UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

Resolución: RPC-SO-02-No.053-2021

PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGISTER

Título del proyecto:
Guía de ciberseguridad para la protección de datos sensibles en clínicas de salud aplicando normas Hippa
Línea de Investigación:
Ciencias de la ingeniería aplicadas a la producción, sociedad y desarrollo sustentable
Campo amplio de conocimiento:
Tecnologías de la información y la comunicación (TIC)
Autor/a:
Carlos Augusto López Pazmiño
Tutor/a:
PhD. Renato M. Toasa PhD. Maryory Urdaneta

Quito – Ecuador

2025

APROBACIÓN DEL TUTOR

Yo, **Renato M. Toasa** con C.I: **1804724167** en mi calidad de Tutor del proyecto de investigación titulado: GUÍA DE CIBERSEGURIDAD PARA LA PROTECCIÓN DE DATOS SENSIBLES EN CLÍNICAS DE SALUD APLICANDO NORMAS HIPPA.

Elaborado por: **Carlos augusto López Pazmiño**, de C.I: **1718935750**, estudiante de la Maestría: Seguridad Informática, de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., marzo de 2025

Firmado electrónicamente por:
RENATO MAURICIO
TOASA GUACHI

_____

Firma

APROBACIÓN DEL TUTOR

Yo, **Maryory Urdaneta** con C.I: **1759316126** en mi calidad de Tutor del proyecto de investigación titulado: GUÍA DE CIBERSEGURIDAD PARA LA PROTECCIÓN DE DATOS SENSIBLES EN CLÍNICAS DE SALUD APLICANDO NORMAS HIPPA.

Elaborado por: **Carlos augusto López Pazmiño**, de C.I: **1718935750**, estudiante de la Maestría: Seguridad Informática, de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., marzo de 2025

MARYORY URDANETA HERRERA

Firmado digitalmente por MARYORY URDANETA HERRERA
Fecha: 2025.03.08 13:01:50 -05'00'

Firma

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Yo, **Carlos Augusto López Pazmiño** con C.I: **1718935750**, autor/a del proyecto de titulación denominado: GUÍA DE CIBERSEGURIDAD PARA LA PROTECCIÓN DE DATOS SENSIBLES EN CLÍNICAS DE SALUD APLICANDO NORMAS HIPPA. Previo a la obtención del título de Magister en Seguridad Informática.

1. Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar el respectivo trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
2. Manifiesto mi voluntad de ceder a la Universidad Tecnológica Israel los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autor@ del trabajo de titulación, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital como parte del acervo bibliográfico de la Universidad Tecnológica Israel.
3. Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de prosperidad intelectual vigentes.

Quito D.M., marzo de 2025

Firmado electrónicamente por:
CARLOS AUGUSTO
LOPEZ PAZMIÑO

Firma

Tabla de contenidos

Índice de tablas

Índice de figuras

INFORMACIÓN GENERAL

Contextualización del tema

En el mundo actual, la ciberseguridad ha tenido un crecimiento significativo, por lo que se ha convertido en una preocupación primordial para las organizaciones de todos los sectores, y el sector de la salud no es la excepción. Los centros de atención médica en nuestra nación, al igual que en diversas regiones del país, gestionan volúmenes significativos de datos sensibles de los pacientes, lo que las hace un blanco deseable para los criminales cibernéticos, quienes pueden utilizar esta información para cometer el hurto de identidad, llevar a cabo estafas relacionadas con la salud o incluso realizar chantajes, tanto a las compañías prestadoras como a los pacientes.

La protección de esta información no solo es una obligación ética, sino también legal, y el incumplimiento puede acarrear graves consecuencias.

HIPAA es la Ley de Portabilidad y Responsabilidad del Seguro Médico. Esta ley estadounidense se aprobó en 1996 para garantizar la protección de los datos personales de salud, incluyendo las copias impresas y la información compartida verbal o digitalmente (Docuware, 2025).

Los ataques cibernéticos a servicios públicos, la pérdida de datos y las redes vulneradas son noticia y prioridad para los gobiernos. Esto impulsa a empresas y ciudadanos a tomar medidas, especialmente en los países más propensos a estos incidentes (Kio Tech, 2024).

En este escenario, resulta crucial implementar normativas como la HIPAA. Esta legislación estadounidense establece directrices destinadas a resguardar la información sanitaria de los pacientes. Aunque es específica de los Estado Unidos, los conceptos de confidencialidad y la defensa de datos médicos que esta norma contempla son de aplicación mundial y han influido en leyes similares en diversas clínicas ecuatorianas, reconociendo que cada nación posee su propio sistema legal de protección de datos. Para comenzar, como se ha mencionado previamente, los sistemas de información en el sector sanitario son por lo general complejos y abarcan varias disciplinas. Así, existen múltiples formas de poner en riesgo los principios básicos a través de diferentes plataformas o aplicaciones informáticas; por ejemplo, el historial médico digital de un paciente, los dispositivos de monitoreo asociados a este, o las numerosas aplicaciones de salud, lo que genera numerosas oportunidades para posibles ciberataques.

Ecuador cuenta con varias leyes y regulaciones que buscan proteger la privacidad de los datos médicos de sus ciudadanos, comprender como se relaciona las operaciones diarias de una

organización, realizar una contextualización analizando cómo estas tecnologías pueden enriquecer las experiencias de aprendizaje y fomentar la colaboración entre estudiantes que terminaron sus estudios y/o están cursando los mismos de esta manera poder prepararlos para un mundo laboral cada vez más digital en el ámbito de salud.

La HIPAA garantiza que las empresas traten su información médica personal con especial cuidado, encriptándola, restringiendo quién puede acceder a ella y garantizando que los sistemas que la almacenan sean seguros y se prueben continuamente. Cada vez que recibe atención médica, la HIPAA trabaja entre bastidores para mantener su PHI a salvo de los cibercriminales (THALESGROUP, 2023).

Según el informe Thales Data Threat Report (2023), entre los encuestados de los sectores de la salud y las ciencias biológicas, el error humano (76 %) es la principal causa notificada de violaciones de datos en la nube, muy por delante de la falta de MFA, la segunda más alta, con un 11 %. Para agravar los problemas, la complejidad de la gestión de la identidad y el cifrado es un problema grave. El 60 % de los encuestados del sector sanitario tiene cinco o más sistemas de gestión de claves en uso.

El 27 de diciembre de 2024, la Oficina de Derechos Civiles (OCR) del Departamento de Salud y Servicios Humanos (HHS) de los EE. UU. emitió un Aviso de propuesta de reglamentación (NPRM) para modificar la reglamentación de seguridad de la Ley de Portabilidad y Responsabilidad de Seguros Médicos de 1996 (HIPAA) a fin de fortalecer las protecciones de ciberseguridad para la información médica electrónica protegida (ePHI), que se espera que entre en vigencia el 7 de marzo de 2025 luego de un período de comentarios. La HIPAA no es una reglamentación estática. Desde su publicación original, se ha actualizado periódicamente para seguir siendo relevante (THALESGROUP, 2023).

En la actualidad no existe una herramienta que permita a las organizaciones o en la gran mayoría del sector de salud que cumplan con la normativa, sin embargo, existen empresas o proveedores que se encargan de la regulación ante las soluciones de seguridad de datos los cuales son ajustables a las normas Hippa, encargándose de proteger datos y las rutas de acceso a ellos. Lo que permite cumplir con el mayor requerimiento de seguridad.

Es posible que en 2025 se implementen nuevas regulaciones de la HIPAA, como la actualización propuesta de la Norma de Privacidad de la HIPAA, cuya norma final se debió haber aprobado hace tiempo. En enero de 2025 se propuso una actualización de la Norma de Seguridad de la HIPAA, aunque es probable que no se publique una norma final hasta 2026, en 2024 se implementaron nuevas regulaciones de la HIPAA cuando se publicó una norma final que

actualizaba la Norma de Privacidad de la HIPAA para fortalecer la privacidad de la atención de la salud reproductiva y se publicó una norma final que alineaba más estrechamente las regulaciones de la Parte 2 con la HIPAA (NUEVAS REGULACIONES DE HIPAA, 2025).

Problema de investigación

Las infracciones en la ciberseguridad pueden llevar a que los pacientes pierdan el dominio sobre sus datos personales. Esto afecta el concepto de autonomía, ya que impide que los pacientes ejerzan su derecho a gestionar quién tiene acceso a su información y de qué manera se utiliza. En las clínicas del Ecuador los beneficios claves son el fortalecimiento de confianza de los pacientes con las clínicas generando una mayor transparencia y lealtad, de esta manera se generará una mejor imagen de la clínica. Para esto se deberá incluir como prioridad los diferentes procesos internos y analizar de manera directa; como afecta el tema de seguridad al realizar las tareas y actividades basándose en la gestión de documentos hasta una toma de decisiones.

Las regulaciones HIPAA que se aplican a la investigación clínica están diseñadas para proteger la privacidad y seguridad de la información de salud de las personas y al mismo tiempo permitir el avance del conocimiento médico a través de la investigación (PAUBOX, 2024).

La importancia de las regulaciones de la normativa Hipaa sobre las investigaciones clínicas proporcionan un marco sólido para salvar la seguridad de los datos de los pacientes. Para todo esto las razones para que las normas Hipaa realicen una investigación eficaz en las clínicas de salud se basan en la garantía de confidencialidad esto se debe a que la privacidad se garantiza fácilmente con los procedimientos de consentimientos adecuados.

El consentimiento informado garantía que los pacientes estén debidamente informados sobre el uso de la información médica protegida. Brindando confianza en el aporte de sus datos personales. La ética profesional apoyada en un marco legal el cual proporciona la conducta ética garantizando que se respeten los derechos de los pacientes durante el proceso.

Objetivo general

Diseñar una guía de trabajo integral para fortalecer la ciberseguridad en clínicas de salud, asegurando la protección de datos sensibles de pacientes y el cumplimiento de normativas Hipaa.

Objetivos específicos

- Contextualizar los fundamentos teóricos sobre ciberseguridad en el sector salud, incluyendo conceptos clave, amenazas y vulnerabilidades comunes, así como el marco legal y normativo relevante, con énfasis en la ley Hipaa y otras regulaciones aplicables.
- Diagnosticar el estado actual de la ciberseguridad en clínicas de salud seleccionadas.
- Desarrollar una guía de capacitación en ciberseguridad para el personal médico y administrativo.
- Evaluar la guía de trabajo global mediante la opinión de especialistas en seguridad informática y trabajadores de la salud.

Vinculación con la sociedad y beneficiarios directos:

La siguiente guía se centra en abordar los requerimientos de seguridad de las clínicas para proteger la información sensible de cada uno de los pacientes, manteniendo la ética seguridad del personal médico y su entorno.

Los beneficiarios directos serán las clínicas de salud ya que permitirá contar con una guía que facilite la buena práctica informática y el resguardo de información sensible de los diferentes pacientes que acuden a las clínicas.

Cuando se publique la guía informativa para salvaguardar datos sensibles en centros de salud, se iniciará la difusión o replicación en las distintas clínicas con el objetivo de unificar las actividades y que estas se consideren para el beneficio de los ciudadanos y los centros de salud. Además, dado que la capacitación y la divulgación de la información posibilitan que los profesionales de la salud obtengan los conocimientos y competencias requeridas para realizar sus tareas de forma más efectiva.

Al capacitar al equipo médico sobre los procedimientos y protocolos fijado por las normas Hippa para la buena práctica médica y de manera ética en las clínicas, se refuerza la claridad y confianza hacia los pacientes. El personal médico estará listo para aplicar los temas de ética y responsabilidad en la seguridad de la información sensible de los pacientes lo que contribuirá a generar confianza permanente en ellos.

La formación puede abarcar elementos vinculados al registro, atención y servicio al usuario. Esto contribuye a establecer una cultura al servicio y dedicación en los pacientes. Ofreciendo una interacción significativa con las clínicas tanto en el momento del registro de información sensible como posteriormente. Esto crea una confianza directa y minimiza la posibilidad de

desconfianza entre los pacientes, además de mejorar el uso de los recursos disponibles en beneficio de los pacientes, las clínicas y el Ecuador.

Los beneficiarios directos serán los pacientes, personal sanitario, clínicas y hospitales. Ya que contarán con directrices que permitirán la implementación de las medidas de ciberseguridad; el personal recibirá una formación sobre las prácticas seguras respecto al manejo de datos. Dejando de esta manera a los pacientes como beneficiarios inmediatos quienes palparán una mejora en la protección de sus datos y manejo de su información.

CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

1.1 Contextualización general del estado del arte

HIPAA es fundamental para fomentar la adopción de procesos estandarizados dentro de la industria de la salud para proteger la información almacenada electrónicamente sobre el estado de salud, el tratamiento y el pago de un individuo (SAILPOINT, 2025).

En el área de salud es fundamental que se garantice la privacidad de la información electrónica de los pacientes para ayudar a proteger los historiales médicos, para ello se han creado leyes federales que establecen una serie de estándares normativos que se deben aplicar por las empresas y organizaciones. Una de ellas es la HIPAA (Fuentes, 2024).

Las normas HIPAA establecen una serie de principios y directrices que pueden ayudar a las clínicas a proteger la información de los pacientes. A pesar de los desafíos que existen, las clínicas de salud en Ecuador pueden beneficiarse enormemente de la aplicación y guía de normas HIPAA. Algunos de los aspectos más importantes de HIPAA incluyen:

En privacidad establece los estándares de protección de datos de salud, incluyendo cómo se puede utilizar y divulgar esta información.

Cualquier centro de cuidado de la salud, proveedores de servicios de atención y planes de salud o seguro médico que transmitan vía electrónica una información médica deben velar por el cumplimiento de la HIPAA (Fuentes, 2024).

En seguridad establece los estándares de protección de datos de salud electrónica de los pacientes, incluyendo la implementación de medidas de seguridad técnicas, administrativas y físicas.

En la parte ética y profesional ante violación de datos sensibles de los pacientes se requiere que las clínicas de salud notifiquen a los pacientes y a las autoridades en caso de una violación de la seguridad de la información.

La implementación de HIPAA puede ser un proceso complejo, y al adoptar los principios y directrices de HIPAA, las clínicas pueden fortalecer su protección de la información del paciente y reducir su riesgo de sufrir un ciberataque.

Además de HIPAA, existen otras normas y estándares internacionales que pueden ser útiles para las clínicas de salud en Ecuador, como la ISO 27001 que ayudan también a empresas a proteger su información valiosa de diversas amenazas. La combinación de diferentes normas y

estándares puede ayudar a las clínicas a crear una estrategia de ciberseguridad integral y adaptada a sus necesidades específicas.

Personal médico

El personal médico de las clínicas tiene un papel fundamental por el cual velar, y es el cumplimiento de las normas Hippa para proteger la privacidad y seguridad de la información de registros de datos sensibles de los pacientes en todo momento, evitando divulgarla a personas no autorizadas. Por lo que el acceso a la información solo la llevará el personal autorizado previamente capacitado quien almacenará y manejará la información de salud de los pacientes ya sea de manera física o digital siguiendo los protocolos establecidos por las clínicas.

Gestión por competencias

Se enfoca en identificar y desarrollar habilidades de los empleados, para que desempeñen las funciones de manera clara y precisa. Sobre todo, porque genera una mejora continua.

Inducción Médica

En el ámbito de la salud es un proceso que permite al personal médico actualizar sus conocimientos y habilidades para ofrecer una atención de calidad, lo que se busca es mejorar la calidad de los servicios médicos manteniendo al personal médico actualizado en un entorno constante de evolución con el fin de mejorar la atención con los pacientes, enseñando habilidades interpersonales como la empatía y la escucha activa.

Características de la capacitación

- Es un proceso médico de mejora continua.
- Se basa en la necesidad de la clínica.
- Está orientado en un cambio de conocimientos.
- Se aplica evaluaciones para su retroalimentación.

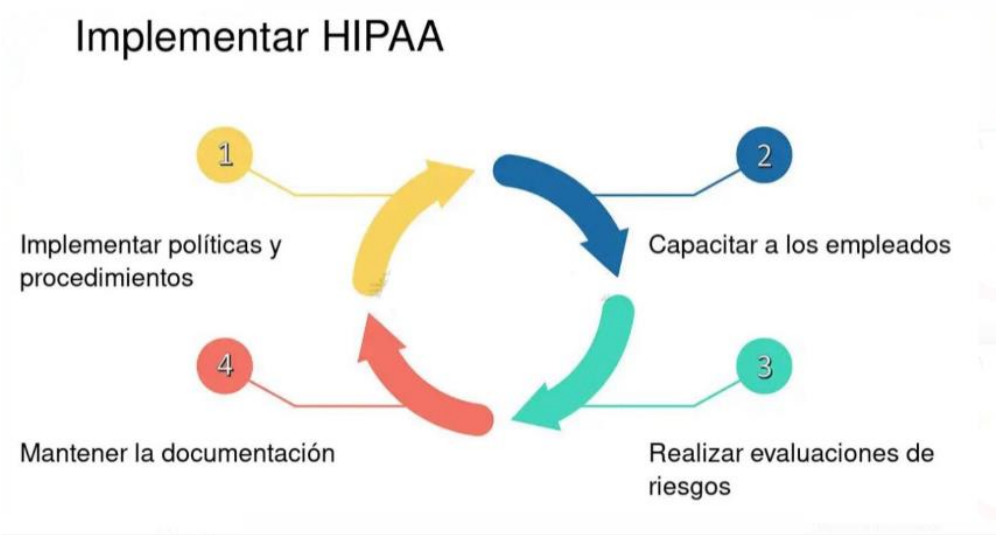
Elementos de un plan de capacitación

- Inducción al personal médico sobre las normas Hippa.
- informar los principios de salud.
- Revisar la normativa vigente.

La implementación de la ley Hipaa se representa en la siguiente figura 1.

Figura 1

Pasos para implementar Hipaa



Ley Hipaa

Según los estipulado en la sección "Normas de seguridad: Reglas generales" de la Normativa de Seguridad de HIPAA, cada centro que esté sujeto a esta orden tiene que:

- Asegurar que la información personal necesaria sea creada, recibida, mantenida o enviada con su confidencialidad, integridad y acceso garantizados.
- Resguardar contra cualquier riesgo y amenaza que se pueda prever razonablemente para la seguridad o integridad de EPHI; y
- Defenderse de usos o revelaciones que se puedan anticipar y que no estén autorizados por la Regla de Privacidad.
- La privacidad se define como "la característica que asegura que los datos o la información no son accesibles ni divulgados a individuos o procesos sin autorización".
- La autenticidad se describe como "la característica que garantiza que los datos o la información no han sido modificados o eliminados de forma no permitida".
- La accesibilidad se considera "la característica que asegura que los datos o la información están al alcance y son utilizables cuando lo solicita una persona autorizada".

