UNIVERSIDAD PRIVADA ANTENOR ORREGO

FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA DE COMPUTACIÓN Y SISTEMAS

Tesis para obtener el

Título Profesional de Ingeniero de Computación y Sistemas

"Modelo de auditoria basado NT MINSA N° 22-2005 y NTP ISOIEC: 27001-2014 para evaluar los sistemas de información de gestión de historias clínicas en los centros de salud ocupacional de la provincia de Trujillo - 2019"

Línea de Investigación

GESTIÓN DE PROYECTOS TECNOLÓGICOS

AUTORES:

Br. Jesús Eduardo Calixto Tello

Br. Julio César González Mayanga

ASESOR:

Ing. Jaime Eduardo Díaz Sánchez

AGOSTO DEL 2019

Trujillo, Perú

“MODELO DE AUDITORIA BASADO NT MINSA N° 22-2005 E NTP ISOIEC: 27001-2014 PARA EVALUAR LOS SISTEMAS DE INFORMACIÓN DE GESTIÓN DE HISTORIAS CLÍNICAS EN LOS CENTROS DE SALUD OCUPACIONAL DE LA PROVINCIA DE TRUJILLO - 2019”

Desarrollado por:

_____
Br. Julio César González Mayanga
Tesista

_____
Br. Jesús Eduardo Calixto Tello
Tesista

Aprobado por:

_____
Dr. Jorge Lorenzo Huapaya Escobedo
Presidente
Nº CIP: 17215

_____
Ing. Edward Fernando Castillo Robles
Secretario
N° CIP: 192352

_____
Ms. Jose Antonio Calderón Sedano
Vocal
N° CIP: 139198

_____
Ing. Jaime Eduardo Díaz Sánchez
Asesor
N° CIP: 73304

PRESENTACIÓN

Señores Miembros del Jurado:

De conformidad a lo estipulado en el Reglamento de Grados y Títulos de la Universidad Privada Antenor Orrego y el Reglamento interno de la Escuela Profesional de Ingeniería de Computación y Sistemas, pongo a vuestra disposición la presente Tesis titulada: “MODELO DE AUDITORIA BASADO NT MINSA N° 22-2005 E NTP ISOIEC: 27001-2014 PARA EVALUAR LOS SISTEMAS DE INFORMACIÓN DE GESTIÓN DE HISTORIAS CLÍNICAS EN LOS CENTROS DE SALUD OCUPACIONAL DE LA PROVINCIA DE TRUJILLO - 2019”, para obtener el Título Profesional de Ingeniero de Computación y Sistemas.

El contenido del presente trabajo ha sido desarrollado tomando como marco de referencia los lineamientos establecidos por la Escuela Profesional de Ingeniería de Computación y Sistemas y los conocimientos adquiridos durante nuestra formación profesional, consulta de fuentes bibliográficas e información obtenida en la institución de la Superintendencia Nacional de Registros Públicos Zona Registral V – Sede Trujillo.

DEDICATORIA

Siempre agradecer primero a Dios, el que me ha dado fortaleza y salud para continuar y poder haber llegado hasta este momento tan importante de mi formación profesional.

A mi padres: ***Julio González,*** quien siempre dándome su ejemplo e inculcándome buenos valores y conocimientos necesarios para llegar a esta etapa de mi vida *y mi madre* ***Janet Mayanga Conde*** quien siempre fue mi incondicional apoyo en todo momento, por siempre alentarme a enfrentarme a retos nuevos en la vida, a ambos por ser el pilar más importante y por demostrarme siempre su cariño, ha sabido formarme con sentimientos, hábitos y valores, lo cual me ha ayudado a salir adelante en los momentos más difíciles quienes con sus consejos ha sabido guiarme para culminar mi carrera profesional.

A mi familia en general, por siempre apoyarme en todos los sentidos durante mi carrera profesional.

A mi pareja: ***Jeunisse Danae Calle Medina*** que me ha brindado su apoyo incondicional, por apoyarme a retomar este camino y nunca dejarme flaquear en el proceso.

A mi asesor **Ing. Jaime Eduardo Díaz Sánchez** por su trabajo de transmitirme sus diversos conocimientos, especialmente del campo y de los temas que corresponden a mi profesión, pero sobre todo por su apoyo, paciencia y gran colaboración para realizar esta obra, ya que sin ayuda no se hubiera podido realizar.

En general, les pido a todos disculpas por el tiempo tardado, muchas gracias.

Julio Cesar González Mayanga

DEDICATORIA

Para comenzar dedico está obra a Dios por permitirme tener vida, salud y fuerza, para poder realizar uno de mis más grandes proyectos que es ser Ingeniero de Sistemas, el cual se está logrando con mucho esfuerzo y dedicación.

A mi madre **Flor Guadalupe Calixto Tello** por brindarme su amor, apoyo, paciencia, compresión y educación durante toda mi vida y mi carrera profesional; ya que nunca se ha rendido conmigo y siempre ha estado para darme todo lo necesario y brindarme las herramientas para mi desarrollo personal y profesional; además de ser mi motivación e inspiración para poder superarme cada día más.

A mis abuelos **Meyer Calixto Flores** y **Luz Violeta Tello Carrillo** quienes con sus palabras de aliento no me dejaban decaer para que siguiera adelante y siempre sea perseverante y cumpla con mis ideales

A mis tíos **Guillermo Eduardo Calixto Tello, Luz Estela Calixto Tello y Cesar Luis Martín Calixto Tello** por ser ejemplos de formación personal y profesional, ya que ellos también me enseñaron que con el trabajo y perseverancia se encuentra el éxito profesional

A mi asesor **Ing. Jaime Eduardo Díaz Sánchez** por su trabajo de transmitirme sus diversos conocimientos, especialmente del campo y de los temas que corresponden a mi profesión, pero sobre todo por su apoyo, paciencia y gran colaboración para realizar esta obra, ya que sin ayuda no se hubiera podido realizar.

Y en general a todos mis **maestros, amigos y compañeros** quienes sin esperar nada a cambio compartieron su conocimiento, alegrías y tristezas en diferentes momentos de mi vida.

Jesús Eduardo Calixto Tello

AGRADECIMIENTOS

Expresamos nuestro profundo agradecimiento a:

En primer lugar, a Dios quien nos dio la vida y nos ha llenado de bendiciones en todo este tiempo, a él que, con su infinito amor, nos ha dado la sabiduría suficiente para culminar nuestra carrera universitaria.

Queremos expresar nuestro más sincero agradecimiento, reconocimiento y cariño a nuestros padres por todo el esfuerzo que hicieron para darnos una profesión y hacer de nosotros personas de bien, gracias por los sacrificios y la paciencia que demostraron todos estos años; gracias a ustedes hemos llegado a donde estamos.

Gracias a nuestros hermanos quienes han sido nuestros amigos fieles y sinceros, en los que hemos podido confiar y apoyarnos para seguir adelante.

Gracias a todas aquellas personas que de una u otra forma nos ayudaron a crecer como personas y como profesionales.

Todos los ingenieros los cuales nos proporcionaron las enseñanzas necesarias para nuestra formación como ingenieros de Computación y Sistemas, y también de manera especial a nuestro asesor de tesis quién con sus conocimientos y apoyo supo guiar el desarrollo de la presente tesis desde el inicio hasta la culminación.

“MODELO DE AUDITORIA BASADO NT MINSA N° 22-2005 E NTP ISOIEC: 27001-2014 PARA EVALUAR LOS SISTEMAS DE INFORMACIÓN DE GESTIÓN DE HISTORIAS CLÍNICAS EN LOS CENTROS DE SALUD OCUPACIONAL DE LA PROVINCIA DE TRUJILLO - 2019”

RESUMEN

Por: Bach. Calixto Tello, Jesús Eduardo
Bach. González Mayanga, Julio César

Del estándar internacional de seguridad de la información ISO 27001-2014 y la Norma Técnica MINSA N° 22-2005 se concluye que al intersectar ambas normativas se tiene como resultado pautas para llegar a generar un modelo de auditoria basado en lo común de estas normas, el que nos permite evaluar la seguridad de la información en los sistemas de gestión de salud ocupacional cumpliendo con las normativas establecidas en dicho sector.

Este modelo de auditoria permitirá evaluar la seguridad de la información en los sistemas de información de los centros de salud ocupacional, acorde a lo establecido en la NT MINSA N° 22-2005 bajo los estándares internacionales de la NTP ISOIEC 27001-2014.

El modelo de auditoria ha sido creado tomando como muestra, población, casuística y realidad problemática, el sistema de la clínica Lezama de Salud Ocupacional SCRL ubicada en la ciudad de Trujillo, La Libertad, Perú.

El modelo está definido en 9 procesos que involucran el control de acceso, privilegios, simultaneidad, accesibilidad, confidencialidad, recuperabilidad, inviolabilidad y resguardo de información. Estos 9 procesos permiten realiza una auditoria basada en las normas ya anteriormente mencionadas.

Se contó con entradas de informaciones brindadas y/o obtenidas de la empresa auditada, las cuales fueron analizadas y evaluadas en cada uno de los procesos por cada una de sus actividades o subprocesos.

Una vez evaluado el modelo de auditoria fue sometido a evaluación a través de juicio de expertos, los cuales comprobaron la validez y veracidad del modelo creado.

Palabras Clave: Coeficiente de V de Aiken, juicio de expertos, metodología, plan de acción, Backups, Auditoria, Objetivo de control, ISO.

“AUDIT MODEL BASED NT MINSA N ° 22-2005 E NTP ISOIEC: 27001-2014 TO EVALUATE CLINICAL TRIAL MANAGEMENT INFORMATION SYSTEMS AT OCCUPATIONAL HEALTH CENTERS OF THE TRUJILLO PROVINCE – 2019”

ABSTRACT

By: Bach. Calixto Tello, Jesús Eduardo
Bach. González Mayanga, Julio César

From the international standard of information security ISO 27001-2014 and the Technical Standard MINSA N ° 22-2005 it is concluded that when intersecting both regulations results in guidelines to generate an audit model based on the common of these standards, which allows us to evaluate the security of information in occupational health management systems complying with the regulations established in said sector. This audit model will allow the evaluation of information security in the information systems of occupational health centers, in accordance with the provisions of NT MINSA No. 22-2005 under the international standards of NTP ISOIEC 27001-2014. The audit model has been created taking as a sample, population, casuistry and problematic reality, the SCRL Lezama Occupational Health clinic system located in the city of Trujillo, La Libertad, Peru. The model is defined in 9 processes that involve the control of access, privileges, simultaneity, accessibility, confidentiality, recoverability, inviolability and protection of information. These 9 processes allow an audit based on the aforementioned standards. There were entries of information provided and / or obtained from the audited company, which were analyzed and evaluated in each of the processes for each of its activities or subprocesses. Once the audit model was evaluated, it was submitted for evaluation through expert judgment, which verified the validity and veracity of the model created.

Key words: Aiken V coefficient, expert judgment, methodology, action plan, Backups, Audit, Control objective, ISO

Contenido

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO I: INTRODUCCIÓN

1. INTRODUCCIÓN

1.1. Realidad problemática

Cuando hablamos de Auditoria no referimos a un examen críticos que es realizado por una persona o un grupo de personas especializadas evaluando un sistema de información o información relacionada a un proceso, dichas personas son independientes del sistema auditado (persona, organización, sistema, proceso, proyecto o producto). La auditoría informática es un proceso necesario que debe ser realizado por personal especializado para garantizar que todos los recursos tecnológicos operen en un ambiente de seguridad y control eficientes, de manera que la entidad tenga la seguridad de que opera con información verídica, integral, exacta y confiable. Además, la auditoría deberá contener observaciones y recomendaciones para el mejoramiento continuo de la tecnología de la información en la institución. (Rodriguez, 2012)

La Salud Ocupacional y la Medicina Ocupacional son consideradas hoy como pilares fundamentales en el desarrollo de un país, al estar sus acciones dirigidas a la promoción y protección de la salud de los trabajadores y la prevención de accidentes de trabajo y enfermedades ocupacionales.

Existen diversas empresas acreditadas para desarrollar de sistema de información en salud ocupacional entre ellas:

- **MEDIWEB**, conformada por un equipo de ingenieros que en colaboración con profesionales de la salud y que han desarrollado innovadores sistemas para clínicas con el fin de brindar un manejo integral de las operaciones que realizan en ellas. (PERU M. , s.f.)
- **LOLIMSA**, pertenece al reducido grupo de empresas especializadas en el desarrollo de tecnologías de la información para el sector salud, en más de 2,000 clientes en 10 países en Latinoamérica, los que incluyen hospitales, clínicas, centros médicos, cadenas de farmacias y laboratorios clínicos. (PERU L. , s.f.)

- **SISTEMAS CLÍNICOS**, están conformados por un grupo de médicos ex-residentes del Hospital Italiano de Buenos Aires que junto a un grupo de programadores se dedican exclusivamente a brindar soluciones informáticas en Salud, utilizando como plataforma la tecnología web. (ARGENTINA, s.f.)

  Lezama Consultores de Salud Ocupacional SCRL fue creado el 27 de Marzo del 2002, con el objeto de dedicarse a las Prestaciones de Servicios de Salud Ocupacional con atención de salud, actividades de Asesoría, Asistencia técnica, Capacitación y adiestramiento en Prevención de Riesgos Ocupacionales a empresas de los diferentes sectores económicos, en el Departamento de la Libertad y en el ámbito Nacional. Actualmente, se cuenta la una estructura organizacional mostrada en la Imagen N° 2. Lezama Consultores, cuenta con Servicio de Admisión, Triaje, Evaluación oftalmológica, Evaluación médica ocupacional, Audiometría, Espirómetria, Electrocardiograma, Evaluación Psicocensometrico y Servicios de Laboratorio y Radiología. Su personal está calificado y acreditado para realizar los exámenes médicos ocupacionales. Asimismo, desarrolla programas de capacitación en prevención de riesgos ocupacionales, Implementación de sistemas de seguridad y salud en la en las empresas.

  En el Perú, el Ministerio de Salud en al año 2005 emitió la Norma Técnica de Salud N° 22-MINSA-2005 (Ministerio de Salud, 2005), con la finalidad establecer las normas y procedimientos para la administración y gestión de las historias clínicas. Así como estandarizar el contenido básico de la Historia Clínica para garantizar un apropiado registro de las atenciones de salud.

  El estándar NTP ISO/IEC 27001:2014 (ISO, 2013) es el estándar que proporciona requisitos para un sistema de gestión de seguridad de la información. Específica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI) Las organizaciones optan por aplicar la norma con el fin de beneficiarse de las mejores prácticas que contiene.

  Actualmente el siguiente proyecto de tesis se desarrolla basado en que no se cuenta con un modelo de auditoria que enfoque ambos estándares (Norma Técnica de

Salud N° 22-MINSA-2005 y NTP ISO/IEC 27001:2014) con la finalidad de obtener la información más exacta y requerida, para el mejoramiento de los estándares de confidencialidad de la información.

1.2. Delimitación del problema

El presente trabajo de investigación se limita al diseño y elaboración de un modelo de auditoria basado en la ISO 27001:2014 adaptado a la NTP MINSA N°22:2005, este modelo no será aplicado para validar su cumplimiento. Se otorgara una validación y comprobación a través de un juicio a experto (V de AIKEN) siendo esta la actividad final.

1.3. Características y análisis del problema

1.3.1. Características

a. No se evalúa la integridad, accesibilidad y confidencialidad de las historias clínicas informatizadas adaptadas a la NTP MINSA N°22:2005.
b. Falta de control en verificar la generación de copia de resguardo.
c. No se considera en la evaluaciones las opciones de reporte y acceso
d. Falta de control al evaluar la adecuada duplicidad de datos.
e. Falta de seguridad en los servidores y resguardo de información.
f. Incumplimiento del rol de usuario del sistema.
g. La confidencialidad de la información no es la adecuada.

1.3.2. Análisis

a. No se realiza una evaluación adaptada en la NTP MINSA N°22:2005 enfocándose en la integridad, accesibilidad y confidencialidad de los datos de las historias clínicas informatizadas en los centros de salud ocupacional.
b. Falta de control de la seguridad de la información y seguimiento de control y verificación de resguardo de la información.
c. No se evalúan y controlan el acceso a las opciones de generación de reportes o información que se pueden obtener del sistema.

d. Se debe evaluar el adecuado uso de la duplicidad de datos, evaluando la integridad, consistencia y confidencialidad de la información ya que al presentarse duplicidad esta se puede ver expuesta.

e. Falta de verificación y medidas preventivas para posibles ataques a servidores, así como la información expuesta en la organización o internet y la seguridad del almacén de copias de resguardo.

f. No se verifica el cumplimiento de los usuarios que acceden al sistema de acuerdo a sus roles asignados.

g. La confidencialidad de la información no es la adecuada conforme a los estándares que se proponen en el modelo de auditoria basado en la NT MINSA N° 22-2005 e NTP ISO/IEC 27001:2014, ya que se busca la protección, buen uso y restricción de la información.

1.4. Formulación del Problema

¿Cómo impacta el uso de un modelo de auditoria basado en la ISO 27001-2014 adaptado a la NTP MINSA 22-2005 en el nivel de Seguridad de los sistemas de información de historias clínicas de los Centros de Salud Ocupacional?

1.5. Formulación de la Hipótesis

Un modelo de auditoria basado en la ISO 27001-2014 adaptado a la NTP MINSA 22-2005 va a permitir probablemente, mejorar el nivel de seguridad en términos de la integridad, accesibilidad y confidencialidad de los sistemas de información para la gestión de historias clínicas de los Centros de Salud Ocupacional.

$NSSIH_A$: Nivel de Seguridad en los Sistemas de Información de Historias Clínicas Actuales
$NSSIH_P$: Nivel de Seguridad en los Sistemas de Información de Historias Clínicas Posterior la evaluación.
MA: Modelo de Auditoria

NSSIHA -> MA -> NSSIHP

Hipótesis Alternativa (H1): Se mejorará la integridad, accesibilidad y confidencialidad de los sistemas de información de historias clínicas actuales, al aplicar el modelo de auditoria basado en la ISO 27001.

