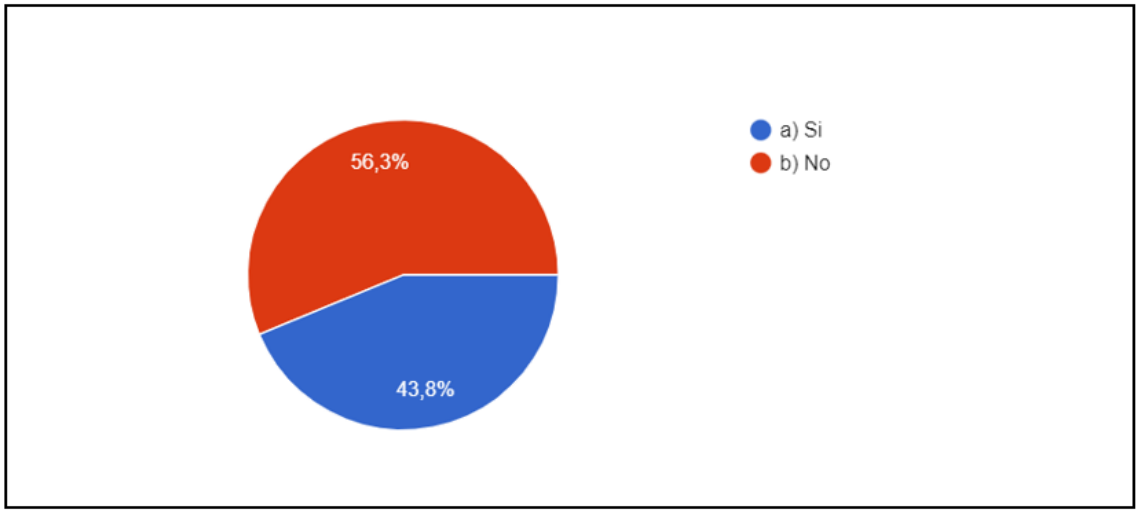
Pregunta 5: ¿Conoce usted que es un comité de seguridad de la información?



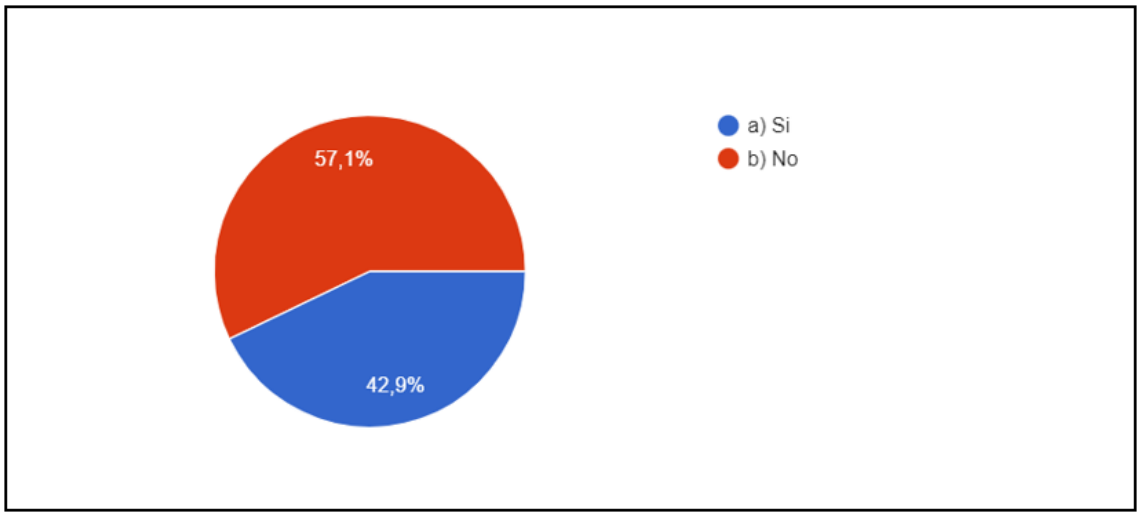
Pregunta 6: ¿Usted sabe qué un comité de seguridad de la información es designado por la máxima autoridad de su empleador?



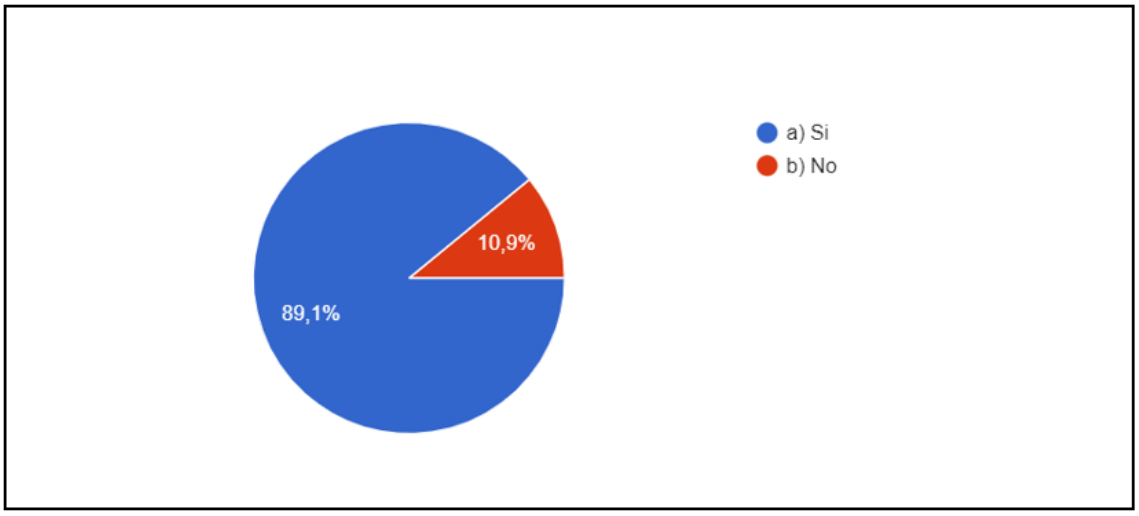
Pregunta 7: ¿Usted conoce que el comité de seguridad de la información es la unidad que realiza el seguimiento del cumplimiento del acuerdo ministerial No? 025-2019?



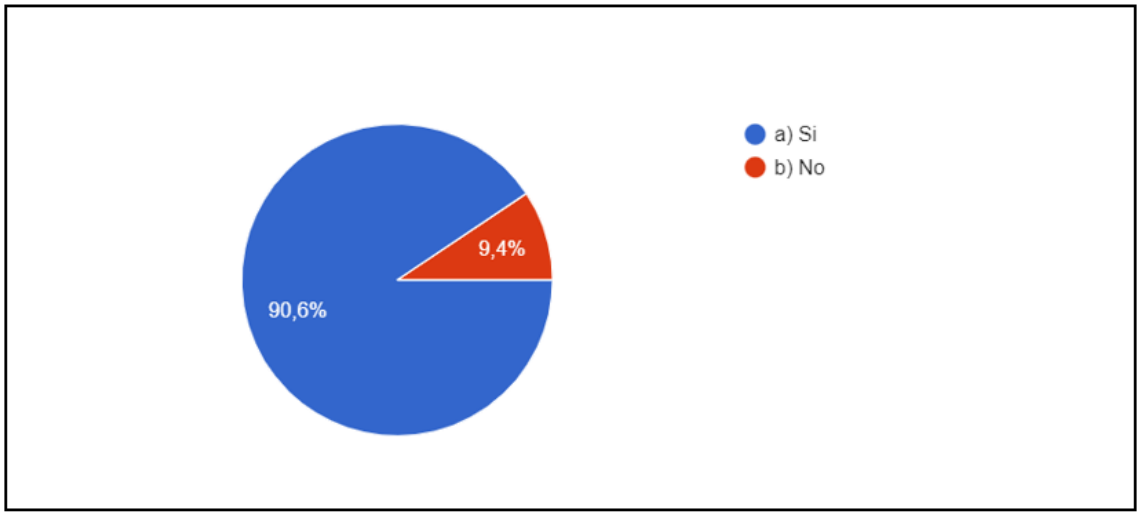
Pregunta 8: ¿Está familiarizado(a) con la norma ISO/IEC 27110:2021 - Tecnología de la información, ciberseguridad y protección de la privacidad — Directrices para el desarrollo del marco de ciberseguridad?



