UNIVERSIDAD NACIONAL JOSÉ FAUSTINO SÁNCHEZ CARRIÓN

FACULTAD DE INGENIERÍA INDUSTRIAL, SISTEMAS E INFORMÁTICA

ESCUELA PROFESIONAL DE INGENIERIA INFORMATICA

AUDITORIA EN SEGURIDAD INFORMÁTICA Y EL ALINEAMIENTO CON LAS POLÍTICAS DE SEGURIDAD DEL HOSPITAL SAN JUAN BAUTISTA - HUARAL

TESIS

PARA OPTAR POR EL TÍTULO PROFESIONAL DE:

INGENIERO INFORMATICO

PRESENTADO POR EL BACHILER:

DONAYRE UCHUYA, Edson Andre

Asesor:

Mg. Ing. Edwin Iván Farro Pacifico

CIP: 91782

HUACHO - PERÚ

2017

MIEMBROS DEL JURADO Y ASESOR

……
PRESIDENTE
Dr. Angel Huamán Tena
CIP: 41456

……
SECRETARIO
Mg. Máximo Dario Palomino Tiznado
CIP: 26572

…….
VOCAL
Mg. Juan Carlos Meyhuay Fidel
CIP: 78338

…….
ASESOR
Mg. Edwin Iván Farro Pacifico
CIP: 91782

DEDICATORIA

A Dios por darnos sabiduría y permitirnos llegar
a este nivel intelectual.
A nuestros padres por ser guías en el sendero de cada acto que
realizamos hoy, mañana y siempre.

El Autor

INDICE GENERAL

Índice de tablas

Índice de figuras

AUDITORIA EN SEGURIDAD INFORMÁTICA Y EL ALINEAMIENTO CON LAS POLÍTICAS DE SEGURIDAD DEL HOSPITAL SAN JUAN BAUTISTA - HUARAL

AUDIT IN COMPUTER SECURITY AND ALIGNMENT WITH SAFETY POLICIES OF SAN JUAN BAUTISTA HOSPITAL - HUARAL

***DONAYRE UCHUYA, Edson Andre*[1]**

RESUMEN

Objetivo: Diseñar un modelo de auditoria en seguridad informática que permita un alineamiento con las políticas de seguridad del hospital San Juan Bautista Huaral **Métodos:** La población compuesta por funcionarios, médicos y asistentes y la muestra es 92 personas. Se utilizó el instrumento de medición de actitudes de escala de Likert. La confiabilidad del instrumento fue validada mediante el coeficiente alfa de Cronbach (0.87 y 0,88). **Resultados:** Los resultados muestran que más del 60% de encuestados están de acuerdo con la Implementación de Auditoria en Seguridad Informática y el Alineamiento con las Políticas de Seguridad del Hospital San Juan Bautista – Huaral.

Conclusión: Existe una correlación positiva significativa moderada entre Auditoria en seguridad informática y política de seguridad (Rho = 0.61; p = 0.00 < 0.05).

Palabras claves: Auditoria en seguridad informática, política de seguridad y alineamiento.

ABSTRACT

Objective: Design a computer security audit model that allows an alignment with the security policies of the hospital San Juan Bautista Huaral Methods: The population composed of officials, doctors and assistants and the sample is 92 people. The Likert scale attitude measurement instrument was used. The reliability of the instrument was validated by Cronbach's alpha coefficient (0.87 and 0.88). Results: The results show that more than 60% of respondents agree with the Implementation of Computer Security Audit and the Alignment with the Security Policies of the Hospital San Juan Bautista - Huaral. Conclusion: There is a moderate significant positive correlation between Computer security audit and security policy (Rho = 0.61, p = 0.00 <0.05).

Keywords: Audit in computer security, security policy and alignment.

[1]Escuela Profesional de Ingeniería Informática. Facultad de Ingeniería Industrial, Sistemas e Informática Universidad Nacional José Faustino Sánchez Carrión. Huacho – Perú.

INTRODUCCIÓN

La información es el principal activo de toda organización según los más modernos paradigmas de la gestión y toma de decisiones, pudiendo hacer su aparición de muchas formas: impresa o escrita en papel, almacenada electrónicamente, transmitida por correo.

En el hospital San Juan de Huaral, se tiene claro que información está constantemente bajo la amenaza de muchas fuentes, que pueden ser internas, externas, accidentales o maliciosas para con la organización.

Para esto se requiere establecer un modelo de auditoria informática que se adecue con las políticas de seguridad de la organización, asegurando la confidencialidad, integridad, disponibilidad y adaptación de la información.

El estudio comprende, en el capítulo I, se desarrolla el marco de la realidad problemática formulada sobre las bases de revisiones bibliográficas, los objetivos y la justificación de la investigación.

En el capítulo II, denominado marco teórico, se detalla sobre la institución en estudio y se mencionan estudios nacionales y extranjeros que fueron tomados en cuenta; así mismo se exponen las bases teórico científicas de las variables enfocadas.

En el capítulo III, denominado marco metodológico, se precisan los elementos principales del protocolo de investigación como: hipótesis, variables, tipo de investigación, diseño, método de estudio, población y muestra, técnicas de acopio de datos y método de análisis de datos.

En el capítulo IV, se presenta el diseño de auditoria informática el cual presenta el desarrollo de la misma.

En el capítulo V, se muestran los resultados estadísticos, los análisis e interpretación de los Resultados de la encuesta.

En el capítulo VI, contiene la discusión, conclusiones y recomendaciones a las que se ha llegado en la investigación.

En el capítulo VII, se muestran las fuentes de información, las cuales fueron consideradas para este trabajo de investigación.

CAPÍTULO I

PLANTEAMIENTO DEL PROBLEMA

1.1. Descripción de la realidad problemática

Con el transcurrir de los años, se puede evidenciar que gran parte de las organizaciones, sin considerar el tamaño, acumulan gran cantidad de datos de los servicios que brinda, del personal que labora dentro, de sus estados financieros, entre otros. Esto hace que cada vez el volumen de los datos sea más grande, para que luego pase a ser recolectado, procesado, almacenado y puesto a la disposición del personal interesado, como información visible y disponible a través de la tecnología de la informática.

Es alarmante, como entidades pueden perder información relevante que pueden conllevar a tomar decisiones estratégicas equivocadas, permitir que información confidencial se vuelva pública. Es por esto, que, desde el punto de vista de la investigación, proteger la Información confidencial es un requisito muy importante.

La unidad de estadística e informática del hospital San Juan Bautista Huaral, tiene el control de los flujos de la información de toda la institución; bajo una directiva en políticas de seguridad sobre administración de red, debido a que cuenta con escaso personal en informática y solo se encargan de administrar la seguridad de la red dejando de lado otros aspectos que incluyen la seguridad informática que implica salvaguardar la información importante del hospital, es por ello que cada día se ven en la necesidad de seguir alineándose a las políticas de seguridad, por ello la importancia de auditar la entidad y poder monitorear como se están cumpliendo las políticas de seguridad

informática y encontrar los puntos donde hace falta implementarlas. Ya que un ataque simple o un descuido puede originar daños considerables a una entidad como en este caso el hospital San Juan Bautista Huaral si no contaran con controles que mitiguen la probabilidad que estos sucesos ocurran.

1.2. Formulación del Problema

1.2.1. Problema General

¿Cómo el diseño de un modelo de auditoría informática permitirá el alineamiento con las políticas de seguridad del hospital San Juan Bautista Huaral?

1.2.2. Problemas Específicos

- ¿En qué medida el modelo de auditoria en seguridad física permitirá alinear las políticas de seguridad del hospital San Juan Bautista Huaral?
- ¿De qué manera un modelo de seguridad lógica, permitirá el alineamiento de las políticas de seguridad en el hospital San Juan Bautista Huaral?
- ¿De qué forma la adaptabilidad del modelo de auditoría informática, permitirá el alineamiento de las políticas de seguridad en el hospital San Juan Bautista Huaral?

1.3. Objetivo de la investigación

1.3.1 Objetivo General

Diseñar un modelo de auditoria en seguridad informática que permita un alineamiento con las políticas de seguridad del hospital San Juan Bautista Huaral.

1.3.2. Objetivos Específicos

- Determinar la medida con la cual el modelo de auditoria en seguridad física permitirá alinear las políticas de seguridad del hospital San Juan Bautista Huaral.
- Analizar la manera en que el modelo de auditoria en seguridad lógica permitirá alinear las políticas de seguridad del hospital San Juan Bautista Huaral.
- Establecer la forma con la cual la adaptabilidad del modelo de auditoria de seguridad informática permitirá alinear las políticas de seguridad del hospital San Juan Bautista Huaral.

1.4. Justificación de la Investigación

En actualidad no se presta tanta importancia a la seguridad informática en las entidades, instituciones o empresas; la presente investigación se justifica en la necesidad que tienen estas organizaciones sean grandes o pequeñas de asegurar su información frente al uso masivo de tecnología, paralelamente aumentan los ataques de hackers, empleados que pueden perder valiosa información, todo esto conllevaría a una económica, que podría interrumpir la continuidad del negocio.

CAPÍTULO II

MARCO TEORICO

2.1. Antecedentes de la Investigación

A. Internacionales

Álvarez B. (2005) Realizó una tesis titulada "*Seguridad en Informática (Auditoria de Sistemas)*" Para obtener el grado de Maestro en Ingeniería de Sistemas Empresariales, Universidad Iberoamericana.

Objetivo General:

Desarrollar un modelo de gestión para la auditoria de redes inalámbricas de área local con la finalidad de verificar la vulnerabilidad y riesgos en las redes inalámbricas.

Metodología:

La metodología utilizada está en base fue COBIT para analizar todos los procesos de TI.

Conclusión:

Las organizaciones modernas que operan o centran gran parte de su actividad en el negocio a través de Internet necesitan dotar sus sistemas e infraestructuras informáticas de las políticas y medidas de protección más adecuadas que garanticen el continuo desarrollo y sostenibilidad de sus actividades; en este sentido, cobra especial importancia el hecho de que puedan contar con profesionales especializados en las nuevas tecnologías de seguridad que implementen y gestionen de manera eficaz sus sistemas.

Como consecuencia, la información en todas sus formas y estados se ha convertido en un activo de altísimo valor, el cual se debe proteger y asegurar para garantizar su integridad, confidencialidad y disponibilidad, entre otros servicios de seguridad.

Martínez V. (2010) Realizó una tesis titulada "*Concientización En Seguridad De La Información, La Estrategia Para Fortalecer El Eslabón Más Débil De La Cadena*" Para optar por el título de Especialista en Dirección Estratégica de Empresas, Fundación Universitaria Iberoamericana.

Objetivo General:

Elaborar un programa de concienciación en Seguridad de la Información que pueda ser usado por las empresas, para garantizar un tratamiento seguro de la Información sensible y confidencial de la compañía, evitando se vuelva pública de una manera no autorizada.

Metodología:

Esta investigación se realizó considerando la norma ISO 27001:2005 que es un estándar para evaluar los niveles seguridad de información y COBIT 4.1 para la evaluación de riesgo.

Conclusión:

La información es uno de los activos más importantes para la compañía, por lo tanto, se le debe dar un tratamiento seguro haciendo que la información se convierta en el eje central sobre el cual gira la seguridad, definiendo acciones de protección y mecanismos de control para garantizar al negocio, la confiabilidad de dicha información.

Reyes M. (2011) Realizó una tesis titulada "*Propuestas para impulsar la seguridad informática en materia de educación*" Para optar por el título de Ingeniero en Computación, Universidad Nacional Autónoma de México.

Objetivo General:

Realizar una investigación que permita estudiar, analizar y determinar la situación actual de la seguridad informática en México y su contraste a nivel internacional.

Metodología:

Esta investigación utilizó el modelo de MAGERIT para el análisis y gestión de riesgo.

Conclusión:

Actualmente la información juega un papel importante en el mundo de los negocios por ello es necesario que se cuente con un sistema de seguridad acorde a las necesidades tanto para las empresas como de los usuarios particulares, ya que las primeras son el punto débil de los hackers por el sólo hecho de manejar información delicada.

Cadme C., Duque D. (2012) Realizaron una tesis titulada "*Auditoría de Seguridad Informática ISO 27001 para la empresa de alimentos ITALIMENTOS CIA.LTDA*" Universidad Politécnica Salesiana - Cuenca.

Objetivo General:

Realizar una Auditoría para alinear la empresa con la ISO 27001 para garantizar la seguridad, rendimientos y privacidad de los sistemas y máquinas de la empresa; para esto hizo un análisis exhaustivo que describió la situación actual de la empresa concluyendo con las propuestas de solución que tuvo su auditoria.

Metodología: Para la investigación se utilizará de la norma ISO 27001 para el analizar el nivel de seguridad de información, lo cual permitirá identificar de manera oportuna las deficiencias de la institución.

Conclusión:

La información es uno de los activos más importantes para la compañía, por lo tanto, se le debe dar un tratamiento seguro haciendo que la información se convierta en el eje central sobre el cual gira la seguridad, definiendo acciones de protección y mecanismos de control para garantizar al negocio, la confiabilidad de dicha información.

B. Nacionales

Villena M. (2006) Realizó una tesis titulada "*Sistema De Gestión De Seguridad De Información Para Una Institución Financiera*" Para optar por el título de Ingeniero Informático, Pontificia Universidad Católica del Perú.

Objetivo General:

El objetivo de la presente tesis es establecer los principales lineamientos para poder implementar de manera exitosa, un adecuado modelo de sistema de gestión de seguridad de información (SGSI) en una institución financiera en el Perú, el cual apunte a asegurar que la tecnología de información usada esté alineada con la estrategia de negocio y que los activos de información tengan el nivel de protección acorde con el valor y riesgo que represente para la organización.

Metodología:

Para el desarrollo se presentan ciertos aspectos importantes relacionados al tema de seguridad de información y su administración como Gobierno de TI, BS 7799, ISO 1799, COBIT, AS/NZS 4360:2004.

Conclusión:

De acuerdo a lo expuesto en la presente tesis, para implantar una adecuada gestión de seguridad de información en una institución financiera, el primer paso es obtener el apoyo y soporte de la alta gerencia, haciéndolos participes activos de lo que significa mantener adecuadamente protegida la información de la institución financiera. Al demostrarles lo importante que es la protección de la información para los procesos de negocio, se debe esperar de la alta gerencia su participación continua.

Contando con el apoyo de la alta gerencia se ha dado el primer gran paso. Este apoyo luego se debe transmitir a los dueños de procesos de negocio más importantes de la institución financiera, que generalmente son jefes de áreas. Dándoles a conocer la importancia de la seguridad de información en los procesos que manejan, se espera el apoyo de todo el personal a su cargo.

Córdova N. (2008) Realizó una tesis titulada "*Plan de Seguridad Informática para una Entidad Financiera*" Para optar por el título de Ingeniero de Sistemas, Universidad Nacional Mayor de San Marcos.

Objetivo General:

El objetivo del presente trabajo es realizar un diagnóstico de la situación actual en cuanto a la seguridad de información que el Banco ABC actualmente administra y diseñar un Plan de Seguridad de la Información (PSI) que permita desarrollar

operaciones seguras basadas en políticas y estándares claros y conocidos por todo el personal del Banco. Adicionalmente, el presente trabajo contempla la definición de la estrategia y los proyectos más importantes que deben ser llevados a cabo para culminar con el Plan de Implementación.

Metodología:

La estrategia empleada para la planificación y desarrollo del presente trabajo, está basada en la metodología Enterprise Security Arquitecture (ESA) para el diseño de un modelo de seguridad, como marco general establece el diseño de políticas, normas y procedimientos de seguridad para el posterior desarrollo de controles sobre la información de la empresa.

Conclusión:

Dentro de las conclusiones más importantes tenemos:

Para nadie es un secreto la importancia de implementar un programa completo de seguridad de la información.

Sin embargo, crear un programa de seguridad con componentes "bloqueadores de cookies" rara vez produce resultados efectivos.

Lo más efectivo es utilizar una metodología comprobada que diseñe el programa de seguridad con base en las necesidades de su empresa, recuerde cada empresa es diferente.

La clave para desarrollar con éxito un programa efectivo de seguridad de la información consiste en recordar que las políticas, estándares y procedimientos de seguridad de la información son un grupo de documentos interrelacionados. La relación de los documentos es lo que dificulta su desarrollo, aunque es muy poderosa cuando se pone en práctica. Muchas organizaciones ignoran esta interrelación en un esfuerzo por simplificar el proceso de desarrollo. Sin embargo, estas mismas

relaciones son las que permiten que las organizaciones exijan y cumplan los requerimientos de seguridad.

Ampuero C. (2011) Realizó una tesis titulada "*Diseño De Un Sistema De Gestión De Seguridad De Información Para Una Compañía De Seguros*" Para optar por el título de Ingeniero Informático, Pontificia Universidad Católica del Perú.

Objetivo General:

Desarrollar un sistema de gestión de seguridad de Información para ayudar al área de TI de una compañía de seguros**.**

Metodología:

Con el pasar de los años la seguridad de información ha tomado una mayor importancia, lo que trajo consigo que un grupo de especialistas a nivel mundial en temas relacionados a seguridad, riesgos y temas afines, desarrollen diversos marcos de trabajo, metodologías, estándares, buenas prácticas, distintos modelos para diseñar un SGSI, leyes, normativas, entre otros, con la finalidad de brindar a las empresas la oportunidad de adoptarlas y proteger adecuadamente la información de sus clientes.

Este capítulo busca explicar a groso modo parte de todo aquello que se ha desarrollado hasta el momento, que guarda relación con temas de seguridad y con el desarrollo de la tesis utilizando COBIT 4.1.

Conclusión:

De acuerdo con lo expuesto en la presente tesis, actualmente se vive en una época en la que la información y los datos poseen una importancia decisiva en la gran mayoría de compañías, convirtiéndose así en su activo más importante. Por ejemplo, si en algún momento se da un terremoto y se cae el edificio de la compañía, se puede volver a reconstruir; si se realiza una mala inversión en la bolsa, se puede volver a recuperar el dinero. En cambio, si llegamos a perder la información de la compañía,

es muy probable que no podamos volver a recuperarla si no se tienen las consideraciones debidas, con lo que es probable que la empresa deje de operar.

2.2. Bases Teóricas

2.2.1. Auditoria

La auditoría se ha empleado incorrectamente y se le ha considerado como una evaluación cuyo único fin es detectar errores y señalar fallas. Por eso se ha llegado a usar la frase "tiene auditoría" como sinónimo de que, desde antes de realizarse, ya se encontraron fallas y por lo tanto se está haciendo auditoría. El concepto de auditoría es más amplio; no solo detecta errores: es un examen que se realiza con objeto de evaluar la eficiencia y eficacia de una sección o de un organismo, y determinar cursos alternativos de acción para mejorar la organización, y lograr los objetivos propuestos.

La palabra auditoría viene del latín *auditorius*, y ésta proviene "auditor", el que tiene la virtud de oír; el diccionario lo define como "revisor de cuentas colegiado". El auditor tiene la virtud de oír y revisar cuentas, pero debe estar encaminado a un objetivo específico, que es el evaluar la eficiencia y eficacia con que se está operando para que, por medio del señalamiento de cursos alternativos de acción, se tomen decisiones que permitan corregir los errores, en caso que existan, o bien mejorar la forma de actuación. (Echenique, 2008:17).

2.2.2. Clasificación de auditoria

La auditoría se clasifica en:

- Auditorita Externa.

  La principal característica de este tipo de auditoría es que la realizan auditores totalmente ajenos a la empresa, por lo menos en el ámbito profesional y laboral, esto permite que el auditor externo utilice su libre albedrío en la aplicación de los métodos, técnicas y herramientas de auditoría con las cuales hará la evaluación de las actividades y operaciones de la empresa que audita y, por lo tanto, la emisión de resultados será absolutamente independiente.

- Auditoria Interna.

  En la realización de estos tipos de evaluación, el auditor que lleva a cabo la auditoría labora en la empresa donde se realiza la misma y, por lo tanto, de alguna manera, está involucrado en su operación normal, debido a esto, el auditor puede tener algún tipo de independencia con las autoridades de la institución, lo cual puede llegar a influir en el juicio que emita sobre la evaluación de las áreas de la empresa. (Muñoz C., 2010:95).

2.2.3. Auditoria de seguridad informática

Una Auditoría de Seguridad Informática es el estudio que comprende el 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, los servidores y las redes de comunicaciones.

Durante una Auditoría de Seguridad Informática se realizan los siguientes tipos de auditorías expuestos anteriormente: Auditoría de la seguridad lógica y Auditoría de las comunicaciones.

Una vez obtenidos los resultados, se detallan, archivan y reportan a los responsables quienes deben establecer medidas preventivas de refuerzo, siguiendo siempre un proceso secuencial que permita a los administradores mejorar la seguridad de sus sistemas aprendiendo de los errores cometidos con anterioridad.

Dentro de las Auditorías de Seguridad Informática existen dos tipos principales en función del ámbito desde el que se comprueba la seguridad:

- **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 es estudiado y se analiza el grado de seguridad que ofrece en las entradas exteriores.

La Auditoría de Seguridad Informática consta de las siguientes fases:

- **Enumeración de redes, topologías y protocolos.** Esta fase de reconocimiento pretende extraer la mayor información valiosa posible acerca de la red que va a ser auditada. Es fundamental el uso de herramientas de detección de equipos en esta fase.

- **Análisis de servicios y aplicaciones.** Esta fase consiste en detectar qué servicios están activos en qué puertos y qué software junto con su versión están ejecutando. Para obtener está información se utilizan técnicas, que mediante el uso de paquetes malformados extraen la información deseada.

- **Detección, comprobación y evaluación de vulnerabilidades.** En esta fase se hace uso de las Bases de Datos existentes con información acerca de vulnerabilidades en software anticuado. Por lo tanto, lo que se hace es comprobar que el software detectado en la fase anterior no es vulnerable.

- **Análisis de las comunicaciones.** Esta fase suele constar de una comprobación de si la red es vulnerable a ataques de tipo Man-in-the-Middle. Por lo general la mayoría de redes suele ser débil a estos ataques y en caso de que lo sea, se

realiza un análisis más exhaustivo de las comunicaciones existentes.

Este análisis exhaustivo consiste en verificar si se utilizan protocolos de comunicación seguros mediante conexiones cifradas o por el contrario viajan las claves en texto plano por la red.

Finalmente, si se obtienen contraseñas cifradas también existe la posibilidad de intentar descifrarlas para verificar que el nivel de seguridad de las mismas es el adecuado.

Medidas específicas de corrección. Finalmente se redacta un informe con los datos extraídos de la auditoría y con recomendaciones sobre las medidas de corrección que deberían ser adoptadas. (Piattini M., 2001:4-9).

2.2.4. Políticas de seguridad

Definir el concepto de política de seguridad no es algo fácil, se puede decir que la Seguridad Informática consiste en que un sistema se comporte como el usuario espera que lo haga, y a su vez mantenerlo libre de amenazas y riesgos. Por más de dos décadas se ha manejado que la seguridad se logra a partir de tres conceptos, conocidos como la triada de la seguridad: confidencialidad, integridad y disponibilidad. (Monzón C., 2009:32).

2.2.5. Elementos de la política de seguridad informática

A. Confidencialidad

Consiste en mantener la información secreta a todos, excepto a aquellos que tienen autorización para verla. Cuando la información de naturaleza confidencial ha sido accedida, usada, copiada o revelada, por una persona que no está autorizada, entonces se presenta una ruptura de confidencialidad. La confidencialidad es un requisito para mantener la privacidad de las personas.

La confidencialidad es una propiedad de difícil recuperación, pudiendo minar la confianza de los demás en la organización que no es diligente en el mantenimiento del secreto. (Monzón C., 2009:54).

B. Integridad

Significa que se debe asegurar que la información no ha sido alterada por medios no autorizados o desconocidos. Un ataque no debe ser capaz de sustituir información legítima por falsa. (Monzón C., 2009:56).

C. Disponibilidad

Significa que todos aquellos elementos que sirven para el procesamiento de la información, así como los que sirven para facilitar la seguridad, estén activos y sean alcanzables siempre que se quiera. (Monzón C., 2009:57).

Figura 1. Triada de la seguridad.

2.2.6. Auditoria de Seguridad Informática

Cuando hablamos de la seguridad en un sistema informático, podemos encontrar diversos tipos de seguridad, dependiendo de la naturaleza material de los elementos que utilicemos o de si se ocupan de evitar el ataque o incidente o recuperar el sistema una vez que este se haya producido.

A. Seguridad activa y pasiva

Activa

Se entiende por seguridad activa todas aquellas medidas que se utilizan para detectar amenazas, y en caso de su detección generar los mecanismos adecuados para evitar el problema.

Pasiva

Está formada por las medidas que se implantan para, una vez producido el incidente de seguridad, minimizar su repercusión y facilitar la recuperación del sistema; por ejemplo, teniendo siempre al día copias de seguridad de los datos.

(Cervigón A; Alegre M, 2011:65)

B. Seguridad física y lógica

Física

Se utiliza para proteger el sistema informático utilizando barreras físicas y mecanismos de control. Se emplea para proteger físicamente el sistema informático.

Las amenazas físicas se pueden producir provocadas por el hombre, de forma accidental o voluntaria, o bien por factores naturales.

Lógica

La seguridad lógica se encarga de asegurar la parte software de un sistema informático, que se compone de todo lo que no es físico, es decir los programas y los datos.

La seguridad lógica se encarga de controlar que el acceso al sistema informático, desde el punto de vista software, se realice correctamente y por usuarios autorizados, ya sea desde dentro del sistema informático, como desde fuera, es decir, desde una red externa, usando una VPN, la web (protocolos http, https), transmisión de ficheros (FTP), entre otros.

2.2.7. Razones para la seguridad informática

Preservar la información y la integridad de un sistema informático es algo muy importante para una empresa u organización, por lo que en pérdidas económicas y de tiempo podría suponer, sin olvidarnos del peligro que podría acarrear el acceso al sistema de un usuario no autorizado.

Igualmente, es también importante para un usuario que emplee su ordenador en el ámbito doméstico, por lo que podría suponer el perder documentos o fotos personales, sin olvidarnos del inconveniente que supondría el no poder disponer de su equipo durante un tiempo determinado o el coste de intentar recuperar la información perdida. Ver figura 2.

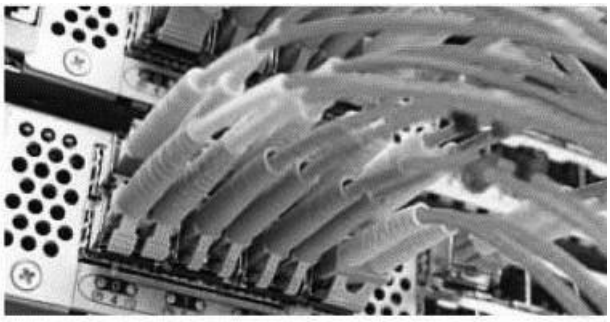


Figura 2. Conexiones de ordenadores en red.

Además, cada día es más frecuente realizar cualquier gestión a través de la web, ya sea de tipo personal, económica, administrativa, etc. Para estos tipos de gestiones se puede utilizar una clave de acceso, un certificado digital, o bien el DNI electrónico, entre otros, pero hay que tener cuidado y utilizar sistemas de protección cuando se envía información confidencial como, por ejemplo, el número de la tarjeta de crédito, a través de una red de ordenadores, en especial si se hace en lugares públicos. (Cervigón A; Alegre M, 2011:91). Ver figura 3.

Figura 3. Tarjeta de Crédito.

2.2.8. Estándar de seguridad informática NTP-ISO/IEC 17799:2007

2.2.8.1 Norma Técnica Peruana (NTP – ISO/IEC 17799:2007)

Con fecha 23 de julio del 2004 la PCM a través de la ONGEI, dispone el uso obligatorio de la Norma Técnica Peruana NTP-ISO/IEC 17799:2004 EDI. Tecnología de la Información: Código de Buenas Prácticas para la

Gestión de la Seguridad de la Información" en entidades del Sistema Nacional de Informática. (Lázaro M., 2008:56)

Se Actualizó el 25 de agosto del 2007 con la Norma Técnica Peruana NTP - ISO/IEC 17799:2007 EDI.

2.2.8.2 Marco de las recomendaciones de la NTP – ISO/IEC 17799:2007

La NTP - ISO 17799 es una compilación de recomendaciones para las prácticas exitosas de seguridad, que toda organización puede aplicar independientemente de su tamaño o sector.

La NTP fue redactada para que fuera flexible y no induce a las organizaciones que la cumplan al pie de la letra, se deja a estas dar una solución de seguridad de acuerdo a sus necesidades.

Las recomendaciones de la NTP - ISO 17799 son neutrales en cuanto a la tecnología. La norma discute la necesidad de contar con firewalls, pero no profundiza sobre los tipos de firewalls y cómo se utilizan. En este sentido La Norma Técnica Peruana ISO 17799, se emite para ser considerada en la implementación de estrategias y planes de seguridad de la información de las entidades públicas. (Lázaro M., 2008:58)

2.2.8.3 Dominios de Control NTP – ISO/IEC 17799:2007

INDECOPI (2007), publicó:

1. **Política de seguridad:** Se necesita una política que refleje las expectativas de la organización en materia de seguridad, a fin de suministrar administración con dirección y soporte. La política también se puede utilizar como base para el estudio y evaluación en curso.
2. **Aspectos organizativos para la seguridad:** Sugiere diseñar una estructura de administración dentro la organización, que establezca la responsabilidad de los grupos en ciertas áreas de la seguridad y un proceso para el manejo de respuesta a incidentes.

3. **Clasificación y control de activos:** Inventario de los recursos de información de la organización y con base en este conocimiento, debe asegurar que se brinde un nivel adecuado de protección.

4. **Seguridad de recursos humanos:** Necesidad de educar e informar a los empleados actuales y potenciales sobre lo que se espera de ellos en materia de seguridad y asuntos de confidencialidad. Implementa un plan para reportar los incidentes.

5. **Seguridad física y del entorno:** Responde a la necesidad de proteger las áreas, el equipo y los controles generales.

6. Gestión de comunicaciones y operaciones
7. **Control de accesos:** Establece la importancia de monitorear y controlar el acceso a la red y los recursos de aplicación como protección contra los abusos internos e intrusos externos.
8. **Adquisición, desarrollo y mantenimiento de los sistemas:** Recuerda que, en toda labor de la tecnología de la información, se debe implementar y mantener la seguridad mediante el uso de controles de seguridad en todas las etapas del proceso.
9. **Gestión de incidentes de la seguridad de la información:** Asegurar que los eventos y debilidades en la seguridad de la información sean comunicados de manera que permitan una acción correctiva a tiempo.
10. **Gestión de continuidad del negocio:** Aconseja estar preparado para contrarrestar las interrupciones en las actividades de la empresa y para proteger los procesos importantes de la empresa en caso de una falla grave o desastre.
11. **Cumplimiento:** Evitar brechas de cualquier ley civil o criminal, estatutos, obligaciones regulatorias o contractuales y de cualquier requerimiento de seguridad. Ver figura 4.

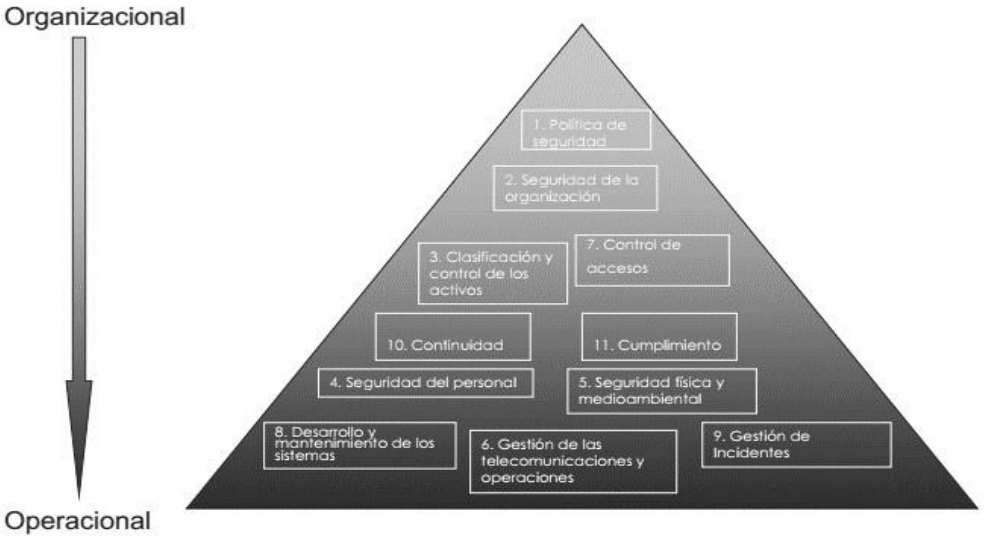


Figura 4. Los 11 dominios de la ISO 17799-2007.

2.2.9. COBIT 4.1

Es una herramienta para la administración de las tecnologías de información. Fue desarrollada por ISACA como un estándar para la seguridad de la tecnología de información y buenas prácticas de control.

Está orientado a la gestión, auditoria de sistemas, control y seguridad. Define lo que es necesario hacer para implementar una efectiva estructura de control.

Permite atender las brechas entre los riesgos del negocio, necesidades de control y aspectos de tecnología. Brinda, además, buenas prácticas a través de una plataforma de dominios y procesos y presenta actividades en una estructura lógica y administrativa.

La gestión y administración de una organización debe garantizar que exista una plataforma de control interno que dé soporte a los procesos de negocio. COBIT se concentra en los requerimientos del negocio relacionados a efectividad,

eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad de la información que fluye en la organización.

COBIT maneja el control desde el punto de vista de políticas, estructuras organizacionales y procedimientos. En cuanto a la administración y gestión, estas son manejadas desde la perspectiva del gobierno corporativo, es decir, señalando los lineamientos para que todos los individuos involucrados en la administración, uso, diseño, desarrollo y mantenimiento de los sistemas de información cumplan con los objetivos del negocio. Se maneja también, el concepto de objetivo de control el cual estable un propósito a ser cumplido implementando procedimientos de control dentro de una actividad particular de tecnologías de información.

Existen actualmente otros modelos de control como el COSO (USA), Cadbury (Reino Unido), CoCo (Canadá) y King (Sudáfrica), los cuales están concentrados exclusivamente en el control, sin proveer un modelo claro para dar soporte a los procesos de negocio. El propósito de COBIT es cubrir esta brecha brindando una base para el cumplimiento de los objetivos de negocio con la adecuada gestión de la tecnología de información.

Su objetivo principal es el desarrollo de políticas claras y buenas prácticas para la seguridad y control de la tecnología de información para organizaciones comerciales, gubernamentales, y financieras entre otras. El desarrollo de COBIT está centrado en objetivos de control desde la perspectiva de los objetivos de negocio. A esto se agregan objetivos de control con fines de auditoria.

COBIT se compone de:

- **Guías de Administración (Management Guidelines):** Para asegurar una organización exitosa, se debe administrar efectivamente la unión entre los

procesos de negocios y los sistemas de información. Las guías de administración consisten en:

* Modelos de Maduración (Maturity Models), que ayudan a determinar las fases y niveles esperados de control, comparándolos con normas actuales.

* Factores Críticos de Éxito (Critical Success Factors), para identificar las acciones más importantes para alcanzar el control sobre los procesos de tecnología de información.

* Indicadores Clave de Cumplimiento (Key Goal Indicators), para definir niveles objetivo de desempeño.

* Indicadores Clave de Desempeño, para medir si un proceso de control de tecnología está cumpliendo con su objetivo.

- **Resumen Ejecutivo (Executive Summary):** Específicamente diseñado para ejecutivos y administradores, consiste en una explicación de los conceptos y principios claves de COBIT. Se incluye una síntesis de la plataforma o Framework, la cual muestra un detalle más amplio de los conceptos y principios, a la vez que se identifican los dominios (Planeamiento y Organización, Adquisición e Implementación, Entrega y Soporte, Monitoreo) y procesos de tecnología.
- **Plataforma (Framework):** Una organización exitosa está construida sobre una sólida plataforma de datos e información. La plataforma explica cómo los procesos de tecnología de información entregan la información que el negocio necesita para cumplir con sus objetivos. Esta entrega es controlada por medio de 34 controles de alto nivel, uno por cada proceso de tecnología, contenidos en cuatro dominios. La plataforma identifica cuál de los siete criterios de información (efectividad, eficiencia, confidencialidad, integridad, disponibilidad,

cumplimiento y fiabilidad) y cuál de los recursos de tecnología (personas, aplicaciones, tecnología, instalaciones y datos) son importantes para que los procesos de tecnología brinden un soporte completo a los objetivos de negocio.

- **Objetivos de Control (Control Objectives):** La clave para mantener la rentabilidad en un ambiente tecnológicamente cambiante es medir qué tan bien se puede mantener el control. Los objetivos de control de COBIT brindan lo necesario para delinear una política clara y buenas prácticas para controles de tecnología de información. Se incluyen los aspectos óptimos o resultados deseados que deben alcanzarse, implementando alguno de los 318 objetivos de control específicos detallados, a través de los 34 procesos de tecnología de información.
- **Guías de Auditoria (Audit Guidelines):** Para cumplir con los objetivos trazados, periódicamente deben auditarse los procedimientos. Las guías de auditoria sugieren actividades que pueden desarrollarse para cada uno de los 34 objetivos de control de alto nivel, controlando de esta manera el riesgo asociado en caso no se cumpla con alguno.

Herramientas de implementación (Implementation Tool Set): Contiene herramientas para diagnóstico de controles de tecnología, aspectos de gestión de conocimiento, guías de implementación, preguntas frecuentes, casos de estudio de organizaciones que actualmente emplean COBIT, y presentaciones que pueden emplearse para introducir el COBIT en las organizaciones. Estas herramientas están diseñadas para facilitar la implementación del COBIT, mostrar lecciones aprendidas de organizaciones que rápida y exitosamente aplicaron COBIT en sus ambientes de trabajo. (ISACA, 2007:42-80). Ver figura 5.

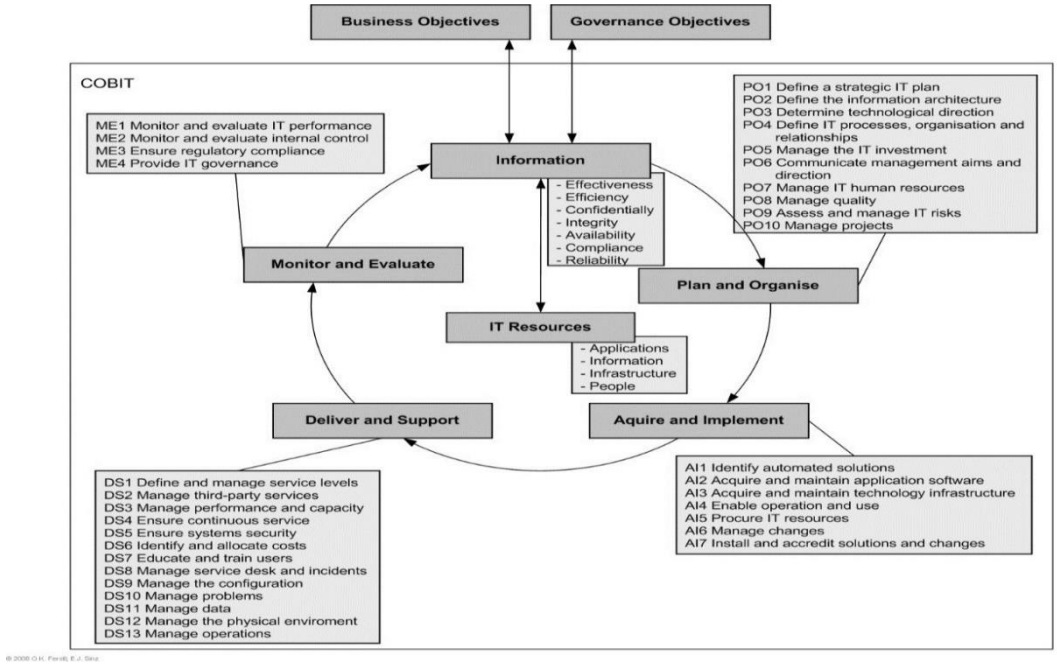


Figura 5. Estructura de COBIT 4.1.

2.3. Definiciones conceptuales

- **Antivirus:** Programa que permite detectar y desinfectar virus en un sistema operativo.
- **Aplicación:** Solución informática que permite automatizar determinadas actividades que pueden resultar ser complejas.
- **Auditoría:** Permite recolectar, agrupar y evaluar. Encontrando deficiencias y corregirlas con la finalidad de salvaguardar los activos.
- **Base De Datos:** Repositorio de información organizada que contiene tablas, columnas, registros.
- **Cifrado:** Transcrita en letras o símbolos alguna información que se quiere ocultar.

- **Conexión:** Enlace, empalme. Acción y efecto de conectar y conectarse.
- **Confidencialidad:** Mantener información secreta, privada.
- **Copias De Seguridad**: Hacer copias de documentos, archivos y otra información importante.
- **Desencriptar:** Traducir a un lenguaje común información oculta.
- **Directiva:** Conjunto de instrucciones.
- **Disponibilidad:** Elementos disponibles, alcanzables siempre que se requiera.
- **Eficacia:** Activo, que logra hacer efectivo un propósito.
- **Eficiencia:** Capacidad para hacer cosas.
- **Emisión:** Acción y efecto de emitir, poner en circulación.
- **Firewall:** Es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.
- **FTP:** En informática, es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red
- **Hackers:** Persona con grandes conocimientos de informática que se dedica a acceder ilegalmente a sistemas informáticos ajenos y a manipularlos.
- **Hardware:** Conjunto de elementos físicos o materiales que constituyen una computadora o un sistema informático.
- **Integridad:** Asegurar que alguna información no sea alterada.
- **Intrusión:** Que se ha introducido sin derecho ni permiso.
- **Malware:** Código maligno, software malicioso o software malintencionado, es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o Sistema de información sin el consentimiento de su propietario.

- **Protocolo:** Conjunto de reglas y normas que permiten que dos o más entidades de un sistema de comunicación se comuniquen entre ellos para transmitir información por medio de cualquier tipo de variación de una magnitud física.
- **Puerto:** Es una forma genérica de denominar a una interfaz a través de la cual los diferentes tipos de datos se pueden enviar y recibir.
- **Red:** Es un conjunto de equipos informáticos y software conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas.
- **Riesgo:** Contingencia o proximidad de un daño.
- **Servidor**: Es un nodo que forma parte de una red, provee servicios a otros nodos denominados clientes.
- **Sistema Operativo:** Conjunto de órdenes y programas que controlan los procesos básicos de una computadora y permiten el funcionamiento de otros programas.
- **Software:** Conjunto de programas y rutinas que permiten a la computadora realizar determinadas tareas.
- **Topologías:** La forma en que está diseñada la red, sea en el plano físico o lógico.
- **UPS:** Es una fuente de suministro eléctrico que posee un batería con el fin de seguir dando energía a un dispositivo en el caso de interrupción eléctrica.
- **VPN:** Es una tecnología de red que permite una extensión segura de la red local sobre una red pública o no controlada como Internet.

2.4. Formulación de Hipótesis

2.4.1. Hipótesis general

El diseño de un modelo de auditoría en seguridad informática permite el alineamiento con las políticas de seguridad del hospital San Juan Bautista Huaral.

2.4.2. Hipótesis especificas

- El diseño del modelo de auditoria en seguridad física, permite alinear significativamente las políticas de seguridad del hospital San Juan Bautista Huaral.
- El diseño de un modelo de auditoria en seguridad lógica permite alinear significativamente las políticas de seguridad del hospital San Juan Bautista Huaral.
- La adaptabilidad del modelo de auditoria en seguridad informática permite alinear significativamente las políticas de seguridad del hospital San Juan Bautista Huaral.

CAPÍTULO III

METODOLOGIA

3.1. Diseño metodológico

3.1.1. Tipo de Investigación

La investigación que se encuentra relacionada con el tipo del problema y sus propósitos establecidos se identifica con una investigación aplicada.

Se estableció esta investigación, porque existe el interés de buscar soluciones para el problema planteado. A través de ella se pretende hallar alguna relación entre una auditoria informática y el alineamiento de las políticas de seguridad información del hospital San Juan Bautista Huaral.

La investigación propuesta es de nivel descriptivo correlacional, ya que tiene como objetivo hallar la relación entre dos variables, en un determinado lugar y tiempo, que intervienen en una determinada situación del presente estudio.

3.1.2. Enfoque y método

La investigación tiene un enfoque cuantitativo, cuya característica será medir un fenómeno y se utilizará estadísticas.

La investigación tendrá un diseño no experimental, y transversal, debido a que en un determinado tiempo se procederá a describir y analizar las particularidades del estudio planteado.

3.2. Población

3.2.1. Población

La población objetivo a investigar está constituida por el personal que labora en el hospital San Juan Bautista Huaral (usuarios que tienen acceso a través de un equipo a los diferentes sistemas de información de la institución), siendo un total de 92 colaboradores.

Tabla 3.1. Tamaño de la población.

CATEGORIA	Nº DE ESTACIONES
DIRECCIÓN EJECUTIVA	4
Director, Subdirector, Órgano de Control Institucional	
JEFE DE ÁREAS	16
Planeamiento Estratégico, Estadística e Informática, Gestión de la Calidad, Apoyo a la Docencia e Investigación, Unidad de Personal, Unidad de Logística, Economía, Departamentos de Servicios de Salud, etc.	
PROFESIONALES	34
Profesionales licenciados. médicos, ingenieros,	
PROFESIONALES TECNICOS	25
Personales técnicos administrativos, técnicos en computación, etc.	
ASISTENTES	13
Personal de las diferentes áreas que cumplen otras funciones.	

3.3. Operacionalización de variables e indicadores

Ver cuadro adjunto.

VARIABLE GENERAL	DEFINICIÓN CONCEPTUAL	DIMENSIONES	DEFINICIÓN OPERACIONAL	INDICADORES
V1 Auditoria en Seguridad Informática	Es el estudio que comprende el 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, los servidores y las redes de comunicaciones. (Piattini, 2001)	Auditoría en seguridad física	Está involucrada con la gestión de la seguridad, plan de contingencia, la protección física de los datos, gestión de riesgo, control de accesos.	• Gestión de la seguridad • Protección física • Plan de contingencia
		Auditoría en seguridad lógica	Se basa en los niveles de protección de la información en un mismo medio a través de controles de acceso, herramientas y técnicas.	• Control de acceso • Herramientas y técnicas
		Adaptabilidad	Se verá reflejada a partir de métodos y procedimientos que se apliquen en base a normal y modelos que se adecuen a las necesidades de la institución.	• Métodos y procedimientos • Normas y documentos

V2 Políticas de seguridad	La política de seguridad es un conjunto de leyes, reglas y prácticas que regulan la manera de dirigir, proteger y distribuir recursos en una organización. (Monzón, 2009)	Políticas de seguridad de la información	Permiten establecer el nivel de impacto, nivel de resultados en el caso que se presenten acontecimientos inesperados que atenten contra la información.	• Nivel de impacto • Nivel de resultado
		Mejora continua	Su nivel de eficiencia y productividad dependerá de la situación económica que permitirá obtener los recursos necesarios.	• Nivel de eficiencia • Nivel de productividad

3.4. Técnicas a emplear

3.4.1. Descripción de los instrumentos

Se utilizó tres tipos de fuentes, estas son:

- Revisión de fuentes bibliográficas.
- Revisión de informes.

Técnicas. - Las técnicas empleadas son:

- Recolección de datos relacionados al tema.
- Observación de características la variable independiente.

- Observación de características la variable dependiente.
- Observación de características de otras variables.

Instrumentos. - Los instrumentos a utilizar son:

- Fichas de documentación.
- Registros de las variables.
- Encuesta de información.

3.5. Técnica para el procesamiento de la información

Para elaborar las tablas y realizar su análisis, empleamos la estadística descriptiva e inferencial, con el apoyo del software SPSS y la hoja de cálculo EXCEL.

Los procesamientos de los datos se harán de la siguiente forma:

Presentación de datos y resultados.

- Ordenamiento.
- Clasificación.
- Selección.
- Codificación.
- Tabulación.
- Tablas.
- Gráficos.

Cálculo de valores estadísticos.

- Tablas Estadísticas.
- Estadígrafos Descriptivos e Inferenciales.

CAPÍTULO IV

DISEÑO DE AUDITORIA INFORMATICA

4.1. Desarrollo de la auditoria Informática

4.1.1. Cronograma de Trabajo

La presente auditoria informática se realizó en el hospital San Juan Bautista, ubicada en el distrito de Huaral.

Empresa: Hospital San Juan Bautista Huaral

Tabla 4.1. Programa de auditoria Informática..

Fase	Actividad
I	Visita Preliminar • Solicitud de manuales y documentos. • Elaboración de cuestionarios. • Recopilación de la información organizacional: estructura orgánica, recursos humanos, presupuestos.
II	Desarrollo de la auditoria • Aplicación del cuestionario al personal. • Entrevistas a jefes y usuarios que pertenecen a la institución. • Análisis de las claves de acceso, control, seguridad, confiabilidad y respaldos. • Evaluación de la estructura orgánica: Unidades, áreas, funciones, autoridades y responsabilidades. • Evaluación de los recursos humanos y la situación presupuestal y financiera: Desempeño, capacitación, condiciones de trabajo, recursos en materiales, infraestructura y equipos. • Evaluación de los sistemas: relevamiento de hardware y software, evaluación del diseño lógico y desarrollo del sistema. • Evaluación del proceso de datos y de los equipos de cómputo: Seguridad de los datos, control de operación, seguridad física y procedimiento de respaldo.

III	Revisión y pre-informe • Revisión de los documentos de trabajo. • Determinación del diagnóstico e implicancia. • Elaboración del borrador.
IV	Informe • Elaboración y presentación del informe.

4.1.2. Documentos a solicitar

• Políticas de seguridad, estándares, normas, y procedimientos.

• Plan de seguridad, contingencia y continuidad.

• Contratos, seguros.

• Organigrama y manual de funciones.

• Manual de sistemas.

• Registros.

• Entrevistas.

• Archivos.

• Requerimientos de usuarios.

4.1.3. Revisión de la organización

El Hospital San Juan Bautista Huaral es un establecimiento sanitario para la atención y asistencia a enfermos por medio de profesionales médicos, de enfermería y personal auxiliar y de servicios técnicos durante 24 horas, 365 días del año y disponiendo de tecnología, aparatología, instrumental y farmacología adecuadas.

4.1.3.1 Principales actividades

Sistema Asistencial

Engloba a todas las áreas del hospital que tienen una función asistencial, es decir atención directa del paciente por parte de profesionales del equipo de salud. Hay dos áreas primordiales en la asistencia directa del paciente:

- Los consultorios externos para atender pacientes con problemas ambulatorios (que no requieren internación).
- Las áreas de unidad del paciente, para cuidado de problemas que sí requieren hospitalización.

Sistema Administrativo Contable

Este sistema tiene que ver con las tareas administrativas de un hospital. En él se encuentran áreas como admisión y egreso de pacientes, otorgamiento de turnos para consultorios externos, departamento de recursos humanos, oficinas de auditoría, farmacia, entre otras. En sí toda oficina que trabaja con el público en algún proceso o trámite con documentación, es una oficina administrativa. El área contable del hospital se encarga primariamente de la facturación de las prestaciones dadas a las entidades de cobertura correspondientes.

Sistema Gerencial

Está compuesto según los hospitales por gerencias o direcciones. Las más destacadas es la Gerencia Médica, que organiza o dirige el

funcionamiento global del hospital, sus políticas de prevención, diagnóstico y tratamiento, y el presupuesto, entre otros temas.

Sistemas De Información

Se refiere al sistema informático que tiene el hospital y que soporta su funcionamiento en redes de computadoras y programas diseñados especialmente para el correcto funcionamiento de todas las áreas. Es manejada generalmente por la Unidad de Estadística e Informática.

Sistema Técnico

Engloba a todas las dependencias que proveen soporte, mantenimiento preventivo en una institución.

Docencia e Investigación

La docencia en un hospital es un punto clave en la formación de profesionales. La docencia y la investigación están ligadas en varios aspectos, con programas bien organizados para que el nuevo profesional del equipo de salud obtenga la mejor formación posible.

4.1.3.2 Funciones generales

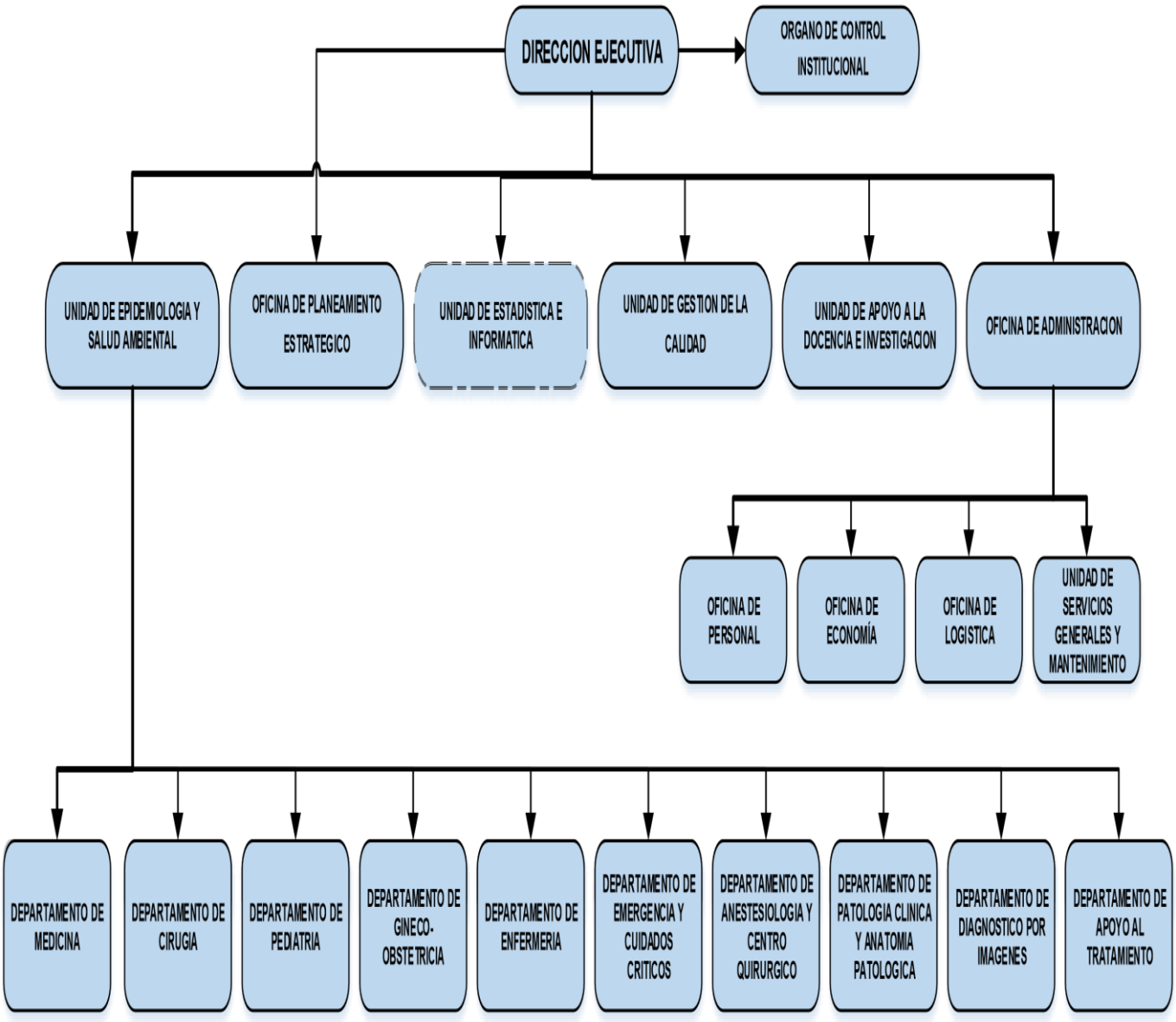
- Planificar, ejecutar e impulsar, a través de los órganos correspondientes, el conjunto de acciones destinadas a proporcionar al ciudadano, el ambiente adecuado para las proporcionar una adecuada atención integral.

- Formular un plan de desarrollo en concordancia con las necesidades y requerimientos de la población organizada.
- Conducir los distintos programas de estrategias sanitarias, conforme lo establece el ministerio de salud, velando por su ejecución.

4.1.3.3 Organigrama institucional

ORGANIGRAMA ESTRUCTURAL HOSPITAL "SAN JUAN BAUTISTA HUARAL"

APROBADO CON ORDENANZA REGIONAL N°08-2014-CR-RLO



4.1.3.4 Análisis FODA de la institución

Tabla 4.2. Análisis FODA de la institución

FORTALEZAS	OPORTUNIDADES
• Personal directivo y técnico con experiencia. • Capacidad de convocatoria.	* Búsqueda de reducción de costos, aprovechando los sistemas de información. * Calidad de servicio. * Predisposición y voluntad de los nuevos directivos para el cambio tecnológico.
DEBILIDADES	**AMENAZAS**
• Falta de planes y programas informáticos. • Falta de identificación del personal con la institución. • Inestabilidad laboral del personal. • No existe programas de capacitación y actualización al personal. • Rotación permanente del personal imposibilitando continuidad a los objetivos propuestos.	• Estandarizar y uniformizar la información relevante.

4.1.4. Plan de auditoria Informática

Tabla 4.3. Plan de Auditoria Informática

Plan de Auditoria Informática

1. Metodología

La metodología de investigación a utilizar en el proyecto para la evaluación de la situación actual en la que se encuentra la institución es necesario llevar a cabo las siguientes actividades:

- Solicitud de los estándares utilizados y programa de trabajo
- Aplicación del cuestionario al personal
- Análisis y evaluación del a información
- Elaboración del informe
- Para la evaluación de los sistemas tanto en operación como en desarrollo se llevarán a cabo las siguientes actividades:
    - Solicitud del análisis y diseño del os sistemas en desarrollo y en operación
    - Solicitud de la documentación de los sistemas en operación (manuales técnicos, de operación del usuario, diseño de archivos y programas)
    - Recopilación y análisis de los procedimientos administrativos de cada sistema (flujo de información, formatos, reportes y consultas)
    - Análisis de llaves, redundancia, control, seguridad, confidencial y respaldos

- Análisis del avance de los proyectos en desarrollo, prioridades y personal asignado
- Entrevista con los usuarios de los sistemas o Evaluación directa de la información obtenida contra las necesidades y requerimientos del usuario
- Análisis objetivo de la estructuración y flujo de los programas.
- Análisis y evaluación de la información recopilada
- Elaboración del informe.

- Para la evaluación de los equipos se llevarán a cabo las siguientes actividades:
  - Solicitud de los estudios de viabilidad y características de los equipos actuales, proyectos sobre ampliación de equipo, su actualización
  - Solicitud de contratos de compra y mantenimientos de equipo y sistemas
  - Solicitud de contratos y convenios de respaldo o
  - Solicitud de contratos de Seguros
  - Elaboración de un cuestionario sobre la utilización de equipos, memoria, archivos, unidades de entrada/salida, equipos periféricos y su seguridad
  - Visita técnica de comprobación de seguridad física y lógica de las instalaciones de la Dirección de Informática

- Evaluación técnica del sistema electrónico y ambiental de los equipos y del local utilizado
- Evaluación de la información recopilada, obtención de gráficas, porcentaje de utilización de los equipos y su justificación

Finalmente, elaboración y presentación del informe final (conclusiones y recomendaciones)

2. Justificación

- Desconocimiento en el nivel directivo de la situación informática de la institución.
- Falta total o parcial de nivel de seguridad lógica y física que garanticen la integridad de la información, equipos y personal.
- Falta de una planificación informática.
- Descubrimiento de fraudes efectuados a través de un ordenador.
- Documentación incompleta de sistemas que revela la dificultad para efectuar el mantenimiento de estos.

3. Motivo de la Auditoria Informática

3.1 Síntomas de descoordinación y desorganización

* No coinciden los objetivos del área informática y la propia Institución.

* Los estándares de productividad se desvían sensiblemente de los promedios conseguidos habitualmente. Puede ocurrir con algún cambio masivo de personal, reestructuración fallida de alguna área o la modificación de alguna norma importante.

3.2 Síntomas de insatisfacción de los usuarios

* No se atienden las peticiones de cambios de los usuarios. Ejemplos: cambios de software en los terminales de usuario, refrescamiento de paneles, variación de los ficheros que deben ponerse diariamente a su disposición, etc.

* No se reparan las averías de hardware ni se resuelven incidencias en plazos razonables. El usuario percibe que está abandonado y desatendido permanentemente.

* No se cumplen en todos los casos los plazos de entrega de resultados periódicos. Pequeñas desviaciones pueden causar importantes desajustes en la actividad del usuario, en especial en los resultados de aplicaciones críticas y sensibles.

3.3 Síntomas de debilidades económico-financiero

* Incremento desmesurado de costes.

* Necesidad de justificación de inversiones informáticas (la empresa no está absolutamente convencida de tal necesidad y decide contrastar opiniones).

* Desviaciones presupuestarias significativas.

* Costos y plazos de nuevos proyectos (deben auditarse simultáneamente a desarrollo de proyectos y al órgano que realizó la petición).

3.4 Síntomas de inseguridad de la información

- Seguridad lógica
- Seguridad física
- Confidencialidad

4.1.5. Desarrollo de la auditoria Informática

4.1.5.1 Plan de Trabajo: Diagnóstico de Seguridad de la Información para el Hospital San Juan Bautista Huaral

Tabla 4.4. Diagnóstico de Seguridad de la Información Hospital San Juan Bautista Huaral

Plan de Trabajo: Diagnóstico de Seguridad de la Información
Hospital San Juan Bautista Huaral

I. OBJETIVO Y ALCANCE

El objetivo del trabajo está dirigido a asesorar al Hospital San Juan Bautista Huaral para que desarrolle un plan de acción que permita contar con una infraestructura para administrar los riesgos de información y de tecnología de información de acuerdo con las mejores prácticas y cumplir con la normatividad del organismo regulador.

1.1. Objetivos del Trabajo

Objetivo General

- Desarrollar un plan de trabajo basado en el diagnóstico de seguridad de información para el Hospital San Juan Bautista Huaral.

Objetivo Especifico

- Determinar si la infraestructura tecnológica instalada es suficiente para dar soporte a los sistemas de información, base de datos y sistemas de red con la que trabaja el Hospital San Juan Bautista Huaral.
- Determinar si los niveles de seguridad son adecuados, para asegurar el cumplimiento de las políticas normativas del Hospital San Juan Bautista Huaral.

1.2. Alcance del Trabajo

Este trabajo se ejecutará en el Hospital San Juan Bautista Huaral donde se formulará un plan de seguridad de la información, un plan de continuidad del negocio.

El periodo en el que se está evaluando la información proporcionada por la empresa data desde (enero 2015 a julio 2016), para lo cual se está utilizando el criterio de la ISO 17799 con sus 11 dominios correspondientes.

II. METODOLOGÍA

Para el presente diagnostico se está utilizando la ISO 17799 y posteriormente evaluar el nivel de cumplimiento mediante una comparación de controles existentes.

La metodología que se empleará toma como referencia y a la guía de estándar internacional, que es: **ISO/IEC 17799:**

Es una norma internacional que ofrece recomendaciones para realizar la gestión de la seguridad de la información dirigida a los responsables de iniciar, implantar o mantener la seguridad de una organización.

Tiene como objetivo proporcionar una base común para desarrollar normas de seguridad dentro de las organizaciones, un método de gestión eficaz de la seguridad y para establecer transacciones y relaciones de confianza entre instituciones públicas y privadas. La ISO 17799 establece once dominios:

- **Política de seguridad:** Dirigir y dar soporte a la Gestión de la seguridad de la información - directrices y recomendaciones.
- **Organización de seguridad:** Definir los roles y las responsabilidades. Monitorea a los socios y ya terceros.
- **Clasificación y control de activos:** Inventario y nivel de protección de los activos.
- **Seguridad ligada al personal:** Reducir riesgos de errores humanos, robos, fraudes o mal uso de los recursos.

- **Seguridad física y del entorno:** Evitar accesos no autorizados, violación, daños o perturbaciones a las instalaciones y a los datos.
- **Gestión de comunicaciones y operaciones:** Asegurar la operación correcta y segura de los recursos de tratamiento de información.
- **Control de acceso:** Evitar accesos no autorizados a los sistemas de información (de usuarios, computadores, redes, etc.)
- **Desarrollo y mantenimiento de sistemas:** Asegurar que la seguridad está incorporada dentro de los sistemas de información. Evitar pérdidas, modificaciones, mal uso.
- **Gestión de incidentes:** Gestionar los incidentes que afectan la seguridad de la información.
- **Gestión de continuidad del negocio:** Reaccionar a la interrupción de las actividades del negocio y proteger sus procesos críticos frente a fallas, ataques o desastres.
- **Conformidad con la legislación:** Evitar el incumplimiento de leyes, regulaciones, obligaciones y de otros requerimientos de seguridad.

III. PROCEDIMIENTO A UTILIZAR

Durante el desarrollo del presente informe se hará uso de herramientas como la entrevista y el cuestionario dirigido al personal, asegurándonos que la encuesta tenga las preguntas esenciales para la investigación basada en la ISO mencionada anteriormente.

Esto la finalidad de obtener la información correspondiente y así poder estimar el nivel de cumplimiento de la empresa.

IV. IDENTIFICACIÓN Y EVALUACIÓN DE LOS RIESGOS DE INFORMACIÓN Y TECNOLOGÍA DE LA INFORMACIÓN

Para evaluar los riesgos de información y tecnología de información se tendrán en cuenta los siguientes objetivos, según los once dominios:

4.1. Política de Seguridad

Proporcionar dirección gerencial y apoyo a la seguridad de la información en concordancia con los requerimientos comerciales, leyes y regulaciones.

4.2. Organización de la Seguridad de la Información

Manejar la seguridad de la información dentro de la organización y los medios de proceso de información a los cuales entidades externas tienen acceso.

4.3. Gestión de Activos

Mantener la protección de los activos organizacionales y asegurar que la información reciba un nivel de protección apropiado.

4.4. Seguridad de los Recursos Humanos

Para el grupo de personas dentro de una organización como empleados, contratistas o terceros, antes del empleo deben entender sus responsabilidades, roles y así lograr reducir riesgo de robo, fraude o mal uso de los medios, tener conocimiento de las amenazas de la seguridad de la información, a la terminación o cambio del empleo asegurar que salgan de la organización o cambien de empleo de una manera ordenada.

4.5. Seguridad Física y Ambiental

En las áreas seguras se debe evitar el acceso físico no autorizado, información de la organización y a la interferencia al local. Además evitar la pérdida, robo o compromiso de los activos y la interrupción de las actividades de la organización.

4.6. Gestión de las Comunicación y Operaciones

Asegurar la operación correcta y segura de los medios de procesamiento de información, mantener el nivel apropiado de la seguridad de la información, minimizar el riesgo de las fallas de los sistemas, proteger la integridad del software, hacer una copia de respaldo de la información, asegurar la protección de la información en red.

Evitar la divulgación, modificación, eliminación no autorizada de los activos, mantener la seguridad de la información mediante acuerdos de intercambio con una entidad externa, detectar actividades de procesamiento de información no autorizados.

4.7. Control de Acceso

Controlar el acceso a la información, gestionar usuarios autorizados, evitar el acceso no autorizado a los servicios de red, sistemas operativos, sistemas de aplicación y asegurar la seguridad de la información cuando se use computación móvil y teletrabajo.

4.8. Adquisición, desarrollo y Mantenimiento de los Sistemas de Información

Asegurar que la seguridad sea parte integral de los SI, evitar errores, pérdida, modificación no autorizada en las aplicaciones, proteger la confidencialidad, autenticidad e integridad de la información, garantizar la seguridad de los archivos del sistema, reducir riesgos de las vulnerabilidades técnicas publicadas.

4.9. Gestión de un Incidente en la Seguridad de la Información

Asegurar que los eventos y debilidades en la seguridad de la información sea comunicada para tomar una decisión correctiva oportuna, y asegurar que se aplique un enfoque efectivo a la gestión de la seguridad de la información.

4.10. Gestión de la Continuidad Comercial

Contrarrestar las interrupciones de las actividades comerciales, y proteger los procesos comerciales críticos de los efectos de fallas.

4.11. Cumplimiento de los Requerimientos Legales

Evitar violaciones contra cualquier ley, obligación contractual y requerimiento de seguridad. Asegurar el cumplimiento de los sistemas con las políticas y estándares de seguridad organizacional, maximizar la efectividad y minimizar la interferencia del proceso de auditoría de los sistemas de información.

Nivel de Cobertura del Área de Soporte y Tecnologías de Información ISO 17799

Tabla 4.5. Nivel de Cobertura del Área de Soporte y TI.

Símbolo	Nivel de Cobertura según ISO 17799	Leyenda Descriptiva
	**Razonablemente cubierto**	Los requerimientos sugeridos por el equipo de trabajo basado en la ISO 17799 están razonablemente cubiertos.
	**Sustancialmente cubierto**	Falta realizar algunas actividades para cubrir razonablemente los requerimientos sugeridos por el equipo de trabajo basado en la ISO 17799.
	**Parcialmente cubierto**	Se han realizado actividades que cubren parcialmente los requerimientos sugeridos por el equipo de trabajo basado en la ISO 17799.
	**Limitadamente cubierto**	Se han realizado algunas actividades para cubrir los requerimientos sugeridos por el equipo de trabajo basado en la ISO 17799.
	**No cubierto**	No se ha realizado ninguna actividad relacionada con los requerimientos sugeridos por el equipo de trabajo basado en la ISO 17799.

4.1.5.2 **Análisis:** Diagnóstico de Seguridad de la Información para el Hospital San Juan Bautista Huaral

Tabla 4.6. Encuesta basada en la NTP/ IEC ISO 17799.

HOSPITAL SAN JUAN BAUTISTA HUARAL		
POLÍTICAS DE SEGURIDAD		
N°	**Pregunta**	**Respuesta**
1	¿Existen documento(s) de políticas de seguridad de S.I.?	Si, la institución cuenta con políticas de seguridad formales que indiquen los procedimientos de seguridad a ser

		adoptados para salvaguardar la información.
2	¿Se llega a comunicar los documentos de política de seguridad de de información a todos los empleados y entidades externas relevantes?	Si, la institución hace presente la comunicación de dichos documentos de seguridad, tanto de manera interna como externa.
3	¿Regularmente se realizan revisiones de la política de seguridad de información?	Dispone de una revisión de políticas de seguridad anualmente.

ORGANIZACIÓN DE LA SEGURIDAD

Organización Interna

N°	Pregunta	Respuesta
1	¿Existe un compromiso de la gerencia con la seguridad de información de la empresa?	Si, existe apoyo activo por parte de la gerencia para salvaguardar información de la institución.
2	¿Los representaste de la organización coordinan las actividades de seguridad de información?	Si, los distintos representantes de la organización coordinan las actividades en cuando a la seguridad de la información.
3	¿Existe un proceso de autorización para los medios de procesamiento de información?	Si, los componentes de hardware y software son verificados por el responsable del área para asegurar que todas las políticas y requerimientos de seguridad.
4	¿Se revisa regularmente los acuerdos de confidencialidad según las necesidades de la organización?	Si, se establecen los acuerdos de confidencialidad entre la institución y el cliente.
5	¿Se mantiene contacto con las autoridades de la empresa?	Se tiene un contacto, pero solo con algunas autoridades relevantes, no con

		todas las necesarias.
6	¿Se tiene contacto con grupos u otros foros de seguridad especializados en la seguridad de información?	No se tiene contacto con grupos u otros foros de seguridad especializados en la seguridad de información.
7	¿Existe una revisión independiente de la seguridad de información a intervalos planeados o cambios para la implementación de seguridad de información?	No existen revisiones independientes de la seguridad de la información.

Entidades Externas

N°	Pregunta	Respuesta
1	¿Existe un proceso para la identificación de riesgos relacionados con las entidades externas?	Si se logra identificar los riesgos de la información y los medios de procesamiento de información que involucran grupos externo
2	¿Se evalúa todos los requerimientos de seguridad antes de otorgar a los clientes acceso a la información?	Si, se evalúa todos los requerimientos de seguridad, luego se al cliente acceso a la información de la empresa
3	¿Existe un tratamiento de seguridad los contratos con terceras personas?	Si, existe un acuerdo de los clientes con la empresa que garantiza, procedimientos para proteger los activos: información, software, hardware. Sin alterar la confidencialidad, integridad, disponibilidad y cualquier otra propiedad relevante de los activos.

GESTIÓN DE ACTIVOS

Responsabilidad por los Activos		
1	¿Los activos están claramente identificados en el inventario?	Si, la empresa maneja un inventario actualizado de su activos tales como hardware, software, otros.
2	¿La información y activos tienen como propietarios a una parte designada por la organización?	Si, la empresa ha designado información y activos asociados con los medios de procesamiento de la información, pero solo a ciertas partes de la organización.
3	¿Se identifican documentan e implementan las reglas para el uso aceptable de información y activos?	Existen reglas, pero no están definidas para el uso aceptable de la información y los activos asociados a los medios de procesamiento de la información

Clasificación de la Información

N°	**Pregunta**	**Respuesta**
1	¿La información es clasificada en términos de su valor, requerimientos legales, confidencialidad y grado crítico para la organización?	Se realiza una clasificación de la información, pero solo de la información de alto riesgo; pero esta clasificación no está plasmado en un documento formal
2	¿Se ha desarrollado e implementado un apropiado conjunto de procedimientos para etiquetar y manejar la información?	Si, la empresa ha desarrollado e implantado un procedimiento para manejar en concordancia la información con el esquema de clasificación de la empresa.

SEGURIDAD LIGADA A LOS RECURSOS HUMANOS **Antes del Empleo**		
N°	**Pregunta**	**Respuesta**

2	¿Existe un control de selección a los candidatos a empleados?	Si, la empresa lleva a cabo chequeos de verificación de antecedentes de todos los candidatos, los cuales deben ser proporcionales a requerimientos de la empresa.
3	¿Existe una estipulación de términos y condiciones de empleo?	Los empleados firman un contrato estipulando términos y condiciones donde hay puntos sobre seguridad de la información.

Durante el Empleo

N°	Pregunta	Respuesta
1	¿Existe una gestión de responsabilidades hacia los empleados?	Si, cada miembro de la organización tiene sus funciones asignadas durante la jornada.
2	¿Existe una capacitación y educación en la seguridad de la información?	Se realizan capacitaciones, pero no periódicamente, tampoco se realizan talleres.
3	¿Existe un proceso disciplinario para los empleados que han cometido una violación en la seguridad?	Si, la empresa cuenta con un proceso en contra de indisciplina, y más aún cuando se trata de la seguridad de la información.

Terminación o Cambio de Empleo

N°	Pregunta	Respuesta
1	¿Se tiene definido y asignado claramente las responsabilidades para realizar terminación o cambio de empleo?	Si se tiene definido y asignado para un cambio de empleo, terminación de empleo o requerimiento de un nuevo personal, hay una comisión que la integra el jefe de RR.HH.
2	¿Existe un proceso de devolución de activos que estén en posición de los empleados?	Si, cada pertenencia del trabajador pasa por previa revisión con la finalidad de que no se filtre información.

SEGURIDAD FÍSICA Y DEL AMBIENTE

Áreas Seguras

N°	Pregunta	Respuesta
1	¿Existe un perímetro de seguridad física para proteger áreas que contienen información?	Si, la empresa cuenta con una seguridad perimetral para áreas que contiene información vital para la empresa (como por ejemplo la sala de servidores)
2	¿Existen controles de entrada físicos?	Si, la empresa cuenta con controles a dichas áreas que contienen información.
3	¿Existe seguridad en las oficinas, habitaciones y medios?	Dispone de controles de ingreso apropiados para las oficinas.
4	¿Se aplica protección contra las amenazas externas y ambientales?	Si se aplican medidas de protección.
5	¿Se tiene diseñado y aplicado la protección física y lineamientos para trabajar en áreas seguras?	Si, existen controles y restricciones en las diferentes áreas.
6	¿Existe un control a las áreas de acceso público, entrega y carga?	No existe dicho control.

Seguridad del Equipo

N°	Pregunta	Respuesta
1	¿Existe una correcta ubicación de los equipos para la reducción de riesgos de las amenazas?	Si, los equipos se encuentran ubicados estratégicamente para evitar cualquier tipo de incidente.
2	¿Existe un plan de acción si llegara a una interrupción un servicio público?	No se cuenta con dicho plan.

3	¿Existe una seguridad de cableado en la organización?	Si, la empresa cuenta con una seguridad de cableado para proteger al equipo informático de intercepción o daño.
4	¿Existe un control de manteniendo de equipos informáticos?	Si, existe en la empresa un correcto mantenimiento de hardware para permitir su continua disponibilidad.
5	¿A los equipos se les aplica seguridad cuando están fuera del local?	Si existen controles de seguridad para los equipos fuera de la empresa como cámaras de vigilancia, contraseñas en equipos informáticos.
6	¿Existe un control para el traslado de sin propiedad (equipo informático)?	Los equipos, software no son retirados antes una autorización por escrito.

GESTIÓN DE COMUNICACIONES Y OPERACIONES

Procedimiento y Responsabilidades Operacionales

N°	Pregunta	Respuesta
	¿Todos los procedimientos operativos identificados en la política de seguridad están documentados?	No, todos los procedimientos operativos en la política están documentados.
	¿Están establecidas las responsabilidades para controlar los cambio de equipos.	No, existen responsabilidades específicas.
	¿Existe una separación de los entornos	Si, la empresa creyó por conveniente

3	de desarrollo y producción?	separar dichos entornos para reducir los riesgos de acceso no autorizados

Gestión de la Entrega del Servicio de Terceros

N°	Pregunta	Respuesta
1	¿Se tiene un control para asegurar que los terceros implementen, operen y mantengan los controles de seguridad incluidos en el contrato?	La entrega de un servicio por tercero incluye los acuerdos de seguridad en el contrato.
2	**¿**Existe un monitoreo y revisión de servicios de terceros?	Si, existe un monitoreo y revisión por parte de servicios de terceros.
3	¿Se tiene un control del manejo de cambios en los servicios de terceros?	No existe dicho control.

Planeación y Aceptación del Sistema

N°	Pregunta	Respuesta
1	¿Se tiene un monitoreo de las proyecciones del uso de los recursos para asegurar el desempeño del sistema requerido?	No se realiza este monitoreo.
2	¿Existen criterios de aceptación de nuevos SI, incluyendo actualizaciones y nuevas versiones?	No, toco cambio a nivel de SI pasa por previa aprobación de la gerencia.

Protección Contra Software Malicioso y Código Móvil

N°	Pregunta	Respuesta
1	¿Existen controles contra software maligno?	Si, la empresa cuenta con controles de detección y prevención ante un software maligno.
	¿Existen Controles contra códigos	No se tiene implementado

2	móviles?	

Respaldo (Back-Up)

N°	Pregunta	Respuesta
1	¿Se realizan copias de back-up de la información esencial para el negocio?	Si, la empresa tiene establecido periodos para generar copias de seguridad de su información.

Gestión de Seguridad de Redes

N°	Pregunta	Respuesta
1	¿Existe algún control en las redes de la organización?	Si, la empresa cuenta con un control en las redes de la organización, para protegerlas de amenazas y mantener la seguridad de los sistemas
2	¿Se cuenta con seguridad en los servicios de red?	Si existe un manejo de privilegios en la red.

Gestión de Medios

N°	Pregunta	Respuesta
1	¿Existe procedimientos para la gestión de medios removibles?	La institución cuenta con procedimientos para la gestión de medios removibles
2	¿Existe procedimientos formales para la eliminación de medios?	Si, los documentos son eliminados y la información que se maneja en la empresa no sale de su establecimiento.
3	¿Se tiene establecido los procedimientos para el manejo y almacenaje de la información?	Si existe un procedimiento para manejo y almacenaje de información.
4	¿Se tiene protegido la documentación un acceso no autorizado?	Aseguran que existen usuarios responsables en el manejo de la documentación en caso de acceso no autorizado

Intercambio de Información

N°	Pregunta	Respuesta
1	¿Está establecidos procedimientos y políticas de información y software?	La empresa tiene establecido procedimientos y políticas de información y software.
2	¿Están establecidos los acuerdos para el intercambio de información y software entre la organización y entidades externas?	Si, la empresa ha establecido acuerdos para el intercambio de información y software con entidades externas.
3	¿Los medios físicos están protegidos contra el acceso no -autorizado?	Si, la empresa cuenta con una protección hacia los medios físicos contra el acceso no autorizado, mal uso, etc.
4	¿Los mensajes electrónicos están protegidos adecuadamente?	Se utilizan los sistemas de mensajería/ Google Apps como método de protección para los mensajes electrónicos
5	¿Están implementadas políticas y procedimientos para proteger la información asociada con la interconexión de los sistemas de información comercial?	La institución tiene implementadas políticas y procedimientos para proteger la información asociada con la interconexión de los sistemas de información comercial

Servicios de Comercio Electrónico

N°	Pregunta	Respuesta
1	¿Está protegida la información involucrada en el comercio electrónico?	Existe una protección en la transmisión de la información a través de redes públicas – tesoro público/ Ministerio de Economía

2	¿Esta protegía la información involucrada en las transacciones en línea?	Si, la información está protegida ante transacciones en línea, para evitar transacciones incompletas o rutas equivocadas.
3	¿La información disponible públicamente está protegida?	La institución tiene información disponible de domino público, que se encuentra protegida.

Monitoreo

N°	Pregunta	Respuesta
1	¿Existe un registro de auditoria?	La institución mantiene sus registros de actividades de auditoria, para poder utilizarlas en investigaciones futuras.
2	¿Existen procedimientos para el monitoreo del uso de medios de procesamiento de información?	Se tienen procedimientos establecidos para el monitoreo de información, mostrando el resultado de actividades.
3	¿Existe una protección de la información del registro de monitoreo?	La empresa utiliza procedimientos para monitorear el uso de los medios de procesamiento de información y el resultado de las actividades.
4	¿Se registra las actividades del administrador y operador del sistema?	Si se registran las actividades del administrador y operador del sistema
5	¿Se registran las fallas encontradas en el monitoreo?	Si se lleva el control de las fallas encontradas para la posterior corrección.

CONTROL DE ACCESOS

Requerimiento Comercial para el Control del Acceso

N°	Pregunta	Respuesta
1	¿Existe una política de control de accesos?	La institución documenta y revisa la política de control de acceso, con la finalidad de garantizar óptimos

		resultados.

Gestión del Acceso del Usuario

N°	Pregunta	Respuesta
1	¿Existe un procedimiento formal de registro y baja de accesos?	La institución cuenta con procedimientos formales para registrar y/o dar de bajar los accesos que se crean convenientes.
2	¿Se controla y restringe la asignación y uso de privilegios en entornos multiusuario?	Se mantiene controlado la asignación y uso de privilegios orientado a entornos multi-usuario.
3	¿Existe una gestión de los password de usuarios?	Existe un procedimiento de asignación de claves secretas a través del área de Informática
4	¿Existe una revisión de los derechos de acceso de los usuarios?	Periódicamente la gerencia revisa los derechos de acceso de los usuarios.

Responsabilidades del Usuario

N°	Pregunta	Respuesta
1	¿Existe el uso del password?	Los usuarios de la institución se basan en las políticas de seguridad, como el uso de password en sus equipos de trabajo.
2	¿Se protege el acceso de los equipos desatendidos?	Si están asegurado los equipos con el bloqueo de pantalla.
3	¿Existen políticas de limpieza en el puesto de trabajo?	Si, la empresa cuenta con dicha política de limpieza para los medios de procesamiento de información.

Control de Acceso a Redes

N°	Pregunta	Respuesta

1	¿Existe una política de uso de los servicios de red?	Existe una política en la cual los usuarios tienen accesos a los servicios que se les ha autorizado utilizar
2	¿Existe una autenticación de usuarios en conexiones externas?	La institución utiliza métodos para autenticar y controlar el acceso de usuarios remotos.
3	¿Se controla el acceso físico y lógico a los puertos?	La institución maneja procesos de identificación automática del equipo, para validar las conexiones.
4	¿Existe una segregación de redes?	La institución cuenta con grupos de trabajo, de esta maneja obtiene las redes segregadas para la mejor fluidez del negocio.
5	¿Existe un control de la conexión de redes?	Se tiene controlado el acceso físico y lógico de las estaciones (puertos) de trabajo.
6	¿Existe un control del routing (dispositivo para la interconexión de redes informáticas) de las redes internas y externas?	Existe un manejo de routing para controlar el número de conexiones de los usuarios.

Control de Acceso al Sistema de Operación

N°	Pregunta	Respuesta
1	¿Existe una identificación única de usuario y una automática de terminales?	Mantiene controles de identificación única para los usuarios y una automática para las terminales.
2	¿Existe una identificación y autenticación del usuario?	Existe identificación y autentificación del usuario para el uso exclusivo del personal.

3	¿Existe un sistema de gestión de clave?	La institución maneja un sistema de gestión de clave, que permite es esta cumplan un determinado nivel de seguridad, y que sean cambiadas periódicamente.
4	¿Existe un control con las sesiones inactivas?	Existe una política de seguridad que consiste en dar de baja las sesiones que se encuentran inactivas por un determinado periodo de tiempo.
5	¿Existe restricciones sobre los tiempos de conexión?	La institución no cuenta con restricciones de tiempo de conexión en las aplicaciones que utilizan sus usuarios.

Control de Acceso a la Aplicación e Información

N°	Pregunta	Respuesta
1	¿Existe Restricción al acceso de información?	Se restringe los accesos de los usuarios tanto a nivel de soporte como al de aplicación.
2	¿Existe un ambiente de cómputo dedicado a los sistemas sensibles?	No cuenta con un ambiente de cómputo dedicado a sistemas sensibles.

Computación Móvil y Teletrabajo

N°	Pregunta	Respuesta
1	¿Se ha incorporado medidas de seguridad a la computación móvil?	No ha incorporado medidas de seguridad orientadas a la computación móvil.
2	¿Está controlado el teletrabajo por la organización?	La organización no tiene completamente controlado el teletrabajo.

ADQUISICIÓN DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS

Requerimiento de Seguridad de los Sistemas

N°	Pregunta	Respuesta
1	¿Existen especificaciones de los requerimientos de seguridad?	Se toman en cuenta los requerimientos de las distintas áreas de la organización, con la finalidad de garantizar los niveles aceptables en la Seguridad de la información

Procesamiento correcto en las aplicaciones

N°	Pregunta	Respuesta
1	¿Existe un control de chequeos de validación?	Existen controles que validan las entradas de los datos que son procesados por las diversas aplicaciones.
2	¿Hay integridad en los mensajes de las aplicaciones?	Existen controles que garantizan la integridad en los mensajes que muestran las aplicaciones al término de cada proceso ejecutado.
3	¿Se valida el output de data de una aplicación?	Se validan los datos de salida de las aplicaciones.

Controles Criptográficos

N°	Pregunta	Respuesta
1	¿Existen políticas de controles criptográficos?	Existen políticas que garantizan la protección de la información mediante el encriptado.
2	¿Se utiliza una gestión de clave para dar soporte a las técnicas de criptografía en la organización?	Existe una gestión de clave al momento de proceder a encriptar o desencriptar la información.

Seguridad de los Archivos del Sistema

N°	Pregunta	Respuesta
1	¿Cuenta con un control para la instalación de software en los sistemas operacionales?	No se tiene establecido procedimientos para el control de instalación de software.
2	¿Cuenta con protección la data de prueba?	La organización cuenta con protección dirigida a la data de prueba.
3	¿Existe un control de acceso de código fuente del programa?	La organización guarda cuidadosamente el código fuente de sus aplicaciones con la finalidad que estas no sean alteradas.

Seguridad en los Procesos de Desarrollo y Soporte

N°	Pregunta	Respuesta
1	¿Existe un control para los procedimientos de controles de cambio?	Si la empresa cuenta con un procedimiento de controles de cambio
2	¿Existe la gestión de los cambios en los Sistemas Operativos (S.O.)?	Existen procedimientos establecidos antes de cambiar el sistema operativo de las estaciones de trabajos.
3	¿Existen restricciones sobre los cambios en los paquetes de software?	Se limita las modificaciones a los paquetes de software.
4	¿Hay un control para evitar las filtraciones de información?	Existen controles para evitar las filtraciones de información.

Gestión de Vulnerabilidad Técnica

N°	Pregunta	Respuesta
1	¿Se controlan las vulnerabilidades de los equipos?	Si se controla obteniendo oportunamente la información sobre las vulnerabilidades técnicas de los sistemas de información, aunque solo toman medidas apropiadas los riegos.

ADMINISTRACIÓN DE INCIDENTES

Reporte de Eventos y Debilidades en la Seguridad de la Información

N°	Pregunta	Respuesta
1	¿Se comunican los eventos de seguridad?	Cuenta con procesos que reportan eventos de seguridad lo más rápido posible a los canales gerenciales.
2	¿Se comunican las debilidades de seguridad?	Los miembros de la organización se encuentran capacitados para reportar cualquier debilidad observada en la seguridad de los servicios o sistemas.

Gestión de Incidentes y Mejoras en la Seguridad de la Información

N°	Pregunta	Respuesta
1	¿Están definidas las responsabilidades antes de un incidente?	Si se ha establecido responsabilidades y procedimientos gerenciales que aseguran una respuesta rápida, efectiva y ordenada de los incidentes de seguridad de información.

Gestión de Incidentes y Mejoras en la Seguridad de la Información

N°	Pregunta	Respuesta
2	¿Existe mecanismos para permitir cuantificar y monitorear los incidentes de la S.I?	Se llegan a cabo mecanismos que permiten monitorear y cuantificar incidentes en la seguridad de la información.
3	¿Existe una recolección de evidencia cuando un incidente involucra acciones legales?	La institución efectúa una recolección de evidencia cuando un incidente involucra acciones legales.

GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

Aspectos de la Seguridad de la Información de la Gestión de la Continuidad Comercial

N°	Pregunta	Respuesta
1	Existen procesos para la gestión de la continuidad.	Cuenta con procesos establecidos que gestiones la continuidad del negocio.
2	Existe un plan de continuidad del negocio y análisis de impacto.	La institución tiene constituida un plan de continuidad y análisis de impacto que entrará en ejecución si ocurriese un evento que interrumpa los procesos comerciales.
3	Existe un diseño, redacción e implantación de planes de continuidad.	Existen colaboradores que se encargan del diseño, redacción e implantación de plan de continuidad.
4	Existe un marco de planificación para la continuidad del negocio.	La institución contempla un marco de planificación para la continuidad del negocio.
5	Existen prueba, mantenimiento y revisiones de los planes de continuidad del negocio.	Periódicamente se realiza revisiones al plan de continuidad de negocio para mantenerlo actualizado ante posibles eventos que llegasen a ocurrir.

CUMPLIMIENTO

Cumplimiento con requerimientos legales

N°	Pregunta	Respuesta
1	Se tiene en cuenta el cumplimiento con la legislación por parte de los sistemas.	Actualiza periódicamente los documentos como políticas y estándares de seguridad.
2	Existe el resguardo de la propiedad intelectual.	Cuenta con procedimientos que aseguran el cumplimiento de los requerimientos legislativos, reguladores sobre el uso de material con respecto a los derechos de propiedad intelectual.
3	Existe el resguardo de los registros de la organización.	La institución mantiene protegido los registros importantes para la organización para que no suceda perdida, falsificación o destrucción.
4	Existe la protección de data y privacidad de información personal	Garantiza total protección y privacidad tal como lo requiere la legislación.
5	Se emplean controles criptográficos en el cumplimiento de leyes y regulaciones	Se emplean controles criptográficos. Utiliza controles en cumplimientos de acuerda a ley y regulaciones relevantes.

Cumplimiento con las políticas y estándares de seguridad y el cumplimiento técnico

N°	Pregunta	Respuesta
1	Existe cumplimiento con las políticas y estándares de seguridad	Cumple con los procedimientos de seguridad como políticas y estándares.
2	Hay un control del cumplimiento técnico.	Se efectúan chequeos regulares a los sistemas de información para el cumplimiento con estándares de seguridad

Consideraciones de auditoria de los sistemas de información

N°	Pregunta	Respuesta
1	Existe cumplimiento con las políticas y estándares de seguridad	Cumple con los procedimientos de seguridad como políticas y estándares.
2	Se protege las herramientas de auditoria de los SI. Si se protege a las herramientas de auditoria de los sistemas, para evitar algún posible mal uso.	

4.1.5.3. **Informe**: Diagnóstico de Seguridad de la Información para el Hospital San Juan Bautista Huaral

I. RESUMEN EJECUTIVO

De acuerdo a las normas internacionales y estándares de calidad, ISO/IEC 27001 e ISO/IEC 17799 que ha sido preparado para proporcionar un modelo que establece, implementa, opera, monitorea, revisa, mantiene y mejora un sistema de gestión de seguridad de la información, este debe contar con un Plan de Seguridad de la Información. Sin embargo, a partir de la información proporcionada por la institución, se ha podido establecer que no existe una política de seguridad establecida.

Si bien existen directivas definidas en el área de seguridad informática con respecto a la seguridad lógica y física de los sistemas de Información e información en general, estos han sido establecidos en gran medida por el conocimiento de mejores prácticas de los responsables de cada una de las áreas, ya que ellos son los encargados de transmitir estos conocimientos.

1.1. Objetivo y Alcance

Objetivo

- El objetivo de este trabajo es asesorar al Hospital San Juan Bautista Huaral para que puedan tener un plan de acción identificando los riesgos de la información y la tecnología, sirviendo de guía la ISO/IEC 17799. Cabe resaltar que al culminar este presente informe la institución debe evaluar y llegar a cabo la ejecución de las actividades aquí mencionadas.

1.2 Alcance del Trabajo

El alcance del informe comprende:

- Administración del área de TI Estructura organizacional.
- Procedimientos para combatir o mitigar los riesgos.
- Aspectos de la Seguridad físicas y lógicas.
- Acatar la normal de la ISO/EIC 17799.
- Prevenir las inseguridades. Auditoria

II. METODOLOGIA

Durante el desarrollo del trabajo de auditoria se utilizarán diferentes metodologías como las normas ISO 17799 e ISO 27001. El marco de riesgos de TI los cuales aseguraran que se contemple la totalidad de los aspectos relevantes de la seguridad de información que nos ayudaran en el diagnóstico de la misma y que representan el criterio de evaluación.

La relación de las metodologías utilizadas y el alcance de las mismas se resumen a continuación.

Tabla 4.7. Metodologías y alcance.

Base Teórica	**Alcance**
ISO/IEC 17799	Norma Internacional para la Gestión de Seguridad de la Información
ISO/IEC 27001	Norma Internacional para Sistemas Gestión de Seguridad de la Información
Marco de Riesgos	Marco de Gestión de Riesgos relacionados con la Tecnología de Información

La aplicación de estas metodologías permitió desarrollar un trabajo a la medida de las características y necesidades del Hospital San Juan Bautista Huaral, concentrando esfuerzos en los temas más significativos.

Nuestras metodologías se basan en un marco global e integrado definido en los principios Objetivos, Riesgos, Controles y Alineamiento (ORCA). ORCA ayuda a las organizaciones a alinear sus objetivos estratégicos con sus propios riesgos y controles. ORCA es una metodología de la gestión de riesgos que supervisa constantemente el efecto de un cambio en la interna o externa de proceso dentro de una organización. Muestra cómo la organización, las unidades de negocio y los procesos de negocio y priorizar describen individualmente sus estrategias y objetivos de negocio. Basado en la premisa de que los riesgos deben ser gestionados con el fin de oportunidades en la planificación específica de los procesos de gestión y control de riesgos para hacer frente a posibles amenazas y oportunidades, ayudando a la organización a alinear sus objetivos estratégicos con sus propios riesgos, controles y procesos.

III. PROCEDIMIENTO UTILIZADO

Durante el desarrollo del presente informe se hará uso de herramientas como la entrevista y el cuestionario dirigido al personal, asegurándonos que la encuesta tenga las preguntas esenciales para la investigación basadas en las ISO mencionadas anteriormente.

Esto la finalidad de obtener la información correspondiente y así poder estimar el nivel de cumplimiento de la institución.

IV. ANÁLISIS DE BRECHA

Tabla 4.8. Análisis de Brecha

Símbolo	Nivel de Cobertura	Leyenda Descriptiva
	**Razonablemente cubierto**	Los requerimientos sugeridos por el equipo de trabajo basado en la ISO 17799 están razonablemente cubiertos.
	**Sustancialmente cubierto**	Falta realizar algunas actividades para cubrir razonablemente los requerimientos sugeridos por el equipo de trabajo basado en la ISO 17799.
	**Parcialmente cubierto**	Se han realizado actividades que cubren parcialmente los requerimientos sugeridos por el equipo de trabajo basado en la ISO 17799.
	**Limitadamente cubierto**	Se han realizado algunas actividades para cubrir los requerimientos sugeridos por el equipo de trabajo basado en la ISO 17799.
	**No cubierto**	No se ha realizado ninguna actividad relacionada con los requerimientos sugeridos por el equipo de trabajo basado en la ISO 17799.

V. PROCESAMIENTO

5.1. Levantamiento De Información

El Hospital San Juan Bautista Huaral cuenta con directivas que establece el área de cómputo para la administración de la red y gestión de la información, políticas de seguridad lógica tiene los backups de los servidores,

actualizaciones de antivirus, en seguridad física sensores de fuego y extintores en cada oficina y áreas de la planta y brigadas por parte del personal entre otros. Revisión y análisis de la información proporcionada por el personal de la empresa.

5.2. Comparación Y Evaluación De Resultados

En el siguiente cuadro comparativo contrastara los resultados obtenidos de los cuestionarios y entrevistas a los jefes de las diferentes áreas de TI de la organización con los controles establecidos en el estándar internacional ISO/IEC 27001 e ISO/IEC 17799.

Situación Actual	Mejores Practicas	Análisis De Brecha
1. Políticas De Seguridad		
1.1. Políticas de Seguridad		
• El Hospital San Juan Bautista Huaral cuenta con políticas de seguridad formales que indiquen los procedimientos de seguridad a ser adoptados para salvaguardar la información.	• La gerencia debe aprobar un documento de política, este se debe publicar y comunicar a todos los empleados y entidades externas relevantes.	
• Si, la institución hace información	· La política de seguridad de la	

presente documentos de seguridad, tanto de manera interna como externa. • Dispone de una revisión de políticas de seguridad anualmente.	debe ser revisada regularmente a intervalos planeados o si ocurren cambios significativos para asegurar la continua idoneidad, eficiencia y efectividad.
2. Organización de la seguridad	
2.1. Organización Interna	
• Existe apoyo activo por parte de la gerencia para salvaguardar información de la empresa. • Los distintos representantes de la organización coordinan las actividades en cuando a la seguridad de la información.	• La gerencia debe apoyar activamente la seguridad dentro de la organización a través de una dirección clara, compromiso demostrado, asignación explicita y reconocimiento de las responsabilidades de la seguridad de la información.

Fuente: Elaboración propia

Situación Actual	Mejores Practicas	Análisis De Brecha
Organización Interna		
• Los componentes de hardware y software son verificados por el responsable del área para asegurar que todas las políticas y requerimientos de seguridad. • Se establecen los acuerdos de confidencialidad entre la empresa y cliente. • Se tiene un contacto, pero solo con algunas autoridades relevantes, no con todas las necesarias. • No existen revisiones independientes de la seguridad de la información.	• Las actividades de seguridad de la información deben ser coordinadas por representantes de las diferentes partes de la organización con las funciones y roles laborales relevantes. • Se deben definir claramente las responsabilidades de la seguridad de la información. • Se debe definir e implementar un proceso de autorización gerencial para los nuevos medios de procesamiento de información. • Se deben identificar y revisar regularmente los requerimientos de confidencialidad o los acuerdos de no divulgación reflejando las necesidades de la organización para la protección de la información.	

Situación Actual	Mejores Practicas	Análisis De Brecha
Organización Interna		
	• Se debe mantener los contactos apropiados con las autoridades relevantes. • Se deben mantener contactos apropiados con los grupos de interés especial u otros foros de seguridad especializados y asociaciones rofesionales. • El enfoque de la organización para manejar la seguridad de la información y su implementación (es decir; objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información) se debe revisar independientemente a intervalos planeados, o cuando ocurran cambios significativos para la implementación de la seguridad.	

Situación Actual	Mejores Practicas	Análisis De Brecha
2.2. Entidades Externas		
• La organización logra identificar los riesgos de la información y los medios de procesamiento de información que involucran grupos externo. • Se evalúa todos los requerimientos de seguridad, luego se al cliente acceso a la información de la empresa. • Existe un acuerdo de los clientes con la empresa que garantiza, procedimientos para proteger los activos: información, software, hardware; sin alterar la confidencialidad, integridad, disponibilidad y cualquier otra propiedad relevante de los activos.	Se deben identificar los riesgos que corren la información y los medios de procesamiento de información de la organización y se deben implementar los controles apropiados antes de otorgar acceso. Se deben tratar todos los requerimientos de seguridad identificados antes de otorgar a los clientes acceso a la información o activos de la organización. Los acuerdos que involucran acceso, procesamiento, comunicación o manejo por parte de terceras personas a la información o los medios de procesamiento de información de la organización; agregar productos o servicios a los medios de procesamiento de la información deben abarcar los requerimientos de seguridad necesarios relevantes.	

.

Situación Actual	Mejores Practicas	Análisis De Brecha
3. Gestión De Activos		
3.1. Responsabilidad Por Los Activos		
• La institución maneja un inventario actualizado de sus activos tales como hardware, software, otros. • La institución ha designado información y activos asociados con los medios de procesamiento de la información, pero solo a ciertas partes de la organización. • Existen reglas pero no están bien definidas para el uso aceptable de la información y los activos asociados a los medios de procesamiento de la información, solo se tiene conocimiento verbalmente y se hace conocer a los usuarios y algo de esto está plasmado en sus directivas	• Todos los activos deben estar claramente identificados; y se debe elaborar y mantener un inventario de todos los activos importantes. • Toda la información y los activos asociados con los medios de procesamiento de la información deben ser propiedad de una parte designada de la organización. • Se deben identificar, documentar e implementar las reglas para el uso aceptable de la información y los activos asociados con los medios de procesamiento de la información.	
3.2. Clasificación De La Información		
• Se realiza una clasificación de la información, pero solo de la información de alto riesgo; pero esta clasificación no está plasmado en un documento formal.	• La información debe ser clasificada en términos de su valor, requerimientos legales, confidencialidad y grado crítico para la organización	

Situación Actual	Mejores Practicas	Análisis De Brecha
Clasificación De La Información		
•La empresa ha desarrollado e implantado un procedimiento para manejar en concordancia la información con el esquema de clasificación de la empresa.	• Se debe desarrollar e implementar un apropiado conjunto de procedimientos para etiquetar y manejar la información en concordancia con el esquema de clasificación adoptado por la organización.	
4. Seguridad Ligada A Los Recursos Humanos		
4.1. Antes Del Empleo		
• La empresa lleva a cabo chequeos de verificación de antecedentes de todos los candidatos, los cuales deben ser proporcionales a los requerimientos de la empresa.	• Se deben llevar a cabo chequeos de verificación de antecedentes de todos los candidatos a empleados, contratistas y terceros en concordancia con las leyes, regulaciones y ética relevante, y deben ser proporcionales a los requerimientos comerciales, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos.	

.

Fuente: Elaboración propia

Situación Actual	Mejores Practicas	Análisis De Brecha
Antes Del Empleo		
La empresa tiene estipulado los roles de los empleados. Los empleados firman un contrato estipulando términos y condiciones donde hay puntos sobre seguridad de la información.	Se deben definir y documentar los roles y responsabilidades de seguridad de los empleados, contratistas y terceros en concordancia con la política de la seguridad de información de la organización. Como parte de su obligación contractual; los empleados, contratistas y terceros deben aceptar y firmar los términos y condiciones de su contrato de empleo, el cual debe establecer sus responsabilidades y las de la organización para la seguridad de la información.	
4.2. Durante El Empleo		

Situación Actual	Mejores Practicas	Análisis De Brecha
Durante El Empleo		
• Se realizan capacitaciones, pero no periódicamente, tampoco se realizan talleres. • La empresa cuenta con un proceso en contra de indisciplina, y más aún cuando se trata de la seguridad de la información.	Todos los empleados de la organización y, cuando sea relevante, los contratistas y terceros, deben recibir el apropiado conocimiento, capacitación y actualizaciones regulares de las políticas y procedimientos organizacionales, conforme sean relevantes para su función laboral. Debe existir un proceso disciplinario formal para los empleados que han cometido una violación en la seguridad.	

4.3. Terminación O Cambio De Empleo

• Se tiene definido y asignado para un cambio de empleo, terminación de empleo o requerimiento de un nuevo personal, hay una comisión que la integra el jefe de RR.HH. • Cada pertenencia del trabajador pasa por previa revisión con la finalidad de que no se filtre información.	Se deben definir y asignar claramente las responsabilidades para realizar la terminación o cambio del empleo. Todos los empleados, contratistas y terceros deben devolver todos los activos de la organización que estén en su posesión a la terminación de su empleo, contrato o acuerdo.	

Situación Actual	Mejores Practicas	Análisis De Brecha
Terminación O Cambio De Empleo		
La empresa cuenta con un control de accesos de usuarios (empleados), eliminando cuentas de usuario a empleados que ya no laboran en la empresa.	Los derechos de acceso de todos los empleados, contratistas y terceros a la información y medios de procesamiento de la información deben ser eliminados a la terminación de su empleo, contrato o acuerdo, o se deben ajustar al cambio.	
5. Seguridad Física Y Ambiental		

5.1. Áreas Seguras

• La empresa cuenta con una seguridad perimetral para áreas que contiene información vital para la empresa (como por ejemplo la sala de servidores). • La organización cuenta con controles establecidos a dichas áreas que contienen la información.	□ Se debe utilizar perímetros de seguridad (barreras tales como paredes y puertas de ingreso controlado o recepcionistas) para proteger áreas y medios de procesamiento de información. □ Se deben proteger las áreas seguras mediante controles de entrada apropiados para asegurar que sólo se permita acceso al personal autorizado. Se debe diseñar y aplicar seguridad física en las oficinas, habitaciones y medios.

Situación Actual	Mejores Practicas	Análisis De Brecha
Áreas Seguras		
• Dispone de controles de ingreso apropiados para las oficinas. • El Hospital San Juan Bautista Huaral maneja diseños de protección física en caso suceda cualquier evento que atente contra los activos del negocio. • Existen controles y restricciones en las diferentes áreas. • No existe un control a las áreas de acceso público, entrega y carga.	• Se debe diseñar y aplicar protección física contra daño por fuego, inundación, terremoto, explosión, disturbios civiles y otras formas de desastre natural o creado por el hombre. • Se debe diseñar y aplicar protección física y lineamientos para trabajar en áreas seguras. • Se deben controlar los puntos de acceso como las áreas de entrega y descarga y otros puntos donde personas no autorizadas pueden ingresar a los locales, y cuando fuese posible, se deben aislar de los medios de procesamiento de la información para evitar un acceso no autorizado.	
5.2. Seguridad Del Equipo		
Los equipos se encuentran ubicados estratégicamente para evitar cualquier tipo de incidente.	El equipo debe estar ubicado o protegido para reducir los riesgos de las amenazas y peligros ambientales, y las oportunidades para el acceso.	

.

Situación Actual	Mejores Practicas	Análisis De Brecha
Seguridad Del Equipo		
• No existe un plan de acción si llegara a una interrupción un servicio público • La empresa cuenta con una seguridad de cableado para proteger al equipo informático de intercepción o daño. • Existe en la empresa un correcto mantenimiento de hardware para permitir su continua disponibilidad. • Existen controles de seguridad para los equipos fuera de la empresa como cámaras de vigilancia, contraseñas en equipos informáticos. • Se mantienen controles para la eliminación segura de información y es posible poder recuperar la información eliminada. • Los equipos, software no son retirados sin antes una autorización por escrito.	El equipo debe ser protegido de fallas de energía y otras interrupciones causadas por fallas en los servicios públicos. El cableado de la energía y las telecomunicaciones que llevan data o sostienen los servicios de información deben ser protegidos de la intercepción o daño. El equipo debe ser mantenido correctamente para permitir su continua disponibilidad e integridad. Se debe aplicar seguridad al equipo fuera del local tomando en cuenta los diferentes riesgos de trabajar fuera del local de la organización. Todos los ítems de equipo que contengan medios de almacenaje deben ser chequeados para asegurar que se haya removido o sobre-escrito de manera segura cualquier data confidencial y software con licencia antes de su eliminación.	

Situación Actual	Mejores Practicas	Análisis De Brecha
6. Gestión De Comunicaciones Y Operaciones		
6.1. Procedimiento Y Responsabilidades Operacionales		
• No todos los procedimientos operativos en la política están documentados. • No están establecidas las responsabilidades para controlar los cambios en equipos. • Se han segregado los deberes y áreas de responsabilidad ante cual incidente que ocurra. • La empresa creyó por conveniente separar dichos entornos para reducir los riesgos de acceso no autorizados.	Se deben documentar y mantener los procedimientos de operación, y se deben poner a disposición de todos los usuarios que los necesiten. Se deben controlar los cambios en los medios y sistemas de procesamiento de la información. Se deben segregar los deberes y áreas de responsabilidad para reducir las oportunidades de una modificación no autorizada o no-intencionada o un mal uso de los activos de la organización. Se deben separar los medios de desarrollo, prueba y operacionales para reducir los riesgos de accesos no-autorizados o cambios en el sistema de operación.	

.

Situación Actual	Mejores Practicas	Análisis De Brecha
6.2. Gestión De La Entrega Del Servicio De Terceros		
• La entrega de un servicio por tercero incluye los acuerdos de seguridad en el contrato. • Existe monitoreo y revisión por parte de servicios de terceros. • Carece de controles de manejo de cambios en los servicios de terceros.	Se debe asegurar que los terceros implementen, operen y mantengan los controles de seguridad, definiciones de servicio y niveles de entrega incluidos en el contrato de entrega del servicio de terceros. Los servicios, reportes y registros provistos por terceros deben ser monitoreados y revisados regularmente, y las auditorías se deben llevar a cabo regularmente. Se deben manejar los cambios en la provisión de servicios, incluyendo el mantenimiento y mejoramiento de las políticas, procedimientos y controles de seguridad existentes, tomando en cuenta el grado crítico de los sistemas y procesos comerciales involucrados y la reevaluación de los riesgos.	

Situación Actual	Mejores Practicas	Análisis De Brecha
6.3. Planeación Y Aceptación Del Sistema		
• No se tiene un monitoreo de las proyecciones del uso de los recursos para asegurar el desempeño del sistema requerido. • La institución carece de criterios de aceptación hacia los nuevos sistemas de información, incluyendo actualizaciones y nuevas versiones.	Se deben monitorear, afinar y realizar proyecciones del uso de los recursos para asegurar el desempeño del sistema requerido. • Se deben establecer los criterios de aceptación para los sistemas de información nuevos, actualizaciones y versiones nuevas y se deben llevar a cabo pruebas adecuadas del (los) sistema(s) durante su desarrollo y antes de su aceptación.	
6.4. Protección Contra Software Malicioso Y Código Móvil		
• La empresa cuenta con controles de detección y prevención ante un software maligno. • No existen controles contra códigos móviles.	• Se deben implementar controles de detección, prevención y recuperación para protegerse de códigos malicioso. • Cuando se autoriza el uso de un código móvil, a configuración debe asegurar que el código móvil autorizado opere de acuerdo a una política de seguridad claramente definida, y se debe evitar que se ejecute un código móvil no-autorizado	

Situación Actual	Mejores Practicas	Análisis De Brecha
6.5. Respaldo (Back-Up)		
□ La institución tiene establecido periodos para generar copias de seguridad de su información.	□ Se deben realizar copias de back-up o respaldo de la información comercial y software esencial y se deben probar regularmente de acuerdo a la política.	
6.6. Gestión De Seguridad De Redes		
• La institución cuenta con un control en las redes de la organización, para protegerlas de amenazas y mantener la seguridad de los sistemas. • El Hospital San Juan Bautista Huaral cuenta con un manejo de privilegios en la red(es) de la empresa de la cual se encarga el administrador de redes.	□ Las redes deben ser adecuadamente manejadas y controladas para poderlas proteger de amenazas, y para mantener la seguridad de los sistemas y aplicaciones utilizando la red, incluyendo la información en tránsito. Se deben identificar los dispositivos de seguridad, niveles de servicio y los requerimientos e incluirlos en cualquier contrato de servicio de red, ya sea que estos servicios sean provistos en-casa o sean abastecidos externamente.	

Situación Actual	Mejores Practicas	Análisis De Brecha
6.7. Gestión de Medios		
• El Hospital San Juan Bautista Huaral e cuenta con procedimientos para la gestión de medios removibles. • Los documentos son eliminados y la información que se maneja en la empresa no sale de su establecimiento. • Existe un procedimiento para manejo y almacenaje de información. • El Hospital San Juan Bautista Huaral asegura que existan usuarios responsables en el manejo de la documentación en caso de acceso no autorizado.	Deben existir procedimientos para la gestión de medios removibles. Los medios deben ser eliminados utilizando procedimientos formales y de una manera segura cuando ya no se les requiere. Se deben establecer los procedimientos para el manejo y almacenaje de la información para proteger dicha información de una divulgación no autorizada o un mal uso. Se debe proteger la documentación de un acceso no autorizado.	
6.8. Intercambio De Información		
• La institución tiene establecido procedimientos y políticas de información y software.	• Se deben establecer política, procedimientos y controles de intercambio formales para proteger el intercambio de información a través del uso de todos los tipos de medios de comunicación.	

Situación Actual	Mejores Practicas	Análisis De Brecha
Intercambio De Información		
• La institución ha establecido acuerdos para el intercambio de información y software con entidades externas. • Se cuenta con una protección hacia los medios físicos contra el acceso no autorizado, mal uso, etc. • Se utilizan los sistemas de mensajería/ Google Apps como método de protección para los mensajes electrónicos • El Hospital San Juan Bautista Huaral tiene implementadas políticas y procedimientos para proteger la información asociada con la interconexión de los sistemas de información comercial.	Se deben establecer acuerdos para el intercambio de información y software entre la organización y entidades externas. Los medios que contienen información deben ser protegidos contra un acceso no-autorizado, mal uso o corrupción durante el transporte más allá de los límites físicos de una organización. Se debe proteger adecuadamente los mensajes electrónicos. Se deben desarrollar e implementar políticas y procedimientos para proteger la información asociada con la interconexión de los sistemas de información comercial.	

6.9. Servicio De Comercio Electrónico	
• El hospital San Juan Bautista Huaral tiene información disponible de dominio público, que es protegida.	• Se debe proteger la integridad de la información disponible públicamente para evitar la modificación no autorizada. 

Fuente: Elaboración propia

Hospital San Juan

Situación Actual	Mejores Practicas	Análisis De Brecha
Servicio De Comercio Electrónico		
• Existe una protección en la transmisión de la información a través de redes públicas, tesoro público Ministerio de Economía. • La información está protegida ante transacciones en línea, para evitar transacciones incompletas o rutas equivocadas.	Se debe proteger la información involucrada en el comercio electrónico que se trasmite a través de redes públicas de cualquier actividad fraudulenta, disputa contractual y divulgación y modificación no autorizada. Se debe proteger la información involucrada en las transacciones en-línea para evitar la transmisión incompleta, rutas equivocadas, alteración no autorizada del mensaje, divulgación no-autorizada, y duplicación o reenvío no autorizado del mensaje.	

6.10. Monitoreo

El Hospital San Juan Bautista Huaral mantiene sus registros de actividades de auditoria, para poder utilizarlas en investigaciones futuras.	Se deben producir registros de la actividades de auditoria, excepciones y eventos de seguridad de la información y se deben mantener durante un período acordado para ayudar en investigaciones futuras y monitorear.	

Situación Actual	Mejores Practicas	Análisis De Brecha
Se tienen procedimientos establecidos para el monitoreo de información, mostrando el resultado de actividades. • La institución utiliza procedimientos para monitorear el uso de los medios de procesamiento de información y el resultado de las actividades. • Se registran las actividades del administrador y operador del sistema. • Se lleva el control de las fallas encontradas para la posterior corrección.	Se deben establecer procedimientos para monitorear el uso de los medios de procesamiento de información y el resultado de las actividades de monitoreo se debe revisar regularmente. Se deben establecer procedimientos para monitorear el uso de los medios de procesamiento de información y el resultado de las actividades de monitoreo se debe revisar regularmente. Se deben proteger los medios de registro y la información del registro contra alteraciones y acceso no-autorizado. Se deben registrar las actividades del administrador y operador del sistema. Las fallas se deben registrar, analizar y se debe tomar la acción apropiada. Los relojes de los sistemas de procesamiento de información relevantes de una organización o dominio de seguridad deben estar sincronizados con una fuente de tiempo exacta	

Situación Actual	Mejores Practicas	Análisis De Brecha
7. Control De Accesos		
7.1. Requerimiento Comercial Para El Control Del Acceso		
• La institución documenta y revisa la política de control de acceso, con la finalidad de garantizar óptimos resultados.	• Se debe establecer, documentar y revisar la política de control de acceso en base a los requerimientos de seguridad y comerciales	
Gestión Del Acceso Del Usuario		
• La institución cuenta con procedimientos formales para registrar y/o dar de bajar los accesos que se crean convenientes. • Asimismo, se mantiene controlado la asignación y uso de privilegios orientado a • entornos multi-usuario. • Existe procedimientos para la asignación de claves secretas a través del área de Informática. • Periódicamente la gerencia revisa los derechos de acceso de los usuarios.	• Debe existir un procedimiento formal para la inscripción y desinscripción para otorgar acceso a todos los sistemas y servicios de información. • Se debe restringir y controlar la asignación y uso de los privilegios. • La asignación de claves se debe controlar a través de un proceso de gestión formal. • La gerencia debe revisar los derechos de acceso de los usuarios a intervalos regulares utilizando un proceso formal.	

Situación Actual	Mejores Practicas	Análisis De Brecha
7.2. Responsabilidades Del Usuario		
• Los usuarios de la institución se basan en las políticas de seguridad, como el uso de password en sus equipos de trabajo. • El Hospital San Juan Bautista Huaral asegura los equipos mediante el bloqueo de pantalla con la finalidad de que la información que se maneja en una estación de trabajo no sea extraída. • La institución cuenta con política de limpieza para los medios de procesamiento de información. • Se debe requerir que los usuarios sigan	buenas prácticas de seguridad en la selección y uso de claves. • Se debe requerir que los usuarios se aseguren de dar la protección apropiada al equipo desatendido. • Se debe adoptar una • política de escritorio limpio para los documentos y medios de almacenaje removibles y una política de pantalla limpia para los medios de procesamiento de la información.	
7.3. Control De Acceso A Redes		
• Existe una política en la cual los usuarios tienen accesos a los servicios que se les ha autorizado utilizar. • Se tiene controlado el acceso físico y lógico de las estaciones (puertos) de trabajo.	• Los usuarios sólo deben tener acceso a los servicios para los cuales han sido específicamente autorizados a usar. • Se debe utilizar métodos de autenticación para controlar el acceso de usuarios remotos.	

Fuente: Elaboración propia

Situación Actual	Mejores Practicas	Análisis De Brecha
Control De Acceso A Redes		
• El Hospital San Juan Bautista Huaral utiliza métodos para autenticar y controlar el acceso de usuarios remotos. • La institución maneja procesos de identificación automática del equipo, para validar las conexiones. • El Hospital San Juan Bautista Huaral cuenta con grupos de trabajo, de esta maneja obtiene las redes segregadas para la mejor fluidez del negocio. • Existe un manejo de routing para controlar el número de conexiones de los usuarios. • Se debe considerar la identificación automática del equipo como un medio para autenticar las conexiones desde equipos y ubicaciones específicas. • Los servicios de información, usuarios y sistemas de información se deben segregar en las redes.	• Se debe restringir la capacidad de conexión de los usuarios en las redes compartidas, especialmente aquellas que se extienden a través de los límites organizaciones, en concordancia con la política de control de acceso y los requerimientos de las aflicciones comerciales. • Se deben implementar controles "routing" para las redes para asegurar que las conexiones de cómputo y los flujos de información no infrinjan la política de control de acceso de las aplicaciones comerciale	

Fuente: Elaboración propia

Evaluación de Riesgo para Bautista Huaral

Situación Actual	Mejores Practicas	Análisis De Brecha
7.4. Control De Acceso Al Sistema De Operación		
• Mantiene controles de identificación única para los usuarios y una automática para las terminales. • Existe identificación y autentificación del usuario para el uso exclusivo del personal. • La institución maneja un sistema de gestión de clave, que permite es esta cumplan un determinado nivel de seguridad, y que sean cambiadas periódicamente. • Existe una política de seguridad que consiste en dar de baja las sesiones que se encuentran inactivas por un determinado periodo de tiempo. • La institución no cuenta con restricciones de tiempo de conexión en las aplicaciones que utilizan sus usuarios. • Se debe controlar el acceso los servicios operativos mediante un procedimiento de registro seguro.	• Todos los usuarios deben tener un identificador singular (ID de usuario) para su uso personal y exclusivo, se debe elegir una técnica de autenticación adecuada para verificar la identidad del usuario. • Los sistemas de manejo de claves deben ser interactivos y deben asegurar la calidad de las claves. • Se debe restringir y controlar estrictamente el uso de los programas de utilidad que podrían superar al sistema y los controles de aplicación. • Las sesiones inactivas deben cerrarse después de un período de inactividad definido. • Se debe utilizar restricciones sobre los tiempos de conexión para proporcionar seguridad adicional a las aplicaciones de alto riesgo.	

Fuente: Elaboración propia

Situación Actual	Mejores Practicas	Análisis De Brecha
7.5. Control De Acceso A La Aplicación E Información		
• Restringe los accesos de los usuarios tanto a nivel de soporte como al de aplicación. • No cuenta con un ambiente de computo dedicado a sistemas sensibles	• Se debe restringir el acceso de los usuarios y personal de soporte al sistema de información y aplicación en concordancia con la política de control de acceso definida. • Los sistemas sensibles deben tener un ambiente de computo dedicado (aislado).	
7.6. Computación Móvil Y Teletrabajo		
• No ha incorporado medidas de seguridad orientadas a la computación móvil. • La organización no tiene completamente controlado el teletrabajo.	• Se debe establecer una política formal y adoptar las medidas de seguridad apropiadas para proteger contra los riesgos de utilizar medios de computación y comunicación móviles. • Se deben desarrollar e implementar políticas, planes operacionales y procedimientos para actividades de tele-trabajo.	

Fuente: Elaboración propia

Situación Actual	Mejores Practicas	Análisis De Brecha
8. Adquisición, Desarrollo Y Mantenimiento De Los Sistemas		
8.1. Requerimiento de Seguridad De Los Sistemas		
• Se toman en cuenta los requerimientos de las distintas áreas de la organización, con la finalidad de garantizar los niveles aceptables en la seguridad de la información.	• Los enunciados de los requerimientos comerciales para sistemas nuevos, o mejorar los sistemas existentes deben especificar los requerimientos de los controles de seguridad.	
8.2. Procesamiento Correcto En Las Aplicaciones		
• Existen controles que validan las entradas de los datos que son procesados por las diversas aplicaciones. • Existen controles que garantizan la integridad en los mensajes que muestran las aplicaciones al término de cada proceso ejecutado.	• El insumo de data en las aplicaciones debe ser validado para asegurar que esta data sea correcta y apropiada. • Se deben incorporar chequeos de validación en las aplicaciones para detectar cualquier corrupción de la información a través de errores de procesamiento o actos deliberados.	

		• Se deben identificar los requerimientos para asegurar la autenticidad y protección de la integridad de mensaje en las aplicaciones, y se deben identificar e implementar los controles apropiados.	
.	**Situación Actual**	**Mejores Practicas**	**Análisis Brecha**
Procesamiento Correcto		**En Las Aplicaciones**	
	Existen controles que validan las salidas de los datos que son procesados por las diversas aplicaciones.	Se debe validar el output de data de una aplicación para asegurar que el procesamiento de la información almacenada sea correcto y apropiado para las circunstancias.	
8.3. Controles Criptográficos			
	• Existen políticas que garantizan • la protección de la información mediante el encriptado. • Existe una gestión de clave al momento de proceder a encriptar o desencriptar la información.	• Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información. • Se debe utilizar una gestión clave para dar soporte al uso de las técnicas de criptografía	

8.4. Seguridad De Los Activos	Del Sistema	
• No se tiene establecido procedimientos para el control de instalación de software. • Los datos de prueba pasan por un cuidadoso proceso de selección y protección. • La empresa guarda cuidadosamente el código fuente de sus aplicaciones con la finalidad que estas no sean alteradas.	• Se debe contar con procedimientos para controlar la instalación de software en los sistemas operacionales. • Se debe seleccionar cuidadosamente, proteger y controlar la data de prueba. • Se debe restringir el acceso al código fuente del programa.	

Situación Actual	Mejores Practicas	Análisis De Brecha
8.5. Seguridad En Los Procesos De	**Desarrollo Y Soporte**	
• La institución cuenta con procedimiento de controles cambio. • Existen procedimientos establecidos antes de cambiar el sistema operativo de las estaciones de trabajos. • Se limita las modificaciones a los paquetes de software. • Existen controles para evitar las filtraciones de información.	• La implementación de cambios se debe controlar mediante el uso de procedimientos formales de control de cambios. • Cuando se cambian los sistemas operativos, se deben revisar y probar las aplicaciones críticas del negocio para asegurar que no exista un impacto adverso en las operaciones o seguridad organizacional.	

	• No se deben fomentar las modificaciones a los paquetes de software, se deben limitar a los cambios necesarios y todos los cambios deben ser controlados estrictamente. • Se deben evitar las oportunidades de filtraciones en la información. • El desarrollo de software que ha sido outsourced debe ser supervisado y monitoreado por la organización.

.

Fuente: Elaboración propia

Situación Actual	Mejores Practicas	Análisis De Brecha
8.6. Gestión De Vulnerabilidad Técnica		
• Se controla obteniendo oportunamente la información sobre las vulnerabilidades técnicas de los sistemas de los sistemas de información, aunque solo toman medidas apropiadas para medir riesgos.	• Se debe obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información en uso; se debe evaluar la exposición de la organización antes esas vulnerabilidades; y se deben tomar las medidas apropiadas para tratar el riesgo asociado	
.		
9. Administración De Incidentes (Gestión De Incidentes En Seg. Infor.)		
9.1. Reporte De Eventos Y Debilidades En La Seguridad De La Inf.		
• Cuenta con procesos que reportan eventos de seguridad lo más rápido posible a los canales gerenciales. • Los miembros de la organización se encuentran capacitados para reportar cualquier debilidad observada en la seguridad de los servicios o sistemas.	• Los eventos de seguridad de la información deben reportarse a través de los canales gerenciales apropiados lo más rápidamente posible. • Se debe requerir que todos los empleados, contratistas y terceros usuarios de los sistemas y servicios de información tomen nota y reporten cualquier debilidad observada o sospechada en la seguridad de los sistemas o servicios.	

Fuente: Elaboración propia

Situación Actual	Mejores Practicas	Análisis De Brecha
9.2. Gestión De Incidentes Y Mejoras En La Seguridad De La Inf.		
• Se deben establecer las responsabilidades y procedimientos gerenciales para asegurar una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información. • Se llegan a cabo mecanismos que permiten monitorear y cuantificar incidentes en la seguridad de la información. • La empresa efectúa una recolección de evidencia cuando un incidente involucra acciones legales.	• Se deben establecer las responsabilidades y procedimientos gerenciales para asegurar una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información. • Deben existir mecanismos para permitir cuantificar y monitorear los tipos, volúmenes y costos de los incidentes en la seguridad de la información. • Cuando la acción de seguimiento contra una persona u organización después de un incidente en la seguridad de la información involucra una acción legal (sea civil o criminal), se debe recolectar, mantener y presentar evidencia para cumplir las reglas de evidencia establecidas en la(s) Jurisdicción(es) relevantes.	

Fuente: Elaboración propia

Situación Actual	Mejores Practicas	Análisis De Brecha
10. Gestión De La Continuidad Del Negocio		
10.1. Aspectos de la seguridad de la información de la gestión de la continuidad comercial		
• La institución tiene constituida un plan de continuidad y análisis de impacto que entrará en ejecución si ocurriese un evento que interrumpa los procesos comerciales. • Existen colaboradores que se encargan del diseño, redacción e implantación de plan de continuidad. • La institución contempla un marco de planificación para la continuidad del negocio. • Periódicamente se realiza revisiones al plan de continuidad de negocio para mantenerlo actualizado ante posibles eventos que llegasen a ocurrir.	• Se deben desarrollar e implementar planes para mantener o restaurar las operaciones y asegurar la disponibilidad de la información en el nivel requerido y en las escalas de tiempo requeridas después de la interrupción o falla en los procesos comerciales críticos. • Se debe mantener un solo marco referencial de planes de continuidad comercial para asegurar que todos los planes sean consistentes y para tratar consistentemente los requerimientos de la seguridad de la información e identificar las prioridades de pruebas y mantenimiento.	

Fuente: Elaboración propia

Situación Actual	Mejores Prácticas	Análisis De Brecha
Aspectos De La Seguridad De La Información De La Gestión De La Continuidad Comercial		
▪ Cuenta con procesos establecidos que gestiones la continuidad del negocio.	▪ Se debe desarrollar y mantener un proceso gerencial para la continuidad del negocio a través de toda la organización para tratar los requerimientos de seguridad de la información necesarios para la continuidad comercial de la organización. ▪ Se deben identificar los eventos que causan interrupciones en los procesos comerciales, junto con la probabilidad e impacto de dichas interrupciones y sus consecuencias para la seguridad de la información.	

Fuente: Elaboración propia

Situación Actual	Mejores Practicas	Análisis De Brecha
11. Cumplimiento		
11.1. Aspectos Con Requerimientos Legales		
• Actualiza periódicamente los documentos como políticas y estándares de seguridad. • Cuenta con procedimientos que aseguran el cumplimiento de los requerimientos legislativos, reguladores sobre el uso de material con respecto a los derechos de propiedad intelectual. • La institución mantiene protegido los registros importantes para la organización para que no suceda perdida, falsificación o destrucción.	• Se deben definir explícitamente, documentar y actualizar todos los requerimientos estatutarios, reguladores y contractuales y el enfoque de la organización relevante para cada sistema de información y la organización. ▪ Se deben implementar los procedimientos apropiados para asegurar el cumplimiento de los requerimientos legislativos, reguladores y contractuales sobre el uso de material con respecto a los derechos de propiedad intelectual y sobre el uso de los productos de software patentados. ▪ Se deben proteger los registros importantes de una organización de pérdida, destrucción y falsificación, en concordancia con los requerimientos estatuarios, reguladores contractuales y comerciales.	

Situación Actual	Mejores Practicas	Análisis De Brecha
Aspectos Con Requerimientos Legales		
• Garantiza total protección y privacidad tal como lo requiere la legislación. • Utiliza controles en cumplimientos de acuerda a ley y regulaciones relevantes.	• Se deben asegurar la protección y privacidad tal como se requiere en la legislación relevante, las regulaciones y, si fuese aplicable, las cláusulas contractuales. • Se debe desanimar a los usuarios de utilizar los medios de procesamiento de la información para propósitos no-autorizados. • Se deben utilizar controles en cumplimiento con los acuerdos, leyes y regulaciones relevantes.	
11.2. Cumplimiento con las políticas Y Estándares De Seguridad, y el cumplimiento técnico		
• Cumple con los procedimientos de seguridad como políticas y estándares.	• Los gerentes deben asegura que todos los procedimientos de seguridad dentro de su área de responsabilidad sean realizados correctamente en cumplimiento con las políticas y estándares de seguridad.	

Fuente: Elaboración propia

Situación Actual	Mejores Practicas	Análisis De Brecha
Cumplimiento con las políticas y estándares de seguridad, y el cumplimiento técnico		
• Se efectúan chequeos regulares a los sistemas de información para el cumplimiento con estándares de seguridad.	• Los sistemas de información deben chequearse regularmente para el cumplimiento con los estándares de implementación de la seguridad.	
11.3. Consideraciones de auditoria de los sistemas de información		
• Existen controles de auditoria realizados a la empresa por parte de una institución externa. • Se protege a las herramientas de auditoría de los sistemas, para evitar algún posible mal uso.	• Se deben planear cuidadosamente los requerimientos y actividades de las auditorias que involucran chequeo de los sistemas operacionales y se debe acordar minimizar el riesgo de interrupciones en los procesos comerciales. • Se debe proteger el acceso a las herramientas de auditoría de los sistemas de información para evitar cualquier mal uso o compromiso posible.	

.

Fuente: Elaboración propia

5.3. Validación

DOMINIO	EVALUACIÓN	CONCLUSIÓN
1. Políticas de seguridad		La institución carece de revisiones a las policías de seguridad.
2. Organización de la seguridad		No existe contacto con grupos de seguridad especializados de la seguridad de la información. La revisión independiente de la seguridad en intervalos planeados o cambios para la implementación.
3. Gestión de activos		Los activos se encuentran claramente identificados, a su vez forman parte de la organización. El Hospital San Juan Bautista Huaral identifica, documenta e implementan las reglas para el uso aceptable de información.
4. Seguridad ligada a los recursos humanos		Si la institución verifica antecedentes de todos empleados, y se realizan capacitaciones. El Hospital San Juan Bautista Huaral cuenta con un control de acceso de usuario.
5. Seguridad física y del ambiente		La organización cuenta con una seguridad perimetral para áreas que contiene información vital, pero no existe un plan de acción si llegara a una interrupción de servicio público.
6. Gestión de comunicaciones y operaciones		En la institución no todos los procedimientos operativos están documentados.

DOMINIO	EVALUACIÓN	CONCLUSIÓN
7. Control De Accesos		El Hospital San Juan Bautista Huaral documenta y revisa la política de control de acceso, La empresa maneja procesos de identificación automática para validar las conexiones.
8. Adquisición, desarrollo y mantenimiento los Sistemas		El Hospital San Juan Bautista Huaral cuenta con procesos de controles de cambio
9. Administración de incidentes		El Hospital San Juan Bautista Huaral cuenta con procesos que reportan eventos de seguridad, llevan a cabo mecanismos que permiten monitorear incidentes en la seguridad de la información.
10. Gestión de la continuidad del negocio		La institución cuenta con procesos establecidos que gestionen la continuidad del negocio, cuenta con un plan para la continuidad del negocio el cual se realiza periódicamente.
11. Cumplimiento		El Hospital San Juan Bautista Huaral cuenta con documentos como política y estándares de seguridad los cuales los actualiza periódicamente.

Fuente: Elaboración propia

5.4. Recomendación

	DOMINIO ISO	RECOMENDACIÓN
1.	**Políticas de seguridad**	La gerencia debiera establecer claramente la dirección de la política en línea con los objetivos comerciales y demostrar su apoyo, y su compromiso con, la seguridad de la información, a través de la emisión y mantenimiento de una política de seguridad de la información en toda la organización.
2.	**Organización de la seguridad**	Cuando existe la necesidad comercial de trabajar con grupos externos que pueden requerir acceso a la información y a los medios de procesamiento de información de la organización, u obtener o proveer un producto y servicio de o a un grupo externo, se debiera llevar a cabo una evaluación del riesgo para determinar las implicancias en la seguridad y los requerimientos de control. Se debieran acordar y definir los controles en un acuerdo con el grupo externo.
3.	**Gestión de activos**	Todos los activos debieran ser inventariados y contar con un propietario nombrado. Los propietarios debieran identificar todos los activos y se debiera asignar la responsabilidad por el mantenimiento de los controles apropiados.
4.	**Seguridad ligada a los recursos humanos**	Las responsabilidades de seguridad debieran ser tratadas antes del empleo en descripciones de trabajo adecuadas y en los términos y condiciones del empleo. Se debieran definir las responsabilidades de la gerencia para asegurar que se aplique la seguridad a lo largo de todo el Tiempo del empleo de la persona dentro de la organización.

DOMINIO ISO		RECOMENDACIÓN
5.	**Seguridad física y del ambiente**	Los medios de procesamiento de información crítica o confidencial debieran ubicarse en áreas seguras, protegidas por los perímetros de seguridad definidos, con las barreras de seguridad y controles de entrada apropiados. Debieran estar físicamente protegidos del acceso no autorizado, daño e interferencia.
6.	**Gestión de comunicaciones y operaciones**	Se debieran establecer las responsabilidades y procedimientos para la gestión y operación de todos los medios de procesamiento de la información. Esto incluye el desarrollo de los procedimientos de operación apropiados.
7.	**Control de accesos**	Se recomienda controlar el acceso a la información, medios de procesamiento de la información y procesos gerenciales sobre la base de los requerimientos y de seguridad. Se debe tomar en cuenta las políticas para la divulgación y autorización de la información.
8.	**Adquisición, desarrollo y mantenimiento de los sistemas**	Se debiera identificar y acordar los requerimientos de seguridad antes del desarrollo y/o implementación de los sistemas de información, todos los requerimientos de seguridad en la fase de requerimientos de un proyecto; y debieran ser justificados, acordados y documentados como parte del caso comercial general para un sistema de información.
DOMINIO ISO		**RECOMENDACIÓN**

9. Administración de incidentes	Debieran establecer procedimientos formales de reporte y de la intensificación de un evento. Todos los usuarios empleados deben estar al tanto de los procedimientos para el reporte de los diferentes tipos de eventos y debilidades que podrían tener un impacto en la seguridad de los activos organizacionales. Se requiere que reporten cualquier evento y debilidad de la seguridad de la información lo más rápidamente posible en el punto de contacto designado.
10. Gestión de la continuidad del negocio	Se debería implementar el proceso de gestión de la continuidad del negocio para minimizar el impacto sobre la organización y recuperarse de la pérdidas de activos de información (lo cual puede ser resultado de, por ejemplo, desastres naturales, accidentes, fallas del equipo y acciones deliberadas) hasta un nivel aceptable a través de una combinación de controles preventivos y de recuperación. En este proceso debiera identificar los procesos gerenciales críticos e integrar los requerimientos de gestión de la seguridad de la información de la continuidad del negocio con otros requerimientos de continuidad relacionados con aspectos como operaciones, personal, materiales, transporte y me dios.
11. Cumplimiento	Se debiera buscar la asesoría sobre los requerimientos legales específicos de los asesores legales de la organización o profesionales legales calificados adecuados.

Fuente: Elaboración propia

4.1.5.4 Análisis de Riesgo para el Hospital San Juan Bautista Huaral

I. INTRODUCCION

El propósito de este trabajo es, poder llegar a implantar un plan de seguridad para el Hospital San Juan Bautista Huaral con la finalidad de mantener protegida

todos sus activos y la información que contenga, investigando así, la privacidad, accesibilidad y moralidad de sus datos.

La privacidad de datos proporciona la empresa la capacidad de manera segura toda la información que accidentalmente pueda ser filtrada o amenazada, ya sea por el personal o la propia empresa.

La moralidad información en la empresa solo debe ser accedida por el personal autorizado. Y la accesibilidad de información solo puede ser dada el tiempo necesario y requerido.

II. OBJETIVO Y ALCANCE

2.1 Objetivo

Como objetivo del trabajo se realizará un análisis de riesgo del Hospital San Juan Bautista Huaral lo cual se trata de poder gestionar y a la vez identificar los riesgos que por algún error en la seguridad de la información podrían ocasionar perdidas en el negocio, ya sea de información de la empresa, comprometiendo la privacidad, accesibilidad y la moralidad de la información.

2.2 Alcance Del Trabajo

Poder evaluar las amenazas de la seguridad a la que se encuentra expuesta la información.

III. METODOLOGÍA

Durante la ejecución del proyecto se utilizó metodologías específicas para la realización del Plan de Seguridad de Información, las cuales aseguran que se contemple la totalidad de los aspectos relevantes para cada componente de revisión.

La relación de metodología utilizada y el alcance de las mismas se resumen a continuación:

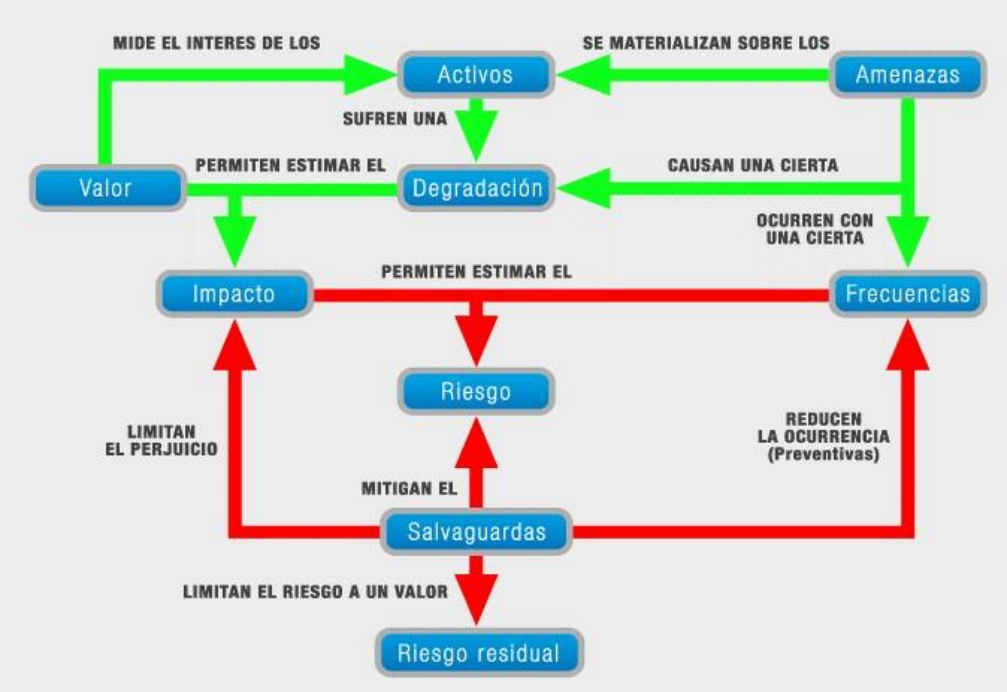
METODOLOGÍA	ALCANCE
MAGERIT	Metodología para el desarrollo de un modelo de seguridad, que involucra el diseño de políticas y normas de seguridad. Metodología utilizada para definir el proyecto del Plan de Seguridad de la Información.

Es la metodología de análisis y gestión de riesgos de los sistemas de información elaborada por el Consejo Superior de Administración Electrónica, como respuesta a la percepción de que, en la Administración, y, en general, toda la sociedad, dependen de forma creciente de las tecnologías de la información para el cumplimiento de su misión.

MAGERIT está directamente relacionada con la generalización del uso de las tecnologías de la información, esto supone beneficios para los usuarios; y da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza. Interesa a todos aquellos que trabajan con información digital y sistemas informáticos para tratarla. Si éstos, son valiosos, MAGERIT permitirá saber cuánto valor está en juego y ayudará a protegerlo. Conocer el

riesgo al que están sometidos los elementos de trabajo es imprescindible para poder gestionarlos. Con MAGERIT se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista.

Figura 6. Ejemplo de Magerit.



3.1 Descripción

Hay varias aproximaciones al problema de analizar los riesgos soportados por los sistemas TIC, como pueden ser guías informales, aproximaciones metódicas y herramientas de soporte. Todas buscan objetivar el análisis de riesgos para saber cuán seguros (o inseguros) son los sistemas y no llamarse a engaño. El gran reto de todas estas aproximaciones es la complejidad del problema al que se enfrentan; complejidad en el sentido de que hay muchos elementos que considerar y que, si no se es riguroso, las conclusiones serán de poco fiar. Es por ello

que en MAGERIT se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista, según esto.

3.2 Etapas MAGERIT

- **Planificación Del Proyecto De Riesgos:** Como consideraciones iniciales para arrancar el proyecto de Análisis y Gestión de Riesgos (AGR), se estudia la oportunidad de realizarlo, se definen los objetivos que ha de cumplir y el ámbito que abarcará, planificando los medios materiales y humanos para su realización e inicializando el propio lanzamiento del proyecto.
- **Análisis De Riesgos:** Se identifican y valoran las diversas entidades, obteniendo una evaluación del riesgo, así como una estimación del umbral de riesgo deseable.
- **Gestión De Riesgos:** Se identifican las funciones y servicios de salvaguarda reductoras del riesgo, seleccionando los que son aceptables en función de las salvaguardas existentes y las restricciones, tras simular diversas combinaciones.
- **Selección De Salvaguardas:** Se prepara el plan de implantación de los mecanismos de salvaguarda elegidos y los procedimientos de seguimiento para la implantación. Se recopilan los documentos del Análisis y Gestión de Riesgos (AGR), para obtener los documentos

finales del proyecto y realizar las presentaciones de resultados a diversos niveles.

3.3 Ventaja De MAGERIT

Las decisiones que deban tomarse y que tengan que ser validadas por la dirección estarán fundamentadas y serán fácilmente defendibles.

3.4 Desventaja De MAGERIT

El hecho de tener que traducir de forma directa todas las valoraciones en valores económicos hace que la aplicación de esta metodología sea realmente costosa.

IV. PROCEDIMIENTO UTILIZADO

Durante el desarrollo del trabajo se utilizaron los siguientes procedimientos revisión y análisis de la información y documentación proporcionada por personal de la institución. Métodos de recolección de datos como el uso de cuestionarios y entrevistas apoyados en las buenas prácticas.

1. DESARROLLO DEL ANALISIS DE RIESGO

El propósito de poder determinar cuál de los activos de las instituciones tienen mayores vulnerabilidades ya se por factores externo o internos, es identificando las causas potenciales que faciliten o impidan alcanzar los objetivos.

Para generar esta información se desempeñaron los siguientes puntos:

- Identificación de los activos de la empresa: Se evaluaron los distintos activos físicos y de software de la empresa generando una lista de los activos que son más vitales para la empresa.
- Asignar importancia a los Activos: Hay que clasificar los activos según el impacto que sufriría la organización si faltase o fallara tal activo.
- Identificar las Amenazas: Listar los factores de riesgo relevantes a los que pueden verse sometidos cada uno de los activos.
- Descripción de consecuencias y salvaguardas: Con los resultados se generará una descripción de los riesgos que podrían sufrir la organización si los activos llegan a ser afectado por dichas amenazas, y se detallara de qué forma se protegerá dichas amenazas.
- Asignar probabilidades de ocurrencia de las Amenazas: Se estimará la probabilidad de ocurrencia que cada una de las amenazas representa con respecto a los activos.

1.1 Activos Y Amenazas

Presentamos la lista de activos reconocidos en el Hospital San Juan Bautista Huaral, asignando un valor a la importancia que tienen en empresa, ponderada en una escala del 1 al 10.

Esta importancia es un valor subjetivo que refleja el nivel del impacto que puede tener la organización si un incidente afecta a los activos, sin considerar las medidas de seguridad que existan sobre los mismos.

Estimación De Nivel De Impacto

CATEGORIA	ID	DEFINICIÓN DEL ACTIVO	NIVEL DE IMPACTO
Entorno	**1**	Personal	8
	2	Arquitectura tecnológica de redes	7
	3	Personal con experiencia en proceso	8
	4	Dispositivos de conectividad	8
	5	Infraestructura	9
Sistemas De Información	**6**	PC's	10
	7	Servidor	10
	8	Sistema administrativo	7
	9	Software	6
	10	Dispositivos de entrada / salida	4
Información	**11**	Información	8
	12	Conocimiento	8

Estimación de Nivel de Riesgo

A continuación, se listan las amenazas que pueden afectar a dichos activos, indicando la probabilidad de que estas contingencias ocurran, en una escala del 1 al 3.

TIPO	ID	SUB-TIPO	AMENAZA	PROBABILIDAD
Accidentes	**1**	**A1**	Incendio	1
	2	**A1**	Terremoto	1
	3	**A2**	Interrupción de servicio de comunicación	3
	4	**A3**	Altas y bajas de Luz	2
	5	**A3**	Cortes de energía eléctrica inesperado	1

NOTA: Esta probabilidad fue evaluada teniendo en cuenta las medidas de seguridad existentes en el Hospital San Juan Bautista Huaral.

TIPO	ID	SUB-TIPO	AMENAZA	PROBABILIDAD
Errores	**6**	**E1**	Fallas de aire acondicionado	2
	7	**E2**	Error Humano	2
	8	**E2**	Personal no calificado	1
	9	**E3**	Ubicación inadecuada de equipos	1
	10	**E4**	Fallas de servidores	1
Intencionales Presenciales	**11**	**P1**	Fraudes	2
	12	**P2**	Robo de equipo	2
	13	**P2**	Robo de información	1
	14	**P1**	Deshonestidad	2
	15	**P3**	Retiro/Ausencia intempestiva de personal	1
Intencionales Remotas	**16**	**R1**	Hacker	2
	17	**R1**	Virus	2

NOTA: Esta probabilidad fue evaluada teniendo en cuenta las medidas de seguridad existentes en el Hospital San Juan Bautista Huaral

1.2. Posibles Consecuencias Y Medidas Existentes

En el presente cuadro se listan los activos de la empresa, las amenazas que los afectan directamente y las consecuencias que puede acarrear la materialización de estas amenazas. Se describen también las salvaguardas o información referida a las medidas que ha tomado el Hospital San Juan Bautista Huaral para mitigar estas consecuencias. Por último, se han evaluado estas medidas, indicando si son deficientes, mejorables o eficientes.

ESCALA DE EFECTIVIDAD	
Definición	**Abreviatura**
Eficiente	E
Mejorable	M
Deficiente	D

.

Activos Del Hospital San Juan Bautista Huaral

SOFTWARE				
Amenaza	**Consecuencia**	**¿Se protege?**	**¿Cómo?**	**Efectividad**
Virus	Perdida de información Infectar el software	Si	Instalación de antivirus en las PC's Actualización constante del antivirus	M
Factor Humano	Usos malintencionados Habilitar configuraciones que no correspondan Dejan errores en el software	Si	Establecer políticas aceptables de selección de personal y outsourcing	M

PERSONAL - I				
Amenaza	**Consecuencia**	**¿Se protege?**	**¿Cómo?**	**Efectividad**
Fraude	Desconfianza en el personal	Si	Buenas políticas de seguridad Acuerdos de no divulgación y fuga de información	M
Incendio	Destrucción del ambiente laboral Daños a la integridad física	Si	Instalación de extintores	M
Robo De Equipos	Escasez de confianza en la seguridad Deficiencia en las actividades	Si	Restricción de acceso al personal no autorizado	M

.

PERSONAL - II				
Amenaza	**Consecuencia**	**¿Se protege?**	**¿Cómo?**	**Efectividad**
Robo Información	Paralización de las actividades Control deficiente de las operaciones	Si	Implementación de buenas políticas de seguridad de información	E
Vandalismo	Avería del equipo Lesiones en la integridad del personal	Si	Protección de las puertas principales Personal de seguridad	E
Deshonestidad	Poca confianza en el personal encargado Mala reputación del área de informática	No	Falta de valores y profesionalismo de algunos empleados	D
Ubicación Inadecuada De Equipos	Pérdida de tiempo en el traslado de equipos	Si	Ubicación adecuada de los equipos conforme a sus respectivas áreas	E

DISPOSITIVOS DE CONECTIVIDAD - I				
Amenaza	**Consecuencia**	**¿Se protege?**	**¿Cómo?**	**Efectividad**
Terremotos O Movimientos Telúricos	Destrucción total o parcial de los dispositivos Destrucción total o parcial de los dispositivos	Si	Construcción de material noble El ambiente no es el adecuado y no los soportarían un fuerte movimiento telúrico	M

DISPOSITIVOS DE CONECTIVIDAD - II				
Amenaza	**Consecuencia**	**¿Se protege?**	**¿Cómo?**	**Efectividad**
Corte De Energía Eléctrica Inesperado	Degradación de los dispositivos Paralización del funcionamiento de los dispositivos	Si	Cuenta con UPS	E
Factor Humano	Mal funcionamiento de los dispositivos Paralización de las actividades en red	Si	Falta de capacitación al personal, ellos se dan solos	M
Robo De Equipo	Perdida de los dispositivos Paralización del funcionamiento normal	Si	Ambientes internos, con puertas de acero inoxidable de la institución	M

SISTEMA ADMINISTRATIVO - I				
Amenaza	**Consecuencia**	**¿Se protege?**	**¿Cómo?**	**Efectividad**
Personal No Calificado	Ingreso de datos que no corresponden Dejan errores en el sistema Activar opciones que no corresponden Dejar en mal funcionamiento el sistema	Si respecto	Personal con conocimiento básicos al	M
Políticas mal definida	Acceso a personas no autorizadas No hay responsabilidades por accidentes	Si	Algunas áreas cuentan con un MOF y ciertos planes que apoyan en el correcto funcionamiento de las actividades	E

.

SISTEMA ADMINISTRATIVO - II				
Amenaza	**Consecuencia**	**¿Se protege?**	**¿Cómo?**	**Efectividad**
Retiro / Ausencia intempestiva del personal	En caso de emergencia, paralización del funcionamiento del sistema Propenso a la intervención de personal no calificado	Si	Cuenta con dos más personas a que conocen el manejo de los sistemas.	M
Virus	Desquiciar el sistema Destrucción de información	Si	Se instalan antivirus los cuales se actualizan constantemente	E

SERVIDORES - I				
Amenaza	**Consecuencia**	**¿Se protege?**	**¿Cómo?**	**Efectividad**
Incendio	Destrucción total o parcial de los servidores Perdida de la información Destrucción total o parcial de los servidor La parte administrativa del hospital se vería muy afectada	Si ambientes del	Instalación de extintores, pero se necesita mejorar	M

.

SERVIDORES - II				
Amenaza	**Consecuencia**	**¿Se protege?**	**¿Cómo?**	**Efectividad**
Terremoto	Destrucción de los servidores. Perdida de información contenida en los servidores. Deficiencia en las actividades normales de la institución. Destrucción total o parcial de los ambientes de los equipos. Perdida de la información. Destrucción total o parcial de los ambientes del servidor. La parte administrativa del hospital se vería muy afectada.	Si	Construcción de material noble, pero se necesita mejorar porque no soportaría un fuerte movimiento telúrico.	M
Altas Y Bajas De Energía Eléctrica	Avería de los servidores Mal procesamiento de la información	Si	Cuenta con estabilizadores híbridos y supresores de pico	E
Error Humano	Manipulación inadecuada de los servidores Interrumpen los procesos cotidianos de los equipos	Si	Son pocas las veces que se capacita al personal	M

SERVIDORES - III				
Amenaza	**Consecuencia**	**¿Se protege?**	**¿Cómo?**	**Efectividad**
Corte De Energía Eléctrica Inesperado	Avería de los servidores Perdida de la información Si Cuenta con UPS, baterías de celda y Deficiencia en las actividades normales grupo electrógeno de la institución			E
Falta De Aire Acondicionado	Avería en los servidores Recalentamiento del servidor	Si	La sala de servidores cuenta con ventiladores aéreos	M

ARQUITECTURA DE TECNOLOGIA DE REDES - I				
Amenaza	**Consecuencia**	**¿Se protege?**	**¿Cómo?**	**Efectividad**
Incendio	Destrucción total o parcial de la arquitectura de redes Paralización de las operaciones necesita mejorar normales	Si	Instalación de extintores, pero se	M
Error Humano	Daño de la arquitectura tecnológica de redes (Sin intención) Deficiencia en las actividades del supresores de pico hospital	Si	Cuenta con estabilizadores híbridos y	E

ARQUITECTURA DE TECNOLOGIA DE REDES - II				
Amenaza	**Consecuencia**	**¿Se protege?**	**¿Cómo?**	**Efectividad**
Personal No Calificado	Mala distribución o ubicación de este activo	Si	Cuenta con personal con conocimientos básicos al respecto	M
Terremoto	Destrucción total o parcial de la arquitectura tecnológica de redes Paralización de las operaciones normales de la institución . Destrucción total o parcial de los ambientes de los equipos	Si	Construcción de material noble, pero se necesita mejorar porque no soportaría un fuerte movimiento telúrico	M
Ubicación Inadecuada De Equipos	Obstaculiza el trabajo de los empleados. Propensos a sufrir algún daño o pérdida	Si	Los equipos están ordenados según su área	E
Vandalismo	Destrucción total o parcial de este activo Perdida de algunos equipos Destrucción total o parcial de los ambientes de los equipos	Si	Cuenta con estabilizadores híbridos y supresores de pico	E

.

CONOCIMIENTO				
Amenaza	**Consecuencia**	**¿Se protege?**	**¿Cómo?**	**Efectividad**
Personal No Calificado	Imparte conocimientos inadecuados Fomenta los malos hábitos y corrompen a los demás empleados	Si	Aceptable política de selección de personal y outsourcing (se puede mejorar).	M
Vandalismo	Perturba la concepción adecuada de conocimientos.	Si	Personal de seguridad. Puertas principales	E
Políticas mal definidas	Debería existir una base de conocimientos donde se registre toda experiencia	Si	Existe un compromiso por parte de las autoridades en crear un base de conocimientos	M
Retiro/ Ausencia intempestiva	Pérdida o ausencia de personal clave cuyo conocimiento es indispensable para la organización	Si	Cuenta con dos más personas a que conocen el manejo de los sistemas. Se puede mejorar	M

.

PC's - I				
Amenaza	**Consecuencia**	**¿Se protege?**	**¿Cómo?**	**Efectividad**
Incendio	Perjudica a las maquinas Provoca perdida de equipos Significa un desembolso para la empresa en la reposición de éstos	Si	Instalación de extintores, pero se necesita mejorar.	M
Terremoto	Perjudicar la integridad de los equipos informáticos Destrucción total o parcial de los ambientes de los equipos Interrumpen los procesos cotidianos de los equipos	Si	Construcción de material noble. Pero no soportarían un fuerte movimiento telúrico.	M
Altas Y Bajas De Energía Eléctrica	Causan perjuicios en las PC's Interrumpen los procesos cotidianos de los equipos	Si	Disponen de estabilizadores para todas las PC's	E
Retiro/ Ausencia intempestiva	Pérdida o ausencia de personal clave cuyo conocimiento es indispensable para la organización	Si	Cuenta con dos más personas a que conocen el manejo de los sistemas. Se puede mejorar	M

PC's - II				
Amenaza	**Consecuencia**	**¿Se protege?**	**¿Cómo?**	**Efectividad**
Corte De Energía Eléctrica Inesperada	Causan perjuicios total o parcial a la integridad de las PC's Interrumpen los procesos cotidianos de los equipos	Si	Cuentan con UPS para las PC's de las áreas más críticas	E
Error Humano	Manipulación inadecuadas de las PC's Interrumpen los procesos cotidianos de los equipos	Si	Se contrata a personal con conocimiento es computación como en ofimática. Pero el personal se capacita por su propia cuenta.	M
Vandalismo	Daña la integridad de los equipos Perdida de los equipos Destrucción de los ambientes de las PC's	Si	Personal de seguridad. Puertas principales hechas de acero	E
Robo De Equipo	Paralización de las operaciones por la pérdida de las PC's	Si	Restricciones de acceso a personal no autorizado	M

PC's - III				
Amenaza	**Consecuencia**	**¿Se protege?**	**¿Cómo?**	**Efectividad**
Virus	Paralización de las maquinas (PC) Perdida de la información Perjudicar el desarrollo de los procesos de los equipos	Si	Se ha instalado software antivirus a cada una de las PC's. Pero se puede mejorar	E

INFRAESTRUCTURA				
Amenaza	**Consecuencia**	**¿Se protege?**	**¿Cómo?**	**Efectividad**
Personal No Calificado	Paraliza todas las operaciones Perjudican a la mayoría de los activos Destruir parcial o totalmente la infraestructura	Si	Construcción de material noble Soportarían un fuerte Movimiento telúrico.	M
Incendios	Paralizan las operaciones que realiza la empresa. Destruir parcial o totalmente la infraestructura	Si	No existen detectores de humo y solo algunos ambientes cuentan con extintores.	M

.

Activos Del Hospital San Juan Bautista Huaral

PERSONAL CON EXPERIENCIA EN LOS PROCESOS				
Amenaza	**Consecuencia**	**¿Se protege?**	**¿Cómo?**	**Efectividad**
Deshonestidad Y Sabotaje	Paralización de los procesos de sistema (Falla sistema, Robo, modificación de información).	Si	Política de seguridad.	M
Retiro/Ausencia Intempestiva Del Personal	Aumento de vulnerabilidades e inestabilidad del sistema / incremento de riesgos en caída de servicios.	No	Política de seguridad.	M

DISPOSITIVOS DE ENTRADA/SALIDA - I				
Amenaza	**Consecuencia**	**¿Se protege?**	**¿Cómo?**	**Efectividad**
Terremotos	Paraliza todas las operaciones. Perjudican a la mayoría de los activos. Paralizan las operaciones que realiza el hospital. Destruir parcial o totalmente la infraestructura.	Si	Soportarían un fuerte Movimiento Construcción de material noble.	M

Activos Del Hospital San Juan Bautista Huaral

DISPOSITIVOS DE ENTREDA/SALIDA - II				
Amenaza	**Consecuencia**	**¿Se protege?**	**¿Cómo?**	**Efectividad**
Incendios	Paralizan las operaciones que realiza el hospital Destruir parcial o totalmente la infraestructura	Si	No existen detectores de humo y solo algunos ambientes cuentan con extintores.	M

PERSONAL - I				
Amenaza	**Consecuencia**	**¿Se protege?**	**¿Cómo?**	**Efectividad**
Incendio	Destrucción total o parcial de la información física (documentos) y la información lógica (Contenidos en discos duros y otros dispositivos de almacenamientos).	Si	Instalación de extintores, pero se necesita mejorar.	M
Terremoto	Degradación y/o destrucción total o parcial de la información física (documentos) y la información lógica (Contenidos en discos duros y otros dispositivos de almacenamientos).	Si	Construcción de material noble, pero se necesita mejorar porque no soportaría un fuerte movimiento telúrico.	M

.

PERSONAL - II				
Amenaza	**Consecuencia**	**¿Se protege?**	**¿Cómo?**	**Efectividad**
Error Humano	Corrupción de información. Perdida de información inesperada.	Si	Son pocas las veces que se capacita al personal.	M
Personal No Calificado	Daños y pérdida de información. Peligro latente en la integridad de la información.	Si	Cuentan con personal con conocimiento básicos al respecto.	M
Robo De Equipo	Perdida de la información lógica (Contenida en discos duros y otros dispositivos de almacenamientos).	Si	Restricciones de acceso de personas no autorizadas.	M
Robo De Información	Perdida de la información física (documentos) y la información lógica (contenida en discos duros y otros dispositivos de almacenamiento).	Si	Implementación de buenas políticas de seguridad de información.	E

.

1.3 Calculo De Los Niveles De Vulnerabilidad Y De Rango

En este cuadro se calculan los niveles de vulnerabilidad y de riesgo en los que incurre cada activo vital identificado. Para esto se tiene en cuenta el nivel de importancia asignado a cada uno y la probabilidad de ocurrencia de estos riesgos. Para realizar dicho cálculo se desarrollaron las siguientes operaciones:

• **Probabilidad De Ocurrencia:** representan la probabilidad de que se materialicen las amenazas identificadas, en una escala del 1 al 2. Esta probabilidad fue evaluada teniendo en cuenta las medidas de seguridad existentes en municipalidad

• **Nivel De Vulnerabilidad:** se calcula el porcentaje de probabilidad de que se materialicen las amenazas, con respecto a la cantidad de amenazas identificadas para dicho activo. Esto es debido a que cada activo está afectado por un número diferente de amenazas posibles, de manera que este cálculo sirve para obtener un porcentaje de probabilidades equilibrado por igual para cualquier activo, independientemente de la cantidad de amenazas que lo afectan.

• **Nivel De Riesgo:** En este momento interviene el nivel de importancia que refleja el nivel de Impacto que puede tener la municipalidad si un incidente afecta a los activos, multiplicando al nivel de vulnerabilidad. De esta forma se obtiene el nivel de riesgo de cada activo con respecto a una amenaza. La suma de estos valores es el nivel de riesgo total que corresponde a cada activo.

ESTIMACIÓN DE RIESGOS					
DEFINICION DEL ACTIVO	**IMPACTO**	**AMENAZAS**	**PROBABILIDAD**	**VULNERABILIDAD**	**RIESGOS**
SOFTWARE	7	Virus	2	100,00	700,00
		Factor humano	2	100,00	700,00
		CANTIDAD DE AMENAZA= 2			
PERSONAL	9	Fraude	2	28,57	257,14
		Vandalismo	2	28,57	257,14
		Robo de equipo	2	28,57	257,14
		Robo de información	2	28,57	257,14
		Deshonestidad	2	28,57	257,14
		Incendio	1	14,29	128,57
		Ubicación Inadecuada de equipos	1	14,29	128,57
		CANTIDAD DE AMENAZA= 7		**171,43**	**1542,86**

ESTIMACIÓN DE RIESGOS					
DEFINICION DEL ACTIVO	**IMPACTO**	**AMENAZAS**	**PROBABILIDAD**	**VULNERABILIDAD**	**RIESGOS**
DISPOSITIVOS DE CONETIVIDAD	9	Terremotos	1	20,00	180
		Corte de energía eléctrica inesperado	1	20,00	180
		Factor humano	2	40,00	360
		Error del mantenimiento del sistema	2	40,00	360
		Robo de equipo	1	20,00	180
		CANTIDAD DE AMENAZA= 5		**140,00**	**1260**
SERVIDORES	10	Incendio	1	14,29	142,86
		Terremoto	1	14,29	142,86
		Altas y bajas de luz	2	28,57	285,71
		Error humano	2	28,57	285,71
		Corte de energía eléctrica inesperado	1	14,29	142,86
		Falta de aire acondicionado	2	28,57	285,71
		CANTIDAD DE AMENAZA= 6		**128,57**	**1285,71**

.

ESTIMACIÓN DE RIESGOS					
DEFINICION DEL ACTIVO	**IMPACTO**	**AMENAZAS**	**PROBABILIDAD**	**VULNERABILIDAD**	**RIESGOS**
ARQUITECTURA DE TECNOLOGÍA DE REDES	8	Incendio	1	16,67	133,33
		Terremoto	1	16,67	133,33
		Error Humano	2	33,33	266,67
		Personal no calificado	1	16,67	133,33
		Ubicación inadecuada de equipos	1	16,67	133,33
		Vandalismo	2	33,33	266,67
		CANTIDAD DE AMENAZA= 6		**133,33**	**1066,67**
SISTEMA ADMINISTRATIVO	6	Personal no calificado	1	25,00	150
		Políticas mal definida	1 1	25,00 25,00	150 150
		Retiro / Ausencia intempestiva del personal			
		Virus	2	50,00	300
		CANTIDAD DE AMENAZA= 4		**125,00**	**750**

ESTIMACIÓN DE RIESGOS					
DEFINICION DEL ACTIVO	**IMPACTO**	**AMENAZAS**	**PROBABILIDAD**	**VULNERABILIDAD**	**RIESGOS**
CONOCIMIENTO	6	Personal no calificado	1	25,00	150
		Políticas mal definida	1 1	25,00 25,00	150 150
		Retiro / Ausencia intempestiva del personal			
		Virus	2	50,00	300
		CANTIDAD DE AMENAZA= 4		**125,00**	**750**
INFRAESTRUCTURA	7	Terremotos	1	50	350
		Incendios	1	50	350
		CANTIDAD DE AMENAZA= 2		**100**	**700**
PC's	9	Incendio	1	12,50	112,5
		Terremoto	1 1	12,50 12,50	112,5
		Corte y energía eléctrica inesperado			112,5
		Error humano	2	25,00	225
		Vandalismo	2	25,00	225

ESTIMACIÓN DE RIESGOS					
DEFINICION DEL ACTIVO	**IMPACTO**	**AMENAZAS**	**PROBABILIDAD**	**VULNERABILIDAD**	**RIESGOS**
PC's	9	Robo de Equipo	2	25,00	225
		CANTIDAD DE AMENAZA= 8		**112,50**	**1012,50**
INFORMACIÓN	10	Incendio	1	16,67	166,67
		Terremoto	1	16,67	166,67
		Error Humano	2	33,33	333,33
		Personal no calificado	1	16,67	166,67
		Robo de equipo	2	33,33	333,33
		Robo de información	1	16,67	166,67
		CANTIDAD DE AMENAZA= 6		**133,33**	**1333,33**
DISPOSITIVOS DE ENTRADA/SALIDA	4	Terremotos	1	50	200
		Incendios	1	50	200
		CANTIDAD DE AMENAZA= 2		**100**	**400**

ESTIMACIÓN DE RIESGOS					
DEFINICION DEL ACTIVO	**IMPACTO**	**AMENAZAS**	**PROBABILIDAD**	**VULNERABILIDAD**	**RIESGOS**
PERSONAL CON EXPERIENCIA EN PROCESOS	5	Deshonestidad y sabotaje	2	100	500
		Retiro/ausencia intempestiva del personal	2	100 **200**	500 **1000**
		CANTIDAD DE AMENAZA= 2			

1.4 Conclusiones

En este cuadro se calculan los niveles de vulnerabilidad y de riesgo en los que incurre cada activo vital identificado. Para esto se tiene en cuenta el nivel de importancia asignado a cada uno y la probabilidad de ocurrencia de estos riesgos. Para realizar dicho cálculo se desarrollaron las siguientes operaciones:

Niveles de Riesgo (R) y Vulnerabilidad (V)

En el cuadro se listan los niveles de Riesgo y Vulnerabilidad para cada activo, considerando la importancia de 1 a 5, y sin tener en cuenta la importancia (es decir con un valor de 1). A la derecha los valores que observamos representan el número de los activos, ordenados en forma descendiente de acuerdo al riesgo y vulnerabilidad que corren dichos activos.

ACTIVO	NIVEL DE RIESGO (R)		NIVEL DE VULNERABILIDAD		ACTIVOS EN ORDEN DESCENDENTE	
	Valor	R (%)	Valor	R (%)	(R)	(V)
Software	1400	10,98	200	11,98	8	7
Personal	1543	12,10	171	10,25	11	9
Dispositivos de conectividad	1260	9,88	140	8,39	3	11
Servidores	1286	10,08	129	7,73	7	12
Arquitectura tecnológica de redes	1067	8,37	133	7,97	6	3
Sistema administrativo	750	5,88	125	7,49	12	8
Conocimiento	1000	7,84	125	7,49	10	10
Infraestructura	700	5,49	100	5,99	9	1
PC's	1013	7,94	113	6,77	2	2
Dispositivos de entrada / salida	400	3,14	100	5,99	1	4
Personal con Experiencia en Procesos	1000	7,84	200	11,98	4	6
Información	1333	10,46	133	7,97	5	5
TOTAL	**12752**	**100,00**	**1669**	**100,00**		

.

Fuente: Elaboración propia

Activos Por Orden de Riesgo (R)		R (%)
Personal	1400	10,9
Información	1333	10,46
Servidores	1286	10,08
Dispositivos de conectividad	1260	9,88
Arquitectura tecnológica de redes	1067	8,37
PC's	1013	7,94
Conocimiento	1000	7,84
Personal con Experiencia en Procesos	1000	7,84
Sistema administrativo	750	5,88
Infraestructura	700	5,49
Dispositivos de entrada / salida	400	3.14
TOTAL	**12752**	**100%**

Activos Por Orden de Vulnerabilidad (R)

ACTIVO	NIVEL DE VULNERABILIDAD (R)	
	VALOR	R (%)
Personal	1543	12,10
Software	1400	10,98
Información	1333	10,46
Servidores	1286	10,08
Dispositivos de conectividad	1260	9,88
Arquitectura tecnológica de redes	1067	8,37
PC's	1013	7,94

Activos Por Orden de Vulnerabilidad (R)

	VALOR	R (%)
Conocimiento	1000	7,84
Personal con Experiencia en Procesos	1000	7,84
Sistema administrativo	750	5,88
Infraestructura	700	5,49
Dispositivos de entrada / salida	400	3.14
TOTAL	**12752**	**100%**

1.5. Análisis de Importancia

Aquí vemos un análisis donde se tiene en cuenta el nivel de riesgo y la importancia con una ponderación de 1 a 10. Se calculó el porcentaje de los riesgos y el porcentaje del impacto respectivamente. Al calcular la diferencia entre estos porcentajes (Dif. de %) se obtiene el porcentaje que muestra cuán sobrevaluados o menospreciados están los activos de acuerdo a sus riesgos. A continuación, se calcula una cifra (Dif. de importancia) que representan los porcentajes anteriormente mencionados, de la siguiente manera:

- Para aplicar la diferencia de porcentajes a la importancia actual, se multiplican

  · (Importancia) * (Dif. De %)

- Este resultado no está en escala de 1 a 10, por lo que, con una regla de tres simple, se centran los valores:

  100 % ⟶ 10 puntos de importancia
  Importancia * Dif. De % ⟶ **X** (= Diferencia de importancia)

- A este resultado se le suma (o resta de acuerdo al signo) a la importancia actual, obteniendo la importancia que debería tener cada activo (importancia ideal), de acuerdo al nivel de riesgos encontrado.

  Importancia ideal = Importancia actual + Diferencia de importancia

Activos Del Hospital San Juan Bautista Huaral

ANALISIS DE IMPORTANCIA

	NIVEL DE RIESGO (R)		IMPORTANCIA		DIF. DE IMPORTANCIA		
ACTIVO	**VALOR**	**R (%)**	**IMPOR.**	**%**	**DIF. DE %**	**DIF. IMPOR.**	**IMPOR. IDEAL**
Software	1400	10,98	7	6,80	0,042	0,293	7,089
Personal	1543	12,10	9	8,74	0,034	0,303	9,040
Dispositivos de conectividad	1260	9,88	10	9,71	0,002	0,017	9,726
Servidores	1286	10,08	9	8,74	0,013	0,121	8,859
Arquitectura tecnológica de redes	1067	8,37	9	8,74	-0,004	-0,033	8,705
Sistema administrativo	750	5,88	8	7,77	-0,019	-0,151	7,616
Conocimiento	1000	7,84	9	8,74	-0,009	-0,081	8,657
Infraestructura	700	5,49	8	7,77	-0,023	-0,182	7,585
PC's	1013	7,94	10	9,71	-0,018	-0,177	9,532
Dispositivos de entrada / salida	400	3,14	8	7,77	-0,046	-0,370	7,397
Personal con Experiencia en Procesos	1000	7,84	9	8,74	-0,009	-0,081	8,657
Información	1333	10,46	7	6,80	0,037	0,256	7,052
TOTAL	**12752**	**100,00**	**103**	**100.00**	**0,00**	**-0,085**	**99,915**

CAPÍTULO V

RESULTADOS ESTADISTICOS

5.1. Análisis e interpretación de resultados de la encuesta

Para poder llevar a cabo el análisis e interpretación de los resultados es necesario mencionar que la encuesta ha sido dirigida a cada uno de los interesados para el beneficio de la investigación.

El modelo del cuestionario que se muestra en el Anexo 02, teniendo un total de 92 personas encuestadas.

5.1.1. Descripción de resultados

Pregunta 01: ¿Contar con un adecuado sistema de gestión de seguridad de la información permitirá un control adecuado de los sistemas que maneja el hospital San Juan Bautista?

Tabla 4.9. Respuestas de la pregunta 01.

	Frecuencia	**Porcentaje**
En desacuerdo	6	7
No sabe, no opina	5	5
De acuerdo	55	60
Completamente de acuerdo	26	28
Total	92	100

Interpretación:

Se observa en la tabla 4.9, que el 60% de los encuestados está de acuerdo que contar con un adecuado sistema de gestión de seguridad de la información permitirá un control adecuado de los sistemas que maneja el hospital San Juan Bautista; así mismo el 5% no sabe, no opina.

Pregunta 02: ¿Las herramientas de seguridad con las que cuenta el hospital San Juan Bautista Huaral son las necesarias para una adecuada protección física de la información?

Tabla 5.0. Respuestas de la pregunta 02.

	Frecuencia	**Porcentaje**
Completamente en desacuerdo	1	1
En desacuerdo	8	9
No sabe, no opina	3	3
De acuerdo	56	61
Completamente de acuerdo	24	26
Total	92	100

Interpretación:

Se observa en la tabla 5.0, que el 61% de los encuestados está de acuerdo que las herramientas de seguridad con las que cuenta el hospital San Juan Bautista Huaral son las necesarias para una adecuada protección física de la información; así mismo el 1% está completamente en desacuerdo.

Pregunta 03: ¿La institución debe tener un plan de contingencia en caso de desastres naturales que resguarde la información?

Tabla 5.1. Respuestas de la pregunta 03.

	Frecuencia	**Porcentaje**
Completamente en desacuerdo	3	3
En desacuerdo	15	17
De acuerdo	49	53
Completamente de acuerdo	25	27
Total	92	100

Interpretación:

Se observa en la tabla 5.1, que el 53% de los encuestados está de acuerdo que la institución debe tener un plan de contingencia en caso de desastres naturales que resguarde la información; así mismo 3% de los encuestados está completamente en desacuerdo.

Pregunta 04: ¿Deberían existir procedimientos para el registro y control de acceso del personal que se encarga del ingreso y procesamiento de información?

Tabla 5.2. Respuestas de la pregunta 04.

	Frecuencia	**Porcentaje**
Completamente en desacuerdo	4	5
En desacuerdo	13	14
No sabe, no opina	3	3
De acuerdo	48	52
Completamente de acuerdo	24	26
Total	92	100

Interpretación:

Se observa en la tabla 5.2, que el 52% de los encuestados está de acuerdo que deberían existir procedimientos para el registro y control de acceso del personal que se encarga del ingreso y procesamiento de información; así mismo el 3% no saben, no opinan.

Pregunta 05: ¿Las herramientas y técnicas que utiliza la institución son las necesarias para proteger lógicamente la información?

Tabla 5.3. Respuestas de la pregunta 05.

	Frecuencia	**Porcentaje**
No sabe, no opina	2	2
De acuerdo	51	56
Completamente de acuerdo	39	42
Total	92	100

Interpretación:

Se observa en la tabla 5.3, que el 56% de los encuestados está de acuerdo que las herramientas y técnicas que utiliza la institución son las necesarias para proteger lógicamente la información; así mismo el 2% no saben, no opinan.

Pregunta 06: ¿Los métodos, procedimientos de seguridad que se aplican en el hospital San Juan Bautista se alinean con sus objetivos y metas?

Tabla 5.4. Respuestas de la pregunta 06.

	Frecuencia	**Porcentaje**
En desacuerdo	6	7
No sabe, no opina	8	9
De acuerdo	59	64
Completamente de acuerdo	19	20
Total	92	100

Interpretación:

Se observa en la tabla 5.4, que el 64% de los encuestados está de acuerdo que los métodos, procedimientos de seguridad que se aplican en el hospital San Juan Bautista se alinean con sus objetivos y metas; así mismo el 7% está en desacuerdo. Se observa que ninguno de los encuestados seleccionó la opción completamente en desacuerdo.

Pregunta 07: ¿Se comunica los documentos y normas de seguridad a todos los empleados y unidades que integran la institución?

Tabla 5.5. Respuestas de la pregunta 07.

	Frecuencia	**Porcentaje**
Nunca	1	1
Casi nunca	7	8
A veces	4	4
Casi siempre	54	59
Siempre	26	28
Total	92	100

Interpretación:

Se observa en la tabla 5.5, que el 59% de los encuestados afirma que casi siempre se comunica los documentos y normas de seguridad a todos los empleados y unidades que integran la institución; así mismo el 1% menciona que nunca se comunica.

Pregunta 08: ¿Cree usted que las políticas de seguridad tienen un impacto positivo en el área donde labora?

Tabla 5.6. Respuestas de la pregunta 08.

	Frecuencia	**Porcentaje**
Completamente en desacuerdo	2	2
En desacuerdo	7	8
No sabe, no opina	5	5
De acuerdo	56	61
Completamente de acuerdo	22	24
Total	92	100

Interpretación:

Se observa en la tabla 5.6, que el 61% de los encuestados está de acuerdo que las políticas de seguridad tienen un impacto positivo en el área donde labora; así mismo el 2% está completamente en desacuerdo.

Pregunta 09: ¿Cumplir con las políticas de seguridad del hospital San Juan Bautista da como resultado una adecuada gestión de la información?

Tabla 5.7. Respuestas de la pregunta 09.

	Frecuencia	**Porcentaje**
En desacuerdo	5	5
No sabe, no opina	9	10
De acuerdo	56	61
Completamente de acuerdo	22	24
Total	92	100

Interpretación:

Se observa en la tabla 5.7, que el 61% de los encuestados está de acuerdo que cumplir con las políticas de seguridad del hospital San Juan Bautista da como resultado una adecuada gestión de la información; así mismo el 5% está en desacuerdo. Se observa que ninguno de los encuestados seleccionó la opción completamente en desacuerdo.

Pregunta 10: ¿Las políticas de seguridad que establece el hospital San Juan Bautista influyen con el manejo eficiente de información?

Tabla 5.8. Respuestas de la pregunta 10.

	Frecuencia	**Porcentaje**
En desacuerdo	3	3
No sabe, no opina	5	5
De acuerdo	63	69
Completamente de acuerdo	21	23
Total	92	100

Interpretación:

Se observa en la tabla 5.8, que el 69% de los encuestados está de acuerdo que las políticas de seguridad que establece el hospital San Juan Bautista influyen con el manejo eficiente de información; así mismo el 3% está en desacuerdo. Se observa que ninguno de los encuestados seleccionó la opción completamente en desacuerdo.

Pregunta 11: ¿Las políticas de seguridad del hospital San Juan Bautista deberían actualizarse para mejorar la productividad del servicio que brindan?

Tabla 5.9. Respuestas de la pregunta 11.

	Frecuencia	**Porcentaje**
En desacuerdo	5	6
No sabe, no opina	4	4
De acuerdo	62	67
Completamente de acuerdo	21	23
Total	92	100

Interpretación:

Se observa en la tabla 5.9, que el 67% de los encuestados está completamente de acuerdo que las políticas de seguridad del hospital San Juan Bautista deberían actualizarse para mejorar la productividad del servicio que brindan; así mismo el 6% está en desacuerdo. Se observa que ninguno de los encuestados seleccionó la opción completamente en desacuerdo.

Pregunta 12: Considera usted: ¿Que el diseño de un modelo de auditoría en seguridad informática permitirá el alineamiento con las políticas de seguridad del hospital San Juan Bautista Huaral?

Tabla 6.0. Respuestas de la pregunta 12.

	Frecuencia	**Porcentaje**
Completamente en desacuerdo	1	1
En desacuerdo	13	14
No sabe, no opina	2	2
De acuerdo	51	56
Completamente de acuerdo	25	27
Total	92	100

Interpretación:

Se observa en la tabla 6.0, que el 56% de los encuestados está de acuerdo que el diseño de un modelo de auditoría en seguridad informática permitirá el alineamiento con las políticas de seguridad del hospital San Juan Bautista Huaral; así mismo el 1% está en completamente en desacuerdo.

Pregunta 13: Considera usted: ¿Que el diseño del modelo de auditoria en seguridad física, permitirá alinear las políticas de seguridad del hospital San Juan Bautista Huaral?

Tabla 6.1. Respuestas de la pregunta 13.

	Frecuencia	**Porcentaje**
No sabe, no opina	1	1
De acuerdo	53	58
Completamente de acuerdo	38	41
Total	92	100

Interpretación:

Se observa en la tabla 6.1, que el 58% de los encuestados está de acuerdo que el diseño del modelo de auditoria en seguridad física, permitirá alinear las políticas de seguridad del hospital San Juan Bautista Huaral; así mismo el 41% de los encuestados están completamente de acuerdo y el 1% no saben, no opinan.

Pregunta 14: Considera usted: ¿Que el diseño del modelo de auditoria en seguridad física, permitirá alinear las políticas de seguridad del hospital San Juan Bautista Huaral?

Tabla 6.2. Respuestas de la pregunta 14.

	Frecuencia	**Porcentaje**
En desacuerdo	2	2
No sabe, no opina	3	3
De acuerdo	66	72
Completamente de acuerdo	21	23
Total	92	100

Fuente: Elaboración propia

Interpretación:

Se observa en la tabla 6.2, que el 72% de los encuestados está de acuerdo que el diseño de un modelo de auditoria en seguridad lógica permitirá alinear las políticas de seguridad del hospital San Juan Bautista Huaral; mientras que el 2% está en desacuerdo. Se observa que ninguno de los encuestados seleccionó la opción completamente en desacuerdo.

Pregunta 15: Considera usted: ¿Que la adaptabilidad de los modelos de auditoria en seguridad informática permitirá alinear las políticas de seguridad del hospital San Juan Bautista Huaral?

Tabla 6.3. Respuestas de la pregunta 15.

	Frecuencia	Porcentaje
Completamente en desacuerdo	1	1
En desacuerdo	12	13
No sabe, no opina	1	1
De acuerdo	52	57
Completamente de acuerdo	26	28
Total	92	100

Fuente: Elaboración propia

Interpretación:

Se observa en la tabla 6.3, que el 57% de los encuestados está de acuerdo que la adaptabilidad del modelo de auditoria en seguridad informática permitirá alinear las políticas de seguridad del hospital San Juan Bautista Huaral; mientras que el 1% está completamente en desacuerdo.

5.1.2. Contrastación de hipótesis

5.1.2.1. Hipótesis general

H_0: El diseño de un modelo de auditoría en seguridad informática no permite el alineamiento con las políticas de seguridad del hospital San Juan Bautista Huaral.

H_G: El diseño de un modelo de auditoría en seguridad informática permite el alineamiento con las políticas de seguridad del hospital San Juan Bautista Huaral.

Tabla 6.4. Contrastación hipótesis general de las variables auditoria en seguridad informática y el alineamiento de las políticas de seguridad.

Descripción	Valor
Correlación Rho	0.61
Significancia bilateral (p. valor)	0
Significancia estadística (α)	0.05
Nivel de confianza	0.95
Nº de encuestados	92

Fuente: Elaboración propia

Conclusión:

Se observa en la tabla 6.4, que la correlación entre las variables auditoria en seguridad informática y el alineamiento con las políticas de seguridad es de 0.61 (correlación alta) y es directa debido a que el valor es positivo, además se observa que el valor significante bilateral (p. valor) es menor que el valor significante estadístico (α) por lo que la hipótesis nula $\mathbf{H_0}$ se rechaza y la $\mathbf{H_G}$ se acepta.

5.1.2.2. Hipótesis especifica N° 01

Tabla 6.5. Correlación de hipótesis especifica 01.

VARIABLES	Preguntas de la variable independiente (Auditoria en seguridad física)		
Preguntas de la variable dependiente (Políticas de seguridad)	**Pregunta 01.** ¿Contar con un adecuado sistema de gestión de seguridad de la información permitirá un control adecuado de los sistemas que maneja el hospital San Juan Bautista?	**Pregunta 02.** ¿Las herramientas de seguridad con las que cuenta el hospital San Juan Bautista Huaral son las necesarias para una adecuada protección física de la información?	**Pregunta 03.** ¿La institución debe tener un plan de contingencia en caso de desastres naturales que resguarde la información?
Pregunta 08. ¿Cree usted que las políticas de seguridad tienen un impacto positivo en el área donde labora?	0.42	0.19	0.23
Pregunta 09. ¿Cumplir con las políticas de seguridad del hospital San Juan Bautista da como resultado una adecuada gestión de la información?	0.21	0.22	0.29
Pregunta 10. ¿Las políticas de seguridad que establece el hospital San Juan Bautista influyen con el manejo eficiente de información?	0.29	0.39	0.30
Pregunta 11. ¿Las políticas de seguridad del hospital San Juan Bautista deberían actualizarse para mejorar la productividad del servicio que brindan?	0.30	0.40	0.20

Tabla 6.6. Tabla de contingencia de la variable auditoria en seguridad física y las políticas de seguridad.

PREGUNTAS		**Pregunta 08.** ¿Cree usted que las políticas de seguridad tienen un impacto positivo en el área donde labora?					
		Completamente en desacuerdo	En desacuerdo	No sabe, no opina	De acuerdo	Completamente de acuerdo	Total
Pregunta 01. ¿Contar con un adecuado	En desacuerdo	1	3	1	1	0	6
sistema de gestión de seguridad de la	No sabe, no opina	0	1	1	3	0	5
información permitirá un control adecuado de	De acuerdo	1	3	2	37	12	55
los sistemas que maneja el hospital San Juan Bautista?	Completamente de acuerdo	0	0	1	15	10	26
Total		2	7	5	56	22	92

H_0: El diseño del modelo de auditoria en seguridad física no permite alinear significativamente las políticas de seguridad del hospital San Juan Bautista Huaral.

H_{E1}: El diseño del modelo de auditoria en seguridad física permite alinear significativamente las políticas de seguridad del hospital San Juan Bautista Huaral.

Tabla 6.7. Valores significantes de coeficientes de correlación de Spearman.

Descripción	Valor
Correlación Rho	0.42
Significancia bilateral (p. valor)	0.001
Significancia estadística (α)	0.05
Nivel de confianza	0.95
Nº de encuestados	92

Conclusión:

Se observa en la tabla 6.7, que la correlación entre las variables auditoria en seguridad física y políticas de seguridad es de 0.42 (correlación moderada) y es directa debido a que el valor es positivo, además se observa que el valor significante bilateral (p. valor) es menor que el valor significante estadístico (α) por lo que la hipótesis nula **H0** se rechaza y la **H_{E1}** se acepta.

5.1.2.3. Hipótesis especifica Nº 02

Tabla 6.8. Correlación de hipótesis especifica 02.

VARIABLES	Preguntas de la variable independiente (Auditoria en seguridad lógica)	
Preguntas de la variable dependiente (Políticas de seguridad)	**Pregunta 04.** ¿Deberían existir procedimientos para el registro y control de acceso del personal que se encarga del ingreso y procesamiento de información?	**Pregunta 05.** ¿Las herramientas y técnicas que utiliza la institución son las necesarias para proteger lógicamente la información?
Pregunta 08. ¿Cree usted que las políticas de seguridad tienen un impacto positivo en el área donde labora?	0.33	0.35
Pregunta 09. ¿Cumplir con las políticas de seguridad del hospital San Juan Bautista da como resultado da como resultado una adecuada gestión de la información?	0.22	0.41
Pregunta 10. ¿Las políticas de seguridad que establece el hospital San Juan Bautista influyen con el manejo eficiente de información?	0.23	0.29
Pregunta 11. ¿Las políticas de seguridad del hospital San Juan Bautista deberían actualizarse para mejorar la productividad del servicio que brindan?	0.15	0.21

Tabla 6.9. Tabla de contingencia de la variable auditoria en seguridad lógica y las políticas de seguridad.

PREGUNTAS		**Pregunta 09.** ¿Cumplir con las políticas de seguridad del hospital San Juan Bautista da como resultado una adecuada gestión de la información?				Total
		En desacuerdo	No sabe, no opina	De acuerdo	Completamente de acuerdo	
Pregunta 05. ¿Las herramientas y técnicas que utiliza la institución son las necesarias para proteger lógicamente la información?	No sabe, no opina.	0	0	2	0	2
	De acuerdo	5	7	32	7	51
	Completamente de acuerdo	0	2	22	15	39
Total		5	9	56	22	92

Fuente: Elaboración propia

H_0: El diseño de un modelo de auditoria en seguridad lógica no permite alinear significativamente las políticas de seguridad del hospital San Juan Bautista Huaral.

He_2: El diseño de un modelo de auditoria en seguridad lógica permite alinear significativamente las políticas de seguridad del hospital San Juan Bautista Huaral.

Tabla 7.0. He2 Valores significantes de coeficientes de correlación de Spearman.

Descripción	Valor
Correlación Rho	0.41
Significancia bilateral (p. valor)	0.001
Significancia estadística (α)	0.05
Nivel de confianza	0.95
Nº de encuestados	92

Conclusión: Se observa en la tabla 7.0, que la correlación entre las variables auditoria en seguridad lógica y políticas de seguridad es de 0.41 (correlación moderada) y es directa debido a que el valor es positivo, además se observa que el valor significante bilateral (p. valor) es menor que el valor significante estadístico (α) por lo que la hipótesis nula Ho se rechaza y la **He_2** se acepta.

5.1.2.4. Hipótesis especifica Nº 03

Tabla 7.1. Correlación de hipótesis especifica 03.

VARIABLES	**Preguntas de la variable independiente (Adaptabilidad)**	
Preguntas de la variable dependiente (Políticas de seguridad)	**Pregunta 06.** ¿Los métodos, procedimientos de seguridad que se aplican en el hospital San Juan Bautista se alinean con sus objetivos y metas?	**Pregunta 07.** ¿Se comunica los documentos y normas de seguridad a todos los empleados y unidades que integran la institución?
Pregunta 08. ¿Cree usted que las políticas de seguridad tienen un impacto positivo en el área donde labora?	0.45	0.39
Pregunta 09. ¿Cumplir con las políticas de seguridad del hospital San Juan Bautista da como resultado una adecuada gestión de la información?	0.28	0.24
Pregunta 10. ¿Las políticas de seguridad establece el hospital San Juan Bautista da como resultado una adecuada gestión de la información?	0.40	0.35
Pregunta 11. ¿Las políticas de seguridad del hospital San Juan Bautista deberían actualizarse para mejorar la productividad del servicio que brindan?	0.28	0.26

Tabla 7.2. Tabla de contingencia de la variable adaptabilidad y políticas de seguridad.

PREGUNTAS		**Pregunta 10.** ¿Las políticas de seguridad que establece el hospital San Juan Bautista influyen con el manejo eficiente de información?				Total
		En desacuerdo	No sabe, no opina	De acuerdo	Completamente de acuerdo	
Pregunta 06. ¿Los métodos, procedimientos de seguridad que se aplican en el hospital San Juan Bautista se alinean con sus objetivos y metas?	En desacuerdo	2	0	4	0	6
	No sabe, no opina	0	2	4	2	8
	De acuerdo	0	3	48	8	59
	Completamente de acuerdo	1	0	7	11	19
Total		3	5	63	21	92

H_0: La adaptabilidad del modelo de auditoria en seguridad informática no permite alinear significativamente las políticas de seguridad del hospital San Juan Bautista Huaral.

He_3: La adaptabilidad del modelo de auditoria en seguridad informática permite alinear significativamente las políticas de seguridad del hospital San Juan Bautista Huaral.

Tabla 7.1. He3 Valores significantes de coeficientes de correlación de Spearman.

Descripción	Valor
Correlación Rho	0.40
Significancia bilateral (p. valor)	0
Significancia estadística (α)	0.05
Nivel de confianza	0.95
Nº de encuestados	92

Conclusión:

Se observa en la tabla 7.1, que la correlación entre las variables adaptabilidad y políticas de seguridad es de 0.40 (correlación moderada) y es directa debido a que el valor es positivo, además se observa que el valor significante bilateral (p. valor) es menor que el valor significante estadístico (α) por lo que la hipótesis nula **H_0** se rechaza y la **He_3** se acepta.

CAPÍTULO VI

DISCUSION, CONCLUSIONES Y RECOMENDACIONES

11.1. Discusiones

En el presente informe de tesis se investigó la auditoria en seguridad informática y el alineamiento con las políticas de seguridad del hospital San Juan Bautista ubicado en la provincia de Huaral, con una muestra de 92 colaboradores, se estudió también la situación actual de la institución, relacionado a los niveles de seguridad que aplica para proteger la información, con base a esto se dio origen a las hipótesis especificas en las que se desarrolla la siguiente investigación.

En base a los resultados hallados en esta investigación se puede afirmar que existe una correlación entre la auditoria en seguridad informática y el alineamiento con las políticas de seguridad, lo cual demuestra que el personal que labora en la institución es consciente que es importante aplicar auditoria en seguridad informática.

La auditoría en seguridad informática y el alineamiento con las políticas de seguridad son dos factores de mucha importancia para la institución al demostrar que existe una correlación entre ambas, pudiéndose aplicar en cualquier institución y adecuándolo con sus propios objetivos. De esta manera se reducirá el riesgo a perder información que puede ser perjudicial para la continuidad del negocio.

Para las futuras investigaciones se recomienda que se realice un análisis con cada miembro que forma parte del hospital San Juan Bautista, lo que involucra a todas las áreas de esta manera la investigación será más completa.

11.2. Conclusiones

Durante la investigación de esta tesis puedo concluir lo siguiente:

- En base a la información recopilada de la encuesta, se obtuvo que 51 personas (56%) del total de la muestra, manifestaron estar de acuerdo que el diseño de un modelo de auditoría en seguridad informática permitió el alineamiento con las políticas de seguridad, así mismo mediante la prueba Rho spearman entre las variables auditoria en seguridad informática y las políticas de seguridad de la hipótesis general, se obtuvo un valor de 0.61 demostrando que si hay correlación alta entre ellas, además se observó que el valor significante bilateral (p. valor = 0) es menor que el valor significante estadístico ($\alpha = 0.05$) por lo que la hipótesis nula es rechazada y la hipótesis alternativa aceptada. Con esto puedo concluir que el modelo de auditoria en seguridad informática alinea las políticas de seguridad del hospital San Juan Bautista Huaral.
- Con la información obtenida de la encuesta, se observó que 53 personas (58%) del total de la muestra, consideran que el diseño de un modelo de auditoria en seguridad física permitió alinear las políticas de seguridad, así mismo mediante la prueba Rho spearman entre las variables auditoria en seguridad física y las políticas de seguridad de la hipótesis especifica 01, se

obtuvo un valor de 0.42 demostrando que si hay correlación moderada entre ellas, además se observó que el valor significante bilateral (p. valor = 0.001) es menor que el valor significante estadístico (α = 0.05) por lo que la hipótesis nula es rechazada y la hipótesis alternativa aceptada. Con esto puedo concluir que el diseño de un modelo de auditoria en seguridad física contribuye con al alineamiento de las políticas de seguridad del hospital San Juan Bautista Huaral.

- De acuerdo a los datos obtenidos en la encuesta, se obtuvo que 66 personas (72%) del total de la muestra, manifestaron estar de acuerdo que el diseño de un modelo de auditoria en seguridad lógica permitió el alineamiento de las políticas de seguridad, así mismo a través de la prueba Rho spearman entre las variables auditoria en seguridad lógica y las políticas de seguridad de la hipótesis especifica 02, se obtuvo un valor de 0.41 demostrando que existe una correlación moderada entre ellas, además se observó que el valor significante bilateral (p. valor = 0.001) es menor que el valor significante estadístico (α = 0.05) por lo que la hipótesis nula es rechazada y la hipótesis alternativa es aceptada. Con esto se puede concluir que el diseño de un modelo de auditoria en seguridad lógica permite el alineamiento de las políticas de seguridad del Hospital San Juan Bautista Huaral.

- En base a la información recopilada de la encuesta, se obtuvo que 52 personas (57%) del total de la muestra, manifestaron estar de acuerdo que la adaptabilidad del modelo de auditoría en seguridad informática permitió el alineamiento con las políticas de seguridad, así mismo mediante la prueba Rho spearman entre las variables auditoria en seguridad informática y las

políticas de seguridad de la hipótesis especifica 03, se obtuvo un valor de 0.40 demostrando que si hay correlación moderada entre ellas, además se observó que el valor significante bilateral (p. valor = 0) es menor que el valor significante estadístico ($\alpha = 0.05$) por lo que la hipótesis nula es rechazada y la hipótesis alternativa aceptada. Con esto puedo concluir que la adaptabilidad del modelo de auditoria en seguridad informática permite el alineamiento de las políticas de seguridad del hospital San Juan Bautista Huaral.

11.3. Recomendaciones

Una vez concluida esta investigación de tesis se procede a sugerir las siguientes recomendaciones:

- Como primera recomendación de este trabajo de tesis, se sugiere tomar en cuenta las recomendaciones planteadas en los diferentes controles auditados en el transcurso de la auditoria y que estén debidamente documentados.

- Los jefes de área son quienes deberán difundir esta cultura y a su vez monitorizar que se haga un correcto uso de las herramientas que procesan información.

Se recomienda a todas las instituciones del sector salud que establezcan periódicamente auditorias en seguridad informática.

CAPÍTULO VII

FUENTES DE INFORMACIÓN

7.1. Fuentes bibliográfica

- Aldegani, G. (1997). *Seguridad informática*. Mp. Ediciones.
- Cervigón, A; Alegre, M (2011). *Seguridad Informática*. Madrid, España.
- Echenique, J (2008). *Auditoria en Informática segunda edición*. México.
- Editorial Editex S. A (2010). *Seguridad Informática*. Madrid, España.
- INDECOPI (2007). EDI. *Tecnología de la Información. Código de buenas Prácticas para la Gestión de la Seguridad de la Información. NTP-ISO/IEC 17799-2007*.Lima, Perú.
- ISACA (2007). COBIT 4.1 Edición en español.
- Lázaro, M (2008). *Seguridad de la Información. Oficina Nacional de Gobierno Electrónico e Informática PCM*. Perú.
- Monzón, C. (2009). *Auditoria de seguridad de redes inalámbricas de área local Wireless Local Área Network (WLAN)*. Universidad Mayor de San Andrés. Bolivia.
- Muñoz, C. (2010). *Auditoría en Sistemas Computacionales*. México.
- Piattini, M (2001). *Auditoria informática. Un enfoque Práctico*. Ra-Ma.

7.2. Fuentes Documentales

- Álvarez, B. (2005). Tesis titulada *Seguridad en Informática (Auditoria de Sistemas).* México.
- Ampuero, C (2011). Tesis titulada *Diseño De Un Sistema De Gestión De Seguridad De Información Para Una Compañía De Seguros*. Perú.
- Cadme, C; Duque, D (2012). Tesis titulada *Auditoría de Seguridad Informática ISO 27001 para la empresa de alimentos ITALIMENTOS CIA.LTDA.* Ecuador.
- Córdova, N (2008). Tesis titulada *Plan de Seguridad Informática para una Entidad Financiera*. Perú.
- Martínez, V (2010). Tesis titulada *Concientización En Seguridad De La Información, La Estrategia Para Fortalecer El Eslabón Más Débil De La Cadena.* Colombia.
- Reyes, M (2011). Tesis titulada *Propuestas para impulsar la seguridad informática en materia de educación.* México.
- Santa María, B. (2011). Tesis titulada *Buenas Prácticas para Auditar Redes Inalámbricas Aplicadas a las Empresas del Rubro Hotelero de la Ciudad de Chiclayo*. Perú.
- Tola, D. (2012). Tesis titulada *Implementación De Un Sistema De Gestión De Seguridad De La Información Para Una Empresa De Consultoría Y Auditoría, Aplicando La Norma ISO/IEC 27001*. Ecuador.
- Villena, M (2006). Tesis titulada *Sistema De Gestión De Seguridad De Información Para Una Institución Financiera*. Perú.

ANEXO 1: Matriz de Consistencia

Título: Auditoria en seguridad informática y el alineamiento con las **políticas de seguridad** del hospital San Juan Bautista Huaral

Problema Principal	Objetivo General	Hipótesis Principal	Variables	Dimensiones	Indicadores
¿Cómo el diseño de un modelo de auditoría informática permitirá el alineamiento con las políticas de seguridad del hospital San Juan Bautista Huaral?	Diseñar un modelo de auditoria en seguridad informática que permita un alineamiento con las políticas de seguridad del hospital San Juan Bautista Huaral.	El diseño de un modelo de auditoría en seguridad informática permitirá el alineamiento con las políticas de seguridad del hospital San Juan Bautista Huaral.	Auditoria en seguridad informática	Auditoria en seguridad física	• Gestión de la seguridad • Protección física • Plan de contingencia
Problema Específicos	**Objetivos Específicos**	**Hipótesis Específicas**			
¿En qué medida el modelo de auditoria en seguridad física permitirá alinear las políticas de seguridad del hospital San Juan Bautista Huaral?	Determinar la medida con la cual el modelo de auditoria en seguridad física permitirá alinear las políticas de seguridad del hospital San Juan Bautista Huaral.	El diseño del modelo de auditoria en seguridad física, permitirá alinear significativamente las políticas de seguridad del hospital San Juan Bautista Huaral.		Auditoria en seguridad lógica	• Control de acceso • Herramientas y técnicas
¿De qué manera un modelo de seguridad lógica, permitirá el alineamiento de las políticas de seguridad en el hospital San Juan Bautista Huaral?	Analizar la manera en que el modelo de auditoria en seguridad lógica permitirá alinear las políticas de seguridad del hospital San Juan Bautista Huaral.	El diseño de un modelo de auditoria en seguridad lógica permitirá alinear significativamente las políticas de seguridad del hospital San Juan Bautista Huaral.		Adaptabilidad	• Métodos y procedimientos • Normas y documentos
¿De qué forma la adaptabilidad del modelo de auditoría informática, permitirá el alineamiento de las políticas de seguridad en el hospital San Juan Bautista Huaral?	Establecer la forma con la cual la adaptabilidad del modelo de auditoria de seguridad informática permitirá alinear las políticas de seguridad del hospital San Juan Bautista Huaral.	La adaptabilidad del modelo de auditoria en seguridad informática permitirá alinear significativamente las políticas de seguridad del hospital San Juan Bautista Huaral.	Políticas de seguridad	Políticas de seguridad de la información	• Nivel de impacto • Nivel de resultado
				Mejora continua	• Nivel de eficiencia • Nivel de productividad

ANEXO 2: Instrumento para toma de datos

Cuestionario: Seguridad Informática en aplicada en la institución

Hospital San Juan Bautista - Huaral		
	Área	Fecha

Indicación: Marque con la casilla que corresponda a su respuesta según su criterio

1. ¿Contar con un adecuado sistema de gestión de seguridad de la información permitirá un control adecuado de los sistemas que maneja el hospital San Juan Bautista?

Completamente en desacuerdo	En desacuerdo	No sabe, no opina	De acuerdo	Completamente de acuerdo
○	○	○	○	○

2. ¿Las herramientas de seguridad con las que cuenta el hospital San Juan Bautista Huaral son las necesarias para una adecuada protección física de la información?

Completamente en desacuerdo	En desacuerdo	No sabe, no opina	De acuerdo	Completamente de acuerdo
○	○	○	○	○

3. ¿La institución debe tener un plan de contingencia en caso de desastres naturales que resguarde la información?

Completamente en desacuerdo	En desacuerdo	No sabe, no opina	De acuerdo	Completamente de acuerdo
○	○	○	○	○

4. ¿Deberían existir procedimientos para el registro y control de acceso del personal que se encarga del ingreso y procesamiento de información?

Completamente en desacuerdo	En desacuerdo	No sabe, no opina	De acuerdo	Completamente de acuerdo
○	○	○	○	○

5. ¿Las herramientas y técnicas que utiliza la institución son las necesarias para proteger lógicamente la información?

Completamente en desacuerdo	En desacuerdo	No sabe, no opina	De acuerdo	Completamente de acuerdo
○	○	○	○	○

6. ¿Los métodos, procedimientos de seguridad que se aplican en el hospital San Juan Bautista se alinean con sus objetivos y metas?

Completamente en desacuerdo	En desacuerdo	No sabe, no opina	De acuerdo	Completamente de acuerdo
○	○	○	○	○

7. ¿Se comunica los documentos y normas de seguridad a todos los empleados y unidades que integran la institución?

Nunca	Casi nunca	A veces	Casi siempre	Siempre
○	○	○	○	○

8. ¿Cree usted que las políticas de seguridad tienen un impacto positivo en el área donde labora?

Completamente en desacuerdo	En desacuerdo	No sabe, no opina	De acuerdo	Completamente de acuerdo
○	○	○	○	○

9. ¿Cumplir con las políticas de seguridad del hospital San Juan Bautista da como resultado una adecuada gestión de la información?

Completamente en desacuerdo	En desacuerdo	No sabe, no opina	De acuerdo	Completamente de acuerdo
○	○	○	○	○

10. ¿Las políticas de seguridad que establece el hospital San Juan Bautista influye con el manejo eficiente de información?

Completamente en desacuerdo	En desacuerdo	No sabe, no opina	De acuerdo	Completamente de acuerdo
○	○	○	○	○

11. ¿Las políticas de seguridad del hospital San Juan Bautista deberían actualizarse para mejorar la productividad del servicio que brindan?

Completamente en desacuerdo	En desacuerdo	No sabe, no opina	De acuerdo	Completamente de acuerdo
○	○	○	○	○

12. Considera usted: ¿Que el diseño de un modelo de auditoría en seguridad informática permitirá el alineamiento con las políticas de seguridad del hospital San Juan Bautista Huaral?

Completamente en desacuerdo	En desacuerdo	No sabe, no opina	De acuerdo	Completamente de acuerdo
○	○	○	○	○

13. Considera usted: ¿Que el diseño del modelo de auditoria en seguridad física, permitirá alinear las políticas de seguridad del hospital San Juan Bautista Huaral?

Completamente en desacuerdo	En desacuerdo	No sabe, no opina	De acuerdo	Completamente de acuerdo
○	○	○	○	○

14. Considera usted: ¿Que el diseño de un modelo de auditoria en seguridad lógica permitirá alinear las políticas de seguridad del hospital San Juan Bautista Huaral?

Completamente en desacuerdo	En desacuerdo	No sabe, no opina	De acuerdo	Completamente de acuerdo
○	○	○	○	○

15. Considera usted: ¿Que la adaptabilidad de los modelos de auditoria en seguridad informática permitirá alinear las políticas de seguridad del hospital San Juan Bautista Huaral?

Completamente en desacuerdo	En desacuerdo	No sabe, no opina	De acuerdo	Completamente de acuerdo
○	○	○	○	○