H1: $NSSIH_A < NSSIH_P$

Hipótesis Nula (H0): El modelo de auditoria basado en la ISO 27001 no permitirá o no mejorará la integridad, accesibilidad y confidencialidad de los sistemas de información de historias clínicas actuales

H0: $NSSIH_A >= NSSIH_P$

1.6. Objetivos del estudio

a. Objetivo General

Diseñar un modelo de auditoria basado en la ISO 27001-2014 adaptado a la NTP MINSA 22-2005 para evaluar el nivel de seguridad de los sistemas de información de historias clínicas en los Centros de Salud Ocupacional y comprobación mediante Juicio de Expertos que el nivel de seguridad mejora.

b. Objetivos Específicos

Etapa 1: "***Identificar las principales características de: NT MINSA N°22 e NTP ISO/IEC 27001:2014"***.

Se realizará el estudio de las normativas usadas en la elaboración de del modelo de auditoria informática, se evaluarán normas, técnicas, estándares y procedimientos del proceso que garanticen el éxito del proceso, así como la mayoría de documentación existente relacionada en la elaboración de dicho modelo.

Etapa 2: ***"Identificar la similitud entre ambas normativas"***.

Se identificará las similitudes entre ambas normativas (NT MINSA N°22 e NTP ISO/IEC 27001:2014) se generará un matriz donde se intersectarán los puntos comunes entre ambas normativas.

Etapa 3: ***"Generar un modelo de auditoria basado en ambas normativas".***

Se elaborará el modelo de auditoria en base a la matriz de intersección, identificando procesos, subprocesos, entradas y salidas.

Etapa 4: ***"Diseñar los artefactos de auditoria para la aplicación del modelo basado en la ISO 27001 adaptado a la NTP MINSA N°22".***

Se elaborarán artefacto de auditoria los cuales serán cuestionarios y checklist que serán usados para la recolección de la información.

Etapa 5: ***"Comprobar que el modelo de auditoria generado, mediante juicio de expertos genera impacto positivo".***

Se comprobará el modelo de auditoria a través del juicio de expertos aplicando la V de AIKEN genera un impacto positivo.

1.7. Justificación del Estudio

- **Tecnológica**

  El modelo de auditoria propuesto se apoya en el uso de la tecnología reforzando la integridad, accesibilidad y confidencialidad de los sistemas de información de historias clínicas ocupacionales.

- **Económica**

  Se estima que el modelo de auditoria diseñado beneficiará a los centros de salud ocupacional que lo apliquen ya que se evaluara la integridad, accesibilidad y confidencialidad permitiendo mejoras en ellas.

- **Legal**

  La aplicación del modelo de auditoria diseñado y el cumplimiento de cada uno de los puntos a evaluar evitar cualquier problema legal a la integridad, accesibilidad y confidencialidad de la información en los sistemas de historias clínicas ocupacionales.

- **Operacional**

  Integridad, accesibilidad y confidencialidad como una característica esencial operacional los sistemas de información de historias clínicas ocupacionales.

- **Sistémica o Social**

  Se buscar brindar un modelo basado en la ISO 27001-2014 adaptado a la NTP MINSA 22-2005 con el cual se evalué la integridad, accesibilidad y confidencialidad como puntos clave en la institución.

- **Académica**

  A través de esta modelo se busca aportar un nuevo enfoque de auditoria para las clínicas de salud ocupacional tomando como puntos clave la integridad, accesibilidad y confidencialidad de la información de historias clínicas, siendo el punto base de estudio para el desarrollo y mejoramiento de este nuevo modelo diseñado.

1.8. Limitaciones del estudio

- Dificultades operacionales para implantar el modelo en forma completa en un periodo de tiempo razonable, por lo que se determina la contrastación mediante juicio a expertos.

CAPÍTULO II: MARCO TEÓRICO

2. MARCO TEÓRICO

2.1. Antecedentes

Existe un variado y extenso conjunto de investigaciones, proyectos, metodologías y herramientas; que tienen como objetivo principal gestionar la confidencialidad, accesibilidad y disponibilidad de la información en las empresas.

Aparte de la familia de normas ISO/IEC 27000 que consideran la seguridad como punto primordial los siguientes trabajos que se mencionan a continuación tratan estas metodologías y/o métodos que son objeto de análisis y referencia para el presente trabajo.

Tesis doctoral: Metodología para la incorporación de medidas de seguridad en sistemas de información de gran implantación.

Autor: *Juan Jesús Muñoz Esteban*

Tutor: *Dr. José Antonio Mañas Árgema.*

Los orígenes de internet y su principio talante han conducido a un modelo de servicio un tanto confiado que arrastre una imagen de inseguridad. Se dispone de multitud de tecnologías de demostrada solvencia técnica, que resuelve problemas en ámbito concretos, pero que no se integran en un modelo global de seguridad.

Tesis doctoral: Estudio de una estrategia para la implantación de los sistemas de gestión de la seguridad de la información.

Autor: *Manuel Fernández Barcell*

Para el cumplimiento los objetivos en materia de seguridad, es necesario que las administraciones, profesionales y empresas puedan organizar su política de seguridad. Muchas organizaciones no abordan de modo serio una política de seguridad “formal” (según norma) por la complejidad de la misma.

Las metodologías y normas existentes relacionadas con los SGSI no aclaran sus ámbitos de aplicación, resultando una amalgama de normas de compleja aplicación.

Tesis de maestría: Modelo de seguridad informática para la gestión académica en la Universidad Nacional del Centro del Perú

Autor: *Mercado Rivas Richarad Yuri.*

Tutor. *Fidel Arauco Canturin.*

Se entiende como seguridad una característica de cualquier sistema que nos indica que ese sistema está en peligro, daño o riesgo. Se entiende como daño o peligro todo aquello que pueda afectar su funcionamiento directo o los resultados que se obtienen del mismo.

Para que un sistema se pueda definir como seguro se debe de dotar de tres características al mismo: integridad, confidencialidad y disponibilidad, dependiendo de las fuentes de amenazas, la seguridad puede dividirse en seguridad lógica y seguridad física.

En el contexto del trabajo de investigación se va a poner énfasis a la seguridad informática en la gestión académica dentro de la Universidad Nacional del Centro del Perú UNCP

2.2. Bases teóricas

Redactar los aportes científicos: conceptos, modelos y teorías que orientan al análisis del problema y objeto de estudio, que permiten el enjuiciamiento crítico de las teorías relacionadas directamente con el problema de estudio. Se debe citar cada concepto, modelo o teoría de acuerdo a las normas APA 6ª edición.

Puede estructurarse en base a:

- Origen y evolución del objeto de estudio
- Análisis de las distintas posiciones del objeto de investigación.
- Valoración crítica de los principales conceptos de las distintas posiciones teóricas sobre el objeto de investigación. Acá se deja en claro la posición que el investigador asume para realizar el diagnóstico de la realidad y la presentación de su propuesta.
- Desarrollo de los conceptos en base a un esquema de contenidos.

2.3. Definición de términos

AUDITORÍA

a. Concepto

La auditoría es el examen crítico y sistemático que realiza una persona o grupo de personas independientes del sistema auditado, que puede ser una persona, organización, sistema, proceso, proyecto o producto.

La auditoría es una serie de métodos de investigación y análisis con el objetivo de producir la revisión y evaluación profunda de la gestión efectuada. (Amado Suárez, 2008).

b. Rol del Auditor

Por su parte, el auditor es una persona capacitada y con la suficiente experiencia para revisar y verificar que los datos contables que la empresa auditada facilita se corresponden realmente con la actividad que ha venido desarrollando.

El auditor tiene que redactar un informe al concluir la auditoría determinando el grado de veracidad y claridad que la organización posee.

c. Tipos de Auditoria

- **Auditoría Informática:** Procesos de recoger, agrupar y evaluar evidencias para determinar si un sistema de información salvaguarda el activo empresarial, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos.
    - **Auditoría Interna**: Es aquella que se hace adentro de la empresa; sin contratar a personas de afuera. Es una actividad independiente y objetiva de aseguramiento y consulta concebida para agregar valor y mejorar las operaciones de una organización. Ayuda a una organización a cumplir sus objetivos aportando un enfoque sistemático y disciplinado para evaluar y mejorar la eficacia de los procesos de gestión de riesgos, control y gobierno.

      Se evalúan los siguientes puntos:

        - Eficacia y eficiencia de las operaciones.
        - Confiabilidad e integridad de la información financiera y operativa.
        - Protección de activos.
        - Cumplimiento de leyes, regulaciones y contratos.

    - **Auditoría Externa**: La auditoría externa es un proceso de evaluación sistemático, exhaustivo, crítico y detallado de un determinado sistema de una empresa. El estudio se llevará cabo por personal ajeno a la empresa, con el fin de que pueda emitir una opinión independiente que de credibilidad frente a terceros, ya que, en la mayoría de los casos, el informe se emitirá bajo fe pública.

      Así, los fines principales de la auditoría externa son adquirir razonabilidad, integridad y autenticidad de los estados analizados, con el objeto de conocer, por la propia empresa, la situación de sus activos y pasivos así como dar a saber dicha situación a clientes, proveedores, accionistas y resto de personas o entidades interesadas. Según el carácter de la función de los auditores externos esta podrá ser obligatoria o voluntaria. El procedimiento de auditoría externa será realizado por una persona o entidad especializada ajena a entidad, capaz de emitir una opción independiente y de emitir al final del proceso un informe completo sobre el estado del sistema analizado. Para ello, la entidad auditada no

podrá poner restricciones a su trabajo y facilitar, en todo momento, toda la documentación o información que precise el auditor.

- **Auditoría Forense:** Cuando se revisan datos y documentos históricos de empresas y se comparan con el fin de detectar principalmente fraudes, robos, trucos fiscales, trucos contables o cualquier otra situación anómala en la que se investiga a los involucrados intelectuales y materiales del hecho; regularmente se hacen estimaciones en dinero de las cifras malversadas.
- **Auditoría de accesibilidad:** consiste en la revisión de la accesibilidad de un sitio web por parte de un experto. Al final de la auditoría, el auditor informa de posibles problemas de accesibilidad y proporciona recomendaciones para solucionar los problemas.

- **Auditoría de seguridad de sistemas de información:** Análisis y gestión de sistemas para identificar y posteriormente corregir las diversas vulnerabilidades que pudieran presentarse en una revisión exhaustiva de las estaciones de trabajo, redes de comunicación o servidores.

Tipos:

- **Auditoría de seguridad interna.** En este tipo de auditoría se contrasta el nivel de seguridad y privacidad de las redes locales y corporativas de carácter interno
- **Auditoría de seguridad perimetral.** En este tipo de análisis, el perímetro de la red local o corporativa es estudiado y se analiza el grado de seguridad que ofrece en las entradas exteriores
- **Test de intrusión.** El test de intrusión es un método de auditoría mediante el cual se intenta acceder a los sistemas, para comprobar el nivel de resistencia a la intrusión no deseada. Es un complemento fundamental para la auditoría perimetral.
- **Análisis forense.** El análisis forense es una metodología de estudio ideal para el análisis posterior de incidentes, mediante el cual se trata de reconstruir cómo se ha penetrado en el sistema, a la par que se valoran los daños ocasionados. Si los daños han provocado la inoperatividad del sistema, el análisis se denomina análisis postmortem.

d. Auditoría Informática:

Muchos autores coinciden en que la auditoría informática (AI) nació como una extensión de la auditoría general, sus investigaciones y desarrollos se originaron a comienzos de la década de los 60, siendo en el año de 1977 cuando realmente la AI adquiere las características que la identifican actualmente, luego de publicarse la primera edición de Systems Auditability and Control (SAC), un trabajo conjunto del Institute of InternalAuditors (IIA), IBM y Stanford ResearchInstitute (SRI). (Lorenzo Gil, n.d.).

Objetivos: El alcance ha de definir con precisión el entorno y los límites en que va a desarrollarse la auditoria informática, se complementa con los objetivos de ésta. El alcance ha de figurar expresamente en el Informe Final, de modo que quede perfectamente determinado no solamente hasta que puntos se ha llegado, sino cuales materias fronterizas han sido omitidas.

e. Tipos de Auditoría Informática

- **Auditoría de la gestión:** La auditoría de gestión es una técnica relativamente nueva de asesoramiento que ayuda a analizar, diagnosticar y establecer recomendaciones a las empresas, con el fín de conseguir con éxito una estrategia. Uno de los motivos principales por el cual una empresa puede decidir emprender una auditoría de gestión es el cambio que se hace indispensable para reajustar la gestión o la organización de la misma.

- **Auditoría legal del Reglamento de Protección de Datos**: Cumplimiento legal de las medidas de seguridad exigidas por el Reglamento de desarrollo de la Ley Orgánica de Protección de Datos.

  Objetivos principales: Tiene como objetivo el estudio Verificación e Identificación de los datos de carácter personal, Niveles de Seguridad, Documento Legal, Documento de Seguridad. Inscripción, modificación y cancelación de ficheros ante la Agencia Española de Protección de Datos, Revisión de la auditoria.

- **Auditoría de los datos**: Clasificación de los datos, estudio de las aplicaciones y análisis de los flujogramas. El análisis de datos encierra dos procedimientos. La organización de los datos y la descripción y análisis de los datos. Las técnicas de análisis de datos se clasifican en dos tipos: Técnicas de análisis cuantitativo y técnicas de análisis cualitativo.

- **Auditoría de las bases de datos**: Es el proceso que permite medir, asegurar, demostrar, monitorear y registrar los accesos a la información almacenada en las bases de datos incluyendo la capacidad de determinar:
  - Quién accede a los datos.
  - Cuándo se accedió a los datos.
  - Desde qué tipo de dispositivo/aplicación.
  - Desde que ubicación en la Red.
  - Cuál fue la sentencia SQL ejecutada.
  - Cuál fue el efecto del acceso a la base de datos.

  Los objetivos Generales de la Auditoría de BD son: Disponer de mecanismos que permitan tener trazas de auditoría completas y automáticas relacionadas con el acceso a las bases de datos incluyendo la capacidad de generar alertas.

- **Auditoría de la seguridad**: Una auditoría de seguridad consiste en apoyarse en un tercero de confianza (generalmente una compañía que se especializada en la seguridad informática) para validar las medidas de protección que se llevan a cabo, sobre la base de la política de seguridad.

  El objetivo de la auditoría es verificar que cada regla de la política de seguridad se aplique correctamente y que todas las medidas tomadas conformen un todo coherente.

  Una auditoría de seguridad garantiza que los conjuntos de disposiciones tomadas por la empresa se consideren seguras.

- **Auditoría de la seguridad física**: Se refiere a la protección de hardware y los soportes de datos, así también como la seguridad de los edificios y las instalaciones que lo albergan. Esto contempla situaciones de incendios, inundaciones, sabotajes, robos, catástrofes naturales, etc.

  Consiste en la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial.

- **Auditoría de la seguridad lógica**: Comprende los métodos de autenticación de los sistemas de información. En validar y evaluar la aplicación de barreras y procedimientos que resguarden el acceso a los datos y solo se permita acceder a ellos a las personas autorizadas para hacerlo. La seguridad lógica al referirse a controles lógicos dentro del software se implementa mediante la construcción de contraseñas en diversos niveles del sistema donde permita solo el acceso en base a niveles de seguridad de usuarios con permiso.

- **Auditoría de las comunicaciones**. La auditoría de comunicación analiza en profundidad los mensajes que emite su organización, y cómo son percibidos estos por las personas a los que van dirigidos, ya sean audiencias internas o externas a la organización.

  La auditoría de comunicación, es una herramienta indispensable para evaluar la identidad (lo que decimos que somos) y la imagen (cómo somos percibidos) de su organización. Identifica si se usa un tono coherente, consistente y honesto, o si por el contrario, se trata de un tono confuso y generador de desconfianza.

  Habitualmente, al realizar una auditoría de comunicación suelen analizarse algunas cuestiones como:

  - Cómo funciona el sistema de comunicación y quiénes lo dirigen.
  - Cómo es percibida la empresa por sus distintos públicos.
  - Qué vínculos existen la comunicación interna y la externa.
  - Contenidos, calidad y valor para las audiencias (internas y externas) de los materiales de comunicación. Etc.

- **Auditoría de la seguridad en producción**: Consiste en auditar un proceso o concreto para obtener una información objetiva y real. La auditoría de seguridad en producción significa planear, organizar, coordinar dirigir y controlar las actividades relacionadas a mantener y garantizar la integridad física de los recursos implicados en la función informática, así como el resguardo de los activos de la empresa.

f. Objetivos de la Auditoria Informática

Piattini sostiene que la auditoria informática confirma la consecución de los objetivos tradicionales de la auditoria: objetivos de protección de activos e integridad de datos; y objetivos de gestión, que abarcan no solamente los de protección de activos, sino también los de eficacia y eficiencia. (Piattini, Del Peso, 2003).

Caridad Simón en sus apuntes de Auditoría Informática (2006, p.15) cita a Ron Weber (1982) quien separa los objetivos de la AI en cuatro grupos: objetivos de salvaguarda de bienes; objetivos de integridad de datos; objetivos de efectividad del sistema y objetivos de eficiencia del sistema. (Caridad Simón, 2006).

g. Base de la Auditoria Informática

Serafín Caridad Simón (2006), en su obra Auditoría Informática, considera a la Auditoría Informática (AI) como la intersección de cuatro disciplinas: Auditoría Tradicional, Ciencias del Comportamiento, Gestión de Sistemas de Información e Informática.

Figura 1**: **Intersección de otras disciplinas. Basado en Caridad Simón, (2006, p.18)

h. Funciones de la Auditoria Informática

Dentro del proceso de auditoría es importante asegurar que se cumplan por lo menos los principios básicos de un proceso formal. Los elementos indispensables para cumplir este requisito son: la planeación, el control y el seguimiento del desempeño, que deberán garantizar lo siguiente:(Apuntes de Auditoría Informática, 2009).

- Que los recursos de informática sean orientados al logro de los objetivos y las estrategias de las organizaciones.
- La elaboración, difusión y cumplimiento de las políticas, controles y procedimientos inherentes a la AI.
- Que se den los resultados esperados por la institución mediante la coordinación y apoyo reciproco con: auditoría, asesores externos, informática, y la alta dirección.

i. Importancia del Control y la Auditoria Informática

Caridad Simón en sus apuntes de Auditoría Informática hace referencia a algunos factores críticos que atentan al bien más preciado de una organización en la actualidad, la información. Estos factores son: coste de la pérdida de datos, toma de decisiones incorrecta, abuso informático, y privacidad de los datos (Caridad Simón, 2006).

j. Guía de Procedimientos para la Auditoria Informática

Fase I: Conocimientos del Sistema

- Aspectos Legales y Políticas Internas: Sobre estos elementos está construido el sistema de control y por lo tanto constituyen el marco de referencia para su evaluación.