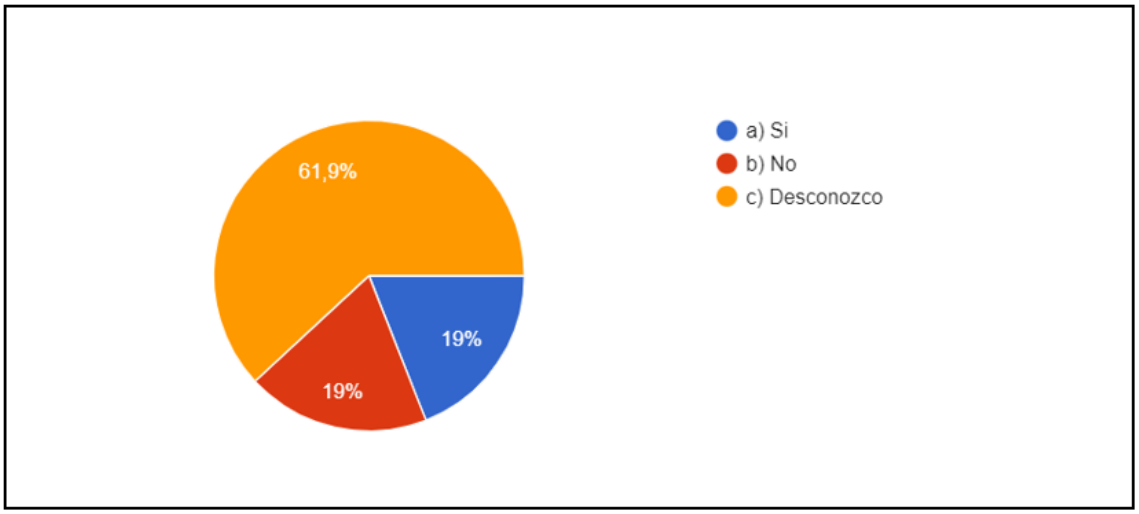
Pregunta 9: ¿Usted considera que en el sector de la salud la ciberseguridad mencionada en la pregunta anterior es un aspecto importante para proteger la información?



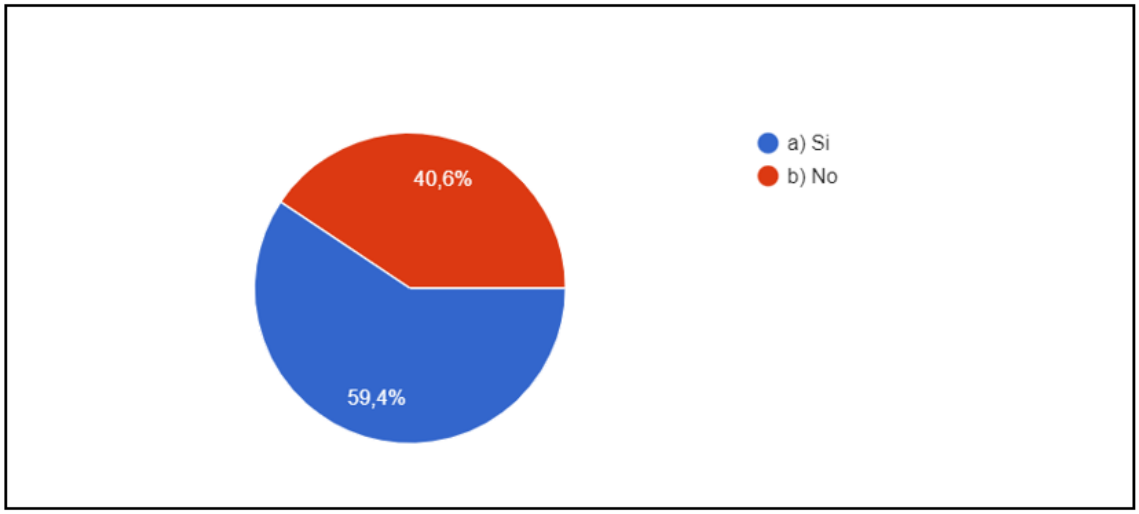
Pregunta 10: Está preocupado por la seguridad de los datos médicos de: colaboradores, pacientes, clientes pagadores, etc…en el sector de la Salud.



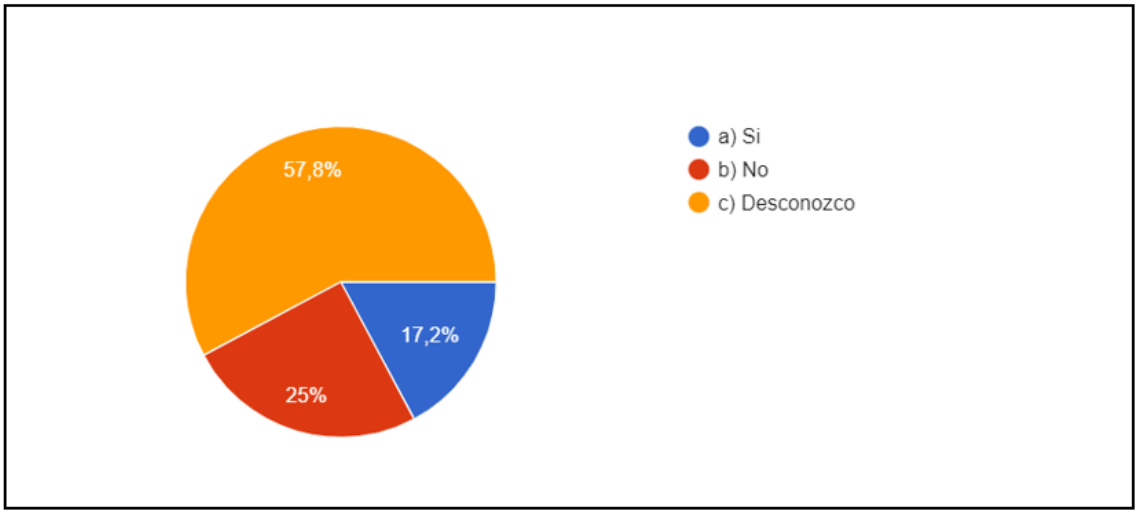
Pregunta 11: Su empleador implementa medidas de seguridad efectivas para proteger los datos médicos?



