UNIVERSIDAD SAN PEDRO
FACULTAD DE INGENIERIA
PROGRAMA DE ESTUDIOS DE INGENIERÍA
INFORMÁTICA Y DE SISTEMAS

Auditoria de seguridad informática para el Hospital Regional de Huacho - 2016

TESIS PARA OBTENER EL TITULO PROFESIONAL DE INGENIERO EN INFORMATICA Y DE SISTEMAS

Autor

Muñoz Fernández, Sandro Arturo

Asesor

Lara Carreño, Marco

Huacho - Perú

2020

PALABRAS CLAVE

Tema : Auditoria

Especialidad : Gestión

KEY WORDS

Theme : Segurity

Speciality : Management

LINEA DE INVESTIGACION

Línea : Sistemas de Gestión

Área : Sociales

Sub área : Economía y negocios

Disciplina : Sistemas de gestión

Titulo

Auditoria de Seguridad Informática para el Hospital Regional de Huacho-2016.

Resumen

El propósito de la presente investigación fue implementar una auditoria de seguridad informática para el hospital regional de huacho-2016, la cual permitió mejorar el nivel de seguridad, dando a conocer vulnerabilidades en su uso, en el Área de informática del Hospital se administra gran cantidad de datos, lo cual son de mucha importancia, ya que cada dato obtenido es de carácter confidencial, por lo cual facilito tomar mejores medidas preventivas y correctivas.

Esta investigación se apoyó utilizando la Norma ISO 27001, la cual permitió evaluar la eficiencia y eficacia de seguridad Informática del Hospital Regional de Huacho. El tipo y nivel de investigación que utilice fue descriptivo.

conclusión, los resultados esperados fueron para permitir identificar y eliminar las vulnerabilidades que existen y para reducir esto incidentes fueron necesario aplicar normas de seguridad, el cual se dieron las recomendaciones adecuadas para el correcto uso de seguridad informática y los cambios que requiere el Hospital Regional de Huacho para poder lograr mejores resultados.

Abstract

The purpose of the present investigation was to implement a computer security audit for the regional hospital of huacho-2016, which allowed to improve the security level, revealing vulnerabilities in its use, of data, which are very important, since each data obtained is of a confidential nature, which is why I facilitate better preventive and corrective measures.

This research was supported using the ISO 27001 standard, which allowed to evaluate the efficiency and effectiveness of IT security at the Huacho Regional Hospital. The type and level of research he used was descriptive.

In conclusion, the expected results were to identify and eliminate the vulnerabilities that exist and to reduce these incidents, it was necessary to apply security standards, which provided adequate recommendations for the correct use of computer security and the changes required by the Regional Hospital of Huacho to achieve better results

INDICE

1. Introducción

El presente proyectos de tesis consiste en implementar una Auditoria de Seguridad Informática para el Hospital Regional de Huacho-2016, el cual al finalizar el proyecto de investigación ayudara al Hospital a identificar y eliminar vulnerabilidades que existen, así poder reducir estos incidentes encontrados en el Área de Informática.

Canales (2007) En su estudio de investigación propuso identificar los puntos débiles en el funcionamiento y administración de los centros de ingeniería de la información de la Facultad de Ingeniería Industrial de la UNJFSC, así como también la correcta utilización y mantenimiento de los recursos informáticos en esta dependencia. Es decir, no se cuenta con un documento oficial por parte de la entidad en la que se estipule la organización, funciones y responsabilidades de los funcionarios de esta área, lo cual en un proceso de auditoría los eximiría de responsabilidades.

Ramos y Ysela (2006) En su estudio realizó una investigación cuyo objetivo es diseñar e implementar un plan de seguridad de la información que permita proteger los activos tecnológicos y evaluar las necesidades de seguridad informática en la relación con la estructura del área de informática, utilizando herramientas de análisis de riesgo, para así desarrollar políticas y procedimientos, que permitan desempeñar de manera óptima y segura las actividades en la UGEL N° 09 – Huaura. Por lo cual su finalidad es aplicar medidas correctivas para los distintos activos de información que reducen considerablemente las vulnerabilidades con las que se contaba, pero es necesario su mantenimiento y actualización, así como a un estudio periódico sobre nuevos activos que se adquieran en el futuro como las nuevas amenazas que puedan sugerir las medidas que se deben adoptar.

Torres y Shirley (2006) realizaron una tesis, cuyo objetivo fue comprobar la existencia de procedimientos y de su correcto funcionamiento, según las normas de seguridad vigentes para el resguardo de información en el área de TI de la Municipalidad distrital de Sayán. Dicha entidad se encuentra propensa a sufrir ciertos ataques ya sean naturales o de otra índole, por no contar con mecanismos y medios formales como planes de contingencia, planes de continuidad de negocios, políticas de seguridades, entre otras; que permitan contrarrestar estos ataques.

Villacís (2006) en su estudio de tesis propuso conocer más a fondo los detalles sobre una evolución en la auditoria Forense informática, las cuales presentan vulnerabilidades muy comunes en el sector informático, lo cual es primordial encontrar sus diferentes soluciones a esta debilidad común en el sector informático. Cuya finalidad es contribuir con todo el material de apoyo para las entidades o empresas, esta tesis pretende ser una guía para las entidades o empresas de todo el país en el futuro, cuya existencia tengan muchos documentos sobre el tema.

Hernández (2006) en sus estudios de tesis propuso ayudar a la organización comercial para tener una concienciación permanente para mantener seguros sus activos e información, tomando en cuenta que la palabra activa son recursos informáticos, relacionados que la organización funcione correctamente y alcance los objetivos propuestos por cada entidad o empresa. Cuyo propósito es conocer la importancia, el valor y la razón de la vulnerabilidad para formar un criterio necesario para mantener segura la información. Por lo tanto, su objetivo es conocer a fondo todo su recurso humano con la cual laboran y sus riesgos a los que están expuesto los datos y la información directa o indirectamente. Lo cual se llegó a la conclusión que cada empresa tome conciencia de lo importante que es tener la información segura y confiable, integrada y disponible, de lo contrario todo esto conllevaría a resultados nefastos para la entidad.

Reyes, M. (2010) en su proyecto de investigación: “Propuesta para impulsar la seguridad informática en materia de educación, tuvo como conclusión lo siguiente: En la actualidad la información desempeña un rol importante en cada negocio, por lo cual es importante tener un sistema de seguridad, que permita proteger a cada usuario con su privacidad para proteger la información.

Villena, M. (2010) En su proyecto de estudio de tesis: “Sistema de Gestión de Seguridad de la Información para una Institución Financieras”, se llegó a una conclusión: Lo importante para obtener una información adecuada y protegida en una institución financiera, primeramente, es contar con el visto bueno y asistencia de gerencia, lo cual permite tener la información adecuadamente protegida por la entidad. Por lo tanto, la información debe ser enviado a cada propietario de la institución, para tener cada usuario responsabilidad al momento de manejar la información.

Se informo de lo importante que es la seguridad en cada proceso que se maneja, contando con el apoyo y poniendo de su parte todo el personal responsable, para gestionar pautas en cada política de seguridad, norma y estándar, respaldado por cada información. Cuyo manejo es de acuerdo a los objetivos que cuenta la entidad, siempre manteniendo actualizado los cambios y actividades.

Freddy Yan y Cinthia Zavala (2013) en su trabajo realizo el proyecto de investigación del estudio de auditoria de sistemas para la GRE La Libertad, que nos permitió evaluar la operación, usando los sistemas de información, los niveles de seguridad, los procedimientos de respaldo de datos, la seguridad de los equipos de cómputo, redes, comunicaciones, a nivel de prestación de servicios informáticos y de tecnología, con el propicito de brindar una recomendación necesaria para incorporar una forma integral a cada sistemas de control y gestión de riesgos en una organización.

A través de un enfoque y un marco metodológico de MAIGTI, nos permitió obtener una mejor manera de actividad para cada una de las fases de la auditoria, lo cual nos permitió facilitar el análisis y la evaluación del centro de datos, concluyendo que su seguridad es vulnerable y débil, para cada una de la aplicación en las normas técnicas y buenas prácticas. De la misma manera, se cumplió y se buscó el beneficio de la organización a través de las recomendaciones emitidas.

Las metodologías son importantes y necesarias para el desarrollo de cualquier proyecto o investigación que nos propongamos a realizar de manera ordenada y eficaz en cada entidad.

Auditoria

La importancia de la auditoria es analizar detalladamente con precisión y veracidad cada registro en una entidad, con el fin de corregir fallas o irregularidades y fraudes en cada entidad. (Martha Carrasco, 2016).