- Características del Sistema Operativo: Organigrama del área que participa en el sistema, Informes de auditoría realizadas anteriormente
- Características de la aplicación de computadora: Manual técnico de la aplicación del sistema, Equipos utilizados en la aplicación de computadora

Fase II: Análisis de las transacciones

- Definición de las transacciones.
- Establecer el flujo de los documentos
- Identificar y codificar los recursos que participan en los sistemas
- Relación entre transacciones y recursos

Fase III: Análisis de riesgos y amenazas

- Identificación de riesgos
- Identificación de las amenazas
- Relación entre recursos/amenazas/riesgos

Fase IV: Análisis de controles

- Codificación de controles
- Relación entre recursos/amenazas/riesgos
- Análisis de cobertura de los controles requeridos

Fase V: Evaluación de Controles

- Objetivos de la evaluación
- Plan de pruebas de los controles
- Pruebas de controles
- Análisis de resultados de las pruebas

Fase VI: Informe de Auditoria

- Informe detallado de recomendaciones
- Evaluación de las respuestas
- Informe resumen para la alta gerencia

Fase VII: Seguimiento de Recomendaciones

- Informes del seguimiento
- Evaluación de los controles implantados

SALUD OCUPACIONAL

De acuerdo con la OMS, la Salud Ocupacional es una actividad multidisciplinaria dirigida a promover y proteger la salud de los trabajadores mediante la prevención y el control de enfermedades y accidentes y la eliminación de los factores y condiciones que ponen en peligro la salud y la seguridad en el trabajo. Además, procura generar y promover el trabajo seguro y sano, así como buenos ambientes y organizaciones de trabajo realzando el bienestar físico, mental y social de los trabajadores y respaldar el perfeccionamiento y el mantenimiento de su capacidad de trabajo. A la vez que busca habilitar a los trabajadores para que lleven vidas social y económicamente productivas y contribuyan efectivamente al desarrollo sostenible, la salud ocupacional permite su enriquecimiento humano y profesional en el trabajo.

a. Funciones:

- **Servicios de Salud para los trabajadores del Ministerio de Salud de la Nación en los términos de las leyes 19.587 y 24.557**
  - Identificación y evaluación de los riesgos que puedan afectar a la salud en el lugar de trabajo
  - Vigilancia de los factores del medio ambiente de trabajo y de las prácticas de trabajo que puedan afectar a la salud de los trabajadores.
  - Asesoramiento en materia de salud, de seguridad y de higiene en el trabajo y de ergonomía.
  - Vigilancia de la salud de los trabajadores en relación con el trabajo.
  - Colaboración en la difusión de informaciones, en la formación y educación en materia de salud e higiene en el trabajo y de ergonomía.
  - Participación en el análisis de los accidentes del trabajo y de las enfermedades profesionales.
  - Asegurar que se reciban las prestaciones correspondientes a la ley de riesgos de trabajo, en cantidad y calidad realizando el seguimiento personal el cada caso.
  - Organismo responsable ante la Aseguradora de Riesgos de Trabajo.

- **Reconocimientos Médicos de Patología Inculpable (Decreto 3413/79 y Convenio de Trabajo del Sector Publico)**

  Afecciones o lesiones de corto tratamiento, largo tratamiento, maternidad, atención grupo familiar, por solicitud del organismo empleador. Deberá aportar: nota presentación del organismo, documento de identidad, certificación médica y estudios obrantes.

Destinado a: Ministerio de Salud de la Nación - Organismos descentralizados de la Administración Pública Nacional - Casas de Provincia - Personal de provincias en tránsito - Universidades Nacionales.

- **Certificación de Aptitud Psicofísica**

  Destinado a: Ministerio de Salud de la Nación - Organismos descentralizados de la Administración Pública Nacional, en el marco del Decreto 3413/79 y Ley de riesgos de trabajo.

- **Juntas Medicas**

  Instancia superior determinante en casos de disenso entre la licencia aconsejada por el médico del/la agente y el Servicio Médico del organismo

  Consideración de los casos de reducción horaria y/o cambio de tareas o destino. En todas las Juntas Médicas el/la agente podrá presentarse acompañada con su médico/a tratante.

- **Medicina Legal**

  Peritación médico-legal a pedido de la Cámara Federal de la Seguridad Social en el ámbito de la Ley 24.241

  Perito de parte en Ministerio de Salud de la Nación.

HISTORIA CLÍNICA

Es el documento médico legal, que registra los datos, de identificación y de los procesos relacionados con la atención del paciente, en forma ordenada, integrada, secuencial e inmediata de la atención que el médico u otros profesionales brindan al paciente. (Ministerio de Salud, 2005)

CLINICA

La clínica (del griego kliní, 'cama, lecho') sigue los pasos de la semiología, ciencia y arte de la medicina, en el proceso indagatorio orientado al diagnóstico de una situación patológica (enfermedad, síndrome, trastorno, etc.), basado en la integración e interpretación de los síntomas y otros datos aportados por la anamnesis durante la entrevista clínica con el paciente, los signos de la exploración física y la ayuda de exploraciones complementarias de laboratorio y de pruebas de imagen. Con el diagnóstico de una enfermedad se pauta un tratamiento. Tradicionalmente la clínica es el diagnóstico realizado al pie de la cama del enfermo a través del relato de su sintomatología y de los signos obtenidos en la exploración física. El clínico es aquel médico que diagnostica y trata a sus pacientes. También se llama clínica al hospital o al centro de salud donde el médico diagnostica y trata a personas con problemas de salud. La historia clínica es donde se recogen todos los datos clínicos.

SEGURIDAD

El término seguridad (del latín securitas) cotidianamente se puede referir a la ausencia de riesgo o a la confianza en algo o en alguien. Sin embargo, el término puede tomar diversos sentidos según el área o campo a la que haga referencia. En términos generales, seguridad se define como "estado de bienestar que percibe y disfruta el ser humano".

Una definición dentro de las Ciencias de la Seguridad es "Ciencia, interdisciplinaria, encargada de evaluar, estudiar y gestionar los riesgos a que se encuentra sometido una persona un bien o el ambiente". Se debe diferenciar la seguridad sobre las personas (seguridad física), la seguridad sobre el ambiente (seguridad ambiental), la seguridad en ambiente laboral (seguridad e higiene, en ingles conocido como safety), etc.

SEGURIDAD INFORMATICA

La seguridad informática o seguridad de tecnologías de la información es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software (bases de datos, metadatos, archivos), hardware y todo lo que la organización valore (activo) y signifique un riesgo si esta información confidencial llega a manos de otras personas, convirtiéndose, por ejemplo, en información privilegiada. El concepto de seguridad de la información no debe ser confundido con el de «seguridad informática», ya que este último solo se encarga de la seguridad en el medio informático, pero la información puede encontrarse en diferentes medios o formas, y no solo en medios informáticos.

NT-MINSA N° 22 -2005

Aprobada en el 2005 y actualizada el 09 Junio 2009 (Peru, 2005)La Historia Clínica y en general todos los registros médicos, constituyen documentos de alto valor médico, gerencial, legal y académico, su correcta administración y gestión contribuyen de manera directa a mejorar la calidad de atención de los pacientes. Por ello, es necesario administrar correctamente todos los mecanismos y procedimientos que siguen las Historias Clínicas desde su apertura, de manera tal, que se pueda responder con criterios de calidad, oportunidad e integridad las demandas cada vez más exigentes de los pacientes/usuarios. La presente Norma Técnica busca dar respuesta a estos nuevos desafíos, contribuyendo a resolver las principales situaciones que, para todos los pacientes usuarios, personal y establecimientos de salud, plantea la Historia Clínica.

NTP ISO/IEC 27001:2014

Esta Norma Internacional ha sido elaborada con la finalidad de proporcionar los requisitos para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de la seguridad de la información. La adopción del sistema de gestión de la seguridad de la información es una decisión estratégica de la organización. El establecimiento e implementación de un sistema de gestión de seguridad de la información depende de las necesidades y objetivos, requisitos de seguridad, procesos organizacionales utilizados y del tamaño y estructura de la organización. Se espera que todos estos factores cambien con el paso del tiempo.

Estructura: (Collazos Balaguer, 2013)

- Introducción
- Objetivo
- Referencias Normativas
- Contexto de la organización
- Liderazgo
- Planificación
- Soporte
- Operación
- Evaluación del desempeño
- Mejora

La NTP ISO/IEC 27001:2014 trabaja en función a 8 principios de gestión: (Collazos Balaguer, 2013)

- Orientación al cliente
- Liderazgo
- Participación del personal
- Enfoque de procesos
- Enfoque de sistemas de gestión
- Mejora Continua
- Enfoque de mejora continua
- Relación mutuamente beneficiosa con el proveedor

Entrada: ANEXO A. Objetivo de Control y controles dicho anexo tiene 14 categorías de control (del 5 al 18) (ISO, 2013)

5. Política de seguridad de la información
6. Organización de la seguridad de la información
7. Seguridad de los recursos Humanos
8. Gestión de activos
9. Control de acceso
10. Criptografía
11. Seguridad física y medioambiental
12. Seguridad en las operaciones
13. Seguridad de las comunicaciones
14. Adquisición, desarrollo y mantenimiento de los sistemas.
15. Relación con los proveedores
16. Gestión de los incidentes de seguridad de la información
17. Gestión de los aspectos de la seguridad de la información para la continuidad del negocio
18. Cumplimiento

Y cuenta con 35 Objetivos de control (ISO, 2013):

1. Dirigir y dar soporte a la gestión de la seguridad de la información en concordancia con los requisitos del negocio, las leyes y las regulaciones.
2. Gestionar la seguridad de la información dentro de la organización
3. Garantizar la seguridad del trabajo a distancia y del uso de los equipos móviles
4. Asegurar que los empleados, contratistas y usuarios externos entiendan sus responsabilidades y que estos sean adecuados a los roles para los cuales han sido considerados y reducir asi el riesgo de estafa, fraude o mal uso de las instalaciones.
5. Garantizar que los trabajadores y los contratistas sean conscientes y cumplan con las responsabilidades de la seguridad de la información.
6. Proteger los intereses de la organización como parte del proceso de cambio o término del empleo.

7. Identificar los activos de la organización y definir las responsabilidades adecuadas de protección.
8. Garantizar que la información reciba un nivel adecuado de protección de acuerdo a su importancia dentro de la organización.
9. Prevenir la divulgación, modificación, retiro o destrucción no autorizada de la información almacenada en los medios de comunicación.
10. Controlar los accesos a la información
11. Garantizar el acceso al usuario autorizado para evitar el acceso no autorizado a los sistemas y servicios
12. Hacer a los usuarios responsables de salvaguardar la autenticación de su información.
13. Evitar el acceso no autorizado a los sistemas y aplicaciones
14. Asegurar el uso adecuado y efectivo de la criptografía para proteger la confidencialidad autenticidad y/o integridad de la información
15. Evitar acceso físico no autorizado daño e interferencia a la información e instalaciones de procesamiento de la información de la organización
16. Evitar la pérdida, daño, robo o actos en los que se comprometan activos y la interrupción de las operaciones de la organización.
17. Asegurar la operación correcta y segura de los recursos de procesamiento de información
18. Garantizar que la información y las instalaciones de procesamiento de la información estén protegidos contra el malware.
19. Proteger la información contra la perdida
20. Registrar eventos y generar evidencias
21. Garantizar la integridad de los sistemas operacionales
22. Evitar la explotación de las vulnerabilidades técnicas
23. Minimizar el impacto de las actividades de las auditorias en los sistemas operacionales
24. Garantizar la protección de la información en las redes y de sus instalaciones de procesamiento de la información
25. Mantener la seguridad de la información transferida dentro de la organización y con cualquier entidad externa
26. Garantizar que la seguridad de la información forme parte integral de los sistemas de información a lo largo de todo el ciclo de vida. Esto incluye también los requisitos del sistema de la información que proveen servicios mediante las redes públicas.

27. Garantizar que se diseñe e implemente la seguridad de la información dentro del ciclo del programa de desarrollo de los sistemas de la información
28. garantizar la protección de los datos utilizados para la verificación
29. Garantizar la protección de los activos de la información a los que los proveedores tiene acceso
30. Mantener un nivel acordado de seguridad de la información y de la prestación del servicio alineado a los acuerdos del proveedor
31. Garantizar una aproximación consistente y efectiva a la gestión de los incidentes de seguridad de la información, incluyendo la comunicación sobre los eventos y debilidades de la seguridad
32. La continuidad de la seguridad de la información debe estar incrustada en los sistemas de gestión de la continuidad del negocio de la organización
33. Garantizar la disponibilidad de las instalaciones de procesamiento de la información
34. Evitar el incumplimiento de las obligaciones legales, regulatorias o contractuales relacionadas a la seguridad, de la información y al cualquier requisito de seguridad
35. Garantizar que la seguridad de la información sea implementada y operada de acuerdo a las políticas y procedimientos organizacionales

EVIDENCIAS

Cualquier documento, fichero, registro, dato, etc. contenido en un soporte informático; susceptible de tratamiento digital, Ejemplos:

- Documentos de Ofimática
- Comunicaciones Digitales
- Imágenes digitales
- Bases de Datos
- Ficheros de Registros de Actividad

COEFICIENTE DE VALIDEZ V (V de AIKEN, 1985)

Es un coeficiente que se computa como la razón de un dato obtenido sobre la suma máxima de la diferencia de los valores posibles. Puede ser calculado sobre las valoraciones de un conjunto de jueces con relación a un ítem o como las valoraciones de un juez respecto a un grupo de ítems. Asimismo las valoraciones asignadas pueden ser dicotómicas (recibir valores de 0 ó 1) o politómicas (recibir valores de 0 a 5).

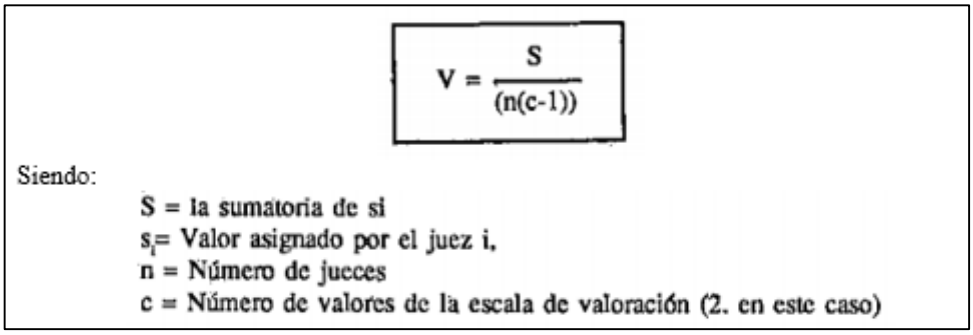

Figura 2: Fórmula de Validez de AIKEN

Este coeficiente puede obtener valores entre 0 y 1. a medida que sea más elevado el valor computado, el ítem tendrá una mayor validez de contenido. El resultado puede evaluarse estadísticamente haciendo uso de la tabla de probabilidades asociadas de cola derecha. Tabuladas por el autor. Es precisamente esta posibilidad de evaluar su significación estadística lo que hace a este coeficiente uno de los más apropiados para estudiar este tipo de validez.

ARTEFACTOS DE LA AUDITORIA

ARTEFACTOS	**¿Por qué?**
CUESTIONARIO	• Facilitan la recopilación de información y no se necesitan muchas explicaciones ni una gran preparación para aplicarlos. • Evitan la dispersión de la información, al concentrarse en preguntas de elección forzosa. • En el ambiente de sistemas es fácil capturar, concentrar y obtener información útil a partir de las respuestas, mediante el uso de la computadora. Incluso se puede proyectar los datos y hacer gráficas. • Hacen impersonal la aportación de respuestas; por lo tanto, en una auditoría ayudan a obtener información útil y confiable si se plantean bien las preguntas.

Tabla 1: Artefacto de la Auditoria

CHECKLIST DE VERIFICACIÓN	• Las Listas de Control, Check Lists u Hojas de Verificación, son formatos creados para realizar actividades repetitivas, controlar el cumplimiento de una lista de requisitos o recolectar datos ordenadamente y de forma sistemática. • Se usan para hacer comprobaciones sistemáticas de actividades o productos asegurándose de que el trabajador o inspector no se olvida de nada importante. • Es importante que las listas de control queden claramente establecidas e incluyan todos los aspectos que puedan aportar datos de interés para la organización. Es por ello preciso que quede correctamente recogido en la lista de control

CAPÍTULO III: MATERIALES Y MÉTODOS

3. MATERIAL Y MÉTODOS

3.1. Material

3.1.1. Población

Centros de salud ocupacional de la Ciudad de Trujillo.

3.1.2. Muestra

Se tomará como muestra no aleatoria el sistema de información para la gestión de historias clínicas del centro de salud ocupacional LEZAMA CONSULTORES DE SALUD OCUPACIONAL SCRL.

3.1.3. Unidad de Análisis

Historias Clínicas digitales gestionadas con el Sistema de Información de Salud Ocupacional de propiedad de “Lezama Consultores de Salud Ocupacional S.C.R.L.”

3.2. MÉTODO

3.2.1. NIVEL DE INVESTIGACIÓN

La naturaleza del problema es una investigación descriptiva pues se detallará el diseño de un modelo de auditoria basado en la ISO 27001-2014 adaptado a la NTP MINSA 22-2005 que evalué la seguridad de los sistemas de información de historias clínicas de los Centros de Salud Ocupacional.

3.2.2. VARIABLES DE ESTUDIO Y OPERACIONALIZACIÓN

Variable Independiente (VI):

Seguridad en los sistemas de información para la gestión de historias clínicas de los Centros de Salud Ocupacional de la Provincia de Trujillo.