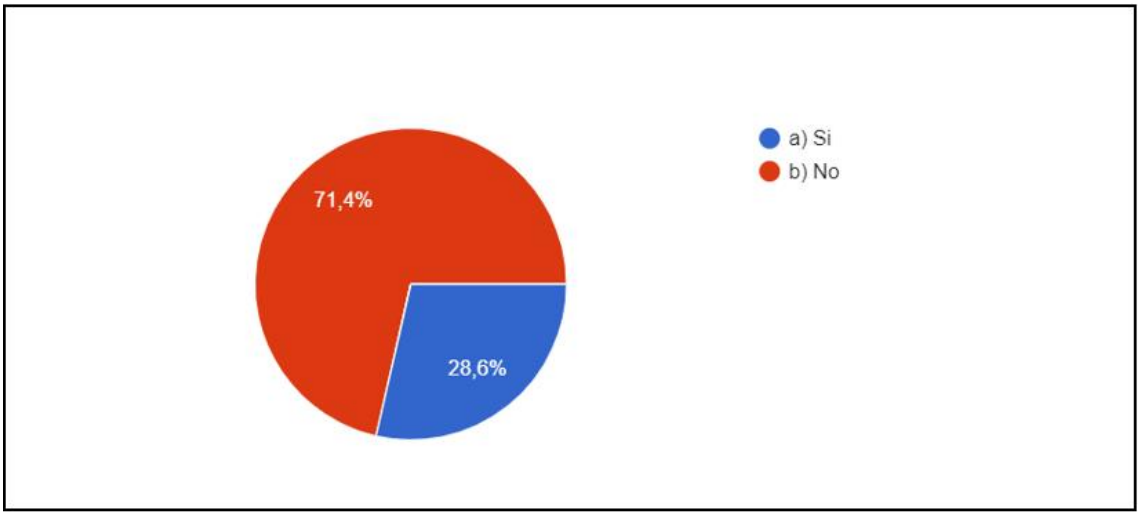
Pregunta 12: Conoce las implicaciones de pérdida, robo, ataque, amenaza, vulnerabilidad, impacto, etc…de los datos médicos de colaboradores, pacientes, clientes pagadores, etc…



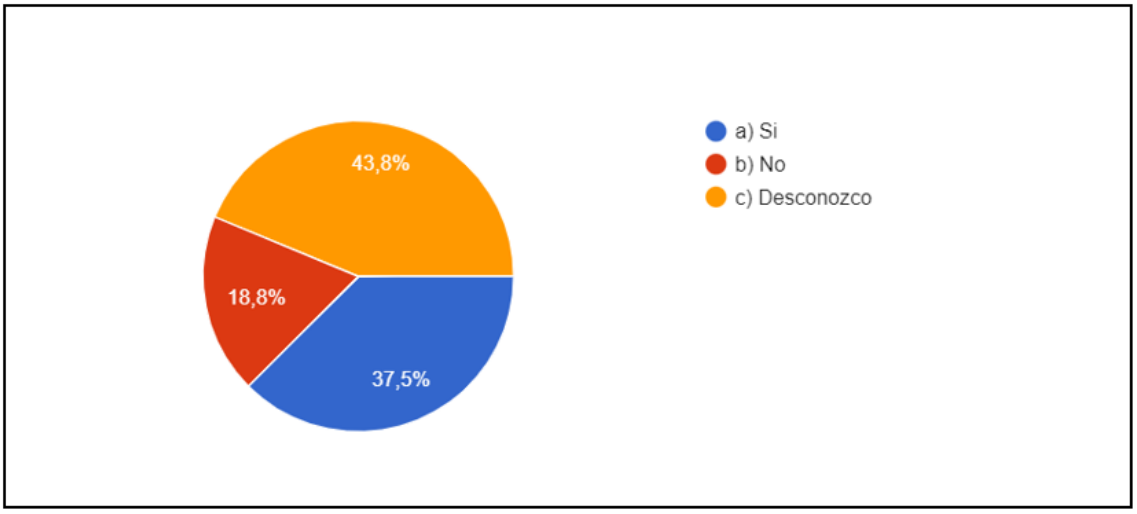
Pregunta 13: Considera que su empleador asigno recursos financieros suficientes para abordar los riesgos de seguridad de los datos médicos.



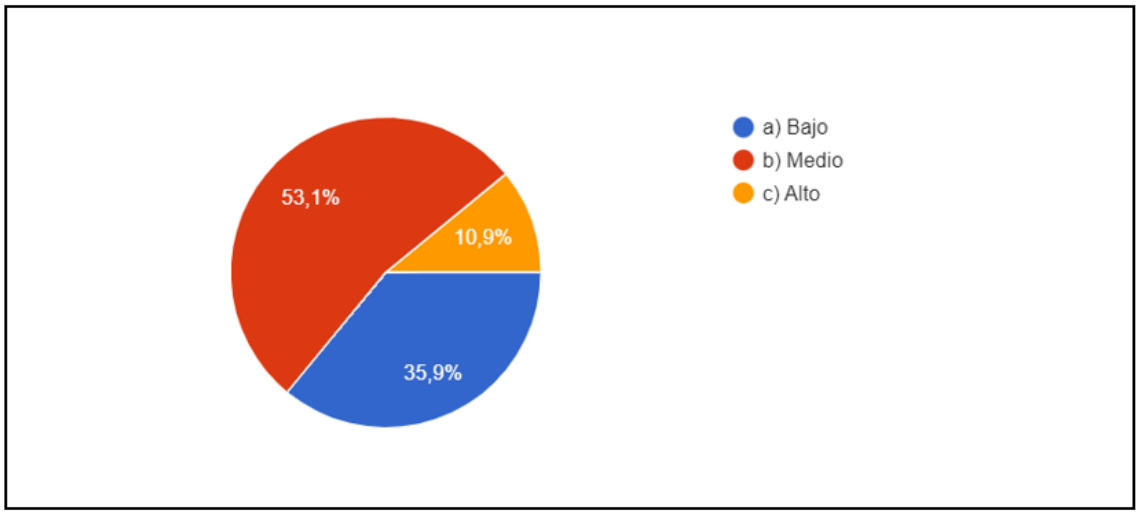
Pregunta 14: Su empleador realiza capacitación para la protección de datos médicos.



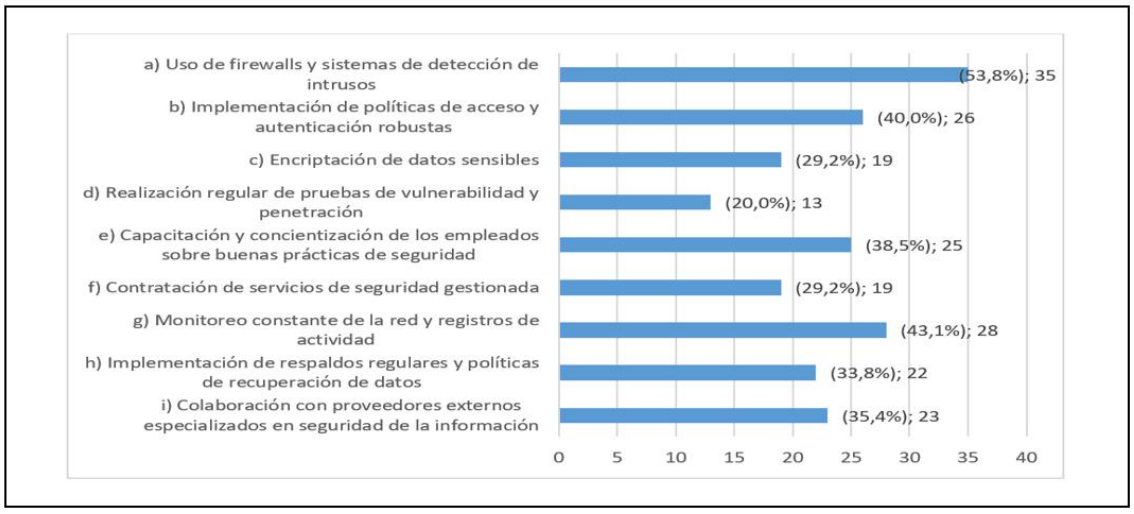
Pregunta 15: Considera que su empleador está comprometido en la mejora continua con la seguridad de los datos médicos.