Según Paulina Brito los resultados principales de una auditoria son lo siguiente: Establecer normas ambientales incluyendo protección, seguridad y salud cualquier entidad. Proponer objetivos y metas para mejorar la entidad. Identificando las unidades o áreas de los procesos que son críticos para la eficiencia operacional de la entidad. De igual manera la auditoría se clasifica en dos formas: Auditoría Interna y Auditoría Externa.

Auditoría Interna

La auditoría interna es un proceso de control que permite controlar, prevenir y proteger sus activos, minimizando riesgos y incrementando los procesos operativos y óptimos de la empresa. (Gago Rios, 2013).

Instituto de Internidad del Perú (IAIP (2012), manifestó que la auditoría interna su porcentaje de incremento de objetivos es muy elevado para proteger las estafas, fraudes y desvíos de bienes o dinero de una entidad.

Por lo tanto, la ISO Según el Instituto de Auditores Internos (2004, p.23) indica que la auditoría interna, tiene una función independiente de procesos que permiten proporcionar un enfoque sistemático disciplinado, para mejorar un proceso eficiente en los controles de la empresa

Elorrega (2009), detalla que la auditoría interna cuenta con un rol importante en una entidad moderna, ya que nos permite un desarrollo económico y social de nuevas prácticas de gestión, encontrando objetivos de información, análisis y evaluación en cada empresa. (p90).

Auditoría Externa.

La auditoría externa es llevada a cabo por profesionales auditores procedente del exterior, con el fin de verificar correctamente los manejos y relación de los procesos de una empresa. (Ogaldez Muñoz, 2011).

Estas auditorías externas son realizadas por grandes compañías y firmas de auditoría independientes, que buscan analizar o evaluar procesos de un punto de vista externo y profesional acerca de las actividades de una empresa en particular. (Ogaldez Muñoz, 2011).

En conclusión, la auditoría externa tiene como objetivo principal obtener una certificación en el sistema de gestión de calidad, lo cual es presentado por las empresas a los clientes potenciales y proveedores, dándole la confianza con su certificación. (Ogaldez Muñoz, 2011).

Auditoria de Seguridad Informática.

Se define como un nivel de evaluación alto en la seguridad de una organización, donde se analizan políticas y procedimientos de seguridad adecuados a la tecnología, llevado de manera oportuna y eficaz en la organización. (Piattini, 2003, p.2).

De igual forma tiene como proceso importante la configuración y capacitación de cada personal especializado en seguridad, para permitir un ambiente seguro y eficaz en la entidad, controlando la información de la organización. (Piattini, 2003, p.3).

La auditoría es:

Un proceso de recopilación, agrupación y evaluación de evidencias que determinan un sistema de información para proteger datos de cada empresa, utilizando de manera eficaz los recursos establecidos.

También es proceso y conjunto de acciones asignadas por auditores capacitados y personal autorizado para garantizar los procesos y recursos de la información entorno al control seguro y eficaz de la gerencia.

Seguridad de la Información.

La Organización Internacional de Normalización (ISO) define la seguridad de la información (SI) como un conjunto de medidas preventivas e reactivas de una organización, cuyas tecnologías nos permite resguardar y proteger cada información.

Lo cual consiste en tres condiciones bases:

Confidencialidad: indica que cada información no puede ser divulgada o maneja de manera inusual a cada individuo que no pertenezca a la organización de cada proceso no autorizado.

Integridad: es mantener los datos exactos tal cual fue generada, sin ser manipuladas por personas no autorizada, de igual forma pueden ser afectadas por virus, software o hardware dañados.

Disponibilidad: es tener facilidad y acceso a los datos e información de la organización por personas autorizadas en el momento que así lo requieran según sea necesario en la entidad. (López, 2019, p.15).

Amenazas y Vulnerabilidades.

Amenazas: son situaciones que desencadenan en un percance en la organización, causando perdidas o daños materiales de datos de información.

Alexander (2007), propone que las amenazas se clasifiquen en grupos para tener una facilidad de decisiones generadas, cuyo propósito es reducir los riesgos en una sola medida.

Lopez (2011), indica los problemas que podemos encontrar:

Naturales: fallas eléctricas, desastres naturales.

Humanas Accidentales: negligencia, perdida no intencional de datos.

Humanas Intencionales: robo de datos, ataques, suplantación de identidad.

Tecnologías: Virus, Hacker, pedida de datos, falla de software y hardware o de la red. (p.15).

Vulnerabilidades: es la potencialidad o la posibilidad de materializar una amenaza sobre los datos.

Lopez (2011), indica que la vulnerabilidad forma parte de un problema que están relacionadas a identificar riesgos que expongan cualquier información del sistema. Lo cual lo expertos de seguridad analizan el riesgo o efecto causal de la relación en los datos.

Lo cual puede presentar fallo en los datos que pueden poner en riesgo la información, también pueden comprometer a la organización, puesto que es necesario de analizarlas y ubicarlas para poder ser eliminadas lo más urgente posible.

En conclusión, se debe analizar y definir los niveles de riesgos o amenazas, que permitan implementar procedimientos que puedan ayudar a eliminar las vulnerabilidades que puedan existir en cada organización. (p.17).

Tecnología de Información (TI):

Conocemos como tecnología de información (TI), a la utilización de procesos tecnológicos específicos de cada computador y ordenador electrónicos para el manejo y procesamiento de la información, especificando la captura y transformación, almacenamiento, protección y recuperación de datos e información.

Sáez Vacas, (1983): la tecnología son las que se aplican en la adquisición, de procesamiento, almacenamiento y perdida de información vocal, icónica, textual o numérica.

Valle, (1986): se consideran tecnologías al manejo y tratamiento de la información, lo cual esta entendida en un conjunto de datos, señales o conocimientos, registrados o transportados sobre soportes físicos de muy diversos tipos. Las tecnologías de la información abarcan técnicas, dispositivos y complejidad.

Tipos de TI:

Podemos realizar una clasificación detallada de tecnologías de la información y comunicación en redes, terminales y servicios.

Redes: la telefonía fija, la banda ancha, la telefonía móvil, las redes de televisión o las redes en el hogar son algunas de las redes de TI.

Terminales: existen dispositivos o terminales que forman parte de las TIC. Lo cuales son el ordenador, el navegador de Internet, el sistema operativo, los teléfonos móviles, los televisores, los reproductores portátiles de audio y video o las consolas de juego (PES).

Servicios en las TI: la tecnología de información cuenta con varios servicios. Las cuales las más importantes son: Correo electrónico, búsqueda de información, banca online, el audio y la música, la televisión y el cine, la educación, los videojuegos y los servicios móviles (celulares).

Papel de las TIC en la empresa:

Optimizar las gestiones de la empresa, cambiando de manera administrativa los recurso, modificando la forma de trabajo basado en equipos tecnológicos con herramientas digitales.

Operaciones Eficiente, permite reducir o eliminar duplicaciones, errores y retrasos que pueden darse durante el trabajo, como también acelerando la automatización de tareas específicas en una entidad.

Seguridad Mejorada, nos permite mantener seguro la información importante y menos expuestos a las vulnerabilidades, evitando la desviación de la información por cibercriminales con facilidad. También, con la tecnología se puede controlar y vigilar remotamente las entidades o empresas.

Globalización, cuentan con un mayor alcance en todo el mercado global, cuyo propósito es poder hacer negocios en cualquier parte del mundo gracias a la tecnología, siendo una pieza fundamental para la globalización económica en cada país, incrementando el comercio internacional.

La tecnología cada día está evolucionando y teniendo muchos cambios en la sociedad y en el mercado laboral. Por lo tanto, debemos sacar provecho a los beneficios que nos puede brindar la tecnología en los negocios optimizando un desempeño eficaz y rápido en una entidad.

ISO/IEC 27001:2013

Tiene como Objetivo proponer una seguridad de información en una entidad u organización. Lo cual es considerada una norma internacional por la Organización Internacional de Normalización (ISO), lo cual fue publicada por primera vez en el año 2005 en base a la Norma Británica BS 7799-2, posterior mente se actualizaría en el año 2013 bajo el nombre de ISO/IEC 27001:2013.

Cuya norma puede ser implementada para un mejor manejo para proponer un proceso adecuado de seguridad en una organización. Cuya metodología establece, implementa, mantiene un sistema de gestión adecuada en la seguridad de la información (SGSI), teniendo coherencia y fácil manejo. Permitiendo una certificación adecuada en la organización por una entidad ya sea pública o privada.