- $I_A < I_P$
- $A_A < A_P$
- $C_A < C_P$

Variable Dependiente (VD):

Modelo de auditoria basado en la ISO 27001-2014 adaptado a la NTP MINSA 22-2005

Operacionalización de la Variables:

Variable	Dimensión	Indicador	Tipo
VD Seguridad en los sistemas de información para la gestión de historias clínicas de los Centros de Salud Ocupacional de la Provincia de Trujillo	Integridad	% de registros completos	Racional
	Accesibilidad	% tiempo disponible	Racional
	Confidencialidad	Controles de acceso	Ordinal
VI Modelo de auditoria basado en la ISO 27001-2014 adaptado a la NTP MINSA 22-2005	Integridad	Número de checklist	Ordinal
	Usabilidad	% de aprobación de Juicio de Expertos	Racional

3.2.3. PROCEDIMIENTO:

3.2.3.1. IDENTIFICAR LAS PRINCIPALES CARACTERÍSTICAS DE: NT MINSA N°22 E NTP ISO/IEC 27001:2014

3.2.3.1.1. Estudio de la NTP MINSA N 22-2005

Provee la correcta administración y gestión, contribuyen de manera directa a mejorar la calidad de atención de los pacientes, así como también a optimizar la gestión de los establecimientos de salud, proteger los intereses legales del paciente, del personal de salud y del establecimiento, así como proporcionar información con fines de investigación y docencia.

Permite administrar correctamente todos los mecanismos y procedimientos que siguen las Historias Clínicas desde su apertura, de manera tal, que se pueda responder con criterios de calidad, oportunidad e integridad las demandas cada vez más exigentes de los pacientes/usuarios y de los prestadores de servicios de salud.

La presente Norma Técnica busca dar respuesta a estos nuevos desafíos, contribuyendo a resolver las principales situaciones para todos los pacientes, usuarios, personal y establecimientos de salud.

La norma tiene como objetivos:

- Establecer las normas y procedimientos para la administración y gestión de la Historia Clínica a nivel del sector salud.
- Estandarizar el contenido básico de la Historia Clínica para garantizar un apropiado registro de la atención de salud.

El estudio se enfocará en las Historias Clínicas Informatizadas. Los establecimientos de salud podrán optar por el uso de la Historia Clínica Informatizada, debiendo sujetarse a la presente norma. Esta indica que el uso de un soporte informático debe garantizar la autenticidad, integridad y conservación en el tiempo de la información.

Todo sistema clínico debe estar acreditado previo a su uso por las Direcciones Regionales de Salud correspondientes. A su vez indica que el sistema de Historia Clínica Informatizada debe ser constantemente auditado para garantizar su calidad.

Esta norma establece los siguientes puntos con los que debe contar el sistema de historias clínicas informatizadas:

- Base de datos relacionados.
- Estructura de datos estandarizado
- Control de acceso restringido – Privilegio de accesos
- Sistema de copias de resguardo
- Registro informatizado de firmas de usuarios.(debe ajustarse a lo establecido en la Ley Nº 27269 Ley de firmas y Certificados Digitales y su Reglamento)
- Simultaneidad de accesibilidad
- Confidencialidad

3.2.3.1.2. Estudio de la NTP ISO/IEC 27001-2014.

ISO 27001 es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan.

El estándar ISO 27001:2013 para los Sistemas Gestión de la Seguridad de la Información permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos.

La aplicación de ISO-27001 significa una diferenciación respecto al resto, que mejora la competitividad y la imagen de una organización.

La Gestión de la Seguridad de la Información se complementa con las buenas prácticas o controles establecidos en la norma ISO 27002.

Esta norma tiene como estructura:

- Objeto y campo de aplicación: La norma comienza aportando unas orientaciones sobre el uso, finalidad y modo de aplicación de este estándar.
- Referencias Normativas: Recomienda la consulta de ciertos documentos indispensables para la aplicación de ISO27001.
- Términos y Definiciones: Describe la terminología aplicable a este estándar.
- Contexto de la Organización: Este es el primer requisito de la norma, el cual recoge indicaciones sobre el conocimiento de la organización y su contexto, la comprensión de las necesidades y expectativas de las partes interesadas y la determinación del alcance del SGSI.
- Liderazgo: Este apartado destaca la necesidad de que todos los empleados de la organización han de contribuir al establecimiento de la norma. Para ello la alta dirección ha de demostrar su liderazgo y compromiso, ha de elaborar una política de seguridad que conozca toda la organización y ha de asignar roles, responsabilidades y autoridades dentro de la misma.
- Planificación: Esta es una sección que pone de manifiesto la importancia de la determinación de riesgos y oportunidades a la hora de planificar un Sistema de Gestión de Seguridad de la Información, así como de establecer objetivos de Seguridad de la Información y el modo de lograrlos.
- Soporte: En esta cláusula la norma señala que para el buen funcionamiento del SGSI la organización debe contar con los recursos, competencias, conciencia, comunicación e información documentada pertinente en cada caso.
- Operación: Para cumplir con los requisitos de Seguridad de la Información, esta parte de la norma indica que se debe planificar, implementar y controlar los procesos de la organización, hacer una valoración de los riesgos de la Seguridad de la Información y un tratamiento de ellos.

- Evaluación del Desempeño: En este punto se establece la necesidad y forma de llevar a cabo el seguimiento, la medición, el análisis, la evaluación, la auditoría interna y la revisión por la dirección del Sistema de Gestión de Seguridad de la Información, para asegurar que funciona según lo planificado.
- Mejora: Por último, en la sección décima vamos a encontrar las obligaciones que tendrá una organización cuando encuentre una no conformidad y la importancia de mejorar continuamente la conveniencia, adecuación y eficacia del SGSI.

Usaremos el Anexo A de la ISO para realizar la intersección con la MINSA N22-2005.

Este Anexo provee una herramienta esencial para la gestión de la seguridad: una lista de los controles (o medidas) de seguridad que pueden ser usados para mejorar la seguridad de la información.

Estos se estructuran en 14 secciones:

- 5 Políticas de seguridad de la Información – controles acerca de cómo deben ser escritas y revisadas las políticas.
- 6 Organización de la seguridad de la información – controles acerca de cómo se asignan las responsabilidades; también incluye los controles para los dispositivos móviles y el teletrabajo
- 7 Seguridad de los Recursos Humanos – controles antes, durante y después de emplear
- 8 Gestión de recursos – controles acerca de lo relacionado con el inventario de recursos y su uso aceptable, también la clasificación de la información y la gestión de los medios de almacenamiento
- 9 Control de Acceso – controles para las políticas de control de acceso, gestión de acceso de los usuarios, control de acceso para el sistema y las aplicaciones, y responsabilidades del usuario
- 10 Criptografía – controles relacionados con la gestión de encriptación y claves
- 11 Seguridad física y ambiental – controles que definen áreas seguras, controles de entrada, protección contra amenazas, seguridad de equipos, descarte seguro, políticas de escritorio y pantalla despejadas, etc.
- 12 Seguridad Operacional – muchos de los controles relacionados con la gestión de la producción en TI: gestión de cambios, gestión de capacidad, malware, respaldo, bitácoras, espejos, instalación, vulnerabilidades, etc.

- 13 Seguridad de las Comunicaciones – controles relacionados con la seguridad de redes, segregación, servicios de redes, transferencia de información, mensajería, etc.
- 14 Adquisición, desarrollo y mantenimiento de Sistemas – controles que definen los requerimientos de seguridad y la seguridad en los procesos de desarrollo y soporte
- 15 Relaciones con los proveedores – controles acerca de qué incluir en los contratos, y cómo hacer el seguimiento a los proveedores
- 16 Gestión de Incidentes en Seguridad de la Información – controles para reportar los eventos y debilidades, definir responsabilidades, procedimientos de respuesta, y recolección de evidencias
- 17 Aspectos de Seguridad de la Información de la gestión de la continuidad del negocio – controles que requieren la planificación de la continuidad del negocio, procedimientos, verificación y revisión, y redundancia de TI
- 18 Cumplimiento – controles que requieren la identificación de las leyes y regulaciones aplicables, protección de la propiedad intelectual, protección de datos personales, y revisiones de la seguridad de la información

3.2.3.2. IDENTIFICAR LA SIMILITUD ENTRE AMBAS NORMATIVAS

3.2.3.2.1. Identificación de los Aspectos relacionados entre ambas normativas

Se realizó un estudio entre ambas normativas y se encontraron aspectos relacionados entre ellas las cuales se pasan a detallar a continuación:

NTP MINSA N° 22-2005 solo centrándonos en lo referido a historias clínicas informatizada establece 12 puntos con los que debe contar. De su totalidad se han tomado 9 puntos que son los siguientes:

1. Control de acceso restringido
2. Privilegios de acceso
3. Sistema de copia de resguardo
4. Registro informatizado de firmas de usuario (según ley 27269)
5. Simultaneidad de accesibilidad
6. Confidencialidad
7. Recuperabilidad
8. Inviolabilidad de los datos que constituyen HC
9. Debe soportar la auditoría

Estos guardan relación con los controles establecidos en la NTP ISO 27001 Anexo A de esta manera se seleccionaron los siguientes controles de la ISO y son los siguientes:

OBJ.CONTROL	CONTROL
A.5.1	A.5.1.1 - Políticas de la seguridad de la información
	A.5.1.2 - Revisión de las políticas de seguridad de la información
A.6.1	A.6.1.1 - Funciones y responsabilidades de la seguridad de la información
A.7.1	A.7.1.2 - Términos y condiciones del empleo
A.7.2	A.7.2.3 - Procesos disciplinarios
A.7.3	A.7.3.1 - Término o cambio de responsabilidades de empleo
A.8.2	A.8.2.1 - Clasificación de la información
	A.8.2.3 - Manejo de los activos
A.9.1	A.9.1.1 - Política de control de acceso
	A.9.1.2 - Acceso a la redes y a los servicios de las redes
A.9.2	A.9.2.1 - Registro y des-registro del usuario
	A.9.2.2-Provisión de acceso al usuario
	A.9.2.3 - Gestión de los derechos de acceso privilegiado
	A.9.2.4 - Gestión de Información de autenticación secreta de usuarios
A.9.3	A.9.3.1 - Uso de información secreta de autenticación
A.9.4	A.9.4.1 - Restricción del acceso a la información
	A.9.4.2 - Procedimiento seguro de logeo
A.10.1	A.10.1.1 - Política del uso de controles criptográficos
	A.10.1.2 - Gestión de las claves
A.12.1	A12.1.3 - Gestión de la capacidad
A.12.2	A.12.2.1 - Controles contra el malware
A.12.3	A.12.3.1 - Backup de la información
A.12.4	A.12.4.1 - Eventos de logeo
	A.12.4.2 - Protección de la información del logeo
A.12.7	A.12.7.1 - Controles de la auditoría sobre los sistemas de información
A.17.1	A.17.1.3 - Verificación, revisión y evaluación de la continuidad de la seguridad de la información
A.18	A.18.4 - Privacidad y protección de la información que permite identificar a las personas
A.18.2	A.18.2.1 - Revisión independiente de la seguridad de la información
	A.18.2.2 - Cumplimiento de las políticas y normas de seguridad de la información
	A.18.2.3 - Revisión del cumplimiento técnico

Tabla 2: NTP ISO 27001 Anexo A

3.2.3.2.2. Documento de relación de la NTP MINSA N22-2005 e NTP ISO 27001-2014

Se tomó como base la NTP ISO 27001 adaptándola con lo expuesto en la NTP MINSA N22-2005 para historias clínicas informatizadas, a lo cual se

identificó la relación entre ambas normativas teniendo como resultado la siguiente tabla de cruce:

N	REQUISITO	O.CONTROL	CONTROL
1	Control de acceso restringido	A.5.1	A.5.1.1 - Políticas de la seguridad de la información
			A.5.1.2 - Revisión de las políticas de seguridad de la información
		A.6.1	A.6.1.1 - Funciones y responsabilidades de la seguridad de la información
		A.9.1	A.9.1.1 - Política de control de acceso
			A.9.1.2 - Acceso a la redes y a los servicios de las redes
		A.9.2	A.9.2.1 - Registro y des-registro del usuario
		A.9.4	A.9.4.1 - Restricción del acceso a la información
			A.9.4.2 - Procedimiento seguro de logeo
		A.10.1	A.10.1.2 - Gestión de las claves
2	Privilegios de acceso	A.9.1	A.9.1.1 - Política de control de acceso
		A.9.2	A.9.2.2-Provisión de acceso al usuario
			A.9.2.3 - Gestión de los derechos de acceso privilegiado
		A.9.4.	A.9.4.2 - Procedimiento seguro de logeo
3	Sistema de copia de resguardo	A.12.3	A.12.3.1 - Backup de la información
		A.17.1	A.17.1.3 - Verificación, revisión y evaluación de la continuidad de la seguridad de la información
4	Registro informatizado de firmas de usuario (según ley 27269)	A.5.1	A.5.1.1 - Políticas de la seguridad de la Información
		A.18	A.18.4 - Privacidad y protección de la información que permite identificar a las personas
5	Simultaneidad de accesibilidad	A.8.2	A.8.2.1 - Clasificación de la información
			A.8.2.3 - Manejo de los activos
		A.9.1	A.9.1.1 - Políticas de control de acceso
		A.9.2	A.9.2.1 - Registro y des-registro del usuario
			A.9.2.2-Provisión de acceso al usuario
			A.9.2.3 - Gestión de los derechos de acceso privilegiado
		A.9.4	A.9.4.1 - Restricción del acceso a la información
		A.12.1	A12.1.3 - Gestión de la capacidad
		A.12.4	A.12.4.1- Eventos de logeo
6	Confidencialidad	A.5.1	A.5.1.1 - Políticas de la seguridad de la Información
		A.7.1	A.7.1.2 - Términos y condiciones del empleo
		A.7.2	A.7.2.3 - Procesos disciplinarios
		A.7.3	A.7.3.1 - Término o cambio de responsabilidades de empleo
		A.9.1	A.9.1.1 - Políticas de control de acceso
			A.9.1.2 - Acceso a redes y a los servicios de las redes
		A.9.2	A.9.2.4 - Gestión de Información de autenticación secreta de usuarios
		A.9.3	A.9.3.1 - Uso de información secreta de autenticación
		A.10.1	A.10.1.1 - Política del uso de controles criptográficos
7	Recuperabilidad	A.12.2	A.12.2.1 - Controles contra el malware
		A.12.3	A.12.3.1 - Backup de la información
8	Inviolabilidad de los datos que constituyen HC	A.5.1	A.5.1.1 - Políticas de la seguridad de la Información
		A.9.1	A.9.1.1 - Políticas de control de acceso
			A.9.1.2 - Acceso a la redes y a los servicios de las redes

		A.9.4	A.9.4.1 - Restricción del acceso a la información
		A.10.1	A.10.1.1 - Política el uso de controles criptográficos
		A.12.4	A.12.4.1 - Eventos de logeo
			A.12.4.2 - Protección de la información del logeo
9	Debe soportar la auditoría	A.12.7	A.12.7.1 - Controles de la auditoría sobre los sistemas de información
		A.18.2	A.18.2.1 - Revisión independiente de la seguridad de la información
			A.18.2.2 - Cumplimiento de las políticas y normas de seguridad de la información
			A.18.2.3 - Revisión del cumplimiento técnico

Tabla 3: NTP MINSA N22-2005

3.2.3.3. GENERAR UN MODELO DE AUDITORIA BASADO EN AMBAS NORMATIVAS

Al comprender ambas normativas e identificar los puntos clave y relación entre sí, se procede a la redacción del modelo de auditoria, el cual contará con los siguientes puntos y estructura:

- Objetivo general
- Objetivos específicos
- Alcance
- Las entradas con las que se debe contar
- Los procesos y subprocesos
- Las salidas que se obtendrá.

La generación del modelo se realizará bajo las siguientes fases lo cual nos llevara a tener como resultado la estructura anteriormente mencionada

a. Elaboración de la matriz de intersección entre ambas Normativas:

La elaboración de la matriz de intersección entre ambas normativas es el resultado de la identificación de los aspectos relacionados entre ambas normas. Esta matriz está definida en el punto 4.2.1.7 de este documento en donde se aprecia el cruce o relación entre la NTP MINSA N22-2005 e NTP ISO 27001-2014.

b. Definir los procesos de la auditoria:

Los procesos son definidos como actividades a realizar en la auditoria, cada uno de ellos serán obtenidos de la matriz de intersección entre ambas normativas.

Se cuenta con 9 requisitos establecidos por la NTP MINSA N22-2005 que son los siguientes:

- Control de acceso restringido
- Privilegios de acceso
- Sistema de copia de resguardo
- Registro informatizado de firmas de usuario (según ley 27269)
- Simultaneidad de accesibilidad
- Confidencialidad
- Recuperabilidad
- Inviolabilidad de los datos que constituyen HC
- Debe soportar la auditoría

En cada uno de ellos se establecerán procesos los cuales están relacionados con cada punto de cruce establecido en la matriz de intersección.

c. Definir las entradas necesarias para los procesos de auditoria:

Para realizar la auditoria y ejecutar los procesos se tiene que tener entradas de información, esta debe ser solicitada o requerida a la organización o empresa auditada.

Los tipos de documentos a solicitar son políticas, procesos y documentación con la que cuente la empresa.

d. Definir la(s) salida(s) posterior a la aplicación del modelo de auditoria:

En este caso como única salida se tendrá el informe de auditoría.

Este plan pasara a ser validado por medio de un proceso de Juicio de Expertos.

3.2.3.4. DISEÑAR LOS ARTEFACTOS DE AUDITORÍA PARA EL MODELO DESEADO

La elaboración de artefactos representa una ayuda para el seguimiento de una auditoria y la obtención de la información, en este se documenta lo que se va a auditar y el método, técnica o procedimiento a seguir. Estos elementos a

auditar son calificados. Además, se les puede asignar un peso a cada elemento para obtener una calificación total.

Técnicas de Evaluación:

- Inspección.
- Confirmación.
- Comparación.
- Revisión documental.
- Acta testimonial.
- Guías de evaluación/auditoria.
- Evaluación.
- Programas de verificación.
- Lista de chequeo o verificación.
- Benchmark.
- Cuestionarios
- Checklist de verificación

Todos los artefactos o tipo de evaluaciones a realizar tienen que estar ligados a los procesos definidos en el modelo de auditoria.