Marco para la Gestión del Riesgo

La normativa de seguridad de HIPAA trata sobre la necesidad de establecer una gestión adecuada de riesgos para salvaguardar de manera eficiente la EPHI. La identificación, exámen y administración del riesgo forman la base de los esfuerzos de conformidad de la normativa de seguridad de una entidad cubierta.

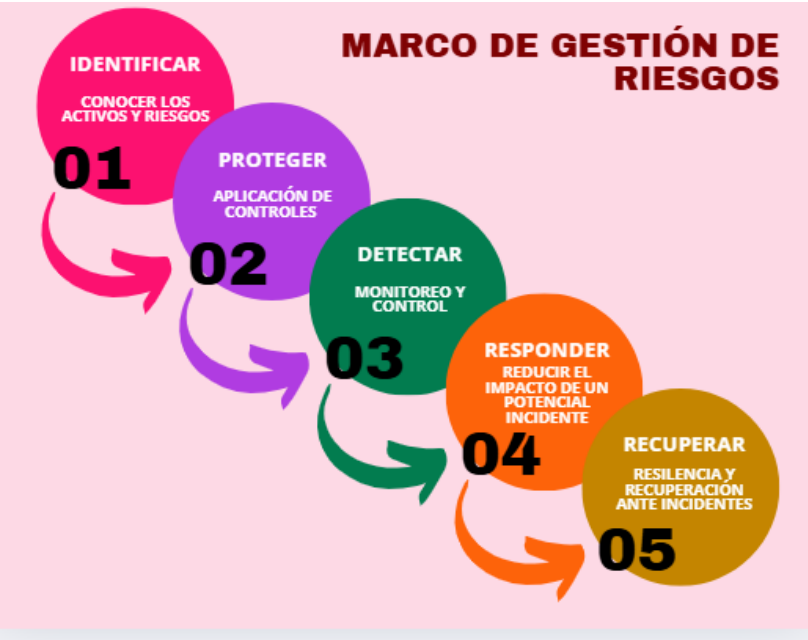
Funcionando como herramientas para crear y sostener la estrategia de una entidad cubierta para asegurar la privacidad, integridad y disponibilidad de la EPHI.

Las entidades cubiertas deben adoptar medidas de seguridad que sean razonables y adecuadas para protegerse frente a amenazas o vulnerabilidades previsibles que puedan comprometer la seguridad de la EPHI. Conforme a la normativa de seguridad, estas entidades están obligadas a evaluar los riesgos y vulnerabilidades presentes en sus ambientes y a establecer controles de seguridad para mitigar dichos riesgos y vulnerabilidades.

La gestión de riesgos se considera un componente fundamental del programa de seguridad de información de la organización, proporcionando un marco efectivo para elegir los controles de seguridad apropiados para un sistema de información: los controles necesarios para proteger a las personas y los activos y operaciones de la entidad. Esta explicación se la puede visualizar en la figura 2.

Figura 2

Marco de gestión de riesgos

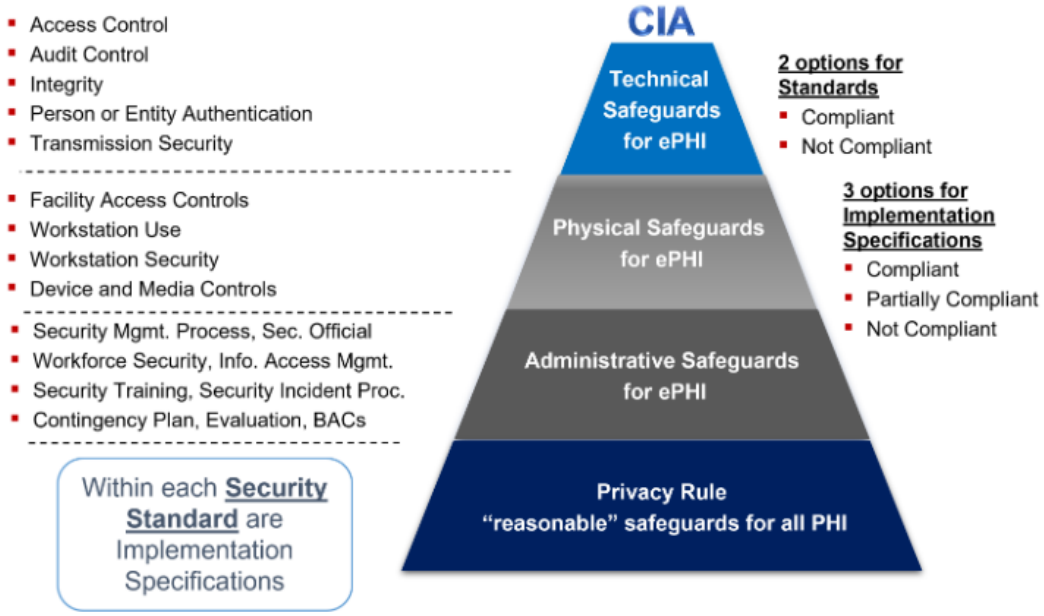


Normas en la seguridad Hipaa

La regulación de Seguridad de la HIPAA determina los criterios y los requisitos de aplicación que las entidades deben respetar para alinearse con la normativa. Todas las entidades, a excepción de los pequeños planes de salud, que manejen, conserven, archiven o transmitan datos que sirvan para identificar a los pacientes tienen la obligación legal de cumplir con los Criterios de Seguridad de la HIPAA, para esto en la figura 3 se reflejan los requisitos de las reglas de privacidad y seguridad.

Figura 3

Requisitos de salvaguarda de las reglas de privacidad y seguridad



Nota: (HIPAA ACADEMY, 2025)

El Modelo de CIA, también conocido como la Triada CIA, representa un enfoque fundamental para gestionar y sincronizar las técnicas de defensa cibernética. Este método se basa en tres principios esenciales: Protección, Lealtad y Disponibilidad. Cada uno de estos principios es crucial en cualquier plan sólido de defensa en el ámbito digital la cual se representa en la figura 4.

Figura 4

Triada de la CIA

Nota: (WALLARM, 2025)

La tabla 1 presenta información de los estándares de garantías administrativas para la normativa Hipaa.

Tabla1

Estándares de garantías administrativas

Normas	**"Especificaciones de implementación"** (HIPAA ACADEMY, 2025)**.**	**R = Requerido**
		A = Direccionable
Proceso - Gestión de Seguridad	**"Análisis de riesgos"** (HIPAA ACADEMY, 2025)**.**	**R**
	"Gestión de riesgos" (HIPAA ACADEMY, 2025)**.**	**R**
	"Política de sanciones" (HIPAA ACADEMY, 2025)**.**	**R**
	"Revisión - actividad del sistema de información" (HIPAA ACADEMY, 2025)**.**	**R**
Responsabilidad de seguridad asignada		**R**

Seguridad - En la fuerza laboral	**"Autorización y/o Supervisión"** (HIPAA ACADEMY, 2025)**.**	**A**
	"Procedimiento de autorización de personal" (HIPAA ACADEMY, 2025)**.**	**A**
	"Procedimientos de terminación" (HIPAA ACADEMY, 2025)**.**	**A**
Gestión de acceso a la información	**Aislamiento de la función de centro de intercambio de información sobre atención sanitaria**	**R**
	Autorización de acceso	**A**
	Establecimiento y modificación de acceso	**A**
Concientización y capacitación en seguridad	**"Recordatorios de seguridad"** (HIPAA ACADEMY, 2025)**.**	**A**
	"Protección contra software malicioso" (HIPAA ACADEMY, 2025)**.**	**A**
	"Monitoreo de inicio de sesión" (HIPAA ACADEMY, 2025)**.**	**A**
	"Gestión de contraseñas" (HIPAA ACADEMY, 2025)**.**	**A**

Procedimientos en caso de incidentes de seguridad	**Respuesta y presentación de informes**	**R**
Plan de contingencia	**"Plan de respaldo de datos"** (HIPAA ACADEMY, 2025)**.**	**R**
	"Plan - recuperación ante desastres" (HIPAA ACADEMY, 2025)**.**	**R**
	"Plan - operación en modo de emergencia" (HIPAA ACADEMY, 2025)**.**	**R**
	"Procedimiento de prueba y revisión" (HIPAA ACADEMY, 2025)**.**	**A**
	"Análisis de criticidad de datos y aplicaciones" (HIPAA ACADEMY, 2025)**.**	**A**
Evaluación		**R**
Contratos comerciales y otros acuerdos	**Contrato escrito u otro acuerdo**	**R**

La tabla2 presenta información de los estándares de protección física de la normativa Hipaa.

Tabla 2

Estándares de protección física

Normas	**Especificaciones de implementación**	**R= Requerido** **A = Direccionable**
Controles de acceso en instalaciones	**"Operaciones de contingencia"** (HIPAA ACADEMY, 2025)	**A**

	"Plan de seguridad de las instalaciones" (HIPAA ACADEMY, 2025)	**A**
	"Procedimientos- control de acceso y validación" (HIPAA ACADEMY, 2025)	**A**
	"Registros de mantenimiento" (HIPAA ACADEMY, 2025)	**A**
Uso estaciones de trabajo		**R**
Seguridad estaciones de trabajo		**R**
Controles en dispositivos y medios	**Desecho**	**R**
	Reutilización de medios	**R**
	Responsabilidad	**A**
	Copia de seguridad - almacenamiento de datos (HIPAA ACADEMY, 2025)	**A**

Riesgos Cibernéticos en el Sector Salud

Vulnerabilidades

Las instituciones de salud son especialmente vulnerables a los ciberataques debido a la gran cantidad de datos sensibles que manejan, la complejidad de sus sistemas de información y la dependencia de terceros.

Tipos de Ataques

Los ataques más comunes en el sector salud incluyen el ransomware, el phishing, los ataques de denegación de servicio y la filtración de datos.

Las principales consecuencias son la pérdida de confianza, los costos financieros, los riesgos para la salud. Al aplicar estos fundamentos teóricos al contexto ecuatoriano permitirá identificar

las vulnerabilidades específicas de la institución y evaluar el cumplimiento de la normativa nacional determinando así las áreas a las que se requiere una mejora.

En Ecuador, la aplicación de los principios de la HIPAA y de otras normativas internacionales puede contribuir a fortalecer la protección de los datos de los pacientes. Esta investigación busca aportar conocimientos y herramientas para mejorar la ciberseguridad en las clínicas ecuatorianas y garantizar la continuidad y calidad de los servicios de salud.

1.2 Proceso investigativo metodológico

El estudio que empleará es de tipo mixto; se trata de un método de investigación que abarca la recolección, el análisis y la fusión de datos cuantitativos y cualitativos. Este método se aplica cuando se necesita una comprensión más profunda del tema de investigación, algo que no podrían proporcionar individualmente estos enfoques.

Los datos numéricos abarcan detalles cerrados, como aquellos que sirven para evaluar opiniones, por ejemplo, mediante escalas de calificación. La evaluación de este tipo de información se lleva a cabo mediante un análisis estadístico de las puntuaciones obtenidas de encuestas, para abordar las interrogantes de investigación o verificar las suposiciones planteadas.

La información cualitativa consiste en datos no estructurados que normalmente son obtenidos por los investigadores a través de entrevistas y observaciones. El examen de esta información cualitativa (como palabras, textos o conductas) generalmente implica la clasificación en diferentes grupos para identificar la variedad de conceptos recopilados durante el proceso de recolección.

Al llevar a cabo una investigación que combine tanto datos numéricos como cualitativos, el investigador obtiene una visión más amplia y profunda de la comprensión y verificación, al mismo tiempo que mitiga las limitaciones de cada método de manera individual. (Questionpro, 2025)

Este tipo de investigación es aplicado, ya que se plantea recoger datos medibles referente al diseño de una guía de ciberseguridad para la protección de datos sensibles aplicando las normas HIPAA.

Población y muestra

Es el conjunto de personas u objetos de los que se desea conocer algo en una investigación. "El universo o población puede estar constituido por personas, animales, registros médicos, los nacimientos, las muestras de laboratorio, los accidentes viales entre otros". (PINEIDA, 2004)

La población se define como el grupo de todos los casos que cumplen ciertas especificaciones; esto significa que incluye el grupo de eventos y/o personas que poseen características similares y que son relevantes para el estudio del investigador.

En este contexto, la población abarca la totalidad de elementos y personas que comparten rasgos similares y son relevantes para el estudio. De hecho, en esta indagación, la población consiste en 60 individuos, que están organizados detallados en la tabla 3.

Tabla 3

Poblamiento

Estudio de Población		
Ciudadano		**Población**
Personal Médico (edad 30-50)		20
Pacientes Hombres/Mujeres (edad 18-50)		20
Pacientes adultos mayores		10
	Total	60

La muestra constituye un subconjunto de la población, la cual puede ser escogida al azar (Díaz, 2019). Para determinar la muestra se toma en cuenta la siguiente fórmula:

Para determinar la muestra se toma en cuenta la siguiente ecuación (1):

$$n = \frac{Z^2 pqN}{e^2(N-1)+Z^2 pq} \quad (1)$$

Donde:

Z= Confiabilidad

E= Margen de fallo (5%, 0.05)

N= Comunidad

n= Tamaño de la ejemplar

P= Probabilidad de que ocurra

q= Probabilidad que no ocurra

e= Error máximo aceptado

$$n = \frac{(1{,}96)^2 * 0{,}5 * 0{,}5 * 60}{(0.05)^2(60-1) + (1{,}96)^2 * 0{,}5 * 0{,}5}$$

$$n = \frac{57.624}{1{,}1079}$$

$n = 52\ personas$

Los instrumentos que serán utilizados en la investigación como ejes primordiales para demostrar los resultados son

- Entrevista
- Encuesta

1.3 Análisis de resultados

El personal médico encuestado en las diferentes casas de salud no cuenta con un guía de capacitación sobre las normas y leyes vigentes basadas en las normas Hippa; sino más bien se adaptan en permanecer pendientes a los requerimientos efectuados por parte de la entidad contratada. De la misma manera los pacientes encuestados en las diferentes casas de salud mantienen un desconocimiento general de la protección de datos que deben brindar las clínicas ya que se limitan a otorgar toda la información personal sin responsabilidad a cambio de recibir una atención médica. Por lo expuesto, se presenta una encuesta de preguntas y respuestas sobre ciberseguridad y protección de datos sensibles en clínicas de salud. Esta encuesta está orientada a evaluar el nivel de conocimiento y las prácticas de ciberseguridad dentro de las instituciones de salud, considerando la normativa HIPAA.

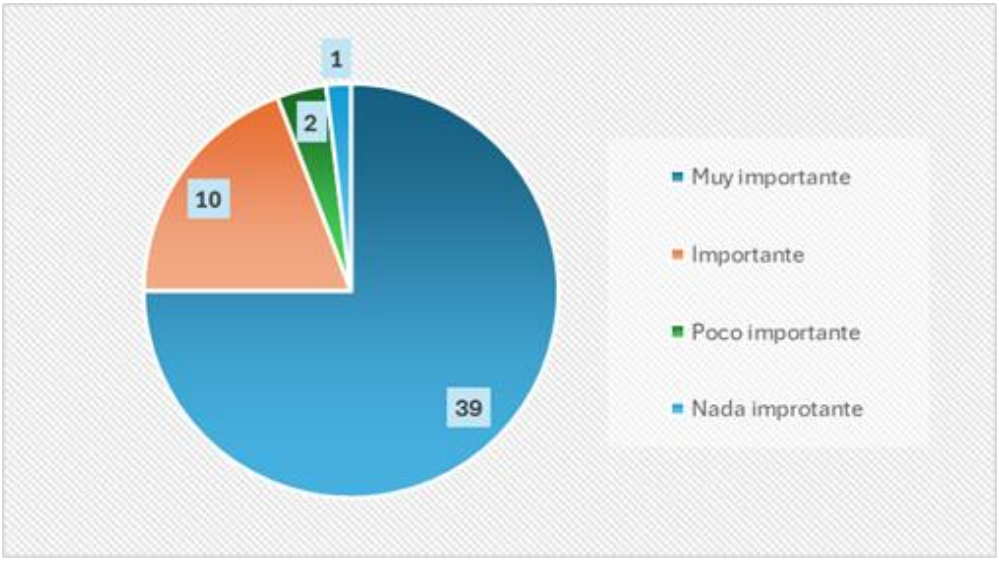
1.3.1 Análisis de encuestas realizadas

Pregunta 1. ¿Qué tan importante considera la protección de datos personales en clínicas de salud?

Según la encuesta realizada a 52 personas; 39 de ellas consideran que “es muy importante” la protección de datos en las clínicas, mientras que 10 personas opinan que es “importante”; 2 encuestados creen que es “poco importante” y el restante considera “nada importante” la protección de datos. Como se muestra en la figura 5.

Figura 5

Importancia de protección de datos

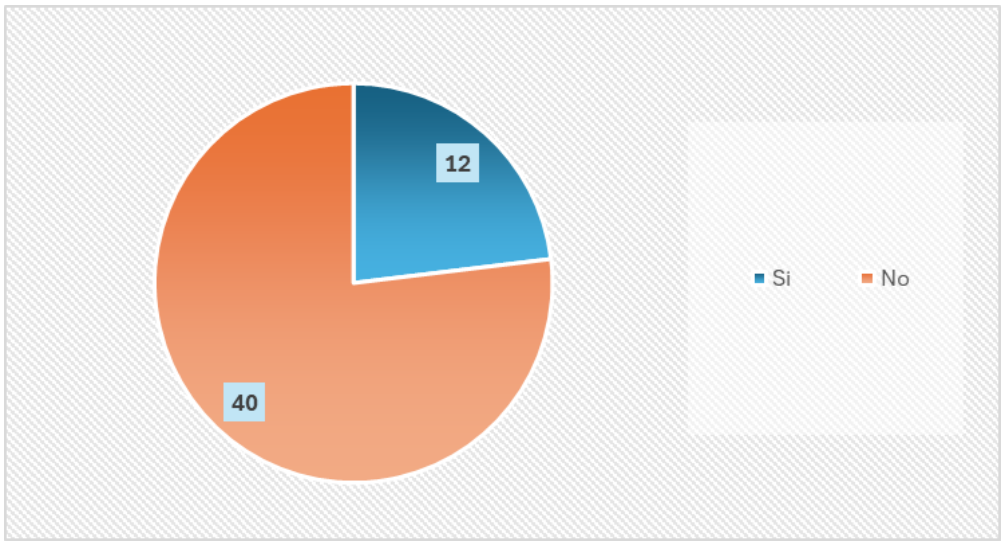


Pregunta 2. ¿Ha escuchado hablar sobre la normativa HIPAA y su relación con la protección de datos en salud?