Un aspecto de la norma ISO 27001 incluye el ciclo de Deming el cual puede consistir en un proceso basado en una mejora continua, conocido como el ciclo PHVA: Planificar, Hacer, Verificar y Actuar, lo cual se basa en un procedimiento seguro y confiable mediante el cual se determinan los objetivos y procesos necesarios que se pueden planear e implementar (Planificar), posteriormente se procede con la implementación de los procesos (Hacer), luego, se revisan y se evalúan todos los procesos comparándolos con las políticas y objetivos sobre los resultados (Verificar), y por último, se emprenden las acciones para el mejoramiento del sistema (Actuar).

ISO/IEC 27002:2013

Es una norma internacional emitida por la Organización Internacional de Normalización (ISO) donde podemos observar el dominio y mecanismo de control que pueden tener la organización en cuanto a su seguridad de datos e información. Esta norma nos ofrece como un guía para tener una base o implementar normal de control en una organización basas en seguridad, gestionando las buenas prácticas para una seguridad eficaz y permanente. Se encuentra asociada con el Anexo A de la ISO/IEC 27001:2013.

Su publicación se dio por primera vez en el año 1995 con el nombre de ISO 17799, a lo cual el nombre correcto y original es Norma Britanica BS 7799-1. Posterior mente la Organización Internacional de Normalización (ISO) en conjunto con la Comisión Electrónica Internacional (IEC) en el año 2000 publica el estándar 17799:2000. Tras larga duración y en un periodo después de una ardua revisión y verificación, en el año 2005 se publica una nueva versión de ISO/IEC 17799:2005. Con la aprobación de la norma ISO/IEZAC 27001:2005 y el estándar IGFSO/DIEC 17799:2005 paso a llamarse en Julio de 2007 ISO/IEC 27002:2007.

La investigación se justifica de manera social, porque busca implementar una auditoria de seguridad informática aplicando normas de seguridad, el cual permitió identificar y eliminar las vulnerabilidades que existen, pues se considera que los datos obtenidos en el área de informática son de carácter confidencial, para esto se utilizara las normas de seguridad, ya que el hospital necesita que los datos sean manejados de manera íntegra, disponible y confiable.

El presente trabajo de investigación se justifica científicamente, buscando conocimientos precisos y concretos sistematizados, para tener un mejor sustento sobre la implementación de normas de seguridad de auditoria de seguridad informática para el hospital regional de huacho - 2016, el cual facilito la identificación y eliminación de vulnerabilidades existente en el hospital a fin de poder solucionar las dificultades identificadas. Esta investigación se apoyó utilizando la Norma ISO/IEC 27001, el cual es un estándar de calidad de seguridad de la información, esto permitirá determinar las normas de seguridad que generen confianza en el manejo de datos del área de informática del hospital. Esta Norma es operativamente viable debido a que existen modelos de auditorías ya implementadas que demuestran las mejoras que se ha realizado en otras instituciones o empresa.

Actualmente en la Oficina de informática del Hospital Regional de Huacho, se administra gran cantidad de datos, cuyos datos está manipuladas por el personal de dicha Oficina, se le asigna al personal registrar todos los datos al sistema, dicho personal tiene acceso a todos los datos del Hospital, permitiendo que estas sean totalmente vulnerable y disponible para cualquier persona.

De percibir con esas causas, los datos serían muy accesibles a cualquier eventualidad, ocasionando un mal uso o robo de datos, perjudicando completamente al hospital. Por tal motivo la presente investigación pretende aportar una norma de seguridad clara, permitiendo desarrollar un buen uso adecuado del manejo de datos, aplicando la Norma ISO/IEC 27001. Según lo expuesto en la problemática se cree conveniente realizar el siguiente proyecto de investigación: ¿Cómo implementar una auditoria de seguridad informática para el hospital regional de huacho -2016?

En vista de que el proyecto de investigación de tesis tiene un alcance descriptivo, lo cual no es posible plantear una hipótesis debido a que no intenta correlacionar o explicar una causalidad de variables. Por lo tanto, la Hipótesis es Implícita. Para tal fin se planteó el objetivo general: Implementar Auditoria de Seguridad Informática para el Hospital Regional de Huacho-2016., y como objetivos específicos: es Analizar la situación actual en que se encuentra su seguridad informática del Hospital Regional de Huacho, Identificar las deficiencias y vulnerabilidades de Seguridad Informática para el Hospital Regional de Huacho, Establecer normas de seguridad, bajo la Norma ISO/IEC 27001 de Seguridad Informática para el Hospital Regional de Huacho.

Tabla 1: Conceptualización y Operacionalización de las variables

Variables	Definición Conceptual	Operacionalización de las Variables		Diseño Metodológico
		Indicadores	**Índices / Escala**	
Variable 1: **Auditoria**	Es un proceso que recoge, agrupa y evalúa evidencias cuyo propósito es salvaguardad los datos de una organización, eficazmente y eficientemente durante el proceso de una auditoria en una entidad.	- Recoger los datos del Hospital - Agrupar los datos del Hospital - Evaluar Evidencias - Mantener la integridad. - Salvaguardar los activos. - Uso eficiente de los recursos	- Pésimo - Malo - Regular - Bueno - Muy Bueno	**Tipo y Nivel de Investigación:** Básica y Descriptiva. **Diseño de Investigación:** No Experimental. **Unidad de Análisis:** Hospital Regional de Huacho. **Población:** 10 personales
Variable 2: **Seguridad de la Información**	Está basado en un sistema de control de seguridad, aplicado a los sectores comerciales y entidades grandes y pequeñas, documentado e integrado. Cuyo propósito es identificar las áreas de control necesarias para ser cubiertas y seguras para un eficaz y ordenado control de la información.	- Política de seguridad - Seguridad Organizacional - Clasificación y control de activos - Gestión de operaciones y comunicaciones - Control de acceso - Desarrollo y mantenimiento de sistemas.	- Pésimo - Malo - Regular - Bueno - Muy Bueno	

2. Metodología

El tipo del proyecto de investigación que se realizo es básico y el nivel es de investigación descriptiva, que permitió observar las deficiencias y vulnerabilidades más relevantes en seguridad informática del Hospital Regional de Huacho, 2016.

El diseño del proyecto de investigación es no experimental, de carácter descriptivo y de corte transversal. Es no experimental porque trata de observar las características de los hechos reales, en los cuales no se interviene o manipula deliberadamente los fenómenos de estudios. Es de corte trasversal porque se intenta analizar el fenómeno en un periodo de tiempo determinado en año 2016 en un solo momento.

El método del proyecto de investigación es descriptiva simple, sistemática y empírica. De la demostración de la hipótesis se infirió que del análisis de las variables se dan sin intervención directa del investigador, y dichas relaciones se observan tal como se han dado en el contexto del Hospital.

Este proyecto de investigación tiene un enfoque mixto, porque se observó y midió las variables contenidas en la hipótesis, para formular inferencias y análisis estadísticos. Y se realizó la entrevista a algunos empleados en el lugar de los hechos. Para el presente proyecto de investigación, la población de estudio está conformada por (10) personas que laboran, a la vez procesan información en el Hospital esto se convierte en nuestra muestra, por lo cual no se tuvo necesidad de aplicar la muestra estadística, previa y óptima.

Las técnicas e instrumentos de recolección de datos e información que se emplearan para el presente proyecto son: la encuesta, entrevista y los instrumentos de cuestionario de preguntas y guía de entrevista personal. Lo cual, se elaborarán preguntas abiertas y cerradas que brindarán tener información muy certera y directa en cuanto a los objetivos específicos planteados, para obtener mayor información y eficaz para reforzar el tema del proyecto de investigación.

Se empleará la Normal ISO/IEC 27001 para la implementación de una Auditoria de Seguridad Informática del Hospital Regional de Huacho-2016.

Para el proyecto de investigación se realizará únicamente el análisis de la información, donde el método de recolección de datos será la aplicación o elaboración de encuesta al personal que labora en la Oficina Informática, con el propósito de conocer los requerimientos o deficiencias mínimas que deberán tenerse en cuenta para la implementación de una auditoria de seguridad informática para el Hospital Regional de Huacho.

3. Resultados

Se Analizó la situación real y actual que se encuentra la Seguridad informática en el Hospital Regional de Huacho, para tal fin se aplicó un cuestionario.

Tabla 02

Registro de acceso del Personal no autorizado a sus respectivas áreas

Código	Categoría	Nº de Empleados	Porcentaje %
A	Pésimo	0	0
B	Malo	3	30
C	Regular	4	40
D	Bueno	3	30
E	Muy Bueno	0	0
	Total	10	100

Interpretación: se observa que en la Tabla 01, el 40 % de los empleados señalan como regular el registro de acceso para el personal no autorizado al área de Informática y Estadística, lo que permite apreciar que la falta de seguridad en el tema de accesos puede involucrar a terceros en caso de sabotaje o fraude informático.