3.2.3.5. VALIDAR EL MODELO DE AUDITORÍA GENERADO, MEDIANTE JUICIO DE EXPERTOS

Cuando todos los expertos hayan concluido con la revisión del modelo de Auditoria propuesto, cada uno de ellos pasara a brindar las observaciones respectivas de acuerdo a sus conocimientos y experiencias referentes al tema. Con todas estas observaciones recibidas se procederá a analizarlas para ver si hay coincidencias entre ellas y al final obtener un solo listado de observaciones, las cuales nos ayudaran a pasar a la última etapa que vendría a ser la redacción del informe de mejoras para el plan de auditoria.

Al término de cada verificación realizada por los expertos, se les brindara un documento en donde firmaran, para que por medio de este quede constancia de quien ha realizado la verificación correspondiente.

3.2.4. TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS

La recopilación de datos involucra la investigación documental, la realización de cuestionarios, entrevista, observación directa, inspección y comparación documentaria.

METODO	INSTRUMENTO	TECNICA	ALMACENAMIENTO	PROCESAMIENTO
Observación Directa	Impresión de Pantalla	Captura de imágenes	JPG, PNG	Visor de Imágenes de Windows
Entrevista Grabada	Smartphone	Grabación	Formatos MP3	Reproductor de Windows Media
Encuesta	Hojas de Preguntas	Cuestionario	Folder	Microsoft Word 2013

Tabla 4: Técnicas e Instrumentos para la Recolección de Datos.

3.2.5. TÉCNICAS DE PROCESAMIENTO DE DATOS

3.2.5.1. Validación por Juicio de Expertos

Mediante la validación de juicio a expertos se comprobara si el modelo de auditoria basado en la ISO 27001-2014 adaptado a la NTP MINSA 22-2005 va a permitir probablemente, mejorar el nivel de seguridad en términos de la integridad, accesibilidad y confidencialidad de los sistemas de información de gestión de historias clínicas de los Centros de Salud Ocupacional de la Provincia de Trujillo.

Se seleccionará 5 ingenieros, los cuales cuentan con experiencia y/o estudios en auditoria informática. Los expertos llenaran un checklist de validación para demostrar si el modelo de auditoria mejora la seguridad en los sistemas de Salud ocupacional y los instrumentos y procesos son los correctos para dicho fin. Los datos requeridos para obtener un buen análisis de la auditoria a realizar

3.2.5.2. Recolección de datos o respuestas:

Esto nos lleva a desarrollar un plan detallado de procesos, que nos lleven a reunir todos los datos con un propósito específico, que será obtener la información referente al uso del Sistema de Historias clínicas ocupacionales.

Ahora los datos obtenidos de los cuestionarios o Checklist, se transferirán a una matriz de datos y se preparan para un análisis

3.2.5.3. Libro de códigos

Cuando se tengan el cuestionario de preguntas o checklist cada uno deberá tener un código único el cual hará referencia a las variables y códigos asignados dentro de la **NTP MINSA N22-2005 e NTP ISO 27001-2014**, de esta manera nos ayudara a interpretar los datos durante el análisis de datos.

3.2.5.4. Guardar los datos para un posterior Análisis

Cuando contemos con los datos obtenidos de los cuestionarios o Checklist pasaremos a definir los programas estadísticos para el correcto procesamiento de datos, como por ejemplo se podrán utilizar hojas de cálculo.

3.2.5.5. Procesamiento de la Información

Ahora pasaremos a agrupar y estructurar todos los datos con el propósito de responder al problema de investigación ya listado anteriormente

3.2.5.6. Publicación de resultados

Los resultados se representarán mediante gráficos estadísticos indicando el nivel de las respuestas, basándonos cuales fueron las más asertivas o cuales fueron omitidas por parte de los usuarios encuestados

3.2.5.7. Análisis de los datos o resultados

Los datos finalmente obtenidos y procesados pasaran a ser descritos en un compendio de datos finales

CAPÍTULO IV: RESULTADOS

4. RESULTADOS

En este capítulo, se muestran los resultados obtenido al diseñar un modelo de auditoria basado en la ISO 27001-2014 adaptado a la NTP MINSA 22-2005 el cual es aplicable a los centros de salud ocupacional con un sistema de información para la gestión de historias clínicas informatizadas evaluando y reforzando los puntos base del modelo (integridad, accesibilidad y confidencialidad).

4.1. Principales características de NT MINSA N°22 y NTP ISO/IEC 27001:2014

Como resultado del análisis de las principales características de las normativas NT MINSA N°22 e NTP ISO/IEC 27001:2014 se obtuvo los siguientes cuadros en los cuales se listan los principales puntos de ambas normativas por separado.

La normativa MINSA permite administrar correctamente todos los mecanismos y procedimientos que siguen las Historias Clínicas, también indica los siguientes puntos clave a considerar para los sistemas de Historias Clínicas Informatizada el cual debe ser constantemente auditado.

De los cuales han sido seleccionados solo 9 puntos, teniendo como criterio de discriminación la futura relación que se tendrá con la NTP ISO 27001-2014.

Estos puntos serán tomados como base para la futura intercepción entre ambas normativas.

- Control de acceso restringido – Privilegio de accesos
- Privilegios de acceso
- Sistema de copia de resguardo
- Registro informatizado de firmas de usuario (según ley 27269)
- Simultaneidad de accesibilidad
- Confidencialidad
- Recuperabilidad
- Inviolabilidad de los datos que constituyen HC
- Debe soportar la auditoría

La NTP ISO/IEC 27001:2014 ha sido tomada para la Gestión de la Seguridad de la Información, permitir la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos. Las características tomas de esta norma se centran en el Anexo A y su estructura de 14 secciones.

4.2. Relación de la NTP MINSA N22-2005 y NTP ISO 27001-2014

Se realizó la relación o intersección entre ambas normativas, se tomó como base los 9 puntos de la normativa MINSA, se procedió a seleccionar y a adaptar cada uno de los puntos (controles) listados en el anexo A de la NTP ISO 27001-2014 en los puntos seleccionados del MINSA.

Finalizado se obtiene un cuadro de intersección entre ambas normativas (Tabla 3) el cual será usado para la elaboración del modelo de auditoria.

4.3. Modelo de Auditoria basado en la ISO 27001-2014 adaptado a la NTP MINSA 22-2005

Habiendo realizado el estudio de la matriz de intersección y de los puntos que la componen, se procedió a unificar estos, obteniendo un listado de procesos y actividades los cuales son de uso en el MODELO DE AUDITORIA. El modelo considera 9 dominios los cuales son los requisitos establecidos por la NTP MINSA N22-2005.

Dicha normativa (NTP MINSA N22-2005) no detalla cada uno de los dominios tomados en este estudio.

4.3.1. PERSONAL RESPONSABLE:

Se deberá designar roles o cargos necesarios para la correcta ejecución de la auditoria, se proponen los siguientes:

a. Director del Programa:

Es el responsable global de las auditorías en el centro de salud ocupacional. Supervisa las auditorias y aprueba el Plan de Auditorías. El Director del Programa es también responsable de asegurar el soporte necesario para mantener la actividad auditora.

b. Director de Auditorías/Director de Gestión de Calidad

El Director de Auditorías es la persona designada por el propio Director del Programa para organizar las Auditorías Clínicas. En nuestro Servicio este puesto coincide con el de Director de Gestión de Calidad. Es responsable de:

- Organizar el Plan de Auditorías.
- Nombrar los Auditores para llevar efectivamente a cabo cada auditoría.
- Nombrar un Supervisor de Auditoría para cada auditoría que se realice. Normalmente alguien con más experiencia en el tema que se va a auditar.

- Definir las áreas o los temas que van a ser auditados, el alcance y el plan concreto de cada auditoría.

c. Auditor

El Auditor es un miembro del equipo médico. Suele ser un miembro del equipo con menor tiempo de experiencia, dado su carácter también docente. Su labor es hacer la auditoría. Puede elegir colaboradores para determinadas tareas específicas. Cuando sea así, se encarga de dirigir y gestionarlos. Es el encargado de preparar la auditoría y advierte a las áreas donde se va a hacer una auditoria de la fecha, el ámbito y los miembros del equipo auditor. Esto se hará, al menos con una semana de antelación. Posteriormente ejecuta la auditoria de acuerdo con el plan previsto, hace el informe correspondiente según el procedimiento que ha establecido y presenta los resultados al resto del equipo del Programa de Trasplante.

d. Equipo de Auditoria:

Incluye al Auditor, al Supervisor de Auditoría y a cualquier ayudante que se considere oportuno para la realización de la auditoría.

e. Auditados:

Un auditado es un miembro del equipo de trasplante al que se le hace la auditoría, bien entendido que no se trata de auditoría personal sino de auditoría del área de responsabilidad, que normalmente es compartida (por ejemplo, toda la enfermería cuando se auditan sus registros, o los médicos de consultas externas cuando se auditan los ingresos). El auditado debe:

- Facilitar los medios adecuados para que los auditores dispongan de todo lo necesario.
- Facilitar el acceso a registros e información.
- Asegurar que toda la documentación está disponible antes del inicio de la auditoría.
- Cooperar para conseguir que la auditoria se pueda realizar según el plan previsto.
- Avisar al resto de profesionales del área de qué va a producirse una auditoría.

4.3.2. DOCUMENTOS Y EQUIPOS:

- Lista de Entradas (Anexo N°02)
- Puntos a Evaluar (Anexo N°03)
- Diagrama de Flujo del Proceso
- Solicitudes para revisión de registros e historias clínicas

4.3.3. DOMINIOS DEL MODELO DE AUDITORIA

1. Control de acceso restringido
    - Analizar y evaluar las políticas de la seguridad de la información
    - Evaluar las funciones y responsabilidades de la seguridad de la información
    - Analizar las políticas de control de acceso
    - Comprobar los accesos a la redes y a los servicios de las redes
    - Verificar el registro y des-registro del usuario
    - Comprobar las restricciones de acceso a la información
    - Validar el procedimiento de logeo
    - Analizar y evaluar la gestión de las claves
2. Privilegios de acceso
    - Analizar las políticas de control de acceso
    - Comprobar los accesos de usuarios
    - Analizar y evaluar la gestión de los derechos de acceso privilegiado
    - Comprobar el procedimiento de logeo
3. Sistema de copia de resguardo
    - Comprobar el procedimiento y resguardo de la información
    - Verificar y evaluar la continuidad de la seguridad de la información
4. Registro informatizado de firmas de usuario (según ley 27269)
    - Verificar las políticas de la seguridad de la información
    - Comprobar la privacidad y protección de la información que permite identificar a las personas
5. Simultaneidad de accesibilidad
    - Evaluar la clasificación de la información
    - Verificar las políticas de control de acceso simultaneo
    - Analizar el registro y des-registro del usuario
    - Validar y evaluar los accesos simultáneos de usuarios
    - Analizar y evaluar la gestión de los derechos de acceso privilegiado
    - Verificar las restricciones de acceso simultaneo a la información
    - Analizar y evaluar la gestión de la capacidad

- Verificar los eventos de logeo

6. Confidencialidad
   - Verificar las políticas de la seguridad de la información
   - Analizar y evaluar los términos y condiciones del empleo
   - Analizar y evaluar los términos o cambios de responsabilidades de empleo
   - Verificar las políticas de control de acceso
   - Verificar los accesos a la redes y a los servicios de las redes
   - Analizar y evaluar la gestión de Información de autenticación secreta de usuarios
   - Validar el uso de información secreta de autenticación
   - Analizar y evaluar las política del uso de controles criptográficos
7. Recuperabilidad
   - Verificar y evaluar la continuidad de la seguridad de la información
   - Verificar el procedimiento y resguardo de la información
8. Inviolabilidad de los datos que constituyen HC
   - Analizar y evaluar las políticas de la seguridad de la información
   - Verificar las políticas de control de acceso
   - Verificar los accesos a la redes y a los servicios de las redes
   - Validar la restricción del acceso a la información
   - Analizar y evaluar las política del uso de controles criptográficos
   - Verificar los eventos de logeo
   - Verificar la protección de la información del logeo
9. Debe soportar la auditoría
   - Analizar y evaluar los controles de la auditoría sobre los sistemas de información
   - Revisión independiente de la seguridad de la información
   - Verificar el cumplimiento de las políticas y normas de seguridad de la información
   - Revisión del cumplimiento técnico

Tipos de Auditoria a realizar:

Se realizarán dos tipos de auditorías: semestrales y anules.

Las auditorías anuales son las que analizan en profundidad problemas muy generales de la práctica clínica, mientras que las auditorías semestrales (auditorías rápidas) se realizarán de un modo muy sencillo para evaluar problemas asistenciales u organizativos cotidianos.

Así, por ejemplo, las auditorías anuales abarcarán temas como normativas, incidencia más la evaluación del cumplimiento de los puntos a evaluar, mientras que las semestrales se harán sobre temas como cumplimentación de los puntos a evaluar, consentimiento informado en la historia clínica de los pacientes y validación del levantamiento de observaciones realizadas en auditorias pasadas. Estas últimas se harán de manera más ágil, sin necesidad de hacer búsquedas y análisis exhaustivos, simplemente revisando unos pocos documentos pertinentes (historias clínicas, informes, documentos y gráficas).

Plan de auditoria

Se organiza generalmente un programa anual de 2 auditorías semestrales (dos al año) y, 1 auditoría anual, en la que se evaluara a fondo todos los puntos expuestos anteriormente, estas auditorías lo autoriza y aprueba el Director de Programa.

Para las auditorías semestrales, el plan debe indicar al ámbito de cada auditoría, la fecha de finalización de la misma y el equipo auditor. Siempre que sea posible, el equipo auditor debería ser definido al menos 6 semanas antes de la fecha prevista de finalización de auditoría.

Cualquier desviación del Plan de Auditorías anual debe ser documentada en el propio informe de la auditoría con la explicación correspondiente de la desviación producida. El Plan debe ser difundido a todos los componentes de los servicios evaluados, administración y alta gerencia, para que proceda a facilitar el acceso a registros que pudieran necesitarse.

La marcha del Plan de Auditorías debe ser comunicada y analizada en la reunión mensual de la Oficina de Gestión de Calidad. Cualquier cambio debe ser aprobado por el Director del Programa y comunicado por el Director de Gestión de Calidad a todo el personal implicado

Preparación de una auditoría semestral. La reunión previa

El equipo de auditoría debe organizar, al menos, una reunión previa dirigida por el Director de Gestión de Calidad. En esta reunión el equipo de auditoria define:

- El esquema de auditoria
- Los estándares de la auditoria
- Las responsabilidades y tareas del equipo
- La duración estimada de la auditoría
- Una lista de comprobación (checklist) para la evaluación de documentos, información y procesos.
- Auditorías previas para evaluar problemas similares y recomendaciones hechas

• Cualquier documento específico que se considere necesario. Así se evitan pérdidas de tiempo durante el proceso auditor.
• Considera en la evaluación el Anexo 2

a. Notificación:

Cualquiera de las áreas o temas específicos que vayan a auditarse deben quedar claramente definidas por el auditor, de manera que los responsables de cada área lo sepan con antelación y se pueda pautar la fecha, tiempo a emplear y número de personas que van a participar, y así puedan mantener una actividad normal durante el tiempo que dura la auditoría. También debe ser advertida la administración y alta gerencia si es necesario el uso de registros o historias clínicas

Realizar la auditoría Anual

El equipo auditor debe actuar con diplomacia. Debe esforzarse en desarrollar una auditoría limpia y una evaluación compensada del área o tema, de manera que las buenas prácticas y los buenos modos de trabajar también sean valorados y registrados en la auditoría. Cualquier discrepancia observada debe ponerse en conocimiento del auditado con el propósito de que pueda ofrecer explicaciones. Todas las observaciones relevantes deben registrarse claras y concisas, haciendo referencia a los estándares cuando ello sea apropiado. Siempre que los hallazgos de una auditoría indiquen un potencial problema en un área concreta, debería hacerse una segunda auditoría de seguimiento con una muestra mayor

Comunicar Hallazgos

Deben comunicarse tanto las observaciones negativas como las positivas (buenas prácticas).

El Auditor hará el informe de la auditoría anual utilizando el formato estandarizado y acordado en consenso.

Como fase final de la auditoría se distribuirá un borrador del informe entre todos los auditados (si procede) con las acciones que haya que realizar en la semana siguiente a la finalización de la auditoría. Con ello se decide conjuntamente con los el personal implicado cómo será el plan de mejora que debe hacerse tras cada auditoría, y se incluirá en el propio informe final.

De este plan de mejora se hará un seguimiento estrecho durante los 10 días siguientes a la emisión del borrador del informe y el personal implicado en las acciones de mejora debe hacer un breve resumen de lo que ha ocurrido, para que

se incluya en el informe final. El informe de la auditoría debe ser finalmente autorizado por el Supervisor Auditor y por el Director de Gestión de Calidad. El informe es público y se distribuirá entre todos los miembros del equipo de trasplante.

Los resultados de la auditoría serán presentados por el Auditor en la fecha establecida y en el foro adecuado que será decidido por el Director del Programa. Esto puede hacerse aprovechando las reuniones habituales del equipo de trasplante, tanto de enfermería como de facultativos.

Archivo de los informes y de las presentaciones

La copia impresa y firmada del informe se custodiará en el archivo de la administración de la empresa, así como una copia electrónica de la presentación pública del informe.