Acorde a la encuesta ejecutada, un porcentaje de 40 personas respondieron que desconocen la normativa HIPPA, mientras que 12 encuestados están familiarizados sobre la misma. Como se muestra en la figura 6.

Figura 6

Normas Hipaa

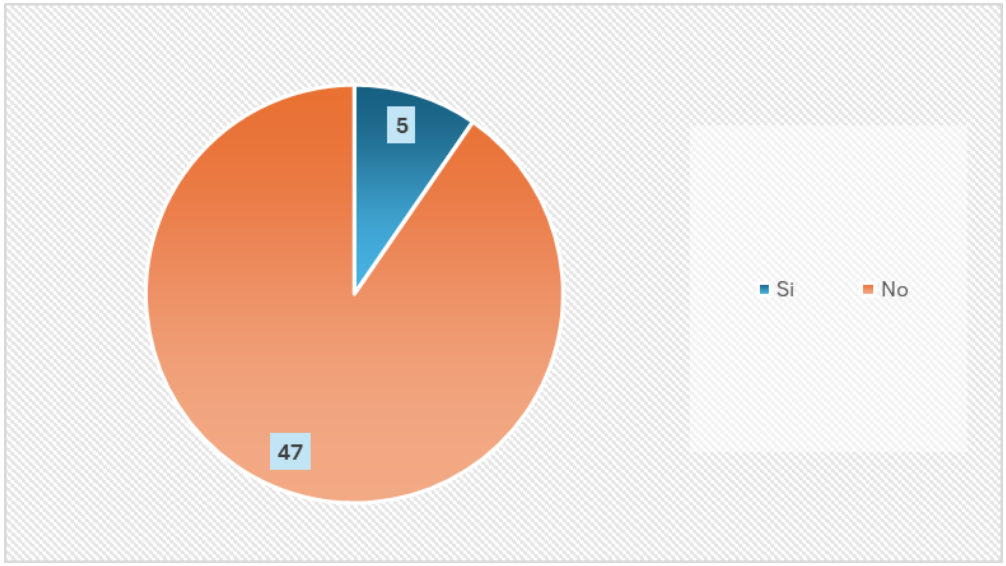


Pregunta 3. ¿Ha recibido información sobre cómo se protegen sus datos en la clínica donde trabaja o se atiende?

En base a la encuesta realizada, un total de 47 personas no han recibido información de cómo se protegen sus datos, mientras que 5 encuestados han recibido. Como se muestra en la figura 7.

Figura 7

Información sobre protección de datos

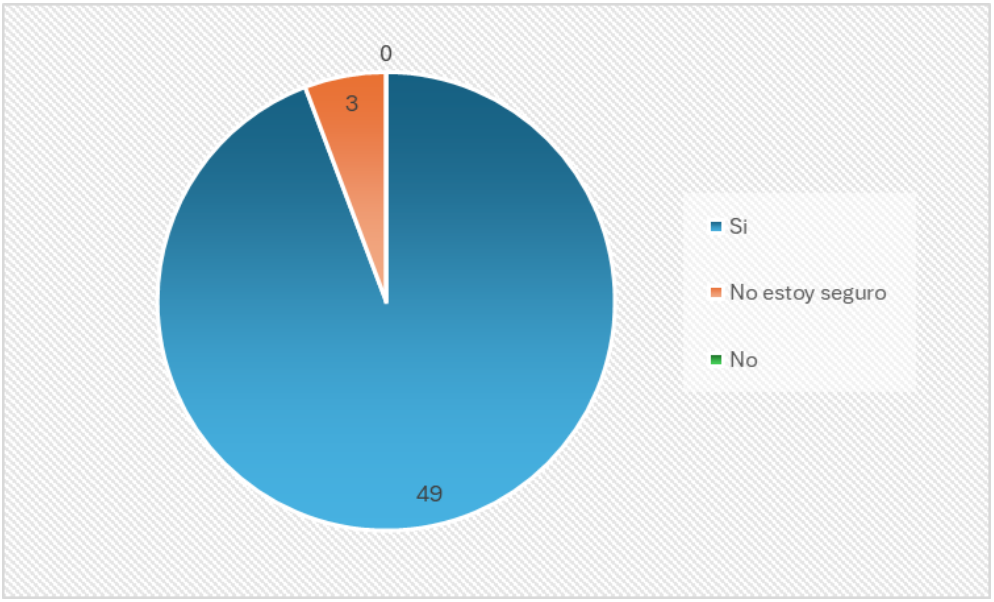


Pregunta 4. ¿Cree que las clínicas deberían mejorar sus medidas de seguridad digital?

Acorde a la encuesta ejecutada de los 52 encuestados, 49 personas mencionan que, si se debiera mejorar las medidas de seguridad, 3 personas no están seguros y ninguna persona considera lo contrario. Como se muestra en la figura 8.

Figura 8

Medidas de seguridad

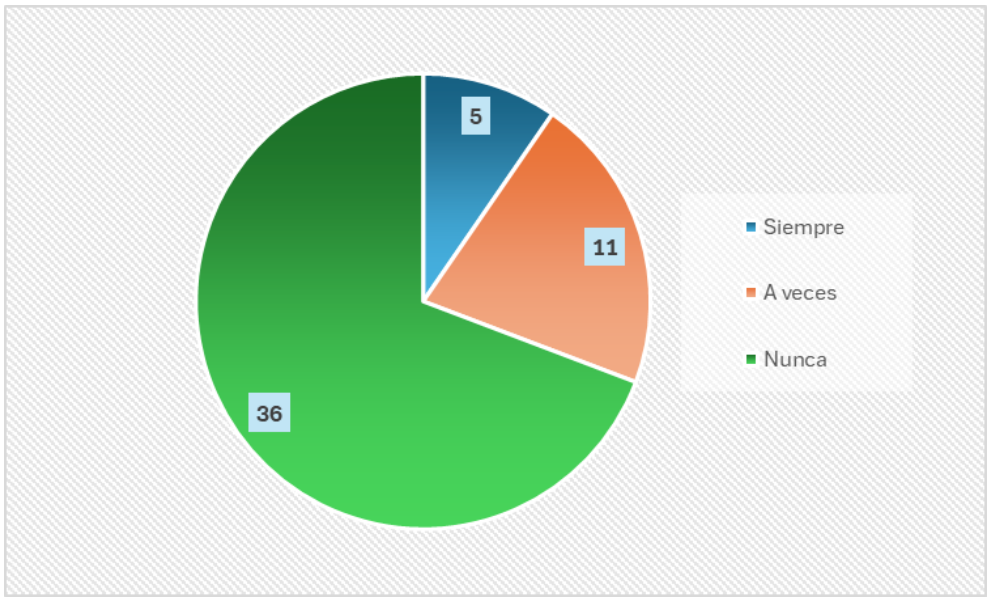


Pregunta 5. ¿Con qué frecuencia revisa las políticas de privacidad al proporcionar sus datos en una clínica?

36 personas de los 52 encuestados, nunca revisan las políticas, 11 de ellas suelen hacerlo a veces, mientras que 5 personas siempre revisan las políticas de privacidad. Como se muestra en la figura 9.

Figura 9

Metodología de capacitación

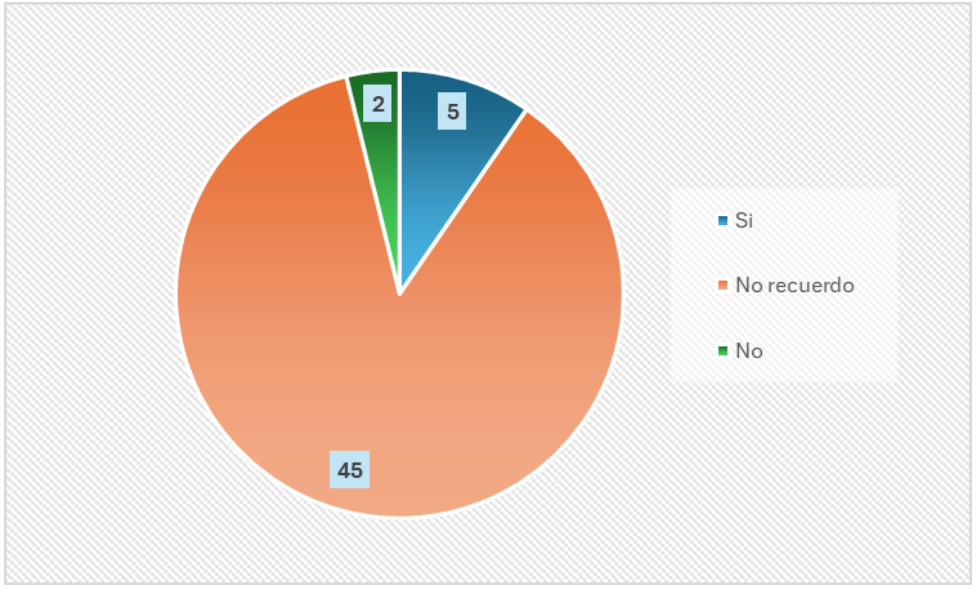


Pregunta 6. ¿Le han solicitado consentimiento para el almacenamiento y uso de su información médica en alguna clínica?

La mayoría de los encuestados (45) no recuerda si se les solicitó consentimiento para el uso de su información médica. Solo 5 personas afirman haberlo dado, mientras que 2 de los mismos aseguran que no se les pidió. Como se muestra en la figura 10.

Figura 10

Consentimiento

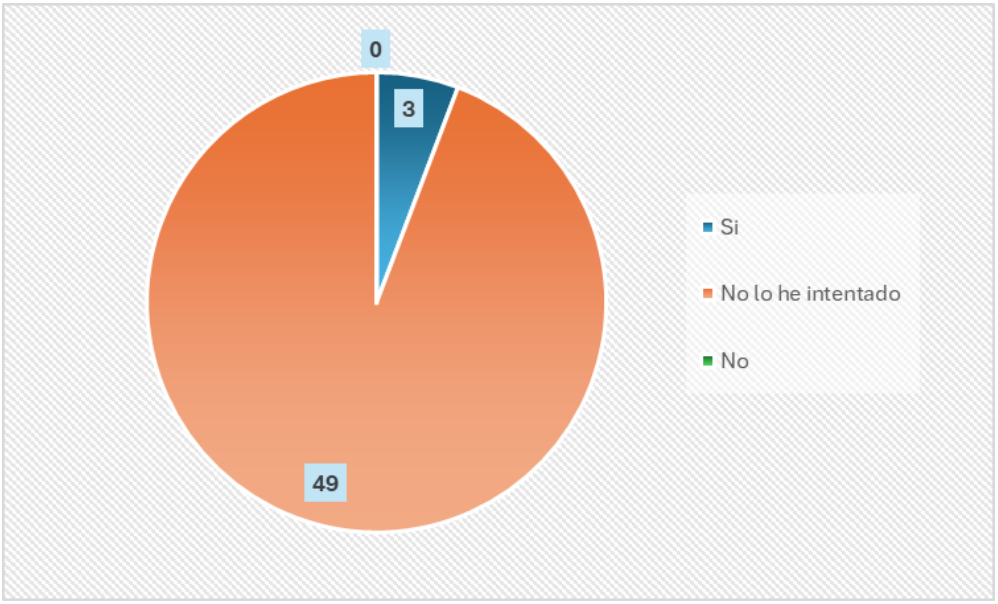


Pregunta 7. ¿Alguna vez ha tenido dificultades para acceder a su historial clínico por razones de seguridad?

Según la encuesta realizada, 49 de los 52, no ha intentado acceder a su historial, 3 tuvieron dificultades y ninguno respondió que no. Como se muestra en la figura 11.

Figura 11

Acceso a información

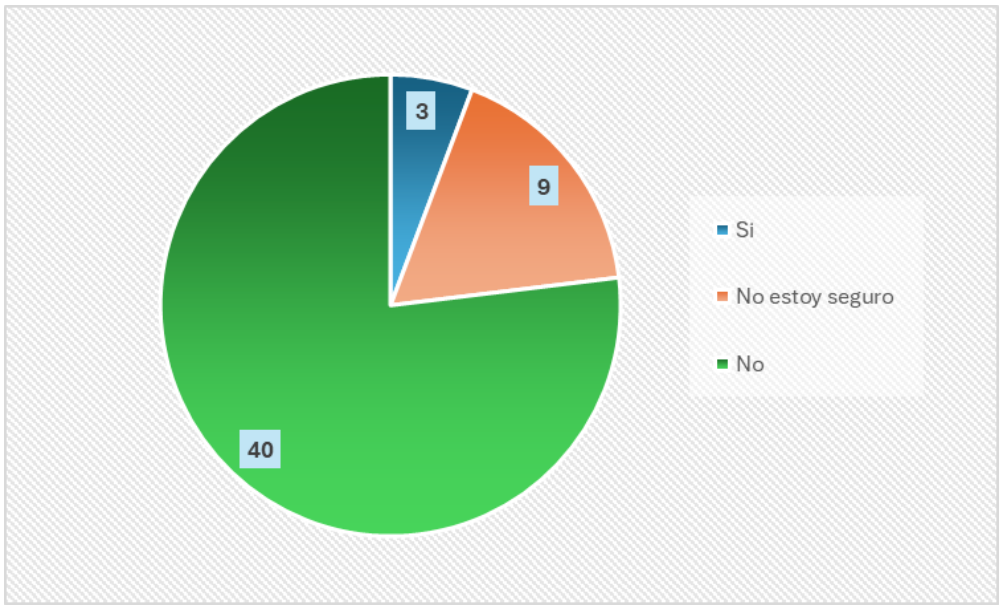


Pregunta 8. ¿Ha notado si en su clínica se toman medidas para proteger la privacidad de la información médica (ejemplo: ¿uso de claves, acceso restringido)?

Según la encuesta planteada 40 personas no han notado si se toman medidas de seguridad, 9 de ellas mencionan no estar seguros de aquella medida y 3 afirman que sin lo han notado. Como se muestra en la figura 12.

Figura 12

Medidas de protección

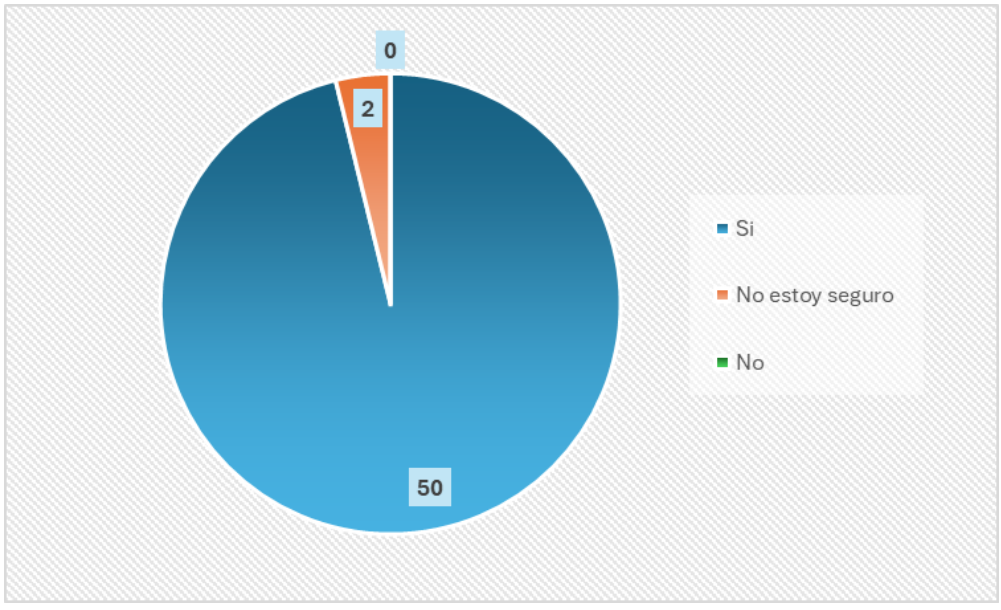


Pregunta 9. ¿En su experiencia, los datos de los pacientes en la clínica se manejan con confidencialidad?

Según las personas encuestadas, 50 afirman que los datos si se manejan con confidencialidad, mientras que 2 de ellas no están seguros del hecho y 0 personas mencionan que no. Como se muestra en la figura 13.

Figura 13

Confidencialidad

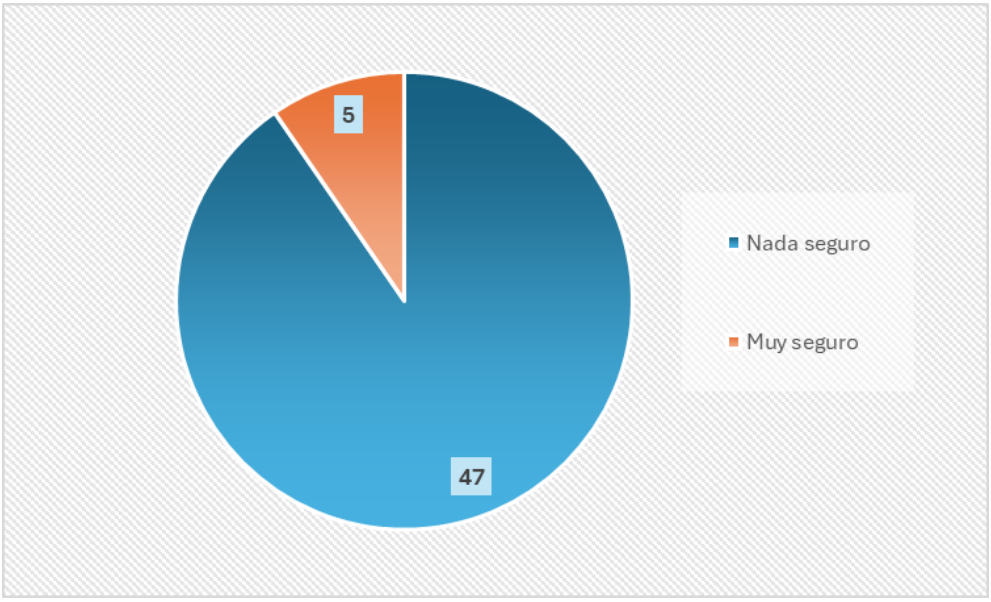


Pregunta 10. En una escala del 1 al 5, donde 1 es “Nada seguro” y 5 “Muy seguro" ¿Qué tan seguro se siente sobre la protección de su información en clínicas de salud?