Tabla 03

Manejo la seguridad de la información en su respectiva área

Código	Categoría	Nª de Empleados	Porcentaje %
A	**Pésimo**	**0**	**0**
B	**Malo**	**3**	**30**
C	**Regular**	**5**	**50**
D	**Bueno**	**2**	**20**
E	**Muy Bueno**	**0**	**0**
	Total	**10**	**100**

Interpretación: se observa que, en la tabla, que el 50% de los empleados señalan como regular la seguridad de la información en sus respectivas áreas, lo que permite apreciar la falta de capacitación sobre el manejo de información y las medidas preventivas y correctivas, estos factores se pueden dar tanto por desconocimiento del tema como por el nivel de conocimiento del manejo de sus informaciones.

Tabla 04

Permisos de Ingreso a la Red en el área de trabajo

Código	Categoría	Nº Empleados	Porcentaje %
A	Pésimo	0	0
B	Malo	2	20
C	Regular	6	60
D	Bueno	2	20
E	Muy Bueno	0	0
	Total	10	100

Interpretación: En la Tabla 3, el 60% de los empleados señalan como regular la administración de permisos en sus respectivas áreas, los que permite apreciar un mal criterio en la administración de permisos, estos factores pueden poner en riesgo la confidencialidad, integridad y autenticidad de la información del empleado.

Tabla 05
Mecanismos de Protección en el área de trabajo

Código	Categoría	Nº Empleados	Porcentaje %
A	Pésimo	0	0
B	Malo	0	0
C	Regular	8	80
D	Bueno	2	20
E	Muy Bueno	0	0
	Total	10	100

Interpretación: se observa que en la Tabla 04, que el 80% de los empleados señalan como regular el sistema de protección de datos en la información en sus respectivas áreas, lo que permite apreciar que la falta de medios de protección y la capacitación para su manejo no ha sido optima por ende no se asegura el manejo adecuado de la información.

Tabla 06
Opinión de los equipos de Computo

Código	Categoría	Nº Empleados	Porcentaje %
A	Pésimo	0	0
B	Malo	0	0
C	Regular	5	50
D	Bueno	5	50
E	Muy Bueno	0	0
	Total	10	100

Interpretación: se observa que en la Tabla 5, el 50% de los empleados señalan como bueno los equipos de cómputo en sus respectivas áreas, lo que permite apreciar que se tiene una aceptación media en los equipos de cómputo, estos factores nos permiten mitigar molestias sobre los equipos en las distintas áreas.

Tabla 07
Conexiones de red en área de trabajo

Código	Categoría	Nº Empleados	Porcentaje %
A	Pésimo	0	0
B	Malo	3	30
C	Regular	6	60
D	Bueno	1	10
E	Muy Bueno	0	0
	Total	10	100

Interpretación: observamos en la Tabla 06, el 60% de los empleados señalan como regular las conexiones de red, lo que permite apreciar que no se están aplicando estándares de buenas prácticas para el cableado, estos factores generan problemas en la cobertura de la red.

Tabla 08
Mecanismos de Seguridad al ingreso a internet

Código	Categoría	Nº Empleados	Porcentaje %
A	Pésimo	0	0
B	Malo	5	50
C	Regular	4	40
D	Bueno	1	10
E	Muy Bueno	0	0
	Total	10	100

Interpretación: se observa que en la Tabla, el 50 % de los empleados señalan como mala la seguridad en las redes de internet, lo que permite apreciar que la falta de medidas preventivas en el ingreso a internet, estos factores se dan por faltas de políticas para el uso del internet en la que haya restricciones a páginas web que no son confiables y por la instalación de un Firewall que nos sirva de medida preventiva en la interacción del empleado en su ingreso a internet.

Tabla 09
Seguridad del Antivirus en su PC

Código	Categoría	Nº Empleados	Porcentaje %
A	Pésimo	0	0
B	Malo	1	10
C	Regular	5	50
D	Bueno	4	40
E	Muy Bueno	0	0
	Total	10	100

Interpretación: se observa que en la Tabla 08, el 50 % de los empleados señalan como regular la seguridad que brinda el antivirus, lo que denota que se necesitan aplicar otras medidas preventivas para la detección de virus informático, estos factores se pueden dar tanto por desconocimiento del tema, como por una mala configuración del antivirus la cual debe acogerse a los requisitos recomendados del sistema operativo para sacar el mayor provecho del mismo.

Tabla 10
Seguridad de la Oficina en el área de trabajo

Código	Categoría	Nº Empleados	Porcentaje %
A	Pésimo	0	0
B	Malo	2	20
C	Regular	5	50
D	Bueno	3	30
E	Muy Bueno	0	0
	Total	10	100

Interpretación: se observa que, en la Tabla 09, el 50 % de los empleados señalan como regular la seguridad en las oficinas, lo que permite apreciar que no gozan con las medidas optimas de seguridad en ellas, esto denota el ingreso de terceros y por ende se necesita tener equipos de cómputo protegidos en caso se tenga acceso a ellos.

Tabla 11
Reglas de Seguridad de la información en su entidad

Código	Categoría	Nº de Empleados	Porcentaje %
A	Pésimo	0	0
B	Malo	1	10
C	Regular	4	40
D	Bueno	5	50
E	Muy Bueno	0	0
	Total	10	100

Interpretación: se observa que, en la Tabla 10, el 50 % de los empleados señalan como regular las reglas de seguridad en la entidad, lo que permite apreciar que hay reglas de seguridad y el personal tiene conocimiento de ello, esto denota que debe haber un seguimiento a las reglas de seguridad para el cumplimiento de las mismas.

Aplicación de la auditoria y metodología

Planificación de Auditoria

Conocimiento de la Entidad

El Hospital Regional de Huacho está situado a 150 km. Al norte de Lima, cuya fundación fue el 02 de octubre de 1970, siendo un Hospital Centro de Salud con solo las 4 especialidades Básicas.

Su crecimiento en la Institución ha sido a través de un Planeamiento Estratégico, donde fueron transformándolo en un Hospital de Especialidades, donde se hace docencia en salud: Medicina, Enfermería y Nutrición, como sede o convenio de la "Universidad Nacional José Faustino Sánchez Carrión de Huacho", siendo estas actividades las que nos constituyen en un Centro de Creación de Proyectos de Desarrollo Institucional e Investigación en las diferentes áreas de la Salud.

Nuestro Hospital es un Centro Referencial; sus inversiones están ligadas al desarrollo de infraestructura y equipamiento moderno, con gabinetes de alta tecnología, paralelo a los recursos humanos capacitados; de tal forma que gerenciar estos servicios va ligado al buen trato y eficiente de nuestros clientes; pero que en nuestra concepción humanística jamás dejaran de ser nuestro paciente, los cuales pueden demandar una atención especializada.

Dentro de lo que consideramos nuestra visión a largo plazo, están en convertirnos en un Centro de Investigación y Docencia con escuelas de Post-Grado, tanto en lo referente a las Gerencias de Salud como las especialidades de las diferentes disciplinas de la Medicina, perfeccionando la equidad, eficiencia y calidad de nuestro sector.

Visión

Brindar atención de salud especializada e integral en condiciones de plena accesibilidad a la población mediante la prevención de los riesgos, protegiendo del daño, recuperando la salud y rehabilitando sus capacidades, construyendo entornos saludables con énfasis en la salud materna infantil y en la población de mayor pobreza.

Misión

Red de salud y Hospital acreditados, calificados y potenciados para categorizar a un mayor nivel de atención; líderes de modernidad y eficiencia en la atención de salud, reconocidos a nivel local y regional; con adecuada capacidad resolutiva y con recursos humanos capacitados según perfil epidemiológico que cumplen con los lineamientos de salud y garantizan mayor accesibilidad a la población de menores recursos.

Objetivos de la Auditoria

Analizar la situación actual que se encuentra su Seguridad de datos informáticos del Hospital Regional de Huacho.

Identificar las deficiencias y vulnerabilidades de Seguridad Informática para el Hospital Regional de Huacho.

Establecer normas de seguridad, bajo la Norma ISO/IEC 27001 de Seguridad Informática para el Hospital Regional de Huacho.

Alcance

Se auditará al Área de Informática del Hospital Regional de Huacho, el sistema de seguridad informática.