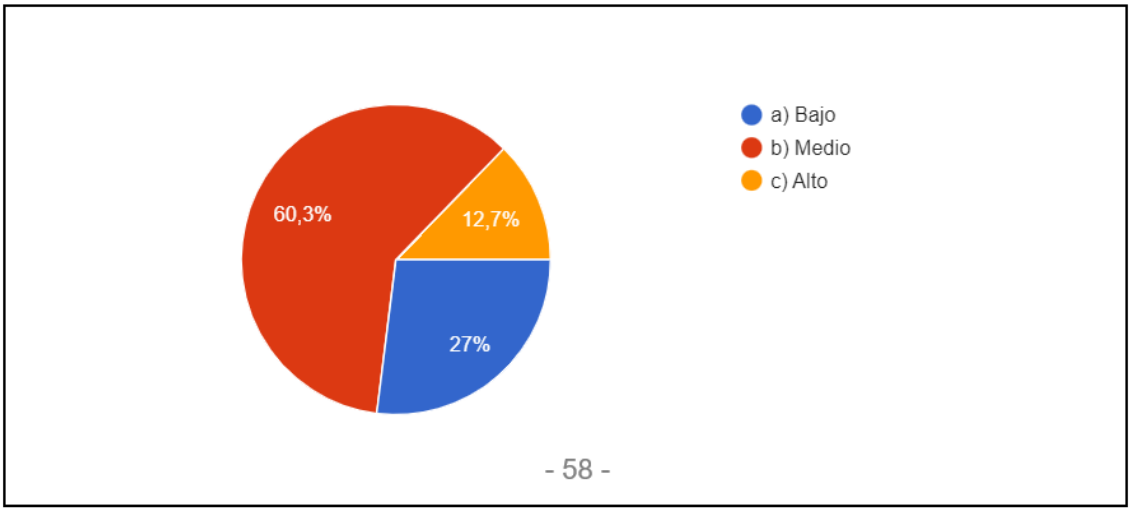
Pregunta 16: ¿Qué tan preparado está su empleador para hacer frente a posibles ataques a los datos médicos?



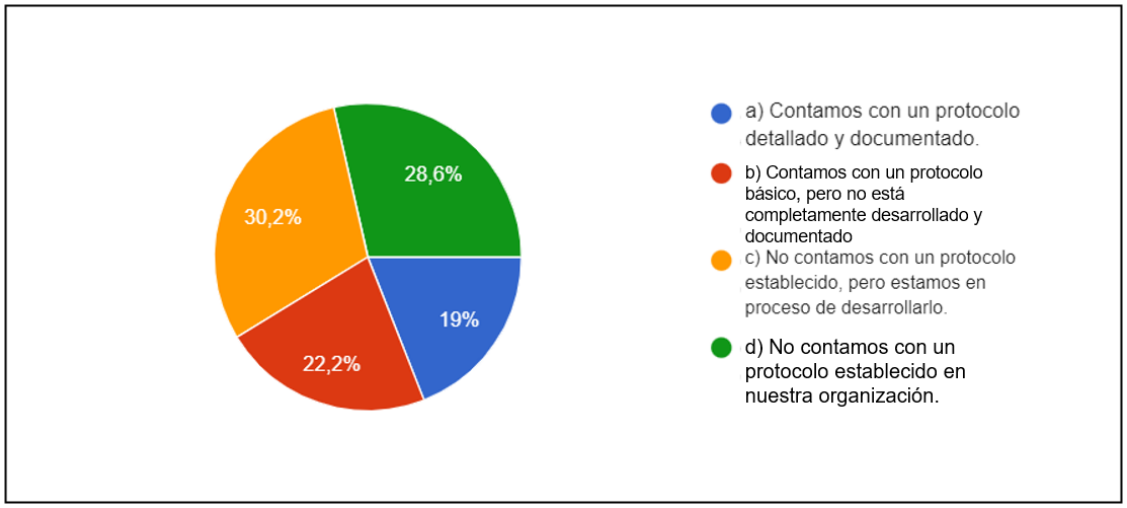
Pregunta 17: ¿Cuál de estas medidas de protección que permiten prevenir y mitigar posibles ataques a los datos médicos usted conoce que se implementó en su empleador? (Seleccione las medidas que conoce, pueden ser varias opciones)?



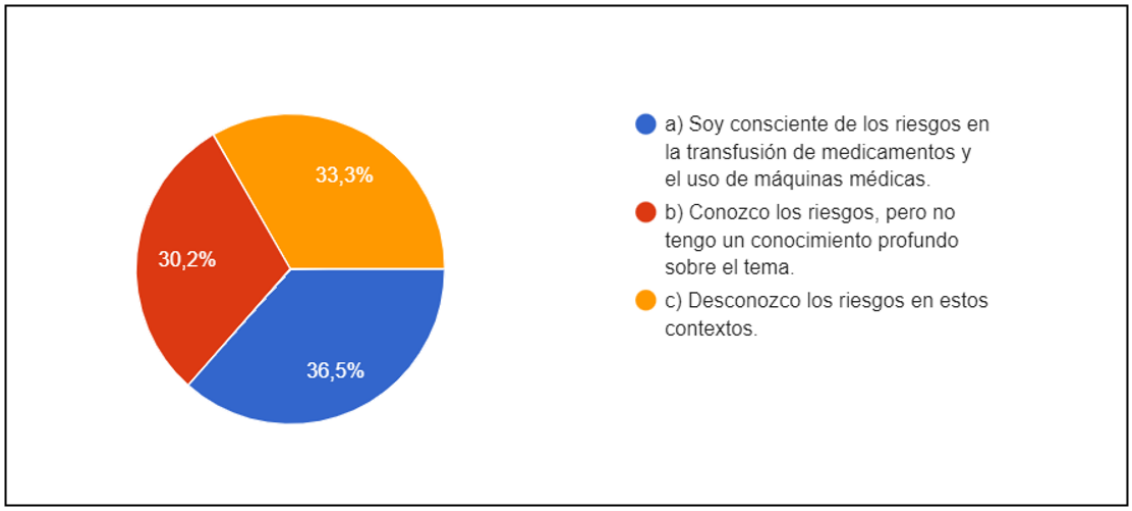
Pregunta 18: ¿En qué parámetro considera que las medidas para proteger y prevenir de posibles ataques a los datos médicos propuestas por su empleador son satisfactorias?



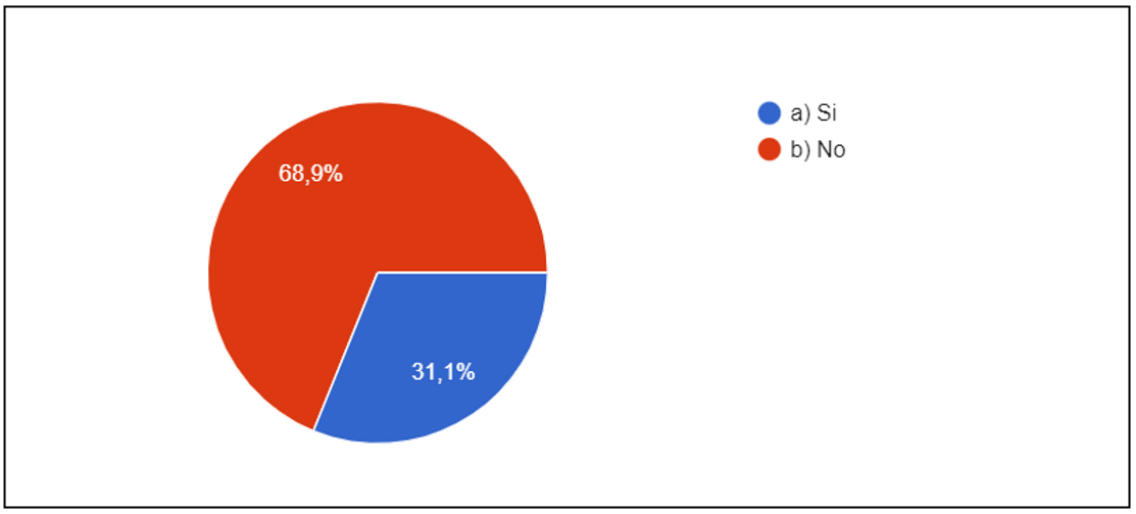
Pregunta 19: ¿Conoce usted si su empleador cuenta con un protocolo formal establecido para responder a posibles ataques de ciberseguridad, de acuerdo, a los siguientes puntos?



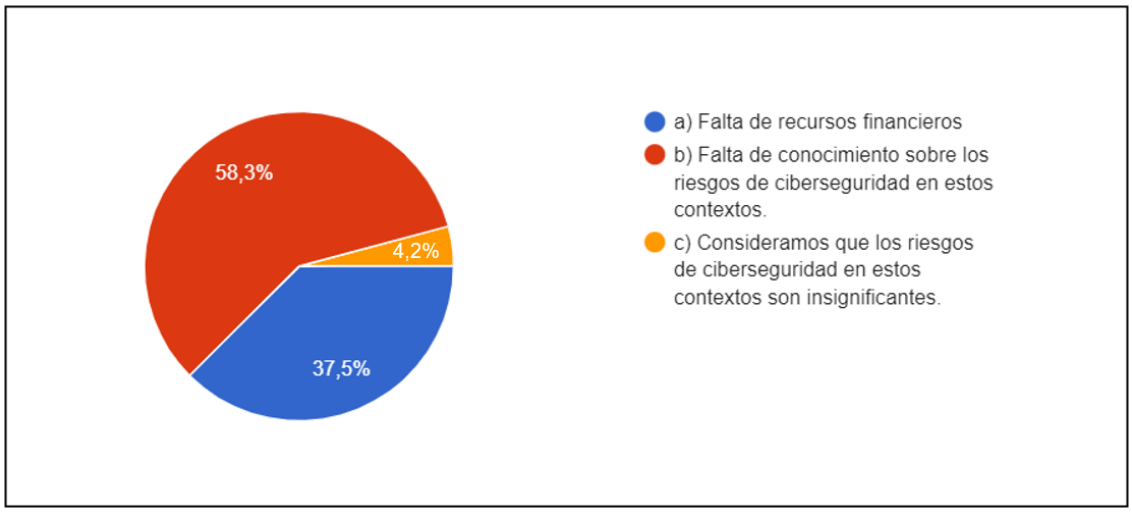
Pregunta 20: Los ataques de ciberseguridad afectan las transfusiones de medicamentos y el funcionamiento de las máquinas médicas. ¿Qué opción considera más aceptable?



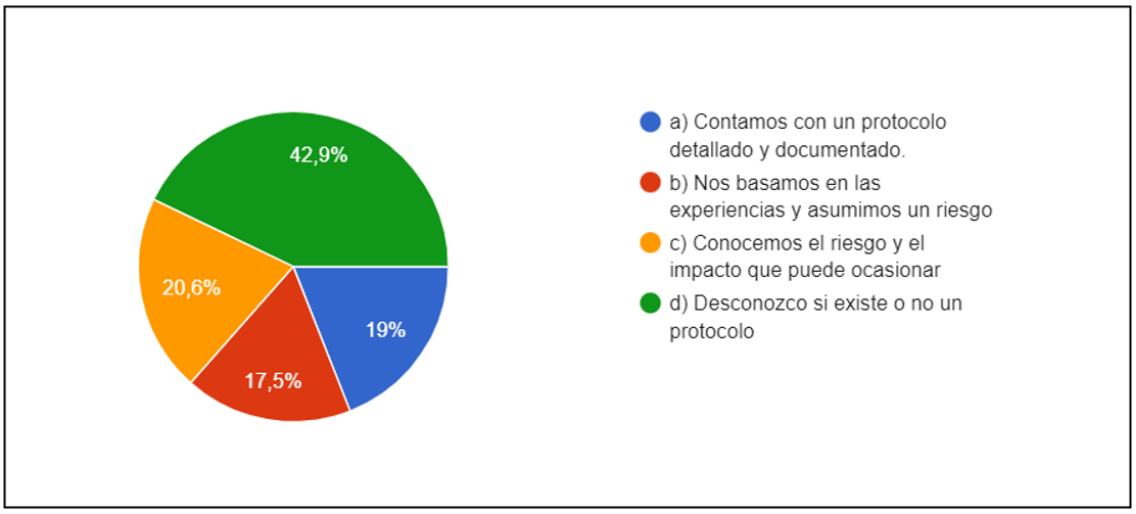
Pregunta 21: ¿Su empleador cuenta con un protocolo establecido para controlar y prevenir ataques de ciberseguridad en la transfusión de medicamentos y el uso de máquinas médicas?



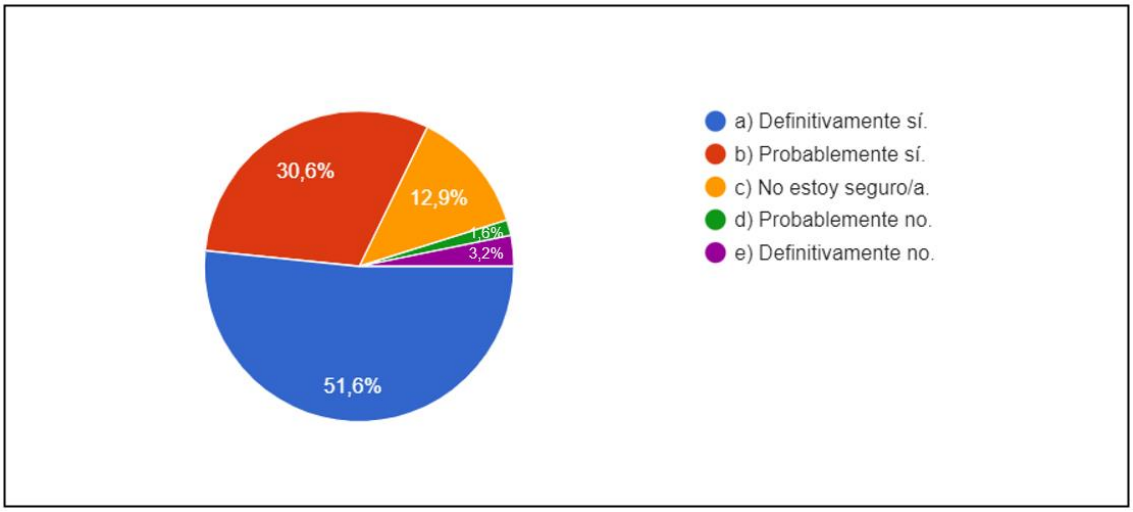
Pregunta 22: Si la respuesta es "No", escoja de las siguientes opciones el por qué no se implementa un protocolo:



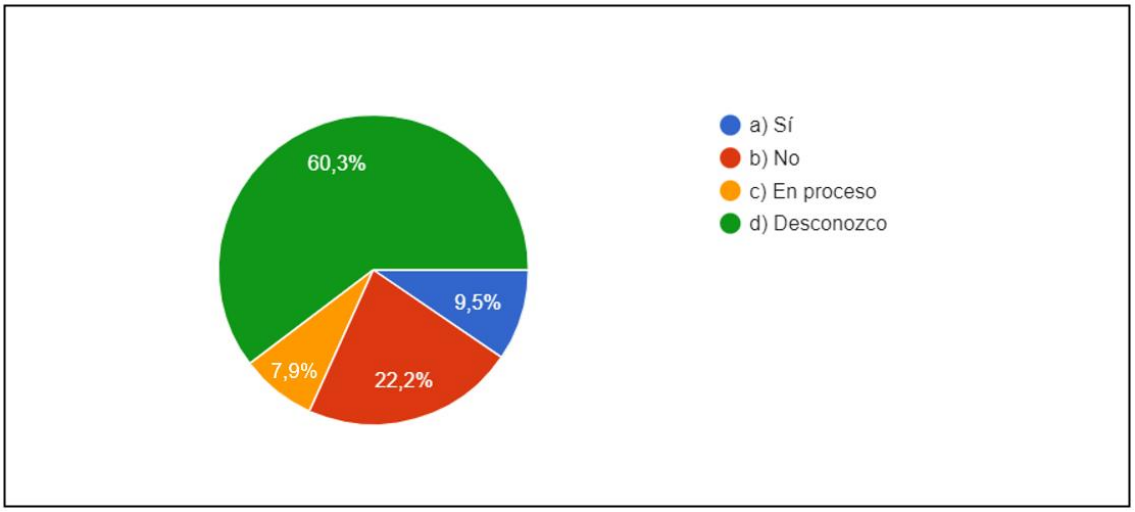
Pregunta 23: ¿Existe un protocolo de evaluación de riesgo para controlar y prevenir ataques de ciberseguridad en la transfusión de medicamentos y el uso de máquinas médicas en su empleador?:



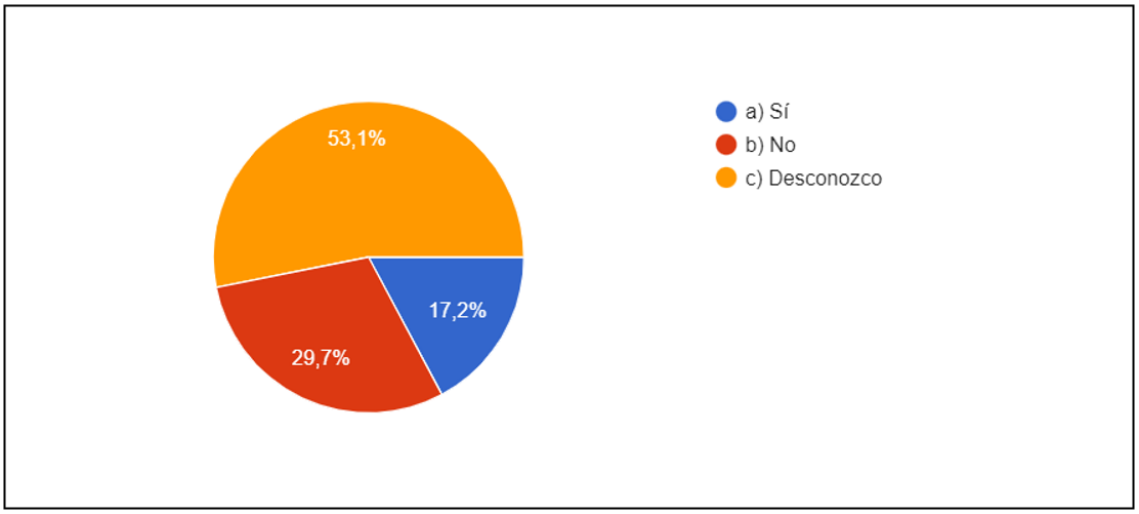
Pregunta 24: Considera que su empleador debería aplicar la norma ISO/IEC 27110:2021 para desarrollar las directrices y obtener un marco de ciberseguridad que mejore la seguridad de los datos médicos?:



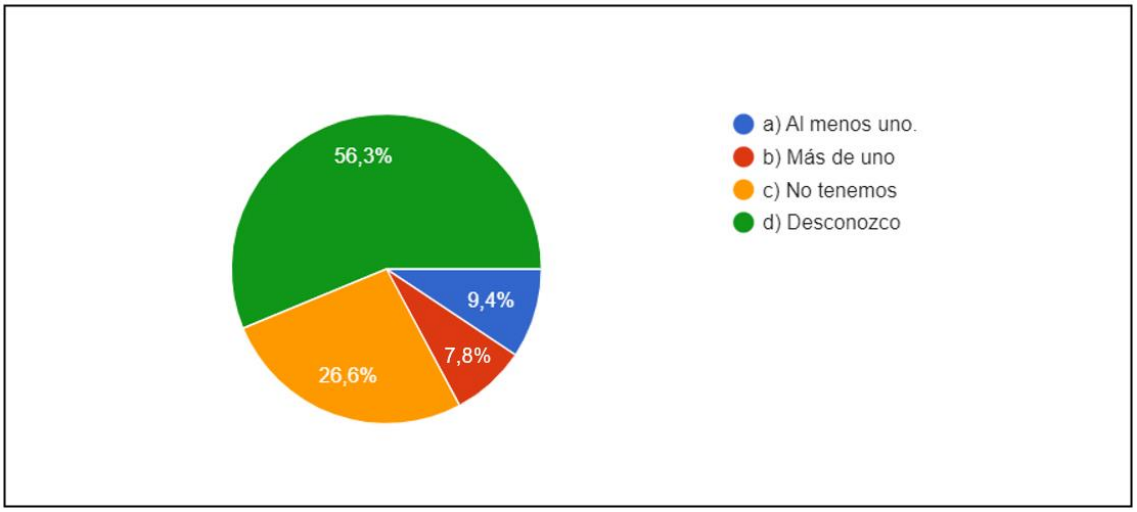
Pregunta 25: Su empleador cuenta con alguna certificación ISO de ciberseguridad, como por ejemplo ISO 27001, ISO 27701 u otras relacionadas?:



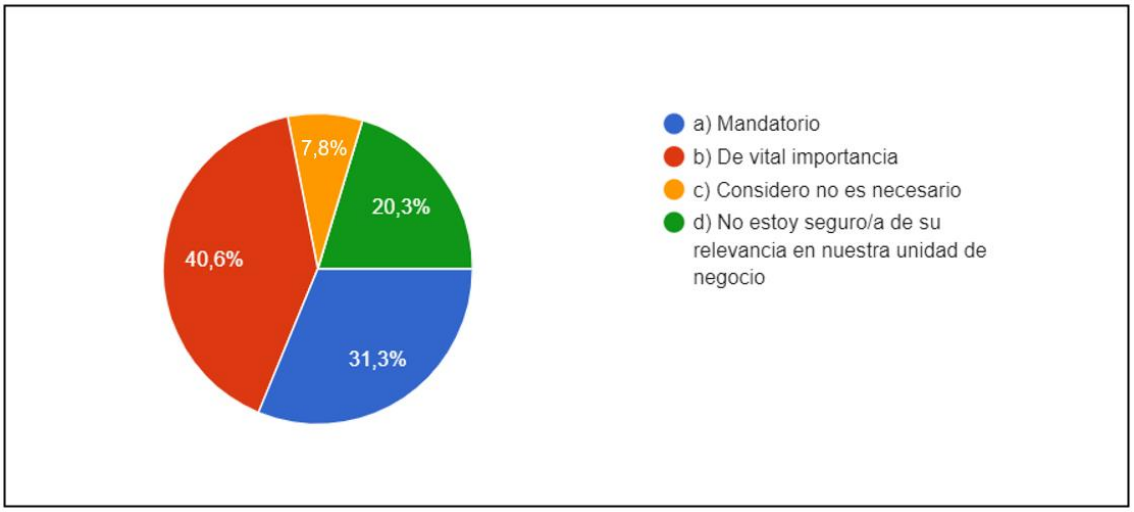
Pregunta 26: ¿Considera que su empleador aplica Sistemas de Gestión de Seguridad de la Información (SGSI) para el control y protección de la seguridad de los datos médicos?:



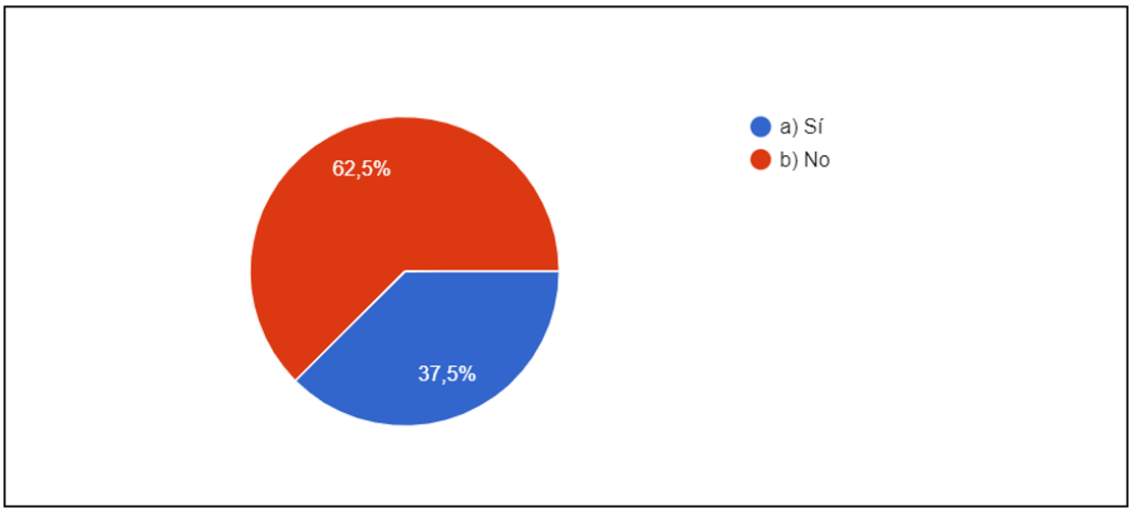
Pregunta 27: ¿En su unidad de negocio existe uno o varios colaboradores que cuenten con certificación en seguridad de la información ISO 27001?:



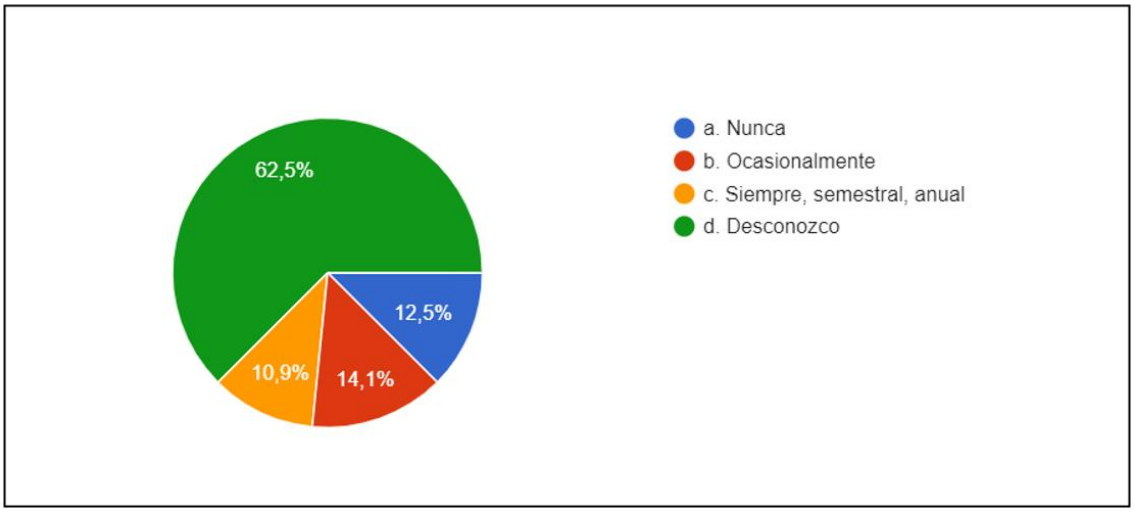
Pregunta 28: Es importante tener uno o varios colaboradores con certificación en Seguridad de la Información - ISO 27001 dentro de su unidad de negocio y/o empleador?:



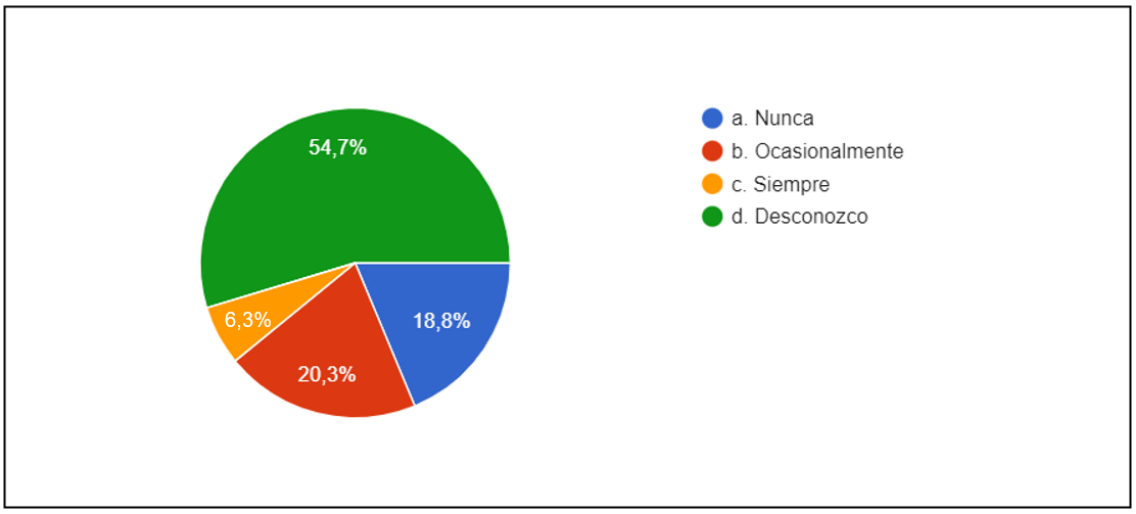
Pregunta 29: ¿Conoce algún problema reciente o actual relacionado con la vulnerabilidad de la pérdida, robo, ataque, amenaza, vulnerabilidad, impacto, etc…de la seguridad de los datos médicos?:



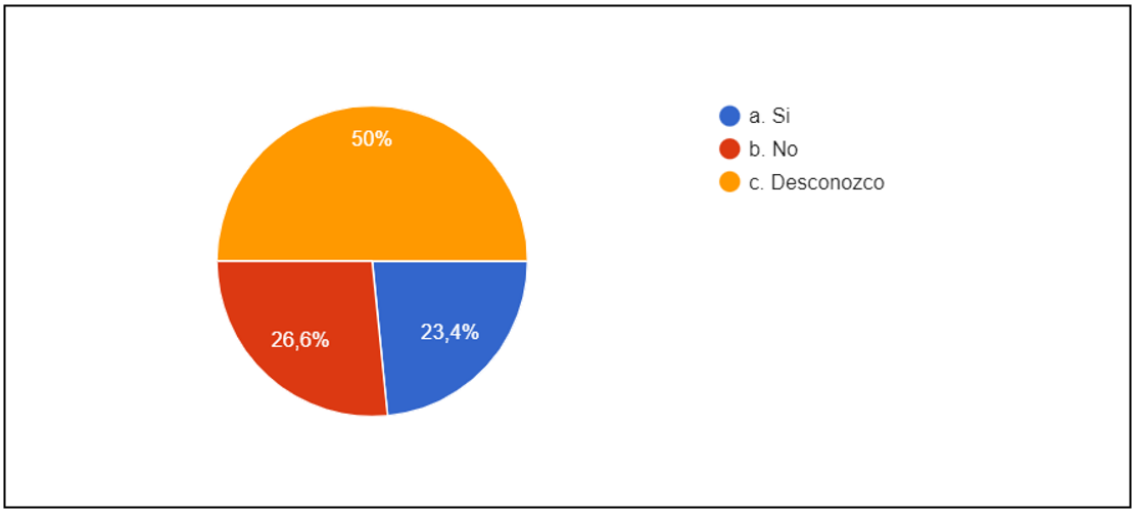
Pregunta 30: ¿Conoce si realizan auditorias regulares de seguridad de la información en su empleador para evaluar el cumplimiento de los estándares y normas establecidos?:



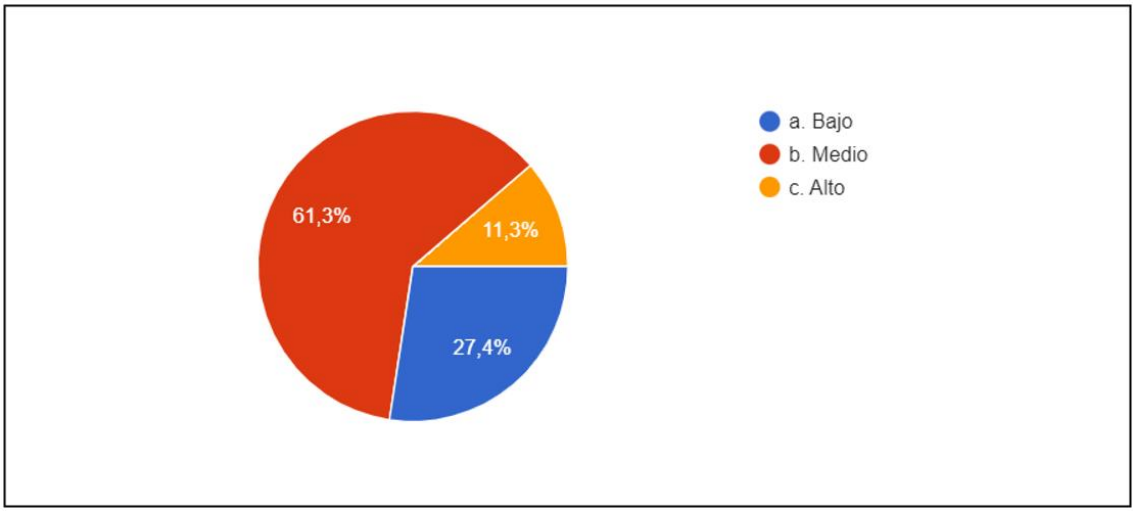
Pregunta 31: ¿Con qué frecuencia se realizan evaluaciones periódicas de vulnerabilidad y pruebas de penetración para identificar posibles brechas de seguridad en los sistemas y aplicaciones de su empleador?:



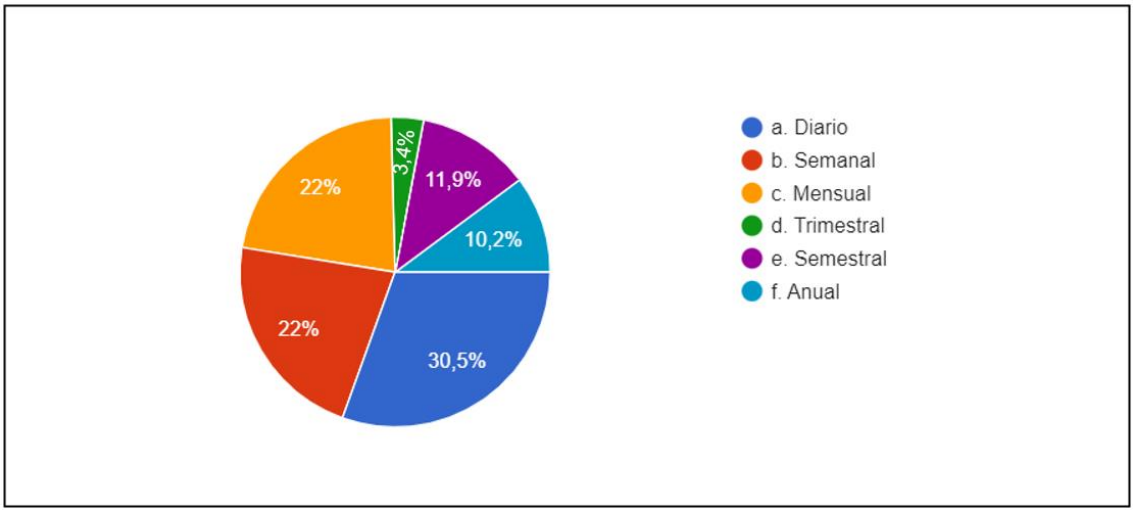
Pregunta 32: ¿Tiene su empleador un equipo dedicado a la seguridad de la información que se encargue de gestionar, supervisar, prevenir, informar aspectos relacionados con la seguridad de la Información?:



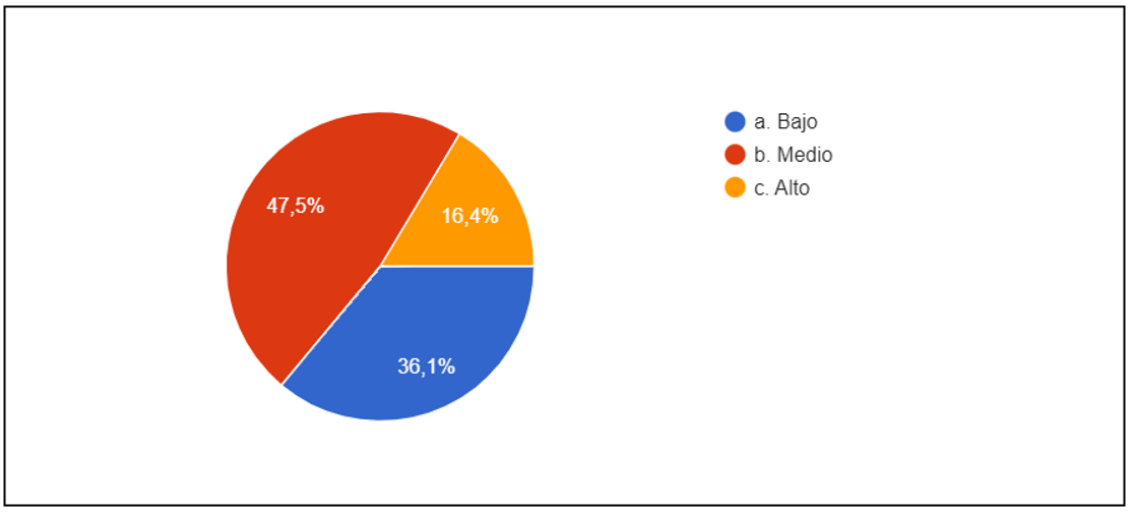
Pregunta 33: ¿En qué nivel se implementan medidas de control de acceso físico y lógico para proteger los activos críticos y los sistemas de información de su organización?:



Pregunta 34: ¿Conoce con qué frecuencia se realizan copias de seguridad de las bases de datos de su empleador para garantizar la disponibilidad y recuperación de la información en caso de una pérdida, robo, ataque, amenaza, vulnerabilidad, impacto, etc…de la seguridad de los datos?:



Pregunta 35: Conoce en qué nivel se implementan medidas de seguridad adicionales, como: monitoreo de seguridad en tiempo real, detección de intrusos y análisis de comportamiento, para identificar y responder de manera proactiva a las amenazas pérdida, robo, ataque, amenaza, vulnerabilidad, impacto, etc… a la seguridad de los datos médicos?:


47,5%
16,4%
36,1%
a. Bajo
b. Medio
c. Alto