La mayor cantidad de encuestados confirman que se sienten seguros de su protección de datos, mientras que 5 de los mismos mencionan que no es seguro su protección de datos. Como se muestra en la figura 14.

Figura 14

Seguridad de información

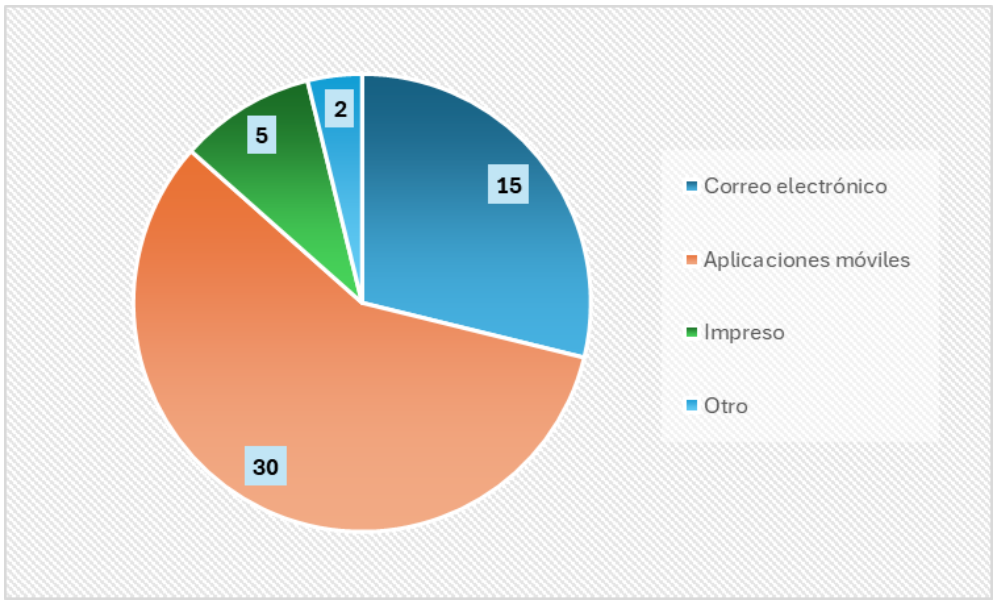


Pregunta 11. ¿Qué método prefiere para recibir información médica?

Según las personas encuestadas, 30 prefieren que la información se envíe por los aplicativos móviles, 15 mencionan vía por correo electrónico, mientras que 5 de ellas optan por que sea impreso y 2 por otro medio. Como se muestra en la figura 15.

Figura 15

Método de información

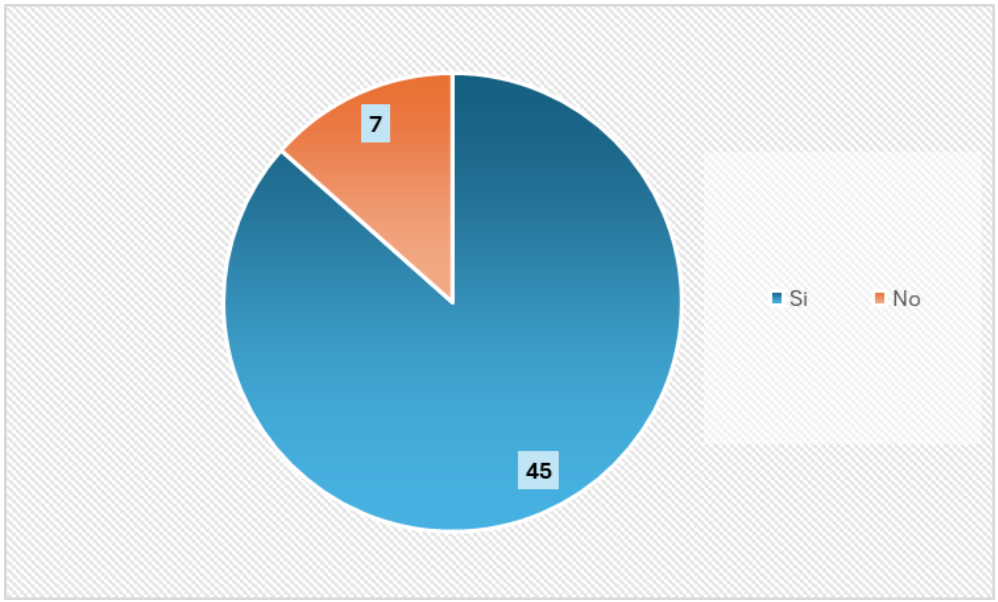


Pregunta 12. ¿Cree que el uso de plataformas digitales ha mejorado la seguridad y acceso a los datos de salud?

Según la encuesta realizada la mayor cantidad se elige que sí ha mejorado la seguridad mientras que 7 de ellos se anteponen. Como se muestra en la figura 16.

Figura 16

Uso de plataformas

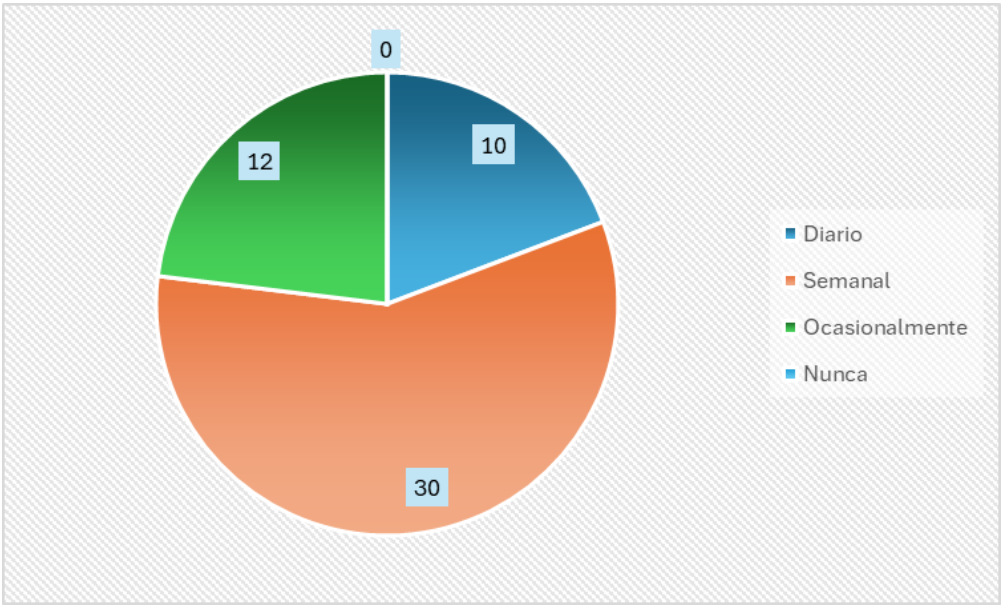


Pregunta 13. ¿Con qué frecuencia utiliza dispositivos electrónicos para acceder a información médica?

Según la encuesta realizada 30 personas utilizan semanalmente dispositivos electrónicos para acceder a la información, 10 de ellos la hacen diariamente y 12 ocasionalmente. Como se muestra en la figura 17.

Figura 17

Frecuencia de uso

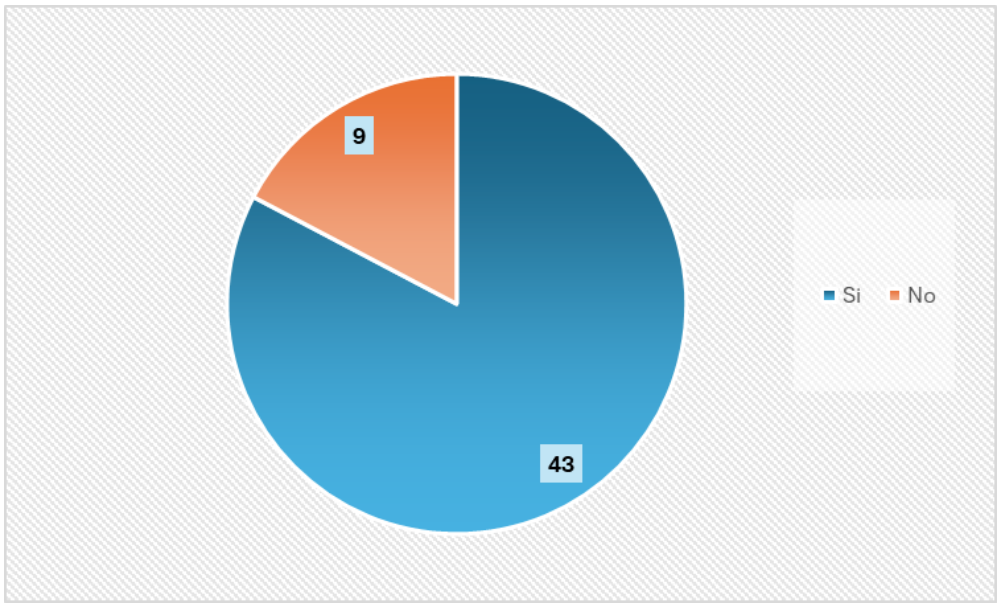


Pregunta 14. ¿Ha recibido advertencias o alertas sobre intentos de acceso no autorizado a su información médica?

Según la encuesta ejecutada, 43 personas afirman que han recibido alertas de intento de acceso sin previa autorización, mientras que el resto niega haber recibido advertencias. Como se muestra en la figura 18.

Figura 18

Alerta de acceso

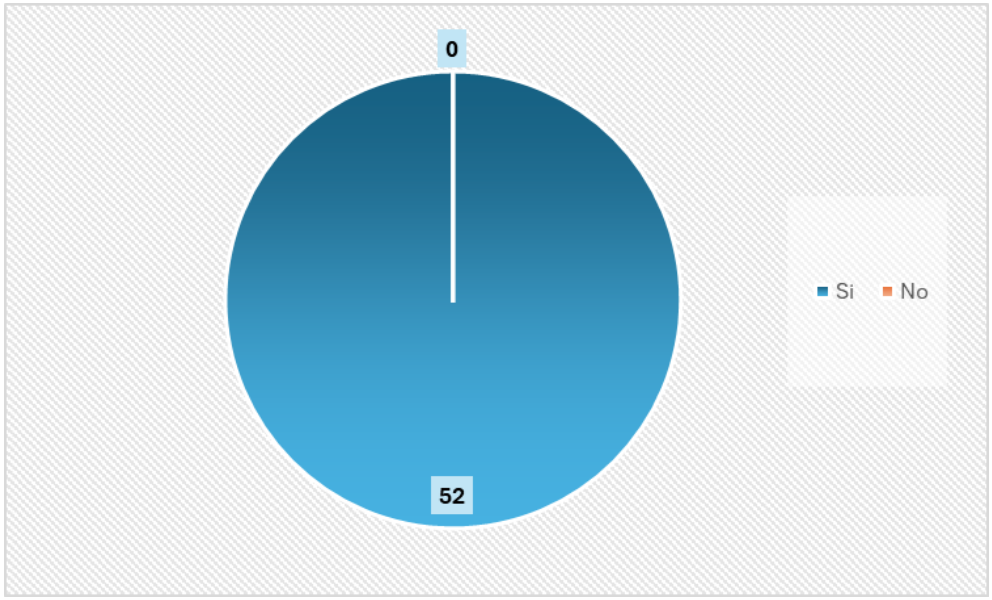


Pregunta 15. ¿Considera que las clínicas deberían implementar autenticación de dos factores para acceder a los historiales médicos?

Según los encuestados 52 están totalmente de acuerdo. Como se muestra en la figura 19.

Figura 19

Factor de autenticación

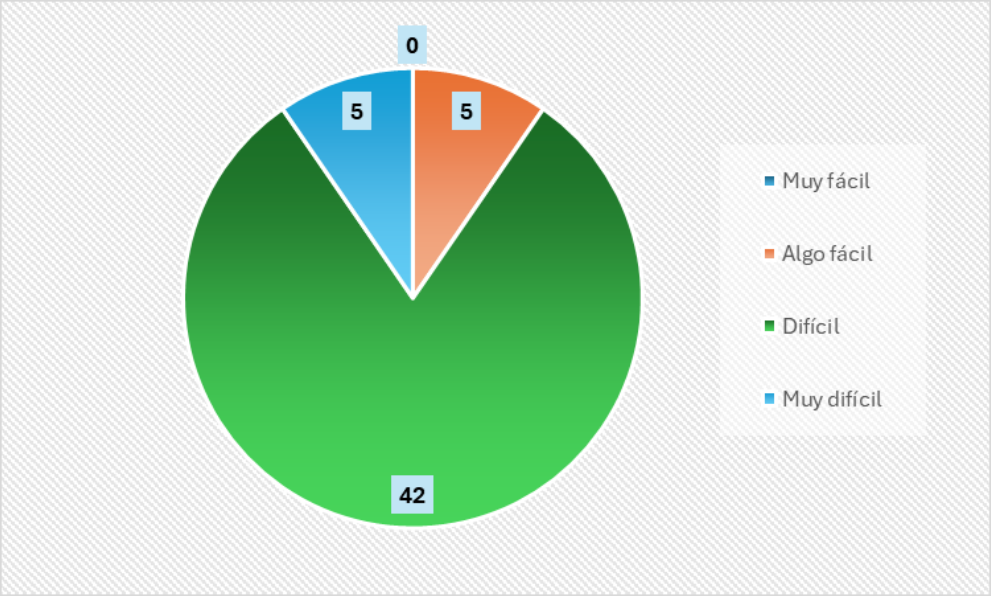


Pregunta 16. ¿Qué tan fácil cree que sería para una persona no autorizada acceder a datos médicos en una clínica?

Según las 52 personas encuestadas, 42 hacen referencia que es difícil el acceso a la información, 5 que es muy difícil y 5 más argumentan que es algo fácil el acceso a la misma. Como se muestra en la figura 20.

Figura 20

Acceso a la información

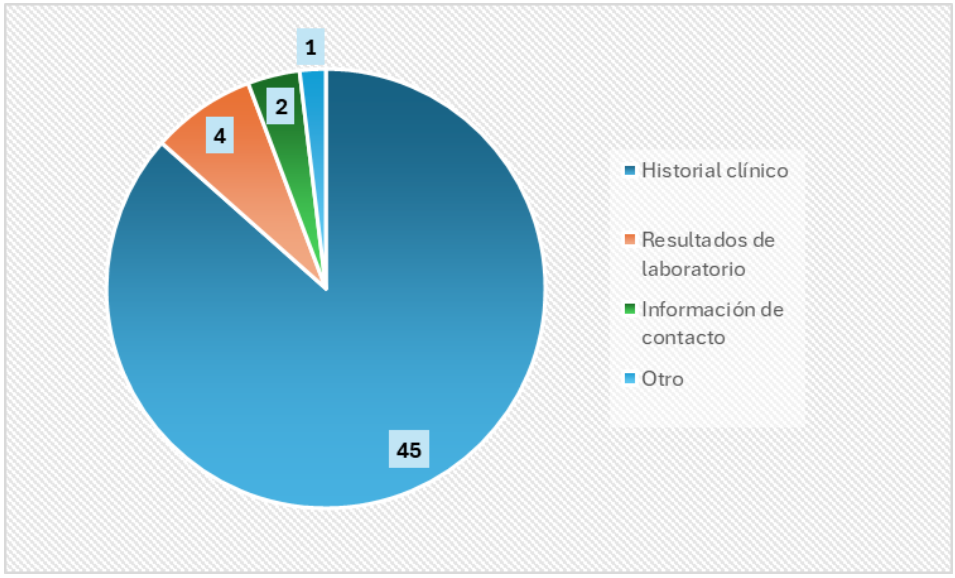


Pregunta 17. ¿Qué tipo de datos médicos considera más sensibles y que requieren mayor protección?

Según los encuestados, 45 consideran que el historial clínico es la información más sensible, 4 argumentan los resultados de laboratorio, 2 se van por la información de contacto y una persona por otro dato. Como se muestra en la figura 21.

Figura 21

Sensibilidad de información

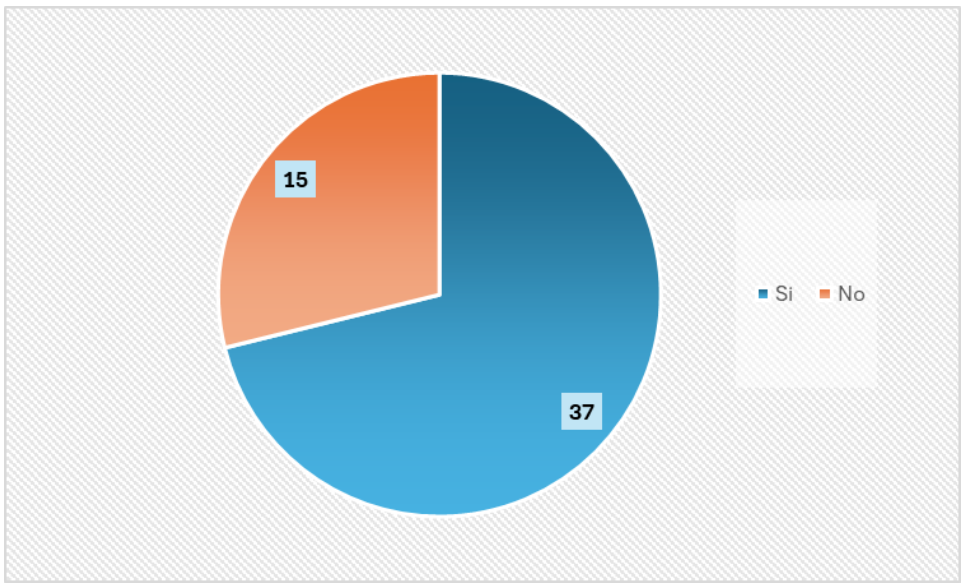


Pregunta 18. ¿Cree que los médicos y el personal de salud reciben suficiente capacitación en ciberseguridad?

Según los encuestados 37 personas consideran que, si se recibe la suficiente capacitación, mientras que 15 personas se oponen ante ello. Como se muestra en la figura 22.

Figura 22

Capacitaciones en las clínicas

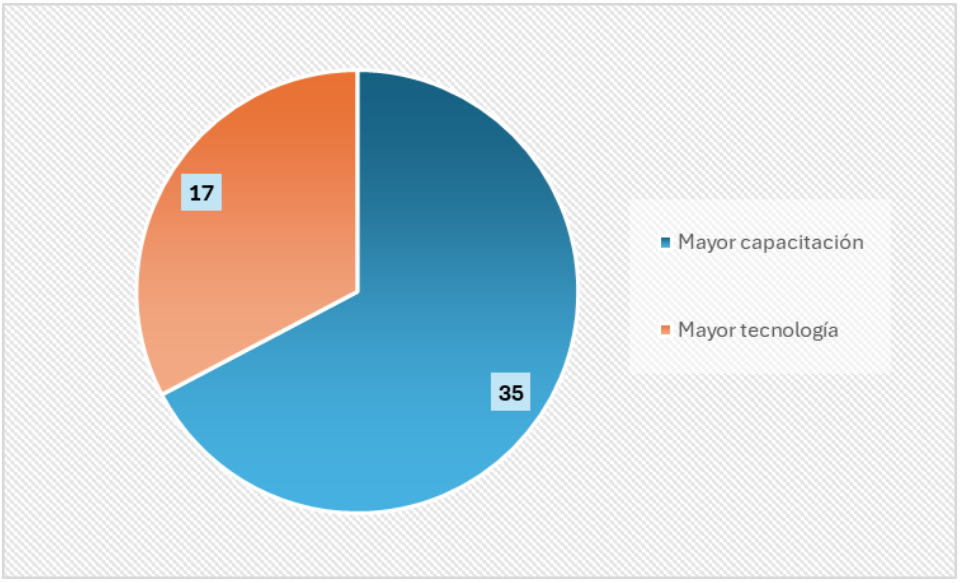


Pregunta 19. ¿Qué medida cree que mejoraría la seguridad de los datos médicos?

Según los encuestados 35 personas mencionan que una medida de seguridad que mejoraría la misma es con mayor capacitación, mientras que 17 de ellos consideran que tener más tecnología potenciaría la seguridad. Como se muestra en la figura 23.

Figura 23

Medidas de seguridad

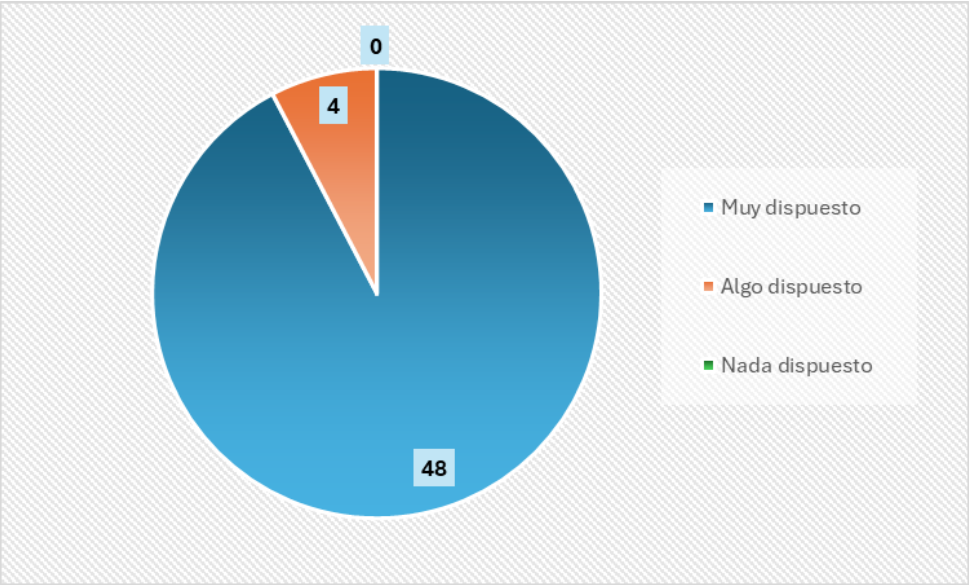


Pregunta 20. ¿Qué tan dispuesto estaría a cambiar su forma de acceso a la información médica si eso mejora la seguridad?

Según los encuestados 48 consideran que están muy dispuestos a actualizar su información, 4 estarían algo indispuestos y nadie estaría renuente a hacerlo. Como se muestra en la figura 24.

Figura 24

Cambio de información



1.3.2 Análisis de entrevistas realizadas

Para Denzin y Lincoln (2005), la entrevista es "una conversación, es el arte de realizar preguntas y escuchar respuestas". Como técnica de recogida de datos, está fuertemente influenciada por las características personales del entrevistador.

Como parte de la guía y para tener una visión más clara se ha realizado la entrevista a médicos y pacientes.

ENTREVISTA 1

Paciente 1

CARGO: Ingeniera Informática

CASA DE SALUD: CENTRO DE SALUD

1. ¿Qué tan familiarizado está con las leyes y regulaciones ecuatorianas sobre protección de datos de pacientes, incluyendo la norma HIPAA (Health Insurance Portability and Accountability Act), si aplica en su contexto?
   No sabía que existían leyes de privacidad.

2. ¿Recuerda haber firmado algún documento relacionado con la privacidad y el uso de sus datos? ¿Le explicaron su contenido?

   No.

3. En una escala del 1 al 5, donde 1 es "nada seguro" y 5 "muy seguro", ¿cuán seguro se siente que su información médica está protegida contra accesos no autorizados en esta casa de salud?

   Mi respuesta es 2.

4. ¿Le preocupa que su información médica personal fuera víctima de un ciberataque o filtración de datos? ¿Por qué?

   Claro, porque mi salud es algo privado.

5. ¿Qué tan importante considera que es para las casas de salud invertir en sistemas de ciberseguridad para proteger la información de los pacientes?

   Es muy importante.

6. ¿Ha utilizado alguna vez servicios de telemedicina o ha compartido su información médica a través de plataformas digitales proporcionadas por esta casa de salud? Si es así, ¿qué tan cómodo se sintió con la seguridad de ese proceso?

   No.

7. ¿Confía en que las autoridades sanitarias del Ecuador están tomando medidas adecuadas para proteger su información médica en línea?

   No.

8. ¿Qué tipo de información le gustaría recibir de esta casa de salud sobre las medidas de ciberseguridad que implementan para proteger sus datos?

   Que me den un documento en el cual me digan que la información de mi salud está protegida.

9. ¿Estaría dispuesto a participar en programas de concienciación o capacitación sobre ciberseguridad y protección de datos en el ámbito de la salud?

   Por supuesto que sí.

10. En su opinión, ¿qué podría hacer esta casa de salud para aumentar su confianza en la seguridad de su información personal y médica?

    Entregar más información referente a la privacidad de los datos que estamos entregando

ENTREVISTA 2

Paciente 2

Diagnóstico: Psicología

CASA DE SALUD: CLÍNICA

1. ¿Qué tan familiarizado está con las leyes y regulaciones ecuatorianas sobre protección de datos de pacientes, incluyendo la norma HIPAA (Health Insurance Portability and Accountability Act), si aplica en su contexto?

   No, desconozco de leyes y regulaciones Hipaa.

2. ¿Recuerda haber firmado algún documento relacionado con la privacidad y el uso de sus datos? ¿Le explicaron su contenido?

   No recuerdo haber firmado un documento que tenga relación con la privacidad de mis datos.

3. En una escala del 1 al 5, donde 1 es "nada seguro" y 5 "muy seguro", ¿cuán seguro se siente que su información médica está protegida contra accesos no autorizados en esta casa de salud?

   Un 4.

4. ¿Le preocupa que su información médica personal fuera víctima de un ciberataque o filtración de datos? ¿Por qué?

   Si, porque al contener mi número de cédula, correo electrónico, nombres completos, cualquier persona puede usar esa información para falsificaciones, de igual manera podrían entrar a plataformas municipales donde con el número de cédula se pueden realizar trámites delicados.

5. ¿Qué tan importante considera que es para las casas de salud invertir en sistemas de ciberseguridad para proteger la información de los pacientes?

   Debería ser muy importante proteger los datos personales de sus clientes ya que son ellos se pueden hacer bastantes trámites.

6. ¿Ha utilizado alguna vez servicios de telemedicina o ha compartido su información médica a través de plataformas digitales proporcionadas por esta casa de salud? Si es así, ¿qué tan cómodo se sintió con la seguridad de ese proceso?

   La verdad no me sentía muy cómoda ya que me pedían datos e información muy delicada. Pero por temas de tiempo tuve que seguir con el proceso.

7. ¿Confía en que las autoridades sanitarias del Ecuador están tomando medidas adecuadas para proteger su información médica en línea?

   No confío mucho.

8. ¿Qué tipo de información le gustaría recibir de esta casa de salud sobre las medidas de ciberseguridad que implementan para proteger sus datos?

   Me gustaría estar informada acerca de qué protección me brindan al momento de proporcionar mis datos personales, para cualquier motivo yo tenga un respaldo.

9. ¿Estaría dispuesto a participar en programas de concienciación o capacitación sobre ciberseguridad y protección de datos en el ámbito de la salud?

   Si claro.

10. En su opinión, ¿qué podría hacer esta casa de salud para aumentar su confianza en la seguridad de su información personal y médica?

    Que nos proporcionen más información digerible y llevadera, ya que hay mucha gente que ya es mayor de edad y no comprenden ciertos términos. Que la información o seguridad que nos brindan sea segura.

ENTREVISTA 3

Médico 1

CARGO: Médico

CASA DE SALUD: CLÍNICA

1. ¿Qué tan familiarizado está con las leyes y regulaciones ecuatorianas sobre protección de datos de pacientes, incluyendo la norma HIPAA (Health Insurance Portability and Accountability Act), si aplica en su contexto?

   Conozco de las leyes y regulaciones, sin embargo, nos hace falta profundizar los temas para impartirla a nuestros pacientes.
2. ¿Recuerda haber firmado algún documento relacionado con la privacidad y el uso de sus datos? ¿Le explicaron su contenido?

   No
3. En una escala del 1 al 5, donde 1 es "nada seguro" y 5 "muy seguro", ¿cuán seguro se siente que su información médica está protegida contra accesos no autorizados en esta casa de salud?

   4
4. ¿Le preocuparía que su información médica personal fuera víctima de un ciberataque o filtración de datos? ¿Por qué?

   No

5. ¿Qué tan importante considera que es para las casas de salud invertir en sistemas de ciberseguridad para proteger la información de los pacientes?

   Muy importante
6. ¿Ha utilizado alguna vez servicios de telemedicina o ha compartido su información médica a través de plataformas digitales proporcionadas por esta casa de salud? Si es así, ¿qué tan cómodo se sintió con la seguridad de ese proceso?

   No
7. ¿Confía en que las autoridades sanitarias del Ecuador están tomando medidas adecuadas para proteger su información médica en línea?

   Si
8. ¿Qué tipo de información le gustaría recibir de esta casa de salud sobre las medidas de ciberseguridad que implementan para proteger sus datos?

   No se
9. ¿Estaría dispuesto a participar en programas de concienciación o capacitación sobre ciberseguridad y protección de datos en el ámbito de la salud?

   Si

10. En su opinión, ¿qué podría hacer esta casa de salud para aumentar su confianza en la seguridad de su información personal y médica?
    Usar servicios informáticos con experiencia

ENTREVISTA 4

Médico 2

CARGO: Auxiliar médico

CASA DE SALUD: CENTRO

1. ¿Qué tan familiarizado está con las leyes y regulaciones ecuatorianas sobre protección de datos de pacientes, incluyendo la norma HIPAA (Health Insurance Portability and Accountability Act), si aplica en su contexto?

   Desconozco totalmente del tema de seguridad en salud

2. ¿Recuerda haber firmado algún documento relacionado con la privacidad y el uso de sus datos?
   No ¿Le explicaron su contenido? No
3. En una escala del 1 al 5, donde 1 es "nada seguro" y 5 "muy seguro", ¿cuán seguro se siente que su información médica está protegida contra accesos no autorizados en esta casa de salud?
   4
4. ¿Le preocupa que su información médica personal fuera víctima de un ciberataque o filtración de datos? No ¿Por qué?
   Porque para mí ninguna enfermedad es secreta para generar disturbio Social.
5. ¿Qué tan importante considera que es para las casas de salud invertir en sistemas de ciberseguridad para proteger la información de los pacientes?
   No sería importante para mí ya que con eso se pudiera invertir en medicamentos que en verdad hacen falta.
6. ¿Ha utilizado alguna vez servicios de telemedicina o ha compartido su información médica a través de plataformas digitales proporcionadas por esta casa de salud? Si es así, ¿qué tan cómodo se sintió con la seguridad de ese proceso?
   No.

7. ¿Confía en que las autoridades sanitarias del Ecuador están tomando medidas adecuadas para proteger su información médica en línea?

   Si.

8. ¿Qué tipo de información le gustaría recibir de esta casa de salud sobre las medidas de ciberseguridad que implementan para proteger sus datos?

   Información básica de ciberseguridad.

9. ¿Estaría dispuesto a participar en programas de concienciación o capacitación sobre ciberseguridad y protección de datos en el ámbito de la salud?

   Si.

10. En su opinión, ¿qué podría hacer esta casa de salud para aumentar su confianza en la seguridad de su información personal y médica?

    Mejorar el sistema, actualizar la seguridad ya que cada instante los ciberataques son más frecuentes y al estar en la vanguardia de los nuevos métodos de ataque la seguridad sería el método más eficiente para combatirlos.

CAPÍTULO II: PROPUESTA

2.1 Fundamentos teóricos aplicados

Ciberseguridad en el sector sanitario

La delincuencia cibernética en el ámbito de la salud representa alto riesgo en la era digital. Con el incremento de la digitalización de historiales médicos y la telemedicina, los ataques online pueden resultar en efectos devastadores.

Revelar datos sensibles o impedir el acceso a sistemas puede poner en riesgo la confidencialidad de los pacientes y disminuir la calidad del servicio médico. Para abordar esta situación, es crucial establecer medidas sólidas de ciberseguridad como forma de protección (Cervera, 2024)

Vulnerabilidad a los ataques cibernéticos y principales amenazas.

Según Cervera (2024) la privacidad implica salvaguardar información de manera que únicamente pueda ser consultada por individuos con permiso. La privacidad puede verse amenazada si hay acceso ilegal a la información. Es esencial considerar la gestión de accesos, el encriptado de datos, la verificación de usuarios y las regulaciones sobre privacidad. Por ejemplo, en un centro de salud, los expedientes médicos deben ser accesibles únicamente para el médico autorizado que está atendiendo al paciente específico.

Triada CIA

Como eje principal en los lineamientos de seguridad se toma se destaca la triada de Confidencialidad, Integridad y Disponibilidad (CIA), que sirve como el marco que orienta las normativas de seguridad de la información dentro de una entidad, esencial en el área de la ciberseguridad y la salvaguarda de información.

Guía de ciberseguridad para la protección de datos sensibles

En la actualidad la tecnología ha avanzado en el margen de la protección de datos sensibles el cual se ha convertido en una preocupación primordial para organizaciones de todos los tamaños basándose en los riesgos cibernéticos aplicados en los datos de los pacientes. La creciente sofisticación de las amenazas cibernéticas y el valor cada vez mayor de la información personal y confidencial exigen un enfoque integral y actualizado para la ciberseguridad. Para ello esta guía tiene como objetivo proporcionar un marco práctico y teóricamente sólido para ayudar a las organizaciones a proteger sus datos sensibles de manera efectiva.

Una guía de capacitación que se realiza de forma técnica es un documento estructurado que forma parte del trabajo de investigación y que tiene como objetivo orientar el proceso de enseñanza-aprendizaje en un área específica. Generalmente, se incluye en estudios que buscan mejorar habilidades, conocimientos o competencias en un grupo determinado (OPENAI, 2024).

Ciberseguridad y ética

Con una base sólida y, ante todo, bien organizada, se transforma en una inversión en lugar de un gasto para la empresa; esto se debe a que el equipo humano formula nuevas formas de implementar, adquiere conocimientos renovados y, por lo tanto, presenta menos debilidades, además de estar integrado en el ámbito de la evolución tecnológica. Así, las clínicas logran una mayor ganancia, fiabilidad y, sobre todo, conciencia ética al construir confianza con sus pacientes.

El bienestar, desde tiempos antiguos con el juramento hipocrático hasta el presente guiado por principios de bioética, se basa en la conducta ética y moral para su resguardo y mantenimiento. Según la Enciclopedia de Bioética del Instituto Joseph y Rose Kennedy, la bioética se define como el estudio ordenado de la acción humana en el ámbito de las ciencias biológicas y la salud, considerando los aspectos de valores éticos (García, 2010).

En el estado de la seguridad de datos, Forrester (2024) examina los desafíos que enfrentan las empresas y proporciona un desglose regional de las tendencias para mostrar las principales causas y los efectos comerciales de las violaciones de datos, cómo responden las empresas a ellas y qué tecnologías clave están ayudando a prevenirlas (FORRESTER, 2024).

Protección de la información médica protegida

Las organizaciones de salud guardan fotos, informes clínicos, observaciones de los doctores, tratamientos, sensibilidades, y otros datos digitales. Los profesionales de la salud tienen la obligación principal de “no causar daño” (RadiologyInfo™, 2023).

La protección de los datos médicos de los pacientes describe los procedimientos que el personal médico debe adoptar para “resguardar la información de salud” (PHI).

La integridad de los resultados de las investigaciones depende de la exactitud y confiabilidad de los datos sanitarios. El cumplimiento de las normas HIPAA garantiza que la recopilación, el almacenamiento y la transmisión de la información sanitaria protegida mantengan un alto nivel de exactitud de los datos (PAUBOX, 2024).

Crecimiento en la Ciberseguridad

Algunos de los factores que favorecen el mercado son el aumento de los ciberataques, con mayores preocupaciones de privacidad y seguridad existe una mayor adopción de soluciones avanzadas de ciberseguridad. Además, existe una creciente adopción de soluciones basadas en la nube en el sector salud, el aumento en la adopción de dispositivos y teléfonos inteligentes conectados, y la adopción de la tecnología 5G, son factores que se esperan que contribuyan al crecimiento del mercado durante el período de pronóstico (KRIPTOS, 2024).

Implementación de tecnología

Si implementamos un nuevo software de gestión de proyectos de seguridad, la contextualización en un entorno administrativo implicaría analizar cómo este software se integrará con los sistemas existentes en caso de existir y de no haberlos como sería el ingreso informático y que impactos administrativos se darían, de qué manera se puede llegar a los usuarios y empleados y cómo se capacitará al personal, se medirá el impacto en la productividad al realizar cada actividad. En base al entorno de aprendizaje y el tema educativo nos centraremos en el enfoque de cómo relacionar el aprendizaje y la enseñanza aplicado en estudiantes y/o personal médico (PACIENCIA, 2015).

La contextualización de la seguridad informática en clínicas de salud en Ecuador implica entender los desafíos específicos que enfrentan estas instituciones. Estos desafíos pueden incluir la falta de recursos y personal capacitado, la rápida evolución de las amenazas cibernéticas, y la necesidad de equilibrar la seguridad con la accesibilidad y la eficiencia en la atención al paciente.

Calcular la rentabilidad de una inversión, es clave para saber con seguridad, lo que se busca es averiguar cuánto hemos ganado (o esperamos ganar) con la operación, un ejercicio que no es tan sencillo como pudiera parecer a simple vista (BBVA, 2024). La cual se representa en la ecuación (2).

$$RENTABILIDAD = BENEFICIO / INVERSIÓ \quad (2)$$

Mejora Continua

Cuando se menciona el concepto de mejora continua, se hace alusión a la expansión del saber para llevar a cabo las tareas de forma más efectiva y utilizando recursos materiales, tecnológicos y educativos, siempre con el objetivo de lograr un perfeccionamiento incesante y mantenerse al día con los progresos (CRESPO GARCIA, 2020).

Esta actividad es esencial en la administración de calidad y se implementa en múltiples sectores, incluyendo la industria, el comercio, la enseñanza y la sanidad, que es nuestra área, entre otros. Estas directrices aseguran que la información delicada esté resguardada frente a accesos no permitidos, alteraciones y pérdidas.

Las empresas pueden utilizar herramientas como el índice de rentabilidad (PI) para determinar la rentabilidad potencial de un proyecto. El análisis de los márgenes de beneficio también ayuda a las empresas a realizar un seguimiento de los ingresos y la salud financiera general. (WRIKE, 2025).

La progresión constante se fundamenta en la creencia de que siempre es posible avanzar y que ajustes pequeños y regulares pueden resultar en grandes beneficios a largo plazo para las clínicas. Obtener opiniones y recomendaciones de los trabajadores sobre posibles mejoras en la seguridad, para lo cual se realizará un seguimiento de la efectividad de las modificaciones. Esto nos lleva a preservar una ventaja competitiva que pone de manifiesto ante los clientes y el equipo la dedicación de la organización a la seguridad tecnológica.

Protección cibernética en salud

La Ciberseguridad es la principal práctica aplicada en proteger las redes y sistemas informáticos contra los accesos no autorizados, incitando al robo o daño de información por parte de los ciber delincuentes siendo así un campo amplio que conlleva una variedad de tecnología y una constante evolución para poder garantizar la confidencialidad, integridad y sobre todo la disponibilidad de información. En el mundo actual la información es almacenada es presa fácil cuando no se dispone de una seguridad de alto nivel siendo parte fundamental de organizaciones e individuos:

La protección de amenazas se aplica esencialmente en:

- Hackers
- Phishing

- Ataques de denegación DoS
- Malware

Para ello es importante contar con el accionar y cómo funciona la Ciberseguridad, es por ello que las medidas técnicas incluyen:

- Firewall
- Antivirus
- Cifrado
- Autenticación

Y sobre ello recaen en las organizaciones las políticas de seguridad, capacitación incluyendo buenas guías prácticas educando al personal sobre las mejores prácticas y de cómo identificar posibles ataques. De esta manera se fomentar a el procedimiento para responder a un incidente de seguridad.

Protección de datos sensibles

Los datos personales sensibles constituyen en sí mismos un desafío regulatorio permanente, lo cual constituye un valor de la guía que presentamos, al ir exponiendo de forma meticulosa buenas prácticas esenciales en la materia, como el de tratamiento de la información o el propio dato personal, hasta llegar a las categorías especiales de datos reconocidas en el Reglamento general de protección de datos (RGPD).

Se refiere a la serie de medidas y los derechos que buscan proteger la información privada de las personas y lo que busca es generar confianza, lealtad y transparencia. Esto implica los accesos no autorizados, amenazas a la seguridad de la información. El personal o empleados desempeñan el papel fundamental en la protección de datos sensibles dentro de la organización.

Hippa

La HIPAA (Health Insurance Portability and Accountability Act) es una ley de los Estados Unidos, promulgada en 1996, que protege la privacidad y seguridad de la información médica de los pacientes. (OPENAI, CHATGPT, 2025)

Objetivos principales de la HIPAA:

1. Protección de la privacidad en el cual se restringe el acceso y uso de la información de salud personal (Información de la salud protegida)

2. Seguridad de los datos cuando se establece medidas para prevenir el acceso no autorizado, pérdidas o robos de información médica.

3. Portabilidad del seguro de salud en la que se facilita la continuidad del seguro médico cuando una persona cambia de trabajo.

4. Normas para el intercambio electrónico de datos cuando regula cómo se comparten electrónicamente los registros médicos.

2.2 Descripción de la propuesta

El enfoque de esta guía es precisamente mejorar la seguridad de la información personal sensible que ingresa a las clínicas de salud, se centra en desarrollar una guía práctica y exhaustiva para fortalecer la seguridad en el sector de la salud, específicamente en clínicas, considerando la criticidad de la información que manejan y las regulaciones existentes, para todo esto se ha realizado un análisis profundo sobre la teoría de ciberseguridad en el sector salud, incluyendo las normas Hipaa y las guías de buena práctica.

Se determinarán los riesgos más relevantes ligados a la gestión de información confidencial en centros médicos, tomando en cuenta factores tecnológicos y factores humanos.

El desarrollo de la guía contendrá normativas y métodos para la protección adecuada de la información, sugerencias acerca de soluciones tecnológicas como por ejemplo cortafuegos y plataformas de identificación de amenazas.

Se desarrollarán planes de aprendizaje permanente para empleados en la materia de ciberseguridad.

Estructura general

Este organizador ofrece un formato definido que facilite la cobertura de todos los elementos significativos concernientes a la seguridad cibernética en los centros de salud, los cuales garantizan el cumplimiento de las regulaciones Hippa de manera que se resguarde correctamente la información sensible. Como se muestra en la figura 25.

Figura 25

Estructura de la Propuesta

Se debe establecer un área dedicada a la gestión de la seguridad de la información, encargada de identificar los riesgos implementando controles y capacitando al personal para las buenas

Explicación del aporte

Este organizador explica de manera clara y precisa el funcionamiento de la guía de ciberseguridad enfocado en las clínicas de salud. La formación de las buenas prácticas será desarrollada permanentemente por parte del personal médico quienes son responsables de salvaguardar la información sensible de cada uno de los pacientes, se emitirán informes mensuales de los casos de información sensible, así como también se realizarán evaluaciones constantes para medir vulnerabilidades.

Una estructura organizativa adecuada para manejar la ciberseguridad en centros de salud debe ser diversa, con el respaldo del liderazgo de los superiores enfocados siempre en fomentar una cultura de seguridad. La unión de un liderazgo sólido y una formación constante con directrices precisas y una estrategia activa para el seguimiento y la reacción ante las vulnerabilidades facilitará la protección de la información delicada.

Los efectos anticipados de aplicar este manual incluyen equipos médicos formados en la seguridad y protección de información sensible, iniciativas con seguridad y habilidades para

identificar y reducir vulnerabilidades; estos efectos proporcionan beneficios externos importantes para aumentar la fiabilidad y competitividad de otras instituciones médicas, mejorando de manera constructiva el manejo de datos delicados.

2.2 Estrategias y/o técnicas

Para establecer una ciberseguridad eficaz en los centros de atención médica, es fundamental emplear diferentes métodos que se enfoquen tanto en la salvaguarda de la información como en la evasión de ataques cibernéticos. A continuación, se describen las estrategias más apropiadas. Como se muestran en la figura 26.

Figura 26

Técnicas y Estrategias

La aplicación adecuada de estas tácticas y métodos no solo salvaguardará la información confidencial en centros de salud, sino que también fortalecerá la confianza de los pacientes y asegurará la conformidad con normas importantes. Es fundamental adoptar una estrategia anticipativa y flexible respecto a la seguridad informática, considerando el aumento y la complejidad de los riesgos digitales en la industria.

Las encuestas y entrevistas como técnicas metodológicas tienen un gran aporte para la investigación de esta guía.

2.3 Validación de la propuesta

La propuesta ha sido validada por un grupo de tres analistas expertos en ciberseguridad, cuyos pormenores se encuentran en el Anexo 3, quienes han compartido sus opiniones, observaciones y sugerencias.

Para elegir a los especialistas, se ha tomado en cuenta un perfil que satisfaga los siguientes requisitos:

- Educación pertinente al tema en estudio
- Experiencia del profesional en el sector de la informática
- Disposición para colaborar.

La tabla 4 proporciona datos específicos sobre los participantes escogidos para la verificación del modelo.

Tabla 4

Descripción de perfil de validadores

Nombres y Apellidos	Años de experiencia	Titulación Académica	Cargo
Carlos Andrés Cuesta Cruz	4 años	Ingeniero en Redes Magister Gestión y Administración de proyectos	Analista Provincial de Seguridad Informática y Proyectos Tecnológicos Electorales
Geovani Enrique Proaño Tiuma	14 años	Ingeniero en informática	Asistente Electoral Transversal
Gustavo Cazar	26 años	Ingeniero en Informática, Magister Gestión de Tecnologías de la Información	Especialista Electoral

2.4 Matriz de articulación de la propuesta

En la tabla 5 representa la articulación del producto realizado con los sustentos teóricos, metodológicos, estratégicos-técnicos y tecnológicos empleados en la Guía de ciberseguridad para la protección de datos sensibles en clínicas de salud aplicando normas Hippa.

Tabla 5

Matriz de articulación

EJES O PARTES PRINCIPALES	SUSTENTO TEÓRICO	SUSTENTO METODOLÓGICO	ESTRATEGIAS / TÉCNICAS	DESCRIPCIÓN DE RESULTADOS	INSTRUMENTOS APLICADOS
Introducción Ciberseguridad	Contextualización del problema Importancia de la protección de datos Objetivos Generales Objetivos Específicos.	Investigación documental Revisión de leyes y normativas relacionados en la protección de datos a nivel nacional. Estudio de incidentes y vulnerabilidades para identificación de amenazas.	Fuentes bibliográficas en ciberseguridad.	Análisis e interpretación de resultados lo cual permite un mayor enfoque en la compresión de seguridad de datos sensibles.	Investigación Bibliográfica. Entrevista

Marco Teórico	Definiciones de ciberseguridad. Análisis y norma Hipaa Aplicación en sector salud	Revisión de mejores prácticas Investigación con expertos. Análisis del entorno sanitario. Monitoreo y evaluaciones continuas.	Revisión de guías. Análisis cibernéticos Análisis de flujos de información. Evaluaciones de ciberseguridad. Recopilación de opiniones de pacientes	Elaboración de guía de mejores prácticas de datos sensibles. Evaluación de los riesgos. Análisis de riesgos. Medición de cumplimiento de normativas.	Monitoreos. Evaluaciones continuas
Desarrollo de una Guía de Ciberseguridad Enel sector sanitario.	Política para el manejo de datos sensibles. Aplicación de normas Hipaa. Procedimiento y recomendaciones	Investigación de campo. Investigación de normas y políticas.	Observación. Desarrollo. Fuentes bibliográficas.	Proporcionan el conjunto de buenas prácticas, lo cuál permite confidencialidad en la información y seguridad de datos de los pacientes.	Guía de Ciberseguridad para sector sanitario. Presentaciones.

Planes de Capacitación en Personal Médico. **Información a los pacientes de casa de salud**	Desarrollo de programas de formación continua. Contenidos. Metodología.	Indagación documental. Procedimientos informáticos.	Evaluaciones periódicas. Aprendizaje activo Recursos multimedia. Y tecnología de primera.	Creación de una Guía. Otorga habilidades para manejos de ciberseguridad y protección de datos sensibles.	Ejercicios prácticos. Monitoreos/Evaluaciones. Capacitaciones

CONCLUSIONES

La ciberseguridad en el ámbito de la salud representa un área muy compleja y en continuo cambio, motivada por la digitalización de los datos médicos. Es fundamental entender conceptos importantes como la privacidad, la integridad y la disponibilidad de la información, así como las amenazas y debilidades comunes, para salvaguardar la información sensible de los pacientes. La normativa vigente, destacando la Ley HIPAA y otras regulaciones, fija los criterios y requisitos necesarios para asegurar la protección de los datos de salud. La base teórica ofrece un soporte firme para enfrentar los retos de la ciberseguridad en este sector crucial.

La evaluación del estado presente de la ciberseguridad en clínicas de salud elegidas muestra que es crucial mejorar las medidas para proteger la información. Se encontraron debilidades en aspectos como la administración de claves, la protección de las redes y la formación del personal. La escasa comprensión de los riesgos cibernéticos y la aplicación irregular de las normativas de seguridad representan obstáculos recurrentes. Este análisis ofrece datos significativos para crear estrategias de optimización y dar prioridad a las acciones requeridas para reforzar la ciberseguridad en estas organizaciones.

La guía de capacitación en ciberseguridad desarrollada aborda las necesidades específicas del personal médico y administrativo, proporcionando conocimientos y herramientas prácticas para proteger la información de salud. Los módulos de capacitación cubren temas como la identificación de amenazas, el uso seguro de dispositivos y aplicaciones, y el cumplimiento de las políticas de seguridad. La guía se diseñó para ser accesible y fácil de entender, utilizando ejemplos y escenarios relevantes para el entorno de trabajo. La implementación de esta guía contribuirá a mejorar la conciencia y las habilidades del personal en materia de ciberseguridad.

La evaluación de la guía de trabajo global por parte de especialistas en seguridad informática y trabajadores de la salud proporciona información valiosa sobre su efectividad y aplicabilidad. Los especialistas destacaron la importancia de la guía para abordar las vulnerabilidades identificadas y fortalecer la ciberseguridad en las clínicas. Los trabajadores de la salud valoraron la claridad y utilidad de la guía, así como su relevancia para su trabajo diario. La retroalimentación recibida permitirá realizar ajustes y mejoras en la guía para garantizar su eficacia y maximizar su impacto en la protección de la información de salud.

RECOMENDACIONES

Se aconseja llevar a cabo un examen constante y reciente de las normativas y los estándares de seguridad cibernética que son pertinentes para el área de la salud, en particular la Ley HIPAA y otras disposiciones importantes. Es esencial investigar a fondo las nuevas amenazas y las vulnerabilidades que son propias del ámbito sanitario, tales como el ransomware y los asaltos a equipos médicos interconectados. Se propone estimular la investigación y la creación de modelos teóricos que hagan frente a las dificultades particulares de la seguridad cibernética en el sector salud, teniendo en cuenta la creciente digitalización de los datos médicos.

Es aconsejable llevar a cabo evaluaciones de seguridad regulares y detalladas en las instalaciones de atención médica, empleando herramientas y métodos estandarizados. Es esencial efectuar pruebas de intrusión y estudios de vulnerabilidades para reconocer y reducir posibles amenazas. Se propone crear un plan de acción individualizado para cada clínica, dando prioridad a las medidas de seguridad en función del grado de riesgo y la importancia de la información. Se sugiere destinar recursos a tecnologías de seguridad de última generación, tales como sistemas de detección de intrusos y cortafuegos avanzados.

Es aconsejable ajustar el manual de formación a los requisitos y funciones concretas del personal médico y administrativo, incorporando casos y situaciones pertinentes a su labor cotidiana. Es esencial añadir secciones sobre el manejo seguro de dispositivos móviles y la salvaguarda de la información personal de los pacientes. Se propone llevar a cabo sesiones de entrenamiento prácticas y simulacros de incidentes de seguridad con el fin de fortalecer el conocimiento adquirido. Se sugiere revisar y renovar el manual de formación regularmente para que se mantenga al día con las nuevas amenazas y las mejores estrategias en ciberseguridad.

Se aconseja llevar a cabo un estudio preliminar de la guía de trabajo diseñada a nivel global en un conjunto representativo de centros de atención médica, recogiendo comentarios exhaustivos sobre su aplicación y eficacia. Es esencial obtener la perspectiva de profesionales en ciberseguridad y personal de la salud de diversas jerarquías y especialidades. Se propone emplear cuestionarios, charlas y grupos de discusión para reunir información cualitativa y cuantitativa sobre la guía. Se sugiere aprovechar la información obtenida para hacer modificaciones y mejoras en la guía, garantizando que sea funcional, pertinente y sencilla de aplicar.

BIBLIOGRAFÍA

BBVA. (2024). *BBVA*. Obtenido de Cómo calcular la rentabilidad de una inversión: https://www.bbva.com/es/salud-financiera/como-calcular-la-rentabilidad-de-una-inversion/

Cervera. (13 de 01 de 2024). *PUBMED CENTRAL*. Obtenido de PUBMED CENTRAL: https://pmc.ncbi.nlm.nih.gov/articles/PMC10823061/

CRESPO GARCIA. (2020). Mejora Continua en el proceso contable. *ESPACIOS*, pág. 11.

Docuware. (01 de 2025). *Docuware*. Obtenido de Docuware: https://start.docuware.com/es/glosario-de-terminos/hipaa

dspace.espoch. (2017). Obtenido de dspace.espoch: http://dspace.espoch.edu.ec/bitstream/123456789/7544/1/20T00915.pdf

FORRESTER. (2024). *FORCEPOINT*. Obtenido de FORCEPOINT: https://www.forcepoint.com/resources/industry-analyst-reports/forrester-state-data-security-2024-fb?sf_src_cmpid=7016T000002gGOSQA2&utm_term=cyber%20security%20report&utm_campaign=WW.ALL.DV.AD.SeP.VaC.Visibility_and_Control.Ever&utm_source=google&utm_medi

Fuentes. (29 de 04 de 2024). *DELTAPROTEC*. Obtenido de Requisitos de cumplimiento de la HIPAA: https://www.deltaprotect.com/blog/requisitos-de-cumplimiento-de-la-hipaa

García. (2010). *Philosophica*. Obtenido de Enciclopedia filosófica: https://www.philosophica.info/voces/bioetica/Bioetica.html

HIPAA ACADEMY. (2025). Obtenido de Estándares de garantías administrativas.: https://hipaaacademy.net/hipaa-security-rule/

HIPAA ACADEMY. (2025). *HIPAA ACADEMY*. Obtenido de HIPAA ACADEMY: https://hipaaacademy.net/hipaa-security-rule/

HIPAA ACADEMY. (2025). *HIPAA ACADEMY*. Obtenido de Estándares de protección física: https://hipaaacademy.net/hipaa-security-rule/

informe Thales Data Threat Report, H. a. (2023). *informe Thales Data Threat Report, Healthcare and Life Sciences Edition.*

KIO TECH. (2024). *KIO TECH*. (KIO TECH) Recuperado el 20 de Febrero de 2025, de La importancia de la ciberseguridad y la ciberdefensa para los países:

https://www.kio.tech/blog/importancia-de-ciberseguridad-y-ciberdefensa-para-los-paises

KRIPTOS. (2024). *KRIPTOS*. Obtenido de Informe de Ciberseguridad en el sector de la salud: https://www.kriptos.io/es/es-post/ciberseguridad-sector-salud

Mati Suárez. (s.f.). *La entrevista como instrumento de investigación.* Qualitative Data Analysis for Applied Policy Research.

METODOLOGIA DE LA INVESTIGACIÓN. (2014). *Hernández, Fernández y Baptista*, 174.

NIST. (14 de 02 de 2024). *Centro de recursos de seguridad informática*. Obtenido de SP 800-66r2 final, Implementación de la regla de seguridad HIPAA: una guía de recursos de ciberseguridad: https://csrc.nist.gov/News/2024/nist-publishes-sp-80066-revision-2-implementing-th

NUEVAS REGULACIONES DE HIPAA. (2025). *STEVE ALDER*.

OPENAI. (2024).

OPENAI. (2025). *CHATGPT*. Obtenido de CHATGPT: https://chatgpt.com/c/67b4db87-b5f0-800e-9c22-6e1f0debcd88

PACIENCIA. (2015). *REPOSITORIO*. Obtenido de METODOLOGIAS DE: https://repositorio.uca.edu.ar/bitstream/123456789/522/1/metodologias-desarrollo-software.pdf

PAUBOX . (2024). Obtenido de PAUBOX: https://www-paubox-com.translate.goog/blog/hipaa-regulations-that-apply-to-clinical-research?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=sge#:~:text=Las%20regulaciones%20HIPAA%20que%20se,informaci%C3%B3n%20de%20salud%20de%20personas%20.

PAUBOX. (2024). Obtenido de PAUBOX: https://www-paubox-com.translate.goog/blog/hipaa-regulations-that-apply-to-clinical-research?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=sge#:~:text=Las%20regulaciones%20HIPAA%20que%20se,informaci%C3%B3n%20de%20salud%20de%20personas%20.

PINEIDA, A. &. (09 de 08 de 2004). *SCIELO.* Obtenido de PUNTO CERO: http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S1815-02762004000100012

questionpro. (2025). Obtenido de questionpro: https://www.questionpro.com/blog/es/investigacion-mixta/

RadiologyInfo™. (01 de 05 de 2023). *Radiologyinfo para pacientes*. Obtenido de Radiological Society of North America, Inc. (RSNA).: https://www.radiologyinfo.org/es/info/article-patient-privacy

SAILPOINT. (2025). *SailPoint Technologies*. Obtenido de SAILPOINT: https://www.sailpoint.com/identity-library/hipaa

THALESGROUP. (2023). Obtenido de THALESGROUP: https://cpl.thalesgroup.com/blog/data-security/what-2025-hipaa-changes-mean-to-you

WALLARM. (2025). *WALLARM*. Obtenido de Definición de la tríada de la CIA: https://lab.wallarm.com/what/definicion-de-la-triada-de-la-cia-ejemplos-de-confidencialidad-integridad-y-disponibilidad/?lang=es

WRIKE. (2025). *WRIKE*. Obtenido de https://www.wrike.com/es/professional-services-guide/rentabilidad-de-un-proyecto/

ANEXOS

ANEXO 1

FORMATO DE ENCUESTA

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

GUÍA DE CIBERSEGURIDAD PARA LA PROTECCIÓN DE DATOS SENSIBLES EN CLÍNICAS DE SALUD APLICANDO NORMAS HIPPA

ENCUESTA

Objetivo:

- *Determinar las necesidades del personal médico y de pacientes sobre las seguridades que tienen sus datos personales y la información médica entregada a las clínicas de salud.*

Pregunta 1. ¿Qué tan importante considera la protección de datos personales en clínicas de salud?

Pregunta 2. ¿Ha escuchado hablar sobre la normativa HIPAA y su relación con la protección de datos en salud?

Pregunta 3. ¿Ha recibido información sobre cómo se protegen sus datos en la clínica donde trabaja o se atiende?

Pregunta 4. ¿Cree que las clínicas deberían mejorar sus medidas de seguridad digital?

Pregunta 5. ¿Con qué frecuencia revisa las políticas de privacidad al proporcionar sus datos en una clínica?

Pregunta 6. ¿Le han solicitado consentimiento para el almacenamiento y uso de su información médica en alguna clínica?

Pregunta 7. ¿Alguna vez ha tenido dificultades para acceder a su historial clínico por razones de seguridad?

Pregunta 8. ¿Ha notado si en su clínica se toman medidas para proteger la privacidad de la información médica (ejemplo: ¿uso de claves, acceso restringido)?

Pregunta 9. ¿En su experiencia, los datos de los pacientes en la clínica se manejan con confidencialidad?

Pregunta 10. En una escala del 1 al 5, donde 1 es “Nada seguro” y 5 es “Muy seguro" ¿Qué tan seguro se siente sobre la protección de su información en clínicas de salud?

Pregunta 11. ¿Qué método prefiere para recibir información médica?

Pregunta 12. ¿Cree que el uso de plataformas digitales ha mejorado la seguridad y acceso a los datos de salud?

Pregunta 13. ¿Con qué frecuencia utiliza dispositivos electrónicos para acceder a información médica?

Pregunta 14. ¿Ha recibido advertencias o alertas sobre intentos de acceso no autorizado a su información médica?

Pregunta 15. ¿Considera que las clínicas deberían implementar autenticación de dos factores para acceder a los historiales médicos?

Pregunta 16. ¿Qué tan fácil cree que sería para una persona no autorizada acceder a datos médicos en una clínica?

Pregunta 17. ¿Qué tipo de datos médicos considera más sensibles y que requieren mayor protección?

Pregunta 18. ¿Cree que los médicos y el personal de salud reciben suficiente capacitación en ciberseguridad?

Pregunta 19. ¿Qué medida cree que mejoraría la seguridad de los datos médicos?

Pregunta 20. ¿Qué tan dispuesto estaría a cambiar su forma de acceso a la información médica si eso mejora la seguridad?

¡Muchas gracias por su colaboración!

ANEXO 2

FORMATO DE ENTREVISTA

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

GUÍA DE CIBERSEGURIDAD PARA LA PROTECCIÓN DE DATOS SENSIBLES EN CLÍNICAS DE SALUD APLICANDO NORMAS HIPPA

ENTREVISTA

Objetivo:

- *Determinar las necesidades del personal médico y de pacientes sobre las seguridades que tienen sus datos personales y la información médica entregada a las clínicas de salud.*

CARGO:

CASA DE SALUD: HOSPITAL / CENTRO / CLÍNICA

1. Cuando acude a esta casa de salud, ¿sabe cómo se maneja y protege su información personal y médica?
2. ¿Recuerda haber firmado algún documento relacionado con la privacidad y el uso de sus datos? ¿Le explicaron su contenido?
3. En una escala del 1 al 5, donde 1 es "nada seguro" y 5 es "muy seguro", ¿cuán seguro se siente que su información médica está protegida contra accesos no autorizados en esta casa de salud?
4. ¿Le preocuparía que su información médica personal fuera víctima de un ciberataque o filtración de datos? ¿Por qué?
5. ¿Qué tan importante considera que es para las casas de salud invertir en sistemas de ciberseguridad para proteger la información de los pacientes?
6. ¿Ha utilizado alguna vez servicios de telemedicina o ha compartido su información médica a través de plataformas digitales proporcionadas por esta casa de salud? Si es así, ¿qué tan cómodo se sintió con la seguridad de ese proceso?
7. ¿Confía en que las autoridades sanitarias del Ecuador están tomando medidas adecuadas para proteger su información médica en línea?

8. ¿Qué tipo de información le gustaría recibir de esta casa de salud sobre las medidas de ciberseguridad que implementan para proteger sus datos?
9. ¿Estaría dispuesto a participar en programas de concienciación o capacitación sobre ciberseguridad y protección de datos en el ámbito de la salud?
10. En su opinión, ¿qué podría hacer esta casa de salud para aumentar su confianza en la seguridad de su información personal y médica?

¡Muchas gracias por su colaboración!

ANEXO 3

VALIDACIÓN DE ESPECIALISTAS

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la calidad del siguiente contenido digital **"Guía de ciberseguridad para la protección de datos sensibles en clínicas de salud aplicando normas Hippa"**. Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide que brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por: CARLOS ANDRES CUESTA CRUZ
Título obtenido: INGENIERIO ELECTRÓNICO
C.I.: 1003820147
E-mail: andrescu7@yahoo.es
Institución de Trabajo: CONSEJO NACIONAL ELECTORAL
Cargo: ANALISTA PROVINCIAL DE SEGURIDAD INFORMÁTICA Y PROYECTOS TECNOLÓGICOS ELECTORALES 2
Años de experiencia en el área: 2 AÑOS

Instructivo:

- Responda cada criterio con la máxima sinceridad del caso.
- Revisar, observar y analizar la propuesta de la plataforma virtual, blog o sitio web.
- Coloque una X en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: "Guía de ciberseguridad para la protección de datos sensibles en clínicas de salud aplicando normas Hippa"

Indicadores	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Pertinencia	**X**				
Aplicabilidad	**X**				
Factibilidad			**X**		
Novedad		**X**			
Fundamentación pedagógica		**X**			
Fundamentación tecnológica		**X**			
Indicaciones para su uso		**X**			
TOTAL	**10**	**20**	**5**	**0**	**0**

Observaciones:

Las organizaciones deben cumplir con la ley para proteger la confidencialidad de los pacientes y cómo gestionan los riesgos relacionados con la seguridad de la información de salud.

Recomendaciones: Es importante que las organizaciones informen sobre los incidentes y el plan de acción para prevenir futuras violaciones a la información de los pacientes.

Lugar, fecha de validación: Quito, 20 de febrero de 2025

Firmado electrónicamente por:
CARLOS ANDRES CUESTA CRUZ

Firma del especialista
Ing. Carlos Andres Cuesta Cruz MSc.

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la calidad del siguiente contenido digital **"Guía de ciberseguridad para la protección de datos sensibles en clínicas de salud aplicando normas Hippa"**. Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide que brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por: GEOVANI ENRIQUE PROAÑO TIUMA
Título obtenido: INGENIERO EN INFORMÁTICA
C.I.: 1716222482
E-mail: enrique.proanio@hotmail.com
Institución de Trabajo: CNE – Delegación de Pichincha
Cargo: Asistente Electoral Transversal
Años de experiencia en el área: 14

Instructivo:

- Responda cada criterio con la máxima sinceridad del caso.
- Revisar, observar y analizar la propuesta de la plataforma virtual, blog o sitio web.
- Coloque una X en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: "Guía de ciberseguridad para la protección de datos sensibles en clínicas de salud aplicando normas Hippa"

Indicadores	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Pertinencia	X				
Aplicabilidad	X				
Factibilidad		X			
Novedad		X			
Fundamentación pedagógica			X		
Fundamentación tecnológica	X				
Indicaciones para su uso		X			
TOTAL	15	12	3		

Observaciones:

Las clínicas y hospitales manejan información personal sensible de los pacientes, y en muchos casos no se informa claramente sobre las medidas de seguridad implementadas para su protección. Algunas instituciones cuentan con sistemas digitales seguros, mientras que otras aún dependen de registros físicos, lo que puede representar un riesgo de acceso no autorizado o pérdida de datos. Además, es fundamental que los pacientes conozcan cómo se gestiona su información y qué derechos tienen sobre ella.

Recomendaciones:

Para mejorar la seguridad de los datos personales, las clínicas deberían implementar cifrado en sus bases de datos, autenticación multifactor para accesos sensibles y restringir permisos según el rol del usuario. Además, es clave capacitar al personal en buenas prácticas de ciberseguridad, realizar auditorías constantes y garantizar que los pacientes sean informados sobre cómo se protege su información.

Lugar, fecha de validación: Quito, 21 de febrero de 2025.

Firma del especialista
Ing. ENRIQUE PROAÑO T.

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la calidad del siguiente contenido digital **"Guía de ciberseguridad para la protección de datos sensibles en clínicas de salud aplicando normas Hippa"**. Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide que brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por:
Título obtenido:
C.I.:1002235131
E-mail: gcazar15@hotmail.com
Institución de Trabajo: Consejo Nacional Electoral-Delegación Provincial Electoral de Pichincha
Cargo: Responsable de la Unidad Provincial de Seguridad Informática y Proyectos Tecnológicos Electorales.
Años de experiencia en el área: 26 años

Instructivo:

- Responda cada criterio con la máxima sinceridad del caso.
- Revisar, observar y analizar la propuesta de la plataforma virtual, blog o sitio web.
- Coloque una X en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: " **"**

Indicadores	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Pertinencia	**5**				
Aplicabilidad	**5**				
Factibilidad		**4**			
Novedad	**5**				
Fundamentación pedagógica	**5**				
Fundamentación tecnológica	**5**				
Indicaciones para su uso		**4**			
TOTAL	**25**	**8**			

Observaciones: La calificación de 4 hace referencia a la factibilidad y al uso, en este caso la factibilidad tiene que ver mucho con los recursos que disponga la Institución para llevar a cabo su implementación, esta información desconozco.

En lo que respecta al uso, tiene relación directa al grado de necesidad que tiene la Institución para su implementación y uso.

Recomendaciones: Por el conocimiento y la experticia en las actividades que cumplo, Entiendo que es muy importante manejar este tipo de normas Hipaa, con la finalidad de salvaguardar de manera íntegra la privacidad y seguridad de la información de los pacientes en una Institución de salud, lo cual felicito y auguro éxitos en su implementación y buen uso que le puedan dar a esta herramienta.

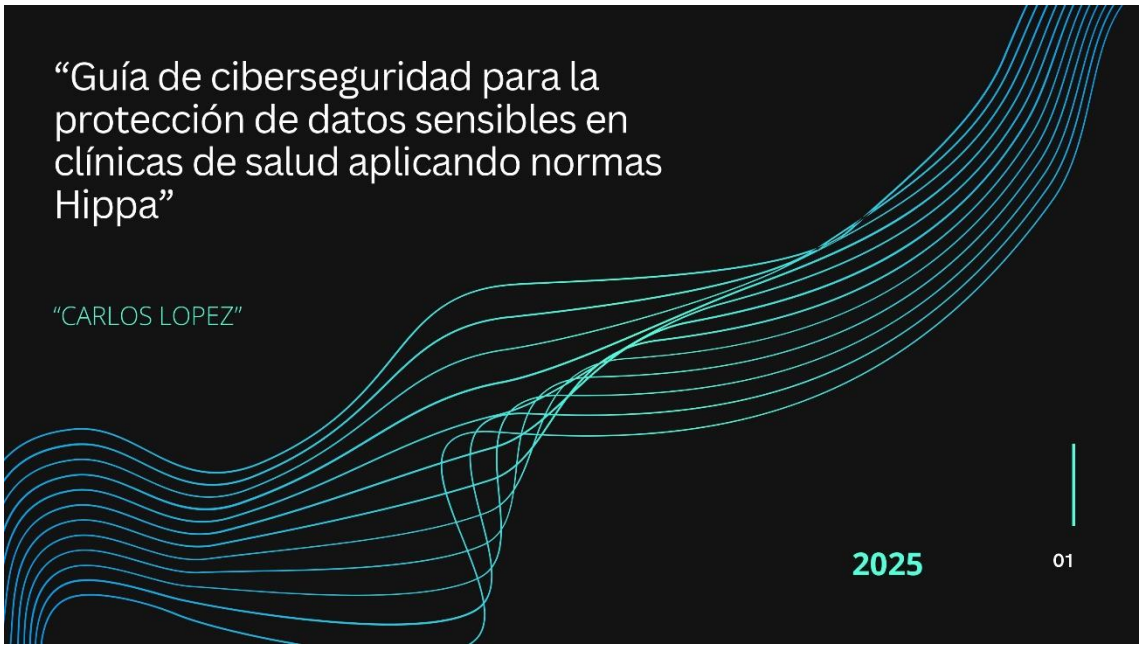
Lugar, fecha de validación: Quito, 28 de febrero de 2025

GUSTAVO BOLIVAR CAZAR VALENZUELA

Firma del especialista
Mgtr. Ing. Gustavo Cazar V.

ANEXO 4

GUIA DE CIBERSEGURIDAD PARA LA PROTECCIÓN DE DATOS SENSIBLES EN CLÍNICAS DE SALUD APLICANDO NORMAS HIPAA



AGRADECIMIENTOS

INGENIEROS / ESPECIALISTAS

Por hacer posible la culminación de esta guía.

INSTITUCIONES / CLÍNICAS

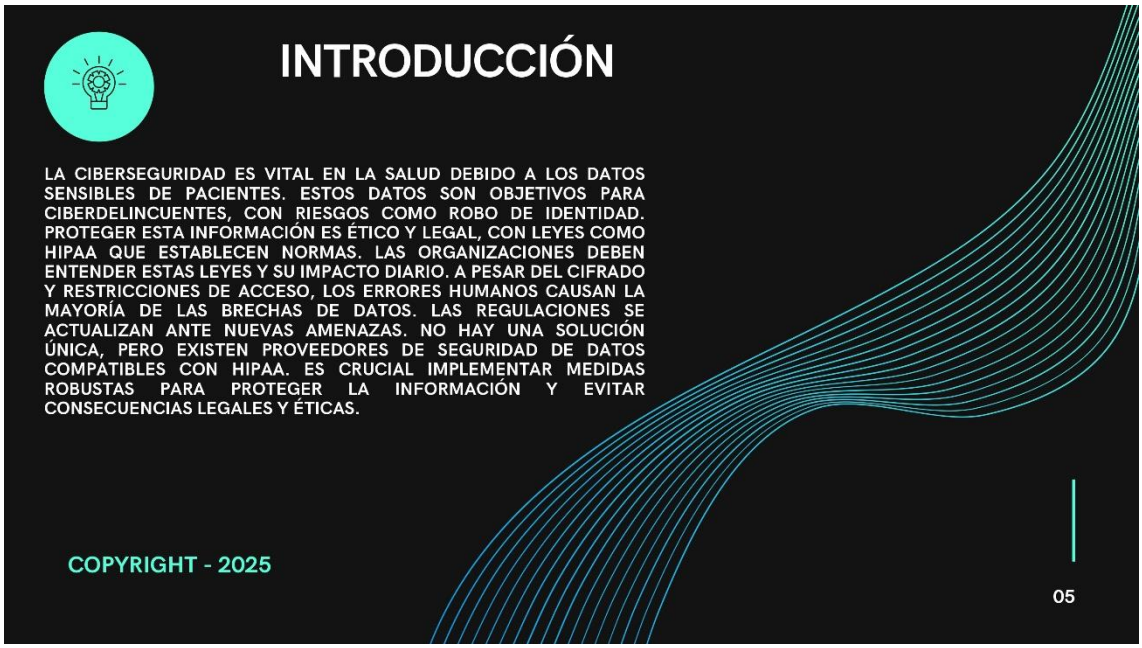
Por abrir sus puesrtas permitiendo que esta guía se ajustara a las necesidades reales.

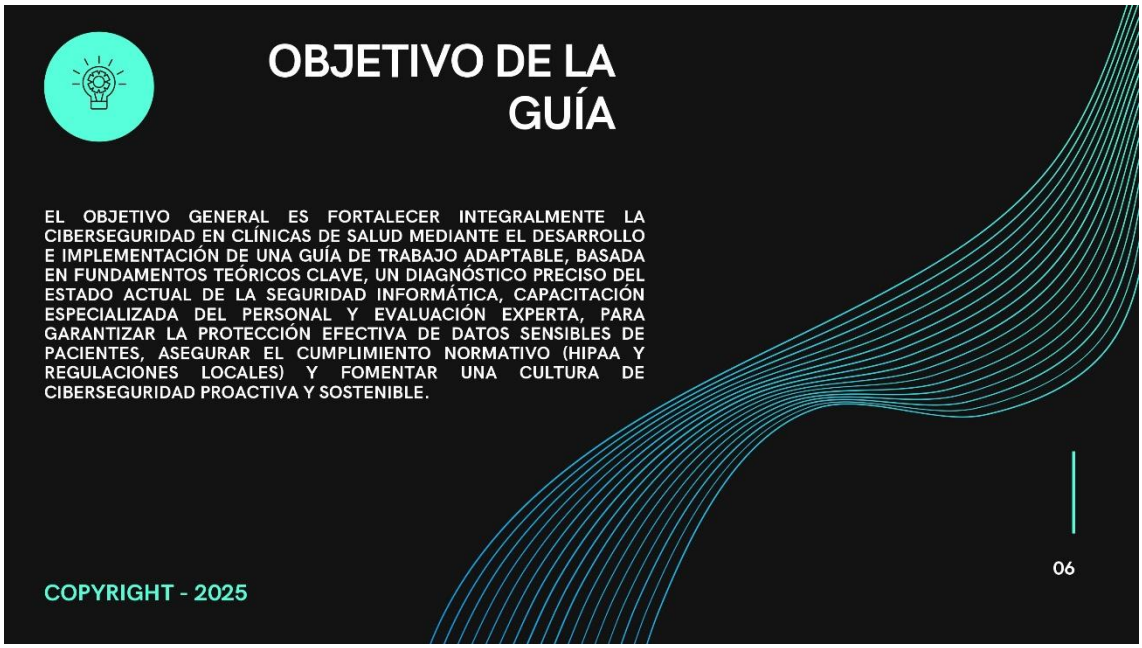
AMIGOS / FAMILIARES

Por su apoyo incondicional y aliento constante durante todo el proceso

Tabla de contenidos

GUÍA


INTRODUCCIÓN
LA CIBERSEGURIDAD ES VITAL EN LA SALUD DEBIDO A LOS DATOS SENSIBLES DE PACIENTES. ESTOS DATOS SON OBJETIVOS PARA CIBERDELINCUENTES, CON RIESGOS COMO ROBO DE IDENTIDAD. PROTEGER ESTA INFORMACIÓN ES ÉTICO Y LEGAL, CON LEYES COMO HIPAA QUE ESTABLECEN NORMAS. LAS ORGANIZACIONES DEBEN ENTENDER ESTAS LEYES Y SU IMPACTO DIARIO. A PESAR DEL CIFRADO Y RESTRICCIONES DE ACCESO, LOS ERRORES HUMANOS CAUSAN LA MAYORÍA DE LAS BRECHAS DE DATOS. LAS REGULACIONES SE ACTUALIZAN ANTE NUEVAS AMENAZAS. NO HAY UNA SOLUCIÓN ÚNICA, PERO EXISTEN PROVEEDORES DE SEGURIDAD DE DATOS COMPATIBLES CON HIPAA. ES CRUCIAL IMPLEMENTAR MEDIDAS ROBUSTAS PARA PROTEGER LA INFORMACIÓN Y EVITAR CONSECUENCIAS LEGALES Y ÉTICAS.
COPYRIGHT - 2025
05


OBJETIVO DE LA GUÍA
EL OBJETIVO GENERAL ES FORTALECER INTEGRALMENTE LA CIBERSEGURIDAD EN CLÍNICAS DE SALUD MEDIANTE EL DESARROLLO E IMPLEMENTACIÓN DE UNA GUÍA DE TRABAJO ADAPTABLE, BASADA EN FUNDAMENTOS TEÓRICOS CLAVE, UN DIAGNÓSTICO PRECISO DEL ESTADO ACTUAL DE LA SEGURIDAD INFORMÁTICA, CAPACITACIÓN ESPECIALIZADA DEL PERSONAL Y EVALUACIÓN EXPERTA, PARA GARANTIZAR LA PROTECCIÓN EFECTIVA DE DATOS SENSIBLES DE PACIENTES, ASEGURAR EL CUMPLIMIENTO NORMATIVO (HIPAA Y REGULACIONES LOCALES) Y FOMENTAR UNA CULTURA DE CIBERSEGURIDAD PROACTIVA Y SOSTENIBLE.
COPYRIGHT - 2025
06

IMPACTO DE OBJETIVOS

CARTERA CREATIVA

PACIENTES	LA PROTECCIÓN DE SUS DATOS SENSIBLES DE SALUD ES EL OBJETIVO PRIMORDIAL
PERSONAL MÉDICO	LA GUÍA DE CAPACITACIÓN LES PROPORCIONARÁ LAS HERRAMIENTAS Y CONOCIMIENTOS NECESARIOS PARA IDENTIFICAR Y PREVENIR AMENAZAS CIBERNÉTICAS
CLÍNICAS	FORTALECERÁN SU INFRAESTRUCTURA DE CIBERSEGURIDAD, REDUCIENDO EL RIESGO DE ATAQUES CIBERNÉTICOS

METODOLOGÍA

INVESTIGACIÓN CUALITATIVA

PARA CONTEXTUALIZAR LOS FUNDAMENTOS TEÓRICOS, ANALIZAR EL MARCO LEGAL

ENTREVISTAS
ENCUESTAS
ANÁLISIS DE DOCUMENTOS

INVESTIGACIÓN CUANTITATIVA

PARA DIAGNOSTICAR EL ESTADO ACTUAL DE LA CIBERSEGURIDAD EN LAS CLÍNICAS SELECCIONADAS. ESTO PODRÍA INCLUIR ENCUESTAS, AUDITORÍAS DE SEGURIDAD Y ANÁLISIS DE DATOS DE INCIDENTES CIBERNÉTICOS.

IDENTIFIACIÓN DE VULNERABILIDADES

MEJORA CONTINUA

La guía de trabajo global debe ser un documento dinámico, que se actualice periódicamente en función de los cambios en el panorama de amenazas y las mejores prácticas de ciberseguridad.

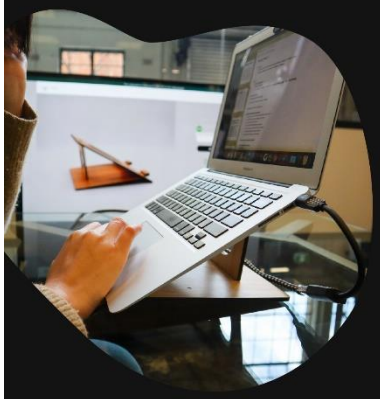
CUMPLIMIENTO

Esto incluye la implementación de controles de seguridad, la gestión de incidentes y la documentación de las actividades de seguridad.

ANÁLISIS DE RIESGO

Permitirá priorizar las medidas de seguridad y enfocar los recursos en las áreas de mayor riesgo.

USO DE LA GUÍA



CIBERSEGURIDAD

Se refiere a la protección de sistemas, redes y datos contra ataques digitales. En el contexto de la salud, implica salvaguardar la información del paciente de accesos no autorizados, modificaciones o destrucciones.

Datos Sensibles de Pacientes (PHI)

Es la información de salud protegida, que incluye datos personales identificables, historiales médicos, información de seguros y cualquier otro dato relacionado con la salud del paciente.

HIPAA
(LEY DE PORTABILIDAD Y RESPONSABILIDAD DEL SEGURO MÉDICO)

Es una legislación estadounidense que establece estándares para la protección de la información de salud del paciente.

AMENAZAS CIBERNÉTICAS

Incluyen malware, ransomware, phishing, ataques de denegación de servicio (DoS)

VULNERABILIDADES

Son debilidades en los sistemas de seguridad que pueden ser explotadas por ciberdelincuentes. Pueden incluir errores humanos, fallos de software o hardware, y falta de políticas de seguridad adecuadas.

PROCEDIMIENTO PASOS Y ESTRATÉGIAS

IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD

Realizar un análisis exhaustivo de todos los activos de información, identificando amenazas y vulnerabilidades potenciales.

Implementar un marco de gestión de riesgos continuo, que incluya evaluaciones periódicas y actualizaciones de los planes de mitigación.

Una clínica realiza un inventario de todos sus dispositivos conectados a la red, incluyendo computadoras, servidores, dispositivos médicos y dispositivos móviles. Luego, evalúa la seguridad de cada dispositivo y la probabilidad de que sea comprometido por un ataque cibernético.

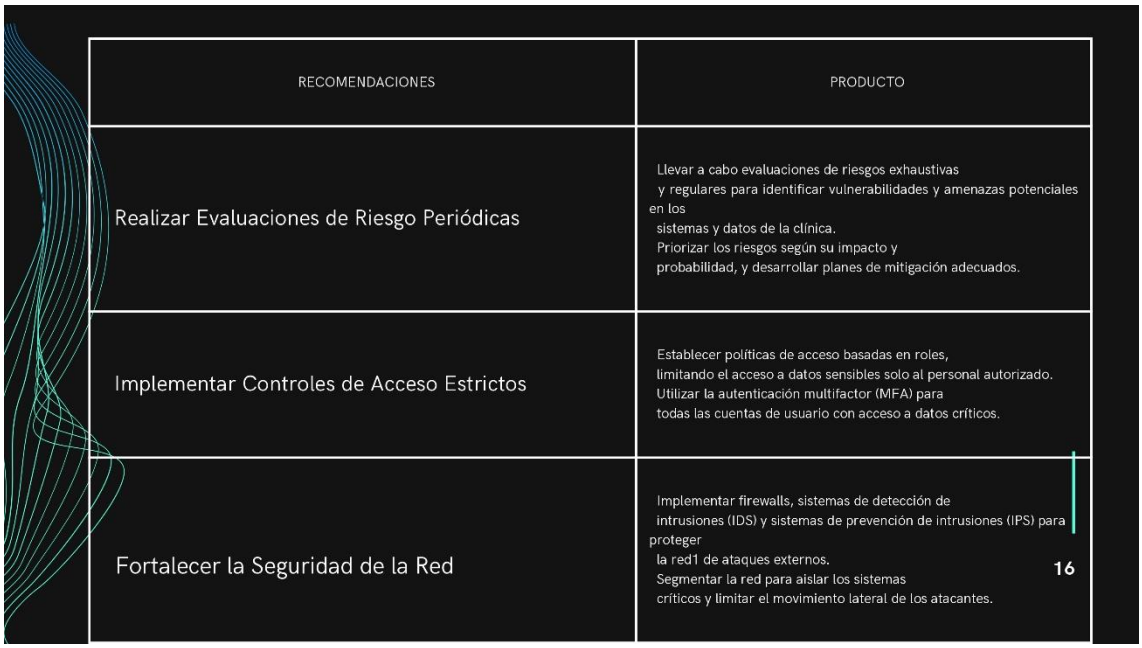
CAPACITACIÓN DEL PERSONAL

Desarrollar un programa de capacitación integral sobre ciberseguridad para todo el personal, incluyendo médicos, enfermeras, administradores y personal de TI

Fomentar una cultura de ciberseguridad en la clínica, donde todos los empleados comprendan su papel en la protección de los datos.

Una clínica realiza sesiones de capacitación periódicas sobre ciberseguridad, utilizando simulaciones de phishing para enseñar a los empleados a reconocer correos electrónicos maliciosos.


GESTIÓN DE INCIDENTES
Realizar simulacros periódicos para probar el plan y garantizar que el personal esté preparado para responder a un incidente.
Establecer un equipo de respuesta a incidentes dedicado y mantener líneas de comunicación abiertas con las autoridades y otros socios relevantes.
Una clínica realiza simulacros de ransomware para probar su plan de respuesta a incidentes, esto incluye simular un ataque de ransomware.
15
COPYRIGHT - 2025


RECOMENDACIONES
PRODUCTO
Realizar Evaluaciones de Riesgo Periódicas
Llevar a cabo evaluaciones de riesgos exhaustivas y regulares para identificar vulnerabilidades y amenazas potenciales en los sistemas y datos de la clínica. Priorizar los riesgos según su impacto y probabilidad, y desarrollar planes de mitigación adecuados.
Implementar Controles de Acceso Estrictos
Establecer políticas de acceso basadas en roles, limitando el acceso a datos sensibles solo al personal autorizado. Utilizar la autenticación multifactor (MFA) para todas las cuentas de usuario con acceso a datos críticos.
Fortalecer la Seguridad de la Red
Implementar firewalls, sistemas de detección de intrusiones (IDS) y sistemas de prevención de intrusiones (IPS) para proteger la red1 de ataques externos. Segmentar la red para aislar los sistemas críticos y limitar el movimiento lateral de los atacantes.
16

Proteger los Datos Sensibles	Cifrar los datos en reposo y en tránsito para protegerlos de accesos no autorizados. Realizar copias de seguridad regulares de los datos y almacenarlas en una ubicación segura y fuera del sitio.
Capacitar al Personal en Ciberseguridad	Desarrollar un programa de capacitación integral y continuo sobre ciberseguridad para todo el personal de la clínica. Enseñar a los empleados a reconocer y evitar ataques de phishing, malware y otras amenazas cibernéticas.
Desarrollar un Plan de Respuesta a Incidentes	Crear un plan de respuesta a incidentes detallado que defina los roles y responsabilidades, los procedimientos de notificación y los pasos para la recuperación. Realizar simulacros periódicos para probar el plan y garantizar que el personal esté preparado para responder a un incidente.

17

Mantener el Software Actualizado	Mantener todos los sistemas operativos, aplicaciones y software antivirus actualizados con los últimos parches de seguridad.
Cumplir con las Normativas de Privacidad	Implementar un proceso de gestión de parches para garantizar que las actualizaciones se apliquen de manera oportuna.
Cumplir con las Normativas de Privacidad	Realizar auditorías periódicas para evaluar el cumplimiento y realizar las correcciones necesarias.

18

ERRORES COMUNES PARA EVITAR.

MUCHAS CLÍNICAS UTILIZAN MÚLTIPLES SISTEMAS DE GESTIÓN DE CLAVES, LO QUE AUMENTA LA COMPLEJIDAD Y EL RIESGO DE ERRORES. NO ABORDAR ESTA COMPLEJIDAD CON SOLUCIONES EFECTIVAS PUEDE RESULTAR EN BRECHAS DE SEGURIDAD.

EL ERROR HUMANO ES UNA DE LAS PRINCIPALES CAUSAS DE VIOLACIONES DE DATOS EN EL SECTOR SALUD. IGNORAR LA NECESIDAD DE CAPACITAR AL PERSONAL EN PRÁCTICAS DE CIBERSEGURIDAD, COMO LA IDENTIFICACIÓN DE PHISHING Y EL MANEJO SEGURO DE DATOS, DEJA A LA CLÍNICA VULNERABLE.

LAS AMENAZAS CIBERNÉTICAS EVOLUCIONAN CONSTANTEMENTE, Y LAS REGULACIONES COMO HIPAA SE ACTUALIZAN PERIÓDICAMENTE. NO MANTENER LAS MEDIDAS DE SEGURIDAD ACTUALIZADAS DEJA A LA CLÍNICA EXPUESTA A NUEVAS VULNERABILIDADES.

SUGERENCIAS PARA UNA MEJOR IMPLEMENTACIÓN.

·UTILIZAR UNA COMBINACIÓN DE CONTROLES TÉCNICOS, ADMINISTRATIVOS Y FÍSICOS PARA PROTEGER LOS DATOS Y SISTEMAS. ESTO INCLUYE FIREWALLS, SISTEMAS DE DETECCIÓN DE INTRUSIONES, CIFRADO, AUTENTICACIÓN MULTIFACTOR Y POLÍTICAS DE ACCESO ESTRICTAS.

·EVALUAR REGULARMENTE LA EFECTIVIDAD DE LAS MEDIDAS DE SEGURIDAD Y REALIZAR AJUSTES SEGÚN SEA NECESARIO. ESTO AYUDA A IDENTIFICAR Y MITIGAR VULNERABILIDADES ANTES DE QUE SEAN EXPLOTADAS.

·INVOLUCRAR A TODO EL PERSONAL EN LA PROTECCIÓN DE LOS DATOS Y PROMOVER UNA ACTITUD PROACTIVA HACIA LA CIBERSEGURIDAD. ESTO INCLUYE LA CAPACITACIÓN CONTINUA, LA COMUNICACIÓN ABIERTA SOBRE INCIDENTES Y LA CREACIÓN DE UN ENTORNO DONDE LOS EMPLEADOS SE SIENTAN CÓMODOS REPORTANDO POSIBLES AMENAZAS

FACTORES DE ÉXITO

Liderazgo comprometido	El apoyo de la alta dirección es fundamental para la implementación exitosa de medidas de ciberseguridad. Los líderes deben demostrar su compromiso con la protección de los datos y asignar los recursos necesarios.
Colaboración y comunicación	La colaboración entre los departamentos de TI, seguridad, legal y clínico es esencial para abordar los desafíos de la ciberseguridad de manera integral. La comunicación abierta y fluida permite la identificación y resolución rápida de problemas
Adaptabilidad y mejora continua	El panorama de amenazas cibernéticas está en constante cambio, por lo que las clínicas deben ser capaces de adaptarse rápidamente a nuevas amenazas y vulnerabilidades. La mejora continua de las medidas de seguridad es crucial para mantener la protección de los datos.

21

REFLEXIÓN

La guía propuesta representa una herramienta esencial para las clínicas de salud, al proporcionar un marco integral que aborda los desafíos y riesgos específicos que enfrentan. Su importancia radica en su capacidad para Salvaguardar la privacidad del paciente

E-MAIL
cklopezp@gmail.com

CELULAR
0961789277

DIRECCIÓN
Quito

22