El tiempo para el desarrollo de la auditoria es de 4 meses:

Inicio: agosto 2016

Termino: noviembre 2016

Se recopilará información a través de encuestas al personal del Área de Informática del hospital Regional de Huacho.

Planeación Específica de la Auditoria:

Se realizará las labores de investigación en la entidad pública del Hospital Regional de Huacho.

- Humano:

- Personal Investigador: Bach. Muñoz Fernández, Sandro Arturo

- Materiales y Equipos:

- Laptop Toshiba
- Impresora Epson
- Cartuchos de Tinta
- 01 USB 8 GB
- Papel Bond 1 millar
- Lapiceros Color Azul, Negro
- Resaltadores

- Horas: 90 horas aprox.

Ejecución:

Técnicas de Muestreo:

Se ha considerado al personal del Área de Informática del Hospital Regional de Huacho que suman a 10 personas en total.

Al ser la población un número pequeño la muestra será la misma que la población ósea 10 personas.

Aplicación del ISO/IEC 27001

Sistema de Gestión la Seguridad de la Información (ISO/IEC 27001)

Es una norma internacional lo cual nos permite asegurar su confidencialidad de datos en una entidad u organización. El estándar ISO/IEC 27001:2013 para los Sistemas Gestión de la Seguridad de la Información permite a las entidades tener una evaluación del percance o riesgo lo cual debe contar con un mejor control o manejo necesarios para eliminar y controlar las vulnerabilidades que puedan ocurrir. La organización del ISO-27001 significa una diferenciación respecto al resto, que mejora la competitividad y la imagen de una organización.

ISO/IEC 27001 es un estándar de seguridad de una informacion (Information technology - Security techniques - Information security management systems - Requirements) lo cual fue aprobado y publicado como estándar internacional en octubre de 2005 por International Organization for Standardization y por la comisión International Electrotechnical Commission. Lo cual especifica los propósitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI) según el conocido como "Ciclo de Deming": PDCA - acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar). Es consistente con las mejores prácticas descritas en ISO/IEC 27002, anteriormente conocida como ISO/IEC 17799, con orígenes en la norma BS 7799-2:2002, desarrollada por la entidad de normalización británica, la British Standards Institution (BSI).

Beneficios Que Aporta Este A Los Objetivos De La Organización

- Tiene una garantía independiente cuyo propósito es controlar internamente los requisitos que pueden gestionar en una entidad.
- Su propósito independiente es respetar las base y leyes de cada entidad u organización.
- Su finalidad es cumplir los requisitos estandarizados de seguridad para una mejor calidad de competencia para el bienestar de los clientes.
- De igual forma verifica correctamente, identifica, evalúa y gestiona cada proceso y procedimiento con toda su documentación establecida para la seguridad de la información de datos.
- Demuestra su eficacia al momento de obtener los resultados favorables en la entidad protegiendo sus datos.
- Nos ayuda a mejorar el rendimiento de la información más rápida y segura.

Nota: las organizaciones que simplemente cumplen la norma ISO/IEC 27001 o las recomendaciones de la norma del código profesional, ISO/IEC 27002 no logran estas ventajas.

NTP-ISO/IEC 27001. Documento titulado **"Código de buenas prácticas para la gestión de la seguridad de la información"**. Nos permite tener mejores recomendaciones para poder realizar una mejor gestión de seguridad de datos en una organización, lo cual nos permite guiarnos con los estándares de seguridad dentro de las organizaciones. Cuya Norma del Sistema de Gestión de Seguridad de la Información (SGSI) reconocido internacionalmente. Proporciona un amplio concepto de lo que un SGSI lo cual permite proteger la información de una organización. La Norma también, tiene como definición en una información como un mejor control en una organización; lo cual permite tener un mejor manejo de los datos de cada organización.

Controles:

Los controles que se consideran esenciales para una organización desde un punto de vista legislativo comprenden:

- Protección de información personal.
- La salvaguarda de los registros de la organización.
- Los derechos de la propiedad intelectual.

Los controles que se consideran la mejor práctica habitual para conseguir la seguridad de la información comprenden:

- La documentación de la política de seguridad de la información.
- La asignación de responsabilidades de seguridad.
- La formación y capacitación para la seguridad de la información.
- El registro de las incidencias de seguridad.
- La gestión de la continuidad del negocio.

Estructura: 10 Dominios de Control

Política de Seguridad

Seguridad Organizacional

Clasificación y Control de Activos

Seguridad del Personal

Seguridad Física y Ambiental

Gestión de Operaciones y Comunicaciones

Control de Acceso

Desarrollo y Mantenimiento de Sistemas

Gestión de Continuidad de Negocios

Cumplimiento

Política de Seguridad: es una organización documentada que permite ayudar a proyectar metas en una organización, para un control mejor en seguridad. Cuyo propósito es tener un control eficaz y manejo adecuado en cada organización.

Políticas.

Las Políticas de Seguridad son una declaración de las responsabilidades, conducta y ética aceptada por la organización para proveer un ambiente seguro en el manejo de la información.

Normas.

Conjunto de disposiciones y reglas basadas en las mejores prácticas en seguridad de información usadas para elaborar e implantar políticas.

Seguridad Organizacional: es un control de información en una organización, cuyo propósito es dar acceso a personas autorizadas para dicho manejo, lo cual permite tener un mejor control en la revisión de datos de una entidad.

Clasificación y Control de Activos: Administrar los activos físicos e intelectuales que son importantes para mantener las protecciones apropiadas. Da responsabilidad a las personas con acceso a los datos de cada entidad.

Activos de Información: Archivos y BD, contratos y acuerdos, material de capacitación, documentación, manual de usuarios, planes de continuidad, informes de auditoría, etc.

Activos de Software: aplicativos de sistema, Software del sistema, instrumentos de desarrollo y utilidades, etc.

Activos Físicos: Computadoras, Equipo de comunicaciones, medios magnéticos, medios de comunicación móviles, etc.

Servicios: Servicios de informática y comunicaciones, iluminaciones eléctricas, calefacción, aire acondicionado, y equipos de cómputo.

Personal: Sus calificaciones, habilidades y experiencias.

Intangibles: Reputación e imagen de la organización.

Seguridad del Personal: es una responsabilidad por parte de cada empleado manejar adecuadamente los datos de la entidad, lo cual permite determinar y evaluar cada riesgo que se puede tener. Por tal motivo, que se debe reclutar personal capacitado para majear esta información.

Seguridad Física y Ambiental: asegurar un ambiente adecuado de trabajo dentro de una entidad, para administrar de formar correcta los sistemas de seguridad. De igual forma cada personal relacionado con el área tiene como finalidad enorme determinar el grado de seguridad dentro del área.

Gestión de Operaciones y Comunicaciones: Transmitir claramente las instrucciones de seguridad a los empleados ayuda a administrar las operaciones diarias de los recursos de procesamiento de información.

Control de Acceso: nos permite tener un mejor control de la información de todo el personal, para poder manejar la seguridad en la entidad. También nos permite controlar los niveles de acceso a la red principal de la entidad.

Desarrollo y Mantenimiento de Sistemas: es importante y primordial las actualizaciones de los sistemas para obtener un mejor control de seguridad de información en la entidad.

Gestión de Continuidad de Negocios: Al utilizar los controles de seguridad contra desastres naturales interrupciones operacionales y fallas potenciales de seguridad ayuda a fomentar la continuidad de funciones del negocio.

Cumplimiento: El uso de asesores legales se está volviendo más importante para asegurar la observancia de una organización con las obligaciones contractuales, la ley y requisitos de seguridad.

Auditoria informática con ISO/IEC 27001:

ISO/IEC 27001 es un proceso que permiten auditar los recursos que comprenden la tecnología de información y seguridad.

Permite realizar un proceso de auditoria lo cual lo primero se tiene que evaluar la eficiencia y eficacia del control y seguridad de Área de Informática del Hospital Regional de Huacho, analizando la función que tienen el área dentro de la organización, debemos cumplir con los objetivos trazados, dando las respectivas sugerencias y recomendaciones para mejorar el nivel de apoyo al cumplimiento de los objetivos permitiendo optimizar sus controles y seguridad, la productividad y desempeño dentro del Hospital.

Por lo tanto, de acuerdo con lo establecido en el marco de Referencia ISO/IEC 27001, podemos determinar las siguientes fases:

Fase 1: Análisis y situaciones del área de Informática.

Realizamos un análisis de recopilación de datos de información cuyo propósito es tener una documentación de todo el análisis recopilado para poder verificar el estado del área de informática.

Fase 2: Realización de la Auditoria.