Seguimiento

Todas las acciones de mejora propuestas deberían completarse cuanto antes. Incluso no debería ser necesario esperar a la comunicación de la auditoría si se estima que debe tomarse una iniciativa urgente. Una vez que el responsable de la mejora la ha concluido debe hacer un pequeño resumen de qué se ha hecho y de cuáles han sido las consecuencias iniciales. El Director de Gestión de Calidad comunicará la finalización de la mejora y la archivará con cualquier otro documento relevante junto al informe de la auditoría. El estado de todas las acciones emprendidas debe ser seguido por el Director de Gestión de Calidad y las que permanecen activas deben ser analizadas mensualmente en la reunión de la Oficina de Gestión de Calidad

Revisión y mejoras:

Los resultados de las auditorías deberían ser revisados regularmente en la reunión de la Oficina de Gestión de Calidad. Esta Oficina hará un informe anual al comienzo de cada ejercicio de todas las auditorías realizadas en los doce meses previos del programa evaluando el progreso y proponiendo mejoras del programa. El informe anual será público y debe ser entregado al Director del Programa y al resto de participantes en el mismo

Áreas y temas auditables

Hay unos temas que se consideran de revisión esencial y que deben auditarse como mínimo una vez al año, por ejemplo:

- Cumplimiento de normativas existentes dadas por el ente regulador

- Historias clínicas por empresa
- Informes médicos generados
- Documentación de interna de la organización (RIT, MOF,etc).
- Cumplimiento con los formatos de evaluaciones medicas
- Revisión de políticas de acceso a la información.
- Evaluar responsabilidades de seguridad asignadas.
- Evaluar procesos de generación de historias clínicas.
- Evaluar la asignación de los accesos privilegiados.
- Revisión y validación de resguardo de información.
- Evaluar las políticas de privacidad y confidencialidad.
- Evaluar las políticas de recuperabilidad

Auditorías Rápidas

Las auditorías rápidas las realizará la persona designada, en el programa anual de auditorías publicada por el Director de Auditorías.

Consistirán en el análisis rápido de un tema de organización, procesos clínicos o de seguridad. Los temas se expondrán en el programa anual y serán del tipo:

- Cumplimentación correcta de las normativas impuesta por el ente supervisor
- Informes de alta
- Consentimiento informado en las Historias Clínicas
- Orden de las Historias Clínicas
- Cumplimentación de las vías clínicas
- Uso diario de antifúngicos
- Uso diario de factores de crecimiento
- Estancias inadecuadas

Las conclusiones que se extraigan de estas auditorías deben plasmarse, siempre que sea necesario, en un informe simplificado de auditoría, en el que se adjuntarán las propuestas para la solución de los problemas.

El responsable de cada auditoría rápida será también el responsable de la implementación de las medidas correctoras y de la evaluación de su funcionamiento (objeto de una nueva auditoría rápida pasado un tiempo).

4.4. Artefactos de auditoria para la aplicación del modelo basado en la ISO 27001 adaptado a la NTP MINSA N°22

Habiendo analizado las principales características de ambas normativas y el modelo de auditoria generado, se procedió a la creación de artefactos de auditoría para la

recolección y validación de la información. Todos los artefactos creados tienen que estar ligados a los procesos definidos en el modelo de auditoria.

Se ha generado un total de 19 artefactos los cuales se encuentran relacionados con el modelo de auditoria creado. Estos se encuentran expuestos como anexos de la presente tesis.

Artefactos de auditoria: Anexo N° 04

4.5. Validación de Juicio a Expertos

Para la validación del modelo de auditoria creado se realizara a través de juicio de expertos. Un total de 5 expertos validaran el modelo de auditoria, mediante de un checklist de validación donde brindaran porcentaje de aprobación, a 9 secciones las cuales se encuentran presentes en el modelo de auditoria.

Sumado el porcentaje de validación de cada sección se tendrá un porcentaje total, el cual deberá superar el 90% para considerar valido el modelo creado.

CheckList de Validación: Anexo Nº 03

CAPÍTULO V:
DISCUSIÓN DE RESULTADOS

5. DISCUSIÓN DE RESULTADOS

En este capítulo se evaluará si el modelo de auditoria basado en la ISO 27001-2014 adaptado a la NTP MINSA 22-2005 permitirá, mejorar la integridad, accesibilidad y confidencialidad de los sistemas de información para la gestión de historias clínicas de los Centros de Salud Ocupacional.

Para ello se sometió a discusión de juicio a experto, un total de 6 expertos evaluaron el modelo creado, que a través de un checklist de aprobación (Anexo Nº05) brindaran su conformidad del modelo evaluado.

5.1. Análisis del Modelo de Auditoria basado en la ISO 27001-2014 adaptado a la NTP MINSA 22-2005

Del estudio de las normativas existentes en la elaboración del modelo de auditoria, se identificó dicho modelo basado en la ISO 27001-2014 adaptado a la NTP MINSA 22-2005 brinda un gran aporte en la evaluación de la integridad, accesibilidad y confidencialidad presente en los sistemas de información de historias clínicas ocupacionales, a su vez dicho modelo permite cumplir lo indicado por el ente regulador en la NT MINSA N° 22-2005.

Para validar que realmente este modelo mejorará la seguridad en los sistemas de información de historias clínicas se sometió a evaluación de juicio a expertos.

Este modelo considera evaluar 9 puntos clave en los sistemas de información, los cuales se verán reforzados tras el cumplimiento de este.

5.2. Análisis de los resultados obtenidos de la evaluación de Juicio a Expertos

El modelo de auditoria creado se sometió a evaluación de juicio de expertos, 6 expertos evaluaron el modelo creado a través de un checklist, el cual toma 8 puntos a considerar:

PUNTOS A EVALUAR
Control de acceso
Privilegio de acceso
Copia de resguardo
Simultaneidad de accesibilidad
Confidencialidad
Recuperabilidad
Inviolabilidad de los datos que constituyen HC
Soporte de auditoría.

Tabla 5: Puntos a evaluar en el Juicio de Expertos.

Cada una de las personas que evaluaron el modelo tienen experiencias en relación al tema tratado, su evaluación radico en analizar la tesis desarrollada, el modelo planteado y cada una de las normativas estudiadas (ISO 27001-2014 y NTP MINSA 22-2005).

La calificación al modelo de auditoria se realizó bajo un check list de validación donde se usó un escala de valor que van desde el 1 al 5 (escala de validación).

Numero	Sigla	Calificación
1	**TD**	Totalmente Desacuerdo
2	**D**	Desacuerdo
3	**N**	Neutro
4	**A**	Acuerdo
5	**TD**	Totalmente de Acuerdo

Tabla 6: Escala de validación - Juicio de Expertos.

Por cada punto de evaluación se le asignó un valor, estos generon un promedio final, dicha puntuación superó el 90% considerándose aprobatoria. Los comentarios y sugerencias realizadas fueron aplicados y solventados. (Anexo 05)

CAPÍTULO VI: CONCLUSIONES

6. CONCLUSIONES

6.1. Se concluye que el modelo de auditoría creado es de mucho aporte en relación a la seguridad de la información, si bien existen normativas que por separado realizan la evaluación de ello, este modelo se plantea como una iniciativa dirigida a los centros de salud ocupacional ya que permitirá cumplir con la normativa impuesta por el ente regulador MINSA y a su vez salvaguardar la integridad, disponibilidad y accesibilidad de la información.

6.2. Al realizar la intersección entre ambas normativas se obtuvo una tabla resultado entre los puntos de similitud a evaluar, esta forma nos permitió generar un modelo de auditoria compuestos de las principales características de las normas anteriormente evaluadas, esta al ser aplicada satisfactoriamente probablemente mejorará el nivel de seguridad de los sistemas de información de gestión de historias clínicas.

6.3. Se generó un serie de artefactos que permitirán recolectar información y evidencias que alimentaran y permitirán la aplicación del modelo generado, estos artefactos constan entre cuestionarios y checklist.

6.4. Este modelo de auditoria fue comprobado a través de juicio de expertos los cuales evaluaron en relación a los aspectos impuestos por la NTP MINSA N22, sus conocimientos de seguridad de la información y diversos procesos de auditoría, a lo cual indicaron que el modelo evaluado podría mejorar el nivel de seguridad en los sistemas de gestión de historias clínicas.

6.5. Por lo tanto el modelo presentado podría mejorar la seguridad de la información en los sistemas de gestión de historias clínicas ocupacionales, de tal forma que cumpliendo con lo establecido se podría lograr un impacto positivo en la seguridad de la información y el cumplimiento de la normativa impuesta por el MINSA.

CAPÍTULO VII: RECOMENDACIONES

7. RECOMENDACIONES

7.1. Se recomienda que teniendo como primera versión el modelo de auditoria y haber sido evaluado por juicio de expertos, este deberá someterse a una evaluación aplicada, realizando una auditoria a dos o tres centros de salud ocupacional que cuenten con un sistema de gestión de las historias clínicas informatizadas. De esta manera se comprobará la efectividad del modelo creado y el impacto que se genere en el nivel de seguridad en referencia a la integridad, accesibilidad y disponibilidad.

7.2. Posterior a cada evaluación realizada se recomienda ir actualizando el modelo de auditoria debido a que este se encuentra en una primera versión.

7.3. Se recomienda que los artefactos de auditoria sean adaptados dependiendo de los centros de salud donde sea aplicado.

7.4. Dicho modelo puede ser aplicado a centros de salud ocupacional, que cuenten con un sistema de gestión de historias clínicas en la cual se desea evaluar la seguridad de la información y lo establecido por la Norma Técnica MINSA N°22.

REFERENCIAS BIBLIOGRÁFICAS

Amado Suárez, A., 2008. *Auditoría de comunicación.* Buenos Aires: La Crujía.

ARGENTINA, S., s.f. *http://www.sistemasclinicos.com/home/.* [En línea].

Auditoria Informatica - SUPERTEL, 2012. *Auditoria Informatica a la superintendencia de Telecomunicaciones,* Cuenca: s.n.

Balaguer, I. M. C., 2013. *ISO 27001 Un cambio en la integracion de los sistemas de gestion,* Lima: s.n.

Comisión de Normalización y de Fiscalización de Barreras Comerciales No Arancelarias, 2008. *Tecnología de la Información. Tecnicas de seguridad, Sistemas de gestion de seguridad,* Lima: INDECOPI.

CONTRALORIA GENERAL DE LA REPUBLICA, 2009. *Manual de Auditoria Gubernamental,* Managua: s.n.

Digna, S. C. L., 2014. *Flujograma de la Clinica Lezama* [Entrevista] (Martes Octubre 2014).

Frey, D., 2004. *AutoCAD 2004.* Madrid: ANAYA Multimedia.

ISO, 2013. *ISO/IEC 27001"Seguridad de la Información: Requisitos".* 2da. ed. Suiza: ISO.

Lattuca, A. & Mora, C. y. o., 1991. *Manual de Auditoría.* Buenos Aires: Federación Argentina de Consejos Profesionales de Ciencias Económicas.

Ministerio de Salud, 2005. *Norma Técnica de Saiud para la Gestión de las Historías Clínicas,* Lima: MINSA.

NEXTEL, 2010. *ISO 27001: El estándar de seguridad de la Información,* Lima: s.n.

PERU, L., s.f. *http://www.lolimsa.com.pe/.* [En línea].

Peru, M. d. S., 2005. *Norma técnica de salud para la gestión de la historia clínica,* Lima: s.n.

PERU, M., s.f. *http://www.mediwebperu.com/nosotros.html.* [En línea].

Rodriguez, V. Q., 2012. *Tesis: Auditoria Informatica a la Superintendencia de Telecomunicaciones,* Ecuador: s.n.

Saldaña Carranza, L. D., 2014. *Guia de Procesos de Salud Ocupacional* [Entrevista] (Lunes Setiembre 2014).

systems, I. s. m., 2005. *ISO/IEC 27001:2005 Information technology.* s.l.:Security techniques .

Violeta, V. G., 2014. Reseña Historica de lezama [Entrevista] (Viernes Setiembre 2014).

Maestro, F. T., 2015. SEGURIDAD EN INFORMATICA (AUDITORIA DE SISTEMAS).

Gabriela, B. M., 2012. AUDITORIA INFORMATICA DE LA COOPERATIVA DE AHORRO Y CREDITO "ALIANZA DEL VALLE" LTDA APLICANDO COBIT 4.0

LORENA M. J., 2013. LA AUDITORIA DE LA INFORMACIÓN

María, R. Ch., 2015. Auditoria al control y mantenimiento de la infraestructura tecnológica del departamento tecnológico de la ESPAM MFL.

Amarilis, L. P., 2014. Auditoria de seguridad física y lógica a los recursos de tecnología de información en la carrera informática de la ESPAM MFL

Karolay, C. C., 2012, Auditoria Informatica orientada a los procesos críticos de crédito generados en la cooperativa de Ahorro y Crédito “Fortuna” aplicando el marco de trabajo COBIT

ANEXOS

ANEXO N° 01: CRONOGRAMA DE TRABAJO

N°	Actividad	Días	Fec.Inicio	Fec.Fin
1	**Estudio de las principales características de NT MINSA N°22 y NTP ISO/IEC 27001:2014**	**14**	**15/06/2019**	**28/06/2019**
1.1	Estudio de las metodologías de auditoria basadas en enfoque de evidencias	3	15/06/2019	17/06/2019
1.2	Estudio de la normativa existente para Auditoria Informática	2	18/06/2019	19/06/2019
1.3	Estudio de la NTP MINSA N 22-2005	3	20/06/2019	22/06/2019
1.4	Estudio de la NTP ISO/IEC 27001-2014	3	23/06/2019	25/06/2019
1.5	Evaluar puntos a relacionar de cada normativa	2	26/06/2019	27/06/2019
1.6	Mejoramiento del marco teórico	1	28/06/2019	28/06/2019
Entregable: *Documentación relacionada a ambas normativas y mejoramiento del marco teorico*				
2	**Relación de la NTP MINSA N22-2005 y NTP ISO 27001-2014**	**4**	**29/06/2019**	**2/07/2019**
2.1	Identificación de los Aspectos relacionados entre ambas normativas	1	29/06/2019	29/06/2019
2.2	Identificar puntos base de la NTP MINSA N22-2005	1	30/06/2019	30/06/2019
2.3	Relacionar aspectos similares de la NTP ISO 27001-2014	1	1/07/2019	1/07/2019
2.4	Elaborar matriz relacionar entre ambas normativas	1	2/07/2019	2/07/2019
Entregable: *Matriz de relación entre NTP MINSA N22-2005 y NTP ISO 27001-2014*				
3	**Modelo de Auditoria basado en la ISO 27001-2014 adaptado a la NTP MINSA 22-2005**	**31**	**3/07/2019**	**2/08/2019**
3.1	Estudio de la matriz de relación entre ambas normativas	3	3/07/2019	5/07/2019
3.2	Comprensión de los procesos internos	2	6/07/2019	7/07/2019
3.3	Elaboración del Modelo de Auditoria	14	8/07/2019	21/07/2019
3.4	Definir los procesos de la auditoria	6	8/07/2019	13/07/2019
3.5	Definir las entradas necesarias para los procesos de auditoria	6	14/07/2019	19/07/2019
3.6	Definir la(s) salida(s) posterior a la aplicación del modelo de auditoria	2	20/07/2019	21/07/2019
3.7	Diseñar los artefactos de auditoría para el modelo deseado	12	22/07/2019	2/08/2019
Entregable: *Modelo de Auditoría*				
4	**Diseño de Artefactos de auditoria**	**3**	**3/08/2019**	**5/08/2019**
4.1	Estudio del modelo de auditoría	1	3/08/2019	3/08/2019
4.2	Elaboración de checklist	1	4/08/2019	4/08/2019
4.3	Elaboración de cuestionarios	1	5/08/2019	5/08/2019
Entregable: Artefactos de auditoría				
5	**Validación del Modelo de Auditoria**	**5**	**6/08/2019**	**10/08/2019**
5.1	Aplicación de la V de AIKEN	3	6/08/2019	8/08/2019
5.2	Estudio de resultado de juicio de expertos	1	9/08/2019	9/08/2019
5.3	Elaboración del cuadro de resultados juicio de expertos	1	10/08/2019	10/08/2019
Entregable: Cuadro de resultados Juicio de Expertos				

Tabla 6: Cronograma de Trabajo.

ANEXO N° 02: LISTA DE ENTRADA PARA EL PROCESO DE AUDITORIA

ENTRADAS

Para realizar la auditoría, se requiere de información la cual debe ser proporcionada y solicitada a la organización, la misma que debe gestionar los accesos disponibilidad de lo solicitado:

- Políticas de Protección o Seguridad de la información.
- Controles de acceso a la información.
- Directiva de la clasificación de la información
- Arquitectura de red y detalle de los equipos conectados.
- Listado de redes existentes y especificación del uso dado.
- Controles de acceso a la red.
- Listado de servicios en red y controles aplicados.
- Usuarios de red y políticas de gestión de usuarios.
- Documentación del sistema informático para la Gestión de Historias Clínicas
- Detalle de los módulos y opciones del sistema informático.
- Proceso de gestión de usuarios y credenciales en el sistema.
- Niveles de acceso por tipo de usuario
- Proceso de autentificación del usuario
- Gestión de las credenciales de usuario (nivel de encriptado, almacenamiento y manipulación)
- Flujo de los procesos dados en la creación y gestión de la historia clínica informatizada.
- Organigrama de la empresa.
- Áreas involucradas en el proceso de gestión de las historias clínicas.
- Nivel de Acceso de cada área.
- Lista de personal, puestos asignados, área y proceso en el que se desempeña.
- Programa de copia de resguardo, documentación de la ejecución, bitácora y evidencias de los resguardos realizados.
- Acceso a log y tablas de auditorías del sistema de información.
- Plan de seguridad de la información.
- Plan o cronograma de auditorías informáticas
- Auditorias Históricas.

ANEXO N° 03: CHECK LIST DE VALIDACION DE JUICIO DE EXPERTOS:

Instrucciones:

Evaluar y calificar el modelo de tesis mediante los 9 aspectos de seguridad y sus actividades listados en el checklist. (Calificar mediante tabla de evaluación)

Calificación	Sigla	Calificación
1	**TD**	Totalmente Desacuerdo
2	**D**	Desacuerdo
3	**N**	Neutro
4	**A**	Acuerdo
5	**TD**	Totalmente de Acuerdo

En relación al detalle de cada uno de los 9 dominios del Modelo de auditoría de Sistemas de Información de Historias Clínicas, califique usted respecto a su pertinencia.