Se realiza la evaluación de los procesos propuestos por ISO/IEC 27001, estableciendo el grado de madurez de los procesos organizacionales del Área de Informática del Hospital Regional de Huacho.

Posteriormente se utilizará una tabla de resumen de objetivos de control propuesto por ISO/IEC 27001, proporcionando una indicación de los procesos, dominio de TI y la manera en que son impactados los criterios de información por los objetivos de alto nivel representados en cada proceso.

Los Criterios están formados por:

La Eficacia: la información es eficaz si satisface las necesidades del consumidor de la información que utiliza la información para una tarea específica. Si el consumidor de la información puede realizar la tarea con dicha información, entonces la información es eficaz.

La Eficiencia: mientras que la eficacia considera la información como un producto, la eficiencia se refiere más al proceso de obtención y uso de la información.

La Fiabilidad: se ve a menudo como un sinónimo de precisión. Sin embargo, también se puede decir que una información es fiable si se considera que es verdadera y creíble.

La Disponibilidad: es una de las metas de la calidad de la información que están bajo los encabezados de accesibilidad y seguridad.

La Confidencialidad: corresponde a la meta de acceso restringido a la información de calidad.

La Conformidad: en el sentido de que esa información debe ajustarse a unas especificaciones está cubierta por cualquiera de las metas de calidad de la información, dependiendo de los requisitos.

La manera como les afecta a cada uno de los procesos está identificada por:

El grado de Impacto Primario (P), es el grado cuyo objetivo principal es impactar un control detallado y definido para la información de interés de la entidad.

El grado de Impacto Secundario (S), es el grado cuyo objetivo es controlar satisfactoriamente de forma indirecta la información de la entidad.

Espacio Blanco (Vacío), es decir que el principal objetivo no impacta sobre la información de la entidad.

Tabla 12

Cuadro de objetivos de control ISO/IEC 27001

Procesos	Criterio de Información					
	Efectividad	Eficiencia	Fiabilidad	Disponibilidad	Confidencialidad	Conformidad
Política de Seguridad	**P**	**S**	**P**	**S**		
Seguridad Organizacional	**S**	**P**	**P**	**S**		
Clasificación y Control de Activos	**P**	**S**	**P**	**S**		
Seguridad del Personal	**P**	**P**	**S**	**S**		
Seguridad Física y Ambiental	**S**	**S**	**P**	**P**		
Gestión de Operaciones y Comunicaciones	**P**		**S**		**P**	
Control de Acceso	**S**	**p**	**S**	**P**	**S**	
Desarrollo y Mantenimiento de Sistemas	**P**		**P**		**P**	
Gestión de Continuidad de Negocios	**S**		**S**		**S**	
Cumplimiento	**P**	**S**		**S**		**P**

Tabla 13
Madurez de los Procesos

Procesos	Modelos de madurez				
	Pésimo	Malo	Regular	Bueno	Muy Bueno
Política de Seguridad			X		
Seguridad Organizacional			X		
Clasificación y Control de Activos			X		
Seguridad del Personal			X		
Seguridad Física y Ambiental			X		
Gestión de Operaciones y Comunicaciones			X		
Control de Acceso			X		
Desarrollo y Mantenimiento de Sistemas			X		
Gestión de Continuidad de Negocios			X		
Cumplimiento			X		

Recomendaciones:

Contiene información que los modelos de madurez en los procesos se califican de manera regular por cada personal de Área TI del Hospital.

Fase 3: Informe Preliminar:

Esta información se basa de acuerdo a una ejecución de la auditoria, alcanzando de manera precisa los objetivos propuesto para la realización de la misma. También se aplica una metodología de ISO/IEC 270001, lo cual tiene procesos de grados de madurez en cada metodología, teniendo como proceso una conclusión y recomendación.

Fase 4: Informes Finales:

En conclusión el informe detallado una vez revisado y verificado se convierte en un informe técnico final, el cual se basado de acuerdo a las capacitaciones del personal del Área TI .

Análisis y discusión

Canales (2007), el estudio, tuvo como objetivo la identificación de puntos débiles en el funcionamiento y administración. Es decir, no se cuenta con un documento oficial por parte de la entidad en la que se estipule la organización, funciones y responsabilidades de los funcionarios de esta área, lo cual en un proceso de auditoría los eximiría de responsabilidades.

Mientras en el presente informe tampoco contamos con documentos oficial por parte de la entidad donde estipule toda la organización, funciones y responsabilidades de cómo funciona el área de Informática, por lo tanto, tuvimos que ser un análisis para ver las carencias y debilidades que podíamos encontrar en el área de informática, cuya finalidad encontramos con vulnerabilidades existen en toda el área. Lo que no permitió implementar normas de Seguridad informática para el funcionamiento adecuado de los equipos de cómputos.

Ramos y Ysela (2006) cuyo propósito es implementar un plan de seguridad informática que permita proteger los datos e información de tecnología y evaluar las necesidades de seguridad informática en la relación con la estructura del área de informática, Por lo cual su finalidad es la aplicación de las medidas correctivas para los distintos activos de información que reducen considerablemente las vulnerabilidades con las que se contaba, pero es necesario su mantenimiento y actualización, así como a un estudio periódico sobre nuevos activos que se adquieran en el futuro como las nuevas amenazas que puedan sugerir las medidas que se deben adoptar.

El presente informe nos permitió implementar un plan de seguridad de información para proteger los datos tecnológicos, y evaluar necesidades de seguridad informática, cuya finalidad fue reducir las considerables vulnerabilidades que se contaba.

Torres y Shirley (2006) cuyo objetivo es comprobar la existencia de procedimientos y de su correcto funcionamiento, según las normas de seguridad vigentes para el resguardo de la información. Dicha entidad se encuentra propensa a sufrir ciertos ataques ya sean naturales o de otra índole, por no contar con mecanismos y medios formales como planes de contingencia, plan de continuidad de negocios, políticas de seguridad, entre otros; que permitan contrarrestar estos ataques.

En el informe pudimos encontrar un mal funcionamiento de normas de seguridad, dicha entidad esta prospera a sufrir ciertos ataques ya sean naturales o de otra índole, por n contar con software originales, que permitan contrarrestar los ataques.

María Hernández (2006)**,** cuyo objetivo es ayudar a la entidad y al personal a tomar las precauciones permanentes para tener un control seguro de la información, lo cual permitiría a la organización tener un mejor funcionamiento para lograr sus metas y objetivos propuestos.

Con respecto a mi informe, conocimos la importancia, el valor y la razón de las deficiencias y vulnerabilidades que se encontraron en la información, lo cual dio a conocer por qué es tan importante tener la información segura. De igual forma, se dio a conocer a todo el personal humano como están expuesto a los riesgos que se encontraron en la entidad, detallando la forma que ellos colaboran al momento de tener la información vulnerable.

CONCLUSIÓNES

- Se detectó que el Hospital no cuenta con medidas implementadas a nivel de Software y Hardware para garantizar su buen funcionamiento y la disponibilidad de los sistemas alojados en cada equipo, por lo cual como recomendación a corto plazo se deberá establecer un programa de mantenimiento preventivo y correctivo.

- Se logró identificar las deficiencia y vulnerabilidades que causaban algún impacto en los procesos de TI, estás deberán ser solucionadas por el Área de Informática para su mejor funcionamiento.

- La auditoría permitió detallar el estado actual de Área de TI del Hospital Regional de Huacho, por lo cual podemos concluir en nuestro informe que en su mayoría no existen Normas bien establecidas de Seguridad Informática, por lo que deberán tomarse medidas correctivas inmediatas en los puntos indicados.

RECOMENDACIONES

- Se recomienda implementar medidas adecuada de software y hardware para el buen funcionamiento de los sistemas alojados en cada equipo, teniendo buenos programas de mantenimiento preventivo y correctivo.

- Se recomienda que el personal solicite el asesoramiento o capacitación para un mejor control y un adecuado manejo de los equipos computo.

- Se recomienda aplicar las Normas de Seguridad Informática adecuadas para el Área de TI del Hospital Regional de Huacho, lo cual debe contener un cronograma de las actividades a desarrollar durante el periodo establecido.

AGRADECIMIENTO

Agradecemos a la Universidad San Pedro – Sede Huacho, por habernos abierto las puertas de este prestigioso templo de saber el cual es grande por la capacidad de los docentes que tiene en sus filas y que están al servicio de la comunidad estudiantil.

A los Ingenieros encargados de brindar la asesoría y en especial a nuestro asesor de tesis Ing. Lara Carreño, lo cual nos permitieron compartir con nosotros sus valiosos conocimientos precisos y concreto lo cual nos brindaron su mayor confianza con la mayor paciencia posible.

A las personas más importante en nuestras vidas, nuestros padres que nos brindaron todo su apoyo, sus consejos, apostando por un mejor futuro nuestro lo cual nos sirvieron mucho en los momentos difíciles y en especial a mi esposa y a mi pequeño hijo que me da las fuerzas para enfrentarme a nuevos retos, es para ustedes que les dedico esta tesis, gracias.

REFERENCIAS BIBLIOGRÁFICAS

Alcántara Flores, J. C. (2015). *Guía de Implementación de la Seguridad Basado en la Norma ISO/IEC 27001, Para Apoyar la Seguridad en los Sistemas Informáticos de la Comisaría del Norte P.N.P. en la Ciudad de Chiclayo.* Chiclayo - Perú: Recuperado de http://tesis.usat.edu.pe/jspui/bitstream/123456789/491/1/TL_Alcantara_Flores_JulioCesar.pdf.

Alexander Lopez, J., & Zuluaga Tamayo, A. F. (2013). *Desarrollo de una Metodología para el Control de Riesgos para Auditoria de Base de Datos.* Pereira - Colombia: Recuperado de http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/4153/0058L864.pdf?sequence=1.

Almeida Paredes, R. C. (2014). *Procedimientos de Auditoría para la Seguridad en la Base de Datos.* Quito - Ecuador: Recuperado de http://www.dspace.uce.edu.ec/bitstream/25000/2232/1/T-UCE-0011-79.pdf.

Auditoria Informatica s,f. (s.f.). Recuperado el 18 de Noviembre de 2016, de http://members.tripod.com/~Guillermo_Cuellar_M/informatica.html

Aula uvs . (s.f.). Recuperado el 25 de Noviembre de 2016, de Aula uvs : Recuperado de http://www.aulauvs.sld.cu

Barahona Guallichico , J., & Garzón Chavez, E. (2014). *Auditoría de los Riesgos Informáticos en el Departamento de Tecnología de la Empresa KUBIEC Usando COBIT 4.1 y la Norma ISO/IEC 27001 como Marco de Referencia.* Quito - Ecuador: Recuperado de http://biblioteca.epn.edu.ec/cgi-bin/koha/opacdetail.pl?biblionumber=26021&shelfbrowse_itemnumber=35896.

Barahona Guallichico , J., & Garzón Chavez, E. (2014). *Auditoría de los Riesgos Informáticos en el Departamento de Tecnología de la Empresa KUBIEC Usando COBIT 4.1 y la Norma ISO/IEC 27001 como Marco de Referencia.* Quito - Ecuador: http://biblioteca.epn.edu.ec/cgi-bin/koha/opacdetail.pl?biblionumber=26021&shelfbrowse_itemnumber=35896.

Barahona Guallichico , J., & Garzón Chavez, E. (2014). *Auditoría de los Riesgos Informáticos en el Departamento de Tecnología de la Empresa KUBIEC Usando COBIT 4.1 y la Norma ISO/IEC 27001 como Marco de Referencia.* QUITO: Recuperado de http://biblioteca.epn.edu.ec/cgi-bin/koha/opacdetail.pl?biblionumber=26021&shelfbrowse_itemnumber=35896.

Barahona Guallichico, J. C., & Garzón Chavez, E. V. (2014). *Auditoría de los Riesgos Informáticos en el Departamento de Tecnología de la Empresa KUBIEC Usando COBIT 4.1 y la Norma ISO/IEC 27001 como Marco de Referencia.* Quito - Ecuador: Recuperado de http://biblioteca.epn.edu.ec/cgi-bin/koha/opacdetail.pl?biblionumber=26021&shelfbrowse_itemnumber.

Bermúdez Molina, K. G., & Bailón Sánchez, E. R. (2015). *Análisis en Seguridad Informática y Seguridad de la Información Basado en la Norma ISO/IEC 27001 – Sistemas de Gestión de Seguridad de la Información Dirigido a una Empresa de Servicios Financieros.* Guayaquil - Ecuador: Recuperado de http://dspace.ups.edu.ec/bitstream/123456789/10372/1/UPS-GT001514.pdf.

Blog Auditoria. (2012). Obtenido de http://auditoria.over-blog.com/article-auditoria-68941282.html

Cano. (2011). Obtenido de http://www.seguridadparatodos.es/2011/10/seguridad-informatica-o-seguridad-de-la.html

Coronel Castro, K. M. (2012). *Auditoría Informática Orientada a los Procesos Críticos de Crédito Generados en la Cooperativa de Ahorro y Crédito "Fortuna" Aplicando el Marco de Trabajo COBIT.* Loja - Ecuador.

Definición de Política . (s.f.). Recuperado el 25 de Noviembre de 2016, de Definición de Política : http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/PoliticasSeguridad.php

Fierro Montenegro, O. L., & García Pinchao, J. (2009). *SABDO: Sistema de Auditoria para Base de Datos Oracle.* Ibarra - Ecuador: Recuperado de http://repositorio.utn.edu.ec/bitstream/123456789/984/1/04-ISC-116.pdf.

Gaona Vásquez, K. (2013). *Aplicación de la Metodología MAGERIT para el Análisis y Gestión de Riesgos de la Seguridad de la Información aplicado a la Empresa Pesquera e Industrial Bravito S.A. en la Ciudad de Machala.* Cuenca - Ecuador: http://dspace.ups.edu.ec/bitstream/123456789/5272/1/UPS-CT002759.pdf.

Gaona Vásquez, K. d. (2013). Cuenca - Ecuador.

Gaona Vásquez, K. d. (2013). *Aplicación de la Metodología MAGERIT para el Análisis y Gestión de Riesgos de la Seguridad de la Información aplicado a la Empresa Pesquera e Industrial Bravito S.A. en la Ciudad de Machala.* Cuenca - Ecuador: Recuperado de http://dspace.ups.edu.ec/bitstream/123456789/5272/1/UPS-CT002759.pdf.

Gaona Vásquez, K. d. (2013). *Aplicación de la Metodología MAGERIT para el Análisis y Gestión de Riesgos de la Seguridad de la Información aplicado a la Empresa Pesquera e Industrial Bravito S.A. en la Ciudad de Machala.* Cuenca - Ecuador: Recuperado de http://dspace.ups.edu.ec/bitstream/123456789/5272/1/UPS-CT002759.pdf.

Gomez Ramirez, V. (2014). *Evalaución de la Seguridad de la Información con la Metodologí Octave.* Institución Univeristaria Pascual Bravo.

Huesca Aguilar, G. (2012). *Auditoria Informatica.* California.

ISO 27001 SGSI s,f. (s.f.). Recuperado el 25 de Noviembre de 2016, de ISO 27001 SGSI s,f: Recuperado de: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001

Lucero Gomez, A. (2012). *Análisis y gestión de riesgos utilizando la metodología Magerit.* Universidad de Cuenca.

Marco teorico s,f. (s.f.). Recuperado el 25 de Noviembre de 2016, de Marco teorico s,f: Recuperado de http://problema.blogcindario.com/2008/10/00014-marco-teorico.html

Monografías. (s.f.). Recuperado el 25 de Noviembre de 2016, de Monografías : Recuperado de www.monografias.com/seguridadinformatica

Monografías s,f. (s.f.). Recuperado el 18 de Noviembre de 2016, de Monografías.com: http://www.monografias.com/trabajos22/auditoria-informatica/auditoria-informatica.shtml

Moreno. (2012). Obtenido de http://es.slideshare.net/j_morenoauditoria- informatica -y-de-sistemas-de-informacion

Politica de Seguridad Informática . (s.f.). Recuperado el 25 de Noviembre de 2016, de Politica de Seguridad Informática : http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/PoliticasSeguridad.php

Politicas de Seguridad . (s.f.). Recuperado el 25 de Noviembre de 2016, de Politicas de Seguridad : http://redyseguridad.fi-p.unam.mx/proyectos/tsi/capi/Cap4.html

Seguridad Informática . (s.f.). Recuperado el 25 de Noviembre de 2016, de Seguridad Informática : Recuperado de www.wikipedia.com/seguridadinformatica

Wikipedia . (s.f.). Recuperado el 25 de Noviembre de 2016, de Wikipedia : https://es.wikipedia.org/wiki/Pol%C3%ADtica_de_seguridad

Wikipedia s,f. (s.f.). Recuperado el 18 de Noviembre de 2016, de Wikipedia: https://es.wikipedia.org/wiki/Auditor%C3%ADa_inform%C3%A1tica

Wikipedia s,f. (s.f.). Recuperado el 25 de Noviembre de 2016, de Wikipedia s,f: Recuperado de https://es.wikipedia.org/wiki/ISO/IEC_27001

Wikipedia s,f. (s.f.). Recuperado el 25 de Noviembre de 2016, de Wikipedia s,f: Recuperado de https://es.wikipedia.org/wiki/ISO/IEC_27001

Yan Carranza, F., & Zavala Vasquez, C. (2013). *Plan de Mejora de la Seguridad de Información y Continuidad del Centro de Datos de la Gerencia Regional de Educación La Libertad Aplicando Lineamientos ISO 27001 y Buenas Prácticas COBIT*. Trujillo - Perú: Recuperado de http://repositorio.upao.edu.pe/bitstream/upaorep/645/1/YAN_FREDDY_MEJORA_SEGURIDAD_COBIT.pdf.

Lázaro, M (2008). Seguridad de la Información. Oficina Nacional de Gobierno Electrónico e Informática PCM. Perú.

Muñoz, C. (2010). Auditoria en Sistemas Computacionales. Mexico.

Piattini, M. (2001). Auditoria Informatica. Un enfoque Practico. Ra-Ma.

ANEXO 1
MATRIZ DE CONSISTENCIA

TEMA: AUDITORIA DE SEGURIDAD INFORMATICA PARA EL HOSPITAL REGIONAL DE HUACHO-2016.

PROBLEMA	HIPÓTESIS	OBJETIVOS	VARIABLES
¿CÓMO IMPLEMENTAR UNA AUDITORIA DE SEGURIDAD INFORMATICA PARA EL HOSPITAL REGIONAL DE HUACHO -2016?	En vista de que el proyecto de investigación tiene un alcance descriptivo, no es posible plantear una hipótesis debido a que no intenta correlacionar o explicar causalidad de variables. Por lo tanto, la Hipótesis es Implícita.	**OBJETIVO GENERAL:** Implementar auditoria de Seguridad Informática para el Hospital Regional de Huacho-2016. **Objetivos específicos:** 1. Analizar la situación actual en que se encuentra la Seguridad Informática para el Hospital Regional de Huacho. 2. Identificar las deficiencias y vulnerabilidades de Seguridad Informática para el Hospital Regional de Huacho. 3. Establecer normas de seguridad bajo la Norma ISO/IEC 27001 de Seguridad Informática para el Hospital Regional de Huacho.	- AUDITORIA - SEGURIDAD DE LA INFORMACION

ANEXOS 2

DESCRIPCION DE LA EMPRESA

El hospital Regional de Huacho está situado a 150 km. Al norte de Lima, fue fundado el 02 de octubre de 1970 siendo un Hospital Centro de Salud con solo las 4 especialidades Básicas.

El crecimiento de nuestro Institución ha sido a través de un Planeamiento Estratégico de ir transformándonos en un Hospital de Especialidades, donde se hace docencia en salud: Medicina, Enfermería y Nutrición, como sede de la "Universidad Nacional José Faustino Sánchez Carrión de Huacho", siendo estas actividades las que nos constituyen en un Centro de Creación de Proyectos de Desarrollo Institucional e Investigación en las diferentes áreas de la Salud.

Nuestro Hospital es un Centro Referencial; sus inversiones están ligadas al desarrollo de infraestructura y equipamiento moderno, con gabinetes de alta tecnología, paralelo a los recursos humanos capacitados; de tal forma que gerenciar estos servicios va ligado al buen trato y eficiente de nuestros clientes; pero que en nuestra concepción humanística jamás dejaran de ser nuestro paciente, los cuales pueden demandar una atención especializada.

Dentro de lo que consideramos nuestra visión a largo plazo, están en convertirnos en un Centro de Investigación y Docencia con escuelas de Post-Grado, tanto en lo referente a las Gerencias de Salud como las especialidades de las diferentes disciplinas de la Medicina, perfeccionando la equidad, eficiencia y calidad de nuestro sector.

HISTORIA

El Hospital Regional de Huacho fue fundado el 02 de octubre de 1970, y creado como Centro Base, se convirtió en Hospital de Apoyo y luego a partir de 1990 es considerado Hospital Regional. Su estructura horizontal, cuenta con 04 pisos, la primera planta está diseñada para las Unidades Administrativas, en el segundo piso se encuentran los Departamentos de Pediatría y Medicina, en el tercero la Sala de Partos y Neonatología con sus servicios de Cuidados Intensivos, el cuarto el Departamentos de Cirugía y las Salas de Operaciones en número de tres, así mismo la Unidad de Hemodiálisis.

El Hospital Regional de Huacho es el Centro Referencial de los Servicios Básicos Huaura – Oyón cuenta con 45 Puestos y 09 Centros de Salud. En la Provincia de Huaura los Centro de Salud de Hualmay, Végueta, Carquín, Santa María y Huaura, en la Costa y en la Sierra el Centro de Salud de Ambar y Centro de Salud de Sayán. En las Provincia de Oyón los centros de salud de Churín y Oyón.

Micro red Hualmay
Micro red Huaura
Micro red Vegueta
Micro red Sayán
Micro red Churín - Oyón

VISION:
Brindar atención de salud especializada e integral en condiciones de plena accesibilidad a la población mediante la prevención de los riesgos, protegiendo del daño, recuperando la salud y rehabilitando sus capacidades, construyendo entornos saludables con énfasis en la salud materna infantil y en la población de mayor pobreza.

MISION:
Red de salud y Hospital acreditados, calificados y potenciados para categorizar a un mayor nivel de atención; líderes de modernidad y eficiencia en la atención de salud, reconocidos a nivel local y regional; con adecuada capacidad resolutiva y con recursos humanos capacitados según perfil epidemiológico que cumplen con los lineamientos de salud y garantizan mayor accesibilidad a la población de menores recursos.

VALORES INSTITUCIONALES:
HONESTIDAD:
Referido al cumplimiento de la función pública observando una intachable, anteponiendo el interés general sobre el particular y velando por la integridad ética, moral y profesional en la administración de los recursos institucionales asignados. Rectitud y transparencia en el trabajo.

RESPONSABILIDAD:
Referido al cumplimiento oportuno, eficiente y eficaz de las tareas inherentes a las funciones asignadas dentro de la institución. Actitud de la persona de asumir y cumplir con la labor asignada.

RESPETO:
Consistente en la capacidad de reconocer las diferencias entre las personas, apreciar y valorar las cualidades, las opiniones y el tiempo del personal de salud con equidad y sin temor, teniendo en cuenta sus valores, virtudes y metas logrando así el fortalecimiento de las relaciones interpersonales.

ANEXO 3

ENCUESTA

Dirigido al: Personal Hospital Regional de Huacho

Reciba un cordial saludo. La presente encuesta tiene por finalidad conocer su opinión acerca de la Seguridad informática en sus respectivas áreas. Por favor responda con la mayor sinceridad posible, se agradece.

Instrucciones:

Marque con un aspa la respuesta que le parezca la indicada.

PREGUNTAS	PESIMO	MALO	REGULAR	BUENO	MUY BUENO
1. ¿QUE LE PARECE EL REGISTRO DE ACCESO DE PERSONAL NO AUTORIZADO A SUS RESPECTIVAS AREAS?					
2. ¿COMO SE MANEJA LA SEGURIDAD DE LA INFORMACIÓN EN TU ÁREA?					
3. ¿QUE OPINION TIENES SOBRE LOS PERMISOS DE INGRESO A LA RED EN TU AREA?					
4. ¿QUE TE PARECEN LOS MECANISMOS DE PROTECCION DE TU INFORMACIÓN EN TU AREA?					
5. ¿QUE OPINION TIENE SOBRE LOS EQUIPOS DE CÓMPUTO?					
6. ¿QUE OPINION TIENE SOBRE LAS CONEXIONES DE RED?					
7. ¿QUE LE PARECE LOS MECANISMOS DE SEGURIDAD A LOS INGRESOS A INTERNET?					
8. ¿QUE LE PARECE LA SEGURIDAD QUE LE BRINDA EL ANTIVIRUS DE SU PC?					
9. ¿QUE LE PARECE LA SEGURIDAD QUE LE BRINDA LA OFICINA DE SU AREA?					
10. ¿QUE OPINION TIENE SOBRE REGLAS DE SEGURIDAD DE LA INFORMACION EN SU ENTIDAD?					

Agradecemos su colaboración y atención prestada a la presente encuesta.

ANEXO 4 – EVIDENCIA EN IMAGENES

Jefe del área de Informática

Cableado sin canaletas

Cableado sin canaletas – riesgo para el personal

Falta de Espacio