PUNTOS A EVALUAR		
* Evaluar según escala: TD(1), D(2), N(3), A(4), TD(5)		Comentarios
Control de acceso		
Politicas de Seguridad de la informaciòn		
Control de acceso a la informaciòn y servicios en redes		
Seguridad de Usuario		
Restriccion de Acceso a la informacion		
Privilegios de acceso		
Control de acceso a la informaciòn		
Control de acceso a usuarios		
Asignaciòn de Privilegios a usuarios		
Proceso de logeo		
Copia de resguardo		
Proceso de resguardo de la informaciòn		
Registro informatizado de firmas de usuario (segun ley 27269)		
Politicas de Seguridad de la informaciòn		
Privacidad y proteccion de los datos de usuarios y pacientes		
Simultaneidad de accesibilidad		
Politicas de control de acceso		
Politicas de Seguridad de la informaciòn		
Registro y de-registro de usuario		
Gestion de Acceso de usuario		
Gestion de la capacidad		
Proceso de logeo		

Confidencialidad		
Terminos o cambios de responsabilidades de empleo		
Politicas de control de acceso		
Politica de uso de controles criptograficos		
Continuidad de la seguridad de la informaciòn		
Recuperabilidad		
Controles contra el malware		
Backup de la informacion		
Inviolabilidad de los datos que constituyen HC		
Control de acceso a la informaciòn		
Restriccion de Acceso a la informacion		
Politica de uso de controles criptograficos		
Procesos de logeo		
Soporte de auditoria		
Politicas de Seguridad de la informaciòn		
Revisión del cumplimiento técnico		

Tabla 7: CheckList Validación de Juicio de Experto.

EVALUACIÓN DE EXPERTOS:

	PUNTOS A EVALUAR					
	Juez 01	**Juez 02**	**Juez 03**	**Juez 04**	**Juez 05**	**Juez 06**
Control de acceso	0.63	0.63	0.56	0.63	0.63	0.75
Privilegios de acceso	0.69	0.63	0.50	0.56	0.63	0.69
Copia de resguardo	3.00	3.00	4.00	3.00	3.00	3.00
Registro informatizado de firmas de usuario (segun ley 27269)	0.63	0.75	0.75	0.75	0.5	0.75
Simultaneidad de accesibilidad	0.63	0.67	0.54	0.58	0.63	0.63
Confidencialidad	0.63	0.75	0.75	0.56	0.56	0.69
Recuperabilidad	0.63	0.63	0.63	0.50	0.50	0.50
Inviolabilidad de los datos que constituyen HC	0.63	0.63	0.50	0.56	0.63	0.63
Soporte de auditoria	0.75	0.75	0.50	0.50	0.75	0.63
TOTAL	91%	94%	97%	85%	87%	92%

PUNTOS A EVALUAR			
* Evaluar según escala: TD(1), D(2), N(3), A(4), TD(5)			
Nombres:	**SEGUNDO KENNY RODRIGUEZ GIL**		
Control de acceso		**0.63**	**Comentarios**
Politicas de Seguridad de la informaciòn	4	0.75	-
Control de acceso a la informaciòn y servicios en redes	4	0.75	-
Seguridad de Usuario	3	0.5	-
Restriccion de Acceso a la informacion	3	0.5	-
Privilegios de acceso		**0.69**	-
Control de acceso a la informaciòn	4	0.75	-
Control de acceso a usuarios	4	0.75	-
Asignaciòn de Privilegios a usuarios	4	0.75	-
Proceso de logeo	3	0.5	-
Copia de resguardo		**3**	-
Proceso de resguardo de la informaciòn	3	0.5	-
Registro informatizado de firmas de usuario (segun ley 27269)		**0.63**	-
Politicas de Seguridad de la informaciòn	4	0.75	-
Privacidad y proteccion de los datos de usuarios y pacientes	3	0.5	-
Simultaneidad de accesibilidad		**0.63**	-
Politicas de control de acceso	4	0.75	-
Politicas de Seguridad de la informaciòn	4	0.75	-
Registro y de-registro de usuario	3	0.5	-
Gestion de Acceso de usuario	4	0.75	-
Gestion de la capacidad	3	0.5	-
Proceso de logeo	3	0.5	-
Confidencialidad		**0.63**	-
Terminos o cambios de responsabilidades de empleo	3	0.5	-
Politicas de control de acceso	4	0.75	-
Politica de uso de controles criptograficos	3	0.5	-
Continuidad de la seguridad de la informaciòn	4	0.75	-
Recuperabilidad		**0.63**	-
Controles contra el malware	3	0.5	-
Backup de la informacion	4	0.75	-
Inviolabilidad de los datos que constituyen HC		**0.63**	-
Control de acceso a la informaciòn	4	0.75	-
Restriccion de Acceso a la informacion	4	0.75	-
Politica de uso de controles criptograficos	3	0.5	-
Procesos de logeo	3	0.5	-
Soporte de auditoria		**0.75**	-
Politicas de Seguridad de la informaciòn	4	0.75	-
Revisión del cumplimiento técnico	4	0.75	-
ESTADO DE EVALUACIÓN		**0.91**	

PUNTOS A EVALUAR			
* Evaluar según escala: TD(1), D(2), N(3), A(4), TD(5)			
Nombres:	SANDRA ZORAIDA MEDRANO PARADO		
Control de acceso		**0.63**	**Comentarios**
Politicas de Seguridad de la informaciòn	4	0.75	-
Control de acceso a la informaciòn y servicios en redes	3	0.5	-
Seguridad de Usuario	3	0.5	-
Restriccion de Acceso a la informacion	4	0.75	-
Privilegios de acceso		**0.63**	-
Control de acceso a la informaciòn	4	0.75	-
Control de acceso a usuarios	4	0.75	-
Asignaciòn de Privilegios a usuarios	3	0.5	-
Proceso de logeo	3	0.5	-
Copia de resguardo		**3**	-
Proceso de resguardo de la informaciòn	3	0.5	-
Registro informatizado de firmas de usuario (segun ley 27269)		**0.75**	-
Politicas de Seguridad de la informaciòn	4	0.75	-
Privacidad y proteccion de los datos de usuarios y pacientes	4	0.75	-
Simultaneidad de accesibilidad		**0.67**	-
Politicas de control de acceso	4	0.75	-
Politicas de Seguridad de la informaciòn	3	0.5	-
Registro y de-registro de usuario	4	0.75	-
Gestion de Acceso de usuario	4	0.75	-
Gestion de la capacidad	4	0.75	-
Proceso de logeo	3	0.5	-
Confidencialidad		**0.75**	-
Terminos o cambios de responsabilidades de empleo	4	0.75	-
Politicas de control de acceso	4	0.75	-
Politica de uso de controles criptograficos	4	0.75	-
Continuidad de la seguridad de la informaciòn	4	0.75	-
Recuperabilidad		**0.63**	-
Controles contra el malware	4	0.75	-
Backup de la informacion	3	0.5	-
Inviolabilidad de los datos que constituyen HC		**0.63**	-
Control de acceso a la informaciòn	4	0.75	-
Restriccion de Acceso a la informacion	3	0.5	-
Politica de uso de controles criptograficos	3	0.5	-
Procesos de logeo	4	0.75	-
Soporte de auditoria		**0.75**	-
Politicas de Seguridad de la informaciòn	4	0.75	-
Revisión del cumplimiento técnico	4	0.75	-
ESTADO DE EVALUACIÓN		**0.94**	

PUNTOS A EVALUAR			
* Evaluar según escala: TD(1), D(2), N(3), A(4), TD(5)			
Nombres:	MARLON ENRIQUE CORREA LEON		
Control de acceso		**0.63**	**Comentarios**
Politicas de Seguridad de la informaciòn	4	0.75	-
Control de acceso a la informaciòn y servicios en redes	4	0.75	-
Seguridad de Usuario	3	0.5	-
Restriccion de Acceso a la informacion	3	0.5	-
Privilegios de acceso		**0.56**	-
Control de acceso a la informaciòn	4	0.75	-
Control de acceso a usuarios	3	0.5	-
Asignaciòn de Privilegios a usuarios	3	0.5	-
Proceso de logeo	3	0.5	-
Copia de resguardo		**3**	-
Proceso de resguardo de la informaciòn	3	0.5	-
Registro informatizado de firmas de usuario (segun ley 27269)		**0.75**	-
Politicas de Seguridad de la informaciòn	4	0.75	-
Privacidad y proteccion de los datos de usuarios y pacientes	4	0.75	-
Simultaneidad de accesibilidad		**0.58**	-
Politicas de control de acceso	4	0.75	-
Politicas de Seguridad de la informaciòn	4	0.75	-
Registro y de-registro de usuario	3	0.5	-
Gestion de Acceso de usuario	3	0.5	-
Gestion de la capacidad	3	0.5	-
Proceso de logeo	3	0.5	-
Confidencialidad		**0.56**	-
Terminos o cambios de responsabilidades de empleo	3	0.5	-
Politicas de control de acceso	4	0.75	-
Politica de uso de controles criptograficos	3	0.5	-
Continuidad de la seguridad de la informaciòn	3	0.5	-
Recuperabilidad		**0.50**	-
Controles contra el malware	3	0.5	-
Backup de la informacion	3	0.5	-
Inviolabilidad de los datos que constituyen HC		**0.56**	-
Control de acceso a la informaciòn	3	0.5	-
Restriccion de Acceso a la informacion	4	0.75	-
Politica de uso de controles criptograficos	3	0.5	-
Procesos de logeo	3	0.5	-
Soporte de auditoria		**0.50**	-
Politicas de Seguridad de la informaciòn	3	0.5	-
Revisión del cumplimiento técnico	3	0.5	-
ESTADO DE EVALUACIÓN		**0.85**	

PUNTOS A EVALUAR			
* Evaluar según escala: TD(1), D(2), N(3), A(4), TD(5)			
Nombres:	HERBERT JUNIOR ORTIZ HUAYANEY		
Control de acceso		**0.625**	**Comentarios**
Politicas de Seguridad de la informaciòn	4	0.75	-
Control de acceso a la informaciòn y servicios en redes	3	0.5	-
Seguridad de Usuario	3	0.5	-
Restriccion de Acceso a la informacion	4	0.75	-
Privilegios de acceso		**0.63**	-
Control de acceso a la informaciòn	4	0.75	-
Control de acceso a usuarios	4	0.75	-
Asignaciòn de Privilegios a usuarios	3	0.5	-
Proceso de logeo	3	0.5	-
Copia de resguardo		**3**	-
Proceso de resguardo de la informaciòn	3	0.5	-
Registro informatizado de firmas de usuario (segun ley 27269)		**0.5**	-
Politicas de Seguridad de la informaciòn	3	0.5	-
Privacidad y proteccion de los datos de usuarios y pacientes	3	0.5	-
Simultaneidad de accesibilidad		**0.63**	-
Politicas de control de acceso	4	0.75	-
Politicas de Seguridad de la informaciòn	4	0.75	-
Registro y de-registro de usuario	3	0.5	-
Gestion de Acceso de usuario	4	0.75	-
Gestion de la capacidad	3	0.5	-
Proceso de logeo	3	0.5	-
Confidencialidad		**0.56**	-
Terminos o cambios de responsabilidades de empleo	3	0.5	-
Politicas de control de acceso	4	0.75	-
Politica de uso de controles criptograficos	3	0.5	-
Continuidad de la seguridad de la informaciòn	3	0.5	-
Recuperabilidad		**0.50**	-
Controles contra el malware	3	0.5	-
Backup de la informacion	3	0.5	-
Inviolabilidad de los datos que constituyen HC		**0.63**	-
Control de acceso a la informaciòn	4	0.75	-
Restriccion de Acceso a la informacion	4	0.75	-
Politica de uso de controles criptograficos	3	0.5	-
Procesos de logeo	3	0.5	-
Soporte de auditoria		**0.75**	-
Politicas de Seguridad de la informaciòn	4	0.75	-
Revisión del cumplimiento técnico	4	0.75	-
ESTADO DE EVALUACIÓN		**0.87**	

PUNTOS A EVALUAR			
* Evaluar según escala: TD(1), D(2), N(3), A(4), TD(5)			
Nombres:	YSRRAEL CROSVIN CAMAN PESQUERIA		
Control de acceso		**0.75**	**Comentarios**
Politicas de Seguridad de la informaciòn	4	0.75	-
Control de acceso a la informaciòn y servicios en redes	4	0.75	-
Seguridad de Usuario	4	0.75	-
Restriccion de Acceso a la informacion	4	0.75	-
Privilegios de acceso		**0.69**	-
Control de acceso a la informaciòn	4	0.75	-
Control de acceso a usuarios	4	0.75	-
Asignaciòn de Privilegios a usuarios	4	0.75	-
Proceso de logeo	3	0.5	-
Copia de resguardo		**3**	-
Proceso de resguardo de la informaciòn	3	0.5	-
Registro informatizado de firmas de usuario (segun ley 27269)		**0.75**	-
Politicas de Seguridad de la informaciòn	4	0.75	-
Privacidad y proteccion de los datos de usuarios y pacientes	4	0.75	-
Simultaneidad de accesibilidad		**0.63**	-
Politicas de control de acceso	4	0.75	-
Politicas de Seguridad de la informaciòn	4	0.75	-
Registro y de-registro de usuario	3	0.5	-
Gestion de Acceso de usuario	4	0.75	-
Gestion de la capacidad	3	0.5	-
Proceso de logeo	3	0.5	-
Confidencialidad		**0.69**	-
Terminos o cambios de responsabilidades de empleo	4	0.75	-
Politicas de control de acceso	4	0.75	-
Politica de uso de controles criptograficos	3	0.5	-
Continuidad de la seguridad de la informaciòn	4	0.75	-
Recuperabilidad		**0.50**	-
Controles contra el malware	3	0.5	-
Backup de la informacion	3	0.5	-
Inviolabilidad de los datos que constituyen HC		**0.63**	-
Control de acceso a la informaciòn	4	0.75	-
Restriccion de Acceso a la informacion	4	0.75	-
Politica de uso de controles criptograficos	3	0.5	-
Procesos de logeo	3	0.5	-
Soporte de auditoria		**0.63**	-
Politicas de Seguridad de la informaciòn	4	0.75	-
Revisión del cumplimiento técnico	3	0.5	-
ESTADO DE EVALUACIÓN		**0.92**	

ANEXO N° 04: INSTRUMENTO DE AUDITORIA:

INSTRUMENTO CHECKLIST CK0001

Cuestionario de Control			CK0001
Proceso	Control de acceso restringido		
Objetivo	Analizar y evaluar las políticas de la seguridad de la información		
CUESTIONARIO			
PREGUNTA	**SI**	**NO**	**OBSERVACION**
Se cuentan con políticas de la seguridad de la información			
Se cuentan con políticas de acceso a la información			
Se cuentan con políticas de inviolabilidad de datos			
Han realizado un proceso previo para evaluar las políticas de seguridad			
Existe niveles de acceso a la información			
Se cuenta con información publica			
Se cuenta con información sensible			
Todos los usuarios pueden acceder a todo tipo de información del sistema			
Todos los usuarios pueden acceder a los datos de usuario			
Todos los usuarios tienen acceso completo al uso del sistema			
Dentro de sus políticas, cuentan con políticas de creación de backups			
Todos los usuarios cuentan con todos los permisos de acceso			
Se cuentan con usuarios con acceso limitado			
Se cuentan con usuarios de categoría administrador			
Algunos usuarios cuentan con firmas digitales			
Cualquier usuario puede crear su firma digital			
El usuario administrador puede ingresar la firma digital de otro usuario			
La información manejada dentro del sistema, está protegida			
Se cuentan con protocolos de seguridad de acceso a la información			
Se cuentan con varios servidores de Trabajo			
Se cuentan con un solo servidor para almacenar la información			
Se cuentan con servidores espejo, para proteger la información			

Tabla 8: INSTRUMENTO CHECKLIST CK0001.

ANEXO N° 04: INSTRUMENTO DE AUDITORIA:

INSTRUMENTO CHECKLIST CK0002

CheckList			CK0002
Proceso	Control de acceso restringido		
Objetivo	Verificar el registro y des-registro del usuario		
CUESTIONARIO			
PREGUNTA	**SI**	**NO**	**OBSERVACION**
Cualquier usuario puede registrar más usuarios			
El usuario administrador es el único usuario con la capacidad de crear más usuarios.			
El usuario creado puede modificar sus permisos de acceso			
El sistema elimina usuario inactivos pasados un tiempo prudencial			
El sistema cuenta con una sección donde se pueden visualizar los usuarios inactivos			
El sistema cuenta con una sección donde se pueden visualizar los usuarios eliminados			
El sistema cuenta con categorías de usuarios			
El sistema cuenta con usuarios que poseen diferentes permisos			
El sistema muestra información de ingreso y salida de los usuarios			
Los usuarios inactivos pueden ingresar al sistema inmediatamente			
Si se elimina un usuario del sistema, se pierde completamente			
El usuario Administrador es el encargado del área de sistemas			
Existen usuarios con accesos restringidos			
Existen usuarios que poseen todos los accesos			
Existen varios superusuarios o usuarios administrativos			
Actualmente existen usuarios que no utilicen sus usuarios			
Se lleva un control de todos los usuarios registrados			
Se lleva un control de todos los usuarios inactivos			
Se lleva un control de todos los usuarios eliminados			
El sistema permite exportar todos los usuarios del sistema indicando el estado de cada uno			

Tabla 9: INSTRUMENTO CHECKLIST CK0002.

ANEXO N° 04: INSTRUMENTO DE AUDITORIA:

INSTRUMENTO CHECKLIST CK0003

Cuestionario de Control			CK0003
Proceso			Control de acceso restringido
Objetivo			Comprobar las restricciones de acceso a la información
CUESTIONARIO			
PREGUNTA	**SI**	**NO**	**OBSERVACION**
El sistema cuenta con niveles de usuario			
El sistema cuenta con un nivel Administrador o Superusuario			
Cualquier usuario puede acceder a toda la información del Sistema			
El sistema cuenta con restricciones de acceso a la información			
El usuario Administrador cuenta con todos los permisos de acceso al Sistema			
El usuario Administrador puede modificar los accesos de los demás usuarios			
El usuario Administrador puede eliminar datos del Sistema			
Cualquier usuario puede modificar su nivel de usuario			
Todos los usuarios tienen acceso a los módulos del Sistema			
Todos los usuarios tienen acceso para realizar mantenimientos a los módulos del Sistema			
Los usuarios pueden eliminar datos del Sistema			
Los usuarios cuentan con todos los permisos de acceso al Sistema			
Se lleva un control de los permisos que posee cada usuario dentro del Sistema			
Se lleva un control de los permisos que se pueden brindar en el sistema			
El usuario Administrador puede registrar nuevos permisos en el Sistema			
Cualquier usuario puede registrar nuevos permisos dentro del Sistema			
La información manejada dentro del Sistema se encuentra clasificada			
La información manejada dentro del Sistema se encuentra restringida para algunos usuarios			
Usuarios externos al Sistema pueden verificar información del Sistema			
Se cuentan con un módulo para que los clientes verifiquen su información dentro del Sistema			

Tabla 10: INSTRUMENTO CHECKLIST CK0003.

ANEXO N° 04: INSTRUMENTO DE AUDITORIA:

INSTRUMENTO CHECKLIST CK0004

Cuestionario de Control			CK0004
Proceso			Privilegios de acceso
CUESTIONARIO			
PREGUNTA	**SI**	**NO**	**OBSERVACION**
El sistema cuenta con privilegios de acceso a la información			
El sistema cuenta con políticas de control de acceso			
Se lleva un control de los accesos que tiene cada usuario			
El usuario Administrador cuenta con todos los privilegios de acceso			
Los usuarios del Sistema cuenta con algunos privilegios de acceso al Sistema			
La información manejada dentro del Sistema se encuentra protegida			
La información manejada dentro del Sistema se encuentra encriptado			
Los usuarios pueden brindar privilegios a otros usuarios			
Los usuarios pueden cambiar sus privilegios de acceso			
El usuario Administrador pueden brindar privilegios a otros usuarios			
Existen una opción para modificar los privilegios de acceso			
El sistema permite crear nuevos privilegios			
El sistema permite eliminar privilegios creados			
El sistema cuenta con un proceso seguro de logueo			
El sistema cuenta con una sección de captcha para ingresar al sistema			
El sistema solicita al usuario ingresar su usuario y contraseña antes de ingresar al sistema			
El sistema valida el proceso de logueo al sistema			
El sistema lleva un registro de todos los logueos dentro del sistema			
Se cuenta con un registro de todos los privilegios que cuenta el sistema			
Se cuenta con un registro de todos los usuarios y sus respectivos privilegios			

Tabla 11: INSTRUMENTO CHECKLIST CK0004.

ANEXO N° 04: INSTRUMENTO DE AUDITORIA:

CHECKLIST CK0005

Cuestionario de Control			CK0005
Proceso			Sistema de copia de resguardo
CUESTIONARIO			
PREGUNTA	**SI**	**NO**	**OBSERVACION**
El sistema cuenta con políticas de copias de resguardo			
Se cuenta con un plan de copias de resguardo			
Se viene cumpliendo el plan de copias de resguardo			
Se realizan las copias de resguardo en caliente			
Se realizan las copias de resguardo en un horario nocturno			
Cuando se realizan las copias de resguardo se inactiva el sistema			
Se realizan copias de resguardo de todas las tablas de la base de datos			
Se realizan copias de resguardo cada semana			
Se realizan copias de resguardo cada mes			
Se realizan copias de resguardo anualmente			
Se realizan copias de resguardo del aplicativo del Sistema			
Cuando se realizan las copias de resguardo, se realiza un testeo del backup			
Se cuenta con un registro de todas las copias del sistema			
Se lleva un control de las copias realizadas al Sistema			
Se cuenta con una bitácora de las copias realizadas al Sistema			
Se elimina las copias del sistema pasado cierto tiempo			
Se mantienen todas las copias del Sistema desde su lanzamiento			
Las copias del Sistema se mantienen en dispositivos externos al servidor			
Las copias del Sistema se almacenan dentro del mismo servidor			
Cuando el sistema produce algún error se restaurar con la última copia realizada			
Cuando la base de datos produce errores se restaurar con la última copia realizada			

Tabla 12: INSTRUMENTO CHECKLIST CK0005

ANEXO N° 04: INSTRUMENTO DE AUDITORIA:

CHECKLIST CK0006

Cuestionario de Control			CK0006
Proceso	Verificar las políticas de la seguridad de la información		
CUESTIONARIO			
PREGUNTA	**SI**	**NO**	**OBSERVACION**
Se cuentan con políticas de seguridad para el control de firmas digitales			
Se cuenta con un módulo de procedimiento para el ingreso de firmas digitales			
Se cuentan con un registro de todas las firmas digitales ingresadas en el sistema			
Se lleva un control de todas las firmas digitales ingresadas al sistema			
Se lleva un control histórico de todas las firmas digitales ingresadas al sistema			
Se ingresa la firma digital, por medio de un equipo externo al sistema			
Se trabaja la firma digital en un formato de imagen (.jpg, .png, etc.)			
Todos los usuarios pueden ingresar firmas digitales al sistema			
El usuario Administrador es el único usuario que puede ingresar firmas digitales al sistema			
El ingreso de la firma digital se realiza una única vez			
Se puede actualizar la firma digital ya ingresada			
Se puede eliminar la firma de un usuario activo			
Se lleva un control de backups de las firmas digitales dentro del sistema			
Se elimina la firma digital de un usuario o paciente eliminado			
La firma digital del paciente se utiliza para otros fines ajenos al sistema			
El paciente puede solicitar su firma digital			
Si se realiza una actualización de firma, se actualiza en otros campos del sistema			
Si se realiza una actualización de firma, se debe realizar en todos los campos del sistema			
Si se elimina la firma digitalizada de un usuario, se elimina en otros campos del sistema			
Si se elimina la firma digitalizada de un usuario, se debe realizar este procedimiento en otros campos del sistema			

Tabla 13: INSTRUMENTO CHECKLIST CK0006

ANEXO N° 04: INSTRUMENTO DE AUDITORIA:

CHECKLIST CK0007

Cuestionario de Control			CK0007
Proceso			Simultaneidad de accesibilidad
CUESTIONARIO			
PREGUNTA	**SI**	**NO**	**OBSERVACION**
Una misma información puede ser verificara por varios usuarios al mismo tiempo			
Una misma información puede ser actualizada por varios usuarios al mismo tiempo, sin corromper los datos			
Se puede realizar el registro de varios usuarios al mismo tiempo			
Se puede realizar la actualización de varios usuarios al mismo tiempo			
Se pueden modificar los permisos de un usuario actualmente logueado			
Se pueden quitar los permisos de un usuario actualmente logueado			
Se pueden restringir los accesos de un usuario actualmente logueado			
Un usuario puede ingresar con su mismo usuario desde dos terminales diferentes			
Se puede verificar los usuarios actualmente logueado			
Se puede verificar los usuarios actualmente deslogueado			
Se puede verificar el modulo que se encuentran trabajando los usuarios			
Se puede verificar a dos terminales que están accediendo con el mismo usuario			
Se tiene un reporte de los usuarios que ingresan al día			
Cualquier usuario puede ingresar información de un cliente en un examen especifico			
La información ingresada por un usuario, es visible en tiempo real por otro usuario.			
En exámenes especiales (Audiometría, espirometria, etc) se delimita el acceso de ingreso de información a solo un usuario			
Se evidencia el acceso simultaneo de más usuarios a un examen medico			
Se registra las acciones de cada usuario que ha ingresado a un examen			
Hay forma de identificar qué información a ingresado cada usuario en el examen medico			
Hay forma de revertir los cambios realizados por un usuario en un examen medico			

Tabla 14: INSTRUMENTO CHECKLIST CK0007

ANEXO N° 04: INSTRUMENTO DE AUDITORIA:

CHECKLIST CK0008

Cuestionario de Control			CK0008
Proceso	Confidencialidad		
PREGUNTA	**SI**	**NO**	**OBSERVACION**
Se cuenta con políticas de seguridad de la información			
Se define términos de confidencialidad de la información al inscribir o registrar un usuario en el sistema			
Existe una clausula o documento que defina condiciones al realizar la contratación de un trabajador			
Existe un proceso disciplinario al faltar un acuerdo de confidencialidad de la información			
Se puede evidenciar una falta de confidencialidad en los registros de auditoria del sistema			
Si el usuario cambia de cargo y responsabilidades se establece nuevos términos de confidencialidad			
Al cambiar el usuario de responsabilidades se le asigna un nuevo perfil o tipo de usuario en el sistema			
Se cuenta con políticas de acceso a la información			
Se tiene definidos niveles de acceso por perfil o tipo de usuario			
Se controla el acceso a la información externa al sistema, documentos compartidos en red			
Se controla el acceso a las redes existente por usuario			
Toda información en red o en el sistema es accedida a través de una autenticación por usuario			
La autenticación es única por usuario			
Se maneja encriptación de las credenciales de usuario			
Las credenciales por usuario son registradas y guardadas de forma segura, encriptado y reguardada			
Cada usuario tiene los privilegios para el cambio de sus credenciales			
Existe un usuario administrador que puede visualizar las credenciales de cada usuario			
Los niveles de encriptación de las credenciales de usuario son totalmente seguras			

Tabla 15: INSTRUMENTO CHECKLIST CK0008

ANEXO N° 04: INSTRUMENTO DE AUDITORIA:

CHECKLIST CK0009

Cuestionario de Control			CK0009
Proceso	Recuperabilidad		
PREGUNTA	**SI**	**NO**	**OBSERVACION**
Se cuenta con protocolos de recuperación de la información			
Se cuenta con programas antivirus activos			
Se cuenta con programas antivirus seguros			
Se cuenta con un plan de respuesta frente a virus o malware			
Se cuenta con licencias oficiales para los antivirus			
Los programas antivirus están siempre están actualizándose			
Los programas antivirus están actualizados			
Los programas antivirus se actualizan automáticamente			
Se cuenta con programas antimalware			
El servidor principal se encuentra limpio de amenazas			
Se actualizan los antivirus diariamente			
Se actualizan los antivirus mensualmente			
Se limpian lógicamente las computadoras semanalmente			
Se realizan backups de los registros de la limpieza de los antivirus			
Se realizan backups de los archivos que tienen los equipos de los usuarios			
Se realizan backups de los sistemas operativos			

Tabla 16: INSTRUMENTO CHECKLIST CK0009

ANEXO N° 04: INSTRUMENTO DE AUDITORIA:

CUESTIONARIO CU001

CUESTIONARIO CU001

USUARIO:

_____

1. Mencione todas las políticas de seguridad que cuenta su Sistema.
   _____
   _____
   _____
   _____
   _____
   _____
   _____
2. ¿Cuáles son los grupos de usuarios que se cuentan actualmente?
   _____
   _____
   _____
   _____
   _____
   _____
   _____
3. ¿El sistema cuenta con niveles de acceso por tipo de usuario y cuáles son los tipos de usuario?

   _____
   _____
   _____
   _____
   _____
   _____
   _____
4. ¿Qué usuarios pueden acceder a los backups de seguridad?

   _____
   _____
   _____
   _____
   _____
   _____
   _____
5. ¿El sistema posee políticas de control de acceso? ¿Cuáles son estas? ¿Son aplicadas en su totalidad?

   _____
   _____
   _____

ANEXO N° 04: INSTRUMENTO DE AUDITORIA:

CUESTIONARIO CU002

CUESTIONARIO CU002 (REGISTRO DE USUARIOS)

USUARIO:

_____

1. ¿Cuántas y Cuáles han sido los últimos usuarios registrados?

2. ¿Cuántos y Cuáles son los usuarios registrados del Sistema?

3. ¿Cuántos y Cuáles son los usuarios eliminados del Sistema?

4. Mencione todas las categorías o tipos de usuario.

5. Mencione todos los superusuarios del sistema.

6. Mencione todos los usuarios registrados.

7. Mencione las restricciones del sistema por usuario.

ANEXO N° 04: INSTRUMENTO DE AUDITORIA:

CUESTIONARIO CU0003

CUESTIONARIO CU0003 (Control de Acceso)

USUARIO: _____

1. Mencione los niveles de usuarios en el Sistema.
   _____
   _____
   _____
   _____
2. Mencione los módulos que posee su Sistema.
   _____
   _____
   _____
   _____
3. Mencione los permisos que posee su Sistema.
   _____
   _____
   _____
   _____
4. ¿Qué usuarios pueden eliminar datos del sistema?
   _____
   _____
   _____
   _____
5. ¿Qué usuarios cuentan con el acceso de Administrador?
   _____
   _____
   _____
   _____
6. ¿Qué información está restringida para la mayoría de usuarios?
   _____
   _____
   _____
   _____

ANEXO N° 04: INSTRUMENTO DE AUDITORIA:

CUESTIONARIO CU0004

CUESTIONARIO CU0004 (Privilegios de acceso)

USUARIO:

_____

1. ¿Qué métodos o procedimientos aplica para proteger la información?

   _____

   _____

   _____

2. ¿Qué usuarios pueden modificar sus privilegios?

   _____

   _____

   _____

3. ¿Qué procedimientos utiliza el sistema para mantener el logueo seguro?

   _____

   _____

   _____

   _____

4. ¿Qué procedimientos utiliza el sistema para validar el logueo?

   _____

   _____

   _____

   _____

5. Mencione todos los privilegios del sistema.

   _____

   _____

   _____

6. Mencione todos los privilegios actualmente ingresados al sistema.

   _____

   _____

   _____

7. Mencione el registro de usuarios y sus privilegios.

ANEXO N° 04: INSTRUMENTO DE AUDITORIA:

CUESTIONARIO CU0005

CUESTIONARIO CU0005 (Copias de resguardo)

Usuario: _____

1. ¿Qué usuarios pueden realizar copias de resguardo?

   _____
   _____
   _____

2. ¿A qué partes del sistema realiza las copias de resguardo?

   _____
   _____
   _____

3. ¿En qué momentos se realizan las copias de resguardo? ¿Por qué?

   _____
   _____
   _____

4. ¿Cada cuánto tiempo se realizan las copias de resguardo? ¿Por qué?

   _____
   _____
   _____

5. ¿Qué medidas de prueba se utiliza para probar las copias de resguardo?

   _____
   _____
   _____

6. Mencione todas las copias de resguardo realizadas con su fecha respectiva.

   _____
   _____
   _____
   _____

7. ¿Qué procedimientos aplica cuando restaura la base de datos?

   _____
   _____
   _____
   _____

ANEXO N° 04: INSTRUMENTO DE AUDITORIA:

CUESTIONARIO CU0006

CUESTIONARIO CU0006 (Seguridad de la información)

USUARIO: _____

1. ¿Qué métodos o procedimientos utiliza para registrar una firma digital?
2. ¿Con que tipo de formato trabaja para guardar una firma digital?
3. ¿Qué usuarios pueden registrar firmas digitales?
4. ¿Qué métodos o procedimientos de copias de resguardo utiliza para guardar backups de las firmas digitales?
5. ¿Qué procedimientos debe realizar un paciente para tener acceso a su firma digital?

ANEXO N° 04: INSTRUMENTO DE AUDITORIA:

CUESTIONARIO CU007

CUESTIONARIO CU007 (ACCESIBILIDAD)

USUARIO:

_____

1. ¿Qué medidas o políticas de control de acceso simultaneo cuenta el sistema?

2. ¿Qué usuarios se encargan de asignar los privilegios a los usuarios del sistema?

3. ¿Cómo se pueden verificar que usuarios se encuentran conectados al sistema?

4. ¿Cómo se lleva el control de lo que los usuarios realizan en el sistema?

5. ¿Cómo se pueden revertir cambios que no eran necesarios dentro del sistema?

ANEXO N° 04: INSTRUMENTO DE AUDITORIA:

CUESTIONARIO CU008

CUESTIONARIO CU008 (Confidencialidad)

USUARIO:

_____

1. ¿Con que políticas de confidencialidad de la información cuenta su sistema informático?

2. Mencione todas las políticas de confidencialidad de la información que los usuarios cuentan y los usuarios a los que se aplican.

3. ¿Qué usuarios pueden modificar sus claves de acceso?

4. ¿Cómo funciona el proceso de autenticación de los usuarios registrados?

5. ¿Cómo los usuarios pueden acceder al sistema de manera externa?

ANEXO N° 04: INSTRUMENTO DE AUDITORIA:

CUESTIONARIO CU009

CUESTIONARIO CU009 (Recuperabildad)

USUARIO:

_____

1. ¿Con que tipos de programas antivirus se cuenta actualmente?

2. ¿Qué medidas de seguridad se cuenta para proteger el servidor principal de amenazas?

3. ¿Qué procedimientos se aplican para mantener los antivirus actualizados?

4. ¿Dónde se almacena la información de los bakcups realizados?

5. ¿Qué medida o control de registro se lleva sobre la restauración de la información?

ANEXO N° 04: INSTRUMENTO DE AUDITORIA:

CUESTIONARIO CU0010

CUESTIONARIO CU0010 (Inviolabilidad de datos)

USUARIO:

_____

1. ¿Qué usuarios pueden registrar pacientes nuevos?
   _____
   _____
   _____
2. ¿Qué usuarios pueden registrar datos en una historia clínica?
   _____
   _____
   _____
3. ¿Qué usuarios pueden modificar los datos en una historia clínica?
   _____
   _____
   _____
4. ¿Qué usuarios pueden eliminar los datos en una historia clínica?
   _____
   _____
   _____
5. ¿Qué medidas de control se tienen para las impresiones de las historias clínicas?
   _____
   _____
   _____
6. ¿Con que modelos de reportes se cuentan actualmente para las historias clínicas?
   _____
   _____
   _____
7. ¿Qué medidas de control se tienen para las historias clínicas eliminadas?
   _____
   _____
   _____

ANEXO N° 05: CARTA DE APROBACIÓN

CARTA DE APROBACIÓN

12 DE AGOSTO DEL 2019

SEÑORES
JESUS CALIXTO TELLO Y JULIO GONZÁLEZ MAYANGA
BACHILLERES EN INGENIERÍA DE COMPUTACIÓN DE SISTEMAS
Universidad Privada Antenor Orrego
Trujillo.-

Estimados Señores:
Por este medio del presente y en base a mis conocimientos y experiencia en Auditoría de Tecnología de Información, brindo mi aprobación a la propuesta de "Modelo de auditoria basado NT MINSA N° 22-2005 e NTP ISOIEC: 27001-2014 para evaluar los sistemas de información de gestión de historias clínicas en los centros de salud ocupacional de la provincia de Trujillo - 2019", puesto que cumple con los estándares y criterios propuestos en la Norma Técnica de Salud N° 22-MINSA-2005 (Ministerio de Salud, 2005) e NTP ISO/IEC 27001:2014 (ISO, 2013)

Atentamente

……..
FIRMA

NOMBRES Y APELLIDOS:

DNI: