+

FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

APLICACIÓN DE LA HERRAMIENTA DE GESTIÓN DE RIESGOS PARA LA SEGURIDAD INFORMÁTICA DEL HONADOMANI SAN BARTOLOMÉ

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE INGENIERÍA DE SISTEMAS

AUTOR:

CALDERÓN ALVARADO, JERSON JOSEPH

ASESOR:

ING. VERGARA CALDERON RODOLFO SANTIAGO

LÍNEA DE INVESTIGACIÓN

GESTIÓN DE TECNOLOGÍAS Y SISTEMAS DE INFORMACIÓN

LIMA – PERÚ

2017

DEDICATORIA

El presente trabajo de investigación se lo dedico a Dios que me ha guiado y dado la sabiduría a lo largo de la carrera. A mis padres Jorge Calderón Quispe y Rosario Alvarado Buleje por apoyarme en todo momento y darme las ánimos para seguir adelante y a mis hermanos por brindarme su amor y comprensión.

AGRADECIMIENTO

Agradezco a cada una de las docentes que me han enseñado a lo largo de estos cinco años de carrera, de manera especial al Inge. Villegas Flores Iván, que me ha apoyado en mi proyecto de tesis y al Ingeniero Vergara Calderón Rodolfo Santiago, que me ha apoyado para el desarrollo de este proyecto.

INDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

GENERALIDADES

- **TÍTULO**

APLICACIÓN DE LA HERRAMIENTA DE GESTIÓN DE RIESGOS PARA LA SEGURIDAD INFORMÁTICA DEL HONADOMANI SAN BARTOLOMÉ

- **AUTOR**

Jerson Joseph, Calderón Alvarado

- **ASESOR**

Ing. Vergara Calderón Rodolfo Santiago

- **TIPO DE INVESTIGACIÓN**

Aplicada – NO Experimental

- **LÍNEA DE INVESTIGACIÓN**

Gestión de tecnologías y sistemas de información

- **LOCALIDAD**

Lima

- **DURACIÓN DE LA INVESTIGACIÓN**

Desde el 29 de agosto del 2016 al 14 de Julio del 2017

CAPÍTULO - 01:

I. INTRODUCCIÓN

En los últimos tiempos las organizaciones sugieren que se apliquen herramientas para la gestión de riesgo; porque es importante evaluar, implementar, medir y mejorar los controles de seguridad de la información día a día, por lo cual la aplicación de la herramienta de gestión de riesgos para la seguridad informatica es fundamental para el proceso óptimo de las necesidades de la organización

El Hospital Nacional Madre Niño San Bartolomé carece de una gestión de riesgos, en donde cada 2 años hacen un mantenimiento a su plan de contingencia pero no les ayuda a identificar sus vulnerabilidades y amenazas de sus activos de información. Donde se reúnen el área de informática y la dirección general del hospital para poder realizar un plan de contingencia para la seguridad de la información. En la gestión de riesgo que plantean no se realizan documentos, ni se argumenta el problema general que ocasiona las incidencias diarias que generan los riesgos y disminuyen las medidas del control de seguridad de información. Al no haber una documentación detallada respecto a la gestión de riesgo, no existe una guía para identificar las vulnerabilidades de los activos de la seguridad de la información que nos ayude a la recolección, agrupación y evaluación de evidencias, permitiendo hacer observaciones y poder corregirlas para la mejora de proceso del hospital, la oficina de informática quisiera tener una herramienta de gestión de riesgos para poder identificar las vulnerabilidad de los activos y las riesgos que estén afectando a los activos de la seguridad informática y así poder administrarla de una mejor manera.

La presente tesis se realizará en el Hospital Nacional Madre Niño San Bartolomé, con la finalidad de aplicar una herramienta de gestión de riesgos para la seguridad informática. El objetivo principal de esta tesis es determinar la influencia de la aplicación de una herramienta de gestión de riesgos para la seguridad informatica del HONADOMANI San Bartolomé. El tipo de investigación es aplicada-no experimental y el diseño de investigación es longitudinal de tendencia. La metodología de desarrollo para la aplicación de la herramienta de gestión de riesgos es MAGERIT, y como herramienta de trabajo para magerit se utilizará la MATRIZ DE RIESGOS DE MAGERIT y la ISO/IEC 27001:2013 para la auditoria.

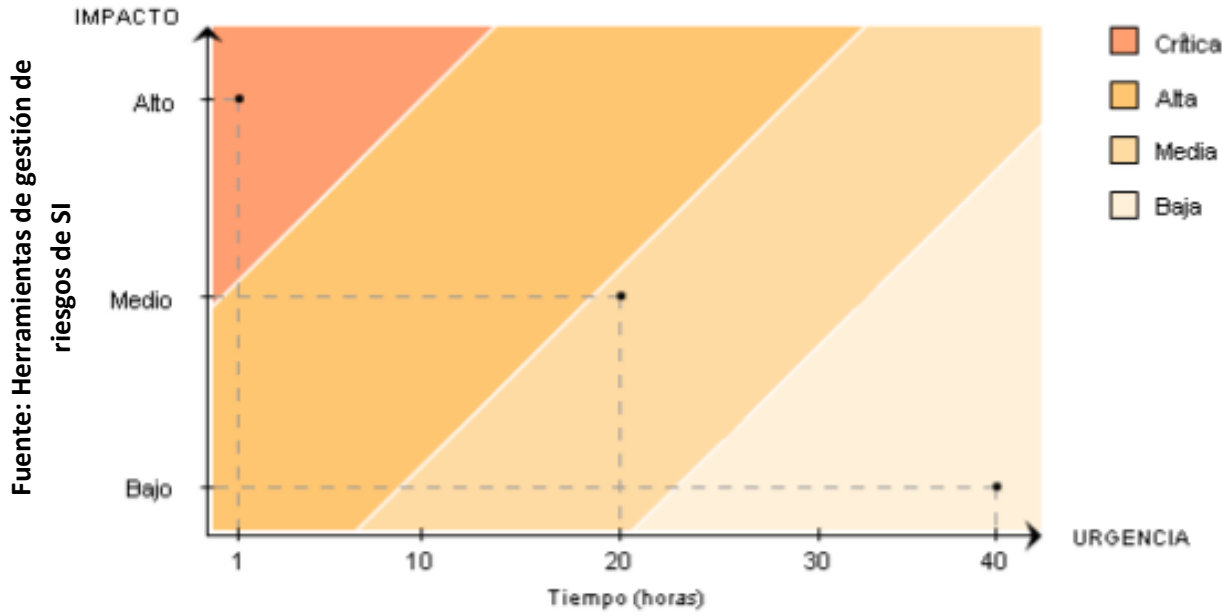
La presente investigación se divide en cuatro capítulos. En el capítulo I, introducción referente al proyecto y en el capítulo II Método

1.1 REALIDAD PROBLEMÁTICA

"La herramienta de gestión de riesgos se define como un plan para la implantación de controles de seguridad en los sistemas de información que permite disminuir la probabilidad de que se materialice una amenaza, reducir la vulnerabilidad del sistema o el posible impacto en la organización, y posibilite la recuperación del sistema en caso de una afectación grave."[1]

La herramienta de gestión de riesgos permite asignar las prioridades a través del impacto y la urgencia que requiere cada activo de información como se mostrará en la figura N°1.

Figura N°1



Fuente: Herramientas de gestión de riesgos de SI

Diagrama de actividades

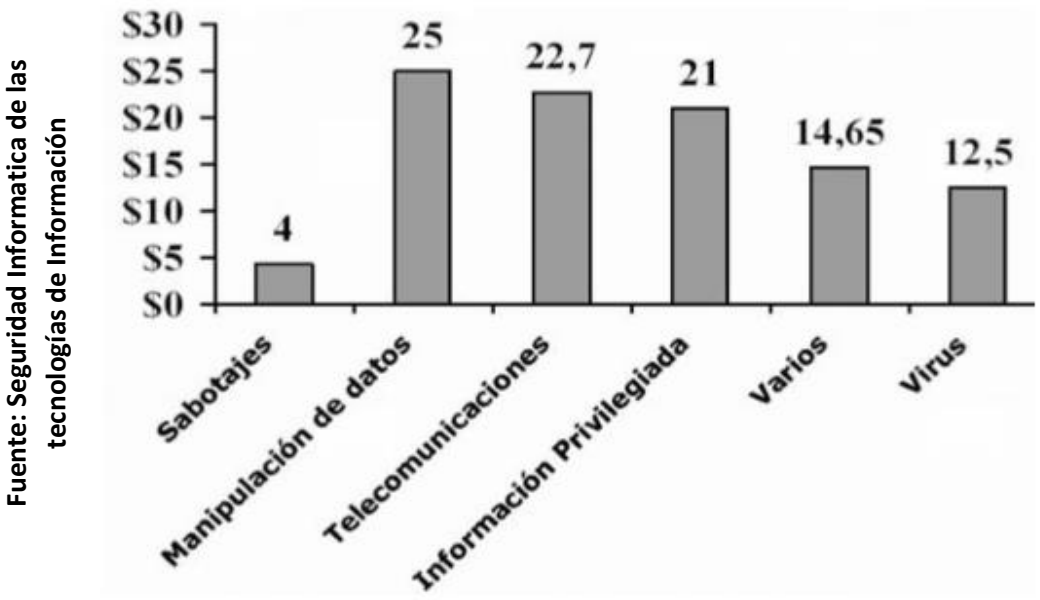
"La seguridad informatica establece políticas de trabajo, conocimientos claros y apoyo de la alta dirección para poder tener los recursos informáticos, a través de ello poder alcanzar un nivel de seguridad razonable y capaz de satisfacer las expectativas de seguridad."[2]

[1] Gabriel Sánchez Pérez, Herramientas de gestión de riesgos de SI, 2012. 20 p. ISBN: 486-23-145632-1-8

[2] Perafan Ruiz John. Seguridad Informatica de las tecnologías de Información, Ecuador, Popayán, 2014. 10 p. ISBN: 120234586-1

Las perdidas monetarias que tienes las organizaciones se mostraran en la figura N°2

Figura N°2



Perdidas monetarias de las organizaciones

El presente proyecto de investigación de tesis se desarrolla en el Hospital Nacional Docente Madre Niño San Bartolomé, ubicada en el distrito de Lima Centro. Esta organización se ha consolidado como una entidad hospitalaria por su atención altamente especializada a la salud sexual y reproductiva de la mujer y a la salud del feto.

De acuerdo a la entrevista realizada al Ingeniero de Sistemas Jardy Spilco León; jefe del área de Sistema e Informática (ver anexo N°2), indica que el Hospital Nacional Docente Madre Niño San Bartolomé no cuenta con una gestión de riesgos para la seguridad informatica que les ayude a identificar las vulnerabilidades y amenazas de sus activos de información. También comento que el hospital al no contar con una gestión de riesgos no incluye políticas, normas y procedimientos para los activos de información, donde esto tiene como alcance definir los escenarios y situaciones que pudieran proveerse con la finalidad de permitir la operación de los sistemas críticos de la institución a través de la gestión de riesgos. El hospital busca con la gestión de riesgos para la seguridad informatica poder minimizar los riesgos que ocasiona cada incidencia y mantener controlado las amenazas que pudieran tener los activos de

información. El Ingeniero comenta que el último plan de contingencia se realizó en el año 2014 teniendo como referencia al análisis de riesgos, pero que él quiere tener una herramienta de análisis para el proceso de gestión de riesgos en la seguridad informática para poder identificar las vulnerabilidades y las amenazas que afecten a las vulnerabilidades que tiene y que podrían tener el Hospital.

Durante los periodos del años 2000 y 2013 se realización 5 auditorías informáticas al área de informática donde los resultados no fueron muy positivo para la institución hospitalaria. Por cada Auditoria se formularon 20 observaciones, de las cuales la mitad de ellas se centraban en la gestión de riesgos y seguridad informática, el resto se centraba en el rol del personal que pertenece al área de informática, las cuales de esas observaciones solo se solucionaban el 30% y las demás quedaban como pendientes, pero cuando se realizaba otra auditoria informática aparecían nuevas observaciones del mismo caso, acerca de la gestión de riesgo y la seguridad informática.

En la gestión de riesgo que se observaba en las auditorias informáticas se citaban que el área de sistemas no puede identificar las vulnerabilidades de los activos de información y las amenazas que podría tener el hospital en caso un activo sea vulnerado, y dentro de la seguridad informatica se citaban los puntos de seguridad lógica para los sistemas de información, la seguridad física para las herramientas tecnológicas del hospital y la seguridad de redes para la integridad y disponibilidad de la seguridad de la información.

“La seguridad lógica se encarga de implementar controles de acceso que están creados para salvaguardar la integridad y confidencialidad de la información almacenada de un dispositivo intermedio o final. También se encarga de controlar y salvaguardar toda información desarrollada por los sistemas y por los programas en aplicación, nos ayuda a identificar a cada usuario y sus actividades que realizan en el sistema, y por ello les restringe el acceso de datos y accesos de red.”[3]

Dentro de la red lógica el hospital no cuentan con registros de listas de control de acceso, cantidad de usuarios que tienen acceso a la red y grupos de accesos

[3] Cisco Networking Academy, principios y guías de Seguridad de información. 3ra. Ed. EE.UU., Manhattan, 2016. 48 p

para la red interna del hospital, además el hospital no cuenta con un respaldo de back-up de información dado que al momento que la red deja de funcionar, el servidor tiene que ser reiniciado y toda la información que los usuarios han realizado durante ese periodo se pierde y el último punto es que el servidor del antivirus es inestable, cuando el usuario de soporte quiere instalar en algún ordenador el antivirus no puede, porque el servidor del antivirus esta con la sesión cerrada..

"La seguridad física permite implementar controles y procesos de la seguridad dentro y fuera del centro de cómputo así como los medios de acceso remoto, implementados para proteger el hardware y los medios de almacenamiento de datos. Es muy importante, que nuestra organización sea la más segura de ataques externos, hackers, virus, etc.; la seguridad será nula si no se ha implementado medidas de control."[4]

Dentro de la red física tenemos la falta de estándares para la infraestructura del área de telecomunicaciones, el cableado estructurado y armado de gabinetes, además no cuentan con documentaciones acerca del mantenimiento preventivo y correctico de equipos, equipos con garantía e inventario de equipos.

"La seguridad en redes es mantener la integridad, disponibilidad, privacidad, control y autenticidad de la información que está integrada en las computadoras, a través de una serie de pasos basados en una política de seguridad que permitan el control adecuado de la información."[5]

Dentro de la seguridad de redes el hospital carece de políticas y normas de seguridad, además no cuenta con una red estable por momentos es inestable para el funcionamiento de sus sistemas de información y herramientas tecnológicas que utilizan los usuarios día a día y finalmente no hay una gestión de riesgos para mitigar los riesgos para la red.

1.2 TRABAJOS PREVIOS

En el año 2013, Karina del rocío Gaona Vásquez, elabora la tesis titulada "Aplicación de la metodología magerit para el análisis y gestión de riesgos de la

[4] Huerta, Seguridad en Unix y redes, Ecuador, Quito. 2012. 150 p.
[5] Bustamante, Seguridad en redes, 1ra Ed, Colombia, Bogotá 2012 40 p. ISBN: 436782657-0

seguridad de la información aplicado a la empresa pesquera e industrial bravito s.a. en la ciudad de Machala", para obtener el tirulo de ingeniería de sistemas en la universidad politécnica salesiana sede cuenca - Ecuador

"La gestión de riesgos son procedimientos formales para encontrar los riesgos que existen en un sistema de información y mediante un estudio responsable, recomienda medidas apropiadas que deberían acogerse para controlarlos, además se podrá saber el estado real de seguridad en una empresa."[6]

El método para esta investigación fue MAGERIT según Gaona está dirigido a los medios electrónicos, informáticos y telemáticos, ya que su uso en la actualidad es frecuente, lo cual ha dado lugar al origen de ciertos riesgos que se deben de evitar con medidas preventivas para lograr confianza en utilizarlos.

Los resultados fueron que se pudo hacer un plan de seguridad gracias a la metodología MAGERIT y que se pudo eliminar fallos de la seguridad, clasificación de inventario y normativas de seguridad.

De este antecedente se escogió a la metodología MAGERIT donde se siguió una serie de pasos estructurados para el análisis y gestión de riesgos, fase fundamental en este estudio ya que se obtuvo resultados realistas del estado de riesgo actual en la empresa donde se supo escoger que medidas serán necesarias para mitigar el riesgo"

De este antecedente se tomó como referencia la metodología MAGERIT, porque nos ayuda a clasificar los niveles de riesgos y a poder comparar con nuestra tesis en la discusión respecto al nivel de cumplimiento de la seguridad informatica.

En el año 2013, Iván Ricardo Narváez Barreiros, elabora la tesis titulada "Aplicación de la norma ISO/IEC 27001 para la implementación de un SGSI en la fiscalía general del estado", para obtener el título de Ingeniero en Sistemas y Computación en la Pontificia Universidad Católica del Perú

"Un SGSI es asegurar de la manera más eficiente que la información disponga de confidencialidad, integridad y disponibilidad, considerando a la información

[6] Gaona, K. Aplicación de la metodología magerit para el análisis y gestión de riesgos de la seguridad de la información, Ecuador, Cuenca, 2013, 8 p. ISBN: 1-542369-742

como un activo importante en la empresa o institución, a la vez de gestionar los riesgos a la que esta pueda ser sometida."[7]

El método para esta investigación fue la ISO27001 que es un estándar internacional que ha sido elaborado para proporcionar un modelo definido para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI.

Los resultados indican cierta cantidad de incidencias en distintos niveles de vulnerabilidad, para este efecto necesitamos establecer mediante una metodología cuales son los posibles tratamientos a nivel general para cada uno de los niveles de vulnerabilidad. En este caso, de acuerdo con la metodología OCTAVE se establece un procedimiento de análisis, identificación y valoración de riesgos, para posteriormente iniciar el proceso para aplicar los respectivos enfoques de mitigación de riesgos.

Las conclusiones analizando las características de la institución que se ha sometido a estudio, se revela la necesidad de implementar un SGSI, debido a la complejidad de los procesos, normativa legal vidente y cantidad de registros que se ingresan y analizan cada día.

De este antecedente se tomará como referencia a la metodología OCTAVE para poder comparar la gestión de riesgos con la metodología MAGERIT.

En el año 2013, Dan Lonita elabora la tesis Current established risk assessment methodologies and tools, para que obtenga el título de master in computer science of information systems in the university of twente – Netherlands.

"La gestión de riesgo es un proceso destinado a un equilibrio eficiente entre las oportunidades dándose cuenta de ganancias y reducir al mínimo las vulnerabilidades y las perdidas"[8]

Una de las metodologías de trabajo en esta tesis es MAGERIT, según Lonita MAGERIT ayuda a determinar los activos relevantes para la organización, sus interrelaciones y su valor. Los activos son los recursos del sistema de

[7] Narváez, Iván, Aplicación de la norma ISO/IEC 27001 para la implementación de un SGSI, Ecuador, Quito, 2013. 9 p. ISBN: 123-78-100253-1-8

[8] Lonita, Current established risk assessment methodologies and tools, Netherlands, Twente. 2013. 12 p. ISBN: 112-30-453689-1-0

información o relacionad con el que son necesarios para que la organización funcione correctamente y lograr los objetivos propuestos por su gestión

Los resultados fueron que se pudo comparar 14 metodologías de riesgos de tecnologías de información, y la que más se adapta a las empresas fue MAGERIT

Las conclusiones son el aumento de la necesidad de proteger adecuadamente los sistemas de información ha recorrido un aumento en el número y la diversidad de metodologías y herramientas para ayudar a lograr esto"

De esta tesis se tomara de referencia la metodología MAGERIT dado que después de una comparación fue la más adaptable para la organización.

En el año 2012, Barrantes Porras Carlos Eduardo y Hugo Herrera Javier Roberto, elaboran la tesis titulada "Diseño e implementación de un sistema de gestión de seguridad de información en procesos tecnológicos", para que obtengan el título de Ingeniero de Computación y Sistemas en la Universidad San Martin de Porres – Perú

"Las organizaciones públicas y privadas día a día generan conocimientos, datos, reportes, actas y material de diferente índole de suma importancia para ellas, lo cual representa toda la información que requieren para su funcionalidad. (…) Debido al crecimiento y expansión de Card Perú S.A., entidad emisora de tarjetas de crédito, la probabilidad de que la información sea interceptada, robada y/o modificada por personas inescrupulosas y sin autorización de acceso de esa, ha aumentado exponencialmente."[9]

La metodología para la gestión del proyecto fue PMBOK y como metodología de la gestión de riesgo MAGERIT

Se propone la implementación de SGSI, el cual nos brindara los procedimientos y lineamientos necesarios para identificar y evaluar los riesgos y las amenazas que ayudaran a salvaguardarse los activos de información de los procesos de tecnología, mantener y mejorar continuamente el SGSI aliándolo de esta manera a los objetivos estratégicos de la organización

[9] Barrantes y Hugo, Diseño e implementación de un sistema de gestión de seguridad de información en procesos tecnológicos, Perú, Lima, 2012. 10 p. ISBN: 568-78-674235-1-5

Los resultados señalan que Tenían un 34% de cumplimiento de los requisitos, (…) después del análisis, gestión y tratamiento del riesgo, proceso en el cual se implementaron todos los controles preventivos, detectivos y correctivos necesarios para minimizar la brecha, se logró mejorar drásticamente el porcentaje de cumplimiento a un 67%

Las conclusiones es poder implementar una política de seguridad y que los colaboradores la conozcan e interiorizan, es de gran utilidad se quiere implementar cualquier sistema de gestión en una organización, ya que les da una visión clara de cómo sus labores cotidianas aportan para el mantenimiento y mejora de un sistema de gestión empresarial

De este antecedente se tomará como referencia a la variable independiente para poder determinar los procesos de la gestión de riesgos en la seguridad informatica.

En el año 2011 Ewelina Gajewska Mikaela Ropel, elabora la tesis titulada, "Risk managment practices in a construction project – a case study", para obtener el grado de master of science thesis in the master's programmer in the chalmers university of technology – Suecia

"La gestión de riesgos consiste en la aplicación sistemática de políticas, procesos y procedimientos para la tarea de establecer el contexto, identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos."[10]

Esta tesis desarrolla un plan de gestión de riesgos de tecnologías de información, toma en general la medida de los riesgos.

Los resultados fueron según la investigación que la acción más común era la mitigación de riesgos. Además se comprobó que los resultados de la probabilidad y el impacto método pueden diferir entre los proyectos debido al hecho de que cada proyecto y su alcance son únicos.

Las conclusiones fueron que mediante la aplicación de un método simple, es posible identificar los riesgos potenciales de una manera fácil. Además se da la posibilidad de detectar cuál de los riesgos identificados tiene mayor impacto en

[10] Ewelina, Mikaela, Risk managment practices in a construction project – a case study, Suecia, 2011 15 p, ISBN: 785623589-1

el tiempo, costo y calidad. Estos riesgos deben ser eliminados o mitigados mediante la adopción de una acción apropiada.

De este antecedente se toma como referencia a la variable independiente que es la gestión de riesgos, porque nos ayuda a darle un nivel de significancia a cada riesgos para poder mitigarlos y tenerlos controlados para cuando vuelvan a aparecer

1.3 TEORÍAS RELACIONADAS AL TEMA

1.3.1 HERRAMIENTA DE GESTIÓN DE RIESGOS

"La herramienta de gestión de riesgos se define como un plan para la implantación de controles de seguridad en los sistemas de información que permite disminuir la probabilidad de que se materialice una amenaza, reducir la vulnerabilidad del sistema o el posible impacto en la organización, y posibilite la recuperación del sistema en caso de una afectación grave."[11]

"La herramienta de gestión de riesgos permite saber cuáles son las principales vulnerabilidades de sus activos de información y cuáles son las amenazas que podrían explotar las vulnerabilidades. En la medida que la empresa tenga clara esta identificación de riesgos podrá establecer las medidas preventivas y correctivas viables que garanticen mayores niveles de seguridad en su información."[12]

"La herramienta de gestión de riesgos nos permite la selección e implantación de salvaguardas que nos ayudan a conocer, prevenir, impedir, reducir los riesgos identificados por la organización."[13]

ANALISIS DE RIESGOS

"El análisis de riesgo nos permite identificar cuáles son los riesgos más relevantes de la organización. Y nos ayuda a clasificar un activo de información por dimensiones:"[14]

[11] Gabriel Sánchez Pérez, Herramientas de gestión de riesgos de SI, 2012. 20 p. ISBN: 486-23-145632-1-8

[12] Camilo Gutiérrez Amaya, Herramientas de gestión de riesgos de información, 2012. 15 p. ISBN: 178952354-1

[13] Duque Ocho0a Blanca, Herramienta de gestión de riesgos para la seguridad informatica, 2013. 19 p. ISBN: 121124569-2

[14] Gabriel Sánchez Pérez, Herramientas de gestión de riesgos de SI, 2012. 40 p. ISBN: 486-23-145632-1-8

DIMENSIONES DE UN ACTIVO:

Confidencialidad: ¿qué daño causaría que lo conociera quien no debe?

Integridad: ¿qué perjuicio causaría que estuviera dañado o corrupto?

Disponibilidad: ¿qué perjuicio causaría no tenerlo o no poder utilizarlo?

Autenticidad: ¿qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?

Trazabilidad: ¿quién hace qué y cuándo? Y ¿qué daño causaría no saber quién accede a qué datos y qué hace con ellos?

Determinar las amenazas relacionadas a los activos

"Es la causa potencial que puede afectar a cada activo, en donde las amenazas son las cosas que ocurren y que pueden ocurrir."[15]

La valoración de amenaza de un activo se puede clasificar de dos maneras, según la degradación del valor y la probabilidad de ocurrencia

Figura N°03

Fuente: Herramientas de gestión de riesgos de SI

MA	muy alta	casi seguro	fácil
A	alta	muy alto	medio
M	media	posible	difícil
B	baja	poco probable	muy difícil
MB	muy baja	muy raro	extremadamente difícil

Degradación del valor

En la figura anterior (Figura N°2) se puede observar la manera como se degrada el valor de una amenaza mediante clasificaciones de muy alta a muy baja.

Figura N°04

Fuente: Herramientas de gestión de riesgos de SI

MA	100	muy frecuente	a diario
A	10	frecuente	mensualmente
M	1	normal	una vez al año
B	1/10	poco frecuente	cada varios años
MB	1/100	muy poco frecuente	siglos

Probabilidad de ocurrencia

[15] Gabriel Sánchez Pérez, Herramientas de gestión de riesgos de SI, 2012. 60 p. ISBN: 486-23-145632-1-8

En la figura anterior (Figura N°3) se puede observar cómo se mide la probabilidad de ocurrencia de un riesgo mediante clasificaciones de muy frecuente a muy poco frecuente.

Determinar el impacto que podría tener un activo tras la amenaza

"Conociendo la degradación del valor y la probabilidad de ocurrencia es sencillo identificar qué impacto tendrán sobre el sistema."[16]

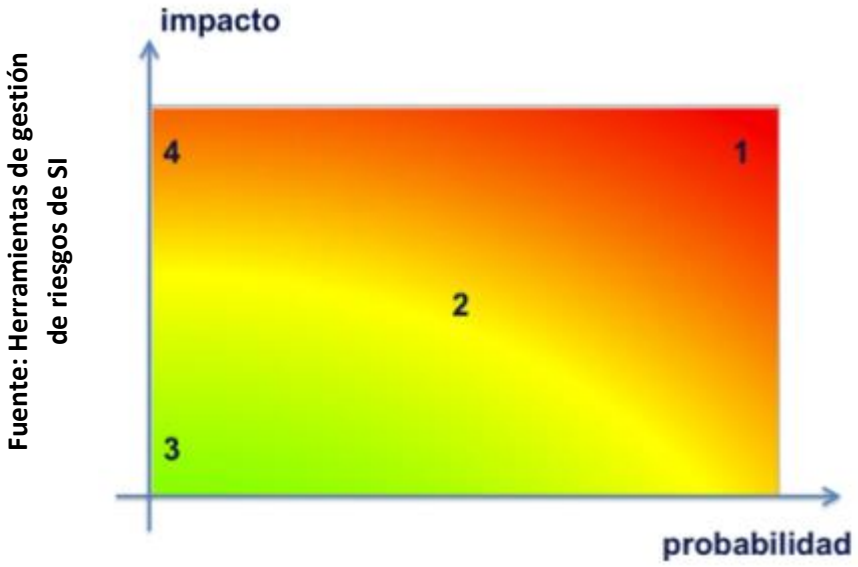
Para ello se necesita saber:

- El valor propio del activo
- Las amenazas a la que están expuestas los activos
- Las amenazas a la que están expuesto los activos dependientes

Determinar el riesgo de una amenaza.

Es conocer el impacto que pueda tener una amenaza hacia un activo y se clasifican mediante zonas de riesgos.

Figura N°05



Fuente: Herramientas de gestión de riesgos de SI

El riesgo en función del impacto y la probabilidad

ZONA1: Riesgos muy probables y de muy alto impacto

ZONA2: Situaciones improbables y de impacto medio

ZONA3: Riesgos improbables y de bajo impacto

[16] Gabriel Sánchez Pérez, Herramientas de gestión de riesgos de SI, 2012. 62 p. ISBN: 486-23-145632-1-8

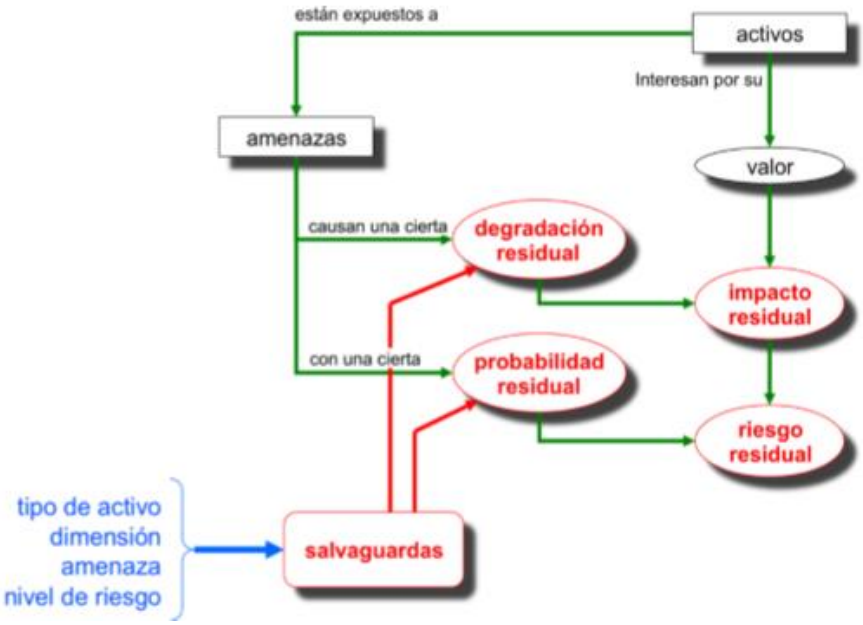
ZONA4: Riesgos improbables pero de muy alto impacto

En la figura anterior (Figura N°4) se observa de cómo está clasificado el riesgo según el riesgo y la probabilidad, además nos permite clasificarlo por zonas para poder clasificarlos por niveles de información.

Determinar las salvaguardas que mitiguen los riesgos

"La salvaguarda son aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo y los activos se protegen según la necesidad de la organización."[17]

Figura N°06



Fuente: Herramientas de gestión de riesgos de SI

Elementos de análisis del riesgo residual

En la figura anterior (figura N°6) se puede ver las medidas que se implementan para lograr la salvaguardas de una información y poder minimizar el riesgo de una manera compacta y segura.

La salvaguarda tiene que acabar con la amenaza hasta hacerla residual y no ocasionar nuevos problema en los activos, en caso vuelva a aparecer otro riesgo con esta salvaguarda poder mitigarla de una manera eficaz. Los tipos de salvaguardas que nos ayudaran reducir el perfil de la amenaza son:

[17] Gabriel Sánchez Pérez, Herramientas de gestión de riesgos de SI, 2012. 63 p. ISBN: 486-23-145632-1-8

Figura N°07

Fuente: Herramientas de gestión de riesgos de SI

efecto	tipo
preventivas: reducen la probabilidad	[PR] preventivas [DR] disuasorias [EL] eliminatorias
acotan la degradación	[IM] minimizadoras [CR] correctivas [RC] recuperativas
consolidan el efecto de las demás	[MN] de monitorización [DC] de detección [AW] de concienciación [AD] administrativas

Tipos de salvaguardas

En la figura anterior (Figura N°7) se puede observar los tipos de salvaguardan que se implementar para poder acabar con un riesgo de información.

La eficacia de la salvaguarda debe de ser al 100% para que cuando suceda alguna amenaza similar se pueda usar nuevamente la salvaguarda y poder mitigarlo de nuevo

Figura N°08

Fuente: Herramientas de gestión de riesgos de SI

factor	nivel	significado
0%	**L0**	inexistente
	L1	inicial / ad hoc
	L2	reproducible, pero intuitivo
	L3	proceso definido
	L4	gestionado y medible
100%	**L5**	optimizado

Eficacia y madurez de las salvaguardas

En la figura anterior (Figura N°8) se puede observar los niveles de eficacia y madures para implementar una salvaguarda de una información, en ella está la significación que se le da a una salvaguarda para poder optimizarla y con ella poder recuperar al sistema en caso tenga una afectación grave por algún riesgo que se genere.

Una manera de conocer los riesgos potenciales es de la siguiente manera:

Figura N°09

Fuente: Herramientas de gestión de riesgos de SI

Elementos del análisis de riesgos potenciales

En la figura anterior (Figura N°9) se puede observar los pasos correctos de poder identificar los elementos del análisis de riesgos potenciales en la organización.

La fórmula para los niveles de riesgo es

$$\mathrm{NR}=\left(\frac{\sum_{i=1}^{n}((POR*i)*(IR*i))}{n}\right)$$

Donde:

NR= Nivel de riesgo

POR= Probabilidad de ocurrencia del riesgo

IR= Importancia del riesgo

I=es el riesgo identificado

N=numero toral de riesgos identificados

Esta fórmula nos ayudara a poder identificar el nivel de riesgo que se presenta en una organización y así mismo nos ayudara a poder clasificarlo según el nivel de importancia

1.3.2 LA SEGURIDAD INFORMÁTICA

"La seguridad informatica establece políticas de trabajo, conocimientos claros y apoyo de la alta dirección para poder tener los recursos informáticos, a través de ello poder obtener un nivel de seguridad optimizada y capaz de cumplir las expectativas de seguridad"[18]

"La seguridad informatica reside en ayudar a las organizaciones a poder reducir sus perfiles de riesgo a través de la administración"[19]

"La seguridad informatica es fundamental para el funcionamiento y quizás incluso sea decisivo para la supervivencia de la organización, por lo cual es importante gestionar y proteger los activos de la información"[20]

Según Perafan Ruiz John nos dice que las dimensiones de una seguridad Informática son las siguientes.

- Seguridad Lógica
- Seguridad Física
- Seguridad de redes

DIMENSIÓN

SEGURIDAD LÓGICA

"La seguridad lógica se encarga de implementar controles de acceso que están creados para salvaguardar la integridad y confidencialidad de la información almacenada de un dispositivo intermedio o final. También se encarga de controlar y salvaguardar toda información desarrollada por los sistemas y por los programas en aplicación, nos ayuda a identificar a cada usuario y sus actividades que realizan en el sistema, y por ello les restringe el acceso de datos y accesos de red"[21]

[18] Perafan Ruiz John. Seguridad Informatica de las tecnologías de Información, Ecuador, Popayán, 2014. 10 p. ISBN: 120234586-1

[19] ISACA, Information Systems Audit and Control Association. 2009. EE.UU, Illinois.

[20] ISO/IEC 27001/2013, Sistema de Gestión de Seguridad de Información, 2013. 4ta. Ed. EE.UU

[21] Cisco Networking Academy, principios y guías de Seguridad de información. 3ra. Ed. EE.UU., Manhattan, 2016. 48 p

INDICADOR

El indicador para medir la seguridad lógica según "Indicadores de desempeño para las instituciones públicas", es el nivel de cumplimiento.

- Nivel de cumplimiento

"Si el nivel de cumplimiento es de 100% es porque se ha alcanzado la meta, pero si el nivel de cumplimiento no se alcanza se restara al 100% el nivel de cumplimiento actual entre la cantidad de dimensiones que se quiera utilizar para poder identificar el nivel de cumplimiento."[22]

La fórmula para calcular el cumplimiento actual es:

$$NCSL = 100\% - \frac{\Sigma(NCA)}{NA}$$

NCSL: Nivel de cumplimiento de la seguridad lógica

NCA Nivel de cumplimiento de activos

NA: Numero de activos

DIMENSIÓN

SEGURIDAD FÍSICA

"La seguridad física permite implementar controles y procesos de la seguridad dentro y fuera del centro de cómputo así como los medios de acceso remoto, implementados para proteger el hardware y los medios de almacenamiento de datos. Es muy importante, que nuestra organización sea la más segura de ataques externos, hackers, virus, etc.; la seguridad será nula si no se ha implementado medidas de control."[23]

INDICADOR

El indicador para medir la seguridad lógica según "Indicadores de desempeño para las instituciones públicas", es el nivel de cumplimiento

[22] Políticas presupuestarias y gestión pública por resultados, Indicadores de desempeño para las instituciones públicas, Guadalajara, Jalisco. 2007

[23] Huerta, Seguridad en Unix y redes, Ecuador, Quito. 2012. 147 p.

- Nivel de cumplimiento

Si el nivel de cumplimiento es de 100% es porque se ha alcanzado la meta, pero si el nivel de cumplimiento no se alcanza se restara al 100% el nivel de cumplimiento actual entre la cantidad de dimensiones que se quiera utilizar para poder identificar el nivel de cumplimiento.

La fórmula para calcular el cumplimiento actual es:

$$NCSF = 100\% - \frac{\Sigma(NCA)}{NA}$$

NCSL: Nivel de cumplimiento de seguridad la física.
NCA Nivel de cumplimiento de activos
NA: Numero de activos

DIMENSION

SEGURIDAD DE REDES

"La seguridad en redes es mantener la integridad, disponibilidad, privacidad, control y autenticidad de la información que está integrada en las computadoras, a través de una serie de pasos basados en una política de seguridad que permitan el control adecuado de la información"[24]

INDICADOR

El indicador para medir la seguridad lógica según "Indicadores de desempeño para las instituciones públicas", es el nivel de cumplimiento

- Nivel de cumplimiento

Si el nivel de cumplimiento es de 100% es porque se ha alcanzado la meta, pero si el nivel de cumplimiento no se alcanza se restara al 100% el nivel de cumplimiento actual entre la cantidad de dimensiones que se quiera utilizar para poder identificar el nivel de cumplimiento.

[24] Bustamante, Seguridad en redes, 1ra Ed, Colombia, Bogotá 2012 40 p. ISBN: 436782657-0

La fórmula para calcular el cumplimiento actual es:

$$NCSR = 100\% - \frac{\Sigma(NCA)}{NA}$$

NCSL: Nivel de cumplimiento de la seguridad de redes

NCA Nivel de cumplimiento de activos

NA: Numero de activos

1.3.3 METODOLOGÍA PARA LA HERRAMIENTA DE ANÁLISIS

MAGERIT "Metodología de análisis y gestión de riesgos de los sistemas de información"

"La herramienta de gestión de riesgos es muy importante para todas las organizaciones que trabajan con equipos informáticos y sistemas de información; si la organización depende de ella, MAGERIT les ayudará a identificar el valor de su información y les ayudara a poder proteger dicha información, también les permitirá conocer el riesgos de la información para poder minimizarlos y generar confianza en la gestión de seguridad de la información."[25]

"Los objetivos de magerit son"[26]

- Hacer conocer que toda organización tiende a tener riesgos y que es necesario gestionarlos de una manera rápida y eficaz.
- Brindar un método sistemático para analizar los riesgos de las TIC´S.
- Prepara la organización a tener auditorias de tecnologías de información

"Las ventajas de magerit son"[27]

- Presenta un análisis de costo beneficio, y expresa una formula del ROI que es Retorno de la Inversión.
- No tiene costo dado que es una normativa de libre aplicación
- Los resultados son ordinales y cardinales

[25] Magerit, Metodología de análisis y gestión de riesgos, EE.UU. 2012, p:19
[26] Magerit, Metodología de análisis y gestión de riesgos, 2012, p:28
[27] Magerit, Metodología de análisis y gestión de riesgos, 2012, p:29

ISO 27005:2008 "Information technology – Security techniques – Information security risk management"

"Establece las directrices para la gestión del riesgo en la seguridad de la información y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos. La ISO/IEC 27005/:2008 es aplicable a todo tipo de organizaciones que llenen de intención de gestionar los riesgos que pueden comprometer la organización de la seguridad de la información."[28]

"La estructura de la ISO/IEC 27005/2008 es:" [29]

1) Establecimiento del contexto
2) Evaluación de riesgo
3) Tratamiento de riesgo
4) Aceptación del riesgo
5) Comunicación del riesgo
6) Monitorización y revisión del riesgo

"Beneficios de la ISO/IEC 27005:2008"[30]

- Reducción del riesgo de pérdida, robo o corrupción de información.
- Los riesgos y sus controles son continuamente revisados
- Continuidad de las operaciones necesarias de negocio tras incidencias de gravedad

ISO/IEC 31000:2009 "Gestión de riesgos: principios y guías"

"Es una metodología de análisis de gestión de riesgos que brinda guías y principios para poder identificar los riesgos de información, donde puede ser aplicado a cualquier tipo de riesgo donde puede ser aplicado a toda una organización, así como a funciones, proyectos y actividades específicas."[31]

"La estructura de la ISO 31000:2008 son las siguientes:"[32]

[28] ISO/IEC 27005:2008, Metodología de gestión de riesgos, 2014, 8 p.
[29] ISO/IEC 27005:2008, Metodología de gestión de riesgos, 2014, 14p.
[30] ISO/IEC 27005:2008, Metodología de gestión de riesgos, 2014, 20 p.
[31] ISO/IEC 31000:2009, Secure Information Technologies, 2014. 15 p.
[32] ISO/IEC 31000:2009, Secure Information Technologies, 2014. 20 p.

1) Gestión de riesgo
2) Análisis de riesgo
3) Identificación de riesgo
4) Estimación del riesgo
5) Evaluación del riesgo

Es la metodología de Análisis y Gestión de Riesgos de los Sistema de Información, elaborada por el Consejo Superior de Administración Electrónica, Actualizada en 2012 en su versión número 3.

Así mismo magerit enfatiza que los riesgos que se presentan comúnmente en una empresa son en referencia a la seguridad informática; en la cual mayoría de las empresas no tienen medidas de prevención para poder mitigarlas de una manera eficaz. Los riesgos a que se expone una organización puede ser en cualquier área, pero las más resaltantes en el área de informática son las siguientes.

Además de contar con el respaldo de tres expertos (Ver Tabla N° 3), para ello, se realizó una evaluación de la Metodología MAGERIT, cuyo resultado fue favorable a la Metodología MAGERIT (Ver Anexo N° 05)

.

Tabla N°01

ÍTEM	EXPERTO NOMBRES Y APELLIDOS	METODOLOGÍA		
		MAGERIT	ISO7IEC 27005	ISO/IEC 31000
01	Bello Gómez Luis	16	11	6
02	Bravo Baldeón Percy	18	13	11
03	Vergara Calderón Rodolfo	18	12	9
TOTAL		**17.3**	**12**	**8.6**

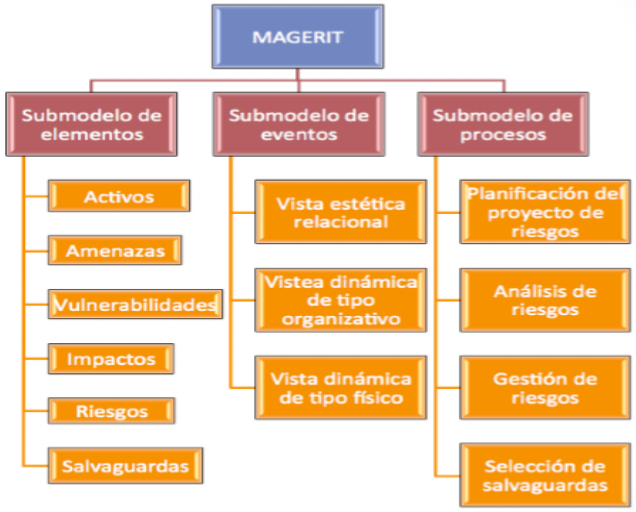
Fuente: Elaboración Propia

Consolidado del Juicio de Experto

METODOLOGIA MAGERIT

Magerit presenta tres tipos de estructura para poder analizar, controlar y administrar el riesgo donde esta submodelo de elementos, submodelo de eventos y submodelo de procesos

Figura N°10



Fuente: Metodología de análisis y gestión de riesgos

Estructura de Magerit

En la figura N°10 se muestra la estructura de magerit que se divide en subelementos para el analizar los elementos del riesgo, los eventos para ver de qué manera influye magerit en la organización y procesos para la gestión de riesgos de la seguridad informatica.

La metodología magerit nos da a conocer los siguientes pasos para poder identificar las salvaguardas.

Los siguientes pasos son:

PASO1: Identificación de activos

En este paso se tienen que identificar cuáles son los activos que se quieran investigar para cada indicador respecto a cualquiera de los 154 requerimientos que nos brinda la ISO/IEC 27001:2013 y clasificarlos según su relación con la dimensión.

PASO2: Valoración de activos

En este paso se valora al activo en su estado actual respecto a las dimensiones de seguridad y el criterio de daño que causa.

PASO3: Identificación y valoración de amenazas

En este paso se identifica la amenaza que afectaría a cada activo de información y se le da un grado de frecuencia respecto a las dimensiones de seguridad.

PASO4: Identificación y valoración de salvaguardas

En este paso se desarrolla la salvaguarda para mitigar la amenaza que se presente por cada activo y además poder comparar con alguna salvaguarda existente que tenga la organización y ver su funcionamiento actual.

PASO5: Impacto de riesgo acumulado

En este paso después de evaluar los 3 primeros pasos se identifica el estado situacional real de la organización, esto también servirá para tener un pre-test

PASO6: Impacto de riesgo residual

Este paso se desarrolla gracias al paso 4, donde se estima un resultado después de implementar las salvaguardas, donde la medición puede ser la misma o aumentada.

PASO7: Matriz de riesgos magerit

En este paso se tendrá una relación entre el riesgo acumulado y el riesgo residual, para poder identificar el pre-test y como se estimaría el post-test con las salvaguardas implementadas.

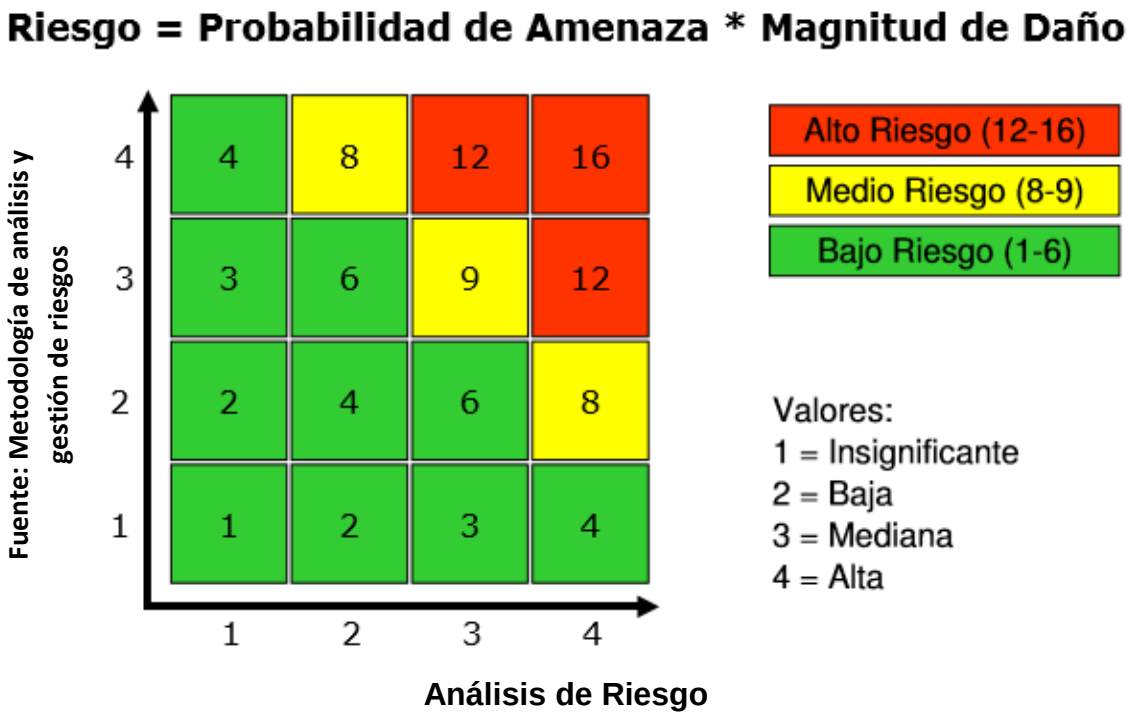
1.3.4 HERRAMIENTAS UTILIZADAS PARA LA GESTION DE RIESGOS MATRIZ DE RIESGOS DE MAGERIT

La Matriz de riesgos de magerit es la basé en el método de Análisis de Riesgo con un grafo de riesgo, nos ayuda a clasificar la probabilidad del riesgo con la salvaguarda que se va a implementar para poder mitigar al riesgo.

Esta matriz nos sirve como herramienta de trabajo porque tiene una serie de procesos que nos ayudara a como trabajar en nuestra organización, para no afectar ningún activo de información que nos retrase en nuestras actividades de trabajo.

Para calcular el grafo de riesgo se usa la formula Riesgo = Probabilidad de Amenaza x Magnitud de Daño, donde la Probabilidad de Amenaza y Magnitud de Daño pueden tomar los valores y condiciones respectivamente

Figura N°11



El Riesgo, que es el producto de la multiplicación Probabilidad de Amenaza por Magnitud de Daño, está agrupado en tres rangos, y para su mejor visualización, se aplica diferentes colores.

Bajo Riesgo = 1 – 6 (verde)
Medio Riesgo = 8 – 9 (amarillo)
Alto Riesgo = 12 – 16 (rojo)

"LA MATRIZ ESTÁ COMPUESTO POR 8 COLUMNAS

1. **Dimensión**: En esta columna se hace referencia a las dimensiones con las que se está trabajando para poder clasificarlas según los activos y poder calcular la diferencia del nivel de cumplimiento actual y final
2. **Activo**: En esta columna se tendrá al activo que tiene relación en cada dimensión, en la cual nos ayudaran a poder calcular el nivel de cumplimiento actual y final, cabe recalcar que los activos se seleccionan de los 154 requerimientos de la norma ISO/IEC 27001:2013.
3. **Cumplimiento actual**: En esta columna se mide el cumplimiento actual de los activos a través de una auditoria inicial que nos permita

calcular el estado actual de la organización en base a dichos activos de información.

4. Amenaza: En esta columna se hace referencia a la amenaza que vulnera al activo , donde se tiene que mitigar la amenaza antes que cause un

5. Frecuencia de la amenaza: En esta columna se evalúa la frecuencia con la que se presenta la amenaza en la organización.

6. Salvaguardas: En esta columna se establece las salvaguardas que nos ayudaran a mitigar las amenazas

7. Degradación de riesgo: En esta columna se evalúa la degradación que genera la salvaguarda en base a la amenaza.

8. Cumplimiento Final: En esta columna se mide el cumplimiento final de los activos a través de una auditoria final que nos permite calcular el estado final de la organización. ”[33]

[33] Magerit, Metodología de análisis y gestión de riesgos, EE.UU. 2012, p:27

ISO/IEC 27001:2013 SISTEMA DE GESTIÓN DE SISTEMAS DE INFORMACIÓN

"Se utilizara esta herramienta de trabajo para que nos sirva de apoyo en la Auditoria que se implementará en el Hospital Nacional Madre Niño San Bartolomé, para tener una línea base de los hallazgos que se encuentren y a su vez poder incluirlas dentro de la gestión de riesgos, para ello los hallazgos se alinearan a la ISO/IEC 27001/2013.

ISO/IEC 27001/2013

Es un estándar internacional de gestión de seguridad de información donde presenta 7 cláusulas que incorporan 154 requerimientos.

1. **INTRODUCCION:** Son las generalidades e introducción de norma ISO/IEC 27001/2013
2. **OBJETIVO:** Se especifica los objetivos y los tratamientos que se van a establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de información dentro del contexto de la organización.
3. **REFERECNCIAS NORMATIVAS:** Son algunas normas que están alineadas a la ISO/IEC 27001:2013 donde hace referencia que todas están normas están actualizadas.
4. **CONTEXTO DE LA ORGANIZACIÓN**
   - 4.1. Comprender la organización y su contexto: La organización debe de determinar cuáles son los aspectos internos y externos que son relevantes que afecten su capacidad de lograr los resultados.
   - 4.2. Comprender las necesidades y expectativas de las partes interesadas: La organización debe de determinar cuáles son las partes interesadas más relevantes al sistema de gestión de seguridad de la información
   - 4.3. Determinar el alcance del sistema de gestión de seguridad de la información: La organización debe de determinar cuáles son los límites del sistema de gestión de seguridad de la información.
   - 4.4. Sistema de gestión de seguridad de la información: La organización debe establecer, implementar, mantener y mejorar continuamente el sistema de gestión de seguridad de la información.

5. **LIDERAZGO**
   - 5.1. Liderazgo y compromiso: La alta dirección debe de mostrar liderazgo y compromiso respecto al sistema de gestión de seguridad de la información.
   - 5.2. Políticas: La alta dirección debe de establecer políticas de seguridad de la información
   - 5.3. Roles, responsabilidades y autoridades organizacionales: La alta dirección debe de establecer responsabilidades y roles para la seguridad de la información
6. **PLANIFICACION:** Cuando se determina los riesgos dentro del sistema de gestión de seguridad de la información
7. **SOPORTE:** La organización debe de determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continúa del sistema de gestión de seguridad de la información.
8. **OPERACIÓN:**
   - 8.1. Planificación y control operacional: La organización debe de planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos de seguridad de la información.
   - 8.2. Evaluación de riesgos de seguridad de la información: La organización debe de evaluar los riesgos de seguridad de la información
   - 8.3. Tratamiento de riesgos de seguridad de la información: La organización debe de implementar el plan de tratamiento de los riesgos en la seguridad de la información.
9. **EVALUACION DEL DESEMPEÑO:** Permite realizar las auditorías internas bajo el control y cumplimiento de las requerimiento, donde también permite gestionar el proceso periódico de la revisión del sistema de gestión de seguridad de información por parte de la dirección.
10. **MEJORA:** Se plantea la mejora continua, las acciones correctivas y acciones preventivas

VENTAJAS DE LA ISO/IEC 27001/2013

- Facilita la integración de los sistemas de gestión
- Los riesgos de la seguridad de información son identificados
- Ayuda a prevenir auditorias "[34]

1.3.5 MARCO CONCEPTUAL

Herramienta de gestión de riesgos

"La herramienta de gestión de riesgos se define como un plan para la implantación de controles de seguridad en los sistemas de información que permite disminuir la probabilidad de que se materialice una amenaza, reducir la vulnerabilidad del sistema o el posible impacto en la organización, y posibilite la recuperación del sistema en caso de una afectación grave[35]

La seguridad informatica

"La seguridad informatica establece políticas de trabajo, conocimientos claros y apoyo de la alta dirección para poder tener los recursos informáticos, a través de ello poder alcanzar un nivel de seguridad razonable y capaz de satisfacer las expectativas de seguridad"[36]

Seguridad lógica

"La seguridad lógica se encarga de implementar controles de acceso que están creados para salvaguardar la integridad y confidencialidad de la información almacenada de un dispositivo intermedio o final. También se encarga de controlar y salvaguardar toda información desarrollada por los sistemas y por los programas en aplicación, nos ayuda a identificar a cada usuario y sus actividades que realizan en el sistema, y por ello les restringe el acceso de datos y accesos de red"[37]

Seguridad Física

[34] ISO/IEC 27001/2013, Sistema de Gestión de Seguridad de Información, 2013. 4ta. Ed. EE.UU
[35] Gabriel Sánchez Pérez, Herramientas de gestión de riesgos de SI, 2012. 20 p. ISBN: 486-23-145632-1-8
[36] ISO/IEC 27001/2013, Sistema de Gestión de Seguridad de Información, 2013. 4ta. Ed. EE.UU
[37] Perafan Ruiz John. Seguridad Informatica de las tecnologías de Información, Ecuador, Popayán, 2014. 10 p. ISBN: 120234586-1

"La seguridad física permite implementar controles y procesos de la seguridad dentro y fuera del centro de cómputo así como los medios de acceso remoto, implementados para proteger el hardware y los medios de almacenamiento de datos. Es muy importante, que nuestra organización sea la más segura de ataques externos, hackers, virus, etc.; la seguridad será nula si no se ha implementado medidas de control"[38]

Seguridad de Redes

"La seguridad en redes es mantener la integridad, disponibilidad, privacidad, control y autenticidad de la información que está integrada en las computadoras, a través de una serie de pasos basados en una política de seguridad que permitan el control adecuado de la información"[39]

1.4 FORMULACIÓN DEL PROBLEMA

PROBLEMA GENERAL

PG: ¿De qué manera influye la herramienta de gestión de riesgos para la seguridad Informática del HONADOMANI San Bartolomé?

PROBLEMAS ESPECÍFICOS

PE1: ¿En qué medida la herramienta de gestión de riesgos influye en el cumplimiento de la seguridad lógica del HONADOMANI San Bartolomé?

PE2: ¿En qué medida la herramienta de gestión de riesgos influye en el nivel de cumplimiento de la seguridad física del HONADOMANI San Bartolomé?

PE3: ¿En qué medida la herramienta de gestión de riesgos influye en el nivel de cumplimiento de la seguridad de redes del HONADOMANI San Bartolomé?

1.5 JUSTIFICACIÓN DEL ESTUDIO

Justificación Tecnológica

"En la herramienta de gestión de riesgos se pondrá en práctica todas las políticas y procesos que nos ayuden a garantizar la operación continua de los

[38] Huerta, Seguridad en Unix y redes, 2012. 147 p.

[39] Bustamante, Seguridad en redes, 1ra Ed, Colombia, Bogotá 2012 40 p. ISBN: 436782657-0

sistemas y minimizar todo tipo de riesgo, el cual va a constituir una herramienta de apoyo y va a optimizar y agilizar los procesos."[40]

La presente tesis se justifica tecnológicamente, dado que la herramienta de gestión de riesgos ayudara a optimizar recursos de hardware y software existentes en el Hospital Nacional Madre Niño San Bartolomé, para la seguridad informática. En ese sentido ya no será necesario que el usuario se queje diariamente por la caída del sistema de información y poder administrar de una mejor manera los recursos del hardware de la sala de telecomunicaciones para la red.

Justificación Económica

"Todo tipo de proyecto que pueda involucrar tecnología de la información no es considerado como un egreso, sino como una inversión, que ha futuro dejará utilidades dentro de la organización."[41]

Para esta investigación, se brinda al Hospital San Bartolomé el costo detallado para la implementación de una herramienta de gestión de riesgos, tomando en cuenta los recursos humanos y materiales necesarios para poder realizar dicho proyecto y así poder mejorar el proceso de gestión de riesgo en la seguridad informatica. Por lo tanto gracias al cuadro estadístico del diagrama de Gantt, se pudo calcular el costo total que ahorra el hospital por la implementación de esta investigación que es un monto de S/. 3,357.10 nuevos soles (ver la tabla N°9 – Costo total del proyecto) con una fecha de 29 de agosto del 2016 al 7 de Julio del 2017

[40] Senn, Ceres. Proyectos de inversión para su formulación y evaluación. 2ª. Ed. México, Santurce 2011. 80 p. ISBN: 1-875619-232

[41] Senn, Ceres. Proyectos de inversión para su formulación y evaluación. 2ª. Ed. México, Santurce 2011. 19p. ISBN: 1-875619-232

HIPÓTESIS

HIPÓTESI GENERAL

HG: La Herramienta de gestión de riesgos mejora el proceso para la seguridad Informática del HONADOMANI San Bartolomé.

HIPÓTESIS ESPECÍFICAS

HE1: La herramienta de gestión de riesgos mejora el nivel de cumplimiento de la seguridad Lógica del HONADOMANI San Bartolomé

HE2: La herramienta de gestión de riesgos mejora el nivel de cumplimiento de la seguridad Física del HONADOMANI San Bartolomé

HE3: La herramienta de gestión de riesgos mejora el nivel de cumplimiento de la seguridad de redes del HONADOMANI San Bartolomé

1.6 OBJETIVOS

OBJETIVO GENERAL

OG: Determinar la influencia de una herramienta de gestión de riesgos para la seguridad informatica del HONADOMANI San Bartolomé.

OBJETIVOS ESPECÍFICOS

OE1: Determinar la influencia de una herramienta de gestión de riesgos en el nivel de cumplimiento de la seguridad lógica del HONADOMANI San Bartolomé.

OE2: Determinar la influencia de una herramienta de gestión de riesgos en el nivel de cumplimiento de la seguridad física del HONADOMANI San Bartolomé.

OE3: Determinar la influencia de una herramienta de gestión de riesgos en el nivel de cumplimiento de la seguridad de redes el HONADOMANI San Bartolomé.

CAPÍTULO – 02:

II. MÉTODO

2.1 TIPO DE ESTUDIO

'La investigación aplicada es el proceso de conocimiento en el que el interés primordial radica en buscar información fundamentalmente empírica sobres problemas que surgen en la organización con el objetivo de plantear alternativas de solución.'[42]

La siguiente investigación es de tipo Aplicada, porque se plantearán diversos conocimientos teóricos para la resolución del problema.

"Las investigaciones No-experimentales tratan de un estudio donde no se hace variar en forma intencional a la variable independiente para ver su efecto en otras variables, además las investigaciones no experimentales tratan de observar el estado actual de la organización sin necesidad de alterar el contexto natural, para posteriormente analizarlos. Es decir en un estudio no experimental no se genera ninguna situación, sino que se observan situaciones ya existentes, no provocadas intencionalmente en la investigación por quien la realiza."[43]

La presente investigación es no-experimental, porque no se va a afectar al comportamiento de trabajo del personal del hospital San Bartolomé, se va a analizar el estado situacional de la seguridad informatica del hospital a través de una auditoria para tener una línea base, posteriormente este resultado se analizará con la metodología MAGERIT para dar resultados finales mediante la matriz de riesgos de MAGERIT y teniendo ya las salvaguardas se procederá a implementarlas. Finalmente con las recomendaciones o salvaguardas ya implementadas se realizara una segunda auditoria para ver el efecto de mejora y cumplimiento de dichas salvaguardas.

[42] Hernández Sampiere. Metodología de investigación científica. 5a. ed. México, Editorial cáliz, 2011. 40 p. ISBN: 1-569874-156

[43] Hernández Sampiere. Metodología de investigación científica. 5a. ed. México, Editorial cáliz, 2011. 50 p. ISBN: 1-569874-156

2.2. DISEÑO DE ESTUDIO

"El tipo de diseño para las investigaciones No-Experimentales es longitudinal porque analizan y recolectan datos a través del tiempo en puntos o periodos de determinadas categorías, variables y contextos, para hacer inferencias respecto al cambio, sus determinantes y consecuencias" [44]

El diseño que se utilizará en esta investigación es Longitudinal, ya que se analizará el estado actual de la organización mediante una auditoria y se recolectarán resultados a través de una segunda auditoria para ver el proceso de mejora del nivel de cumplimiento luego de la implementación de las salvaguardas.

'El subtipo del diseño longitudinal es de tendencia porque analizan cambios dentro de alguna población, además el subtipo de tendencia ayudar a seleccionar cuales son las mejoras que se van a implementar en un corto plazo o hasta mediano plazo.'[45]

El sub tipo del diseño de investigación es de Tendencia, porque se implementarán las salvaguardas y se calculará el nivel de cumplimiento de ellas, tal motivo que habrá una tendencia de mejorar con el fin del llegar al 100% y estar en mejora contínua constantemente.

2.2 VARIABLES, OPERACIONALIZACIÓN

2.2.1 DEFINICIÓN CONCEPTUAL

Variable Independiente (VI): Herramienta de gestión de riesgos

"La herramienta de gestión de riesgos se define como un plan para la implantación de controles de seguridad en los sistemas de información que permite disminuir la probabilidad de que se materialice una amenaza, reducir la vulnerabilidad del sistema o el posible impacto en la

[44] Hernández Sampiere. Metodología de investigación científica. 5a. ed. México, Editorial cáliz, 2011. 55 p. ISBN: 1-569874-156

[45] Hernández Sampiere. Metodología de investigación científica. 5a. ed. México, Editorial cáliz, 2011. 58 p. ISBN: 1-569874-156

organización, y posibilite la recuperación del sistema en caso de una afectación grave."[46]

Variable Dependiente (VD): La seguridad informatica

"La seguridad informatica establece políticas de trabajo, conocimientos claros y apoyo de la alta dirección para poder tener los recursos informáticos, a través de ello poder alcanzar un nivel de seguridad razonable y capaz de satisfacer las expectativas de seguridad."[47]

2.2.2 DEFINICIÓN OPERACIONAL

Variable Independiente (VI): Herramienta de gestión de riesgos

La herramienta de gestión de riesgos permite identificar las vulnerabilidades de los activos de información en el Hospital San Bartolomé, permitiendo identificar cuales con las amenazas que afecten a las vulnerabilidades y clasificarlas por niveles de seguridad, asimismo ayuda en el análisis, diseño e implantación de la gestión de riesgos y generando reportes estadísticos para la toma de decisiones asertivas.

Variable Dependiente (VD): La seguridad informatica

La seguridad informatica permite el análisis, diseño, implantación, monitoreo, mejora continua y optimización de las salvaguardas para los activos de información.

[46] Gabriel Sánchez Pérez, Herramientas de gestión de riesgos de SI, 2012. 20 p. ISBN: 486-23-145632-1-8

[47] Perafan Ruiz John. Seguridad Informatica de las tecnologías de Información, Ecuador, Popayán, 2014. 10 p. ISBN: 120234586-1

2.2.3. Operalización

Tabla N°02

VARIABLE	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	INDICADORES	FORMULA
Variable Independiente: Herramienta de gestión de riesgos	La herramienta de gestión de riesgos se define como un plan para la implantación de controles de seguridad en los sistemas de información que permite disminuir la probabilidad de que se materialice una amenaza, reducir la vulnerabilidad del sistema o el posible impacto en la organización, y posibilite la recuperación del sistema en caso de una afectación grave	La herramienta de gestión de riesgos permite identificar las vulnerabilidades de los activos de información en el Hospital San Bartolomé, permitiendo identificar cuales con las amenazas que afecten a las vulnerabilidades y clasificarlas por niveles de seguridad, asimismo ayuda en el análisis, diseño e implantación de la gestión de riesgos y generando reportes estadísticos para la toma de decisiones asertivas.		
Variable Dependiente: La seguridad informatica	La seguridad informatica establece políticas de trabajo, conocimientos claros y apoyo de la alta dirección para poder tener los recursos informáticos, a través de ello poder alcanzar un nivel de seguridad razonable y capaz de satisfacer las expectativas de seguridad	La seguridad informatica permite el análisis, diseño, implantación, monitoreo, mejora continua y optimización de las salvaguardas para los activos de información	Nivel de cumplimiento de la Seguridad Lógica	$NCSL = 100\% - \frac{\Sigma(NCA)}{NA}$
			Nivel de cumplimiento de la seguridad Física	$NCSf = 100\% - \frac{\Sigma(NCA)}{NA}$

Fuente: Elaboración propia

			Nivel de cumplimiento de la seguridad de redes	$NCSR = 100\% - \frac{\Sigma(NCA)}{NA}$

Operalización de variables

2.3 POBLACION Y MUESTRA

2.3.1. POBLACION

"Una población es un conjunto de todos los elementos que estamos estudiando, acerca de los cuales intentamos sacar conclusiones. Cuando la población es muy grande, es obvio que la observación y/o medición de todos los elementos se multiplica la complejidad, en cuanto al trabajo, tiempo y costos necesarios para hacerlo. Para solucionar este inconveniente se utiliza una muestra estadística."[48]

En esta investigación, la población fue obtenida observando el número de hallazgos que se realizó en la auditoria informatica y las cuales se implementaran una salvaguarda por cada uno donde la organización lo quiere implementar, tal motivo tendremos 13 hallazgos que serán la población para las 3 dimensiones, seguridad lógica, seguridad física y seguridad de redes.

2.3.2. MUESTRA

"Para Hernández si la población es menor a cincuenta individuos, la población es igual a la muestra."[49]

Dado que se conoce el tamaño de la población, se tomara una muestra la cantidad de 13 hallazgos. Porque la población es menor a 50 individuos.

[48] GÓMEZ, Deck. Estadística aplicada a la investigación científica. 2a. ed. EE.UU., Petri, 2012. 80 p. ISBN: 1-542369-742

[49] Hernández citado en castro, metodología de la investigación científica, 2003

2.4 TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS, VALIDEZ Y CONFIABILIDAD

2.4.1 TÉCNICAS

- **ENTREVISTA**

  "Consiste en una conversación preparada como una dinámica de preguntas y respuestas abiertas, en las cuales se socializa sobre una temática determinada relacionada con la problemática a estudiar, esta técnica permite conocer el punto de vista de diferentes partes involucradas en la discusión. Está apoyada por tarjetas de apuntes o de guía donde se encuentra la secuencia de preguntas o de información que se desea conocer o indagar."[50]

  Se realizó el uso de esta técnica el cual se realizó realizada al Ingeniero de Sistemas Jefe de la Unidad de Sistemas e Informática Spilco León Jardy (Ver Anexo 02), con el fin de obtener información amplia, creíble y válida para nuestro propósito, sobre la problemática del proceso de gestión de riesgos en la seguridad informática.

- **OBSERVACIÓN**

  "La observación es una técnica útil para el analista en su progreso de investigación, consiste en observar a las personas cuando efectúan su trabajo. La tarea de observar no puede reducirse a una mera percepción pasiva de hechos, situaciones o cosas.

  La observación es la percepción "activa", lo cual significa concretamente un ejercicio constante encaminado a seleccionar, organizar y relacionar los datos referentes a nuestro problema. No todo lo que aparece ante el campo del observador tiene importancia y, si la tiene, no siempre en el mismo grado; no todos los datos se refieren a las mismas variables o indicadores, y es precio estar alerta

[50] NAMAKFOROOSH, Luis. Técnicas e instrumentos de recolección de datos en los estudios científicos aplicados. 2a. ed. México, Zacateda, 2012. 100 p. ISBN: 785623589-1

para discriminar adecuadamente frente a todo este conjunto posible de informaciones."[51]

INSTRUMENTOS

- **FICHA DE REGISTRO**

  "La ficha de registro es un documento en el que se anotan las observaciones realizadas en un experimento." [52]

  En la presente investigación se usa para anotar las poblaciones de los indicadores.

2.4.2. VALIDEZ DE INSTRUMENTOS

ÍTEM	EXPERTO NOMBRES Y APELLIDOS	V. INSTRUMENTOS		
		NC.SL	NC.SF	NC.SR
01	Bello Gómez Luis	79%	80%	80%
02	Bravo Baldeón Percy	80%	81%	80%
03	Vergara Calderón Rodolfo	80%	80%	80%
TOTAL		80%	80%	80%

Según los porcentajes de los expertos, la validación de instrumentos de cada indicador de las dimensiones seguridad lógica, seguridad física y seguridad de redes, teniendo un promedio de valoración de 80% siendo esto "MUY BUENO"

2.4.3. CONFIABILIDAD DE INSTRUMENTOS

Se realizó la correlación de Pearson por cada dimensión, para poder hallar el coeficiente de correlación del pre-test y del Re-test del indicador nivel de cumplimiento, donde se muestra en la Tabla N°3

[51] GÓMEZ, Deck. Estadística aplicada a la investigación científica. 2a. ed. EE.UU., Petri, 2012. 120 p. ISBN: 1-542369-742

[52] CAPUÑAY, I. Análisis estadístico en los proyectos de investigación. 2a. ed. México, Universidad de Tijuana., 2011, 97 p.

Tabla N°3

Correlaciones

		TEST1_NIVEL_CUMPLIMIENTO	TEST2_NIVEL_CUMPLIMIENTO
TEST1_NIVEL_CUMPLIMIENTO	Correlación de Pearson	1	,741
	Sig. (bilateral)		,092
	N	6	6
TEST2_NIVEL_CUMPLIMIENTO	Correlación de Pearson	,741	1
	Sig. (bilateral)	,092	
	N	6	6

Correlación de Pearson – Seguridad lógica

Según el cuadro de nivel de confiabilidad de Cayetano (2013), podemos validar lo siguiente.

Niveles de Confiabilidad

Escala	Nivel
0.00 < sig. <0.20	Muy bajo
0.20 ≤ sig. < 0.40	Bajo
0.40 ≤ sig. < 0.60	Regular
0.60 ≤ sig. < 0.80	Aceptable
0.80 ≤ sig. < 1.00	Elevado

Fuente: Cayetano 2013

Según el cuadro de confiabilidad mostrado en líneas arriba, y teniendo un coeficiente de correlación de 0.741, podemos decir que nuestro instrumento para la seguridad lógica es confiable con un nivel de “ACEPTABLE”

Tabla N°4

Matriz de correlaciones inter-elementos

	TEST1_NIVEL_DE_CUMPLIMIENTO	TEST2_NIVEL_DE_CUMPLIMIENTO
TEST1_NIVEL_DE_CUMPLIMIENTO	1,000	,950
TEST2_NIVEL_DE_CUMPLIMIENTO	,950	1,000

Correlación de Pearson – Seguridad Física

Según el cuadro de nivel de confiabilidad de Cayetano (2013), podemos validar lo siguiente.

Niveles de Confiabilidad

Escala	Nivel
0.00 < sig. <0.20	Muy bajo
0.20 ≤ sig. < 0.40	Bajo
0.40 ≤ sig. < 0.60	Regular
0.60 ≤ sig. < 0.80	Aceptable
0.80 ≤ sig. < 1.00	Elevado

Fuente: Cayetano 2013

Según el cuadro de confiabilidad mostrado en líneas arriba, y teniendo un coeficiente de correlación de 0.950, podemos decir que nuestro instrumento para la seguridad lógica es confiable con un nivel de “ELEVADO”

Tabla N°5

Correlaciones

		TEST1_NIVEL_DE_CUMPLIMIENTO	TEST2_NIVEL_DE_CUMPLIMIENTO
TEST1_NIVEL_DE_CUMPLIMIENTO	Correlación de Pearson	1	,778
	Sig. (bilateral)		,433
	N	3	3
TEST2_NIVEL_DE_CUMPLIMIENTO	Correlación de Pearson	,778	1
	Sig. (bilateral)	,433	
	N	3	3

Correlación de Pearson – Seguridad de redes

Según el cuadro de nivel de confiabilidad de Cayetano (2013), podemos validar lo siguiente.

Niveles de Confiabilidad

Escala	Nivel
0.00 < sig. <0.20	Muy bajo
0.20 ≤ sig. < 0.40	Bajo
0.40 ≤ sig. < 0.60	Regular
0.60 ≤ sig. < 0.80	Aceptable
0.80 ≤ sig. < 1.00	Elevado

Fuente: Cayetano 2013

Según el cuadro de confiabilidad mostrado en líneas arriba, y teniendo un coeficiente de correlación de 0.778, podemos decir que nuestro instrumento para la seguridad lógica es confiable con un nivel de “ACEPTABLE”

2.4. MÉTODOS DE ANÁLISIS DE DATOS

2.4.1. PRUEBA DE NORMALIDAD

'La prueba de Shapiro- Wilk es para muestras menores a 50, y nos ayuda a poder calcular el nivel de significancia para poder identificar si la distribución es normal o no-normal'[53]

Se procedió a realizar las pruebas de normalidad para el indicador de nivel de cumplimiento a través del método Shapiro-Wilk, debido a que el tamaño de nuestra población es de 13 hallazgos y es menor a 50

El método estadístico a utilizar para la validación de las hipótesis es la Distribución Normal, porque el nivel de significancia del indicador nivel de cumplimiento es mayor a 0.05, además nos ayuda a tomar decisiones de la hipótesis en término de aceptarlas o rechazarlas.

2.4.2. PRUEBA DE HIPOTESIS

2.4.2.1. Definición de Variables

I_a: Indicador medido antes de la herramienta de gestión de riesgos para la seguridad informática en el HONADOMANI San Bartolomé.

I_d: Indicador medido después de la herramienta de gestión de riesgos para la seguridad informática en el HONADOMANI San Bartolomé.

2.4.2.2. Hipótesis Estadística

A. Hipótesis Especifica 1 (HE_1): La herramienta de gestión de riesgos incrementa el nivel de cumplimiento de la segurida0d lógica en el HONADOMANI San Bartolomé

Variables:

I_{a1}: El nivel de cumplimiento de la seguridad lógica medido antes de la aplicación de una herramienta de gestión de riesgos.

I_{d1}: El nivel de cumplimiento de la seguridad lógica medido después de la aplicación de una herramienta de gestión de riesgos.

[53] Hernández Sampiere. Metodología de investigación científica. 5a. ed. México, Editorial cáliz, 2006. 376 p. ISBN: 1-569874-156

Hipótesis Nula (H_0): Una herramienta de gestión de riesgos no aumenta el nivel de cumplimiento de la seguridad lógica en el HONADOMANI San Bartolomé

$$H_A: I_{a1} > I_{d1}$$

Hipótesis Alternativa (H_A): Una herramienta de gestión de riesgos aumenta el nivel de cumplimiento de la seguridad lógica en el HONADOMANI San Bartolomé

$$H_O: I_{a1} \leq I_{d1}$$

B. Hipótesis Especifica 2 (HE_2): La herramienta de gestión de riesgos disminuye el nivel cumplimiento para la seguridad física en el HONADOMANI San Bartolomé

Variables:

I_{a1}: El nivel de cumplimiento se la seguridad física medido antes de la aplicación de una herramienta de gestión de riesgos.

I_{d1}: El nivel de cumplimiento de la seguridad física medido después de la aplicación de una herramienta de gestión de riesgos.

Hipótesis Nula (H_0): Una herramienta de gestión de riesgos no aumenta el nivel de cumplimiento de la seguridad física en el HONADOMANI San Bartolomé

$$H_A: I_{a1} > I_{d1}$$

Hipótesis Alternativa (H_A): Una herramienta de gestión de riesgos aumenta el nivel de cumplimiento de la seguridad física en el HONADOMANI San Bartolomé

$$H_O: I_{a1} \leq I_{d1}$$

C. Hipótesis Específica 3 (HE_3): La herramienta de gestión de riesgos aumenta el cumplimiento en la seguridad de redes en el HONADOMANI San Bartolomé

Variables:

I_{a1}: El cumplimiento de la seguridad de redes medido antes de la implementación de una herramienta de gestión de riesgos.

I_{d1}: El cumplimiento de la seguridad de redes medido después de la implementación de una herramienta de gestión de riesgos.

Hipótesis Nula (H_0): Una herramienta de gestión de riesgos no aumenta el cumplimiento de la seguridad de redes en el HONADOMANI San Bartolomé

$$H_A: I_{a1} > I_{d1}$$

Hipótesis Alternativa (H_A): Una herramienta de gestión de riesgos aumenta el nivel de cumplimiento de la seguridad de redes en el HONADOMANI San Bartolomé

$$H_O: I_{a1} \leq I_{d1}$$

2.4.2.3. Nivel de Significancia

Nivel de significancia (α):0.05

Nivel de confianza (γ = 1-α): 0.95

2.4.2.4. Estadístico de Prueba

"El estadístico de prueba a utilizar será la Saphiro-Wilk, debido a que comprueba si los nuevos valores transformados se distribuyen normalmente. De modo que es muy importante poder contar con un método para comprobar la normalidad de un conjunto de datos originados o transformados.

En las pruebas de hipótesis para la media (0), cuando se conoce que la variable aleatoria no tiene una distribución normal (1) cuando la variable aleatoria tiene una distribución normal, o cuando el valor de la muestra es grande (menor o igual a 50), el valor estadístico de prueba de Saphiro-Wilk y se determina a partir d "[54]

Figura N°12

Fuente: Ortega

$$W_c = \frac{b^2}{\sum_{i=1}^{n}(X_i - \bar{X})^2}$$

Estadístico de Prueba

[54] ORTEGA, VEGA y ZEÑA. Análisis estadístico en estudios científicos. 3a. ed. México, Prateris, 2012. 132 p. ISBN: 563923588-1

$\overline{Xa}$: Media muestral antes de la aplicación de un sistema web.

$\overline{Xd}$: Media muestral después de la aplicación de un sistema web.

s_a: Varianza muestral antes de la aplicación de un sistema web.

s_d: Varianza muestral después de la aplicación de un sistema web.

n_a: Tamaño de la muestra antes de la aplicación de un sistema web.

n_d: Tamaño de la muestra después de la aplicación de un sistema web.

2.4.2.5. Varianza Muestral (S^2)

"La varianza muestral es el promedio de las varianzas de las muestras. Evidentemente se puede utilizar cualquiera de las varianzas muéstrales, pero el promedio de todas ellas proporcionará la mejor estimación debido al mayor número de observaciones que representa, esto se representa de la siguiente manera:"[55]

$$s^2 = \frac{\sum_{i=1}^{n} (x_i - \bar{x})^2}{n - 1}$$

Dónde:

$\bar{X}$**:** Media muestral.

$\mathbf{X_i}$**:** Valores de la variable.

N**:** Tamaño de la población.

2.4.2.6. Región de Rechazo

"En la presente investigación se ha establecido un nivel de confianza γ = 0.95, según la T-Student."[56]

La Región Rechazo es Z

Donde:

X= Media muestral

u= Media poblada

α= Desviación típica

$$Z = \frac{\bar{X} - \mu}{\sigma / \sqrt{n}}$$

[55] GÓMEZ, Deck. Estadística aplicada a la investigación científica. 2a. ed. EE.UU., Petri, 2012. 140 p. ISBN: 1-542369-742

[56] ORTEGA, VEGA y ZEÑA. Análisis estadístico en estudios científicos. 3a. ed. México, Prateris, 2012. 136 p. ISBN: 563923588-1

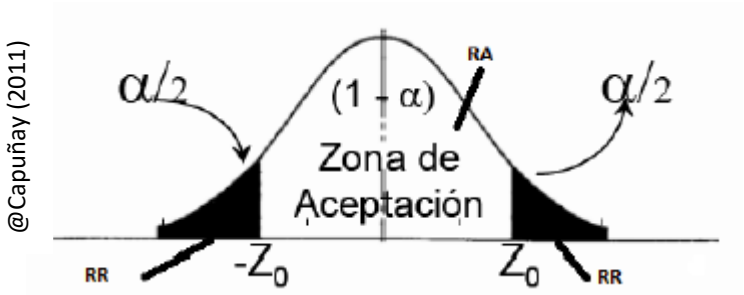
N=.Tamaño de la muestra

Luego la región de rechazo es: Z

2.4.2.7. Análisis de Resultados

Los resultados que se obtendrán serán evaluados a través de la prueba T-Student, con ella se verifica la formulación de la hipótesis, determinando si se rechaza o acepta la hipótesis nula (Ver Figura 14).

Figura N°14



Distribución Normal

Dónde:

Zx: Punto Crítico.

RR: Región de rechazo de la hipótesis nula.

RA: Región de aceptación de la hipótesis nula

CAPÍTULO – 03:

RESULTADOS

1.1. Análisis Descriptivo

En el estudio se aplicó una herramienta de gestión de riesgos para evaluar el nivel de cumplimiento de la seguridad lógica, física y de redes para la seguridad informatica; para ello se aplicó una auditoria inicial para conocer las condiciones iniciales del indicador; posteriormente se aplicó la herramienta de gestión de riesgos para ver los cambios del nivel de cumplimiento de la seguridad lógica, física y redes para la seguridad informatica. Los resultados descriptivos de estas medidas se observan en las siguientes tablas 6, 7 y 8.

INDICADOR: Nivel de cumplimiento de la Seguridad Lógica

Los resultados descriptivos del Nivel de cumplimiento de la Seguridad Lógica se muestran en la Tabla N°6

Tabla N°6

Medidas descriptivas del Nivel de Cumplimiento de la Seguridad Lógica antes y después de aplicar la herramienta de gestión de riesgos.

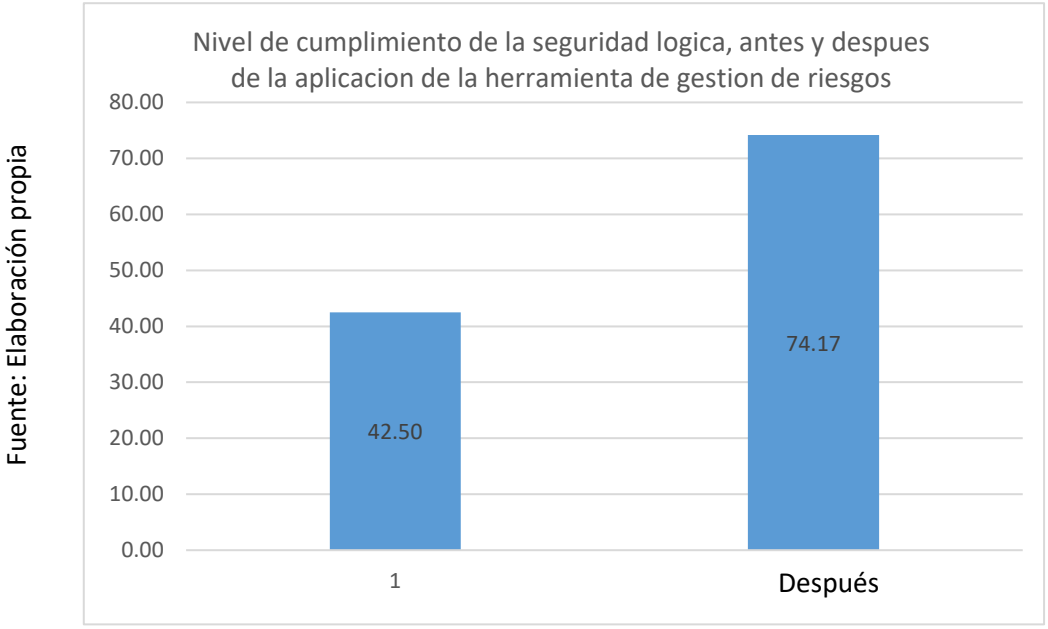
Estadísticos descriptivos

	N	Mínimo	Máximo	Media	Desv. Típ.
TEST1_NIVEL_CUMPLIMIENTO	6	10,00	85,00	42,5000	30,61862
TEST2_NIVEL_CUMPLIMIENTO	6	60,00	95,00	74,1667	12,00694
N válido (según lista)	6				

En el caso del Nivel de Cumplimiento de la Seguridad Lógica, en el pre –test se obtuvo un valor de 42.50%, mientras que en el post-test fue de 74.16% tal como se muestra en la figura N°15; esto indica una gran diferencia entre el antes y después de la aplicación de la herramienta de gestión de riesgos; así mismo el nivel de cumplimiento mínimo fue de 10% antes, y 60% (ver tabla N°6)después de la aplicación de la herramienta de gestión de riesgos.

En cuanto a la dispersión del nivel de cumplimiento, en el pre-test se tuvo una variabilidad de 30.61%; sim embargo en el post-test se tuvo un valor de 12.00%

Figura N°15



Fuente: Elaboración propia

Nivel de cumplimiento de la Seguridad Lógica

INDICADOR: Nivel de cumplimiento de la Seguridad Física

Los resultados descriptivos del Nivel de cumplimiento de la Seguridad Física se muestran en la Tabla N°7

Tabla N°7

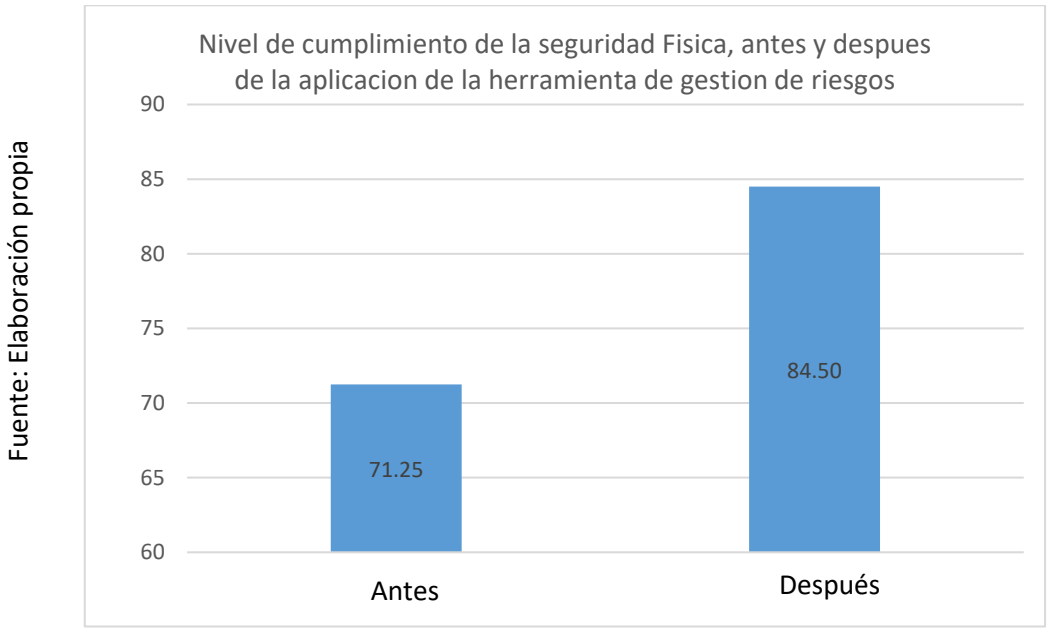
Medidas descriptivas del Nivel de Cumplimiento de la Seguridad Física antes y después de aplicar la herramienta de gestión de riesgos.

Estadísticos descriptivos

	N	Mínimo	Máximo	Media	Desv. Típ.
TEST1_NIVEL_DE_CUMPLIMIENTO	4	60,00	80,00	71,2500	8,53913
TEST2_NIVEL_DE_CUMPLIMIENTO	4	79	90	84,50	5,155
N válido (según lista)	4				

En el caso del Nivel de Cumplimiento de la Seguridad Física, en el pre –test se obtuvo un valor de 71.25%, mientras que en el post-test fue de 84.50% tal como se muestra en la figura N°16; esto indica una gran diferencia entre el antes y después de la aplicación de la herramienta de gestión de riesgos; así mismo el nivel de cumplimiento mínimo fue de 60% antes, y 79% (ver tabla N°7)después de la aplicación de la herramienta de gestión de riesgos. En cuanto a la dispersión del nivel de cumplimiento, en el pre-test se tuvo una variabilidad de 8.53%; sim embargo en el post-test se tuvo un valor de 5.15%

Figura N°16



Fuente: Elaboración propia

Nivel de cumplimiento de la Seguridad Física

INDICADOR: Nivel de cumplimiento de la Seguridad de redes

Los resultados descriptivos del Nivel de cumplimiento de la Seguridad de redes se muestran en la Tabla N°8

Tabla N°8

Medidas descriptivas del Nivel de Cumplimiento de la Seguridad de redes antes y después de aplicar la herramienta de gestión de riesgos.

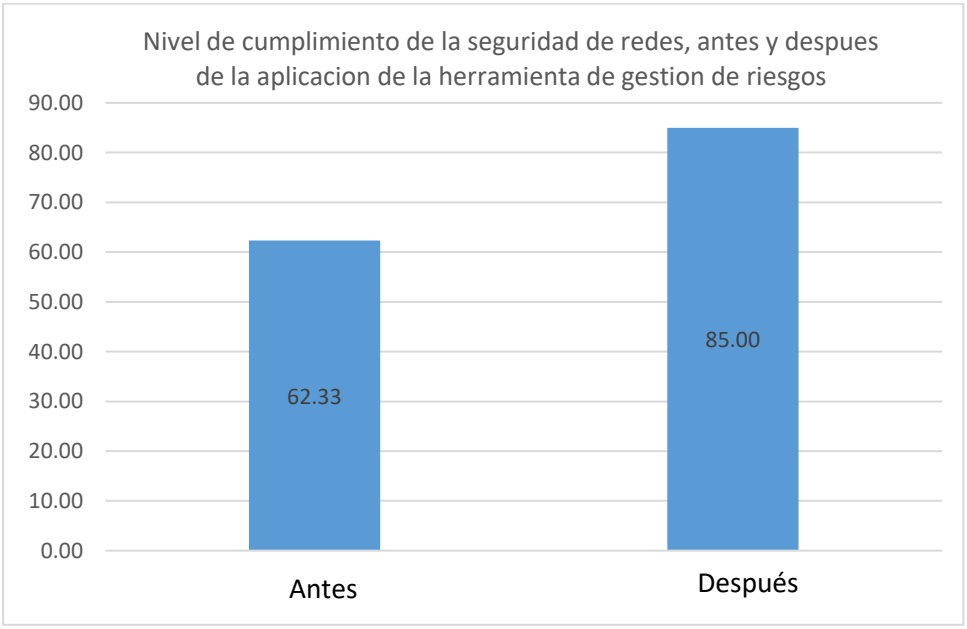
Estadísticos descriptivos

	N	Mínimo	Máximo	Media	Desv. Típ.
TEST1_NIVEL_DE_CUMPLIMIENTO	3	55	67	62.33	6,429
TEST2_NIVEL_DE_CUMPLIMIENTO	3	80	90	85.00	5,000
N válido (según lista)	3				

En el caso del Nivel de Cumplimiento de la Seguridad de redes, en el pre – test se obtuvo un valor de 62.33%, mientras que en el post-test fue de 85.00% tal como se muestra en la figura N°8; esto indica una gran diferencia entre el antes y después de la aplicación de la herramienta de gestión de riesgos; así mismo el nivel de cumplimiento mínimo fue de 55% antes, y 80% (ver tabla N°12)después de la aplicación de la herramienta de gestión de riesgos.

En cuanto a la dispersión del nivel de cumplimiento, en el pre-test se tuvo una variabilidad de 6.42%; sim embargo en el post-test se tuvo un valor de 5.00%

Figura N°17



Fuente: Elaboración propia

Nivel de cumplimiento de la Seguridad de redes

1.2. Análisis Inferencial

Prueba de Normalidad

Se procedió a realizar las prueba de normalidad para los indicadores de seguridad Lógica, Física y redes para la seguridad informatica, a través del método Saphiro-Wilk, 'debido a que el tamaño de la muestra por selección es de 6 salvaguardas y es menor a 50, tal como lo indica Hernández.'[58]. Dicha prueba se realizó introduciendo los datos en el software de cálculo estadístico SPSS 23.0, para un nivel de confiabilidad del 95%, bajo las siguientes condiciones:

Si:

Sig. < 0.05 adopta una distribución no normal

Sig. ≥ 0.05 adopta una distribución normal

Donde:

Sig. : P – valor o nivel crítico del contraste

Los resultados fueron los siguientes

INDICADOR: Nivel de cumplimiento de la Seguridad Lógica

Con el objetivo de seleccionar la prueba de hipótesis; los datos fueron sometidos a la comprobación de su distribución, específicamente si los datos del cumplimiento de la Seguridad Lógica contaban con distribución normal.

[58] Hernández, Metodología científica, 2006, p.376

Tabla N°9

Prueba de normalidad del nivel de cumplimiento de la seguridad lógica antes y después de la aplicación de la herramienta de gestión de riesgos

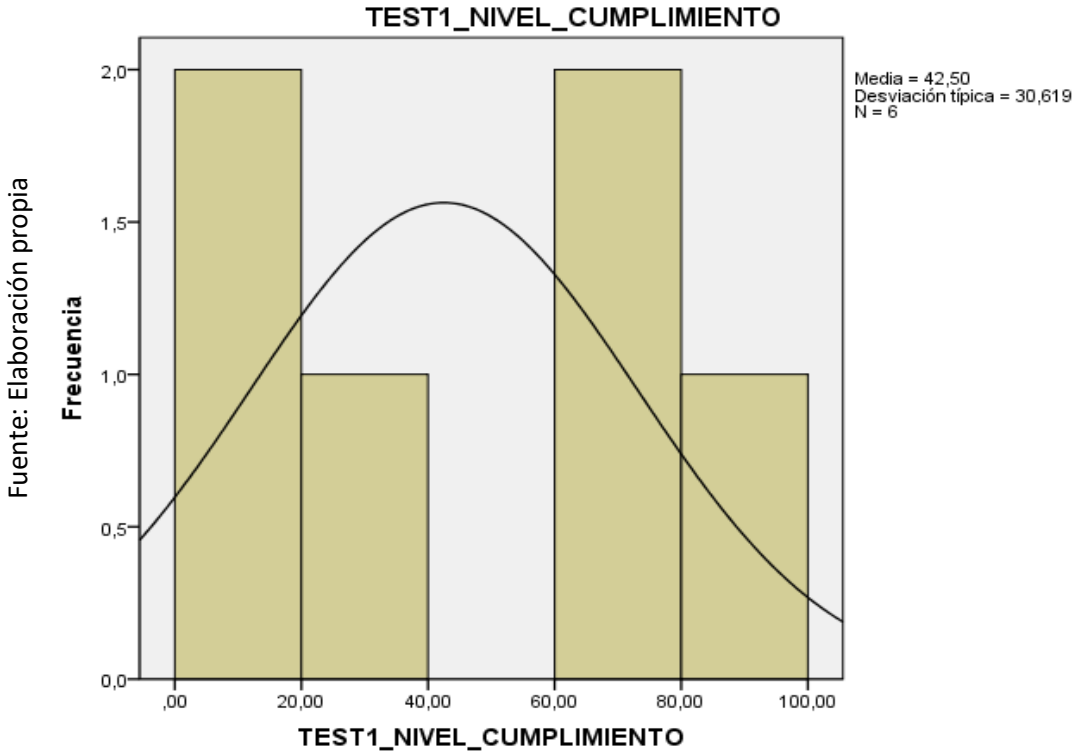
Pruebas de normalidad

	Saphiro-Wilk		
	Estadístico	gl	Sig.
TEST1_NIVEL_CUMPLIMIENTO	,899	6	,366
TEST2_NIVEL_CUMPLIMIENTO	,889	6	,312

Corrección de la significación de Lilliefors

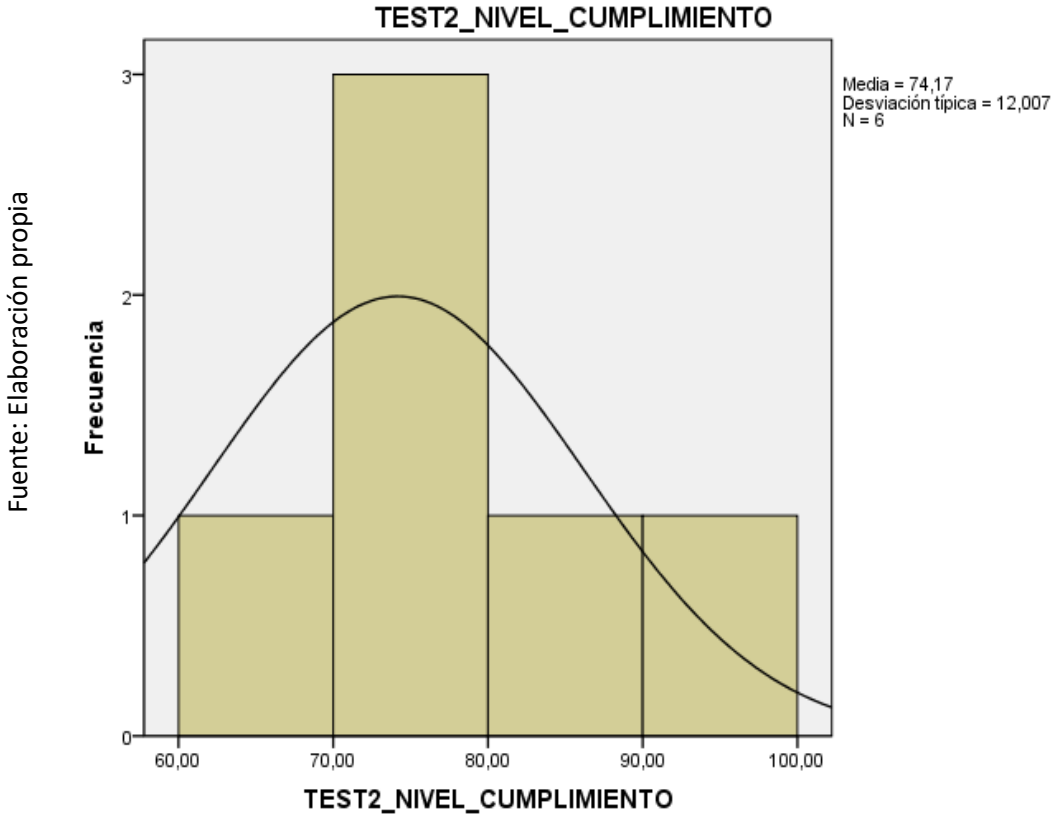
Como se muestra en la Tabla N°9 los resultados de la prueba indican que el Sig. Del nivel de cumplimiento de la seguridad lógica en la seguridad informatica en el Pre-Test fue de 0.366, cuyo valor es mayor a 0.05. Por lo tanto el nivel de cumplimiento de la seguridad lógica se distribuye normalmente. Los resultados de la prueba del Post-Test indican que el Sig. Del nivel de cumplimiento de la seguridad lógica fue de 0.312, cuyo valor es mayor que 0.05, por lo que indica que el nivel de cumplimiento de la seguridad lógica se distribuye normalmente. Lo que confirma la distribución normal de ambos datos de la muestra, se puede apreciar en las Figuras 18 y 19

Figura N°18



Fuente: Elaboración propia

Figura N°19



Fuente: Elaboración propia

INDICADOR: Nivel de cumplimiento de la Seguridad Física

Con el objetivo de seleccionar la prueba de hipótesis; los datos fueron sometidos a la comprobación de su distribución, específicamente si los datos del cumplimiento de la Seguridad Física contaban con distribución normal.

Con el objetivo de seleccionar la prueba de hipótesis; los datos fueron sometidos a la comprobación de su distribución, específicamente si los datos del cumplimiento de la Seguridad Lógica contaban con distribución normal.

Tabla N°10

Prueba de normalidad del nivel de cumplimiento de la seguridad física antes y después de la aplicación de la herramienta de gestión de riesgos

Pruebas de normalidad

	Saphiro-Wilk		
	Estadístico	gl	Sig.
TEST1_NIVEL_CUMPLIMIENTO	,971	3	,850
TEST2_NIVEL_CUMPLIMIENTO	,926	3	,570

b. Corrección de la significación de Lilliefors

Como se muestra en la Tabla N°10 los resultados de la prueba indican que el Sig. Del nivel de cumplimiento de la seguridad Física en la seguridad informatica en el Pre-Test fue de 0.850, cuyo valor es mayor a 0.05. Por lo tanto el nivel de cumplimiento de la seguridad Física se distribuye normalmente. Los resultados de la prueba del Post-Test indican que el Sig. Del nivel de cumplimiento de la seguridad Física fue de 0.570, cuyo valor es mayor que 0.05, por lo que indica que el nivel de cumplimiento de la seguridad Física se distribuye normalmente. Lo que confirma la distribución normal de ambos datos de la muestra, se puede apreciar en las Figuras 20 y 21

Figura N°20

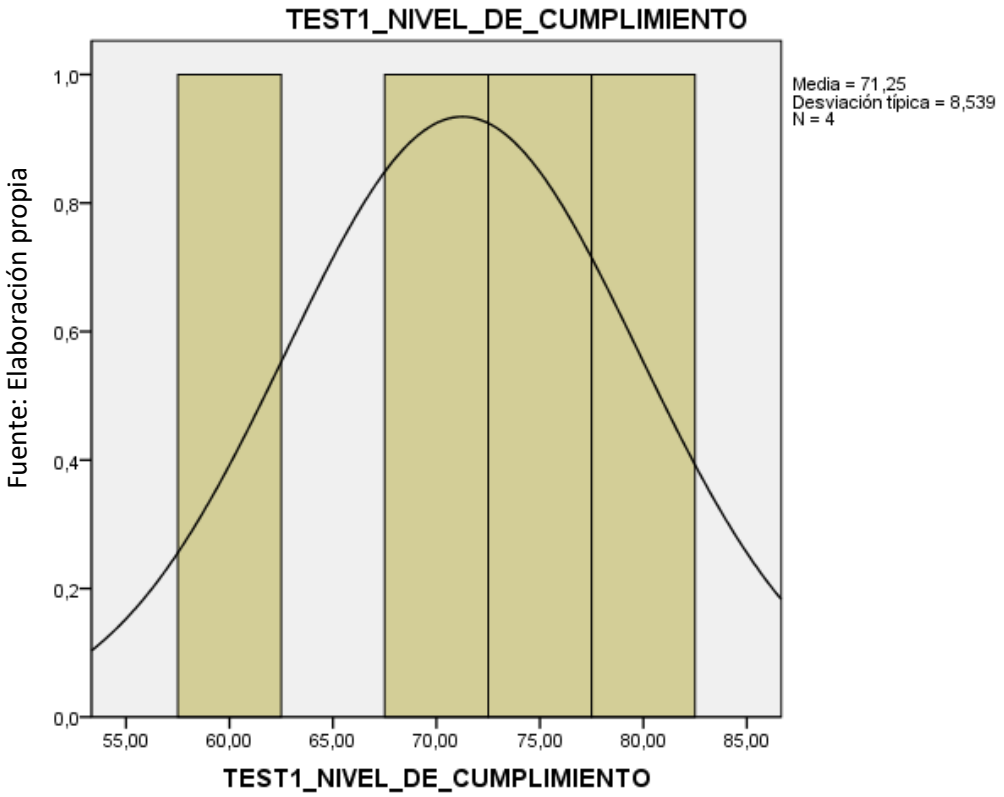
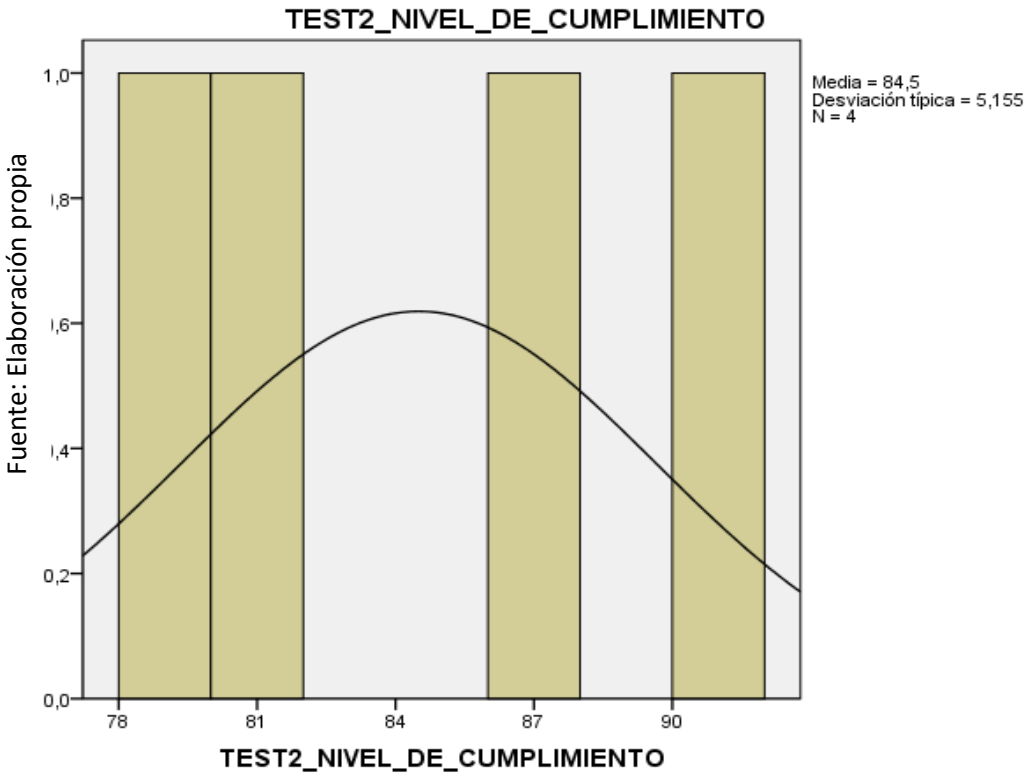


Figura N°21



INDICADOR: Nivel de cumplimiento de la Seguridad de redes
Con el objetivo de seleccionar la prueba de hipótesis; los datos fueron sometidos a la comprobación de su distribución, específicamente si los datos del cumplimiento de la Seguridad de redes contaban con distribución normal.

Con el objetivo de seleccionar la prueba de hipótesis; los datos fueron sometidos a la comprobación de su distribución, específicamente si los datos del cumplimiento de la Seguridad Lógica contaban con distribución normal.

Tabla N°11

Prueba de normalidad del nivel de cumplimiento de la seguridad de redes antes y después de la aplicación de la herramienta de gestión de riesgos

Pruebas de normalidad

	Saphiro-Wilk		
	Estadístico	gl	Sig.
TEST1_NIVEL_CUMPLIMIENTO	,871	3	,298
TEST2_NIVEL_CUMPLIMIENTO	1,000	3	1,000

c. Corrección de la significación de Lilliefors

Como se muestra en la Tabla N°11 los resultados de la prueba indican que el Sig. Del nivel de cumplimiento de la seguridad de redes en la seguridad informatica en el Pre-Test fue de 0,298, cuyo valor es mayor a 0.05. Por lo tanto el nivel de cumplimiento de la seguridad de redes se distribuye normalmente. Los resultados de la prueba del Post-Test indican que el Sig. Del nivel de cumplimiento de la seguridad de redes fue de 1,000, cuyo valor es mayor que 0.05, por lo que indica que el nivel de cumplimiento de la seguridad de redes se distribuye normalmente. Lo que confirma la distribución normal de ambos datos de la muestra, se puede apreciar en las Figuras 22 y 23.

Figura N°22

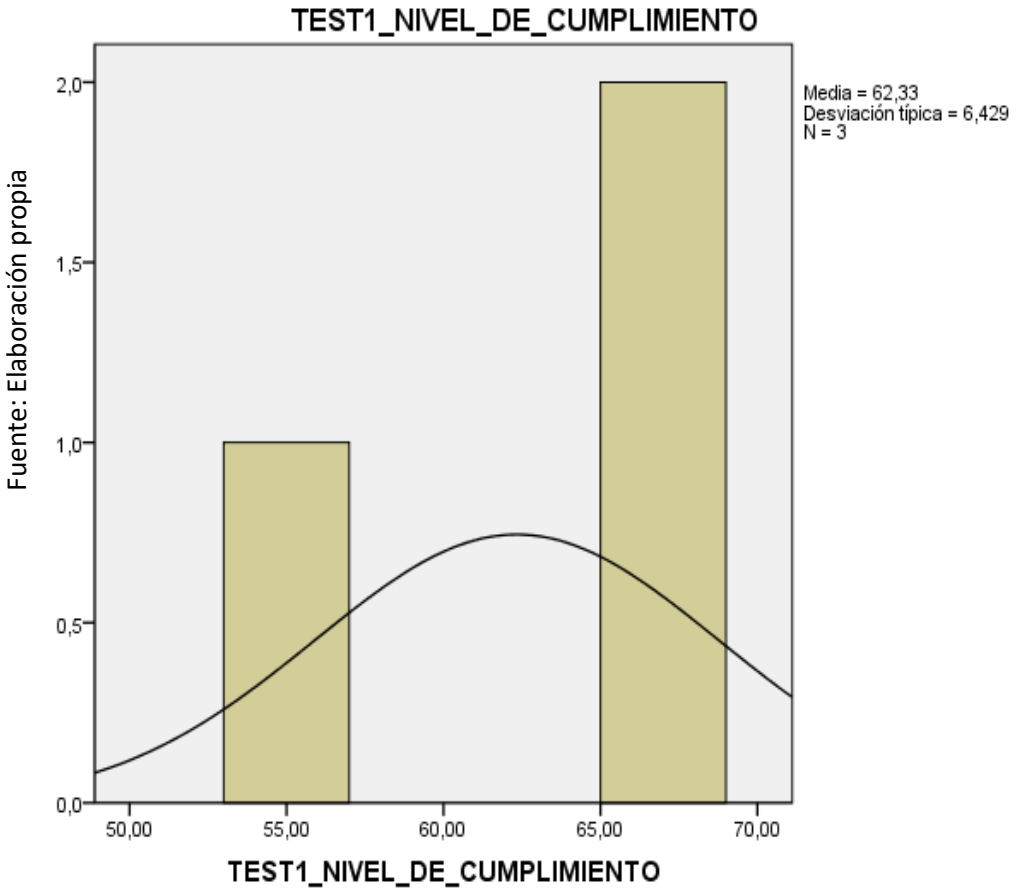
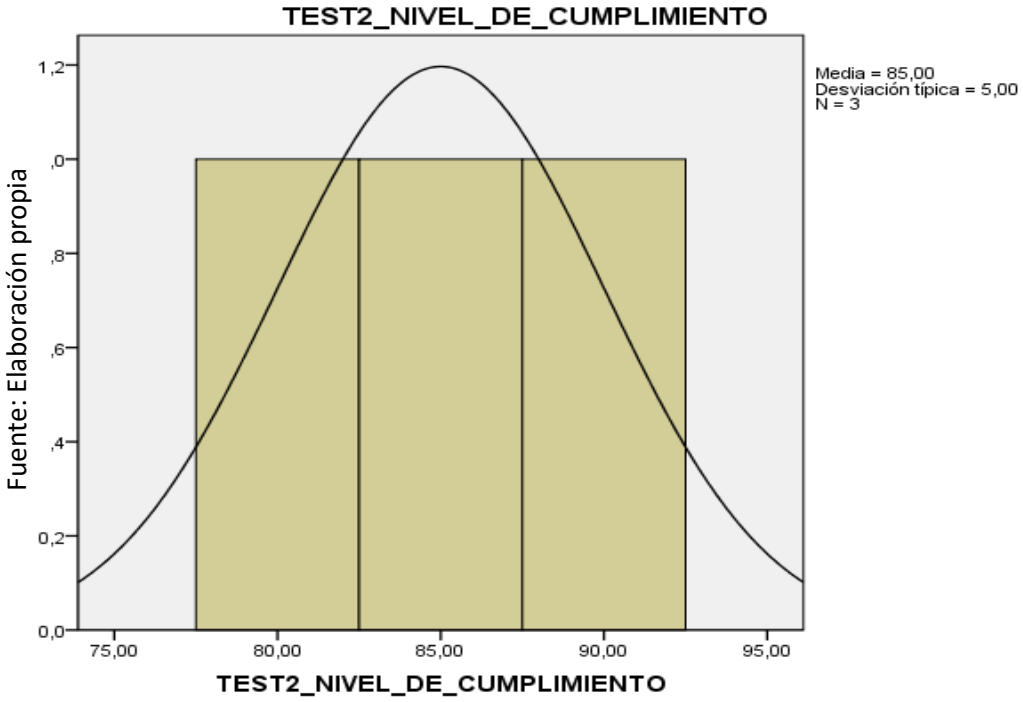


Figura N°23



1.3. Prueba de Hipótesis

1.3.1. Definición de Variables

I_a: Indicador medido antes de la herramienta de gestión de riesgos para la seguridad informática en el HONADOMANI San Bartolomé.

I_d: Indicador medido después de la herramienta de gestión de riesgos para la seguridad informática en el HONADOMANI San Bartolomé.

Hipótesis Estadística

A. Hipótesis Especifica 1 (HE_1): La herramienta de gestión de riesgos incrementa el cumplimiento de la segurida0d lógica en el HONADOMANI San Bartolomé

Variables:

I_{a1}: El nivel de cumplimiento de la seguridad lógica medido antes de la aplicación de una herramienta de gestión de riesgos.

I_{d1}: El nivel de cumplimiento de la seguridad lógica medido después de la aplicación de una herramienta de gestión de riesgos.

Hipótesis Nula (H_0): Una herramienta de gestión de riesgos no aumenta el cumplimiento de la seguridad lógica en el HONADOMANI San Bartolomé

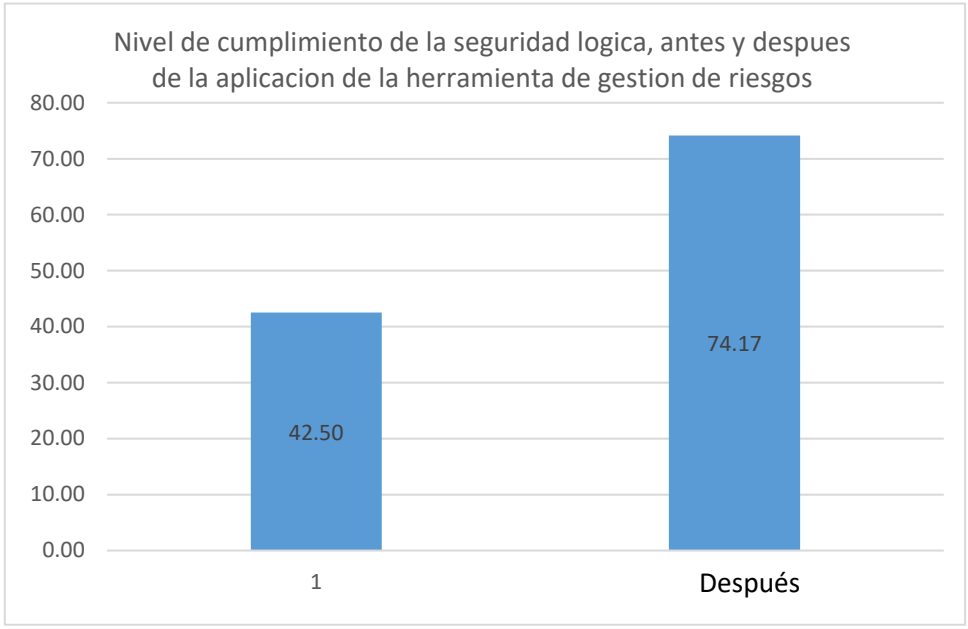
$$H_A: I_{a1} > I_{d1}$$

Hipótesis Alternativa (H_A): Una herramienta de gestión de riesgos aumenta el cumplimiento de la seguridad lógica en el HONADOMANI San Bartolomé

$$H_O: I_{a1} \leq I_{d1}$$

En la figura N°24, el nivel de cumplimiento de la seguridad lógica en el Pre-Test es de 42.50% y en el Post-Test es de 74.17%

Figura N°24



Fuente: Elaboración propia

Nivel de cumplimiento de la Seguridad Lógica

Se concluye de la Figura N°24 que existe un incremento en el nivel de cumplimiento de la seguridad lógica, el cual se puede verificar al comparar las medias respectivas, que asciende de 42.50% al valor de 74.17%

En cuanto al resultado del contraste de hipótesis se aplicó la Prueba T-Student, debido a que los datos obtenidos durante la investigación (Pre-Test y Post-Test) se distribuyen normalmente. El valor de T contraste es de -3.348, el cual es claramente menor que -2.015. (Ver tabla N°12)

Tabla N°12

Prueba de T-Student para el índice de calidad del Inventario en el nivel de cumplimiento de la seguridad lógica antes y después de la aplicación de la herramienta de gestión de riesgos

Prueba de T-Student

		Media	t	gl	Sig. (Bilateral)
Par 1	TEST1_NIVEL_CUMPLIMIENTO	42,5000	-3.348	5	0.020
	TEST2_NIVEL_CUMPLIMIENTO	74,1667			

Evaluando la Sig. (Bilateral), vemos que la significancia estadística es de 0.020, lo cual es < 0.05 por lo que podemos decir que hay diferencias estadísticamente significativas entre las muestras relacionadas (Pre-Test y Post-Test)

Entonces, se rechaza la hipótesis nula, aceptando la hipótesis alterna con un 95% de confianza. Además el valor T obtenido, como se muestra en la Figura N°25, se ubica en la zona de rechazo. Por lo tanto una herramienta de gestión de riesgos aumenta el cumplimiento de la seguridad lógica en el HONADOMANI San Bartolomé en el año 2016.

La fórmula para calcular la región de rechazo es la siguiente

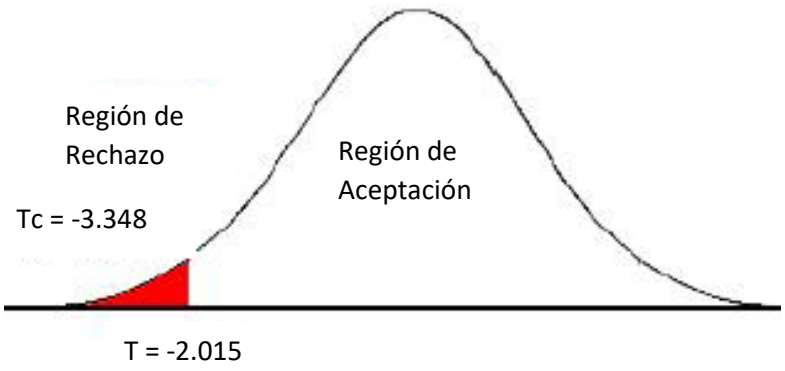
$$Z = \frac{\bar{X} - \mu}{\sigma / \sqrt{n}}$$

$$Tc = \frac{42.50 - 74.17}{23.17/\sqrt{6}} \quad Tc = -\frac{31.67}{\frac{23.17}{2.45}} \quad Tc = \frac{-31.67}{9.457} \quad Tc = -3.348$$

T-Contraste: -3.348 < -2.015

Figura N°25

Fuente: Elaboración propia



Entonces se rechaza la hipótesis nula y se acepta la hipótesis alterna con un 95% de confianza

B. Hipótesis Especifica 2 (HE_2): La herramienta de gestión de riesgos disminuye el cumplimiento para la seguridad física en el HONADOMANI San Bartolomé

Variables:

I_{a1}: El nivel de cumplimiento se la seguridad física medido antes de la aplicación de una herramienta de gestión de riesgos.

I_{d1}: El nivel de cumplimiento de la seguridad física medido después de la aplicación de una herramienta de gestión de riesgos.

Hipótesis Nula (H_0): Una herramienta de gestión de riesgos no aumenta el cumplimiento de la seguridad física en el HONADOMANI San Bartolomé

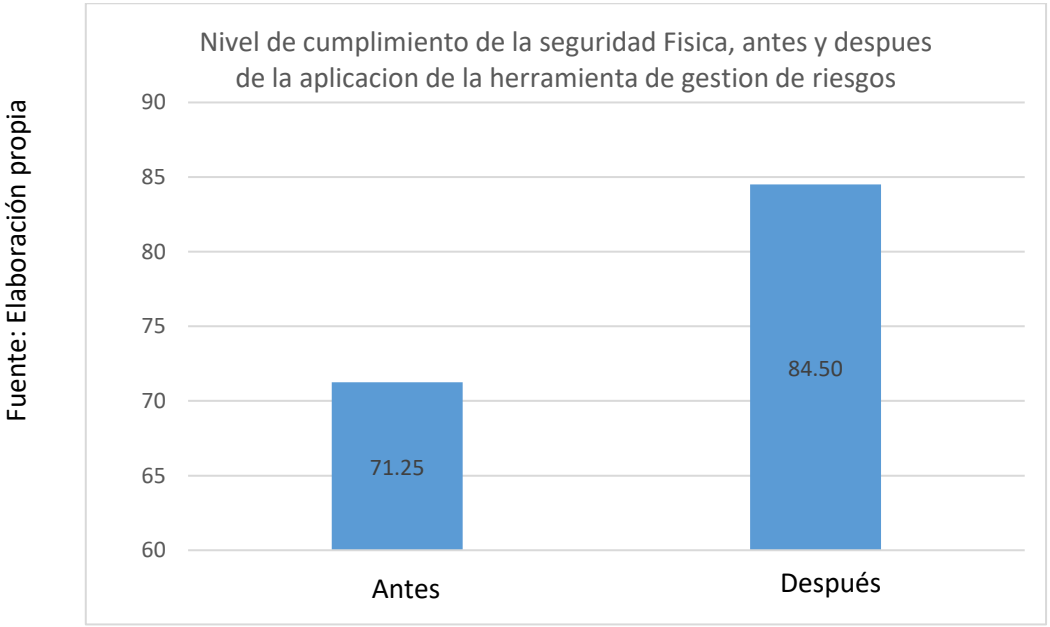
$$H_A: I_{a1} > I_{d1}$$

Hipótesis Alternativa (H_A): Una herramienta de gestión de riesgos aumenta el cumplimiento de la seguridad física en el HONADOMANI San Bartolomé

$$H_O: I_{a1} \leq I_{d1}$$

En la figura N°26, el nivel de cumplimiento de la seguridad Física en el Pre-Test es de 71.25% y en el Post-Test es de 84.50%

Figura N°26



Fuente: Elaboración propia

Nivel de cumplimiento de la Seguridad Física

Se concluye de la Figura N°26 que existe un incremento en el nivel de cumplimiento de la seguridad física, el cual se puede verificar al comparar las medias respectivas, que asciende de 71.25% al valor de 84.50%

En cuanto al resultado del contraste de hipótesis se aplicó la Prueba T-Student, debido a que los datos obtenidos durante la investigación (Pre-Test y Post-Test) se distribuyen normalmente. El valor de T contraste es de -6.662, el cual es claramente menor que -2.353. (Ver tabla N°13)

Tabla N°13

Prueba de T-Student para el índice de calidad del Inventario en el nivel de cumplimiento de la seguridad física antes y después de la aplicación de la herramienta de gestión de riesgos

Prueba de T-Student

		Media	t	gl	Sig. (Bilateral)
Par 1	TEST1_NIVEL_CUMPLIMIENTO	71.2500	-6.662	3	0.007
	TEST2_NIVEL_CUMPLIMIENTO	84.50			

Evaluando la Sig. (Bilateral), vemos que la significancia estadística es de 0.007, lo cual es < 0.05 por lo que podemos decir que hay diferencias estadísticamente significativas entre las muestras relacionadas (Pre-Test y Post-Test)

Entonces, se rechaza la hipótesis nula, aceptando la hipótesis alterna con un 95% de confianza. Además el valor T obtenido, como se muestra en la Figura N°27, se ubica en la zona de rechazo. Por lo tanto una herramienta de gestión de riesgos aumenta el cumplimiento de la seguridad física en el HONADOMANI San Bartolomé

La fórmula para calcular la región de rechazo es la siguiente

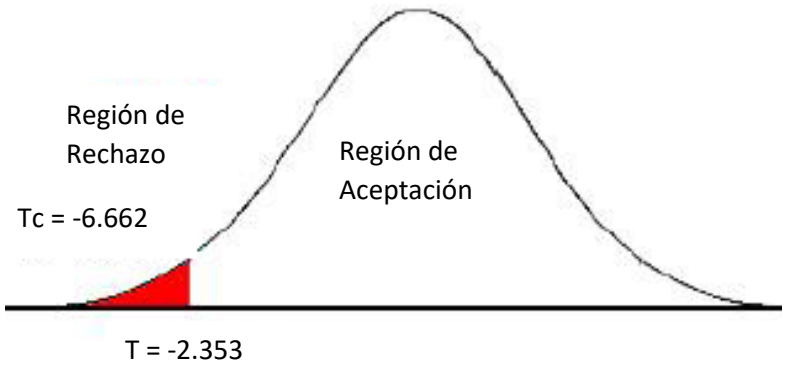
$$Z = \frac{\bar{X} - \mu}{\sigma / \sqrt{n}}$$

$$Tc = \frac{71.25 - 84.50}{3.98/\sqrt{4}} \quad Tc = -\frac{13.25}{3.98/2} \quad Tc = \frac{-13.25}{1.99} \quad Tc = -6.662$$

T-Contraste: -6.662 < -2.353

Figura N°27

Fuente: Elaboración propia



Entonces se rechaza la hipótesis nula y se acepta la hipótesis alterna con un 95% de confianza

C. Hipótesis Específica 3 (HE_3): La herramienta de gestión de riesgos aumenta el cumplimiento en la seguridad de redes en el HONADOMANI San Bartolomé

Variables:

I_{a1}: El cumplimiento de la seguridad de redes medido antes de la implementación de una herramienta de gestión de riesgos.

I_{d1}: El cumplimiento de la seguridad de redes medido después de la implementación de una herramienta de gestión de riesgos.

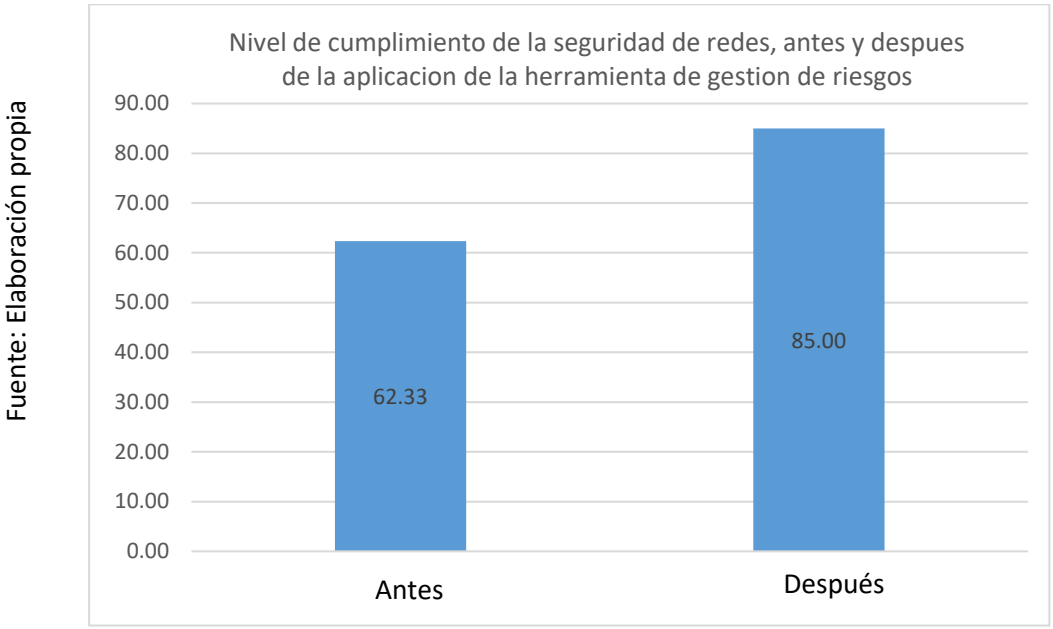
Hipótesis Nula (H_0): Una herramienta de gestión de riesgos no aumenta el cumplimiento de la seguridad de redes en el HONADOMANI San Bartolomé

$$H_A: I_{a1} > I_{d1}$$

Hipótesis Alternativa (H_A): Una herramienta de gestión de riesgos aumenta el cumplimiento de la seguridad de redes en el HONADOMANI San Bartolomé

En la figura N°28, el nivel de cumplimiento de la seguridad de redes en el Pre-Test es de 65.67% y en el Post-Test es de 87.33%

Figura N°28



Fuente: Elaboración propia

Nivel de cumplimiento de la Seguridad de redes

Se concluye de la Figura N°28 que existe un incremento en el nivel de cumplimiento de la seguridad de redes, el cual se puede verificar al comparar las medias respectivas, que asciende de 65.67% al valor de 87.33%

En cuanto al resultado del contraste de hipótesis se aplicó la Prueba T-Student, debido a que los datos obtenidos durante la investigación (Pre-Test y Post-Test) se distribuyen normalmente. El valor de T contraste es de -9,714, el cual es claramente menor que -2,920. (Ver tabla N°14)

Tabla N°14

Prueba de T-Student para el índice de calidad del Inventario en el nivel de cumplimiento de la seguridad de redes antes y después de la aplicación de la herramienta de gestión de riesgos

Prueba de T-Student

		Media	t	gl	Sig. (Bilateral)
Par 1	TEST1_NIVEL_CUMPLIMIENTO	62,33	-9.714	2	0.010
	TEST2_NIVEL_CUMPLIMIENTO	85,00			

Evaluando la Sig. (Bilateral), vemos que la significancia estadística es de 0.010, lo cual es < 0.05 por lo que podemos decir que hay diferencias estadísticamente significativas entre las muestras relacionadas (Pre-Test y Post-Test)

Entonces, se rechaza la hipótesis nula, aceptando la hipótesis alterna con un 95% de confianza. Además el valor T obtenido, como se muestra en la Figura N°29, se ubica en la zona de rechazo. Por lo tanto una herramienta de gestión de riesgos aumenta el cumplimiento de la seguridad de redes en el HONADOMANI San Bartolomé

La fórmula para calcular la región de rechazo es la siguiente

$$Z = \frac{\bar{X} - \mu}{\sigma / \sqrt{n}}$$

$$Tc = \frac{62.33 - 85.00}{4.04/\sqrt{3}} \quad Tc = -\frac{22.67}{\frac{4.04}{1.73}} \quad Tc = \frac{-22.67}{2.335} \quad Tc = -9.714$$

T-Contraste: -9.714 < -2.920

Figura N°29

Fuente: Elaboración propia

Entonces se rechaza la hipótesis nula y se acepta la hipótesis alterna con un 95% de confianza

III. DISCUSIÓN

En base a los resultados en la presente investigación se analiza una comparativa sobre el nivel de cumplimiento de la seguridad lógica, física y redes en la seguridad informatica.

1) En el nivel de cumplimiento de la seguridad lógica para la seguridad informatica en el HONADOMANI San Bartolomé, en la medición del Pre-Test, alcanzó los 42.50% de porcentaje y con la aplicación de la herramienta de gestión de riesgos alcanzo un 74.17%.

   Los resultados obtenidos indican que aumento en un 31.67% el nivel de cumplimiento de la seguridad lógica para la seguridad informatica del HONADOMANI San Bartolomé.

   En la realización de la investigación encontramos similitud con el antecedente de Karina del rocío Gaona Vásquez, en su tesis titulada "Aplicación de la metodología magerit para el análisis y gestión de riesgos de la seguridad de la información aplicado a la empresa pesquera e industrial bravito s.a. en la ciudad de Machala" En donde menciona como conclusión lo siguiente :Los resultados señalan que con la aplicación de la herramienta de gestión de riesgos MAGERI, se calcula el nivel de cumplimiento de la seguridad informatica forma efectiva, en la cual se obtuvo un nivel de cumplimiento de los distintos tipos de seguridad.

   Y en nuestra investigación aumento el nivel de cumplimiento de la seguridad lógica en un 31.37%

2) En el nivel de cumplimiento de la seguridad Física para la seguridad informatica en el HONADOMANI San Bartolomé, en la medición del Pre-Test, alcanzó los 71.25% de porcentaje y con la aplicación de la herramienta de gestión de riesgos alcanzo un 84.50%.

   Los resultados obtenidos indican que aumento en un 13.25% el nivel de cumplimiento de la seguridad Física para la seguridad informatica del HONADOMANI San Bartolomé.

En la realización de la investigación encontramos similitud con el antecedente de Karina del rocío Gaona Vásquez, en su tesis titulada "Aplicación de la metodología magerit para el análisis y gestión de riesgos de la seguridad de la información aplicado a la empresa pesquera e industrial bravito s.a. en la ciudad de Machala" En donde menciona como conclusión lo siguiente :Los resultados señalan que con la aplicación de la herramienta de gestión de riesgos MAGERI, se calcula el nivel de cumplimiento de la seguridad informatica forma efectiva, en la cual se obtuvo un nivel de cumplimiento de los distintos tipos de seguridad.

Y en nuestra investigación aumento el nivel de cumplimiento de la seguridad física en un 13.25%

3) En el nivel de cumplimiento de la seguridad de redes para la seguridad informatica en el HONADOMANI San Bartolomé, en la medición del Pre-Test, alcanzó los 62.33% de porcentaje y con la aplicación de la herramienta de gestión de riesgos alcanzo un 85.00%.

   Los resultados obtenidos indican que aumento en un 22.67% el nivel de cumplimiento de la seguridad de redes para la seguridad informatica del HONADOMANI San Bartolomé.

   En la realización de la investigación encontramos similitud con el antecedente de Karina del rocío Gaona Vásquez, en su tesis titulada "Aplicación de la metodología magerit para el análisis y gestión de riesgos de la seguridad de la información aplicado a la empresa pesquera e industrial bravito s.a. en la ciudad de Machala" En donde menciona como conclusión lo siguiente :Los resultados señalan que con la aplicación de la herramienta de gestión de riesgos MAGERI, se calcula el nivel de cumplimiento de la seguridad informatica forma efectiva, en la cual se obtuvo un nivel de cumplimiento de los distintos tipos de seguridad.

   Y en nuestra investigación aumento el nivel de cumplimiento de la seguridad de redes en un 22.67%

IV. CONCLUSION

Como conclusión llegamos a lo siguiente:

1) En el nivel de cumplimiento de la seguridad lógica para la seguridad informatica en el HONADOMANI San Bartolomé, en la medición del Pre-Test, alcanzó los 42.50% de porcentaje y con la aplicación de la herramienta de gestión de riesgos alcanzo un 74.17%.

   Los resultados obtenidos indican que aumento en un 31.67% el nivel de cumplimiento de la seguridad lógica para la seguridad informatica del HONADOMANI San Bartolomé..

2) En el nivel de cumplimiento de la seguridad Física para la seguridad informatica en el HONADOMANI San Bartolomé, en la medición del Pre-Test, alcanzó los 71.25% de porcentaje y con la aplicación de la herramienta de gestión de riesgos alcanzo un 84.50%.

   Los resultados obtenidos indican que aumento en un 13.25% el nivel de cumplimiento de la seguridad Física para la seguridad informatica del HONADOMANI San Bartolomé.

3) En el nivel de cumplimiento de la seguridad de redes para la seguridad informatica en el HONADOMANI San Bartolomé, en la medición del Pre-Test, alcanzó los 62.33% de porcentaje y con la aplicación de la herramienta de gestión de riesgos alcanzo un 85.00%.

   Los resultados obtenidos indican que aumento en un 22.67% el nivel de cumplimiento de la seguridad de redes para la seguridad informatica del HONADOMANI San Bartolomé.

4) Finalmente después de haber obtenido resultados satisfactorios de los indicadores del estudio, se concluye que la Herramienta de gestión de riesgos mejora el proceso para la seguridad Informática del HONADOMANI San Bartolomé.

V. RECOMENDACIONES

A continuación se menciona las recomendaciones para futuras investigaciones.

- Se recomienda investigar respecto al tema de investigación, en otras empresas, para tener una mejor visión de cómo se maneja en otras empresas.

- Respecto a la seguridad informatica, se recomienda investigar las distintas problemáticas que tienen las empresas para este proceso, y que es lo que requieren para poder solucionarlo.

- Se recomienda mantener un seguimiento de cómo se está utilizando las salvaguardas de la gestión de riesgos, para de alguna manera mejorarlo cada cierto tiempo.

- Se recomienda buscar varios antecedente, para tener una mejor visión de que es lo que se quiere hacer y como lo toman otros autores.

REFERENCIAS

1. Barrantes y Hugo, Diseño e implementación de un sistema de gestión de seguridad de información en procesos tecnológicos, Perú, Lima, 2012. 10 p. ISBN: 568-78-674235-1-5

2. BERNAL, Cesar. Metodología de investigación científica. 2a. ed. México, Editorial cáliz, 2011. 50 p. ISBN: 1-569874-156

3. Bustamante, Seguridad en redes, 1ra Ed, Colombia, Bogotá 2012 40 p. ISBN: 436782657-0

4. Bustamante, Seguridad en redes, 1ra Ed, Colombia, Bogotá 2012 45 p. ISBN: 436782657-0

5. Bustamante, Seguridad en redes, 1ra Ed, Colombia, Bogotá 2012 48p. ISBN: 436782657-0

6. Camilo Gutiérrez Amaya, Herramientas de gestión de riesgos de información, 2012. 15 p. ISBN: 178952354-1

7. Cisco Networking Academy, principios y guías de Seguridad de Información. 3ra. Ed. EE.UU., Manhattan, 2016. 48 p

8. Cisco Networking Academy, principios y guías de Seguridad de información. 3ra. Ed. EE.UU., Manhattan, 2016. 48 p.

9. Cisco Networking Academy, principios y guías de Seguridad de información. 3ra. Ed. EE.UU., Manhattan, 2016. 51 p.

10. Cisco Networking Academy, principios y guías de Seguridad de información. 3ra. Ed. EE.UU., Manhattan, 2016. 54 p.

11. Cisco Networking Academy, principios y guías de Seguridad de información. 3ra. Ed. EE.UU., Manhattan, 2016. 55 p.

12. Cisco Networking Academy, principios y guías de Seguridad de información. 3ra. Ed. EE.UU., Manhattan, 2016. 56p.

13. Colette, Cesar, Seguridad en redes, México, Monterrey, 2011. 17 p.

14. Colette, Cesar, Seguridad en redes, México, Monterrey, 2011 18 p.

15. Colette, Cesar, Seguridad en redes, México, Monterrey, 2011 19 p.
16. Duque Ocho0a Blanca, Herramienta de gestión de riesgos para la seguridad informatica, 2013. 19 p. ISBN: 121124569-2

17. Ewelina, Mikaela, Risk managment practices in a construction project – a case study, Suecia, 2011 15 p, ISBN: 785623589-1

18. Gabriel Sánchez Pérez, Herramientas de gestión de riesgos de SI, 2012. 20 p. ISBN: 486-23-145632-1-8

19. Gabriel Sánchez Pérez, Herramientas de gestión de riesgos de SI, 2012. 40 p. ISBN: 486-23-145632-1-8

20. Gabriel Sánchez Pérez, Herramientas de gestión de riesgos de SI, 2012. 60 p. ISBN: 486-23-145632-1-8

21. Gabriel Sánchez Pérez, Herramientas de gestión de riesgos de SI, 2012. 62 p. ISBN: 486-23-145632-1-8

22. Gabriel Sánchez Pérez, Herramientas de gestión de riesgos de SI, 2012. 63 p. ISBN: 486-23-145632-1-8

23. Gaona, K. Aplicación de la metodología magerit para el análisis y gestión de riesgos de la seguridad
24. de la información, Ecuador, Cuenca, 2013, 8 p. ISBN: 1-542369-742

25. GÓMEZ, Deck. Estadística aplicada a la investigación científica. 2a. ed. EE.UU., Petri, 2012. 80 p. ISBN: 1-542369-742

26. GÓMEZ, Deck. Estadística aplicada a la investigación científica. 2a. ed. EE.UU., Petri, 2012. 120 p. ISBN: 1-542369-742

27. GÓMEZ, Deck. Estadística aplicada a la investigación científica. 2a. ed. EE.UU., Petri, 2012. 128 p. ISBN: 1-542369-742

28. Huerta, Seguridad en Unix y redes, Ecuador, Quito 2012. 147 p.

29. Huerta, Seguridad en Unix y redes, Ecuador, Quito 2012. 150 p.

30. Huerta, Seguridad en Unix y redes, Ecuador, Quito 2012. 151 p.

31. ISACA, Information Systems Audit and Control Association. 2009. EE.UU, Illinois.

32. ISO/IEC 27001/2013, Sistema de Gestión de Seguridad de Información, 2013. 4ta. Ed. EE.UU

33. ISO/IEC 27005:2008, Metodología de gestión de riesgos, 2014, 8 p.

34. ISO/IEC 27005:2008, Metodología de gestión de riesgos, 2014, 20 p.

35. ISO/IEC 31000:2009, Secure Information Technologies, 2014. 15 p.

36. Lonita, Current established risk assessment methodologies and tools, Netherlands, Twente. 2013. 12 p. ISBN: 112-30-453689-1-0

37. NAMAKFOROOSH, Luis. Técnicas e instrumentos de recolección de datos en los estudios científicos aplicados. 2a. ed. México, Zacateda, 2012. 100 p. ISBN: 785623589-1

38. NAMAKFOROOSH, Luis. Técnicas e instrumentos de recolección de datos en los estudios científicos aplicados. 2a. ed. México, Zacateda, 2012. 120 p. ISBN: 785623589-1

39. Narváez, Iván, Aplicación de la norma ISO/IEC 27001 para la implementación de un SGSI, Ecuador, Quito, 2013. 9 p. ISBN: 123-78-100253-1-8

40. Magerit, Metodología de análisis y gestión de riesgos, EE.UU. 2012, p:19

41. ORTEGA, VEGA y ZEÑA. Análisis estadístico en estudios científicos. 3a. ed. México, Prateris, 2012. 21 p. ISBN: 563923588-1

42. ORTEGA, VEGA y ZEÑA. Análisis estadístico en estudios científicos. 3a. ed. México, Prateris, 2012. 52 p. ISBN: 563923588-1

43. Perafan Ruiz John. Seguridad Informatica de las tecnologías de Información, Ecuador, Popayán, 2014. 10 p. ISBN: 120234586-1

44. Senn, Ceres. Proyectos de inversión para su formulación y evaluación. 2ª. Ed. México, Santurce 2011. 80 p. ISBN: 1-875619-232

45. Senn, Ceres. Proyectos de inversión para su formulación y evaluación. 2ª. Ed. México, Santurce 2011. 19p. ISBN: 1-875619-232

ANEXOS

ANEXO – 01: MATRIZ DE CONSISTENCIA

PROBLEMAS	OBJETIVOS	HIPÓTESIS	OPERACIONALIZACIÓN DE VARIABLES				
			VARIABLE	CONCEPTO	DIMENSIONES	INDICADORES	METODOLOGÍA
GENERAL			**INDEPENDIENTE**				
PG: ¿De qué manera influye la herramienta de gestión de riesgos para la seguridad Informática en el Hospital Nacional Madre Niño San Bartolomé?	**OG:** Determinar la influencia de una herramienta de gestión de riesgos para la seguridad Informática en el Hospital Nacional Madre Niño San Bartolomé.	**HA:** La Herramienta de gestión de riesgos mejora la seguridad Informática en el Hospital Nacional Madre Niño San Bartolomé.	HERRAMIENTA DE GESTIÓN DE RIESGOS	La herramienta de gestión de riesgos permite identificar las vulnerabilidades de los activos de información y puede identificar cuales con las am que afecten a las vulnerabilidades. Permitiendo el análisis, diseño e implantación			**TIPO DE INVESTIGACIÓN** Aplicada-No Experimental Población : T1: 13 T1: 13 Muestra T1: 13 T2: 13 **DISEÑO DE LA INVESTIGACIÓN** Longitudinal – de tendencia **TÉCNICAS DE RECOLECCIÓN DE DATOS**
ESPECIFICO			**DEPENDIENTE**				
PE1: ¿En qué medida la herramienta de gestión de riesgos influye en la seguridad lógica del HONADOMANI San Bartolomé? **PE2: ¿En qué medida la herramienta de gestión de riesgos influye en la seguridad física del HONADOMANI San Bartolomé?**	**OE1: Determinar la influencia de una herramienta de gestión de riesgos en la seguridad lógica del HONADOMANI San Bartolomé.** **OE2: Determinar la influencia de una herramienta de gestión de riesgos en la seguridad física del HONADOMANI San Bartolomé.**	**HE1: La herramienta de gestión de riesgos ayuda significativamente en la seguridad informática del HONADOMANI San Bartolomé** **HE2: La herramienta de gestión de riesgos ayuda significativamente en la seguridad informática del HONADOMANI San Bartolomé**	LA SEGURIDAD INFORMATICA	La seguridad informatica permite análisis, diseño, implantación, monitoreo, mejora continua y optimización. También controla los niveles de seguridad de la información	Seguridad Lógica	$NCSL = 100\% - \frac{\Sigma(NCA)}{NA}$	

PE3: ¿En qué medida la herramienta de gestión de riesgos influye en la seguridad de redes del HONADOMANI San Bartolomé?	**OE3: Determinar la influencia de una herramienta de gestión de riesgos en la seguridad de redes el HONADOMANI San Bartolomé.**	**HE3: La herramienta de gestión de riesgos ayuda significativamente en la seguridad informática del HONADOMANI San Bartolomé**			Seguridad Física	$NCSL = 100\% - \frac{\Sigma(NCA)}{NA}$	- Entrevista - Observación **NSTRUMENTOS** - Ficha de registro
					Seguridad de redes	$NCSL = 100\% - \frac{\Sigma(NCA)}{NA}$	

ANEXO 02: ENTREVISTA

HOSPITAL NACIONAL DOCENTE MADRE NIÑO SAN BARTOLOMÉ

ENTREVISTA

ASUNTO: Recopilación de información **FECHA: 15/09/2016**

ENTREVISTADO: Ing. Spilco León Jardy

CARGO: Jefe del Área de Sistemas e Informatica

ENTREVISTADOR: Calderón Alvarado Jerson Joseph

1. ¿Qué es el área de Sistemas e Informatica?

ES UN ÁREA ESPECIALIZADO EN EL DISEÑO, IMPLEMENTACIÓN Y MANTENIMIENTO DE LOS ELEMENTOS QUE CONSTITUYEN LO QUE PODEMOS LLAMAR LA INFRAESTRUCTURA INFORMÁTICA DE LA EMPRESA.

2. ¿Cuáles son las funciones del Área de Sistemas e Informatica en el Hospital Nacional Docente Madre Niño San Bartolomé?

- DISEÑO, IMPLEMENTACIÓN Y ADMINISTRACIÓN DE REDES
- SELECCIÓN E INSTALACIÓN DE SISTEMAS DE INFORMACIÓN
- ADMINISTRACIÓN DE SISTEMAS
- MANTENIMIENTO DE APLICACIONES
- SOPORTE DE APLICACIONES
- OFIMÁTICA
- ELABORACIÓN DE INFORMES

3. ¿Actualmente cuenta con una Gestión de riesgos para la seguridad informática el Hospital Nacional Docente Madre Niño San Bartolomé? ¿Por qué?

NO, PORQUE NO HAY PERSONAL CAPACITADO PARA IMPLEMENTAR UNA HERRAMIENTA DE GESTIÓN DE RIESGOS DE SEGURIDAD DE INFORMACIÓN

HOSPITAL NACIONAL DOCENTE MADRE NIÑO SAN BARTOLOMÉ

4. ¿Cuáles son las incidencias que ocurren con frecuencia en el Hospital Nacional Docente Madre Niño San Bartolomé?

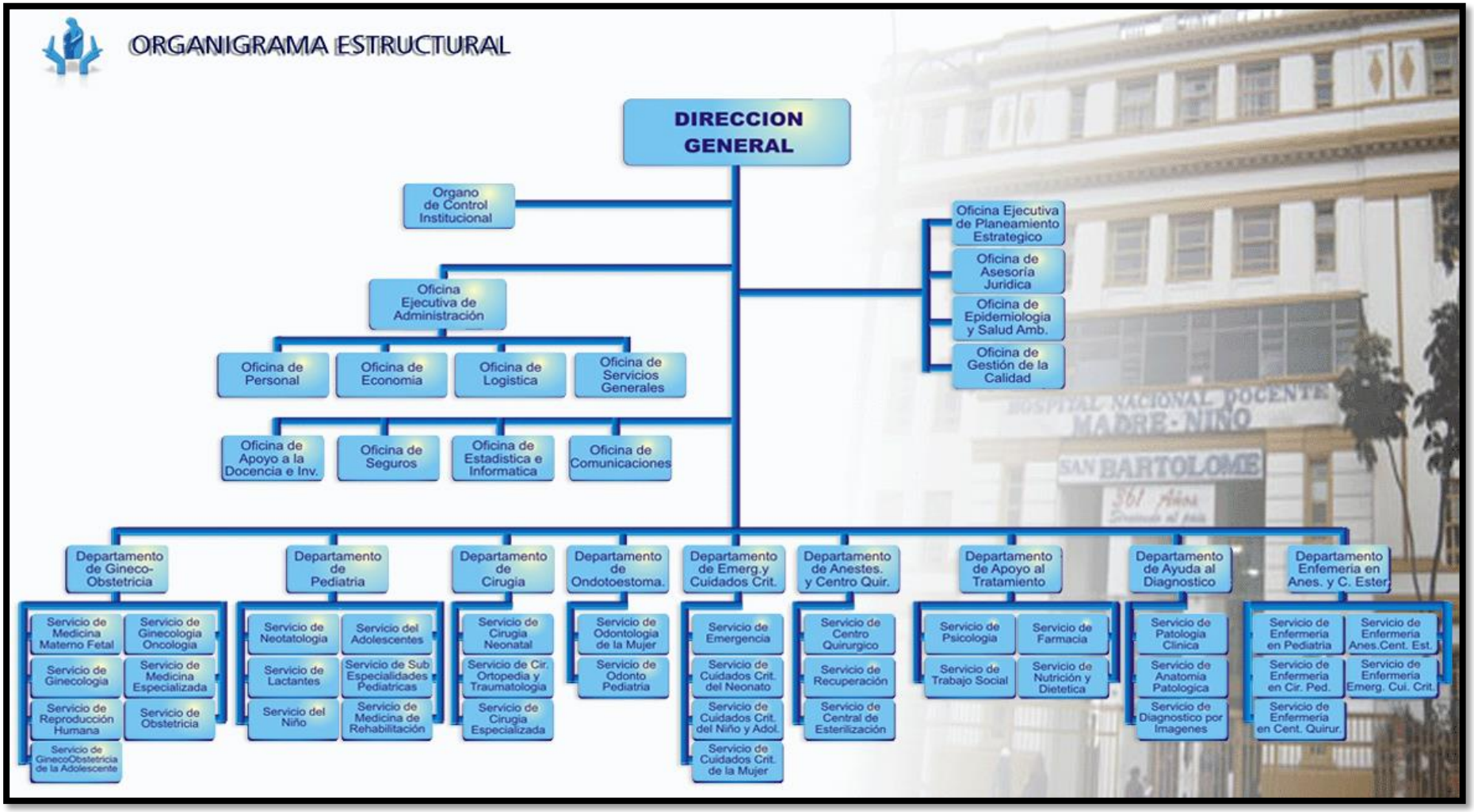
- CONGESTIONAMIENTO DE RED
- ROLES Y RESPONSABILIDADES DEL PERSONAL NO IDENTIFICADOS
- FALTA DE NORMAS Y POLITICAS DE SEGURIDAD
- NO HAY UNA ARQUITECTURA DE RED
- NO HAY DOCUMENTACION DE SCRIPT Y CONTRASEÑAS DE LA SALA DE SERVIDORES

5. ¿Considera que es necesario Implementar una Gestión de riesgos para la seguridad informática en el Hospital Nacional Docente Madre Niño San Bartolomé? ¿Por qué?

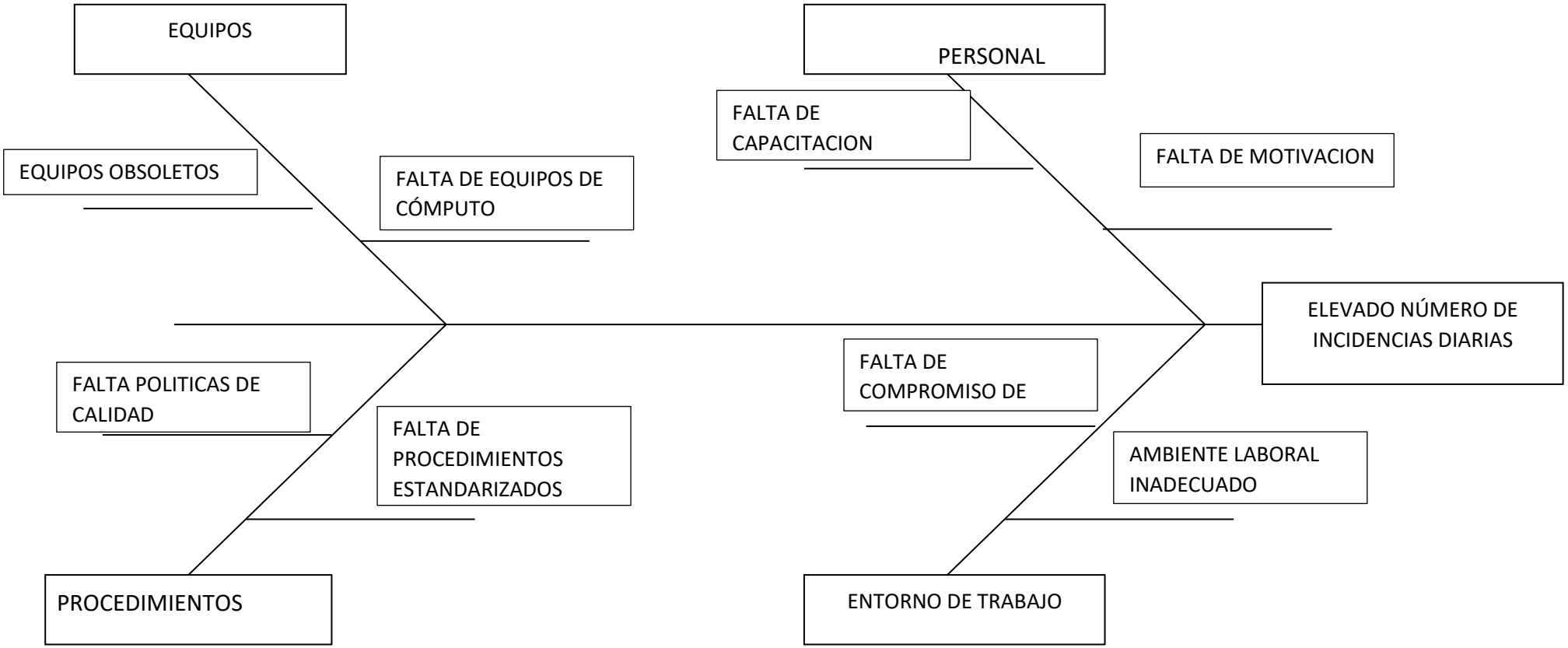
SI; PARA QUE NOS AYUDE A IDENTIFICAR LAS VULNERABILIDADES DE LOS ACTIVOS DE INFORMACION Y QUE POSIBILITE MINIMIZAR LAS INCIDENCIAS DIARIAS PARA PODER ALCANZAR LOS OBJETIVOS Y METAS DE LA ORGANIZACIÓN.

MINISTERIO DE SALUD
HONADOMANI"SAN BARTOLOME"
Ing. JARDY L. ESPILCO LEON
JEFE DE LA UNIDAD DE INFORMÁTICA Y S.
C.I.P. Nº 147.13

ANEXO 03: ORGANIGRAMA ESTRUCTURAL DEL HOSPITAL SAN BARTOLOMÉ



ANEXO 04: DIAGRAMA DE ISHIKAWA



ANEXO 05: PROYECTO DE INVESTIGACION

NOVENO CICLO

DECIMO CICLO

ANEXO 06: TABLA DE EVALUACIÓN DE EXPERTOS- EVALUACIÓN DE METODOLOGÍA DE DESARROLLO

TABLA DE EVALUACIÓN DE EXPERTOS

Apellidos y Nombres del Experto: Bravo Baldeón Percy

Título y/o Grado: Mgtr. Ing. Sistemas

Doctor... ( ) Magister... (X) Ingeniero... ( )

Universidad que labora: Universidad César Vallejo - Sede Lima Norte

Fecha: 06/10/2016

TÍTULO:
HERRAMIENTA DE GESTION DE RIESGOS PARA LA SEGURIDAD INFORMATICA DEL HONADOMANI SAN BARTOLOMÉ

Evaluación para la metodología de gestión de riesgos: MAGERIT"

Mediante la tabla de evaluación de expertos, usted tiene la facultad de calificar las metodologías involucradas, mediante una serie de criterios con puntuaciones especificadas al final de la tabla. Asimismo, le exhortamos en la corrección de los ítems indicando sus observaciones y/o sugerencias, con la finalidad de mejorar la coherencia de las preguntas.

		METODOLOGÍA			
ÍTEM	CRITERIO	MAGERIT	ISO/IEC 27005	ISO/IEC 31000	OBSERVACIONES
1	Metodología que ofrece un mejor método sistemático para analizar los riesgos de TI	3	2	2	
2	Metodología que ayuda a planificar mejor las medidas oportunas para mantener los riesgos bajo control	3	2	2	
3	Metodología que concientiza a la organización de la existencia del riesgo, que se puede presentar en cualquier momento y en cualquier área	3	2	1	
4	Metodología que utiliza modelos cualitativos y cuantitativos	3	2	2	
5	Metodología que implanta salvaguardas para los sistemas de información	3	3	2	
6	Metodología que prepara a la organización a procesos de evaluación, certificación y auditoria	3	2	2	
	TOTAL	18	13	11	

Evaluar con la siguiente puntuación:

1.- Malo 2.- Regular 3.- Bueno

Sugerencias:

FIRMA DEL EXPERTO

TABLA DE EVALUACIÓN DE EXPERTOS

Apellidos y Nombres del Experto: VERGARA CALDERON RODOLFO

Título y/o Grado:

Doctor... ( ) Magister... (X) Ingeniero... ( )

Universidad que labora: Universidad César Vallejo - Sede Lima Norte

Fecha: 06/10/2016

TÍTULO:
HERRAMIENTA DE GESTION DE RIESGOS PARA LA SEGURIDAD INFORMATICA DEL HONADOMANI SAN BARTOLOMÉ

Evaluación para la metodología de gestión de riesgos: MAGERIT"

Mediante la tabla de evaluación de expertos, usted tiene la facultad de calificar las metodologías involucradas, mediante una serie de criterios con puntuaciones especificadas al final de la tabla. Asimismo, le exhortamos en la corrección de los ítems indicando sus observaciones y/o sugerencias, con la finalidad de mejorar la coherencia de las preguntas.

		METODOLOGÍA			
ÍTEM	CRITERIO	MAGERIT	ISO/IEC 27005	ISO/IEC 31000	OBSERVACIONES
1	Metodología que ofrece un mejor método sistemático para analizar los riesgos de TI	3	2	2	
2	Metodología que ayuda a planificar mejor las medidas oportunas para mantener los riesgos bajo control	3	2	2	
3	Metodología que concientiza a la organización de la existencia del riesgo, que se puede presentar en cualquier momento y en cualquier área	3	2	1	
4	Metodología que utiliza modelos cualitativos y cuantitativos	3	2	1	
5	Metodología que implanta salvaguardas para los sistemas de información	3	2	2	
6	Metodología que prepara a la organización a procesos de evaluación, certificación y auditoria	3	2	1	
	TOTAL	18	12	9	

Evaluar con la siguiente puntuación:

1.- Malo 2.- Regular 3.- Bueno

Sugerencias:

FIRMA DEL EXPERTO

TABLA DE EVALUACIÓN DE EXPERTOS

Apellidos y Nombres del Experto: Pedro Gonzales

Título y/o Grado: Magister

Doctor... ( ) Magister... (✓) Ingeniero... ( )

Universidad que labora: Universidad César Vallejo - Sede Lima Norte

Fecha: 03/10/2016

TÍTULO:

HERRAMIENTA DE GESTION DE RIESGOS PARA LA SEGURIDAD INFORMATICA DEL HONADOMANI SAN BARTOLOMÉ

Evaluación para la metodología de gestión de riesgos: MAGERIT"

Mediante la tabla de evaluación de expertos, usted tiene la facultad de calificar las metodologías involucradas, mediante una serie de criterios con puntuaciones especificadas al final de la tabla. Asimismo, le exhortamos en la corrección de los ítems indicando sus observaciones y/o sugerencias, con la finalidad de mejorar la coherencia de las preguntas.

		METODOLOGÍA			
ÍTEM	CRITERIO	MAGERIT	ISO/IEC 27005	ISO/IEC 31000	OBSERVACIONES
1	Metodología que ofrece un mejor método sistemático para analizar los riesgos de TI	3	2	1	
2	Metodología que ayuda a planificar mejor las medidas oportunas para mantener los riesgos bajo control	2	2	1	
3	Metodología que concientiza a la organización de la existencia del riesgo, que se puede presentar en cualquier momento y en cualquier área	3	2	1	
4	Metodología que utiliza modelos cualitativos y cuantitativos	3	2	1	
5	Metodología que implanta salvaguardas para los sistemas de información	2	2	1	
6	Metodología que prepara a la organización a procesos de evaluación, certificación y auditoria	3	1	1	
	TOTAL	16	11	6	

Evaluar con la siguiente puntuación:

1.- Malo 2.- Regular 3.- Bueno

Sugerencias:

FIRMA DEL EXPERTO

ANEXO 07: FICHA DE REGISTRO

SEGURIDAD LOGICA - ANTES

Ficha de registro				
Investigador	Jerson Calderón Alvarado		Tipo de Prueba	Pre-test
Empresa investigada	Hospital San Bartolomé			
Motivo de investigación	Nivel de cumplimiento			
Fecha de Inicio	26/10/2016	Fecha Final		2/11/2016
Variable	Indicador	Medida	Formula	$NCSL = 100\% - \frac{\Sigma(NCA)}{NA}$
Seguridad lógica	Nivel de cumplimiento	Puntos		

ítem	Fecha inicio	Nivel de Cumplimiento de activos	Numero de activos	Nivel de Cumplimiento Antes
1	26/10/2016	450	5	10%
2	1/10/2016	450	5	10%
3	7/10/2016	200	5	60%
4	15/10/2016	200	5	60%
5	22/10/2016	75	5	85%
6	08/10/2016	350	5	30%

SEGURIDAD LOGICA - DESPUES

Investigador	Jerson Calderón Alvarado		Tipo de Prueba	Re-test
Empresa Investigada	Hospital San Bartolomé			
Motivo de investigación	Nivel de cumplimiento			
Fecha de Inicio	13/01/2017	Fecha Final		14/03/2017
Variable	Indicador	Medida	Formula	
Seguridad lógica	Nivel de cumplimiento	Puntos	$NCSL = 100\% - \frac{\Sigma(NCA)}{NA}$	
Ítem	Fecha Inicio	Nivel de Cumplimiento de activos	Numero de activos	Nivel de Cumplimiento Actual
1	13/01/2017	150	5	70%
2	30/12/2017	150	5	70%
3	27/01/2017	150	5	70%
4	13/02/2017	100	5	80%
5	20/02/2017	25	5	95%
6	03/03/2017	200	5	60%

SEGURIDAD FISICA – ANTES

Ficha de registro			
Investigador	Jerson Calderón Alvarado	Tipo de Prueba	Pre-test
Empresa Investigada	Hospital San Bartolomé		
Motivo de investigación	Nivel de cumplimiento		
Fecha de Inicio	26/10/2016	Fecha Final	2/11/2016
Variable	Indicador	Medida	Formula
Seguridad Física	Nivel de cumplimiento	Puntos	$\lvert NCSF = 100\% - \frac{\Sigma(NCA)}{NA} \rvert$

Ítem	Fecha Inicio	Nivel de Cumplimiento de activos	Numero de activos	Nivel de Cumplimiento Antes
7	1/10/2016	200	5	60%
8	15/10/2016	150	5	70%
9	2/11/2016	100	5	80%
10	2/11/2016	125	5	75%

SEGURIDAD FISICA – DESPUES

Ficha de registro						
Investigador	Jerson Calderón Alvarado		Tipo de Prueba		Post-test	
Empresa Investigada	Hospital San Bartolomé					
Motivo de investigación	Nivel de cumplimiento					
Fecha de Inicio	01/05/2017		Fecha Final		28/04/2017	
Variable	Indicador		Medida		Formula	
Seguridad Física	Nivel de cumplimiento		Puntos		$NCSF = 100\% - \frac{\Sigma(NCA)}{NA}$	
Ítem	Fecha Inicio	Nivel de Cumplimiento de activos			Numero de activos	Nivel de Cumplimiento Actual
7	01/05/2017	105			5	79%
8	06/04/2017	93			5	81%
9	17/03/2017	50			5	90%
10	20/04/2017	62			5	88%

SEGURIDAD DE REDES – ANTES

Ficha de registro			
Investigador	Jerson Calderón Alvarado	Tipo de Prueba	Pre-test
Empresa Investigada	Hospital San Bartolomé		
Motivo de investigación	Nivel de cumplimiento		
Fecha de Inicio	26/10/2016	Fecha Final	2/11/2016
Variable	Indicador	Medida	Formula
Seguridad de redes	Nivel de cumplimiento	Puntos	$NCSR = 100\% - \frac{\Sigma(NCA)}{NA}$

Ítem	Fecha Inicio	Nivel de Cumplimiento de activos	Numero de activos	Nivel de Cumplimiento Antes
11	7/10/2016	175	5	65%
12	15/10/2016	165	5	67%
13	22/10/2016	225	5	55%

SEGURIDAD DE REDES – DESPUES

Ficha de registro			
Investigador	Jerson Calderón Alvarado	Tipo de Prueba	Post-test
Empresa Investigada	Hospital San Bartolomé		
Motivo de investigación	Nivel de cumplimiento		
Fecha de Inicio	08/05/2017	Fecha Final	13/06/2017
Variable	Indicador	Medida	Formula
Seguridad de redes	Nivel de cumplimiento	Puntos	$NCSR = 100\% - \frac{\Sigma(NCA)}{NA}$

Ítem	Fecha Inicio	Nivel de Cumplimiento de activos	Numero de activos	Nivel de Cumplimiento Actual
11	08/05/2017	50	5	90%
12	02/06/2017	75	5	85%
13	22/05/2017	100	5	80%

ANEXO 09:

1° HERRAMIENTA DE GESTION DE RIESGOS “MAGERIT”

ANEXO 06: HERRAMIENTA DE GESTION DE RIESGOS "MAGERIT"

IDENTIFICACION DE LOS ACTIVOS

Se clasifica los activos de la seguridad informatica según las dimensiones que se han empleado en esta tesis, donde son: Seguridad Lógica, Seguridad Física y Seguridad de redes, estos activos están alineados a los 140 requerimientos que ofrece la ISO 27001.

Tabla N°1

TIPO	NOMBRE DE ACTIVO	
Seguridad Logica	[SL_CA]	Listas de control de acceso
	[SL_PC]	Registro de acceso a la red
	[SL_MA]	Modalidad de acceso
	[SL_LIU]	Limites sobre la interface de usuario
	[SL_RPC]	Renovacion de palabras claves
	[SL_BI]	Back-up de informacion
	[SL_AA]	Antivirus activo
Seguridad Física	[SF_SOA]	Sistemas operativos actualizados
	[SF_PNA]	Programas no autorizados
	[SF_IE]	Inventario de equipos
	[SF_PCE]	Mantenimiento preventivo y correctivo de equipos
	[SF_EG]	Equipos con garantía
	[SF_UCR]	Ubicación de cables de red
	[SF_GR]	Gabinetes de red
	[SF_SSS]	Situacion de la sala de servidores
	[SF_RI]	Vulnerabilidad de cables de red
Seguridad de redes	[SR_PAR]	Operatividad de la red
	[SR_DS]	Correos enviados
	[SR_OR]	Politicas y normas de seguridad
	[SR_CE]	Claves de los servidores
	[SR_PNS]	Mitigar riesgo de red

Tabla de incentivación de los activos

VALORACION DE LOS ACTIVOS

En la valoración de activos que nos brinda la metodología Magerit utilizaremos las dimensiones de seguridad para poder clasificarlas de una manera práctica, donde estas dimensiones se alinearan a cada activo a través de una entrevista al jefe del área de sistemas.

Tabla N°2

Dimensiones de seguridad	
[C]	Confidencialidad
[I]	Integridad
[D]	Disponibilidad
[A]	Autenticidad
[T]	Trazabilidad

Dimensiones de seguridad

Las dimensiones de seguridad se clasificaran mediante preguntas en donde tienen que tener relevancia con los activos de información

Figura N°1

Confidencialidad: ¿qué daño causaría que lo conociera quien no debe?
Integridad: ¿qué perjuicio causaría que estuviera dañado o corrupto?
Disponibilidad: ¿qué perjuicio causaría no tenerlo o no poder utilizarlo?
Autenticidad: ¿qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?
Trazabilidad: ¿quién hace qué y cuándo? Y ¿qué daño causaría no saber quién accede a qué datos y qué hace con ellos?

Definición de dimensiones de seguridad

La tabla de valoración que nos brinda la metodología Magerit nos ayuda a valorar al activo mediante 2 tipos, sea el valor o el criterio de como actué cada activo de información en la organización.

Tabla N°3

Tabla de valoración de activos			
Valor			Criterio
10	Muy alto	MA	Daño muy grave a la organización
7-9	Alto	A	Daño grave a la organización
4-6	Medio	M	Daño importante a la organización
1-3	Bajo	B	Daño menor a la organización
0	Despreciable	D	Irrelevante a efectos practicos

Valoración y criterios de activos

Se clasificara por separado la variable independiente Seguridad informatica, mediante las dimensiones que se están planteando en esta tesis.

A continuación se verá la valoración de los activos de la seguridad lógica según las dimensiones de seguridad

Tabla N°4

Valoracion de activos: Seguridad Lógica					
Activos	Dimensiones de Seguridad				
	[C]	[I]	[D]	[A]	[T]
Listas de control de acceso	M	M	M	A	A
Registro de acceso a la red	A	A	A	A	A
Modalidad de acceso	A	A	A	A	A
Limites sobre la interface de usuario	MA	MA	MA	MA	MA
Renovacion de palabras claves	MA	MA	MA	MA	MA
Back-up de informacion	A	A	A	A	A
Antivirus activo	A	A	A	A	A

Valoración de activos: Seguridad Lógica

Según la entrevista que se le realizo al jefe del área de sistemas Spilco León Jardy, se pudo definir la importancia y el daño que provocaría cada activo de información para nuestra dimensión SEGURIDAD LÓGICA.

1. Listas de control de acceso
    a) ¿Qué daño causaría que lo conociera quien no debe?
       MEDIO: Porque sería un daño importante a la organización
    b) ¿Qué perjuicio causaría que estuviera dañado o corrupto?
       MEDIO: Porque sería un daño importante a la organización
    c) ¿Qué perjuicio causaría no tenerlo o poder utilizarlo?
       MEDIO: Porque sería un daño importante a la organización
    d) ¿Qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?
       ALTO: Porque sería un daño grave a la organización
    e) ¿Qué daño causaría no sobre quien accede a que dato y que hace con ellos?
       ALTO: Porque sería un daño grave a la organización

2. Registro de acceso a la red
    a) ¿Qué daño causaría que lo conociera quien no debe?
       ALTO: Porque sería un daño grave a la organización
    b) ¿Qué perjuicio causaría que estuviera dañado o corrupto?
       ALTO: Porque sería un daño grave a la organización
    c) ¿Qué perjuicio causaría no tenerlo o poder utilizarlo?
       ALTO: Porque sería un daño grave a la organización
    d) ¿Qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?
       ALTO: Porque sería un daño grave a la organización
    e) ¿Qué daño causaría no sobre quien accede a que dato y que hace con ellos?
       ALTO: Porque sería un daño grave a la organización

3. Modalidad de acceso
    a) ¿Qué daño causaría que lo conociera quien no debe?
       ALTO: Porque sería un daño grave a la organización
    b) ¿Qué perjuicio causaría que estuviera dañado o corrupto?
       ALTO: Porque sería un daño grave a la organización
    c) ¿Qué perjuicio causaría no tenerlo o poder utilizarlo?
       ALTO: Porque sería un daño grave a la organización
    d) ¿Qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?
       ALTO: Porque sería un daño grave a la organización
    e) ¿Qué daño causaría no sobre quien accede a que dato y que hace con ellos?
       ALTO: Porque sería un daño grave a la organización

4. Limites sobre la interface de usuario
    a) ¿Qué daño causaría que lo conociera quien no debe?
       MUY ALTO: Porque sería un daño muy grave a la organización
    b) ¿Qué perjuicio causaría que estuviera dañado o corrupto?
       MUY ALTO: Porque sería un daño muy grave a la organización

c) ¿Qué perjuicio causaría no tenerlo o poder utilizarlo?
MUY ALTO: Porque sería un daño muy grave a la organización
d) ¿Qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?
MUY ALTO: Porque sería un daño muy grave a la organización
e) ¿Qué daño causaría no sobre quien accede a que dato y que hace con ellos?
MUY ALTO: Porque sería un daño muy grave a la organización

5. Renovación de palabras claves
a) ¿Qué daño causaría que lo conociera quien no debe?
MUY ALTO: Porque sería un daño muy grave a la organización
b) ¿Qué perjuicio causaría que estuviera dañado o corrupto?
MUY ALTO: Porque sería un daño muy grave a la organización
c) ¿Qué perjuicio causaría no tenerlo o poder utilizarlo?
MUY ALTO: Porque sería un daño muy grave a la organización
d) ¿Qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?
MUY ALTO: Porque sería un daño muy grave a la organización
e) ¿Qué daño causaría no sobre quien accede a que dato y que hace con ellos?
MUY ALTO: Porque sería un daño muy grave a la organización

6. Back – up de información
a) ¿Qué daño causaría que lo conociera quien no debe?
ALTO: Porque sería un daño grave a la organización
b) ¿Qué perjuicio causaría que estuviera dañado o corrupto?
ALTO: Porque sería un daño grave a la organización
c) ¿Qué perjuicio causaría no tenerlo o poder utilizarlo?
ALTO: Porque sería un daño grave a la organización
d) ¿Qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?
ALTO: Porque sería un daño grave a la organización

e) ¿Qué daño causaría no sobre quien accede a que dato y que hace con ellos?

ALTO: Porque sería un daño grave a la organización

7. Antivirus activo

a) ¿Qué daño causaría que lo conociera quien no debe?

ALTO: Porque sería un daño grave a la organización

b) ¿Qué perjuicio causaría que estuviera dañado o corrupto?

ALTO: Porque sería un daño grave a la organización

c) ¿Qué perjuicio causaría no tenerlo o poder utilizarlo?

ALTO: Porque sería un daño grave a la organización

d) ¿Qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?

ALTO: Porque sería un daño grave a la organización

e) ¿Qué daño causaría no sobre quien accede a que dato y que hace con ellos?

ALTO: Porque sería un daño grave a la organización

A continuación se verá la valoración de los activos de la seguridad física según las dimensiones de seguridad

Tabla N°5

Valoracion de activos: Seguridad Física					
Activos	Dimensiones de Seguridad				
	[C]	[I]	[D]	[A]	[T]
Sistemas operativos actualizados	M	M	M	MA	MA
Programas no autorizados	B	M	M	M	M
Inventario de equipos	A	A	A	A	A
Mantenimiento preventivo y correctivo de equipos	A	A	A	A	A
Equipos con garantía	A	A	A	A	A
Ubicación de cables de red	M	M	M	M	M
Gabinetes de red	A	A	A	A	A
Situacion de la sala de servidores	A	A	A	A	A
Vulnerabilidad de cables de red	A	A	A	A	A

Valoración de activos: Seguridad Física

Según la entrevista que se le realizo al jefe del área de sistemas Spilco León Jardy, se pudo definir la importancia y el daño que provocaría cada activo de información para nuestra dimensión SEGURIDAD FÍSICA.

1. ¿Sistemas operativos actualizados?
    a) ¿Qué daño causaría que lo conociera quien no debe?
    MEDIO: Porque sería un daño importante a la organización
    b) ¿Qué perjuicio causaría que estuviera dañado o corrupto?
    MEDIO: Porque sería un daño importante a la organización
    c) ¿Qué perjuicio causaría no tenerlo o poder utilizarlo?
    MEDIO: Porque sería un daño importante a la organización
    d) ¿Qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?
    MUY ALTO: Porque sería un daño muy grave a la organización
    e) ¿Qué daño causaría no sobre quien accede a que dato y que hace con ellos?
    MUY ALTO: Porque sería un daño muy grave a la organización
2. ¿Programas no autorizados?
    a) ¿Qué daño causaría que lo conociera quien no debe?
    BAJO: Porque sería un daño menor a la organización
    b) ¿Qué perjuicio causaría que estuviera dañado o corrupto?
    MEDIO: Porque sería un daño importante a la organización
    c) ¿Qué perjuicio causaría no tenerlo o poder utilizarlo?
    MEDIO: Porque sería un daño importante a la organización
    d) ¿Qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?
    MEDIO: Porque sería un daño importante a la organización
    e) ¿Qué daño causaría no sobre quien accede a que dato y que hace con ellos?
    MEDIO: Porque sería un daño importante a la organización

3. ¿Inventario de equipos?
    a) ¿Qué daño causaría que lo conociera quien no debe?
       ALTO: Porque sería un daño grave a la organización
    b) ¿Qué perjuicio causaría que estuviera dañado o corrupto?
       ALTO: Porque sería un daño grave a la organización
    c) ¿Qué perjuicio causaría no tenerlo o poder utilizarlo?
       ALTO: Porque sería un daño grave a la organización
    d) ¿Qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?
       ALTO: Porque sería un daño grave a la organización
    e) ¿Qué daño causaría no sobre quien accede a que dato y que hace con ellos?
       ALTO: Porque sería un daño grave a la organización

4. ¿Mantenimiento preventivo y correctivo de equipos?
    a) ¿Qué daño causaría que lo conociera quien no debe?
       ALTO: Porque sería un daño grave a la organización
    b) ¿Qué perjuicio causaría que estuviera dañado o corrupto?
       ALTO: Porque sería un daño grave a la organización
    c) ¿Qué perjuicio causaría no tenerlo o poder utilizarlo?
       ALTO: Porque sería un daño grave a la organización
    d) ¿Qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?
       ALTO: Porque sería un daño grave a la organización
    e) ¿Qué daño causaría no sobre quien accede a que dato y que hace con ellos?
       ALTO: Porque sería un daño grave a la organización

5. ¿Equipos con garantía?
    a) ¿Qué daño causaría que lo conociera quien no debe?
       ALTO: Porque sería un daño grave a la organización
    b) ¿Qué perjuicio causaría que estuviera dañado o corrupto?
       ALTO: Porque sería un daño grave a la organización

c) ¿Qué perjuicio causaría no tenerlo o poder utilizarlo?

ALTO: Porque sería un daño grave a la organización

d) ¿Qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?

ALTO: Porque sería un daño grave a la organización

e) ¿Qué daño causaría no sobre quien accede a que dato y que hace con ellos?

ALTO: Porque sería un daño grave a la organización

6. ¿Ubicación de cables de red?

a) ¿Qué daño causaría que lo conociera quien no debe?

MEDIO: Porque sería un daño importante a la organización

b) ¿Qué perjuicio causaría que estuviera dañado o corrupto?

MEDIO: Porque sería un daño importante a la organización

c) ¿Qué perjuicio causaría no tenerlo o poder utilizarlo?

MEDIO: Porque sería un daño importante a la organización

d) ¿Qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?

MEDIO: Porque sería un daño importante a la organización

e) ¿Qué daño causaría no sobre quien accede a que dato y que hace con ellos?

MEDIO: Porque sería un daño importante a la organización

7. ¿Gabinetes de red?

a) ¿Qué daño causaría que lo conociera quien no debe?

ALTO: Porque sería un daño grave a la organización

b) ¿Qué perjuicio causaría que estuviera dañado o corrupto?

ALTO: Porque sería un daño grave a la organización

c) ¿Qué perjuicio causaría no tenerlo o poder utilizarlo?

ALTO: Porque sería un daño grave a la organización

d) ¿Qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?

ALTO: Porque sería un daño grave a la organización

e) ¿Qué daño causaría no sobre quien accede a que dato y que hace con ellos?

ALTO: Porque sería un daño grave a la organización

8. ¿Situación de la sala de servidores?

a) ¿Qué daño causaría que lo conociera quien no debe?

ALTO: Porque sería un daño grave a la organización

b) ¿Qué perjuicio causaría que estuviera dañado o corrupto?

ALTO: Porque sería un daño grave a la organización

c) ¿Qué perjuicio causaría no tenerlo o poder utilizarlo?

ALTO: Porque sería un daño grave a la organización

d) ¿Qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?

ALTO: Porque sería un daño grave a la organización

e) ¿Qué daño causaría no sobre quien accede a que dato y que hace con ellos?

ALTO: Porque sería un daño grave a la organización

9. ¿Vulnerabilidad de cables de red?

a) ¿Qué daño causaría que lo conociera quien no debe?

ALTO: Porque sería un daño grave a la organización

b) ¿Qué perjuicio causaría que estuviera dañado o corrupto?

ALTO: Porque sería un daño grave a la organización

c) ¿Qué perjuicio causaría no tenerlo o poder utilizarlo?

ALTO: Porque sería un daño grave a la organización

d) ¿Qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?

ALTO: Porque sería un daño grave a la organización

e) ¿Qué daño causaría no sobre quien accede a que dato y que hace con ellos?

ALTO: Porque sería un daño grave a la organización

A continuación se verá la valoración de los activos de la seguridad de redes según las dimensiones de seguridad

Tabla N°6

Valoracion de activos: Seguridad de redes					
Activos	Dimensiones de Seguridad				
	[C]	[I]	[D]	[A]	[T]
Operatividad de la red	MA	MA	MA	MA	MA
Correos enviados	MA	MA	MA	MA	MA
Politicas y normas de seguridad	A	A	A	A	A
Claves de los servidores	A	A	A	A	A
Mitigar riesgo de red	A	A	A	A	A

Valoración de activos: Seguridad de redes

Según la entrevista que se le realizo al jefe del área de sistemas Spilco León Jardy, se pudo definir la importancia y el daño que provocaría cada activo de información para nuestra dimensión SEGURIDAD DE REDES.

1. ¿Operatividad de la red?
   a) ¿Qué daño causaría que lo conociera quien no debe?
      MUY ALTO: Porque sería un daño muy grave a la organización
   b) ¿Qué perjuicio causaría que estuviera dañado o corrupto?
      MUY ALTO: Porque sería un daño muy grave a la organización
   c) ¿Qué perjuicio causaría no tenerlo o poder utilizarlo?
      MUY ALTO: Porque sería un daño muy grave a la organización
   d) ¿Qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?
      MUY ALTO: Porque sería un daño muy grave a la organización
   e) ¿Qué daño causaría no sobre quien accede a que dato y que hace con ellos?
      MUY ALTO: Porque sería un daño muy grave a la organización

2. ¿Correos enviados?
    a) ¿Qué daño causaría que lo conociera quien no debe?
       MUY ALTO: Porque sería un daño muy grave a la organización
    b) ¿Qué perjuicio causaría que estuviera dañado o corrupto?
       MUY ALTO: Porque sería un daño muy grave a la organización
    c) ¿Qué perjuicio causaría no tenerlo o poder utilizarlo?
       MUY ALTO: Porque sería un daño muy grave a la organización
    d) ¿Qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?
       MUY ALTO: Porque sería un daño muy grave a la organización
    e) ¿Qué daño causaría no sobre quien accede a que dato y que hace con ellos?
       MUY ALTO: Porque sería un daño muy grave a la organización

3. ¿Políticas y normas de seguridad?
    a) ¿Qué daño causaría que lo conociera quien no debe?
       ALTO: Porque sería un daño grave a la organización
    b) ¿Qué perjuicio causaría que estuviera dañado o corrupto?
       ALTO: Porque sería un daño grave a la organización
    c) ¿Qué perjuicio causaría no tenerlo o poder utilizarlo?
       ALTO: Porque sería un daño grave a la organización
    d) ¿Qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?
       ALTO: Porque sería un daño grave a la organización
    e) ¿Qué daño causaría no sobre quien accede a que dato y que hace con ellos?
       ALTO: Porque sería un daño grave a la organización

4. ¿Claves de los servidores?

a) ¿Qué daño causaría que lo conociera quien no debe?

ALTO: Porque sería un daño grave a la organización

b) ¿Qué perjuicio causaría que estuviera dañado o corrupto?

ALTO: Porque sería un daño grave a la organización

c) ¿Qué perjuicio causaría no tenerlo o poder utilizarlo?

ALTO: Porque sería un daño grave a la organización

d) ¿Qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?

ALTO: Porque sería un daño grave a la organización

e) ¿Qué daño causaría no sobre quien accede a que dato y que hace con ellos?

ALTO: Porque sería un daño grave a la organización

5. ¿Mitigar riesgo de red?

a) ¿Qué daño causaría que lo conociera quien no debe?

ALTO: Porque sería un daño grave a la organización

b) ¿Qué perjuicio causaría que estuviera dañado o corrupto?

ALTO: Porque sería un daño grave a la organización

c) ¿Qué perjuicio causaría no tenerlo o poder utilizarlo?

ALTO: Porque sería un daño grave a la organización

d) ¿Qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?

ALTO: Porque sería un daño grave a la organización

e) ¿Qué daño causaría no sobre quien accede a que dato y que hace con ellos?

ALTO: Porque sería un daño grave a la organización

IDENTIFICACION Y VALORACION DE LAS AMENAZAS

La identificación de las amenazas es muy importante porque nos ayuda a clasificar el nivel de criterio con la cual se presenta y a su vez poder identificarlos mediantes valores.

Tabla N°7

Frecuencia de amenazas			
Valor			Criterio
100	Muy frecuente	MF	A diario
10	Frecuente	F	Mensualmente
1	Normal	FN	Una vez al año
1/10	Poco frecuente	PF	Cada varios años
1/100	Muy poco frecuente	B	Siglos

Frecuencia de amenazas

En la tabla N°7 se muestra el criterio de evaluación de una amenaza que nos brinda la metodología magerit donde nos permitirá el nivel de frecuencia con la cual se presenta la amenaza para proceder a degradarla y mantener a salvo el activo de información.

La degradación de las amenazas es muy importante porque nos ayuda a eliminar la amenaza e implementar mejoras para poder mantener bajo control las próximas amenazas que se presenten en la seguridad informatica.

Tabla N°8

Degradación de las amenazas	
Valor	Criterio
90% - 100%	Degradación muy considerable del activo
25% - 89%	Degradación medianamente considerable del activo
1% - 24%	Degradación poco considerable del activo

Degradación de las amenazas

En la figura N°8 se muestra en forma porcentual la degradación de la amenaza según el criterio que se quiera tener sobre ella.

En la figura N°9 se observa que se pudo identificar las amenazas que podrían sufrir los activos de información según la entrevista que se hizo al jefe del área de sistemas Spilco león Jardy, por lo tanto mediante la ayuda de la tabla N°7 Frecuencia de amenazas y Tabla N°8 Degradación de las amenazas, se pudo calcular la valoración de las amenazas en la seguridad Lógica

Tabla N°9

Identificación y valoración de Amenazas: Seguridad Lógica							
Amenaza	Frecuencia	Dimensiones de Seguridad					
		[C]	[I]	[D]	[A]	[T]	total
[A1]Mal control de usuarios	100	90%	90%	90%	90%	90%	90%
[A2] Mal control de acceso a la red	100	90%	90%	90%	90%	90%	90%
[A3]Error de acceso a la red	100	40%	40%	40%	40%	40%	40%
[A4]Error de privilegios de usuarios	100	40%	40%	40%	40%	40%	40%
[A5]Error de acceso a los usuarios	10	15%	15%	15%	15%	15%	15%
[A6] Perdida de informacion	10	60%	60%	60%	60%	60%	60%
[A7] Daño de informacion	10	70%	70%	70%	70%	70%	70%

Identificación y valoración de amenazas: Seguridad Lógica

Con que nivel de frecuencia se presentan amenazas en los activos de información. Según lo comentado por el ingeniero se redactara el nivel de frecuencia de las amenazas.

1) La amenaza A1 se presenta muy frecuencia con un valor de 100 afectando al activo listas de control de acceso diariamente
2) La amenaza A2 se presenta muy frecuencia con un de 100 afectando al activo registro de acceso a la red diariamente
3) La amenaza A3 se presenta muy frecuencia con un de 100 afectando al activo modalidad de acceso diariamente
4) La amenaza A4 se presenta muy frecuencia con un de 100 afectando al activo límites sobre la interface de usuario diariamente
5) La amenaza A5 se presenta frecuente con un valor de 10 afectando al activo renovación de palabras claves diariamente
6) La amenaza A6 se presenta frecuente con un valor de 10 afectando al activo back-up de información diariamente
7) La amenaza A7 se presenta frecuente con un valor de 10 afectando al activo antivirus activo diariamente

1. A1 Amenaza: Mal control de usuarios

a) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la confidencialidad del activo listas de control de acceso?
DEGRADACION MUY CONSIDERABLE DEL ACTIVO: 90%

b) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la integridad del activo listas de control de acceso?
DEGRADACION MUY CONSIDERABLE DEL ACTIVO: 90%

c) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la disponibilidad del activo listas de control de acceso?
DEGRADACION MUY CONSIDERABLE DEL ACTIVO: 90%

d) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la autenticidad del activo listas de control de acceso?
DEGRADACION MUY CONSIDERABLE DEL ACTIVO: 90%

e) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la trazabilidad del activo listas de control de acceso?
DEGRADACION MUY CONSIDERABLE DEL ACTIVO: 90%

2. A2 Amenaza: Mal control de acceso a la red

a) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la confidencialidad del activo registro de acceso a la red?
DEGRADACION MUY CONSIDERABLE DEL ACTIVO: 90%
b) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la integridad del activo registro de acceso a la red?
DEGRADACION MUY CONSIDERABLE DEL ACTIVO: 90%
c) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la disponibilidad del activo registro de acceso a la red?
DEGRADACION MUY CONSIDERABLE DEL ACTIVO: 90%
d) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la autenticidad del activo registro de acceso a la red?
DEGRADACION MUY CONSIDERABLE DEL ACTIVO: 90%
e) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la trazabilidad del activo registro de acceso a la red?
DEGRADACION MUY CONSIDERABLE DEL ACTIVO: 90%

3. A3 Amenaza: Error de acceso a la red

a) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la confidencialidad del activo modalidad de acceso?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 40%
b) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la integridad del activo modalidad de acceso?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 40%
c) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la disponibilidad del activo modalidad de acceso?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 40%

d) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la autenticidad del activo modalidad de acceso?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 40%

e) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la trazabilidad del activo modalidad de acceso?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 40%

4. A4 Amenaza: Error de privilegios de usuarios

a) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la confidencialidad del activo limites sobre la interface del usuario?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 40%

b) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la integridad del activo límites sobre la interface del usuario?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 40%

c) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la disponibilidad del activo límites sobre la interface del usuario?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 40%

d) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la autenticidad del activo límites sobre la interface del usuario?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 40%

e) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la trazabilidad del activo límites sobre la interface del usuario?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 40%

5. A5 Amenaza: Error de acceso a los usuarios

a) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la confidencialidad del activo renovación de palabras claves?
DEGRADACION POCO CONSIDERABLE DEL ACTIVO: 15%

b) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la integridad del activo renovación de palabras claves?
DEGRADACION POCO CONSIDERABLE DEL ACTIVO: 15%

c) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la disponibilidad del activo renovación de palabras claves?
DEGRADACION POCO CONSIDERABLE DEL ACTIVO: 15%

d) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la autenticidad del activo renovación de palabras claves?
DEGRADACION POCO CONSIDERABLE DEL ACTIVO: 15%

e) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la trazabilidad del activo renovación de palabras claves?
DEGRADACION POCO CONSIDERABLE DEL ACTIVO: 15%

6. A6 Amenaza: Perdida de información

a) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la confidencialidad del activo back-up de información?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 60%

b) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la integridad del activo back-up de información?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 60%

c) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la disponibilidad del activo back-up de información?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 60%

d) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la autenticidad del activo back-up de información?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 60%

e) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la trazabilidad del activo back-up de información?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 60%

6. A7 Amenaza: Daño de información

a) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la confidencialidad del activo antivirus activo?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 70%

b) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la integridad del activo antivirus activo?

DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 70%

c) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la disponibilidad del activo antivirus activo?

DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 70%

d) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la autenticidad del activo antivirus activo?

DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 70%

e) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la trazabilidad del activo antivirus activo?

DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 70%

la figura N°10 se observa que se pudo identificar las amenazas que podrían sufrir los activos de información, por lo tanto mediante la ayuda de la tabla N°7 Frecuencia de amenazas y Tabla N°8 Degradación de las amenazas, se pudo calcular la valoración de las amenazas en la seguridad Física

Tabla N°10

Identificación y valoración de Amenazas: Seguridad Física							
Amenaza	Frecuencia	Dimensiones de Seguridad					
		[C]	[I]	[D]	[A]	[T]	
[A8]Conflictos de programas	100	60%	60%	60%	60%	60%	60%
[A9] Infeccion de virus en el equipo	10	40%	40%	40%	40%	40%	40%
[A10]Mal control de equipos	10	30%	30%	30%	30%	30%	30%
[A11] Perdida de equipos informaticos	10	30%	30%	30%	30%	30%	30%
[A12]Escaces de equipos en garantia	10	45%	45%	45%	45%	45%	45%
[A13] Identificacion de puntos criticos	100	30%	30%	30%	30%	30%	30%
[A14] Mal control de puertos de red	10	20%	20%	20%	20%	20%	20%
[A15] Mal control de equipos intermedios	10	25%	25%	25%	25%	25%	25%
[A16] Robo de informacion	10	25%	25%	25%	25%	25%	25%

Identificación y valoración de amenazas: Seguridad Física

Con que nivel de frecuencia se presentan las amenazas en los activos de información.

Según lo comentado por el ingeniero se redactara el nivel de frecuencia de las amenazas.

8) La amenaza A8 se presenta muy frecuencia con un de 100 afectando al activo sistemas operativos actualizados diariamente
9) La amenaza A9 se presenta frecuencia con un de 10 afectando al activo inventario de equipos diariamente
10) La amenaza A10 se presenta frecuente con un valor de 10 afectando al activo mantenimiento preventivo y correctivo de equipos diariamente
11) La amenaza A11 se presenta frecuente con un valor de 10 afectando al activo equipos con garantía diariamente
12) La amenaza A12 se presenta frecuente con un valor de 10 afectando al activo programas no autorizados diariamente
13) La amenaza A13 se presenta muy frecuencia con un de 100 afectando al activo ubicación de los cables de red diariamente
14) La amenaza A14 se presenta frecuente con un valor de 10 afectando al activo gabinetes de red diariamente
15) La amenaza A13 se presenta frecuente con un valor de 10 afectando al activo situación de la sala de servidores diariamente
16) La amenaza A14 se presenta frecuente con un valor de 10 afectando al activo vulnerabilidad de cables de red diariamente

1. A8 Amenaza: Conflictos de programas

a) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la confidencialidad del activo sistemas operativos actualizados?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 60%

b) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la integridad del activo sistemas operativos actualizados?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 60%

c) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la disponibilidad del activo sistemas operativos actualizados?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 60%
d) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la autenticidad del activo sistemas operativos actualizados?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 60%
e) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la trazabilidad del activo sistemas operativos actualizados?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 60%

2. A9 Amenaza: Infección de virus en el equipo

a) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la confidencialidad del activo inventario de equipos?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 40%
b) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la integridad del activo inventario de equipos?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 40%
c) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la disponibilidad del activo inventario de equipos?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 40%
d) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la autenticidad del activo inventario de equipos?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 40%
e) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la trazabilidad del activo inventario de equipos?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 40%

3. A10 Amenaza: Mal control de equipos

a) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la confidencialidad del activo mantenimiento preventivo y correctivo de equipos?

DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 30%

b) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la integridad del activo mantenimiento preventivo y correctivo de equipos?

DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 30%

c) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la disponibilidad del activo mantenimiento preventivo y correctivo de equipos?

DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 30%

d) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la autenticidad del activo mantenimiento preventivo y correctivo de equipos?

DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 30%

e) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la trazabilidad del activo mantenimiento preventivo y correctivo de equipos?

DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 30%

4. A11 Amenaza: Perdida de equipos informáticos

a) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la confidencialidad del activo equipos con garantía?

DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 30%

b) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la integridad del activo equipos con garantía?

DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 30%

c) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la disponibilidad del activo equipos con garantía?

DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 30%

d) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la autenticidad del activo equipos con garantía?

DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 30%

e) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la trazabilidad del activo equipos con garantía?

DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 30%

5. A12 Amenaza: Escases de equipos en garantía

a) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la confidencialidad del activo programas no autorizados?

DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 45%

b) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la integridad del activo programas no autorizados?

DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 45%

c) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la disponibilidad del activo programas no autorizados?

DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 45%

d) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la autenticidad del activo programas no autorizados?

DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 45%

e) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la trazabilidad del activo programas no autorizados?

DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 45%

6. A13 Amenaza: Identificación de puntos críticos

a) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la confidencialidad del activo ubicación de los cables de red?

DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 30%

b) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la integridad del activo ubicación de los cables de red?

DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 30%

c) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la disponibilidad del activo ubicación de los cables de red?

DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 30%

d) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la autenticidad del activo ubicación de los cables de red?

DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 30%

e) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la trazabilidad del activo ubicación de los cables de red?

DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 30%

7. A14 Amenaza: Mal control de puertos de red

a) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la confidencialidad del activo gabinetes de red?

DEGRADACION POCO CONSIDERABLE DEL ACTIVO: 20%

b) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la integridad del activo gabinetes de red?

DEGRADACION POCO CONSIDERABLE DEL ACTIVO: 20%

c) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la disponibilidad del activo gabinetes de red?

DEGRADACION POCO CONSIDERABLE DEL ACTIVO: 20%

d) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la autenticidad del activo gabinetes de red?

DEGRADACION POCO CONSIDERABLE DEL ACTIVO: 20%

e) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la trazabilidad del activo gabinetes de red?

DEGRADACION POCO CONSIDERABLE DEL ACTIVO: 20%

8. A15 Amenaza: Mal control de equipos intermedios

a) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la confidencialidad del activo situación de la sala de servidores?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 25%
b) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la integridad del activo situación de la sala de servidores?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 25%
c) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la disponibilidad del activo situación de la sala de servidores?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 25%
d) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la autenticidad del activo situación de la sala de servidores?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 25%
e) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la trazabilidad del activo situación de la sala de servidores?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 25%

9. A16 Amenaza: Robo de información

a) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la confidencialidad del activo vulnerabilidad de cables de red?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 25%
b) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la integridad del activo vulnerabilidad de cables de red?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 25%
c) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la disponibilidad del activo vulnerabilidad de cables de red?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 25%
d) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la autenticidad del activo vulnerabilidad de cables de red?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 25%

e) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la trazabilidad del activo vulnerabilidad de cables de red?

DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 20%

En la figura N°11 se observa que se pudo identificar las amenazas que podrían sufrir los activos de información, por lo tanto mediante la ayuda de la tabla N°7 Frecuencia de amenazas y Tabla N°8 Degradación de las amenazas, se pudo calcular la valoración de las amenazas en la seguridad de redes

Tabla N°11

Identificación y valoración de Amenazas: Seguridad de redes							TOTAL
Amenaza	Frecuencia	Dimensiones de Seguridad					
		[C]	[I]	[D]	[A]	[T]	
[A17]Caida de la red	10	60%	60%	60%	60%	60%	60%
[A18] Correos perdidos	100	50%	50%	50%	50%	50%	50%
[A19] Mal control de la red y acceso de los usuarios	100	25%	25%	25%	25%	25%	25%
[A20] Olvido y confusion de las claves de los	10	33%	33%	33%	33%	33%	33%
[A21]No saber mitigar el riesgo de la falla de la red	10	45%	45%	45%	45%	45%	45%

Identificación y valoración de amenazas: Seguridad de redes

Con que nivel de frecuencia se presentan las amenazas en los activos de información.

Según lo comentado por el ingeniero se redactara el nivel de frecuencia de las amenazas.

1. La amenaza A17 se presenta frecuencia con un valor de 10 afectando al activo políticas y normas de seguridad diariamente
2. La amenaza A18 se presenta muy frecuencia con un de 100 afectando al activo claves de servidores diariamente
3. La amenaza A19 se presenta muy frecuencia con un de 100 al activo operatividad de la red diariamente
4. La amenaza A20 se presenta frecuente con un valor de 10 afectando al activo correos enviados diariamente
5. La amenaza A21 se presenta frecuente con un valor de 10 afectando al activo mitigar riesgos de red diariamente

1. A17 Amenaza: Caída de red

a) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la confidencialidad del activo operatividad de la red?
DEGRADACION MUY CONSIDERABLE DEL ACTIVO: 60%
b) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la integridad del activo operatividad de la red?
DEGRADACION MUY CONSIDERABLE DEL ACTIVO: 60%
c) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la disponibilidad del activo operatividad de la red?
DEGRADACION MUY CONSIDERABLE DEL ACTIVO: 60%
d) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la autenticidad del activo operatividad de la red?
DEGRADACION MUY CONSIDERABLE DEL ACTIVO: 60%
e) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la trazabilidad del activo operatividad de la red?
DEGRADACION MUY CONSIDERABLE DEL ACTIVO: 60%

2. A18 Amenaza: Correos perdidos

a) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la confidencialidad del activo correos enviados?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 50%
b) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la integridad del activo correos enviados?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 50%
c) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la disponibilidad del activo correos enviados?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 50%
d) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la autenticidad del activo correos enviados?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 50%

e) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la trazabilidad del activo correos enviados?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 50%

3. A19 Amenaza: Mal control de la red y acceso de los usuarios

a) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la confidencialidad del activo políticas y normas de seguridad?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 25%
b) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la integridad del activo políticas y normas de seguridad?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 25%
c) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la disponibilidad del activo políticas y normas de seguridad?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 25%
d) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la autenticidad del activo políticas y normas de seguridad?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 25%
e) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la trazabilidad del activo políticas y normas de seguridad?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 25%

4. A20 Amenaza: Olvido y confusión de las claves en los servidores

a) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la confidencialidad del activo claves de los servidores?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 33%
b) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la integridad del activo claves de los servidores?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 33%
c) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la disponibilidad del activo claves de los servidores?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 33%

d) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la autenticidad del activo claves de los servidores?

DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 33%

e) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la trazabilidad del activo claves de los servidores?

DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 33%

5. A21 Amenaza: No saber mitigar el riesgo de la falla de la red

a) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la confidencialidad del activo mitigar riesgos de red?

DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 45%

b) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la integridad del activo mitigar riesgos de red?

DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 45%

c) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la disponibilidad del activo mitigar riesgos de red?

DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 45%

d) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la autenticidad del activo mitigar riesgos de red?

DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 45%

e) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la trazabilidad del activo mitigar riesgos de red?

DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 45%

A CONTINUACIÓN SE MOSTRARÁ EL ESTADO ACTUAL DE LA SEGURIDAD INFORMATICA SEGÚN LA METODOLOGÍA MAGERIT

SEGURIDAD LOGICA

Tabla N°12

	REQUERIMIENTO	ACTIVOS	Porcentaje de cumplimiento actual	Porcentaje por cada indicador
Seguridad Lógica	Control de acceso	Listas de control de acceso	10%	27%
		Registro de acceso a la red	10%	
		Modalidad de acceso	60%	
	Control de acceso interno	Limites sobre la interface de usuario	60%	54%
		Renovacion de palabras claves	85%	
		Back-up de informacion	40%	
		Antivirus activo	30%	
	Porcentaje total de cumplimiento actual		36.11%	

Situación actual de la Seguridad Lógica

En la Tabla N°12 se muestra el porcentaje de cumplimiento actual, donde es la diferencia del 100 % con la amenaza actual del activo, además se calcula el porcentaje de cumplimiento actual por cada indicador.

SEGURIDAD FISICA

Tabla N°13

	REQUERIMIENTO	ACTIVOS	Porcentaje de cumplimiento actual	Porcentaje por cada indicador
Seguridad Física	Funcionamiento de equipos	Sistemas operativos actualizados	40%	60%
		Inventario de equipos	60%	
		Mantenimiento preventivo y correctivo de	70%	
		Equipos con garantía	70%	
	Seguridad de equipos	Programas no autorizados	55%	71%
		Ubicación de cables de red	70%	
		Gabinetes de red	80%	
		Situacion de la sala de servidores	75%	
		Vulnerabilidad de cables de red	75%	
	Porcentaje total de cumplimiento actual		66.11%	

Situación actual de la Seguridad Física

En la Tabla N°13 se muestra el porcentaje de cumplimiento actual, donde es la diferencia del 100 % con la amenaza actual del activo, además se calcula el porcentaje de cumplimiento actual por cada indicador.

SEGURIDAD DE REDES

Tabla N°14

	REQUERIMIENTO	ACTIVOS	Porcentaje de cumplimiento actual	Porcentaje por cada indicador
Seguridad de redes	Niveles de seguridad	Politicas y normas de seguridad	40%	45%
		Claves de los servidores	50%	
	Amenazas	Operatividad de la red	65%	62%
		Correos enviados	67%	
		Mitigar riesgo de red	55%	
	Porcentaje total de cumplimiento actual		55.40%	

Situación actual de la Seguridad de redes

En la Tabla N°14 se muestra el porcentaje de cumplimiento actual, donde es la diferencia del 100 % con la amenaza actual del activo, además se calcula el porcentaje de cumplimiento actual por cada indicador.

IDENTIFICACION Y VALORACION DE LAS SALVAGUARDAS

La identificar de las salvaguardas nos ayuda a poder mitigar los riegos que provocarían las amenazas, donde se identificara mediante el estado y el nivel de eficacia.

Tabla N°15

Eficacia	Nivel	Madurez	Estado
0%	L0	Inexistente	Inexistente
10%	L1	Inicial	Iniciado
50%	L2	Reproducible, pero intuitivo	Parcialmente realizado
90%	L3	Proceso definido	En funcionamiento
95%	L4	Gestionado y medible	Monitorizado
100%	L5	Optimizado	Mejora continua

Cuadro del nivel de madurez y estado de las salvaguardas

En la tabla N°16 se pudo identificar la expectativa del nivel de eficacia que ofrecería la salvaguarda, para depurar cada amenaza que vulnere cada activo de información en la seguridad informatica, teniendo en cuenta las 3 dimensiones: Seguridad

Lógica, Seguridad Física y Seguridad de redes. La expectativa es valorada por el investigador luego que el investigado haya valorado la frecuencia de la amenaza.

Tabla N°16

Dimensión	Amenaza	Salvaguarda	Nivel	Eficacia
Seguridad Lógica	[A1]Mal control de usuarios	Establacer una lista de usuarios con acceso a la red	L1	10%
	[A2] Mal control de acceso a la red	Establacer una lista de cuentas activas	L1	10%
	[A3]Error de acceso a la red	Establecer politicas y administracion de contraseña	L2	60%
	[A4]Error de privilegios de usuarios	Realizar grupos de acceso a internet	L2	60%
	[A5]Error de acceso a los usuarios	Establecer una guia para que el usuario selecciones y realice el mantenimiento de	L2	85%
	[A6] Perdida de informacion	Crear y probar regularmente los respaldos de informacion de acuerdo a las politicas	L1	40%
	[A7] Daño de informacion	Desarrollar e implementar directrices y controles para la deteccion, prevencion y tratamiento de	L1	30%
Seguridad Física	[A8]Conflictos de programas	Establecer una Actualizacion automatica de los sistemas operativos	L1	40%
	[A9] Infeccion de virus en el equipo	Implementar controles de seguridad para la instlacion de cualquier software en un equipo	L2	60%
	[A10]Mal control de equipos	Implementar un procedimiento formal para inventariar los equipos informaticos a todas las	L2	70%
	[A11] Perdida de equipos informaticos	Desarrollar e implementar controles para el mantenimiento preventivo de los equipos	L2	70%
	[A12]Escaces de equipos en garantia	Implementar un procedimiento formal para verificar que equipos estan en garantia	L2	55%
	[A13] Identificacion de puntos criticos	Ordenamiento de cableado estructurado	L2	70%
	[A14] Mal control de puertos de red	Ordenamiento de los gabinetes de red	L2	80%
	[A15] Mal control de equipos intermedios	Implementar un libro de control de acceso	L2	75%
	[A16] Robo de informacion	Bloqueo de puertos de red	L2	75%
Seguridad en redes	[A17]Caida de la red	Implementacion de vlan	L1	40%
	[A18] Correos perdidos	Implementar medidas de respaldo en el servidor de correo para que genere automaticamente	L2	50%
	[A19] Mal control de la red y acceso de los	Implementar el plan de politicas y normas de	L2	65%
	[A20] Olvido y confusion de las claves de los servidores	Implementar un procedimiento de resguardo de sobres sellados	L2	67%
	[A21]No saber mitigar el riesgo de la falla de la red	Implementacion de documentos por cada servidor de procedimiento de fallas	L2	55%

Identificación y valoración de las salvaguardas

RIESGO ACUMULADO

El riesgo acumulado se identifica sin la salvaguarda, para poder tener un antes de cada activo de información afectado por la amenaza. En la siguiente tabla N°17 se identificará la determinación del impacto y riesgo acumulado de las 3 dimensiones: Seguridad Lógica, Seguridad Física y Seguridad de redes, sin la implementación de la salvaguarda y la expectativa se calcula según el investigador.

Tabla N°17

Determinacion del impacto y riesgo acumulado										
Activos	Impacto Potencial Acumulado					Riesgo Acumulado				
	[C]	[I]	[D]	[A]	[T]	[C]	[I]	[D]	[A]	[T]
Listas de control de acceso	M	M	MA	MA	MA	A	A	MA	MA	MA
Registro de acceso a la red	M	MA	MA	MA	MA	A	MA	MA	MA	MA
Modalidad de acceso	M	MA	MA	MA	MA	A	MA	MA	MA	MA
Limites sobre la interface de usuario	M	A	A	A	A	A	MA	MA	MA	MA
Renovacion de palabras claves	M	M	M	M	M	M	M	M	M	M
Back-up de informacion	M	M	M	M	M	A	A	A	A	A
Antivirus activo	M	M	M	M	M	A	A	A	A	A
Sistemas operativos actualizados	M	M	B	B	M	A	A	B	A	B
Programas no autorizados	A	A	M	A	A	A	A	A	MA	MA
Inventario de equipos	M	M	A	M	M	MA	A	A	A	A
Mantenimiento preventivo y correctivo de equipos	M	M	M	A	M	A	A	A	A	A
Equipos con garantía	A	A	A	A	M	A	A	A	A	A
Ubicación de cables de red	A	A	A	A	A	A	A	A	A	A
Gabinetes de red	M	A	A	M	M	A	A	A	A	A
Situacion de la sala de servidores	M	M	M	M	M	M	M	M	M	M
Vulnerabilidad de cables de red	B	A	B	A	B	MA	MA	MA	MA	MA
Operatividad de la red	A	A	A	A	A	MA	MA	MA	MA	MA
Correos enviados	A	A	A	A	A	MA	MA	MA	MA	MA
Politicas y normas de seguridad	M	M	M	A	M	A	A	A	A	A
Claves de los servidores	M	A	M	M	M	A	A	A	A	A
Mitigar riesgo de red	A	M	A	M	M	A	A	A	A	A

Determinación del impacto y riesgo acumulado

RIESGO RESIDUAL

El riesgo acumulado se identifica con la nueva salvaguarda implementada, para poder tener un después de cada activo de información con la amenaza mitigada. La tabla de estimación del impacto nos ayudara a poder identificar el porcentaje de degradación de la amenaza con la salvaguarda implementada.

Tabla N°18

Tabla de estimación del impacto				
Impacto		Degradación		
		0% - 24%	25% - 89%	90% - 100%
Valor	(9-10)	M	A	MA
	(7-8)	M	A	A
	(4-6)	B	M	MA
	(2-3)	MB	B	B
	(0-1)	MB	MB	MB

Tabla de estimación del impacto

La tabla de estimación de riesgo nos ayudara a relacionar el nivel de frecuencia y el impacto para poder estimar el riesgo.

Tabla N°19

Tabla de estimacion del riesgo					
Riesgo		Degradación			
		PF	FN	F	MF
Impacto	MA	M	A	MA	MA
	A	B	A	MA	MA
	M	B	M	A	A
	B	MB	B	MA	A
	MB	MB	MB	B	B

Tabla de estimación del riesgo

En la tabla N°20 se muestra la determinación del impacto y riesgo residual con la salvaguarda implementada por cada activo de información, donde se va a mitigar el riesgo en un porcentaje considerable y poder seguir mejorando la salvaguarda implementada. La expectativa es según el investigador y la aprobación del investigado.

Tabla N°20

Determinacion del impacto y riesgo residual										
Activos	Impacto residual					Riesgo residual				
	[C]	[I]	[D]	[A]	[T]	[C]	[I]	[D]	[A]	[T]
Listas de control de acceso	B	B	MA	MA	MA	A	A	MA	MA	MA
Registro de acceso a la red	B	MA	MA	MA	MA	A	MA	MA	MA	MA
Modalidad de acceso	B	MA	MA	MA	MA	A	MA	MA	MA	MA
Limites sobre la interface de usuario	M	A	A	A	A	A	MA	MA	MA	MA
Renovacion de palabras claves	M	M	M	M	M	M	M	M	M	M
Back-up de informacion	M	M	M	M	M	A	A	A	A	A
Antivirus activo	M	M	M	M	M	A	A	A	A	A
Sistemas operativos actualizados	B	B	B	B	B	B	B	B	B	B
Programas no autorizados	M	M	M	A	A	A	A	A	MA	MA
Inventario de equipos	B	M	M	M	M	MA	A	A	A	A
Mantenimiento preventivo y correctivo de equipos	M	M	M	M	M	A	A	A	A	A
Equipos con garantía	M	M	M	M	M	A	A	A	A	A
Ubicación de cables de red	M	M	M	M	M	A	A	A	A	A
Gabinetes de red	M	M	M	M	M	A	A	A	A	A
Situacion de la sala de servidores	M	M	M	M	M	M	M	M	M	M
Vulnerabilidad de cables de red	B	B	B	B	B	MA	MA	MA	MA	MA
Operatividad de la red	A	A	A	A	A	MA	MA	MA	MA	MA
Correos enviados	A	A	A	A	A	MA	MA	MA	MA	MA
Politicas y normas de seguridad	M	M	M	M	M	A	A	A	A	A
Claves de los servidores	M	M	M	M	M	A	A	A	A	A
Mitigar riesgo de red	M	M	M	M	M	A	A	A	A	A

Determinación del impacto y riesgo residual

MATRIZ DE RIESGOS MAGERIT

TIPO	CODIGO	ACTIVO	CUMPLIMIENTO ACTUAL	AMENAZA	RIESGO ACTUAL		SALVAGUARDA	RIESGO RESIDUAL	ESTIMACION DEL NUEVO CUMPLIMIENTO
					FRECUENCIA			DEGRADACION DEL RIESGO	
Seguridad Lógica	A1	Listas de control de acceso	10%	Mal control de accesos de red	100	MUY FRECUENTE	Establacer una lista de usuarios con acceso a la red	MUY ALTO	80%
	A2	Registro de acceso a la red	10%	Mal control de usuarios de red	100	MUY FRECUENTE	Establacer una lista de cuentas activas	MUY ALTO	80%
	A3	Modalidad de acceso	60%	Error de acceso a la red	100	MUY FRECUENTE	Establecer politicas y administracion de contraseñas	MUY ALTO	85%
	A4	Limites sobre la interface de usuario	60%	Error de privilegios de usuarios	100	MUY FRECUENTE	Realizar grupos de acceso a internet	MUY ALTO	85%
	A5	Renovacion de palabras claves	85%	Error de acceso a los usuarios	10	FRECUENTE	Establecer una guia para que el usuario selecciones y realice el mantenimiento de contraseñas seguras	ALTO	95%
	A6	Back-up de informacion	40%	Perdida de informacion	10	FRECUENTE	Crear y probar regularmente los respaldos de informacion de acuerdo a las politicas	ALTO	85%
	A7	Antivirus activo	30%	Daño de informacion	10	FRECUENTE	Desarrollar e implementar directrices y controles para la deteccion, prevencion y tratamiento de software malicioso	ALTO	80%
Seguridad Física	A8	Sistemas operativos actualizados	40%	Conflictos de programas	100	MUY FRECUENTE	Establecer una Actualizacion automatica de los sistemas operativos	MUY ALTO	85%
	A9	Programas no autorizados	60%	Infeccion de virus en el equipo	10	FRECUENTE	Implementar controles de seguridad para la instlacion de cualquier software en un equipo informatico	ALTO	90%
	A10	Inventario de equipos	70%	Mal control de equipos	10	FRECUENTE	Implementar un procedimiento formal para inventariar los equipos informaticos a todas las areas de trabajo del hospital	ALTO	95%
	A11	Mantenimiento preventivo y correctivo de equipos	70%	Perdida de equipos informaticos	10	FRECUENTE	Desarrollar e implementar controles para el mantenimiento preventivo de los equipos informaticos	ALTO	95%
	A12	Equipos con garantía	55%	Escaces de equipos en garantia	10	FRECUENTE	Implementar un procedimiento formal para verificar que equipos estan en garantia	ALTO	90%
	A13	Ubicación de cables de red	70%	Identificacion de puntos criticos	100	MUY FRECUENTE	Ordenamiento de cableado estructurado	MUY ALTO	85%
	A14	Gabinetes de red	80%	Mal control de puertos de red	10	FRECUENTE	Ordenamiento de los gabinetes de red	ALTO	90%
	A15	Situacion de la sala de servidores	75%	Mal control de equipos intermedios	10	FRECUENTE	Implementar un libro de control de acceso	ALTO	90%
	A16	Vulnerabilidad de cables de red	75%	Robo de informacion	10	FRECUENTE	Bloqueo de puertos de red	ALTO	90%

Seguridad en redes	A17	Operatividad de la red	40%	Caida de la red	10	FRECUENTE	Implementacion de vlan	ALTO	95%
	A18	Correos enviados	50%	Correos perdidos	100	MUY FRECUENTE	Implementar medidas de respaldo en el servidor de correo para que genere automaticamente copias de informacion	MUY ALTO	90%
	A19	Politicas y normas de seguridad	65%	Mal control de la red y acceso de los usuarios	100	MUY FRECUENTE	Implementar el plan de politicas y normas de seguridad:	MUY ALTO	90%
	A20	Claves de los servidores	67%	Olvido y confusion de las claves de los servidores	10	FRECUENTE	Implementar un procedimiento de resguardo de sobres sellados	ALTO	95%
	A21	Mitigar riesgo de red	55%	No saber mitigar el riesgo de la falla de la red	10	FRECUENTE	Implementacion de documentos por cada servidor de procedimiento de fallas	ALTO	95%

LEYENDA	
BLANCO	SE IMPLEMENTA
AMARILLO	NO SE IMPLEMENTA

ANEXO 10:

1° HERRAMIENTA DE GESTION DE RIESGOS “MAGERIT”

ANEXO 06: HERRAMIENTA DE GESTION DE RIESGOS "MAGERIT" POST IDENTIFICACION DE LOS ACTIVOS

Se clasifica los activos de la seguridad informatica según las dimensiones que se han empleado en esta tesis, donde son: Seguridad Lógica, Seguridad Física y Seguridad de redes, estos activos están alineados a los 140 requerimientos que ofrece la ISO 27001.

Tabla N°1

TIPO	NOMBRE DE ACTIVO	
Seguridad Logica	[SL_CA]	Listas de control de acceso
	[SL_PC]	Registro de acceso a la red
	[SL_MA]	Modalidad de acceso
	[SL_LIU]	Limites sobre la interface de usuario
	[SL_RPC]	Renovacion de palabras claves
	[SL_BI]	Back-up de informacion
	[SL_AA]	Antivirus activo
Seguridad Física	[SF_SOA]	Sistemas operativos actualizados
	[SF_PNA]	Programas no autorizados
	[SF_IE]	Inventario de equipos
	[SF_PCE]	Mantenimiento preventivo y correctivo de equipos
	[SF_EG]	Equipos con garantía
	[SF_UCR]	Ubicación de cables de red
	[SF_GR]	Gabinetes de red
	[SF_SSS]	Situacion de la sala de servidores
	[SF_RI]	Vulnerabilidad de cables de red
Seguridad de redes	[SR_PAR]	Operatividad de la red
	[SR_DS]	Correos enviados
	[SR_OR]	Politicas y normas de seguridad
	[SR_CE]	Claves de los servidores
	[SR_PNS]	Mitigar riesgo de red

Tabla de incentivación de los activos

VALORACION DE LOS ACTIVOS

En la valoración de activos que nos brinda la metodología Magerit utilizaremos las dimensiones de seguridad para poder clasificarlas de una manera práctica, donde estas dimensiones se alinearan a cada activo a través de una entrevista al jefe del área de sistemas.

Tabla N°2

Dimensiones de seguridad	
[C]	Confidencialidad
[I]	Integridad
[D]	Disponibilidad
[A]	Autenticidad
[T]	Trazabilidad

Dimensiones de seguridad

Las dimensiones de seguridad se clasificaran mediante preguntas en donde tienen que tener relevancia con los activos de información

Figura N°1

Confidencialidad: ¿qué daño causaría que lo conociera quien no debe?
Integridad: ¿qué perjuicio causaría que estuviera dañado o corrupto?
Disponibilidad: ¿qué perjuicio causaría no tenerlo o no poder utilizarlo?
Autenticidad: ¿qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?
Trazabilidad: ¿quién hace qué y cuándo? Y ¿qué daño causaría no saber quién accede a qué datos y qué hace con ellos?

Definición de dimensiones de seguridad

La tabla de valoración que nos brinda la metodología Magerit nos ayuda a valorar al activo mediante 2 tipos, sea el valor o el criterio de como actué cada activo de información en la organización.

Tabla N°3

Tabla de valoración de activos			
Valor			Criterio
10	Muy alto	MA	Daño muy grave a la organización
7-9	Alto	A	Daño grave a la organización
4-6	Medio	M	Daño importante a la organización
1-3	Bajo	B	Daño menor a la organización
0	Despreciable	D	Irrelevante a efectos practicos

Valoración y criterios de activos

Se clasificara por separado la variable independiente Seguridad informatica, mediante las dimensiones que se están planteando en esta tesis.

A continuación se verá la valoración de los activos de la seguridad lógica según las dimensiones de seguridad

Tabla N°4

Valoracion de activos: Seguridad Lógica					
Activos	Dimensiones de Seguridad				
	[C]	[I]	[D]	[A]	[T]
Listas de control de acceso	B	B	B	B	B
Registro de acceso a la red	MB	B	B	B	B
Modalidad de acceso	M	MA	MA	MA	MA
Limites sobre la interface de usuario	A	A	A	A	A
Renovacion de palabras claves	A	A	A	A	A
Back-up de informacion	A	A	A	A	A
Antivirus activo	M	M	M	M	M

Valoración de activos: Seguridad Lógica

Según la entrevista que se le realizo al jefe del área de sistemas Spilco León Jardy, se pudo definir la importancia y el daño que provocaría cada activo de información para nuestra dimensión SEGURIDAD LÓGICA.

8. Listas de control de acceso
    f) ¿Qué daño causaría que lo conociera quien no debe?
    BAJO: Porque sería un daño menor a la organización
    g) ¿Qué perjuicio causaría que estuviera dañado o corrupto?
    BAJO: Porque sería un daño menor a la organización
    h) ¿Qué perjuicio causaría no tenerlo o poder utilizarlo?
    BAJO: Porque sería un daño menor a la organización
    i) ¿Qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?
    MEDIO: Porque sería un daño importante a la organización
    j) ¿Qué daño causaría no sobre quien accede a que dato y que hace con ellos?
    MEDIO: Porque sería un daño importante a la organización

9. Registro de acceso a la red
    f) ¿Qué daño causaría que lo conociera quien no debe?
    MEDIO: Porque sería un daño importante a la organización
    g) ¿Qué perjuicio causaría que estuviera dañado o corrupto?
    MEDIO: Porque sería un daño importante a la organización
    h) ¿Qué perjuicio causaría no tenerlo o poder utilizarlo?
    MEDIO: Porque sería un daño importante a la organización
    i) ¿Qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?
    MEDIO: Porque sería un daño importante a la organización
    j) ¿Qué daño causaría no sobre quien accede a que dato y que hace con ellos?
    MEDIO: Porque sería un daño importante a la organización

10. Modalidad de acceso
    f) ¿Qué daño causaría que lo conociera quien no debe?
    MEDIO: Porque sería un daño importante a la organización
    g) ¿Qué perjuicio causaría que estuviera dañado o corrupto?
    MEDIO: Porque sería un daño importante a la organización
    h) ¿Qué perjuicio causaría no tenerlo o poder utilizarlo?
    MEDIO: Porque sería un daño importante a la organización
    i) ¿Qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?
    MEDIO: Porque sería un daño importante a la organización
    j) ¿Qué daño causaría no sobre quien accede a que dato y que hace con ellos?
    MEDIO: Porque sería un daño importante a la organización

11. Limites sobre la interface de usuario
    f) ¿Qué daño causaría que lo conociera quien no debe?
    ALTO: Porque sería un daño grave a la organización
    g) ¿Qué perjuicio causaría que estuviera dañado o corrupto?
    ALTO: Porque sería un daño grave a la organización

h) ¿Qué perjuicio causaría no tenerlo o poder utilizarlo?
ALTO: Porque sería un daño grave a la organización

i) ¿Qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?
ALTO: Porque sería un daño grave a la organización

j) ¿Qué daño causaría no sobre quien accede a que dato y que hace con ellos?
ALTO: Porque sería un daño grave a la organización

12. Renovación de palabras claves

f) ¿Qué daño causaría que lo conociera quien no debe?
ALTO: Porque sería un daño grave a la organización

g) ¿Qué perjuicio causaría que estuviera dañado o corrupto?
ALTO: Porque sería un daño grave a la organización

h) ¿Qué perjuicio causaría no tenerlo o poder utilizarlo?
ALTO: Porque sería un daño grave a la organización

i) ¿Qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?
ALTO: Porque sería un daño grave a la organización

j) ¿Qué daño causaría no sobre quien accede a que dato y que hace con ellos?
ALTO: Porque sería un daño grave a la organización

13. Back – up de información

f) ¿Qué daño causaría que lo conociera quien no debe?
ALTO: Porque sería un daño grave a la organización

g) ¿Qué perjuicio causaría que estuviera dañado o corrupto?
ALTO: Porque sería un daño grave a la organización

h) ¿Qué perjuicio causaría no tenerlo o poder utilizarlo?
ALTO: Porque sería un daño grave a la organización

i) ¿Qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?
ALTO: Porque sería un daño grave a la organización

j) ¿Qué daño causaría no sobre quien accede a que dato y que hace con ellos?

ALTO: Porque sería un daño grave a la organización

14. Antivirus activo

f) ¿Qué daño causaría que lo conociera quien no debe?

MEDIO: Porque sería un daño importante a la organización

g) ¿Qué perjuicio causaría que estuviera dañado o corrupto?

MEDIO: Porque sería un daño importante a la organización

h) ¿Qué perjuicio causaría no tenerlo o poder utilizarlo?

MEDIO: Porque sería un daño importante a la organización

i) ¿Qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?

MEDIO: Porque sería un daño importante a la organización

j) ¿Qué daño causaría no sobre quien accede a que dato y que hace con ellos?

MEDIO: Porque sería un daño importante a la organización

A continuación se verá la valoración de los activos de la seguridad física según las dimensiones de seguridad

Tabla N°5

Valoracion de activos: Seguridad Física					
Activos	Dimensiones de Seguridad				
	[C]	[I]	[D]	[A]	[T]
Sistemas operativos actualizados	M	M	M	M	M
Programas no autorizados	MB	B	B	B	B
Inventario de equipos	A	A	A	A	A
Mantenimiento preventivo y correctivo de equipos	M	M	M	M	M
Equipos con garantía	A	A	A	A	A
Ubicación de cables de red	M	M	M	M	M
Gabinetes de red	M	M	M	M	M
Situacion de la sala de servidores	M	M	M	M	M
Vulnerabilidad de cables de red	A	A	A	A	A

Valoración de activos: Seguridad Física

Según la entrevista que se le realizo al jefe del área de sistemas Spilco León Jardy, se pudo definir la importancia y el daño que provocaría cada activo de información para nuestra dimensión SEGURIDAD FÍSICA.

10. ¿Sistemas operativos actualizados?
    a) ¿Qué daño causaría que lo conociera quien no debe?
       MEDIO: Porque sería un daño importante a la organización
    b) ¿Qué perjuicio causaría que estuviera dañado o corrupto?
       MEDIO: Porque sería un daño importante a la organización
    c) ¿Qué perjuicio causaría no tenerlo o poder utilizarlo?
       MEDIO: Porque sería un daño importante a la organización
    d) ¿Qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?
       MEDIO: Porque sería un daño importante a la organización
    e) ¿Qué daño causaría no sobre quien accede a que dato y que hace con ellos?
       MEDIO: Porque sería un daño importante a la organización
11. ¿Programas no autorizados?
    a) ¿Qué daño causaría que lo conociera quien no debe?
       MUY BAJO: Porque sería irrelevante a efectos prácticos.
    b) ¿Qué perjuicio causaría que estuviera dañado o corrupto?
       BAJO: Porque sería un daño menor a la organización
    c) ¿Qué perjuicio causaría no tenerlo o poder utilizarlo?
       BAJO: Porque sería un daño menor a la organización
    d) ¿Qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?
       BAJO: Porque sería un daño menor a la organización
    e) ¿Qué daño causaría no sobre quien accede a que dato y que hace con ellos?
       BAJO: Porque sería un daño menor a la organización

12. ¿Inventario de equipos?

a) ¿Qué daño causaría que lo conociera quien no debe?

ALTO: Porque sería un daño grave a la organización

b) ¿Qué perjuicio causaría que estuviera dañado o corrupto?

ALTO: Porque sería un daño grave a la organización

c) ¿Qué perjuicio causaría no tenerlo o poder utilizarlo?

ALTO: Porque sería un daño grave a la organización

d) ¿Qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?

ALTO: Porque sería un daño grave a la organización

e) ¿Qué daño causaría no sobre quien accede a que dato y que hace con ellos?

ALTO: Porque sería un daño grave a la organización

13. ¿Mantenimiento preventivo y correctivo de equipos?

a) ¿Qué daño causaría que lo conociera quien no debe?

MEDIO: Porque sería un daño importante a la organización

b) ¿Qué perjuicio causaría que estuviera dañado o corrupto?

MEDIO: Porque sería un daño importante a la organización

c) ¿Qué perjuicio causaría no tenerlo o poder utilizarlo?

MEDIO: Porque sería un daño importante a la organización

d) ¿Qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?

MEDIO: Porque sería un daño importante a la organización

e) ¿Qué daño causaría no sobre quien accede a que dato y que hace con ellos?

MEDIO: Porque sería un daño importante a la organización

14. ¿Equipos con garantía?

a) ¿Qué daño causaría que lo conociera quien no debe?

ALTO: Porque sería un daño grave a la organización

b) ¿Qué perjuicio causaría que estuviera dañado o corrupto?

ALTO: Porque sería un daño grave a la organización

c) ¿Qué perjuicio causaría no tenerlo o poder utilizarlo?

ALTO: Porque sería un daño grave a la organización

d) ¿Qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?

ALTO: Porque sería un daño grave a la organización

e) ¿Qué daño causaría no sobre quien accede a que dato y que hace con ellos?

ALTO: Porque sería un daño grave a la organización

15. ¿Ubicación de cables de red?

a) ¿Qué daño causaría que lo conociera quien no debe?

MEDIO: Porque sería un daño importante a la organización

b) ¿Qué perjuicio causaría que estuviera dañado o corrupto?

MEDIO: Porque sería un daño importante a la organización

c) ¿Qué perjuicio causaría no tenerlo o poder utilizarlo?

MEDIO: Porque sería un daño importante a la organización

d) ¿Qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?

MEDIO: Porque sería un daño importante a la organización

e) ¿Qué daño causaría no sobre quien accede a que dato y que hace con ellos?

MEDIO: Porque sería un daño importante a la organización

16. ¿Gabinetes de red?

a) ¿Qué daño causaría que lo conociera quien no debe?

MEDIO: Porque sería un daño importante a la organización

b) ¿Qué perjuicio causaría que estuviera dañado o corrupto?

MEDIO: Porque sería un daño importante a la organización

c) ¿Qué perjuicio causaría no tenerlo o poder utilizarlo?

MEDIO: Porque sería un daño importante a la organización

d) ¿Qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?

MEDIO: Porque sería un daño importante a la organización

e) ¿Qué daño causaría no sobre quien accede a que dato y que hace con ellos?

MEDIO: Porque sería un daño importante a la organización

17. ¿Situación de la sala de servidores?

a) ¿Qué daño causaría que lo conociera quien no debe?

MEDIO: Porque sería un daño importante a la organización

b) ¿Qué perjuicio causaría que estuviera dañado o corrupto?

MEDIO: Porque sería un daño importante a la organización

c) ¿Qué perjuicio causaría no tenerlo o poder utilizarlo?

MEDIO: Porque sería un daño importante a la organización

d) ¿Qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?

MEDIO: Porque sería un daño importante a la organización

e) ¿Qué daño causaría no sobre quien accede a que dato y que hace con ellos?

MEDIO: Porque sería un daño importante a la organización

18. ¿Vulnerabilidad de cables de red?

a) ¿Qué daño causaría que lo conociera quien no debe?

ALTO: Porque sería un daño grave a la organización

b) ¿Qué perjuicio causaría que estuviera dañado o corrupto?

ALTO: Porque sería un daño grave a la organización

c) ¿Qué perjuicio causaría no tenerlo o poder utilizarlo?

ALTO: Porque sería un daño grave a la organización

d) ¿Qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?

ALTO: Porque sería un daño grave a la organización

e) ¿Qué daño causaría no sobre quien accede a que dato y que hace con ellos?

ALTO: Porque sería un daño grave a la organización

A continuación se verá la valoración de los activos de la seguridad de redes según las dimensiones de seguridad

Tabla N°6

Valoracion de activos: Seguridad de redes					
Activos	Dimensiones de Seguridad				
	[C]	[I]	[D]	[A]	[T]
Operatividad de la red	MA	MA	MA	MA	MA
Correos enviados	MA	MA	MA	MA	MA
Politicas y normas de seguridad	M	M	M	M	M
Claves de los servidores	M	M	M	M	M
Mitigar riesgo de red	M	M	M	M	M

Valoración de activos: Seguridad de redes

Según la entrevista que se le realizo al jefe del área de sistemas Spilco León Jardy, se pudo definir la importancia y el daño que provocaría cada activo de información para nuestra dimensión SEGURIDAD DE REDES.

10. ¿Operatividad de la red?

a) ¿Qué daño causaría que lo conociera quien no debe?

MUY ALTO: Porque sería un daño muy grave a la organización

b) ¿Qué perjuicio causaría que estuviera dañado o corrupto?

MUY ALTO: Porque sería un daño muy grave a la organización

c) ¿Qué perjuicio causaría no tenerlo o poder utilizarlo?

MUY ALTO: Porque sería un daño muy grave a la organización

d) ¿Qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?

MUY ALTO: Porque sería un daño muy grave a la organización

e) ¿Qué daño causaría no sobre quien accede a que dato y que hace con ellos?

MUY ALTO: Porque sería un daño muy grave a la organización

11. ¿Correos enviados?

a) ¿Qué daño causaría que lo conociera quien no debe?

MUY ALTO: Porque sería un daño muy grave a la organización

b) ¿Qué perjuicio causaría que estuviera dañado o corrupto?

MUY ALTO: Porque sería un daño muy grave a la organización

c) ¿Qué perjuicio causaría no tenerlo o poder utilizarlo?

MUY ALTO: Porque sería un daño muy grave a la organización

d) ¿Qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?

MUY ALTO: Porque sería un daño muy grave a la organización

e) ¿Qué daño causaría no sobre quien accede a que dato y que hace con ellos?

MUY ALTO: Porque sería un daño muy grave a la organización

12. ¿Políticas y normas de seguridad?

a) ¿Qué daño causaría que lo conociera quien no debe?

MEDIO: Porque sería un daño importante a la organización

b) ¿Qué perjuicio causaría que estuviera dañado o corrupto?

MEDIO: Porque sería un daño importante a la organización

c) ¿Qué perjuicio causaría no tenerlo o poder utilizarlo?

MEDIO: Porque sería un daño importante a la organización

d) ¿Qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?

MEDIO: Porque sería un daño importante a la organización

e) ¿Qué daño causaría no sobre quien accede a que dato y que hace con ellos?

MEDIO: Porque sería un daño importante a la organización

13. ¿Claves de los servidores?

a) ¿Qué daño causaría que lo conociera quien no debe?

MEDIO: Porque sería un daño importante a la organización

b) ¿Qué perjuicio causaría que estuviera dañado o corrupto?

MEDIO: Porque sería un daño importante a la organización

c) ¿Qué perjuicio causaría no tenerlo o poder utilizarlo?

MEDIO: Porque sería un daño importante a la organización

d) ¿Qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?

MEDIO: Porque sería un daño importante a la organización

e) ¿Qué daño causaría no sobre quien accede a que dato y que hace con ellos?

MEDIO: Porque sería un daño importante a la organización

14. ¿Mitigar riesgo de red?

a) ¿Qué daño causaría que lo conociera quien no debe?

MEDIO: Porque sería un daño importante a la organización

b) ¿Qué perjuicio causaría que estuviera dañado o corrupto?

MEDIO: Porque sería un daño importante a la organización

c) ¿Qué perjuicio causaría no tenerlo o poder utilizarlo?

MEDIO: Porque sería un daño importante a la organización

d) ¿Qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?

MEDIO: Porque sería un daño importante a la organización

e) ¿Qué daño causaría no sobre quien accede a que dato y que hace con ellos?

MEDIO: Porque sería un daño importante a la organización

IDENTIFICACION Y VALORACION DE LAS AMENAZAS

La identificación de las amenazas es muy importante porque nos ayuda a clasificar el nivel de criterio con la cual se presenta y a su vez poder identificarlos mediantes valores.

Tabla N°7

Frecuencia de amenazas			
Valor			Criterio
100	Muy frecuente	MF	A diario
10	Frecuente	F	Mensualmente
1	Normal	FN	Una vez al año
1/10	Poco frecuente	PF	Cada varios años
1/100	Muy poco frecuente	B	Siglos

Frecuencia de amenazas

En la tabla N°7 se muestra el criterio de evaluación de una amenaza que nos brinda la metodología magerit donde nos permitirá el nivel de frecuencia con la cual se presenta la amenaza para proceder a degradarla y mantener a salvo el activo de información.

La degradación de las amenazas es muy importante porque nos ayuda a eliminar la amenaza e implementar mejoras para poder mantener bajo control las próximas amenazas que se presenten en la seguridad informatica.

Tabla N°8

Degradación de las amenazas	
Valor	Criterio
90% - 100%	Degradación muy considerable del activo
25% - 89%	Degradación medianamente considerable del activo
1% - 24%	Degradación poco considerable del activo

Degradación de las amenazas

En la figura N°8 se muestra en forma porcentual la degradación de la amenaza según el criterio que se quiera tener sobre ella.

En la figura N°9 se observa que se pudo identificar las amenazas que podrían sufrir los activos de información según la entrevista que se hizo al jefe del área de sistemas Spilco león Jardy, por lo tanto mediante la ayuda de la tabla N°7 Frecuencia de amenazas y Tabla N°8 Degradación de las amenazas, se pudo calcular la valoración de las amenazas en la seguridad Lógica

Tabla N°9

Identificación y valoración de Amenazas: Seguridad Lógica							
Amenaza	Frecuencia	Dimensiones de Seguridad					
		[C]	[I]	[D]	[A]	[T]	total
[A1]Mal control de usuarios	10	30%	30%	30%	30%	30%	30%
[A2] Mal control de acceso a la red	10	30%	30%	30%	30%	30%	30%
[A3]Error de acceso a la red	10	30%	30%	30%	30%	30%	30%
[A4]Error de privilegios de usuarios	10	20%	20%	20%	20%	20%	20%
[A5]Error de acceso a los usuarios	1	5%	5%	5%	5%	5%	5%
[A6] Perdida de informacion	10	60%	60%	60%	60%	60%	60%
[A7] Daño de informacion	1	40%	40%	40%	40%	40%	40%

Identificación y valoración de amenazas: Seguridad Lógica

Con que nivel de frecuencia se presentan amenazas en los activos de información. Según lo comentado por el ingeniero se redactara el nivel de frecuencia de las amenazas.

17) La amenaza A1 se presenta frecuente con un valor de 10 afectando al activo listas de control de acceso diariamente
18) La amenaza A2 se presenta frecuente con un de 10 afectando al activo registro de acceso a la red diariamente
19) La amenaza A3 se presenta frecuente con un valor de 10 afectando al activo modalidad de acceso diariamente
20) La amenaza A4 se presenta frecuente con un valor de 10 afectando al activo límites sobre la interface de usuario diariamente
21) La amenaza A5 se presenta normal con una frecuencia de 1 afectando al activo renovación de palabras claves diariamente
22) La amenaza A6 se presenta frecuente con un valor de 10 afectando al activo back-up de información diariamente
23) La amenaza A7 se presenta normal con un valor de 1 afectando al activo antivirus activo diariamente

2. A1 Amenaza: Mal control de usuarios

a) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la confidencialidad del activo listas de control de acceso?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 30%

b) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la integridad del activo listas de control de acceso?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 30%

c) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la disponibilidad del activo listas de control de acceso?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 30%

d) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la autenticidad del activo listas de control de acceso?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 30%

e) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la trazabilidad del activo listas de control de acceso?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 30%

2. A2 Amenaza: Mal control de acceso a la red

a) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la confidencialidad del activo registro de acceso a la red?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 30%
b) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la integridad del activo registro de acceso a la red?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 30%
c) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la disponibilidad del activo registro de acceso a la red?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 30%
d) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la autenticidad del activo registro de acceso a la red?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 30%
e) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la trazabilidad del activo registro de acceso a la red?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 30%

3. A3 Amenaza: Error de acceso a la red

a) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la confidencialidad del activo modalidad de acceso?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 30%
b) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la integridad del activo modalidad de acceso?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 30%
c) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la disponibilidad del activo modalidad de acceso?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 30%

d) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la autenticidad del activo modalidad de acceso?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 30%

e) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la trazabilidad del activo modalidad de acceso?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 30%

4. A4 Amenaza: Error de privilegios de usuarios

a) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la confidencialidad del activo limites sobre la interface del usuario?
DEGRADACION POCO CONSIDERABLE DEL ACTIVO: 20%

b) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la integridad del activo límites sobre la interface del usuario?
DEGRADACION POCO CONSIDERABLE DEL ACTIVO: 20%

c) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la disponibilidad del activo límites sobre la interface del usuario?
DEGRADACION POCO CONSIDERABLE DEL ACTIVO: 20%

d) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la autenticidad del activo límites sobre la interface del usuario?
DEGRADACION POCO CONSIDERABLE DEL ACTIVO: 20%

e) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la trazabilidad del activo límites sobre la interface del usuario?
DEGRADACION POCO CONSIDERABLE DEL ACTIVO: 20%

5. A5 Amenaza: Error de acceso a los usuarios

a) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la confidencialidad del activo renovación de palabras claves?
DEGRADACION POCO CONSIDERABLE DEL ACTIVO: 5%

b) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la integridad del activo renovación de palabras claves?
DEGRADACION POCO CONSIDERABLE DEL ACTIVO: 5%

c) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la disponibilidad del activo renovación de palabras claves?
DEGRADACION POCO CONSIDERABLE DEL ACTIVO: 5%

d) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la autenticidad del activo renovación de palabras claves?
DEGRADACION POCO CONSIDERABLE DEL ACTIVO: 5%

e) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la trazabilidad del activo renovación de palabras claves?
DEGRADACION POCO CONSIDERABLE DEL ACTIVO: 5%

6. A6 Amenaza: Perdida de información

a) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la confidencialidad del activo back-up de información?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 60%

b) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la integridad del activo back-up de información?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 60%

c) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la disponibilidad del activo back-up de información?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 60%

d) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la autenticidad del activo back-up de información?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 60%

e) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la trazabilidad del activo back-up de información?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 60%

15. A7 Amenaza: Daño de información

a) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la confidencialidad del activo antivirus activo?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 40%

b) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la integridad del activo antivirus activo?

DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 40%

c) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la disponibilidad del activo antivirus activo?

DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 40%

d) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la autenticidad del activo antivirus activo?

DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 40%

e) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la trazabilidad del activo antivirus activo?

DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 40%

la figura N°10 se observa que se pudo identificar las amenazas que podrían sufrir los activos de información, por lo tanto mediante la ayuda de la tabla N°7 Frecuencia de amenazas y Tabla N°8 Degradación de las amenazas, se pudo calcular la valoración de las amenazas en la seguridad Física

Tabla N°10

Identificación y valoración de Amenazas: Seguridad Física							Total
Amenaza	Frecuencia	Dimensiones de Seguridad					
		[C]	[I]	[D]	[A]	[T]	
[A8]Conflictos de programas	100	50%	50%	50%	50%	50%	50%
[A9] Infeccion de virus en el equipo	1	25%	20%	25%	20%	15%	21%
[A10]Mal control de equipos	10	30%	30%	30%	30%	30%	30%
[A11] Perdida de equipos informaticos	1	15%	20%	20%	18%	20%	19%
[A12]Escaces de equipos en garantia	10	45%	45%	45%	45%	45%	45%
[A13] Identificacion de puntos criticos	100	30%	30%	30%	30%	30%	30%
[A14] Mal control de puertos de red	1	10%	10%	10%	10%	10%	10%
[A15] Mal control de equipos intermedios	1	15%	10%	10%	15%	12%	12%
[A16] Robo de informacion	10	25%	25%	25%	25%	25%	25%

Identificación y valoración de amenazas: Seguridad Física

Con que nivel de frecuencia se presentan las amenazas en los activos de información.

Según lo comentado por el ingeniero se redactara el nivel de frecuencia de las amenazas.

24) La amenaza A8 se presenta muy frecuente con un valor de 100 afectando al activo sistemas operativos actualizados diariamente
25) La amenaza A9 se presenta normal con un valor de 1 afectando al activo inventario de equipos diariamente
26) La amenaza A10 se presenta frecuente con un valor de 10 afectando al activo mantenimiento preventivo y correctivo de equipos diariamente
27) La amenaza A11 se presenta normal con un valor de 1 afectando al activo equipos con garantía diariamente
28) La amenaza A12 se presenta frecuente con un valor de 10 afectando al activo programas no autorizados diariamente
29) La amenaza A13 se presenta muy frecuente con un valor de 100 afectando al activo ubicación de los cables de red diariamente
30) La amenaza A14 se presenta normal con una frecuencia de 1 afectando al activo gabinetes de red diariamente
31) La amenaza A13 se presenta normal con un valor de 1 afectando al activo situación de la sala de servidores diariamente
32) La amenaza A14 se presenta frecuente con un valor de 10 afectando al activo vulnerabilidad de cables de red diariamente

5. A8 Amenaza: Conflictos de programas

a) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la confidencialidad del activo sistemas operativos actualizados?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 50%

b) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la integridad del activo sistemas operativos actualizados?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 50%

c) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la disponibilidad del activo sistemas operativos actualizados?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 50%
d) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la autenticidad del activo sistemas operativos actualizados?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 50%
e) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la trazabilidad del activo sistemas operativos actualizados?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 50%

6. A9 Amenaza: Infección de virus en el equipo

a) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la confidencialidad del activo inventario de equipos?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 21%
b) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la integridad del activo inventario de equipos?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 21%
c) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la disponibilidad del activo inventario de equipos?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 21%
d) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la autenticidad del activo inventario de equipos?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 21%
e) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la trazabilidad del activo inventario de equipos?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 21%

7. A10 Amenaza: Mal control de equipos

a) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la confidencialidad del activo mantenimiento preventivo y correctivo de equipos?

DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 30%

b) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la integridad del activo mantenimiento preventivo y correctivo de equipos?

DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 30%

c) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la disponibilidad del activo mantenimiento preventivo y correctivo de equipos?

DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 30%

d) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la autenticidad del activo mantenimiento preventivo y correctivo de equipos?

DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 30%

e) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la trazabilidad del activo mantenimiento preventivo y correctivo de equipos?

DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 30%

8. A11 Amenaza: Perdida de equipos informáticos

a) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la confidencialidad del activo equipos con garantía?

DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 15%

b) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la integridad del activo equipos con garantía?

DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 15%

c) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la disponibilidad del activo equipos con garantía?

DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 15%

d) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la autenticidad del activo equipos con garantía?

DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 15%

e) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la trazabilidad del activo equipos con garantía?

DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 15%

5. A12 Amenaza: Escases de equipos en garantía

a) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la confidencialidad del activo programas no autorizados?

DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 45%

b) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la integridad del activo programas no autorizados?

DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 45%

c) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la disponibilidad del activo programas no autorizados?

DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 45%

d) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la autenticidad del activo programas no autorizados?

DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 45%

e) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la trazabilidad del activo programas no autorizados?

DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 45%

6. A13 Amenaza: Identificación de puntos críticos

a) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la confidencialidad del activo ubicación de los cables de red?

DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 30%

b) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la integridad del activo ubicación de los cables de red?

DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 30%

c) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la disponibilidad del activo ubicación de los cables de red?

DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 30%

d) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la autenticidad del activo ubicación de los cables de red?

DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 30%

e) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la trazabilidad del activo ubicación de los cables de red?

DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 30%

16. A14 Amenaza: Mal control de puertos de red

a) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la confidencialidad del activo gabinetes de red?

DEGRADACION POCO CONSIDERABLE DEL ACTIVO: 10%

b) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la integridad del activo gabinetes de red?

DEGRADACION POCO CONSIDERABLE DEL ACTIVO: 10%

c) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la disponibilidad del activo gabinetes de red?

DEGRADACION POCO CONSIDERABLE DEL ACTIVO: 10%

d) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la autenticidad del activo gabinetes de red?

DEGRADACION POCO CONSIDERABLE DEL ACTIVO: 10%

e) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la trazabilidad del activo gabinetes de red?

DEGRADACION POCO CONSIDERABLE DEL ACTIVO: 10%

17. A15 Amenaza: Mal control de equipos intermedios

a) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la confidencialidad del activo situación de la sala de servidores?
DEGRADACION POCO CONSIDERABLE DEL ACTIVO: 12%

b) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la integridad del activo situación de la sala de servidores?
DEGRADACION POCO CONSIDERABLE DEL ACTIVO: 12%

c) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la disponibilidad del activo situación de la sala de servidores?
DEGRADACION POCO CONSIDERABLE DEL ACTIVO: 12%

d) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la autenticidad del activo situación de la sala de servidores?
DEGRADACION POCO CONSIDERABLE DEL ACTIVO: 12%

e) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la trazabilidad del activo situación de la sala de servidores?
DEGRADACION POCO CONSIDERABLE DEL ACTIVO: 12%

18. A16 Amenaza: Robo de información

a) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la confidencialidad del activo vulnerabilidad de cables de red?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 25%

b) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la integridad del activo vulnerabilidad de cables de red?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 25%

c) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la disponibilidad del activo vulnerabilidad de cables de red?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 25%

d) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la autenticidad del activo vulnerabilidad de cables de red?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 25%

e) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la trazabilidad del activo vulnerabilidad de cables de red?

DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 25%

En la figura N°11 se observa que se pudo identificar las amenazas que podrían sufrir los activos de información, por lo tanto mediante la ayuda de la tabla N°7 Frecuencia de amenazas y Tabla N°8 Degradación de las amenazas, se pudo calcular la valoración de las amenazas en la seguridad de redes

Tabla N°11

Identificación y valoración de Amenazas: Seguridad de redes							Total
Amenaza	Frecuencia	Dimensiones de Seguridad					
		[C]	[I]	[D]	[A]	[T]	
[A17]Caida de la red	10	60%	60%	60%	60%	60%	60%
[A18] Correos perdidos	100	50%	50%	50%	50%	50%	50%
[A19] Mal control de la red y acceso de los usuarios	10	10%	10%	10%	10%	10%	10%
[A20] Olvido y confusion de las claves de los	1	15%	15%	15%	15%	15%	15%
[A21]No saber mitigar el riesgo de la falla de la red	1	20%	20%	20%	20%	20%	20%

Identificación y valoración de amenazas: Seguridad de redes

Con que nivel de frecuencia se presentan las amenazas en los activos de información.

Según lo comentado por el ingeniero se redactara el nivel de frecuencia de las amenazas.

6. La amenaza A17 se presenta frecuente con un valor de 10 afectando al activo políticas y normas de seguridad diariamente
7. La amenaza A18 se presenta muy frecuente con un de 100 afectando al activo claves de servidores diariamente
8. La amenaza A19 se presenta frecuente con un valor de 10 afectando al activo operatividad de la red diariamente
9. La amenaza A20 se presenta normal con un valor de 1 afectando al activo correos enviados diariamente
10. La amenaza A21 se presenta normal con un valor de 1 afectando al activo mitigar riesgos de red diariamente

5. A17 Amenaza: Caída de red

a) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la confidencialidad del activo operatividad de la red?
DEGRADACION MUY CONSIDERABLE DEL ACTIVO: 60%
b) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la integridad del activo operatividad de la red?
DEGRADACION MUY CONSIDERABLE DEL ACTIVO: 60%
c) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la disponibilidad del activo operatividad de la red?
DEGRADACION MUY CONSIDERABLE DEL ACTIVO: 60%
d) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la autenticidad del activo operatividad de la red?
DEGRADACION MUY CONSIDERABLE DEL ACTIVO: 60%
e) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la trazabilidad del activo operatividad de la red?
DEGRADACION MUY CONSIDERABLE DEL ACTIVO: 60%

6. A18 Amenaza: Correos perdidos

a) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la confidencialidad del activo correos enviados?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 50%
b) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la integridad del activo correos enviados?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 50%
c) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la disponibilidad del activo correos enviados?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 50%
d) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la autenticidad del activo correos enviados?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 50%

e) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la trazabilidad del activo correos enviados?
DEGRADACION MEDIANAMENTE CONSIDERABLE DEL ACTIVO: 50%

7. A19 Amenaza: Mal control de la red y acceso de los usuarios

a) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la confidencialidad del activo políticas y normas de seguridad?
DEGRADACION POCO CONSIDERABLE DEL ACTIVO: 10%
b) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la integridad del activo políticas y normas de seguridad?
DEGRADACION POCO CONSIDERABLE DEL ACTIVO: 10%
c) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la disponibilidad del activo políticas y normas de seguridad?
DEGRADACION POCO CONSIDERABLE DEL ACTIVO: 10%
d) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la autenticidad del activo políticas y normas de seguridad?
DEGRADACION POCO CONSIDERABLE DEL ACTIVO: 10%
e) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la trazabilidad del activo políticas y normas de seguridad?
DEGRADACION POCO CONSIDERABLE DEL ACTIVO: 10%

8. A20 Amenaza: Olvido y confusión de las claves en los servidores

a) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la confidencialidad del activo claves de los servidores?
DEGRADACION POCO CONSIDERABLE DEL ACTIVO: 15%
b) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la integridad del activo claves de los servidores?
DEGRADACION POCO CONSIDERABLE DEL ACTIVO: 15%
c) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la disponibilidad del activo claves de los servidores?
DEGRADACION POCO CONSIDERABLE DEL ACTIVO: 15%

d) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la autenticidad del activo claves de los servidores?

DEGRADACION POCO CONSIDERABLE DEL ACTIVO: 15%

e) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la trazabilidad del activo claves de los servidores?

DEGRADACION POCO CONSIDERABLE DEL ACTIVO: 15%

5. A21 Amenaza: No saber mitigar el riesgo de la falla de la red

a) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la confidencialidad del activo mitigar riesgos de red?

DEGRADACION POCO CONSIDERABLE DEL ACTIVO: 20%

b) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la integridad del activo mitigar riesgos de red?

DEGRADACION POCO CONSIDERABLE DEL ACTIVO: 20%

c) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la disponibilidad del activo mitigar riesgos de red?

DEGRADACION POCO CONSIDERABLE DEL ACTIVO: 20%

d) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la autenticidad del activo mitigar riesgos de red?

DEGRADACION POCO CONSIDERABLE DEL ACTIVO: 20%

e) ¿Qué valor de degradación le pondría a la amenaza para que no afecte la trazabilidad del activo mitigar riesgos de red?

DEGRADACION POCO CONSIDERABLE DEL ACTIVO: 20%

MATRIZ DE RIESGOS MAGERIT

A CONTINUACIÓN SE MOSTRARÁ EL ESTADO ACTUAL DE LA SEGURIDAD INFORMATICA SEGÚN LA METODOLOGÍA MAGERIT

SEGURIDAD LOGICA

Tabla N°12

	REQUERIMIENTO	REQUERIMIENTO	Porcentaje de cumplimiento actual	Porcentaje por cada indicador
Seguridad Lógica	Control de acceso	Listas de control de acceso	70%	70%
		Registro de acceso a la red	70%	
		Modalidad de acceso	70%	
	Control de acceso interno	Limites sobre la interface de usuario	80%	69%
		Renovacion de palabras claves	95%	
		Back-up de informacion	40%	
		Antivirus activo	60%	
	Porcentaje total de cumplimiento actual		53.89%	

Situación actual de la Seguridad Lógica

En la Tabla N°12 se muestra el porcentaje de cumplimiento actual, donde es la diferencia del 100 % con la amenaza actual del activo, además se calcula el porcentaje de cumplimiento actual por cada indicador.

SEGURIDAD FISICA

Tabla N°13

	INDICADORES	REQUERIMIENTO	Porcentaje de cumplimiento actual	Porcentaje por cada indicador
Seguridad Física	Funcionamiento de equipos	Sistemas operativos actualizados	50%	70%
		Inventario de equipos	79%	
		Mantenimiento preventivo y correctivo de	70%	
		Equipos con garantía	81%	
	Seguridad de equipos	Programas no autorizados	55%	76%
		Ubicación de cables de red	70%	
		Gabinetes de red	90%	
		Situacion de la sala de servidores	88%	
		Vulnerabilidad de cables de red	75%	
	Porcentaje total de cumplimiento actual		73.11%	

Situación actual de la Seguridad Física

En la Tabla N°13 se muestra el porcentaje de cumplimiento actual, donde es la diferencia del 100 % con la amenaza actual del activo, además se calcula el porcentaje de cumplimiento actual por cada indicador.

MATRIZ DE RIESGOS MAGERIT

SEGURIDAD DE REDES

Tabla N°14

	INDICADORES	REQUERIMIENTO	Porcentaje de cumplimiento actual	Porcentaje por cada indicador
Seguridad de redes	Niveles de seguridad	Politicas y normas de seguridad	40%	45%
		Claves de los servidores	50%	
	Amenazas	Operatividad de la red	90%	85%
		Correos enviados	85%	
		Mitigar riesgo de red	80%	
	Porcentaje total de cumplimiento actual		69.00%	

Situación actual de la Seguridad de redes

En la Tabla N°14 se muestra el porcentaje de cumplimiento actual, donde es la diferencia del 100 % con la amenaza actual del activo, además se calcula el porcentaje de cumplimiento actual por cada indicador.

IDENTIFICACION Y VALORACION DE LAS SALVAGUARDAS

La identificar de las salvaguardas nos ayuda a poder mitigar los riegos que provocarían las amenazas, donde se identificara mediante el estado y el nivel de eficacia.

Tabla N°15

Eficacia	Nivel	Madurez	Estado
0%	L0	Inexistente	Inexistente
10%	L1	Inicial	Iniciado
50%	L2	Reproducible, pero intuitivo	Parcialmente realizado
90%	L3	Proceso definido	En funcionamiento
95%	L4	Gestionado y medible	Monitorizado
100%	L5	Optimizado	Mejora continua

Cuadro del nivel de madurez y estado de las salvaguardas

En la tabla N°16 se pudo identificar la expectativa del nivel de eficacia que ofrecería la salvaguarda, para depurar cada amenaza que vulnere cada activo de información en la seguridad informatica, teniendo en cuenta las 3 dimensiones: Seguridad Lógica, Seguridad Física y Seguridad de redes. La expectativa es valorada por el investigador luego que el investigado haya valorado la frecuencia de la amenaza.

MATRIZ DE RIESGOS MAGERIT

Tabla N°16

Dimensión	Amenaza	Salvaguarda	Nivel	Eficacia
Seguridad Lógica	[A1]Mal control de usuarios	Establacer una lista de usuarios con acceso a la red	L2	70%
	[A2] Mal control de acceso a la red	Establacer una lista de cuentas activas	L2	70%
	[A3]Error de acceso a la red	Establecer politicas y administracion de contraseñas	L2	70%
	[A4]Error de privilegios de usuarios	Realizar grupos de acceso a internet	L2	80%
	[A5]Error de acceso a los usuarios	Establecer una guia para que el usuario selecciones y realice el mantenimiento de contraseñas seguras	L4	95%
	[A6] Perdida de informacion	Crear y probar regularmente los respaldos de informacion de acuerdo a las politicas	L1	40%
	[A7] Daño de informacion	Desarrollar e implementar directrices y controles para la deteccion, prevencion y tratamiento de software	L2	60%
Seguridad Física	[A8]Conflictos de programas	Establecer una Actualizacion automatica de los sistemas operativos	L2	50%
	[A9] Infeccion de virus en el equipo	Implementar controles de seguridad para la instlacion de cualquier software en un equipo	L2	79%
	[A10]Mal control de equipos	Implementar un procedimiento formal para inventariar los equipos informaticos a todas las areas de trabajo	L2	70%
	[A11] Perdida de equipos informaticos	Desarrollar e implementar controles para el mantenimiento preventivo de los equipos	L2	81%
	[A12]Escaces de equipos en garantia	Implementar un procedimiento formal para verificar que equipos estan en garantia	L2	55%
	[A13] Identificacion de puntos criticos	Ordenamiento de cableado estructurado	L2	70%
	[A14] Mal control de puertos de red	Ordenamiento de los gabinetes de red	L3	90%
	[A15] Mal control de equipos intermedios	Implementar un libro de control de acceso	L2	88%
	[A16] Robo de informacion	Bloqueo de puertos de red	L2	75%
Seguridad en redes	[A17]Caida de la red	Implementacion de vlan	L1	40%
	[A18] Correos perdidos	Implementar medidas de respaldo en el servidor de correo para que genere automaticamente copias de	L2	50%
	[A19] Mal control de la red y acceso de los	Implementar el plan de politicas y normas de	L4	90%
	[A20] Olvido y confusion de las claves de los servidores	Implementar un procedimiento de resguardo de sobres sellados	L2	85%
	[A21]No saber mitigar el riesgo de la falla de la red	Implementacion de documentos por cada servidor de procedimiento de fallas	L2	80%

Identificación y valoración de las salvaguardas

RIESGO ACUMULADO

El riesgo acumulado se identifica sin la salvaguarda, para poder tener un antes de cada activo de información afectado por la amenaza. En la siguiente tabla N°17 se identificará la determinación del impacto y riesgo acumulado de las 3 dimensiones: Seguridad Lógica, Seguridad Física y Seguridad de redes, sin la implementación de la salvaguarda y la expectativa se calcula según el investigador.

Tabla N°17

Determinacion del impacto y riesgo acumulado										
Activos	Impacto Potencial Acumulado					Riesgo Acumulado				
	[C]	[I]	[D]	[A]	[T]	[C]	[I]	[D]	[A]	[T]
Listas de control de acceso	M	M	MA	MA	MA	A	A	MA	MA	MA
Registro de acceso a la red	M	MA	MA	MA	MA	A	MA	MA	MA	MA
Modalidad de acceso	M	MA	MA	MA	MA	A	MA	MA	MA	MA
Limites sobre la interface de usuario	M	A	A	A	A	A	MA	MA	MA	MA
Renovacion de palabras claves	M	M	M	M	M	M	M	M	M	M
Back-up de informacion	M	M	M	M	M	A	A	A	A	A
Antivirus activo	M	M	M	M	M	A	A	A	A	A
Sistemas operativos actualizados	M	M	B	B	M	A	A	B	A	B
Programas no autorizados	A	A	M	A	A	A	A	A	MA	MA
Inventario de equipos	M	M	A	M	M	MA	A	A	A	A
Mantenimiento preventivo y correctivo de equipos	M	M	M	A	M	A	A	A	A	A
Equipos con garantía	A	A	A	A	M	A	A	A	A	A
Ubicación de cables de red	A	A	A	A	A	A	A	A	A	A
Gabinetes de red	M	A	A	M	M	A	A	A	A	A
Situacion de la sala de servidores	M	M	M	M	M	M	M	M	M	M
Vulnerabilidad de cables de red	B	A	B	A	B	MA	MA	MA	MA	MA
Operatividad de la red	A	A	A	A	A	MA	MA	MA	MA	MA
Correos enviados	A	A	A	A	A	MA	MA	MA	MA	MA
Politicas y normas de seguridad	M	M	M	A	M	A	A	A	A	A
Claves de los servidores	M	A	M	M	M	A	A	A	A	A
Mitigar riesgo de red	A	M	A	M	M	A	A	A	A	A

Determinación del impacto y riesgo acumulado

RIESGO RESIDUAL

El riesgo acumulado se identifica con la nueva salvaguarda implementada, para poder tener un después de cada activo de información con la amenaza mitigada. La tabla de estimación del impacto nos ayudara a poder identificar el porcentaje de degradación de la amenaza con la salvaguarda implementada.

Tabla N°18

Tabla de estimación del impacto				
Impacto		Degradación		
		0% - 24%	25% - 89%	90% - 100%
Valor	(9-10)	M	A	MA
	(7-8)	M	A	A
	(4-6)	B	M	MA
	(2-3)	MB	B	B
	(0-1)	MB	MB	MB

Tabla de estimación del impacto

La tabla de estimación de riesgo nos ayudara a relacionar el nivel de frecuencia y el impacto para poder estimar el riesgo.

Tabla N°19

Tabla de estimacion del riesgo					
Riesgo		Degradación			
		PF	FN	F	MF
Impacto	MA	M	A	MA	MA
	A	B	A	MA	MA
	M	B	M	A	A
	B	MB	B	MA	A
	MB	MB	MB	B	B

Tabla de estimación del riesgo

En la tabla N°20 se muestra la determinación del impacto y riesgo residual con la salvaguarda implementada por cada activo de información, donde se va a mitigar el riesgo en un porcentaje considerable y poder seguir mejorando la salvaguarda implementada. La expectativa es según el investigador y la aprobación del investigado.

Tabla N°20

Determinacion del impacto y riesgo residual										
Activos	Impacto residual					Riesgo residual				
	[C]	[I]	[D]	[A]	[T]	[C]	[I]	[D]	[A]	[T]
Listas de control de acceso	B	B	MA	MA	MA	A	A	MA	MA	MA
Registro de acceso a la red	B	MA	MA	MA	MA	A	MA	MA	MA	MA
Modalidad de acceso	B	MA	MA	MA	MA	A	MA	MA	MA	MA
Limites sobre la interface de usuario	M	A	A	A	A	A	MA	MA	MA	MA
Renovacion de palabras claves	M	M	M	M	M	M	M	M	M	M
Back-up de informacion	M	M	M	M	M	A	A	A	A	A
Antivirus activo	M	M	M	M	M	A	A	A	A	A
Sistemas operativos actualizados	B	B	B	B	B	B	B	B	B	B
Programas no autorizados	M	M	M	A	A	A	A	A	MA	MA
Inventario de equipos	B	M	M	M	M	MA	A	A	A	A
Mantenimiento preventivo y correctivo de equipos	M	M	M	M	M	A	A	A	A	A
Equipos con garantía	M	M	M	M	M	A	A	A	A	A
Ubicación de cables de red	M	M	M	M	M	A	A	A	A	A
Gabinetes de red	M	M	M	M	M	A	A	A	A	A
Situacion de la sala de servidores	M	M	M	M	M	M	M	M	M	M
Vulnerabilidad de cables de red	B	B	B	B	B	MA	MA	MA	MA	MA
Operatividad de la red	A	A	A	A	A	MA	MA	MA	MA	MA
Correos enviados	A	A	A	A	A	MA	MA	MA	MA	MA
Politicas y normas de seguridad	M	M	M	M	M	A	A	A	A	A
Claves de los servidores	M	M	M	M	M	A	A	A	A	A
Mitigar riesgo de red	M	M	M	M	M	A	A	A	A	A

Determinación del impacto y riesgo residual

MATRIZ DE RIESGOS MAGERIT

TIPO	CODIGO	ACTIVO	CUMPLIMIENTO ACTUAL	AMENAZA	RIESGO ACTUAL		SALVAGUARDA	RIESGO RESIDUAL	ESTIMACION DEL NUEVO CUMPLIMIENTO
					FRECUENCIA			DEGRADACION DEL RIESGO	
Seguridad Lógica	A1	Listas de control de acceso	70%	Mal control de usuarios	10	FRECUENTE	Establacer una lista de usuarios con acceso a la red	MUY ALTO	70%
	A2	Registro de acceso a la red	70%	Mal control de acceso a la red	10	FRECUENTE	Establacer una lista de cuentas activas	MUY ALTO	70%
	A3	Modalidad de acceso	70%	Error de acceso a la red	10	FRECUENTE	Establecer politicas y administracion de contraseñas	MUY ALTO	70%
	A4	Limites sobre la interface de usuario	80%	Error de privilegios de usuarios	10	FRECUENTE	Realizar grupos de acceso a internet	MUY ALTO	80%
	A5	Renovacion de palabras claves	95%	Error de acceso a los usuarios	1	FRECUENTEMENTE NORMAL	Establecer una guia para que el usuario selecciones y realice el mantenimiento de contraseñas seguras	MEDIO	95%
	A6	Back-up de informacion	40%	Perdida de informacion	10	FRECUENTE	Crear y probar regularmente los respaldos de informacion de acuerdo a las politicas	ALTO	40%
	A7	Antivirus activo	60%	Daño de informacion	10	FRECUENTE	Desarrollar e implementar directrices y controles para la deteccion, prevencion y tratamiento de software malicioso	ALTO	60%
Seguridad Física	A8	Sistemas operativos actualizados	40%	Conflictos de programas	10	FRECUENTE	Establecer una Actualizacion automatica de los sistemas operativos	BAJO	50%
	A9	Programas no autorizados	60%	Infeccion de virus en el equipo	10	FRECUENTE	Implementar controles de seguridad para la instlacion de cualquier software en un equipo informatico	ALTO	79%
	A10	Inventario de equipos	70%	Mal control de equipos	10	FRECUENTE	Implementar un procedimiento formal para inventariar los equipos informaticos a todas las areas de trabajo del hospital	ALTO	70%
	A11	Mantenimiento preventivo y correctivo de equipos	70%	Perdida de equipos informaticos	10	FRECUENTE	Desarrollar e implementar controles para el mantenimiento preventivo de los equipos informaticos	ALTO	81%
	A12	Equipos con garantía	55%	Escaces de equipos en garantia	10	FRECUENTE	Implementar un procedimiento formal para verificar que equipos estan en garantia	ALTO	55%
	A13	Ubicación de cables de red	70%	Identificacion de puntos criticos	10	FRECUENTE	Ordenamiento de cableado estructurado	ALTO	70%
	A14	Gabinetes de red	80%	Mal control de puertos de red	1	FRECUENTEMENTE NORMAL	Ordenamiento de los gabinetes de red	ALTO	90%
	A15	Situacion de la sala de servidores	75%	Mal control de equipos intermedios	10	FRECUENTE	Implementar un libro de control de acceso	MEDIO	88%
	A16	Vulnerabilidad de cables de red	75%	Robo de informacion	10	FRECUENTE	Bloqueo de puertos de red	MUY ALTO	75%

MATRIZ DE RIESGOS MAGERIT

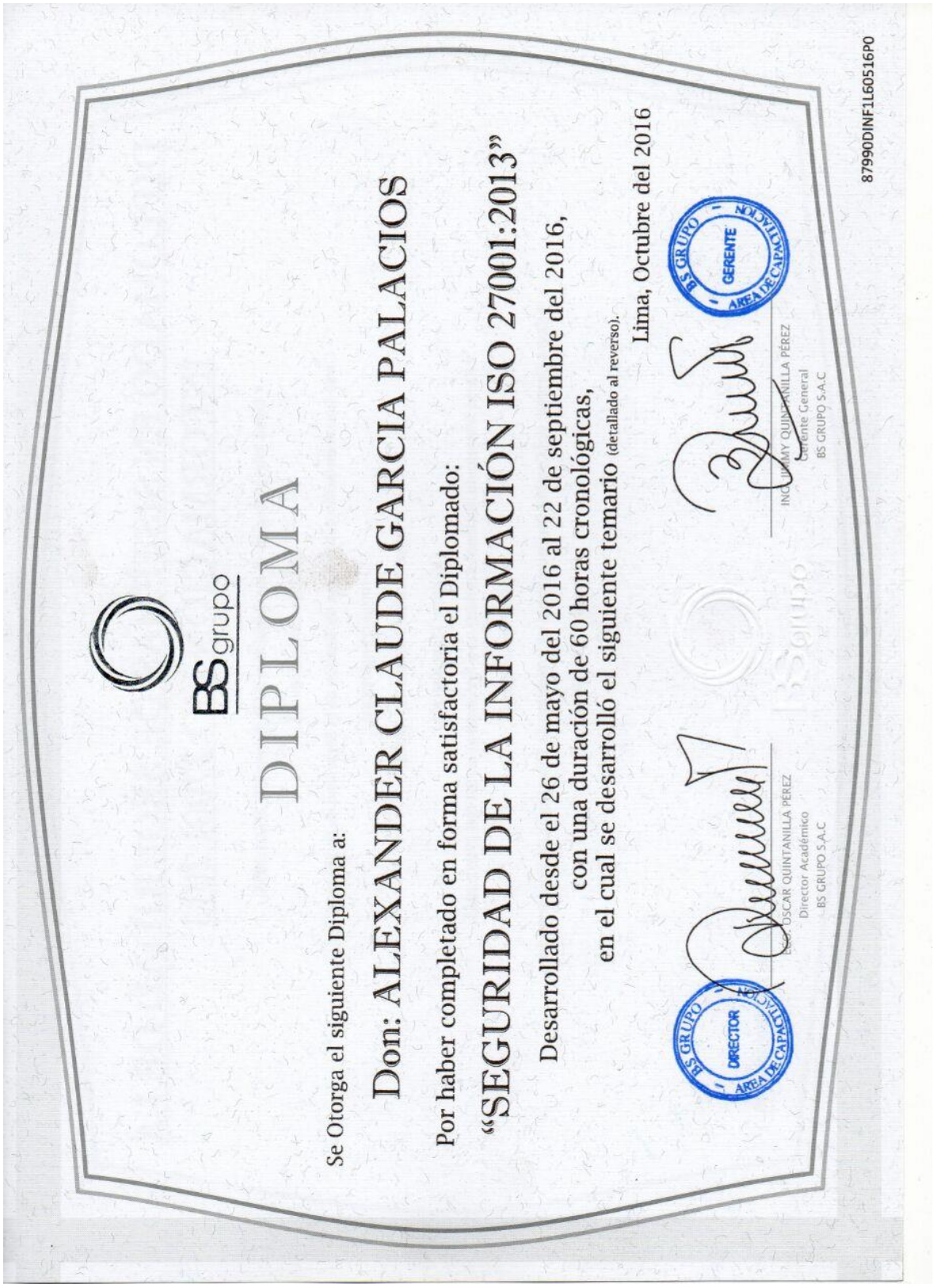
Seguridad en redes	A17	Operatividad de la red	40%	Caida de la red	10	FRECUENTE	Implementacion de vlan	MUY ALTO	40%
	A18	Correos enviados	50%	Correos perdidos	100	MUY FRECUENTE	Implementar medidas de respaldo en el servidor de correo para que genere automaticamente copias de informacion	MUY ALTO	50%
	A19	Politicas y normas de seguridad	65%	Mal control de la red y acceso de los usuarios	10	FRECUENTE	Implementar el plan de politicas y normas de seguridad:	ALTO	90%
	A20	Claves de los servidores	67%	Olvido y confusion de las claves de los servidores	10	FRECUENTE	Implementar un procedimiento de resguardo de sobres sellados	ALTO	85%
	A21	Mitigar riesgo de red	55%	No saber mitigar el riesgo de la falla de la red	10	FRECUENTE	Implementacion de documentos por cada servidor de procedimiento de fallas	ALTO	80%

LEYENDA	
BLANCO	SE IMPLEMENTA
AMARILLO	NO SE IMPLEMENTA

ANEXO 11:

1° AUDITORÍA INFORMÁTICA EN EL HOSPITAL SAN BARTOLOMÉ

Para validar la auditoria se tuvo el apoyo del auditor interno García Palacios Alexander Claude donde se adjunta sus certificados de auditor de ISO/IEC 27001:2013 y en el anexo 15 se adjunta su hoja de vida



BS grupo

DIPLOMA

Se Otorga el siguiente Diploma a:

Don: ALEXANDER CLAUDE GARCIA PALACIOS

Por haber completado en forma satisfactoria el Diplomado:

"SEGURIDAD DE LA INFORMACIÓN ISO 27001:2013"

Desarrollado desde el 26 de mayo del 2016 al 22 de septiembre del 2016,
con una duración de 60 horas cronológicas,
en el cual se desarrolló el siguiente temario (detallado al reverso).

Lima, Octubre del 2016

BS GRUPO DIRECTOR AREA DE CAPACITACION

Lic. OSCAR QUINTANILLA PEREZ
Director Académico
BS GRUPO S.A.C

BS GRUPO GERENTE AREA DE CAPACITACION

ING. JIMMY QUINTANILLA PÉREZ
Gerente General
BS GRUPO S.A.C

87990DINF1L60516P0

AENOR

Otorga el presente

CERTIFICADO

A: **ALEXANDER CLAUDE GARCIA PALACIOS**

Por haber aprobado el curso de:

FORMACIÓN DE AUDITORES INTERNOS EN SISTEMAS DE SEGURIDAD EN TECNOLOGÍAS DE LA INFORMACIÓN

ISO 27001:2013

Realizado el día 20 y 21 de agosto de 2016 en la ciudad de Lima con una duración de 16 horas.

Pedro J. Fernández García
Director General
AENOR PERÚ

N° Registro APE/16/1714

5 de setiembre de 2016

AENOR PERÚ AENOR PERÚ AENOR PERÚ AENOR PERÚ AENOR PERÚ AENOR PERÚ AENOR PERÚ AENOR PERÚ AENOR PERÚ AENOR PERÚ

MATRIZ DE RIESGOS MAGERIT

FACULTAD DE INGENIERÍA

ESCUELA ACADÉMICO-PROFESIONAL INGENIERÍA DE SISTEMAS

“AUDITORIA DE SEGURIDAD INFORMÀTICA EN EL HOSPITAL SAN BARTOLOMÈ”

INTEGRANTES

- ✓ CALDERON ALVARADO JERSON JOSEPH.
- ✓ GARCIA PALACIOS ALEXANDER CLAUDE
- ✓ CAMPOS CASTRO BRIAN
- ✓ ORMEÑO JARAMILLO LUIS

CICLO IX

2016-II

Contenido

GENERALIDADES

MATRIZ DE RIESGOS MAGERIT

I. GENERALIDADES

1.1. TITULO

AUDITORIA DE SEGURIDAD INFORMATICA EN EL HOSPIITAL NACIONAL MADRE NIÑO SAN BARTOLOMÈ

1.2. INTEGRANTES

- ✓ CALDERON ALVARADO JERSON JOSEPH.
- ✓ GARCIA PALACIOS ALEXANDER CLAUDE
- ✓ CAMPOS CASTRO BRIAN
- ✓ ORMEÑO JARAMILLO LUIS

1.3. NOMBRE DE LA EMPRESA A AUDITAR

HOSPITAL NACIONAL MADRE NIÑO SAN BARTOLOMÈ

1.4. TIPO DE AUDITORIA A REALIZAR

AUDITORIA DE SEGURIDAD INFOMATICA

1.5. DURACION DE PROYECTO DE AUDITORIA

SEIS (6) DIAS

DIECISEIS (16 HORAS)

1.6. COSTO DE PROYECTO DE AUDITORIA

MIL DOSCIENTOS OCHENTA Y CUATRO SOLES, NOVENTA CENTIMOS

S/. 1’284.90 NUEVOS SOLES

INTRODUCCION

II. INTRODUCCION

2.1. INTRODUCCION

El presente trabajo trata de identificar la escasa forma de implementación de estándares y guías en el área de sistemas e informática en el hospital San Bartolomé en un periodo de seis (6) días, dado que en el siguiente informe se hará una auditoria de seguridad informática para poder identificar las vulnerabilidades de los procesos del hospital San Bartolomé y poder añadirle posible solución si esta lo necesite.

La información de una empresa es el oro más preciado de ello, por lo cual las categorías de procesos, los procesos y los niveles de capacidad de procesos deben de estar bien estructurado en la empresa, más aun si es una entidad hospitalaria porque tiene información sumamente confidencial.

La auditoría trata de ver los procesos que no se cumplen en una empresa y/o organización, con la finalidad de poder identificarlos y poder sugerir alguna posible mejora si en caso la empresa lo requiera, para ello hemos podido recoger información del hospital San Bartolomé con el área a auditar que es el área de sistemas e informática, luego identificar los objetivos de la auditoria con su alcance debido para poder efectuar una auditoria correcta. Luego ver con que guía de trabajo vamos a trabajar para la empresa, norma y estándar para el área de sistemas e informática y para que sea una auditoria correcta y estructurada hemos realizado un diagrama de Gantt y a raíz de ello hemos podido identificar el tiempo que se culminara la auditoria y el costo de ello.

A continuación se le explicara cada parte del proyecto detalladamente.

2.2. INFORMACION DE LA EMPRESA Y DEL AREA DE TI

El HONADOMANI “San Bartolomé” es un órgano desconcentrado de la Dirección de Salud V Lima Ciudad del Ministerio de Salud, normalizado en el ROF aprobado con RM Nº 884-2003-SA/DM. Es un hospital especializado en atención a la salud sexual y reproductiva de la mujer y la atención integral del neonato, niño y del adolescente. Es un establecimiento de atención recuperativa y de rehabilitación altamente especializada y de enfoque integral a la Mujer con necesidades de atención en su salud sexual y reproductiva y al Neonato, Niño y Adolescente, que proceden de cualquier punto del ámbito nacional

El Hospital “San Bartolomé”, fue fundado el 06 de Enero de 1646, durante el Gobierno del Marqués De Mancera Don Pedro de Toledo y Leiva. Sus fundadores, fueron el célebre Sacerdote Agustino Fray Bartolomé de Vadillo y el religioso Jesuita P. Gabriel Perli.

En 1651 se erigió el Hospital en el barrio de Santa Catalina a la altura de la novena cuadra del Jr. Antonio Miro Quezada, lugar que terminó sufriendo graves estragos durante el terremoto de 1687, siendo parcialmente reconstruido por el Sargento Mayor Manuel Fernández Dávila, Mayordomo del Hospital; gracias a las donaciones del Capitán Francisco Tijero de la Huerta y Segovia.

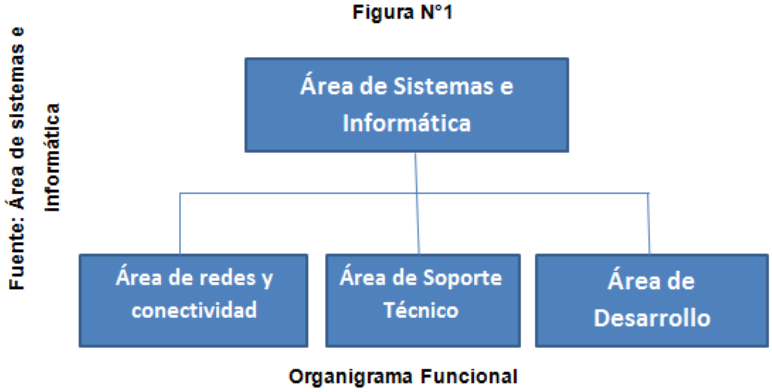
Hacia el año 1970 se incorporan al Hospital el Área Hospitalaria Nº 022 hasta el año 1983, a partir del cual se denomina Hospital Especializado Materno Infantil “San Bartolomé

El área de Sistema e Informática tiene como función principal el mantenimiento de la plataforma SIGHOS. También hace mantenimiento a los sistemas del Rol del Personal, Siaf, Siga y a la sala de telecomunicaciones del hospital.

El área de sistemas se divide en el área de soporte técnico que da mantenimiento a los equipos de cómputo y tiene como función principal solucionar las incidencias diarias, el área de redes y conectividad se encarga de dar mantenimiento a la sala de telecomunicaciones y conectividad del hospital y el área de desarrollo que se encarga de dar mantenimiento a los sistemas que utiliza el hospital.

A continuación, se muestra en la figura 1 como se divide el área de sistemas e informática

Figura N°1



Fuente: Área de sistemas e Informática

Organigrama Funcional

En la figura 1 se muestra que el área de sistemas e informática está dividida en sub áreas, el área de soporte técnico, el área de redes y conectividad y el área de desarrollo

2.2.1. VISION

Ser un hospital reconocido a nivel nacional por la atención que brinda a la salud sexual y reproductiva de la mujer y a la salud del feto, neonato, lactante, niño y adolescente, que ha alcanzado los estándares de sus servicios altamente especializados y garantiza la calidad de sus procesos de atención, con eficiencia y sensibilidad social, en virtud del compromiso e identificación de sus recursos humanos altamente calificados que le permiten continuar siendo el líder de los hospitales de alta complejidad del sector salud.

2.2.2. MISION

Somos un hospital de referencia nacional, que brinda atención altamente especializada a la salud sexual y reproductiva de la mujer y atención integral al feto, neonato, lactante, niño y adolescente; con calidad, eficiencia e inclusión social. Nuestro aporte a la sociedad, se consolida con la Docencia e Investigación que desarrollaremos en forma permanente y nuestra participación activa en los planes y programas nacionales, así como en las acciones de proyección social a la comunidad.

2.2.3. VALORES

El hospital San Bartolomé se identifica con los siguientes valores, que marcaran el curso a seguir para las consecuciones de objetivos trazados, mediante el compromiso de todos sus integrantes.

- **Lealtad:** actuamos con fidelidad a os objetivos institucionales, priorizando la defensa y protección de la persona humana
- **Justicia:** Intervenimos con la probidad, rectitud e imparcialidad procurando el bien común y el iteres en general.
- **Transparencia:** Fomentamos la práctica de valores y principios éticos en nuestras acciones para generar confianza y credibilidad.
- **Compromiso:** Nos esforzamos por gestionar con calidad porque entendemos que nuestras acciones deben coadyuvar el desarrollo sectorial.
- **Trabajo en equipo:** Coadyuvamos a soluciones integrales y eficientes con proactividad y sinergia.

2.2.4. FILOSOFIA

- Somos un equipo de profesionales fraternos, solidarios y cohesionados que impulsa optimas acciones de supervisión y control interno para mejorar el sistema disciplinario y funcional del sector interno.
- Gestionamos nuestros procesos con ética y transparencia para fortalecer las acciones de la lucha contra la corrupción y optimizar el sistema disciplinario y funcional del sector interno.

2.2.5. AREA DE TECNOLOGIA DE INFORMACION

El área de Sistema e Informática tiene como función principal el mantenimiento de la plataforma SIGHOS. También hace mantenimiento a los sistemas del Rol del Personal, Siaf, Siga y a la sala de telecomunicaciones del hospital.

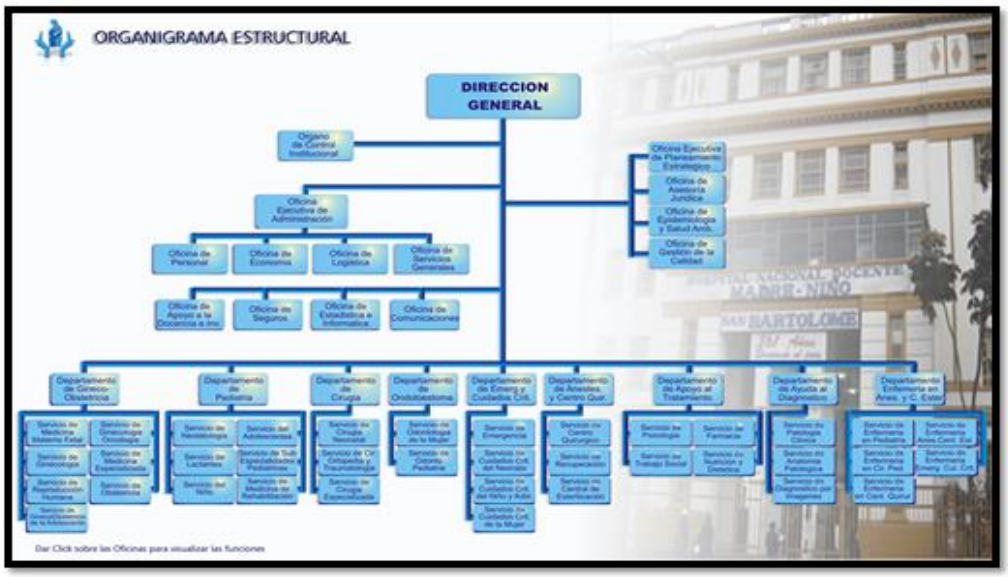
El área de sistemas se divide en el área de soporte técnico que da mantenimiento a los equipos de cómputo y tiene como función principal solucionar las incidencias diarias, el área de redes y conectividad se encarga de dar mantenimiento a la sala de telecomunicaciones y

conectividad del hospital y el área de desarrollo que se encarga de dar mantenimiento a los sistemas que utiliza el hospital.

ORGANIGRAMA DEL HOSPITAL NACIONAL SAN BARTOLOMÈ

Figura N°2

Fuente: Dirección general del Hospital San Bartolomé

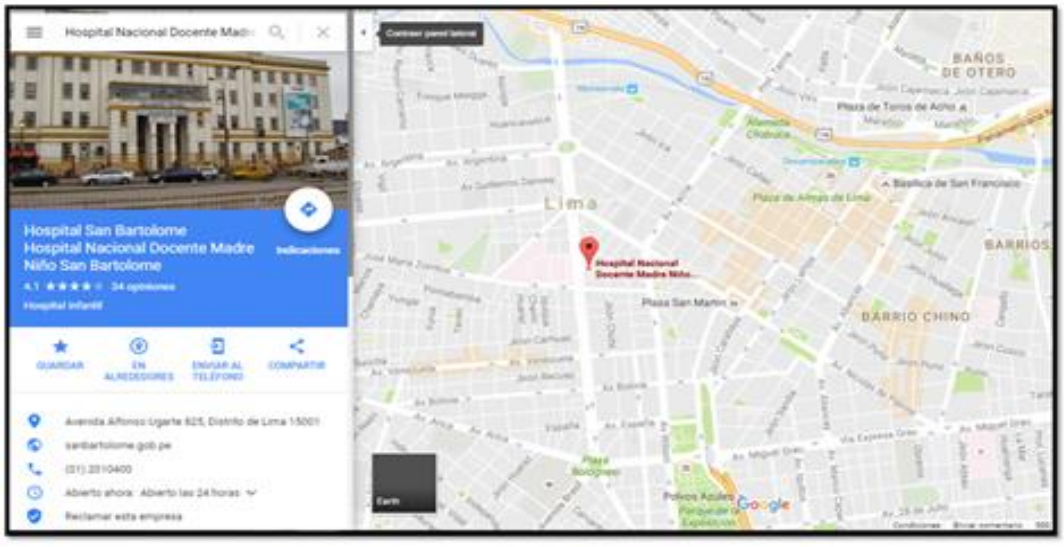


Organización Funcional

UBICACION DE INSPECTORIA GENERAL DE LA PNP

Figura N°3

Fuente: Google Maps



Croquis de Hospital San Bartolomé

2.3. OBJETIVOS DE LA AUDITORIA

El objetivo de la auditoría es verificar la existencia de estos controles y que estén funcionando de manera eficaz, respetando las políticas de la empresa y los objetivos de la empresa. Los objetivos de auditoría se consiguen mediante los procedimientos de auditoría, inicio, planeamiento, ejecución y cierre. Dado que se está enfocando está auditoría en el área de sistemas e informática

2.3.1. OBJETIVO GENERAL

Realizar una auditoría de seguridad informática en el hospital san Bartolomé, con la finalidad de poder identificar las vulnerabilidades de los activos según los niveles de seguridad que se requieran dar y las posibles amenazas que afecten a las vulnerabilidades

2.3.2. OBJETIVOS ESPECIFICOS

1. Identificar la cantidad de usuarios que tienen acceso a la red interna del hospital
2. Identificar la cantidad de usuarios creados con su contraseña
3. Identificar el nivel seguridad que tienen las contraseñas de los usuarios
4. Identificar los niveles de privilegios de acceso que tienen los usuarios
5. Identificar el periodo de cambio de contraseñas de los usuarios
6. Identificar si existe copias de seguridad de la información.
7. Identificar si el antivirus está activo
8. Identificar si los equipos cuentan con sistemas operativos actualizados
9. Identificar si existe la restricción de instalación de software
10. Identificar si existe un control de inventario de los equipos informáticos.
11. Identificar si existe mantenimiento preventivo y correctivo de los equipos informáticos.
12. Identificar si existen equipos con garantía
13. Identificar la correcta ubicación de los cables de red con la finalidad de evitar inferencia.
14. Identificar si existe un ordenamiento estructurado en los gabinetes de la empresa para la supervisión de próximas auditorias.
15. Identificar la situación actual de la sala de servidores

16. Identificar los puntos vulnerables del cableado estructurado y los riesgos que esto implica en la seguridad de la red para que no haya robo de información.
17. Identificar la operatividad de la red en el hospital.
18. Identificar la seguridad de los correos que llegan a su destino
19. Identificar si cuenta con políticas y normas de seguridad de información
20. Identificar las claves de los servidores
21. Identificar planes para mitigar los riesgos de la red

2.4. ALCANCE DE LA AUDITORIA

La auditoría a realizarse abarcará desde el análisis exhaustivo de las funciones organizativas para la seguridad informática, la seguridad lógica, seguridad física y seguridad de redes; siendo ésta analizada con las distintas normativas nacionales e internacionales, así como estándares de los distintos dispositivos utilizados. El periodo de esta evaluación comprende entre las fechas del 26 de OCTUBRE hasta el 02 de NOVIEMBRE del año 2016 y costara S/. 1’284.90 nuevos soles.

2.5. DESCRIPCION Y FUNCIONES DEL EQUIPO AUDITOR

Cargo	Apellidos y Nombres	Tareas Básicas
Auditor Principal	✓ GARCIA PALACIOS ALEXANDER CLAUDE	-Evaluar el ambiente de control y la información recopilada sobre los aspectos objetivos de la auditoria. -Dirigir la planificación de la auditoria y el desarrollo de la estrategia. -Revisar y aprobar la planificación de la auditoria. - Introducir y revisar con el Supervisor los cambios en el programa de auditoria que se consideren necesarios
Auditor Líder de Seguridad informática	✓ CALDERON ALVARADO JERSON JOSEPH	-Coordinar con el Supervisor la distribución del tiempo y la duración de las diversas fases del trabajo. - Examinar e investigar aquellas áreas críticas que se relacionen con los objetivos de las tareas encomendadas.

		- Preparar los papeles de trabajo correspondientes.
Auditor Interno de seguridad Lógica y física	✓ CAMPOS CASTRO BRIAN	- Asistir en obtener información acerca de los aspectos a analizar junto con las normas y reglamentaciones aplicables. - Preparar los papeles de trabajo correspondientes.
Auditor interno de seguridad de redes	✓ ORMEÑO JARAMILLO LUIS	- Desarrollar una evaluación ampliada de los riesgos de control a través de la aplicación de formularios de control interno. - Preparar los papeles de trabajo correspondientes.

2.6. CRITERIOS DE AUDITORIA A UTILIZAR

- La NTP-ISO/IEC 27001 “Sistema de gestión de la seguridad de la información”. Es poder identificar una gestión de seguridad de información y así mismo poder hacer que la empresa cumpla con los estándares establecidos en dicha gestión.
- MODELO OSI: Marco de referencia de capas y estándar de trabajo Para establecer una comunicación entre equipos, lo mismo que para establecerla entre personas, es necesario contar con una serie de normas y protocolos que regulen dicho proceso. Esas normas las fija la sociedad en general o una organización internacional de normalización. Se puede mencionar como una de esas normativas al Modelo OSI.

  El modelo OSI (Open System Interconnection) es la base para la estructuración de la red de comunicaciones, la capa a utilizar será la numero uno:

  - Capa 1: capa de enlace físico

  En este nivel se definen todas las características eléctricas y magnéticas de la red. Se incluye la conexión física ya sean los cables, los conectores y los tipos de señales. Básicamente consiste en proteger físicamente los cables de conexión, los módems y los circuitos.
- La Norma EIA/TIA 568 A y EIA/TIA B, Nos especifica los requerimientos mínimos para el cableado de establecimientos comerciales de oficinas dado que siguen una estructura de cómo se debe implementar la forma de cableado respecto al conector RJ45, según esta norma se verá si es posible la comunicación de equipos y así posible el intercambio de comunicación.
- Estándar ANSI/TIA/EIA-569, Este estándar es para los ductos, pasos y espacios necesarios para la instalación de sistemas estandarizados de telecomunicaciones en el área de redes y así poder mantener un orden en el cableado estructurado en la empresa.

2.7. DOCUMENTACION INICIAL A SOLICITAR

- Se le solicitara el plan de contingencia de la seguridad informática del Hospital Nacional San Bartolomé
  - DOCUMENTO 1

2.8. PLAN DE AUDITORIA

Para hacer una planeación eficaz, lo primero que se requiere es obtener información general sobre la organización y sobre la función de punto a evaluar, que este caso sería la gestión de las redes. Para ello es preciso hacer una investigación preliminar y algunas entrevistas previas, con base en esto planear el programa de trabajo, el cual deberá incluir tiempo, costo, personal necesario y documentos auxiliares a solicitar o formular durante el desarrollo de la misma.

1. Investigación preliminar

Se deberá observar el estado general del área, su situación dentro de la organización, si existe la información solicitada, si es o no necesaria y la fecha de su última actualización. Para analizar y dimensionar la estructura por auditar se debe solicitar:

- ✓ **A nivel del área de informática:** Objetivos a corto y largo plazo.
- ✓ **Recursos materiales y técnicos:** Solicitar documentos sobre los equipos, número de ellos, localización y características.

  - Estudios de viabilidad.
  - Número de equipos, localización y las características (de los equipos instalados y por instalar y programados)
  - Fechas de instalación de los equipos y planes de instalación.
  - Contratos vigentes de compra, renta y servicio de mantenimiento.
  - Contratos de seguros.
  - Convenios que se tienen con otras instalaciones.

- Configuración de los equipos y capacidades actuales y máximas.
- Planes de expansión.
- Ubicación general de los equipos.
- Políticas de operación.
- Políticas de uso de los equipos.

2. Controles

Conjunto de disposiciones metódicas, cuyo fin es vigilar las funciones y actitudes de las empresas y para ello permite verificar si todo se realiza conforme a los programas adoptados, órdenes impartidas y principios admitidos. La clasificación general de los controles consta de 3 controles:

- ✓ **Controles Preventivos:** Son aquellos que reducen la frecuencia con que ocurren las causas del riesgo, permitiendo cierto margen de violaciones.

- ✓ **Controles detectivos:** Son aquellos que no evitan que ocurran las causas del riesgo sino que los detecta luego de ocurridos. Son los más importantes para el auditor. En cierta forma sirven para evaluar la eficiencia de los controles preventivos.

- ✓ **Controles Correctivos:** Ayudan a la investigación y corrección de las causas del riesgo. La corrección adecuada puede resultar difícil e ineficiente, siendo necesaria la implantación de controles detectivos sobre los controles correctivos, debido a que la corrección de errores es en sí una actividad altamente propensa a errores.

a. Planes de contingencia

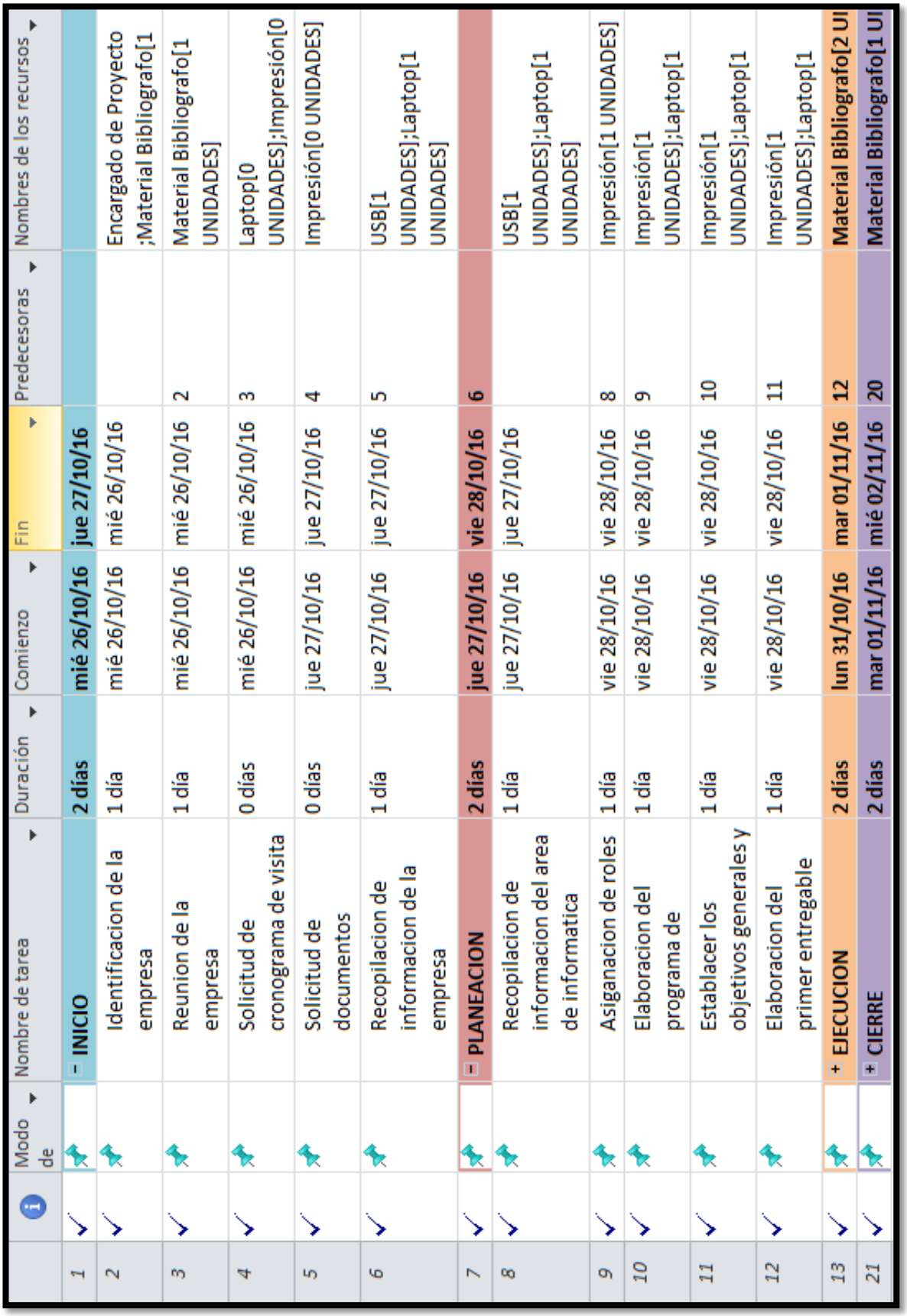
Dentro de las áreas generales, se establecen las siguientes divisiones de Auditoría Informática: de Explotación, de Sistemas, de Comunicaciones y de Desarrollo de Proyectos.

Cada área específica puede ser auditada desde los siguientes criterios generales:

- ✓ Desde su propio funcionamiento interno.
- ✓ Desde el apoyo que recibe de la Dirección y, en sentido ascendente, del grado de cumplimiento de las directrices de ésta.
- ✓ Desde la perspectiva de los usuarios, destinatarios reales de la informática.
- ✓ Desde el punto de vista de la seguridad que ofrece la Informática en general o la rama auditada.
- ✓ Estas combinaciones pueden ser ampliadas y reducidas según las características de la empresa auditada.

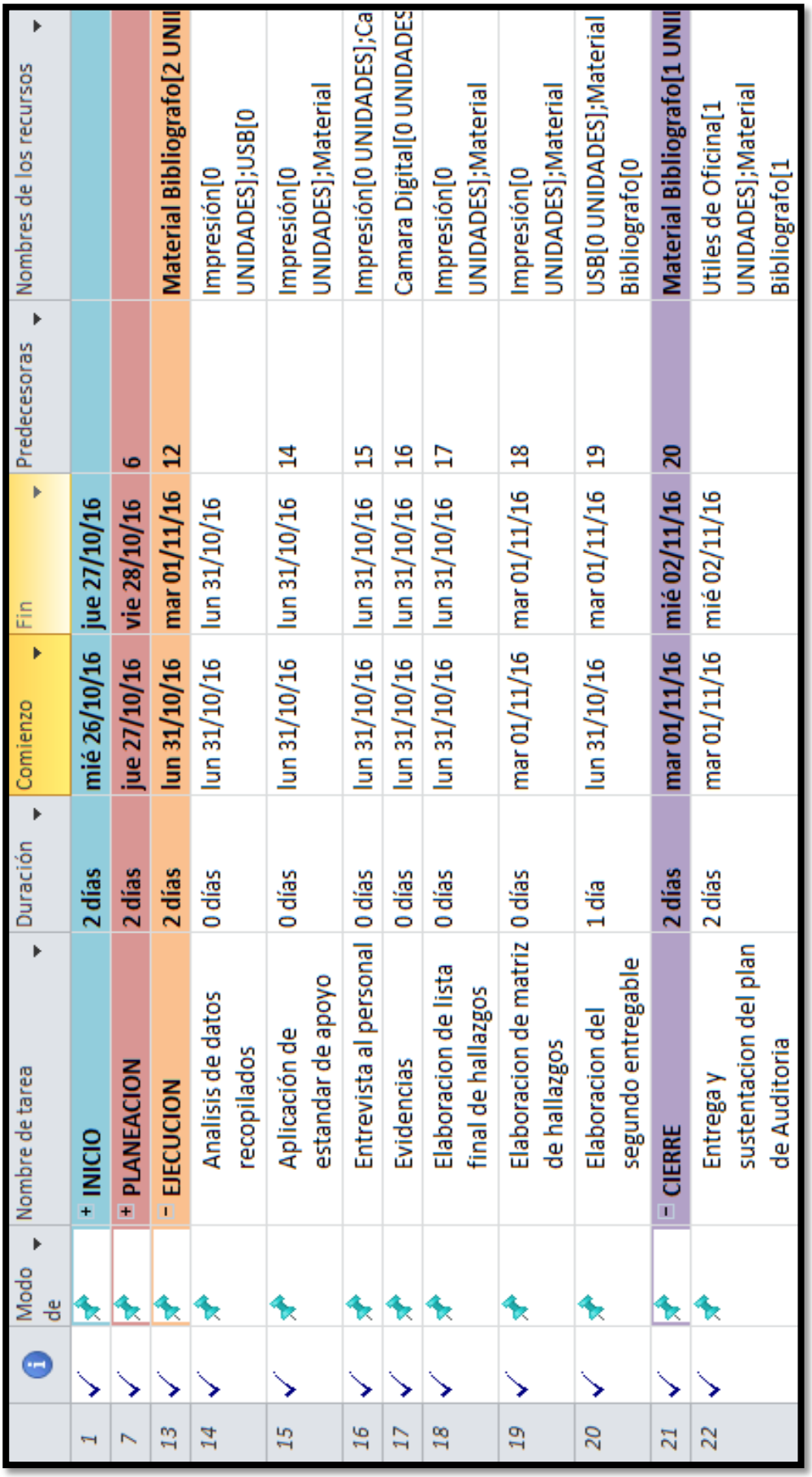
MATRIZ DE RIESGOS MAGERIT

2.8.1. DIAGRAMA DE GANTT



	Modo de	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras	Nombres de los recursos
1		**INICIO**	**2 días**	**mié 26/10/16**	**jue 27/10/16**		
2		Identificacion de la empresa	1 día	mié 26/10/16	mié 26/10/16		Encargado de Proyecto ;Material Bibliografo[1
3		Reunion de la empresa	1 día	mié 26/10/16	mié 26/10/16	2	Material Bibliografo[1 UNIDADES]
4		Solicitud de cronograma de visita	0 días	mié 26/10/16	mié 26/10/16	3	Laptop[0 UNIDADES];Impresión[0
5		Solicitud de documentos	0 días	jue 27/10/16	jue 27/10/16	4	Impresión[0 UNIDADES]
6		Recopilacion de informacion de la empresa	1 día	jue 27/10/16	jue 27/10/16	5	USB[1 UNIDADES];Laptop[1 UNIDADES]
7		**PLANEACION**	**2 días**	**jue 27/10/16**	**vie 28/10/16**	**6**	
8		Recopilacion de informacion del area de informatica	1 día	jue 27/10/16	jue 27/10/16		USB[1 UNIDADES];Laptop[1 UNIDADES]
9		Asiganacion de roles	1 día	vie 28/10/16	vie 28/10/16	8	Impresión[1 UNIDADES]
10		Elaboracion del programa de	1 día	vie 28/10/16	vie 28/10/16	9	Impresión[1 UNIDADES];Laptop[1
11		Establacer los objetivos generales y	1 día	vie 28/10/16	vie 28/10/16	10	Impresión[1 UNIDADES];Laptop[1
12		Elaboracion del primer entregable	1 día	vie 28/10/16	vie 28/10/16	11	Impresión[1 UNIDADES];Laptop[1
13		**EJECUCION**	**2 días**	**lun 31/10/16**	**mar 01/11/16**	**12**	**Material Bibliografo[2 UI**
21		**CIERRE**	**2 días**	**mar 01/11/16**	**mié 02/11/16**	**20**	**Material Bibliografo[1 UI**

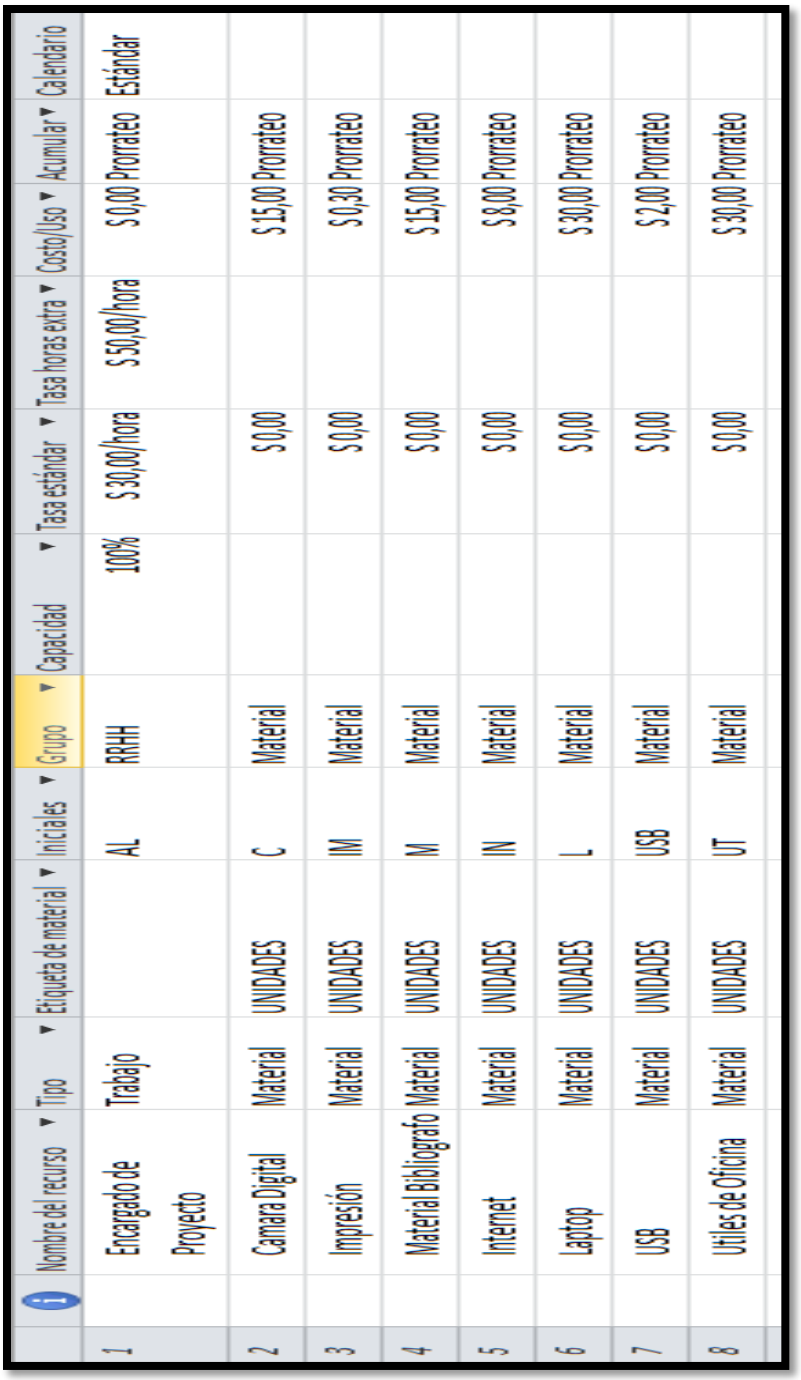
MATRIZ DE RIESGOS MAGERIT



	Modo de	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras	Nombres de los recursos
1		+ **INICIO**	**2 días**	**mié 26/10/16**	**jue 27/10/16**		
7		+ **PLANEACION**	**2 días**	**jue 27/10/16**	**vie 28/10/16**	**6**	
13		- **EJECUCION**	**2 días**	**lun 31/10/16**	**mar 01/11/16**	**12**	**Material Bibliografo[2 UNII**
14		Analisis de datos recopilados	0 días	lun 31/10/16	lun 31/10/16		Impresión[0 UNIDADES];USB[0
15		Aplicación de estandar de apoyo	0 días	lun 31/10/16	lun 31/10/16	14	Impresión[0 UNIDADES];Material
16		Entrevista al personal	0 días	lun 31/10/16	lun 31/10/16	15	Impresión[0 UNIDADES];Ca
17		Evidencias	0 días	lun 31/10/16	lun 31/10/16	16	Camara Digital[0 UNIDADES
18		Elaboracion de lista final de hallazgos	0 días	lun 31/10/16	lun 31/10/16	17	Impresión[0 UNIDADES];Material
19		Elaboracion de matriz de hallazgos	0 días	mar 01/11/16	mar 01/11/16	18	Impresión[0 UNIDADES];Material
20		Elaboracion del segundo entregable	1 día	lun 31/10/16	mar 01/11/16	19	USB[0 UNIDADES];Material Bibliografo[0
21		- **CIERRE**	**2 días**	**mar 01/11/16**	**mié 02/11/16**	**20**	**Material Bibliografo[1 UNII**
22		Entrega y sustentacion del plan de Auditoria	2 días	mar 01/11/16	mié 02/11/16		Utiles de Oficina[1 UNIDADES];Material Bibliografo[1

MATRIZ DE RIESGOS MAGERIT

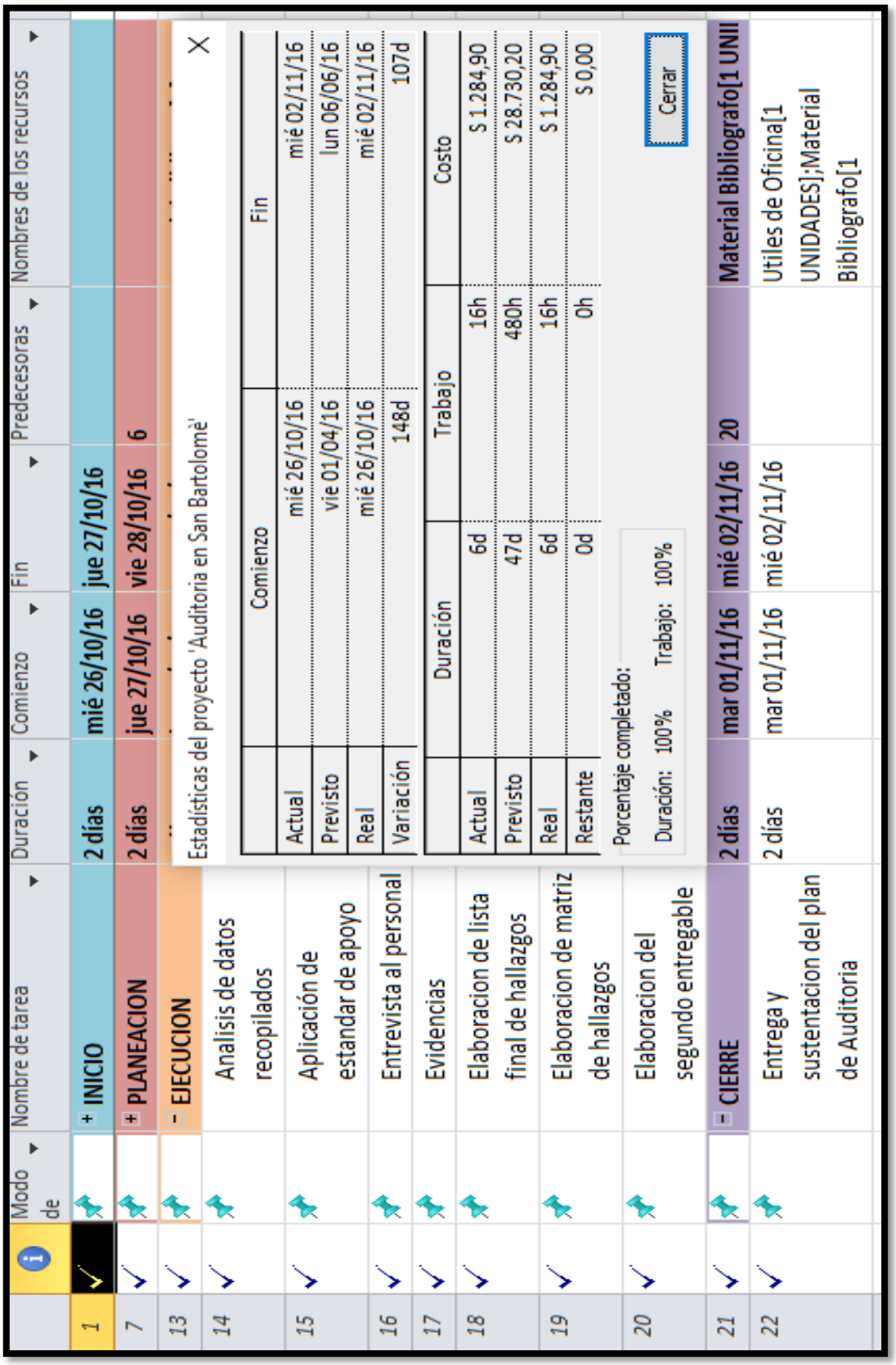
2.8.2. DIAGRAMA HOJA DE RECURSOS

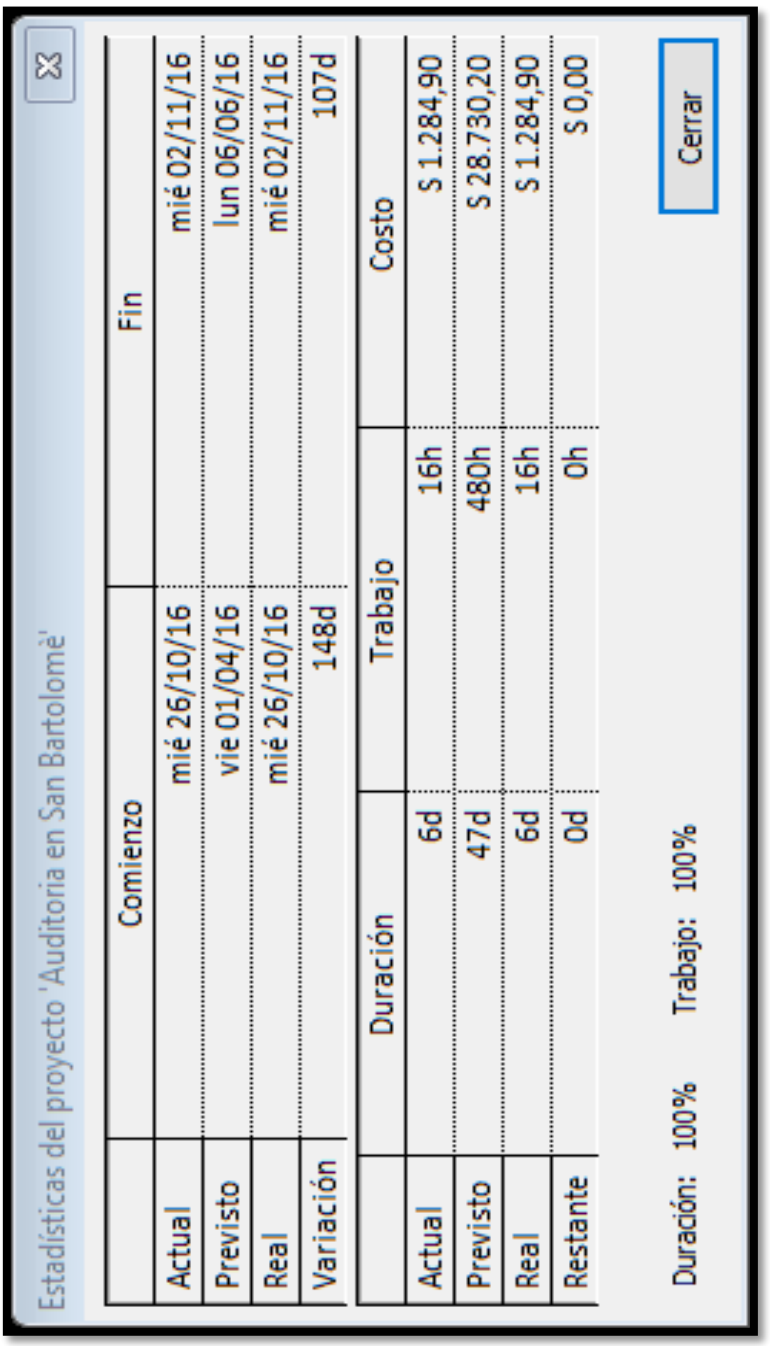


	Nombre del recurso	Tipo	Etiqueta de material	Iniciales	Grupo	Capacidad	Tasa estándar	Tasa horas extra	Costo/Uso	Acumular	Calendario
1	Encargado de Proyecto	Trabajo		AL	RRHH	100%	$30,00/hora	$50,00/hora	$0,00	Prorrateo	Estándar
2	Camara Digital	Material	UNIDADES	C	Material		$0,00		$15,00	Prorrateo	
3	Impresión	Material	UNIDADES	IM	Material		$0,00		$0,30	Prorrateo	
4	Material Bibliografo	Material	UNIDADES	M	Material		$0,00		$15,00	Prorrateo	
5	Internet	Material	UNIDADES	IN	Material		$0,00		$8,00	Prorrateo	
6	Laptop	Material	UNIDADES	L	Material		$0,00		$30,00	Prorrateo	
7	USB	Material	UNIDADES	USB	Material		$0,00		$2,00	Prorrateo	
8	Utiles de Oficina	Material	UNIDADES	UT	Material		$0,00		$30,00	Prorrateo	

MATRIZ DE RIESGOS MAGERIT

ESTADISTICA DEL PROYECTO




Estadísticas del proyecto 'Auditoria en San Bartolomè'
Comienzo
Fin
Actual
mié 26/10/16
mié 02/11/16
Previsto
vie 01/04/16
lun 06/06/16
Real
mié 26/10/16
mié 02/11/16
Variación
148d
107d
Duración
Trabajo
Costo
Actual
6d
16h
$ 1.284,90
Previsto
47d
480h
$ 28.730,20
Real
6d
16h
$ 1.284,90
Restante
0d
0h
$ 0,00
Duración: 100%
Trabajo: 100%
Cerrar

2.8.3. INFORMACION DEL PROYECTO

<table>
<tr><th colspan="3">PROGRAMA DE AUDITORÍA PARA EL HOSPITAL SAN BARTOLOME</th></tr>
<tr><th>ACTIVIDADES</th><th colspan="2">HORARIO APROXIMADO</th></tr>
<tr><td>Reunión Inicial</td><td colspan="2" rowspan="2">1 hora</td></tr>
<tr><td>Asistentes:
- Equipo auditor.
- Representante de la organización.</td></tr>
<tr><td>Objetivo:
- Presentación del equipo auditor.
- Presentación de la organización.
- Confirmación del programa de auditoría.</td><td colspan="2">1 hora</td></tr>
<tr><td rowspan="2">Tiempo Proyectado</td><td colspan="2">Fecha</td></tr>
<tr><td>Inicio</td><td>Fin</td></tr>
<tr><td>Reunión inicial con el responsable de área</td><td>26/10/16</td><td>27/10/16</td></tr>
<tr><td>Recopilación de información de la situación actual del área de redes</td><td>27/10/16</td><td>27/10/16</td></tr>
<tr><td>Entrega del plan de auditoría</td><td colspan="2">28/10/16</td></tr>
<tr><td>Estudio preliminar del área</td><td>28/10/13</td><td>28/10/16</td></tr>
<tr><td>Primer informe preliminar de auditoria</td><td colspan="2">28/10/16</td></tr>
<tr><td>Identificación de riesgos potenciales</td><td>28/10/16</td><td>28/10/16</td></tr>
<tr><td>Análisis de riesgos</td><td>29/10/16</td><td>29/10/16</td></tr>
<tr><td>Análisis del impacto</td><td>30/10/16</td><td>30/10/16</td></tr>
<tr><td>Elaboración del informe de auditoría</td><td>31/1016</td><td>01/11/16</td></tr>
<tr><td>Presentación del informe</td><td colspan="2">01/11/16</td></tr>
<tr><td>Reunión final</td><td colspan="2" rowspan="2">02 Noviembre del 2016</td></tr>
<tr><td>Asistentes:
- Equipo auditor.
- Representante de la organización.</td></tr>
<tr><td>Objeto:
- Dar lecturas de los resultados de la auditoría.
- Comentarios y aclaraciones.</td><td colspan="2">02 Noviembre del 2016</td></tr>
</table>

MATRIZ DE RIESGOS MAGERIT

EMPRESA	**HOSPITAL NACIONAL MADRE NIÑO SAN BARTOLOME**
DIRECCIÓN	AV. Alfonso Ugarte, Lima Central
ALCANCE	• ISO/ IEC 27001/2013 • NORMA TECNICA PERUANA (NTP) • ESTANDAR (MODELO OSI)
GRUPO AUDITOR	• CALDERON ALVARADO JERSON JOSEPH. • GARCIA PALACIOS ALEXANDER CLAUDE • CAMPOS CASTRO BRIAN • ORMEÑO JARAMILLO LUIS
FECHA AUDITORÍA	Del 26 de Octubre hasta el 02 de Noviembre del 2016
LUGAR	Área de Sistemas e Informática
DOCUMENTACIÓN DE REFERENCIA	NTP - EIA/TIA 568 A, EIA/TIA 568 B, EIA/TIA 569 , NTP-ISO/IEC 27001

III. DESARROLLO DE LA AUDITORIA

MATRIZ DE RIESGOS MAGERIT

3.1. DESCRIPCION DE LOS OBJETIVOS ESPECIFICOS Y ACTIVIDADES A REALIZAR PARA SU CUMPLIMIENTO

1. Identificar la cantidad de usuarios que tienen acceso a la red interna del hospital
   i. DESCRIPCION: En la revisión que se hizo en la seguridad lógica se pudo identificar que no se tiene un registro de la cantidad de usuarios que tienen acceso a la red interna del hospital.
   ii. ACTIVIDADES: Se debe de controlar e identificar los usuarios que tienen un usuario y que tienen acceso a la red interna del hospital.

2. Identificar la cantidad de usuarios creados con su contraseña
   i. DESCRIPCION: En la revisión que se hizo en la seguridad lógica se pudo identificar que no se tiene un registro de la cantidad de usuarios que existen y que tienen un equipo informático de disponibilidad en el hospital
   ii. ACTIVIDADES: Se debe de registrar la cantidad de usuarios que tienen una cuenta de acceso.

3. Identificar el nivel seguridad que tienen las contraseñas de los usuarios
   i. DESCRIPCION: En la revisión que se hizo en la seguridad lógica se pudo identificar que no se tiene un control de cantidad de caracteres para la contraseña que tiene el usuario en el hospital San Bartolomé
   ii. ACTIVIDADES: Se debe de establecer una cantidad mínima y máxima de caracteres y con una combinación de números, letras y caracteres especiales para mejorar y establecer una seguridad alta de cuenta

4. Identificar los niveles de privilegios de acceso que tienen los usuarios
   i. DESCRIPCION: En la revisión que se hizo en la seguridad lógica se pudo identificar que se tiene un control de los privilegios de acceso que tienen cada usuario para acceder a la red interna en el hospital San Bartolomé
   ii. ACTIVIDADES: Se debe de controlar y mejorar el nivel de acceso

que tiene cada usuario al acceso y privilegios que debe de tener a la red interna

5. Identificar el periodo de cambio de contraseñas de los usuarios
   i. DESCRIPCION: En la revisión que se hizo en la seguridad lógica se pudo identificar que se tiene un control de periodo de cambio de contraseñas emitiendo mensajes para que el usuario cambie su contraseña en el hospital San Bartolomé
   ii. ACTIVIDADES: Se debe de controlar y mejorar la modificación de contraseñas que tiene cada usuario.

6. Identificar si existe copias de seguridad de la información.
   i. DESCRIPCION: En la revisión que se hizo en la seguridad lógica se pudo identificar que la información cuenta con copias de seguridad de tipo continuas en el hospital San Bartolomé
   ii. ACTIVIDADES: Se debe de tener un registro de los días que se hacen copias de seguridad de la información y planear que días claves se tiene que realizar dichas copias de seguridad.

7. Identificar si el antivirus está activo
   i. DESCRIPCION: En la revisión que se hizo en la seguridad lógica se pudo identificar que algunos equipos informáticos no cuentan con el antivirus actualizado y que en algunos casos no se puede instalar por falta de estabilidad del servidor de antivirus en el hospital San Bartolomé
   ii. ACTIVIDADES: Se debe de tener un registro de aquellos equipos informáticos que están con el antivirus actualizado y que software son propensos a infectarse.

8. Identificar si los equipos cuentan con sistemas operativos actualizados
   i. DESCRIPCION: En la revisión que se hizo en la seguridad física se pudo identificar qué mayoría de los equipos informáticos no tienen su sistema operativo actualizado según lo que requiere el jefe del área de sistemas e informática en el hospital San Bartolomé
   ii. ACTIVIDADES: Se debe de tener un registro de aquellos equipos

informáticos que tiene su sistema operativo actualizado y aquellos que falten actualizar, según los requerimientos del equipo informático.

9. Identificar si existe la restricción de instalación de software
   i. DESCRIPCION: En la revisión que se hizo en la seguridad física se pudo identificar qué mayoría de los equipos informáticos tienen software instalados en los equipos informáticos sin autorización alguna en el hospital San Bartolomé
   ii. ACTIVIDADES: Se debe de tener normas de seguridad respecto a software instalables para que se pueda restringir esas instalaciones

10. Identificar si existe un control de inventario de los equipos informáticos.
    i. DESCRIPCION: En la revisión que se hizo en la seguridad física se pudo identificar qué no se tiene registrado la cantidad de equipos informáticos en un inventario en el hospital San Bartolomé
    ii. ACTIVIDADES: Se debe de tener un registro de aquellos equipos informáticos que tiene su sistema operativo actualizado y aquellos que falten actualizar, según los requerimientos del equipo informático.

11. Identificar si existe mantenimiento preventivo y correctivo de los equipos informáticos.
    i. DESCRIPCION: En la revisión que se hizo en la seguridad física se pudo identificar que no se tiene un plan preventivo de los equipos informáticos en el hospital San Bartolomé
    ii. ACTIVIDADES: Se debe de tener un plan preventivo y correctivo de los equipos informáticos para evitar equipos en estado de inoperatividad.

12. Identificar si existen equipos con garantía
    i. DESCRIPCION: En la revisión que se hizo en la seguridad física se pudo identificar que no se tiene un registro de los equipos informáticos que se encuentran en garantía en el hospital San Bartolomé

ii. ACTIVIDADES: Se debe de tener un registro anual de aquellos equipos que se van quedando sin garantía, para que días previos hacerle su mantenimiento respectivo según el tipo de garantía.

13. Identificar la correcta ubicación de los cables de red con la finalidad de evitar inferencia.
    i. DESCRIPCION: En la revisión que se hizo en la seguridad física, preguntando por alguna documentación en plan de contingencia respecto a la red, se pudo observar que esta no cuenta con un plan respecto al tema, dado que ellos cuentan que no ha existido problema con la red, solo con los puertos de red al momento de identificarlos.
    ii. ACTIVIDADES: Realizar un plan de contingencia para la caída de red, en este caso señalar en que momento reiniciar los servidores y si es posible activar un back-up de respaldo

14. Identificar si existe un ordenamiento estructurado en los gabinetes.
    i. DESCRIPCION: En la revisión que se hizo en la seguridad física se pudo identificar que no se tiene implementado los estándares de cableado estructurado en los gabinetes en el hospital San Bartolomé
    ii. ACTIVIDADES: Se debe de implementar los estándares de cableado estructurado para tener un mejor control de los puertos de acceso de los switch.

15. Identificar la situación actual de la sala de servidores
    i. DESCRIPCION: En la revisión que se hizo en la seguridad física se pudo identificar que no se tienen los estándares para la sala de servidores ya sea en energía eléctrica, aire acondicionado, cableado estructurado y espacio en el hospital San Bartolomé
    ii. ACTIVIDADES: Se debe de implementar las normas y estándares internacionales para un mejor control y administración de ello.

16. Identificar los puntos vulnerables del cableado estructurado y los riesgos que esto implica en la seguridad de la red para que no haya robo de información.
    i. DESCRIPCION: La revisión y análisis de la información proporcionada por el hospital San Bartolomé, evidencia lo siguiente que supuestamente las áreas están separadas, sin embargo las conexiones de red no tienen restricciones, en la cual todas las áreas están conectadas en red, permitiendo la intrusión de un usuario desde otra área.
    ii. ACTIVIDADES: Disponer del personal capacitado para la gestión de redes que realicen un estudio en la conectividad de las redes entre las distintas áreas del hospital San Bartolomé dividiéndolas en VLAN's, para un mayor control en la seguridad de la información y la eficiencia de las comunicaciones, aislando los procesos vulnerables a malversación de datos.

17. Identificar la operatividad de la red en el hospital.
    i. DESCRIPCION: En la revisión que se hizo en la seguridad de redes se identificó que la red es inestable en el hospital San Bartolomé
    ii. ACTIVIDADES: Se debe de identificar cuáles son los recursos que inestabilizan la red y poder administrarla de una mejor manera.

18. Identificar la seguridad de los correos corporativos que llegan a su destino
    i. DESCRIPCION: En la revisión que se hizo en la seguridad de redes se identificó que los mensajes llegan con seguridad a su usuario final en el hospital San Bartolomé
    ii. ACTIVIDADES: Se debe de registrar el periodo de envío y llegada de los mensajes que llegan a los usuarios finales.

19. Identificar si cuenta con políticas y normas de seguridad de información
    i. DESCRIPCION: En la revisión que se hizo en la seguridad de redes se identificó que la seguridad de redes no cuenta con todas las políticas de seguridad por el motivo que no se tiene una documentación de políticas y normas de seguridad en el hospital San Bartolomé
    ii. ACTIVIDADES: Se debe de crear y aprobar una documentación de

políticas y normas de seguridad informática.

20. Identificar la clave de los servidores
    i. DESCRIPCION: En la revisión que se hizo en la seguridad de redes se identificó que no se tiene un registro de las contraseñas que se modifican en los servidores del área de servidores en el hospital San Bartolomé
    ii. ACTIVIDADES: Se debe de implementar un procedimiento de resguardo de sobres sellados donde solo lo tenga el jefe de informatica en su escritorio mediante llaves.

21. Identificar planes para mitigar los riesgos de la red
    i. DESCRIPCION: En la revisión que se hizo en la seguridad de redes se identificó que no se tiene un plan personal y general para mitigar los riesgos de la red en el hospital San Bartolomé
    ii. ACTIVIDADES: Se debe documentar por cada servidor unos procedimientos de fallas para poder resolver dichas fallas.

3.2. DESCRIPCION DE LA METODOLOGIA UTLIZADA PARA CADA OBJETIVO ESPECÍFICO

1. Identificar la cantidad de usuarios que tienen acceso a la red interna del hospital

   Norma ISO/IEC 27001:2013

   En el punto 9.4. (Control de Acceso a la Red) refiere que hay que asegurarse que el acceso de los usuarios a las redes y sus servicios no comprometan la seguridad de dichos servicios

2. Identificar la cantidad de usuarios creados con su contraseña

   Norma ISO/IEC 27001:2013

   En el punto 9.4. (Control de Acceso a la Red) refiere que hay que asegurarse que el acceso de los usuarios a las redes y sus servicios no comprometan la seguridad de dichos servicios

3. Identificar el nivel seguridad que tienen las contraseñas de los usuarios

   Norma ISO/IEC 27001:2013

   En el punto 9.4. (Control de Acceso a la Red) refiere que hay que asegurarse que el acceso de los usuarios a las redes y sus servicios no comprometan la seguridad de dichos servicios

4. Identificar los niveles de privilegios de acceso que tienen los usuarios

   Norma ISO/IEC 27001:2013

   En el punto 9.4. (Control de Acceso a la Red) refiere que hay que asegurarse que el acceso de los usuarios a las redes y sus servicios no comprometan la seguridad de dichos servicios

5. Identificar el periodo de cambio de contraseñas de los usuarios

   Norma ISO/IEC 27001:2013

   En el punto 9.4. (Control de Acceso a la Red) refiere que hay que asegurarse que el acceso de los usuarios a las redes y sus servicios no comprometan la seguridad de dichos servicios

6. Identificar si los equipos cuentan con sistemas operativos actualizados

   Norma ISO/IEC 27001:2013

   En el punto 14 (Adquisición, desarrollo y mantenimiento de sistemas) se refiere que hay que tener un plan preventivo y correctivo para los equipos informáticos, dado que no se tiene que perjudicar la operatividad de la red y las actividades de los usuarios.

7. Identificar si existe la restricción de instalación de software

   Norma ISO/IEC 27001:2013

   En el punto 12.6.2 (Restricciones en la instalación de software) se refiere que hay que tener permisos de la alta dirección para poder instalar un software ajeno a los requerimientos que tiene la organización y documentación del uso que se quiera dar al software

8. Identificar si existe un control de inventario de los equipos informáticos.

   Norma ISO/IEC 27001:2013

   En el punto 14 (Adquisición, desarrollo y mantenimiento de sistemas) se refiere que hay que tener un plan preventivo y correctivo para los equipos informáticos, dado que no se tiene que perjudicar la operatividad de la red y las actividades de los usuarios.

9. Identificar si existe mantenimiento preventivo y correctivo de los equipos informáticos.

   Norma ISO/IEC 27001:2013

   En el punto 14 (Adquisición, desarrollo y mantenimiento de sistemas) se refiere que hay que tener un plan preventivo y correctivo para los equipos informáticos, dado que no se tiene que perjudicar la operatividad de la red y las actividades de los usuarios.

10. Identificar si existen equipos con garantía

    Norma ISO/IEC 27001:2013

    En el punto 14 (Adquisición, desarrollo y mantenimiento de sistemas) se refiere que hay que tener un plan preventivo y correctivo para los equipos informáticos, dado que no se tiene que perjudicar la operatividad de la red

y las actividades de los usuarios.

Norma ISO/IEC 27001:2013

En el punto 15 (Relaciones con proveedores) se refiere que hay que tener comunicación con los proveedores para poder solicitar las partes de los equipos informáticos,

11. Identificar si existe copias de seguridad de la información.

    Norma ISO/IEC 27001:2013

    En el punto 12 (seguridad en las operaciones) se refiere que hay que tener una operatividad correcta y eficaz de la red para no afectar a los procesos de información

12. Identificar si el antivirus está activo

    Norma ISO/IEC 27001:2013

    En el punto 12 (seguridad en las operaciones) se refiere que hay que tener una operatividad correcta y eficaz de la red para no afectar a los procesos de información

13. Identificar la correcta ubicación de los cables de red con la finalidad de evitar inferencia.

    Norma ISO/IEC 27001:2013

    En el punto 11 (Seguridad física y ambiental) Indica los controles para la protección contra interceptaciones o daños el cableado de energía y telecomunicaciones que transporten datos o soporten servicios de información.

14. Identificar si existe un ordenamiento estructurado en los gabinetes

    ANSI/TIA/EIA-569

    El estándar provee especificaciones para el diseño de las instalaciones y la infraestructura edilicia necesaria para el cableado de telecomunicaciones en edificios.

15. Identificar la situación actual de la sala de servidores

    Tanto los estándares ISO como los estándares ANSI/TIA/EIA exigen administrar las instalaciones, incluyendo el equipo de comunicaciones, está referido a las prácticas de diseños y construcción las cuales darán soporte a los medios de transmisión y al área de trabajo correcto. Estos estándares permitirán instalar una planta de cableado estructurado genérico que podrá hacer funcionar cualquier aplicación de datos y de voz, cumpliendo con la seguridad y ciertas restricciones.

    ANSI/TIA/EIA-569

    Determina los diferentes métodos para implementar el cableado estructurado. Respetando las reglas para las implementaciones y medidas que el estándar propone para la correcta implementación de un cableado estructurado.

16. Identificar los puntos vulnerables del cableado estructurado y los riesgos que esto implica en la seguridad de la red para que no haya robo de información.

    Norma ISO/IEC 27001:2013

    En el punto 11 (Seguridad física y ambiental) Indica los controles para la protección contra interceptaciones o daños el cableado de energía y telecomunicaciones que transporten datos o soporten servicios de información.

    Norma ISO/IEC 27001:2013

    En el punto 9 (Control de acceso) Se debería controlar la configuración y el acceso físico y lógico a los puertos de diagnóstico.

17. Identificar la operatividad de la red en el hospital.

    Norma ISO/IEC 27001:2013

    En el punto 12 (seguridad en las operaciones) se refiere que hay que tener una operatividad correcta y eficaz de la red para no afectar a los procesos de información

18. Identificar la seguridad de los correos que llegan a su destino

    Norma ISO/IEC 27001:2013

    En el punto 12 (seguridad en las operaciones) se refiere que hay que tener una operatividad correcta y eficaz de la red para no afectar a los procesos de información

19. Identificar si cuenta con políticas y normas de seguridad de información

    Norma ISO/IEC 27001:2013

    En el punto 5 (Políticas de seguridad de la información) se refiere que hay que tener un documento de las políticas de seguridad e implementarlas dentro de nuestra red interna

20. Identificar la clave de los servidores

    Norma ISO/IEC 27001:2013

    En el punto 9.4. (Control de Acceso a la Red) refiere que hay que asegurarse que el acceso de los usuarios a las redes y sus servicios no comprometan la seguridad de dichos servicios

21. Identificar planes para mitigar los riesgos de la red

    Norma ISO/IEC 27001:2013

    En el punto 8 (Gestión de activos) refiere que hay que tener documentado los activos de información para no depender de personas que falten a sus labores y poder administrar de una manera perfecta los equipos intermedios y administración de la red interna de la organización.

3.3. CLASIFICACION DE LOS HALLAZGOS POR TIPO

MATRIZ DE RIESGOS MAGERIT

NUMERO	HALLAZGO	TIPO
1	No hay un registro para la cantidad de usuarios que tienen acceso a la red interna	SATISFACCION
2	No hay un registro para la cantidad de usuarios creados con su contraseña	SATISFACCION
3	No hay un control para el nivel de seguridad de las contraseñas de los usuarios	SATISFACCION
4	Falta medidas adicionales para controlar los niveles de privilegios de acceso	SATISFACCION
5	Falta de medidas adicionales para controlar el cambio de contraseña de los usuarios	SATISFACCION
6	Mejorar las copias de seguridad de la informacion	NOMINAL
7	Falta de medidas adicionales para que el antivirus este activo	SATISFACCION
8	Falta de control de los equipos que cuentan con sistema operativo actualizado	NOMINAL
9	No hay un control para la restriccion de instalacion de software	SATISFACCION
10	Carencia de inventario en el área de TI	NOMINAL
11	No hay un mantenimiento preventivo a los equipos informaticos	NOMINAL
12	Falta de medidas adicionales para controlar los equipos en garantia	NOMINAL
13	No hay una correcta ubicación de los cables de red	VALORATIVO
14	No hay un ordenamiento estructurado en los gabinetes	VALORATIVO
15	No hay un control de acceso de la situacion actual de la sala de servidores	SATISFACCION
16	No hay un control de los puntos vulnerables y riesgos que ocasionaria el cableado estructurado	VALORATIVO
17	Deficiente control en la operatividad de la red	VALORATIVO
18	Falta medidas adicionales para la seguridad de los correos corporativos	NOMINAL
19	No cuenta con politicas y normas de seguridad de informacion	SATISFACCION
20	Administracion incorrecta de claves de los servdores	SATISFACCION
21	No cuenta con procedimiento para fallas de red en la infraestrutura de red	SATISFACCION

3.4. HALLAZGOS INICIALES

1. No hay un registro para la cantidad de usuarios que tienen acceso a la red interna
2. No hay un registro para la cantidad de usuarios creados con su contraseña
3. No hay un control para el nivel de seguridad de las contraseñas de los usuarios
4. Falta medidas adicionales para controlar los niveles de privilegios de acceso
5. Falta de medidas adicionales para controlar el cambio de contraseña de los usuarios
6. Falta de control de los equipos que cuentan con sistema operativo actualizado
7. No hay un control para la restricción de instalación de software
8. Carencia de inventario en el área de TI
9. No hay un mantenimiento preventivo a los equipos informáticos
10. Falta de medidas adicionales para controlar los equipos en garantía
11. Mejorar las copias de seguridad de la información
12. Falta de medidas adicionales para que el antivirus este activo
13. No hay una correcta ubicación de los cables de red
14. No hay un ordenamiento estructurado en los gabinetes
15. No hay un control de la situación actual de la sala de servidores
16. No hay un control de los puntos vulnerables y riesgos que ocasionaría el cableado estructurado
17. Deficiente control en la operatividad de la red
18. Falta medidas adicionales para la seguridad de los correos corporativos
19. No cuenta con políticas y normas de seguridad de información
20. No hay una gestión de la clave de los servidores
21. No hay planes para mitigar los riesgos de la red

3.5. ANALISIS DE LOS HALLAZGOS INICIALES

1. No hay un registro para la cantidad de usuarios que tienen acceso a la red interna

ANALISIS: Se utilizara este hallazgo porque es fundamental para el hospital poder identificar y controlar quienes son los usuarios que tienen disponibilidad de los servicios que ofrece la red interna

2. No hay un registro para la cantidad de usuarios creados con su contraseña

ANALISIS: Se utilizara este hallazgo porque es fundamental para el hospital poder identificar cuantos usuarios tienen una cuenta para poder realizar sus actividades diarias en un equipo informático de escritorio.

3. No hay un control para el nivel de seguridad de las contraseñas de los usuarios

ANALISIS: Se utilizara este hallazgo porque es fundamental para el hospital poder proteger la información que cada usuario genera en su actividad diaria, con la finalidad de establecer medidas de seguridad en la estructura de la contraseña generada por cada usuario.

4. Falta medidas adicionales para controlar los niveles de privilegios de acceso

ANALISIS: Se utilizara este hallazgo porque es fundamental para el hospital saber que usuarios tienen los privilegios de acceso a los servicios que brinda la red interna y poder clasificarlos según el privilegio de usuario.

5. Falta de medidas adicionales para controlar el cambio de contraseña de los usuarios

ANALISIS: Se utilizara este hallazgo porque es fundamental para el hospital saber que usuarios cambian su contraseña para proteger su información y además quienes hacen caso a las normas de seguridad que el área de informática plantea.

6. Mejorar las copias de seguridad de la información

ANALISIS: No se utilizara este hallazgo porque presentara costos al momento de incorporar discos duros robustos para poder almacenar la información en caso el servidor de back-up deje de funciona, pero este hallazgo es fundamental para el hospital porque es muy importante velar y garantizar la seguridad de la información en el hospital, mediante copias de respaldo según los niveles de información que se tengan en disponibilidad,

7. Falta de medidas adicionales para que el antivirus este activo

ANALISIS: Se utilizara este hallazgo porque es fundamental para el hospital poder identificar las amenazas del virus en la información para poder mitigarlos de una manera eficaz, práctica y sencilla.

8. Falta de control de los equipos que cuentan con sistema operativo actualizado

ANALISIS: No se utilizara este hallazgo porque representara costo al momento de adquirir un software especializado o tener un plan de equipos para poder actualizar los sistemas operativos de ellos, pero este hallazgo es fundamental para el hospital saber que equipos cuentan con la disponibilidad de poder tener su sistema operativo actualizado y que equipos resisten a dicha actualización.

9. No hay un control para la restricción de instalación de software

ANALISIS: Se utilizara este hallazgo porque es fundamental para el hospital implementar controles para que ningún usuario deba instalar algún software ajenos a los que el hospital establece y usa para la ejecución de sus procesos, en caso a ello el usuario debe de enviar un documento del software que desee instalar y el motivo del uso.

10. Carencia de inventario en el área de TI

ANALISIS: No se utilizara este hallazgo porque generará tiempo en pedir permisos a todas las áreas y generar procedimientos para poder inventariar los equipos informáticos, pero este hallazgo es fundamental

para él hospital saber con cuantos equipos cuenta como disponibilidad inmediata en caso uno presente fallas, además tener una visión del presupuesto que generara poder adquirir nuevos equipos informáticos.

11. No hay un mantenimiento preventivo a los equipos informáticos

ANALISIS: Se utilizara este hallazgo porque es fundamental para el hospital poder realizar un mantenimiento preventivo de los equipos con la finalidad de evitar fallas de ellos, esto estaría de la mano junto al inventario de TI,

12. Falta de medidas adicionales para controlar los equipos en garantía

ANALISIS: No se utilizara este hallazgo porque esta enlazado con el inventario de quipos información, pero este hallazgo es fundamental para el hospital saber que equipos cuentan con garantía para poder pedir repuestos de ellos con la finalidad de poder hacer un mantenimiento preventivo.

13. No hay una correcta ubicación de los cables de red

ANALISIS: No se utilizara este hallazgo porque generara costos al momento de adquirir herramientas para el cableado estructurado, pero este hallazgo es fundamental para el hospital para poder tener una estructura de ordenamiento adecuada y para próximas auditorias de seguridad física.

14. No hay un ordenamiento estructurado en los gabinetes

ANALISIS: Se utilizara este hallazgo porque es fundamental para el hospital poder identificar los puertos de red del switch con disponibilidad a ser usado por un nuevo usuario.

15. No hay un control de la situación actual de la sala de servidores

ANALISIS: Se utilizara este hallazgo porque es fundamental para el hospital poder implementar un libro de control de acceso para poder identificar que usuarios entran a la sala de servidores y que hacen dentro de ella.

16. No hay un control de los puntos vulnerables y riesgos que ocasionaría el cableado estructurado

ANALISIS: No se utilizara este hallazgo porque generara costo al adquirir llaves de seguridad para el control de puertos de red o adquirir algún switch de capa 3 para poder administrar los puertos de red, pero este hallazgo es fundamental para el hospital porque permite identificar cuáles son los puntos de red más vulnerables y propensos a ser utilizados por terceros y poder tener un robo de información o infiltración en la red interna del hospital.

17. Deficiente control en la operatividad de la red

ANALISIS: No se utilizara este hallazgo a pesar que es muy importe porque generara costo al momento de adquirir algunos switch de capa 3 para poder implementar las vlan, pero este hallazgo es fundamental para el hospital porque permite mantener la operatividad de la red en buen estado, para que los usuarios puedan realizar sus actividades diarias sin retraso alguno.

18. Falta medidas adicionales para la seguridad de los correos corporativos

ANALISIS: No se utilizara este hallazgo porque generara costo al adquirir dispositivos de almacenamiento, este hallazgo va enlazado con el hallazgo número 6, pero este hallazgo es fundamental para el hospital porque permite mantener seguro los correos que envían a los usuarios finales, dado que es importante velar por la información personal de cada paciente y/o proceso interno que realice el hospital.

19. No cuenta con políticas y normas de seguridad de información

ANALISIS: Se utilizara este hallazgo porque es fundamental para el hospital tener una documentación acerca de las políticas de seguridad de información que el área de informatica establece y en donde los usuarios acaten las normas de seguridad de información.

20. No hay una gestión de la clave de los servidores

ANALISIS: Se utilizara este hallazgo porque es fundamental para el hospital saber cuáles son las contraseñas de los servidores y gestionarlas mediantes sobres donde el único autorizado en tenerlas sea el jefe del área de informatica.

21. No hay planes para mitigar los riesgos de la red

ANALISIS: Se utilizara este hallazgo porque es fundamental para el hospital saber cuáles son las medidas de mitigación de riesgos que tienen cada uno de los encargados del área de informatica.

3.6. RELACION DE LOS HALLAZGOS FINALES

1. No hay un registro para la cantidad de usuarios que tienen acceso a la red interna
2. No hay un registro para la cantidad de usuarios creados con su contraseña
3. No hay un control para el nivel de seguridad de las contraseñas de los usuarios
4. Falta medidas adicionales para controlar los niveles de privilegios de acceso
5. Falta de medidas adicionales para controlar el cambio de contraseña de los usuarios
6. Falta de medidas adicionales para que el antivirus este activo
7. No hay un control para la restricción de instalación de software
8. No hay un mantenimiento preventivo a los equipos informáticos
9. No hay un ordenamiento estructurado en los gabinetes
10. No hay un control de la situación actual de la sala de servidores
11. No cuenta con políticas y normas de seguridad de información
12. Administración incorrecta de claves de los servidores
13. No cuenta con procedimiento para falla de red en la infraestructura de red

MATRIZ DE RIESGOS MAGERIT

MATRIZ DE ANALISIS DE HALLAZGOS

MATRIZ DE ANALISIS DE HALLAZGOS						
N°	**HALLAZGO**	**TIPO**	**DESCRIPCIÓN**	**OBJETIVO**	**NORMATIVA**	**EVIDENCIA**
1	No hay un registro para la cantidad de usuarios que tienen acceso a la red interna	SATISFACCION	En la revisión que se hizo en la seguridad lógica se pudo identificar que no se tiene un registro de la cantidad de usuarios que tienen acceso a la red interna del hospital.	Identificar la cantidad de usuarios que tienen acceso a la red interna del hospital	**Norma ISO/IEC 27001:2013** En el punto 9.4. (Control de Acceso a la Red) refiere que hay que asegurarse que el acceso de los usuarios a las redes y sus servicios no comprometan la seguridad de dichos servicios	ENTREVISTA: PREGUNTA 1
2	No hay un registro para la cantidad de usuarios creados con su contraseña	SATISFACCION	En la revisión que se hizo en la seguridad lógica se pudo identificar que no se tiene un registro de la cantidad de usuarios que existen y que tienen un equipo informático de disponibilidad en el hospital	Identificar la cantidad de usuarios creados con su contraseña	**Norma ISO/IEC 27001:2013** En el punto 9.4. (Control de Acceso a la Red) refiere que hay que asegurarse que el acceso de los usuarios a las redes y sus servicios no comprometan la seguridad de dichos servicios	ENTREVISTA: PREGUNTA 2
3	No hay un control para el nivel de seguridad de las contraseñas de los usuarios	SATISFACCION	En la revisión que se hizo en la seguridad lógica se pudo identificar que no se tiene un control de cantidad de caracteres para la contraseña que tiene el usuario en el hospital San Bartolomé	Identificar el nivel seguridad que tienen las contraseñas de los usuarios	**Norma ISO/IEC 27001:2013** En el punto 9.4. (Control de Acceso a la Red) refiere que hay que asegurarse que el acceso de los usuarios a las redes y sus servicios no comprometan la seguridad de dichos servicios	ENTREVISTA: PREGUNTA 3
4	Falta medidas adicionales para controlar los niveles de privilegios de acceso	SATISFACCION	En la revisión que se hizo en la seguridad lógica se pudo identificar que se tiene un control de los privilegios de acceso que tienen cada usuario para acceder a la red interna en el hospital San Bartolomé	Identificar los niveles de privilegios de acceso que tienen los usuarios	**Norma ISO/IEC 27001:2013** En el punto 9.4. (Control de Acceso a la Red) refiere que hay que asegurarse que el acceso de los usuarios a las redes y sus servicios no comprometan la seguridad de dichos servicios	ENTREVISTA: PREGUNTA 4
5	Falta de medidas adicionales para controlar el cambio de contraseña de los usuarios	SATISFACCION	En la revisión que se hizo en la seguridad lógica se pudo identificar que se tiene un control de periodo de cambio de contraseñas emitiendo mensajes para que el usuario cambie su contraseña en el hospital San Bartolomé	Identificar el periodo de cambio de contraseñas de los usuarios	**Norma ISO/IEC 27001:2013** En el punto 9.4. (Control de Acceso a la Red) refiere que hay que asegurarse que el acceso de los usuarios a las redes y sus servicios no comprometan la seguridad de dichos servicios	ENTREVISTA: PREGUNTA 5

MATRIZ DE RIESGOS MAGERIT

6	Mejorar las copias de seguridad de la informacion	NOMINAL	En la revisión que se hizo en la seguridad lógica se pudo identificar que la información cuenta con copias de seguridad de tipo continuas en el hospital San Bartolomé	Identificar si existe copias de seguridad de la información.	**Norma ISO/IEC 27001:2013 En el punto 14 (Adquisición, desarrollo y mantenimiento de sistemas)** se refiere que hay que tener un plan preventivo y correctivo para los equipos informáticos, dado que no se tiene que perjudicar la operatividad de la red y las actividades de los usuarios.	DOCUMENTO 1 :PLAN DE CONTINGENCIA "PROCEDIMIENTO DE DATOS A RECUPERAR"
7	Falta de medidas adicionales para que el antivirus este activo	SATISFACCION	En la revisión que se hizo en la seguridad lógica se pudo identificar que algunos equipos informáticos no cuentan con el antivirus actualizado y que en algunos casos no se puede instalar por falta de estabilidad del servidor de antivirus en el hospital San Bartolomé	Identificar si el antivirus está activo	**Norma ISO/IEC 27001:2013 En el punto 12.6.2 (Restricciones en la instalación de software)** se refiere que hay que tener permisos de la alta dirección para poder instalar un software ajeno a los requerimientos que tiene la organización y documentación del uso que se quiera dar al software	ENTREVISTA: PREGUNTA 6
8	Falta de control de los equipos que cuentan con sistema operativo actualizado	NOMINAL	En la revisión que se hizo en la seguridad física se pudo identificar qué mayoría de los equipos informáticos no tienen su sistema operativo actualizado según lo que requiere el jefe del área de sistemas e informática en el hospital San Bartolomé	Identificar si los equipos cuentan con sistemas operativos actualizados	**Norma ISO/IEC 27001:2013 En el punto 14 (Adquisición, desarrollo y mantenimiento de sistemas)** se refiere que hay que tener un plan preventivo y correctivo para los equipos informáticos, dado que no se tiene que perjudicar la operatividad de la red y las actividades de los usuarios.	DOCUMENTO 1 :PLAN DE CONTINGENCIA "PROCEDIMIENTO DE DATOS A RECUPERAR"
9	No hay un control para la restriccion de instalacion de software	VALORATIVO	En la revisión que se hizo en la seguridad física se pudo identificar qué mayoría de los equipos informáticos tienen software instalados en los equipos informáticos sin autorización alguna en el hospital San Bartolomé	Identificar si existe la restricción de instalación de software	**Norma ISO/IEC 27001:2013 En el punto 14 (Adquisición, desarrollo y mantenimiento de sistemas)** se refiere que hay que tener un plan preventivo y correctivo para los equipos informáticos, dado que no se tiene que perjudicar la operatividad de la red y las actividades de los usuarios.	ENTREVISTA: PREGUNTA 7
10	Carencia de inventario en el área de TI	NOMINAL	En la revisión que se hizo en la seguridad física se pudo identificar qué no se tiene registrado la cantidad de equipos informáticos en un inventario en el hospital San Bartolomé	Identificar si existe un control de inventario de los equipos informáticos.	**Norma ISO/IEC 27001:2013 En el punto 14 (Adquisición, desarrollo y mantenimiento de sistemas)** se refiere que hay que tener un plan preventivo y correctivo para los equipos informáticos, dado que no se tiene que perjudicar la operatividad de la red y las actividades de los usuarios. **Norma ISO/IEC 27001:2013 En el punto 15 (Relaciones con proveedores)** se refiere que hay que tener comunicación con los proveedores para poder solicitar las partes de los equipos informáticos,	DOCUMENTO 1 :PLAN DE CONTINGENCIA "PROCEDIMIENTO DE DATOS A RECUPERAR"

11	No hay un mantenimiento preventivo a los equipos informaticos	NOMINAL	En la revisión que se hizo en la seguridad física se pudo identificar que no se tiene un plan preventivo de los equipos informáticos en el hospital San Bartolomé	Identificar si existe mantenimiento preventivo y correctivo de los equipos informáticos.	**Norma ISO/IEC 27001:2013** **En el punto 12 (seguridad en las operaciones)** se refiere que hay que tener una operatividad correcta y eficaz de la red para no afectar a los procesos de información	DOCUMENTO 1 :PLAN DE CONTINGENCIA "PROCEDIMIENTO DE DATOS A RECUPERAR"
12	Falta de medidas adicionales para controlar los equipos en garantia	NOMINAL	En la revisión que se hizo en la seguridad física se pudo identificar que no se tiene un registro de los equipos informáticos que se encuentran en garantía en el hospital San Bartolomé	Identificar si existen equipos con garantía	**Norma ISO/IEC 27001:2013** **En el punto 12 (seguridad en las operaciones)** se refiere que hay que tener una operatividad correcta y eficaz de la red para no afectar a los procesos de información	DOCUMENTO 1 :PLAN DE CONTINGENCIA "CENTRO DE COMPUTO ALTERNATIVO"
13	No hay una correcta ubicación de los cables de red	VALORATIVO	En la revisión que se hizo en la seguridad física, preguntando por alguna documentación en plan de contingencia respecto a la red, se pudo observar que esta no cuenta con un plan respecto al tema, dado que ellos cuentan que no ha existido problema con la red, solo con los puertos de red al momento de identificarlos.	Identificar la correcta ubicación de los cables de red con la finalidad de evitar inferencia.	**Norma ISO/IEC 27001:2013** **En el punto 11 (Seguridad física y ambiental)** Indica los controles para la protección contra interceptaciones o daños el cableado de energía y telecomunicaciones que transporten datos o soporten servicios de información.	FOTOS 1
14	No hay un ordenamiento estructurado en los gabinetes	VALORATIVO	En la revisión que se hizo en la seguridad física se pudo identificar que no se tiene implementado los estándares de cableado estructurado en los gabinetes en el hospital San Bartolomé	Identificar si existe un ordenamiento estructurado en los gabinetes de la empresa para la supervisión de próximas auditorias.	**ANSI/TIA/EIA-569** El estándar provee especificaciones para el diseño de las instalaciones y la infraestructura edilicia necesaria para el cableado de telecomunicaciones en edificios.	FOTOS 2
15	No hay un control de acceso de la situacion actual de la sala de servidores	SATISFACCION	En la revisión que se hizo en la seguridad física se pudo identificar que no se tienen los estándares para la sala de servidores ya sea en energía eléctrica, aire acondiciado, cableado estructurado y espacio en el hospital San Bartolomé	Identificar la situación actual de la sala de servidores	Tanto los estándares ISO como los estándares **ANSI/TIA/EIA** exigen administrar las instalaciones, incluyendo el equipo de comunicaciones, está referido a las prácticas de diseños y construcción las cuales darán soporte a los medios de transmisión y al área de trabajo correcto. Estos estándares permitirán instalar una planta de cableado estructurado genérico que podrá hacer funcionar cualquier aplicación de datos y de voz, cumpliendo con la seguridad y ciertas restricciones. **ANSI/TIA/EIA-569** Determina los diferentes métodos para implementar el cableado estructurado. Respetando las reglas para las implementaciones y medidas que el estándar propone para la correcta implementación de un cableado estructurado.	ENTREVISTA: PREGUNTA 8

MATRIZ DE RIESGOS MAGERIT

16	No hay un control de los puntos vulnerables y riesgos que ocasionaria el cableado estructurado	VALORATIVO	La revisión y análisis de la información proporcionada por el hospital San Bartolomé, evidencia lo siguiente que supuestamente las áreas están separadas, sin embargo las conexiones de red no tienen restricciones, en la cual todas las áreas están conectadas en red, permitiendo la intrusión de un usuario desde otra área.	Identificar los puntos vulnerables del cableado estructurado y los riesgos que esto implica en la seguridad de la red para que no haya robo de información.	**Norma ISO/IEC 27001:2013 En el punto 11 (Seguridad física y ambiental)** Indica los controles para la protección contra interceptaciones o daños el cableado de energía y telecomunicaciones que transporten datos o soporten servicios de información. **Norma ISO/IEC 27001:2013 En el punto 9 (Control de acceso)** Se debería controlar la configuración y el acceso físico y lógico a los puertos de diagnóstico.	FOTOS 3
17	Deficiente control en la operatividad de la red	VALORATIVO	En la revisión que se hizo en la seguridad de redes se identificó que la red es inestable en el hospital San Bartolomé	Identificar la operatividad de la red en el hospital.	**Norma ISO/IEC 27001:2013 En el punto 12 (seguridad en las operaciones)** se refiere que hay que tener una operatividad correcta y eficaz de la red para no afectar a los procesos de información	FOTOS 4
18	Falta medidas adicionales para la seguridad de los correos corporativos	NOMINAL	En la revisión que se hizo en la seguridad de redes se identificó que los mensajes llegan con seguridad a su usuario final en el hospital San Bartolomé	Identificar la seguridad de los correos que llegan a su destino	**Norma ISO/IEC 27001:2013 En el punto 12 (seguridad en las operaciones)** se refiere que hay que tener una operatividad correcta y eficaz de la red para no afectar a los procesos de información	DOCUMENTO 1 :PLAN DE CONTINGENCIA "PROCEDIMIENTO DE DATOS A RECUPERAR"
19	No cuenta con politicas y normas de seguridad de informacion	SATISFACCION	En la revisión que se hizo en la seguridad de redes se identificó que la seguridad de redes no cuenta con todas las políticas de seguridad por el motivo que no se tiene una documentación de políticas y normas de seguridad en el hospital San Bartolomé	Identificar si cuenta con politicas y normas de seguridad de información	**Norma ISO/IEC 27001:2013 En el punto 5 (Políticas de seguridad de la información)** se refiere que hay que tener un documento de las políticas de seguridad e implementarlas dentro de nuestra red interna	ENTREVISTA: PREGUNTA 9
20	Administracion incorrecta de claves de los servdores	SATISFACCION	En la revisión que se hizo en la seguridad de redes se identificó que no se tiene un registro de las contraseñas que se modifican en los servidores del área de servidores en el hospital San Bartolomé	Identificar las claves de los servidores	**Norma ISO/IEC 27001:2013 En el punto 9.4. (Control de Acceso a la Red)** refiere que hay que asegurarse que el acceso de los usuarios a las redes y sus servicios no comprometan la seguridad de dichos servicios	ENTREVISTA: PREGUNTA 10
21	No cuenta con procedimiento para fallas de red en la infraestrutura de red	SATISFACCION	En la revisión que se hizo en la seguridad de redes se identificó que no se tiene un plan personal y general para mitigar los riesgos de la red en el hospital San Bartolomé	Identificar planes para mitigar los riesgos de la red	**Norma ISO/IEC 27001:2013 En el punto 8 (Gestión de activos)** refiere que hay que tener documentado los activos de información para no depender de personas que falten a sus labores y poder administrar de una manera perfecta los equipos intermedios y administración de la red interna de la organización.	ENTREVISTA: PREGUNTA 11

SOLICITUDES

SOLICITUD NUMERO 01: PERMISO DE AUDITORIA

MATRIZ DE RIESGOS MAGERIT

SOLICITA: "PERMISO DE AUDITORIA"

SEÑOR: **ING. SISTEMAS. SPILCO LEON JARDY**

JEFE DEL AREA DE SISTEMA E INFORMATICA

Yo JERSON CALDERON ALVARADO, identificado con DNI No. 76034606, actualmente cursando el Noveno ciclo de la carrera de Ingeniería de Sistemas de la Universidad Cesar Vallejo, ante Ud., con el debido respeto me presento y expongo:

Se me brinde el permiso de auditoria de dicha institución para poder realizar mi tesis titulada "Herramienta de gestión de riesgos para la seguridad informatica" y poder beneficiar a dicha institución con la identificación de sus hallazgos y poder implementar mejoras.

POR LO TANTO:

Solicito a usted acceder a mi petición para alcanzar a dicha información solicitada

Los Olivos, 26 de Octubre del 2016

MINISTERIO DE SALUD
HONADOMANI "SAN BARTOLOME"
Ing. JARDY L. ESPILCO LEON
JEFE DE LA UNIDAD DE INFORMATICA Y S.
CIP. Nº 147.3

JERSON CALDERON ALVARADO
DNI. Nro. 76034606

SOLICITUD NUMERO 02: CRONOGRAMA DE VISITAS A LA EMPRESA

SOLICITA: "CRONOGRAMA DE VISITA"

SEÑOR: **ING. SISTEMAS. SPILCO LEON JARDY**

JEFE DEL AREA DE SISTEMA E INFORMATICA

Yo, JERSON CALDERON ALVARADO, identificado con DNI No. 76034606, actualmente cursando el Noveno ciclo de Ingeniería de Sistemas de la Universidad Cesar Vallejo, ante Ud., con el debido respeto me presento y expongo:

Que, los días 27, 28, 31 de Octubre y 1, 2 de Noviembre del 2016 asistiré al hospital Nacional San Bartolomé en las horas de la mañana de 10:00 a 12:00 horas al área de Sistemas, para poder realizar la Auditoria de tecnologías de información.

POR LO TANTO:

Solicito a usted acceder a mi petición para alcanzar a dicha información solicitada

Los Olivos, 26 de Octubre del 2016

JERSON CALDERON ALVARADO

DNI. Nro. 76034606

SOLICITUD NUMERO 03: RECOJO DE EVIDENCIAS PARA LA AUDITORIA INFORMATICA

SOLICITA: RECOJO DE EVIDENCIAS,

MATRIZ DE RIESGOS MAGERIT

SEÑOR: **ING. SISTEMAS. SPILCO LEON JARDY**

JEFE DEL AREA DE SISTEMA E INFORMATICA

Yo JERSON CALDERON ALVARADO, identificado con DNI No. 76034606, actualmente cursando el Noveno ciclo de la carrera de Ingeniería de Sistemas de la Universidad Cesar Vallejo, ante Ud., con el debido respeto me presento y expongo:

Se me brinde el documento de plan de contingencia u otros y se me sellen las fotos para que tomen valides y credibilidad en esta Auditoria de tecnologías de información.

POR LO TANTO:

Solicito a usted acceder a mi petición para alcanzar a dicha información solicitada

Los Olivos, 31 de Mayo del 2016

JERSON CALDERON ALVARADO

DNI. Nro. 76034606

EVIDENCIAS

EVIDENCIA 01

FOTO 1

En la evidencia N°1 – foto 1, se observa que no se tiene una ubicación adecuada del cableado estructurado por falta de canaletas y falta de capacidad del personal encargado de hacer dicho trabajo.

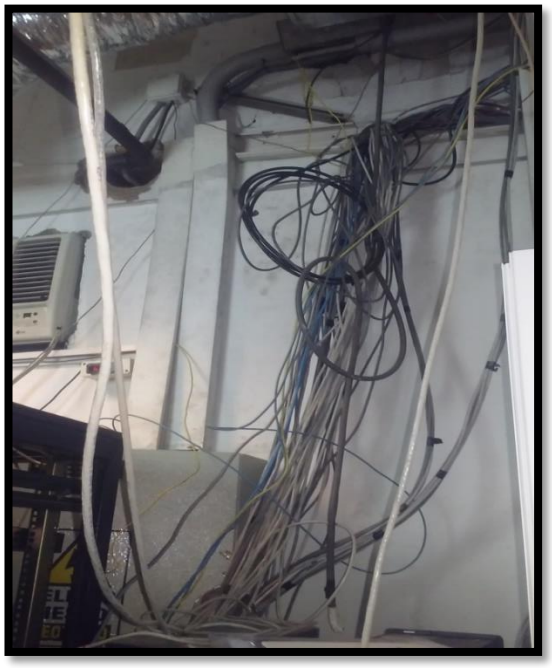


FOTO 2

En la evidencia N°1 – foto 2, se observa que el tendido de cableado estructurado está colgado y no hace seguimiento a estándares internacionales sobre cableado estructurado.

EVIDENCIA 02

FOTO 3

En la evidencia N°2, se observa que no se tiene un control en el ordenamiento del cableado estructurado dentro de los gabinetes.

EVIDENCIA 03

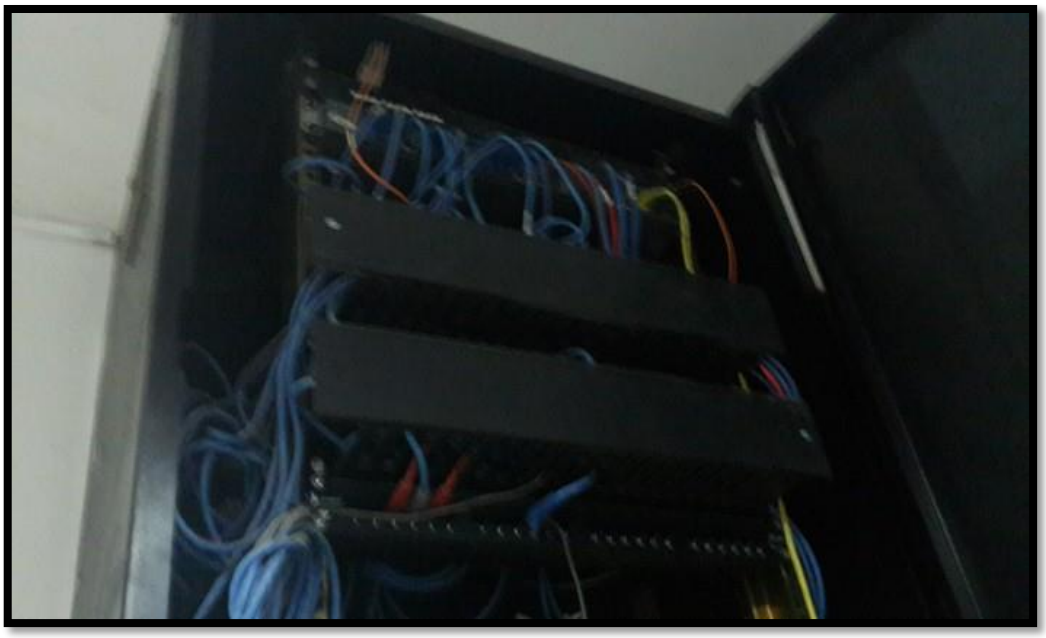


FOTO 4

En la evidencia N°3 – foto 1, se observa que no se tiene un ordenamiento de cableado estructurado en el gabinete correcto y que pueda ayudar a identificar la operatividad de algunos cables e identificar que puertos están disponibles.

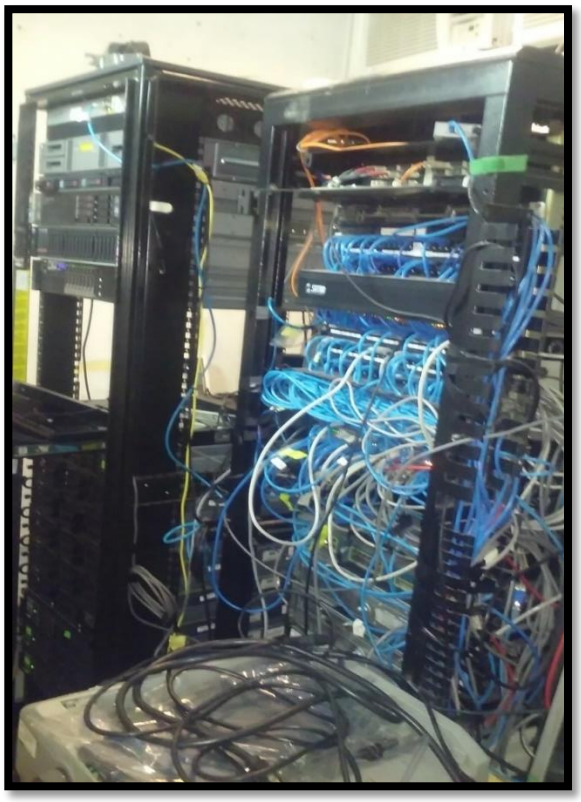


FOTO 5

En la evidencia N°3 – foto 2, se observa que la información puede ser vulnerada en la sala de servidores, así que se tiene que implementar medidas de control de seguridad.

EVIDENCIA 04

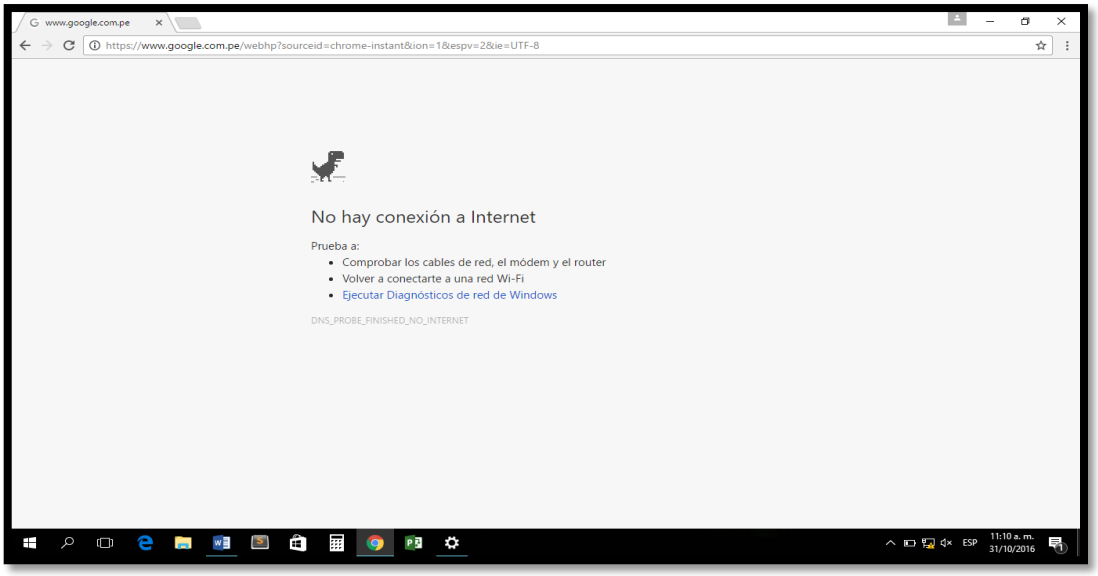


Foto 6

El hospital no cuenta con una estabilidad de la red operativa, dado que la red se para saliendo de operatividad en cada momento

ANEXO 12:

2° AUDITORIA INFORMATICA EN EL HOSPITAL SAN BARTOLOME

FACULTAD DE INGENIERÍA

ESCUELA ACADÉMICO-PROFESIONAL INGENIERÍA DE SISTEMAS

“AUDITORIA DE SEGURIDAD INFORMÀTICA EN EL HOSPITAL SAN BARTOLOMÈ”

INTEGRANTES

- ✓ CALDERON ALVARADO JERSON JOSEPH.
- ✓ GARCIA PALACIOS ALEXANDER CLAUDE
- ✓ CAMPOS CASTRO BRIAN
- ✓ ORMEÑO JARAMILLO LUIS

CICLO X

2017-I

Contenido

GENERALIDADES

IV. GENERALIDADES

4.1. TITULO

AUDITORIA DE SEGURIDAD INFORMATICA EN EL HOSPIITAL NACIONAL MADRE NIÑO SAN BARTOLOMÈ

4.2. INTEGRANTES

- ✓ CALDERON ALVARADO JERSON JOSEPH.
- ✓ GARCIA PALACIOS ALEXANDER CLAUDE
- ✓ CAMPOS CASTRO BRIAN
- ✓ ORMEÑO JARAMILLO LUIS

4.3. NOMBRE DE LA EMPRESA A AUDITAR

HOSPITAL NACIONAL MADRE NIÑO SAN BARTOLOMÈ

4.4. TIPO DE AUDITORIA A REALIZAR

AUDITORIA DE SEGURIDAD INFOMATICA

4.5. DURACION DE PROYECTO DE AUDITORIA

SEIS (6) DIAS

DIECISEIS (16 HORAS)

4.6. COSTO DE PROYECTO DE AUDITORIA

MIL DOSCIENTOS OCHENTA Y CUATRO SOLES, NOVENTA CENTIMOS

S/. 1’284.90 NUEVOS SOLES

INTRODUCCION

V. INTRODUCCION

5.1. INTRODUCCION

El presente trabajo trata de identificar la escasa forma de implementación de estándares y guías en el área de sistemas e informática en el hospital San Bartolomé en un periodo de seis (6) días, dado que en el siguiente informe se hará una auditoria de seguridad informática para poder identificar las vulnerabilidades de los procesos del hospital San Bartolomé y poder añadirle posible solución si esta lo necesite.

La información de una empresa es el oro más preciado de ello, por lo cual las categorías de procesos, los procesos y los niveles de capacidad de procesos deben de estar bien estructurado en la empresa, más aun si es una entidad hospitalaria porque tiene información sumamente confidencial.

La auditoría trata de ver los procesos que no se cumplen en una empresa y/o organización, con la finalidad de poder identificarlos y poder sugerir alguna posible mejora si en caso la empresa lo requiera, para ello hemos podido recoger información del hospital San Bartolomé con el área a auditar que es el área de sistemas e informática, luego identificar los objetivos de la auditoria con su alcance debido para poder efectuar una auditoria correcta. Luego ver con que guía de trabajo vamos a trabajar para la empresa, norma y estándar para el área de sistemas e informática y para que sea una auditoria correcta y estructurada hemos realizado un diagrama de Gantt y a raíz de ello hemos podido identificar el tiempo que se culminara la auditoria y el costo de ello.

A continuación se le explicara cada parte del proyecto detalladamente.

5.2. INFORMACION DE LA EMPRESA Y DEL AREA DE TI

El HONADOMANI “San Bartolomé” es un órgano desconcentrado de la Dirección de Salud V Lima Ciudad del Ministerio de Salud, normalizado en el ROF aprobado con RM Nº 884-2003-SA/DM. Es un hospital especializado en atención a la salud sexual y reproductiva de la mujer y la atención integral del neonato, niño y del adolescente. Es un establecimiento de atención recuperativa y de rehabilitación altamente especializada y de enfoque integral a la Mujer con necesidades de atención en su salud sexual y reproductiva y al Neonato, Niño y Adolescente, que proceden de cualquier punto del ámbito nacional

El Hospital “San Bartolomé”, fue fundado el 06 de Enero de 1646, durante el Gobierno del Marqués De Mancera Don Pedro de Toledo y Leiva. Sus fundadores, fueron el célebre Sacerdote Agustino Fray Bartolomé de Vadillo y el religioso Jesuita P. Gabriel Perli.

En 1651 se erigió el Hospital en el barrio de Santa Catalina a la altura de la novena cuadra del Jr. Antonio Miro Quezada, lugar que terminó sufriendo graves estragos durante el terremoto de 1687, siendo parcialmente reconstruido por el Sargento Mayor Manuel Fernández Dávila, Mayordomo del Hospital; gracias a las donaciones del Capitán Francisco Tijero de la Huerta y Segovia.

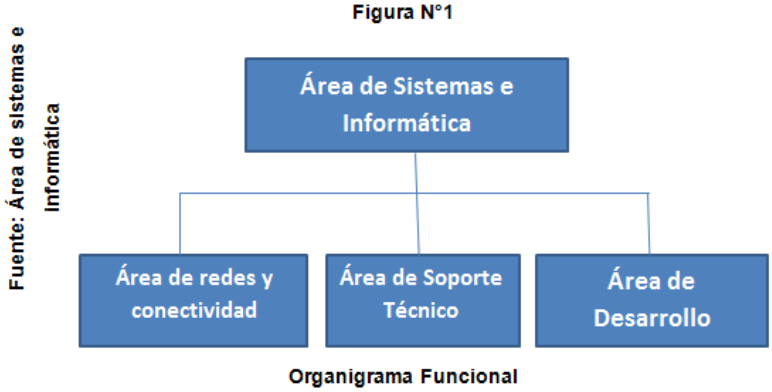
Hacia el año 1970 se incorporan al Hospital el Área Hospitalaria Nº 022 hasta el año 1983, a partir del cual se denomina Hospital Especializado Materno Infantil “San Bartolomé

El área de Sistema e Informática tiene como función principal el mantenimiento de la plataforma SIGHOS. También hace mantenimiento a los sistemas del Rol del Personal, Siaf, Siga y a la sala de telecomunicaciones del hospital.

El área de sistemas se divide en el área de soporte técnico que da mantenimiento a los equipos de cómputo y tiene como función principal solucionar las incidencias diarias, el área de redes y conectividad se encarga de dar mantenimiento a la sala de telecomunicaciones y conectividad del hospital y el área de desarrollo que se encarga de dar mantenimiento a los sistemas que utiliza el hospital.

A continuación, se muestra en la figura 1 como se divide el área de sistemas e informática

Figura N°1



Fuente: Área de sistemas e Informática

Organigrama Funcional

En la figura 1 se muestra que el área de sistemas e informática está dividida en sub áreas, el área de soporte técnico, el área de redes y conectividad y el área de desarrollo

5.2.1. VISION

Ser un hospital reconocido a nivel nacional por la atención que brinda a la salud sexual y reproductiva de la mujer y a la salud del feto, neonato, lactante, niño y adolescente, que ha alcanzado los estándares de sus servicios altamente especializados y garantiza la calidad de sus procesos de atención, con eficiencia y sensibilidad social, en virtud del compromiso e identificación de sus recursos humanos altamente calificados que le permiten continuar siendo el líder de los hospitales de alta complejidad del sector salud.

5.2.2. MISION

Somos un hospital de referencia nacional, que brinda atención altamente especializada a la salud sexual y reproductiva de la mujer y atención integral al feto, neonato, lactante, niño y adolescente; con calidad, eficiencia e inclusión social. Nuestro aporte a la sociedad, se consolida con la Docencia e Investigación que desarrollaremos en forma permanente y nuestra participación activa en los planes y programas nacionales, así como en las acciones de proyección social a la comunidad.

5.2.3. VALORES

El hospital San Bartolomé se identifica con los siguientes valores, que marcaran el curso a seguir para las consecuciones de objetivos trazados, mediante el compromiso de todos sus integrantes.

- **Lealtad:** actuamos con fidelidad a os objetivos institucionales, priorizando la defensa y protección de la persona humana
- **Justicia:** Intervenimos con la probidad, rectitud e imparcialidad procurando el bien común y el iteres en general.
- **Transparencia:** Fomentamos la práctica de valores y principios éticos en nuestras acciones para generar confianza y credibilidad.
- **Compromiso:** Nos esforzamos por gestionar con calidad porque entendemos que nuestras acciones deben coadyuvar el desarrollo sectorial.
- **Trabajo en equipo:** Coadyuvamos a soluciones integrales y eficientes con proactividad y sinergia.

5.2.4. FILOSOFIA

- Somos un equipo de profesionales fraternos, solidarios y cohesionados que impulsa optimas acciones de supervisión y control interno para mejorar el sistema disciplinario y funcional del sector interno.
- Gestionamos nuestros procesos con ética y transparencia para fortalecer las acciones de la lucha contra la corrupción y optimizar el sistema disciplinario y funcional del sector interno.

5.2.5. AREA DE TECNOLOGIA DE INFORMACION

El área de Sistema e Informática tiene como función principal el mantenimiento de la plataforma SIGHOS. También hace mantenimiento a los sistemas del Rol del Personal, Siaf, Siga y a la sala de telecomunicaciones del hospital.

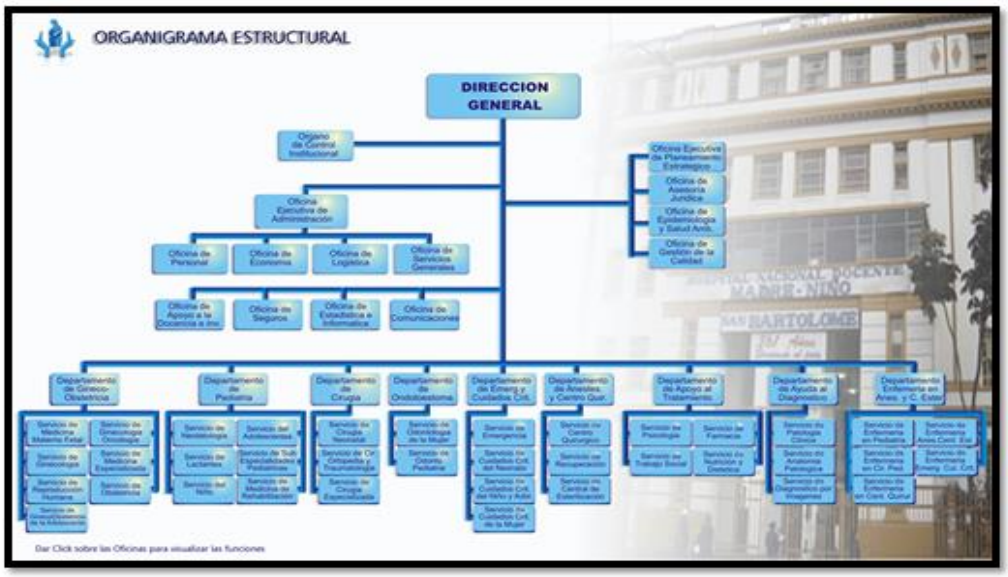
El área de sistemas se divide en el área de soporte técnico que da mantenimiento a los equipos de cómputo y tiene como función principal solucionar las incidencias diarias, el área de redes y conectividad se encarga de dar mantenimiento a la sala de telecomunicaciones y

conectividad del hospital y el área de desarrollo que se encarga de dar mantenimiento a los sistemas que utiliza el hospital.

ORGANIGRAMA DEL HOSPITAL NACIONAL SAN BARTOLOMÈ

Figura N°2

Fuente: Dirección general del Hospital San Bartolomé

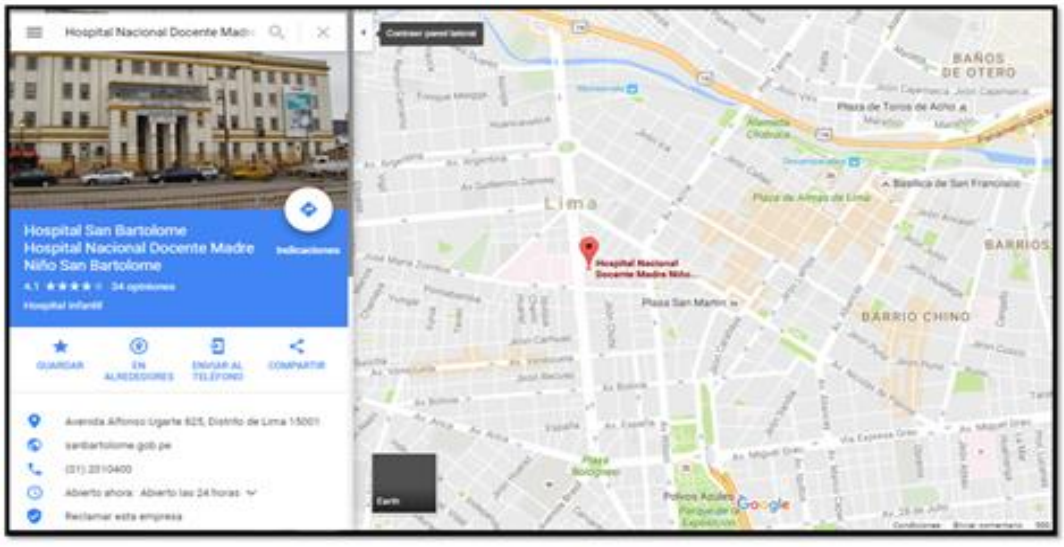


Organización Funcional

UBICACION DE INSPECTORIA GENERAL DE LA PNP

Figura N°3

Fuente: Google Maps



Croquis de Hospital San Bartolomé

5.3. OBJETIVOS DE LA AUDITORIA

El objetivo de la auditoría es verificar la existencia de estos controles y que estén funcionando de manera eficaz, respetando las políticas de la empresa y los objetivos de la empresa. Los objetivos de auditoría se consiguen mediante los procedimientos de auditoría, inicio, planeamiento, ejecución y cierre. Dado que se está enfocando está auditoría en el área de sistemas e informática

5.3.1. OBJETIVO GENERAL

Realizar una auditoría de seguridad informática en el hospital san Bartolomé, con la finalidad de poder identificar las vulnerabilidades de los activos según los niveles de seguridad que se requieran dar y las posibles amenazas que afecten a las vulnerabilidades

5.3.2. OBJETIVOS ESPECIFICOS

22. Identificar la cantidad de usuarios que tienen acceso a la red interna del hospital
23. Identificar la cantidad de usuarios creados con su contraseña
24. Identificar el nivel seguridad que tienen las contraseñas de los usuarios
25. Identificar los niveles de privilegios de acceso que tienen los usuarios
26. Identificar el periodo de cambio de contraseñas de los usuarios
27. Identificar si el antivirus está activo
28. Identificar si existe la restricción de instalación de software
29. Identificar si el antivirus está activo
30. Identificar si existe mantenimiento preventivo y correctivo de los equipos informáticos.
31. Identificar si existe un ordenamiento estructurado en los gabinetes de la empresa para la supervisión de próximas auditorias.
32. Identificar si cuenta con políticas y normas de seguridad de información
33. Identificar las claves de los servidores
34. Identificar planes para mitigar los riesgos de la red

5.4. ALCANCE DE LA AUDITORIA

La auditoría a realizarse abarcará desde el análisis exhaustivo de las funciones organizativas para la seguridad informática, la seguridad lógica, seguridad física y seguridad de redes; siendo ésta analizada con las distintas normativas nacionales e internacionales, así como estándares de los distintos dispositivos utilizados. El periodo de esta evaluación comprende entre las fechas del 05 de JUNIO hasta el 12 de JUNIO del año 2017 y costara S/. 28’730.20 nuevos soles.

5.5. DESCRIPCION Y FUNCIONES DEL EQUIPO AUDITOR

Cargo	Apellidos y Nombres	Tareas Básicas
Auditor Principal	✓ GARCIA PALACIOS ALEXANDER CLAUDE.	-Evaluar el ambiente de control y la información recopilada sobre los aspectos objetivos de la auditoria. -Dirigir la planificación de la auditoria y el desarrollo de la estrategia. -Revisar y aprobar la planificación de la auditoria. - Introducir y revisar con el Supervisor los cambios en el programa de auditoria que se consideren necesarios

MATRIZ DE RIESGOS MAGERIT

Auditor Líder de Seguridad informática	✓ CALDERON ALVARADO JERSON JOSEPH	-Coordinar con el Supervisor la distribución del tiempo y la duración de las diversas fases del trabajo. - Examinar e investigar aquellas áreas críticas que se relacionen con los objetivos de las tareas encomendadas. - Preparar los papeles de trabajo correspondientes.
Auditor Interno de seguridad Lógica y física	✓ CAMPOS CASTRO BRIAN	- Asistir en obtener información acerca de los aspectos a analizar junto con las normas y reglamentaciones aplicables. - Preparar los papeles de trabajo correspondientes.
Auditor interno de seguridad de redes	✓ ORMEÑO JARAMILLO LUIS	- Desarrollar una evaluación ampliada de los riesgos de control a través de la aplicación de formularios de control interno. - Preparar los papeles de trabajo correspondientes.

5.6. CRITERIOS DE AUDITORIA A UTILIZAR

- La NTP-ISO/IEC 27001 “Sistema de gestión de la seguridad de la información”. Es poder identificar una gestión de seguridad de información y así mismo poder hacer que la empresa cumpla con los estándares establecidos en dicha gestión.
- MODELO OSI: Marco de referencia de capas y estándar de trabajo Para establecer una comunicación entre equipos, lo mismo que para establecerla entre personas, es necesario contar con una serie de normas y protocolos que regulen dicho proceso. Esas normas las fija la sociedad en general o una organización internacional de normalización. Se puede mencionar como una de esas normativas al Modelo OSI.

  El modelo OSI (Open System Interconnection) es la base para la estructuración de la red de comunicaciones, la capa a utilizar será la número uno:

  - Capa 1: capa de enlace físico

  En este nivel se definen todas las características eléctricas y magnéticas de la red. Se incluye la conexión física ya sean los cables, los conectores y los tipos de señales. Básicamente consiste en proteger físicamente los cables de conexión, los módems y los circuitos.
- La Norma EIA/TIA 568 A y EIA/TIA B, Nos especifica los requerimientos mínimos para el cableado de establecimientos comerciales de oficinas dado que siguen una estructura de cómo se debe implementar la forma de cableado respecto al conector RJ45, según esta norma se verá si es posible la comunicación de equipos y así posible el intercambio de comunicación.
- Estándar ANSI/TIA/EIA-569, Este estándar es para los ductos, pasos y espacios necesarios para la instalación de sistemas estandarizados de telecomunicaciones en el área de redes y así poder mantener un orden en el cableado estructurado en la empresa.

5.7. DOCUMENTACION INICIAL A SOLICITAR

- Se le solicitara el plan de contingencia de la seguridad informática del Hospital Nacional San Bartolomé
  - DOCUMENTO 1

5.8. PLAN DE AUDITORIA

Para hacer una planeación eficaz, lo primero que se requiere es obtener información general sobre la organización y sobre la función de punto a evaluar, que este caso sería la gestión de las redes. Para ello es preciso hacer una investigación preliminar y algunas entrevistas previas, con base en esto planear el programa de trabajo, el cual deberá incluir tiempo, costo, personal necesario y documentos auxiliares a solicitar o formular durante el desarrollo de la misma.

3. Investigación preliminar

Se deberá observar el estado general del área, su situación dentro de la organización, si existe la información solicitada, si es o no necesaria y la fecha de su última actualización. Para analizar y dimensionar la estructura por auditar se debe solicitar:

- ✓ **A nivel del área de informática:** Objetivos a corto y largo plazo.
- ✓ **Recursos materiales y técnicos:** Solicitar documentos sobre los equipos, número de ellos, localización y características.

  - Estudios de viabilidad.
  - Número de equipos, localización y las características (de los equipos instalados y por instalar y programados)
  - Fechas de instalación de los equipos y planes de instalación.
  - Contratos vigentes de compra, renta y servicio de mantenimiento.
  - Contratos de seguros.
  - Convenios que se tienen con otras instalaciones.

- Configuración de los equipos y capacidades actuales y máximas.
- Planes de expansión.
- Ubicación general de los equipos.
- Políticas de operación.
- Políticas de uso de los equipos.

4. Controles

Conjunto de disposiciones metódicas, cuyo fin es vigilar las funciones y actitudes de las empresas y para ello permite verificar si todo se realiza conforme a los programas adoptados, órdenes impartidas y principios admitidos. La clasificación general de los controles consta de 3 controles:

- ✓ **Controles Preventivos:** Son aquellos que reducen la frecuencia con que ocurren las causas del riesgo, permitiendo cierto margen de violaciones.

- ✓ **Controles detectivos:** Son aquellos que no evitan que ocurran las causas del riesgo sino que los detecta luego de ocurridos. Son los más importantes para el auditor. En cierta forma sirven para evaluar la eficiencia de los controles preventivos.

- ✓ **Controles Correctivos:** Ayudan a la investigación y corrección de las causas del riesgo. La corrección adecuada puede resultar difícil e ineficiente, siendo necesaria la implantación de controles detectivos sobre los controles correctivos, debido a que la corrección de errores es en sí una actividad altamente propensa a errores.

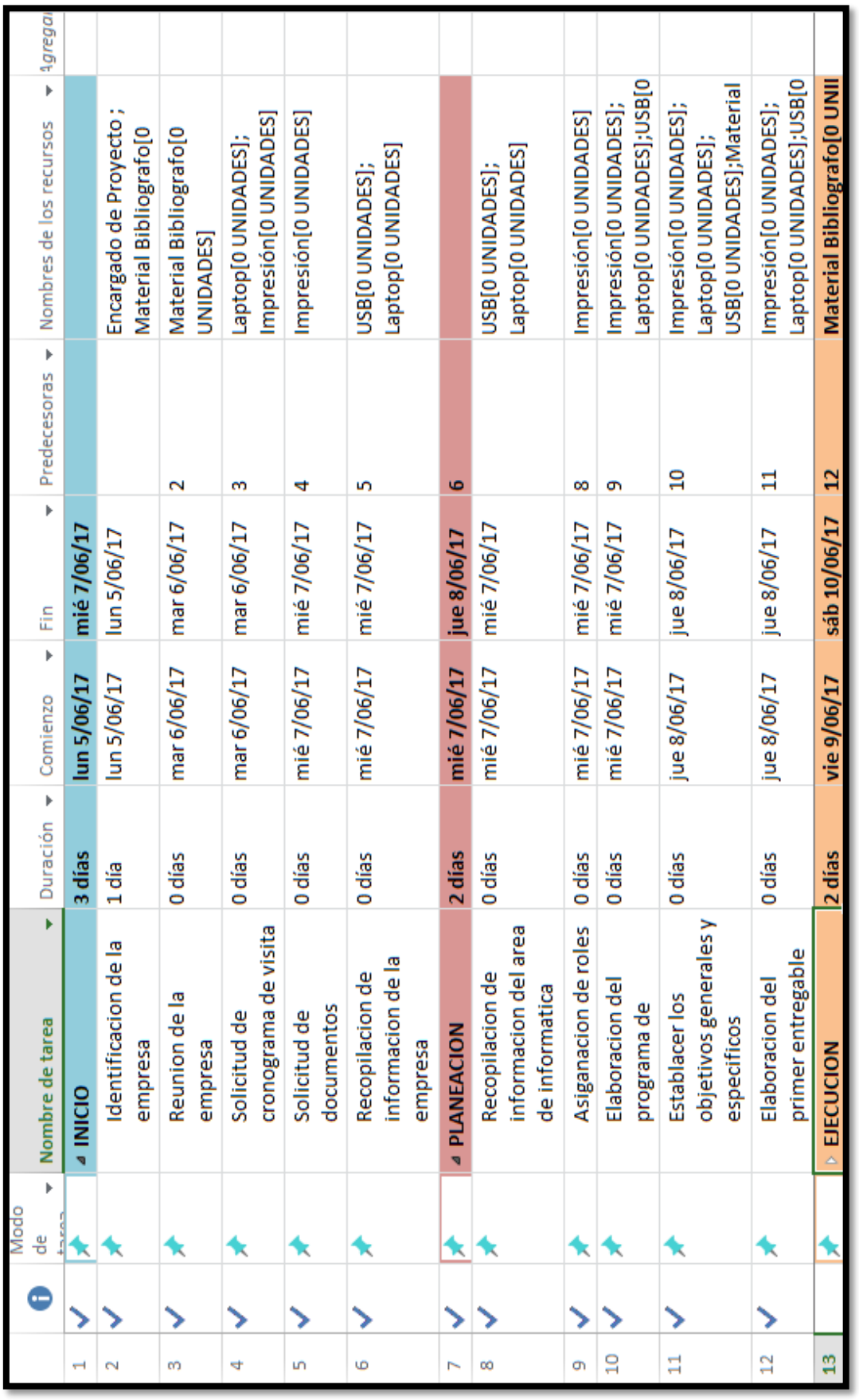
a. Planes de contingencia

Dentro de las áreas generales, se establecen las siguientes divisiones de Auditoría Informática: de Explotación, de Sistemas, de Comunicaciones y de Desarrollo de Proyectos.

Cada área específica puede ser auditada desde los siguientes criterios generales:

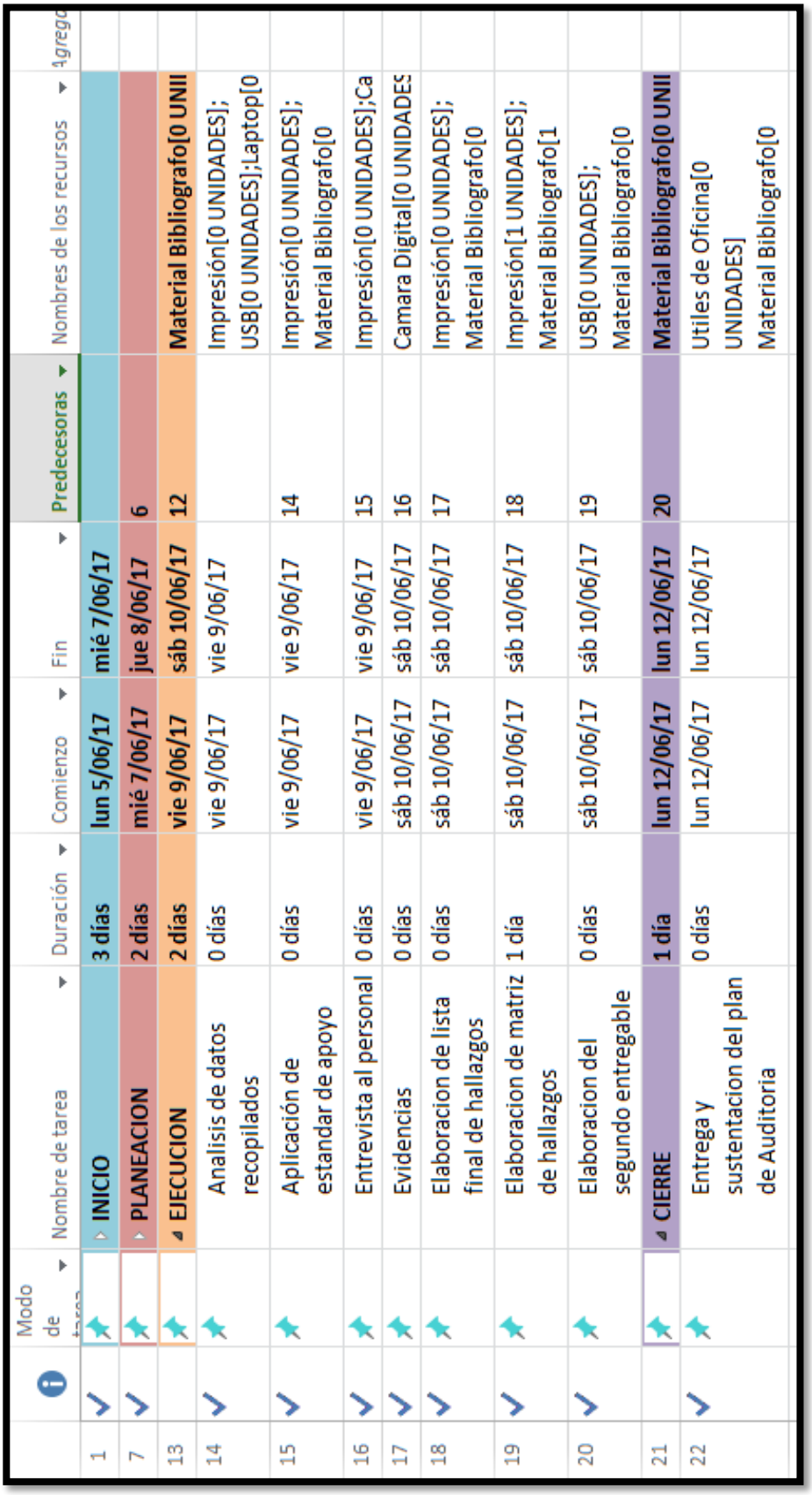
- ✓ Desde su propio funcionamiento interno.
- ✓ Desde el apoyo que recibe de la Dirección y, en sentido ascendente, del grado de cumplimiento de las directrices de ésta.
- ✓ Desde la perspectiva de los usuarios, destinatarios reales de la informática.
- ✓ Desde el punto de vista de la seguridad que ofrece la Informática en general o la rama auditada.
- ✓ Estas combinaciones pueden ser ampliadas y reducidas según las características de la empresa auditada.

5.8.1. DIAGRAMA DE GANTT



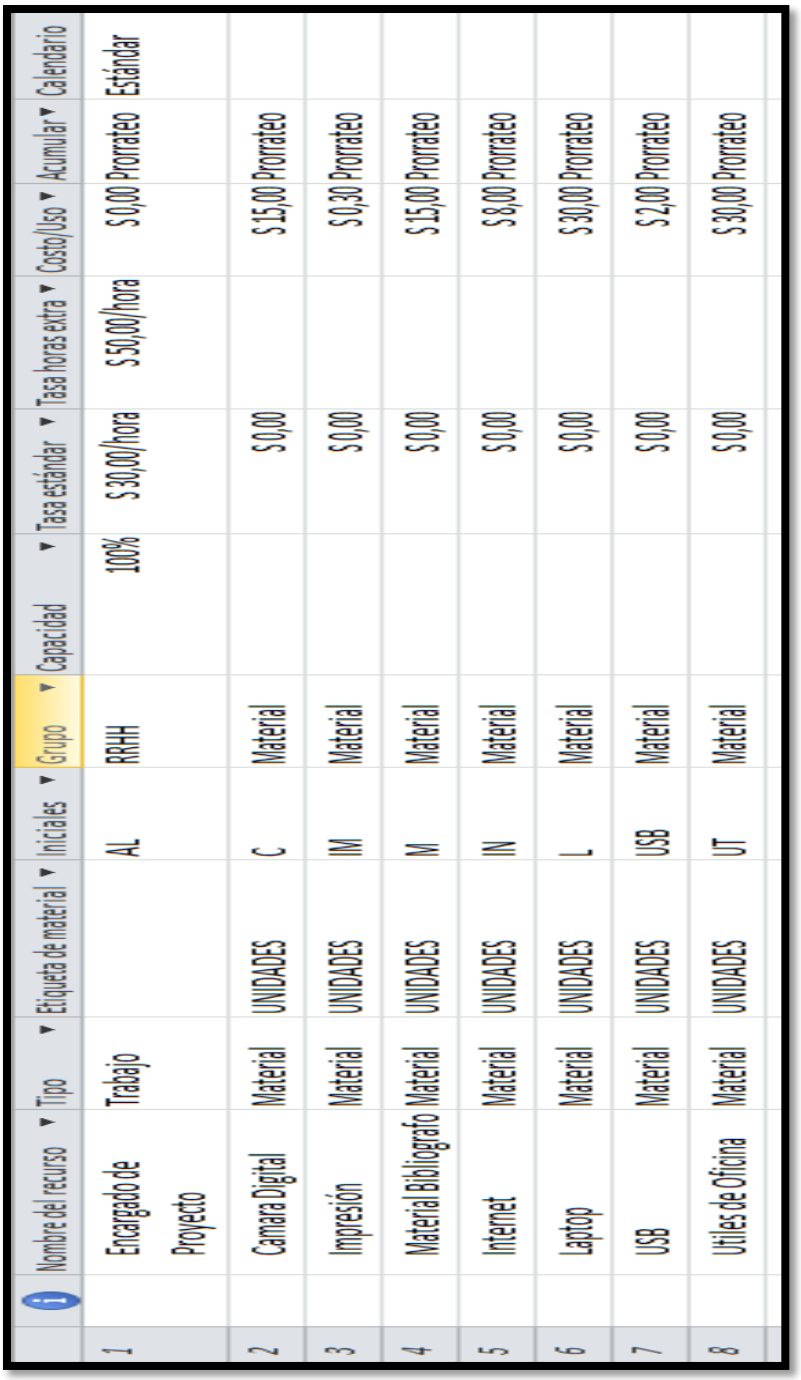
	Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras	Nombres de los recursos	Agrega
1		**INICIO**	**3 días**	**lun 5/06/17**	**mié 7/06/17**			
2		Identificacion de la empresa	1 día	lun 5/06/17	lun 5/06/17		Encargado de Proyecto ; Material Bibliografo[0	
3		Reunion de la empresa	0 días	mar 6/06/17	mar 6/06/17	2	Material Bibliografo[0 UNIDADES]	
4		Solicitud de cronograma de visita	0 días	mar 6/06/17	mar 6/06/17	3	Laptop[0 UNIDADES]; Impresión[0 UNIDADES]	
5		Solicitud de documentos	0 días	mié 7/06/17	mié 7/06/17	4	Impresión[0 UNIDADES]	
6		Recopilacion de informacion de la empresa	0 días	mié 7/06/17	mié 7/06/17	5	USB[0 UNIDADES]; Laptop[0 UNIDADES]	
7		**PLANEACION**	**2 días**	**mié 7/06/17**	**jue 8/06/17**	6		
8		Recopilacion de informacion del area de informatica	0 días	mié 7/06/17	mié 7/06/17		USB[0 UNIDADES]; Laptop[0 UNIDADES]	
9		Asiganacion de roles	0 días	mié 7/06/17	mié 7/06/17	8	Impresión[0 UNIDADES]	
10		Elaboracion del programa de	0 días	mié 7/06/17	mié 7/06/17	9	Impresión[0 UNIDADES]; Laptop[0 UNIDADES];USB[0	
11		Establacer los objetivos generales y especificos	0 días	jue 8/06/17	jue 8/06/17	10	Impresión[0 UNIDADES]; Laptop[0 UNIDADES]; USB[0 UNIDADES];Material	
12		Elaboracion del primer entregable	0 días	jue 8/06/17	jue 8/06/17	11	Impresión[0 UNIDADES]; Laptop[0 UNIDADES];USB[0	
13		**EJECUCION**	**2 días**	**vie 9/06/17**	**sáb 10/06/17**	12	**Material Bibliografo[0 UNII**	

MATRIZ DE RIESGOS MAGERIT



	Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras	Nombres de los recursos	Agrega
1		**INICIO**	**3 días**	**lun 5/06/17**	**mié 7/06/17**			
7		**PLANEACION**	**2 días**	**mié 7/06/17**	**jue 8/06/17**	**6**		
13		**EJECUCION**	**2 días**	**vie 9/06/17**	**sáb 10/06/17**	**12**	**Material Bibliografo[0 UNI**	
14		Analisis de datos recopilados	0 días	vie 9/06/17	vie 9/06/17		Impresión[0 UNIDADES]; USB[0 UNIDADES];Laptop[0	
15		Aplicación de estandar de apoyo	0 días	vie 9/06/17	vie 9/06/17	14	Impresión[0 UNIDADES]; Material Bibliografo[0	
16		Entrevista al personal	0 días	vie 9/06/17	vie 9/06/17	15	Impresión[0 UNIDADES];Ca	
17		Evidencias	0 días	sáb 10/06/17	sáb 10/06/17	16	Camara Digital[0 UNIDADES	
18		Elaboracion de lista final de hallazgos	0 días	sáb 10/06/17	sáb 10/06/17	17	Impresión[0 UNIDADES]; Material Bibliografo[0	
19		Elaboracion de matriz de hallazgos	1 día	sáb 10/06/17	sáb 10/06/17	18	Impresión[1 UNIDADES]; Material Bibliografo[1	
20		Elaboracion del segundo entregable	0 días	sáb 10/06/17	sáb 10/06/17	19	USB[0 UNIDADES]; Material Bibliografo[0	
21		**CIERRE**	**1 día**	**lun 12/06/17**	**lun 12/06/17**	**20**	**Material Bibliografo[0 UNI**	
22		Entrega y sustentacion del plan de Auditoria	0 días	lun 12/06/17	lun 12/06/17		Utiles de Oficina[0 UNIDADES] Material Bibliografo[0	

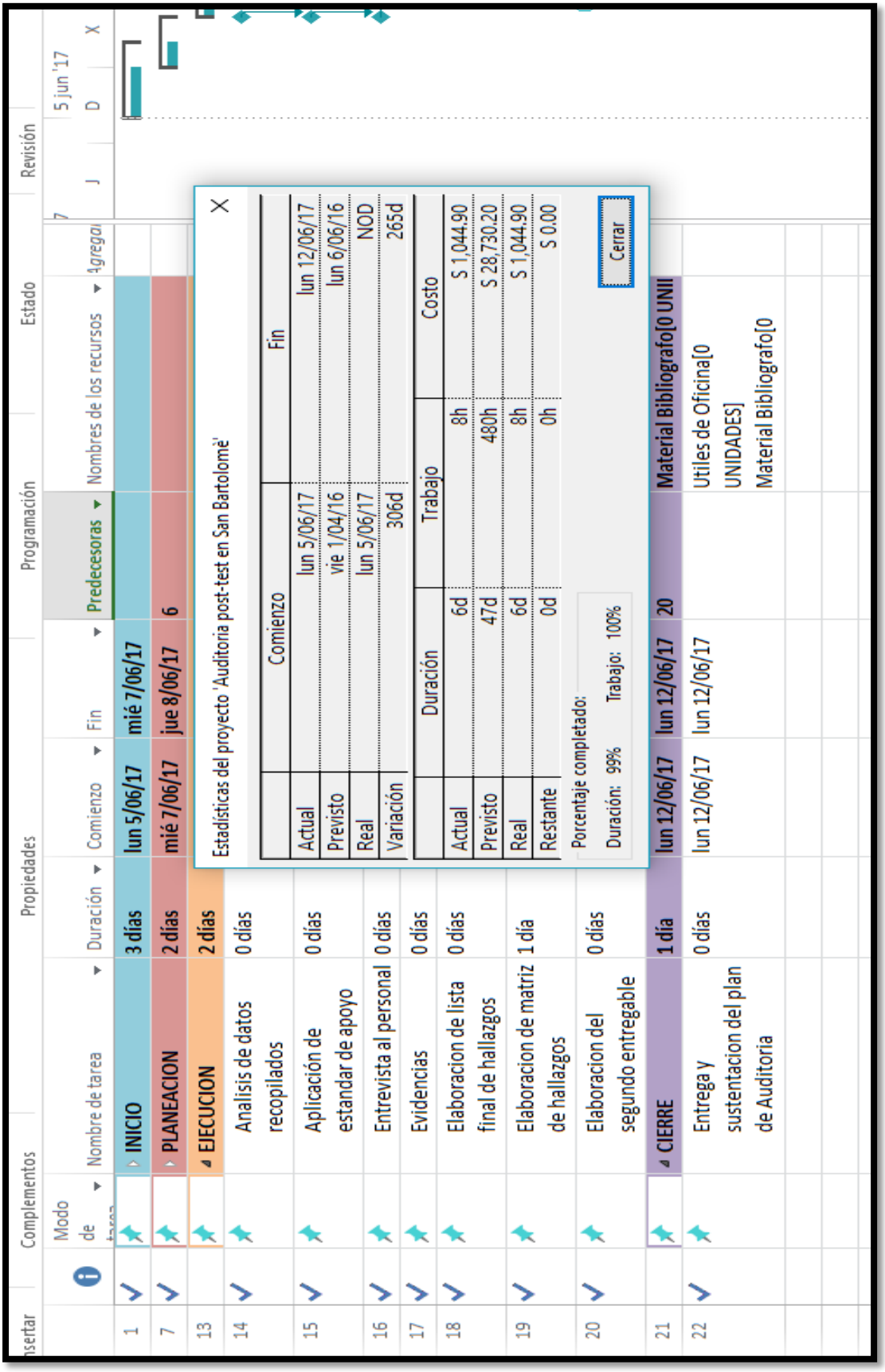
5.8.2. DIAGRAMA HOJA DE RECURSOS

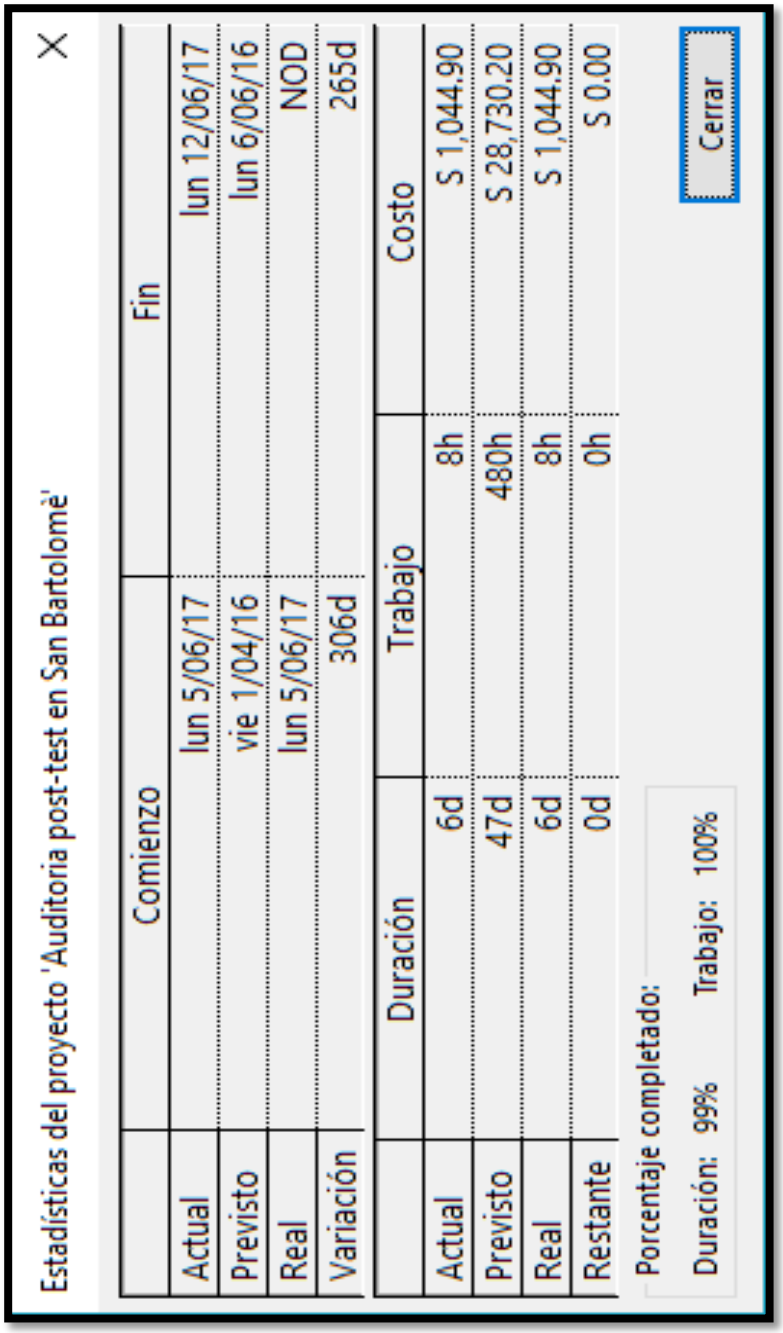


	Nombre del recurso	Tipo	Etiqueta de material	Iniciales	Grupo	Capacidad	Tasa estándar	Tasa horas extra	Costo/Uso	Acumular	Calendario
1	Encargado de Proyecto	Trabajo		AL	RRHH	100%	$30,00/hora	$50,00/hora	$0,00	Prorrateo	Estándar
2	Camara Digital	Material	UNIDADES	C	Material		$0,00		$15,00	Prorrateo	
3	Impresión	Material	UNIDADES	IM	Material		$0,00		$0,30	Prorrateo	
4	Material Bibliografo	Material	UNIDADES	M	Material		$0,00		$15,00	Prorrateo	
5	Internet	Material	UNIDADES	IN	Material		$0,00		$8,00	Prorrateo	
6	Laptop	Material	UNIDADES	L	Material		$0,00		$30,00	Prorrateo	
7	USB	Material	UNIDADES	USB	Material		$0,00		$2,00	Prorrateo	
8	Utiles de Oficina	Material	UNIDADES	UT	Material		$0,00		$30,00	Prorrateo	

ESTADISTICA DEL PROYECTO

MATRIZ DE RIESGOS MAGERIT





5.8.3. INFORMACION DEL PROYECTO

<table>
<tr><th colspan="3">PROGRAMA DE AUDITORÍA PARA EL HOSPITAL SAN BARTOLOME</th></tr>
<tr><th>ACTIVIDADES</th><th colspan="2">HORARIO APROXIMADO</th></tr>
<tr><td>Reunión Inicial</td><td colspan="2" rowspan="3">1 hora</td></tr>
<tr><td>Asistentes:
- Equipo auditor.
- Representante de la organización.</td></tr>
<tr><td>Objetivo:
- Presentación del equipo auditor.
- Presentación de la organización.
- Confirmación del programa de auditoría.</td></tr>
<tr><td rowspan="2">Tiempo Proyectado</td><td colspan="2">Fecha</td></tr>
<tr><td>Inicio</td><td>Fin</td></tr>
<tr><td>Reunión inicial con el responsable de área</td><td>05/06/17</td><td>05/06/17</td></tr>
<tr><td>Recopilación de información de la situación actual del área de redes</td><td>05/06/17</td><td>05/06/17</td></tr>
<tr><td>Entrega del plan de auditoría</td><td colspan="2">06/06/17</td></tr>
<tr><td>Estudio preliminar del área</td><td>06/06/17</td><td>07/06/17</td></tr>
<tr><td>Primer informe preliminar de auditoria</td><td colspan="2">08/06/17</td></tr>
<tr><td>Identificación de riesgos potenciales</td><td>08/06/17</td><td>08/06/17</td></tr>
<tr><td>Análisis de riesgos</td><td>09/06/17</td><td>09/06/17</td></tr>
<tr><td>Análisis del impacto</td><td>10/06/17</td><td>10/06/17</td></tr>
<tr><td>Elaboración del informe de auditoría</td><td>10/06/17</td><td>11/06/17</td></tr>
<tr><td>Presentación del informe</td><td colspan="2">12/06/17</td></tr>
<tr><td>Reunión final</td><td colspan="2" rowspan="3">12 Junio del 2017</td></tr>
<tr><td>Asistentes:
- Equipo auditor.
- Representante de la organización.</td></tr>
<tr><td>Objeto:
- Dar lecturas de los resultados de la auditoría.
- Comentarios y aclaraciones.</td></tr>
</table>

MATRIZ DE RIESGOS MAGERIT

EMPRESA	**HOSPITAL NACIONAL MADRE NIÑO SAN BARTOLOME**
DIRECCIÓN	AV. Alfonso Ugarte, Lima Central
ALCANCE	• ISO/ IEC 27001/2013 • NORMA TECNICA PERUANA (NTP) • ESTANDAR (MODELO OSI)
GRUPO AUDITOR	• CALDERON ALVARADO JERSON JOSEPH. • GARCIA PALACIOS ALEXANDER CLAUDE (AUDITOR LIDER) • CAMPOS CASTRO BRIAN • ORMEÑO JARAMILLO LUIS
FECHA AUDITORÍA	Del 05 de Junio hasta el 12 de Junio del 2017
LUGAR	Área de Sistemas e Informática
DOCUMENTACIÓN DE REFERENCIA	NTP - EIA/TIA 568 A, EIA/TIA 568 B, EIA/TIA 569 , NTP-ISO/IEC 27001

VI. DESARROLLO DE LA AUDITORIA

6.1. DESCRIPCION DE LOS OBJETIVOS ESPECIFICOS Y ACTIVIDADES A REALIZAR PARA SU CUMPLIMIENTO

22. Identificar la cantidad de usuarios que tienen acceso a la red interna del hospital
    i. DESCRIPCION: En la revisión que se hizo en la seguridad lógica se pudo identificar que se implementó un registro de la cantidad de usuarios que tienen acceso a la red interna del hospital.
    ii. ACTIVIDADES: Se debe de mantener actualizado cada 10 días el registro de cantidad de usuarios.

23. Identificar la cantidad de usuarios creados con su contraseña
    i. DESCRIPCION: En la revisión que se hizo en la seguridad lógica se pudo identificar que se implementó un registro de la cantidad de usuarios que existen y que tienen un equipo informático de disponibilidad en el hospital
    ii. ACTIVIDADES: Se debe de mantener actualizado cada 30 días el registro de cantidad de usuarios que tienen una cuenta de acceso.

24. Identificar el nivel seguridad que tienen las contraseñas de los usuarios
    i. DESCRIPCION: En la revisión que se hizo en la seguridad lógica se pudo identificar que se realizó un manual con la cantidad de caracteres para las contraseñas usuarios de red, correos y sistemas internos en el hospital San Bartolomé
    ii. ACTIVIDADES: Se debe de hacer seguimiento a la creación de contraseñas de los usuarios para mejorar y establecer una seguridad alta de cuenta

25. Identificar los niveles de privilegios de acceso que tienen los usuarios
    i. DESCRIPCION: En la revisión que se hizo en la seguridad lógica se pudo identificar que se implementó un registro de control de los privilegios de acceso que tienen cada usuario para acceder a la red interna en el hospital San Bartolomé
    ii. ACTIVIDADES: Se debe de hacer un seguimiento a los privilegios

de acceso que debe de tener cada usuario y además mantener controlado el cambio de ipv4 que se pueda generar.

26. Identificar el periodo de cambio de contraseñas de los usuarios
    i. DESCRIPCION: En la revisión que se hizo en la seguridad lógica se pudo identificar que se tiene un registro de los usuarios que deban de cambiar su contraseña por el tipo de información que manejan en su PC en el hospital San Bartolomé
    ii. ACTIVIDADES: Se debe de hacer un seguimiento, control y mejorar el nivel de seguridad de contraseñas para aquellos usuarios que lo requieran.

27. Identificar si el antivirus está activo
    i. DESCRIPCION: En la revisión que se hizo en la seguridad lógica se pudo identificar que el servidor del antivirus está activo y envía a cuarentena los posibles usuarios de red que están emitiendo virus, además se restringe el acceso de dispositivos de almacenamiento con la finalidad de no infectar con algún virus la información en el hospital San Bartolomé
    ii. ACTIVIDADES: Se debe de tener un registro de aquellos equipos informáticos que están con el antivirus actualizado y un manual de la forma correcta de eliminar un archivo infectado en un usuario de red

28. Identificar si existe la restricción de instalación de software
    i. DESCRIPCION: En la revisión que se hizo en la seguridad física se pudo identificar que hay un usuario administrador local, y usuarios de red administrativos, que permiten la instalación del software en el hospital San Bartolomé
    ii. ACTIVIDADES: Se debe de tener normas y políticas de seguridad respecto a software instalables para que se pueda restringir esas instalaciones

.

29. Identificar si existe mantenimiento preventivo y correctivo de los equipos informáticos.
    i. DESCRIPCION: En la revisión que se hizo en la seguridad física se pudo identificar han implementado un manual para hacer mantenimiento preventivo de los equipos, en área que dan la cara a los clientes en el hospital San Bartolomé
    ii. ACTIVIDADES: Se debe de tener un plan preventivo y correctivo de los equipos informáticos para evitar equipos en estado de inoperatividad y retrasar las actividades de trabajo

30. Identificar si existe un ordenamiento estructurado en los gabinetes.
    i. DESCRIPCION: En la revisión que se hizo en la seguridad física se pudo identificar que se tiene implementado los estándares de cableado estructurado en los gabinetes en el hospital San Bartolomé y respecto a la implementación de un punto de red, el área de logística selecciona al proveedor para que se haga cargo de ello.
    ii. ACTIVIDADES: Se debe de implementar los estándares de cableado estructurado y tener un certificado de ello para tener un mejor control de los puertos de acceso de los switch.

31. Identificar la operatividad de la red en el hospital.
    i. DESCRIPCION: En la revisión que se hizo en la seguridad de redes se identificó que la red es estable, porque ya se han implementado vlan en las áreas de faltaban respecto a equipos de cómputo, POS y Access point en el hospital San Bartolomé
    ii. ACTIVIDADES: Se debe de identificar cuáles son los recursos que inestabilizan la red y poder darle un seguimiento diario..

32. Identificar si cuenta con políticas y normas de seguridad de información
    i. DESCRIPCION: En la revisión que se hizo en la seguridad de redes se identificó que la seguridad de redes cuenta con todas las políticas de seguridad en el hospital San Bartolomé
    ii. ACTIVIDADES: Se debe de mejorar constantemente la documentación de políticas y normas de seguridad informática.

33. Identificar la clave de los servidores
    i. DESCRIPCION: En la revisión que se hizo en la seguridad de redes se identificó que se tiene un registro de las contraseñas que se modifican en los servidores del área de servidores en el hospital San Bartolomé
    ii. ACTIVIDADES: Se debe de implementar un procedimiento más de resguardo de sobres sellados donde solo lo tenga el jefe de informatica en su escritorio mediante llaves.

34. Identificar planes para mitigar los riesgos de la red
    i. DESCRIPCION: En la revisión que se hizo en la seguridad de redes se identificó que se tiene un plan personal y general para mitigar los riesgos de la red en el hospital San Bartolomé
    ii. ACTIVIDADES: Se debe documentar por cada servidor y puntos de red unos procedimientos de fallas para poder resolver dichas fallas.

6.2. DESCRIPCION DE LA METODOLOGIA UTLIZADA PARA CADA OBJETIVO ESPECÍFICO

22. Identificar la cantidad de usuarios que tienen acceso a la red interna del hospital

Norma ISO/IEC 27001:2013

En el punto 9.4. (Control de Acceso a la Red) refiere que hay que asegurarse que el acceso de los usuarios a las redes y sus servicios no comprometan la seguridad de dichos servicios

23. Identificar la cantidad de usuarios creados con su contraseña

Norma ISO/IEC 27001:2013

En el punto 9.4. (Control de Acceso a la Red) refiere que hay que asegurarse que el acceso de los usuarios a las redes y sus servicios no comprometan la seguridad de dichos servicios

24. Identificar el nivel seguridad que tienen las contraseñas de los usuarios

Norma ISO/IEC 27001:2013

En el punto 9.4. (Control de Acceso a la Red) refiere que hay que asegurarse que el acceso de los usuarios a las redes y sus servicios no comprometan la seguridad de dichos servicios

25. Identificar los niveles de privilegios de acceso que tienen los usuarios

Norma ISO/IEC 27001:2013

En el punto 9.4. (Control de Acceso a la Red) refiere que hay que asegurarse que el acceso de los usuarios a las redes y sus servicios no comprometan la seguridad de dichos servicios

26. Identificar el periodo de cambio de contraseñas de los usuarios

Norma ISO/IEC 27001:2013

En el punto 9.4. (Control de Acceso a la Red) refiere que hay que asegurarse que el acceso de los usuarios a las redes y sus servicios no comprometan la seguridad de dichos servicios

27. Identificar si el antivirus está activo

    Norma ISO/IEC 27001:2013

    En el punto 12 (seguridad en las operaciones) se refiere que hay que tener una operatividad correcta y eficaz de la red para no afectar a los procesos de información

28. Identificar si existe la restricción de instalación de software

    Norma ISO/IEC 27001:2013

    En el punto 12.6.2 (Restricciones en la instalación de software) se refiere que hay que tener permisos de la alta dirección para poder instalar un software ajeno a los requerimientos que tiene la organización y documentación del uso que se quiera dar al software

29. Identificar si existe mantenimiento preventivo y correctivo de los equipos informáticos.

    Norma ISO/IEC 27001:2013

    En el punto 14 (Adquisición, desarrollo y mantenimiento de sistemas) se refiere que hay que tener un plan preventivo y correctivo para los equipos informáticos, dado que no se tiene que perjudicar la operatividad de la red y las actividades de los usuarios.

30. Identificar si existe un ordenamiento estructurado en los gabinetes

    ANSI/TIA/EIA-569

    El estándar provee especificaciones para el diseño de las instalaciones y la infraestructura edilicia necesaria para el cableado de telecomunicaciones en edificios.

31. Identificar la operatividad de la red en el hospital.

    Norma ISO/IEC 27001:2013

    En el punto 12 (seguridad en las operaciones) se refiere que hay que tener una operatividad correcta y eficaz de la red para no afectar a los procesos de información

32. Identificar si cuenta con políticas y normas de seguridad de información

    Norma ISO/IEC 27001:2013

    En el punto 5 (Políticas de seguridad de la información) se refiere que hay que tener un documento de las políticas de seguridad e implementarlas dentro de nuestra red interna

33. Identificar la clave de los servidores

    Norma ISO/IEC 27001:2013

    En el punto 9.4. (Control de Acceso a la Red) refiere que hay que asegurarse que el acceso de los usuarios a las redes y sus servicios no comprometan la seguridad de dichos servicios

34. Identificar planes para mitigar los riesgos de la red

    Norma ISO/IEC 27001:2013

    En el punto 8 (Gestión de activos) refiere que hay que tener documentado los activos de información para no depender de personas que falten a sus labores y poder administrar de una manera perfecta los equipos intermedios y administración de la red interna de la organización.

MATRIZ DE RIESGOS MAGERIT

6.3. CLASIFICACION DE LOS HALLAZGOS POR TIPO

NUMERO	HALLAZGO	TIPO	EVIDENCIA
1	No hay un registro para la cantidad de usuarios que tienen acceso a la red interna	NOMINAL	DOCUMENTO 1
2	No hay un registro para la cantidad de usuarios creados con su contraseña	NOMINAL	DOCUMENTO 2
3	No hay un control para el nivel de seguridad de las contraseñas de los usuarios	NOMINAL	DOCUMENTO 3
4	Falta medidas adicionales para controlar los niveles de privilegios de acceso	NOMINAL	DOCUMENTO 4
5	Falta de medidas adicionales para controlar el cambio de contraseña de los usuarios	NOMINAL	DOCUMENTO 5
6	Falta de medidas adicionales para que el antivirus este activo	NOMINAL	DOCUMENTO 6
7	No hay un control para la restriccion de instalacion de software	NOMINAL	DOCUMENTO 7
8	No hay un mantenimiento preventivo a los equipos informaticos	NOMINAL	DOCUMENTO 8
9	No hay un ordenamiento estructurado en los gabinetes	NOMINAL	DOCUMENTO 9
10	Deficiente control en la operatividad de la red	NOMINAL	DOCUMENTO 10
11	No cuenta con politicas y normas de seguridad de informacion	NOMINAL	DOCUMENTO 11
12	Administracion incorrecta de claves de los servidores	NOMINAL	DOCUMENTO 12
13	No cuenta con procedimiento para fallas de red en la infraestrutura de red	NOMINAL	DOCUMENTO 13

6.4. HALLAZGOS INICIALES

1. Si hay un registro para la cantidad de usuarios que tienen acceso a la red interna
2. Si hay un registro para la cantidad de usuarios creados con su contraseña
3. Si hay un control para el nivel de seguridad de las contraseñas de los usuarios
4. Si hay medidas adicionales para controlar los niveles de privilegios de acceso
5. Si hay de medidas adicionales para controlar el cambio de contraseña de los usuarios
6. Si hay medidas adicionales para que el antivirus este activo
7. SI hay un control para la restricción de instalación de software
8. Si hay un mantenimiento preventivo a los equipos informáticos
9. Si hay un ordenamiento estructurado en los gabinetes
10. Si hay un control en la operatividad de la red
11. Si cuenta con políticas y normas de seguridad de información
12. Si hay una gestión de la clave de los servidores
13. Si hay planes para mitigar los riesgos de la red

6.5. ANALISIS DE LOS HALLAZGOS INICIALES

1. Si hay un registro para la cantidad de usuarios que tienen acceso a la red interna

ANALISIS: Se implementó una salvaguarda para este hallazgo que se observó en la Auditoria porque es fundamental para el hospital poder identificar y controlar quienes son los usuarios que tienen disponibilidad de los servicios que ofrece la red interna

2. Si hay un registro para la cantidad de usuarios creados con su contraseña

ANALISIS: Se implementó una salvaguarda para este hallazgo que se observó en la Auditoria porque es fundamental para el hospital poder identificar cuantos usuarios tienen una cuenta para poder realizar sus actividades diarias en un equipo informático de escritorio.

3. Si hay un control para el nivel de seguridad de las contraseñas de los usuarios

ANALISIS: Se implementó una salvaguarda para este hallazgo que se observó en la Auditoria porque es fundamental para el hospital poder proteger la información que cada usuario genera en su actividad diaria, con la finalidad de establecer medidas de seguridad en la estructura de la contraseña generada por cada usuario.

4. Si hay medidas adicionales para controlar los niveles de privilegios de acceso

ANALISIS: Se implementó una salvaguarda para este hallazgo que se observó en la Auditoria porque es fundamental para el hospital saber que usuarios tienen los privilegios de acceso a los servicios que brinda la red interna y poder clasificarlos según el privilegio de usuario.

5. Si hay medidas adicionales para controlar el cambio de contraseña de los usuarios

ANALISIS: Se implementó una salvaguarda para este hallazgo que se observó en la Auditoria porque es fundamental para el hospital saber que usuarios cambian su contraseña para proteger su información y además quienes hacen caso a las normas de seguridad que el área de informática plantea.

6. Si hay medidas adicionales para que el antivirus este activo

ANALISIS: Se implementó una salvaguarda para este hallazgo que se observó en la Auditoria porque es fundamental para el hospital poder identificar las amenazas del virus en la información para poder mitigarlos de una manera eficaz, práctica y sencilla.

7. Si hay un control para la restricción de instalación de software

ANALISIS: Se implementó una salvaguarda para este hallazgo que se observó en la Auditoria porque es fundamental para el hospital implementar controles para que ningún usuario deba instalar algún software ajenos a los que el hospital establece y usa para la ejecución de sus procesos, en caso a ello el usuario debe de enviar un documento del software que desee instalar y el motivo del uso.

8. Si hay un mantenimiento preventivo a los equipos informáticos

ANALISIS: Se implementó una salvaguarda para este hallazgo que se observó en la Auditoria porque es fundamental para el hospital poder realizar un mantenimiento preventivo de los equipos con la finalidad de evitar fallas de ellos, esto estaría de la mano junto al inventario de TI,

9. Si hay un ordenamiento estructurado en los gabinetes

ANALISIS: Se implementó una salvaguarda para este hallazgo que se observó en la Auditoria porque es fundamental para el hospital poder identificar los puertos de red del switch con disponibilidad a ser usado por un nuevo usuario.

10. Deficiente control en la operatividad de la red

ANALISIS: Se implementó una salvaguarda para este hallazgo que se observó en la Auditoria porque es muy importante generar costo al momento de adquirir algunos switch de capa 3 para poder implementar las vlan, pero este hallazgo es fundamental para el hospital porque permite mantener la operatividad de la red en buen estado, para que los usuarios puedan realizar sus actividades diarias sin retraso alguno.

11. Si cuenta con políticas y normas de seguridad de información

ANALISIS: Se implementó una salvaguarda para este hallazgo que se observó en la Auditoria porque es fundamental para el hospital tener una documentación acerca de las políticas de seguridad de información que el área de informatica establece y en donde los usuarios acaten las normas de seguridad de información.

12. Si hay una gestión de la clave de los servidores

ANALISIS: Se implementó una salvaguarda para este hallazgo que se observó en la Auditoria porque es fundamental para el hospital saber cuáles son las contraseñas de los servidores y gestionarlas mediantes sobres donde el único autorizado en tenerlas sea el jefe del área de informatica.

13. Si hay planes para mitigar los riesgos de la red

ANALISIS: Se implementó una salvaguarda para este hallazgo que se observó en la Auditoria porque es fundamental para el hospital saber cuáles son las medidas de mitigación de riesgos que tienen cada uno de los encargados del área de informatica.

6.6. RELACION DE LOS HALLAZGOS FINALES

1. Si hay un registro para la cantidad de usuarios que tienen acceso a la red interna
2. Si hay un registro para la cantidad de usuarios creados con su contraseña
3. Si hay un control para el nivel de seguridad de las contraseñas de los usuarios
4. Si hay medidas adicionales para controlar los niveles de privilegios de acceso
5. Si hay de medidas adicionales para controlar el cambio de contraseña de los usuarios
6. Si hay medidas adicionales para que el antivirus este activo
7. SI hay un control para la restricción de instalación de software
8. Si hay un mantenimiento preventivo a los equipos informáticos
9. Si hay un ordenamiento estructurado en los gabinetes
10. Si hay un control en la operatividad de la red
11. Si cuenta con políticas y normas de seguridad de información
12. Si hay una gestión de la clave de los servidores
13. Si hay planes para mitigar los riesgos de la red

MATRIZ DE ANALISIS DE HALLAZGOS

MATRIZ DE ANALISIS DE HALLAZGOS						
N°	HALLAZGO	TIPO	DESCRIPCIÓN	OBJETIVO	NORMATIVA	EVIDENCIA
1	Si hay un registro para la cantidad de usuarios que tienen acceso a la red interna	NOMINAL	En la revisión que se hizo en la seguridad lógica se pudo identificar que se implementó un registro de la cantidad de usuarios que tienen acceso a la red interna del hospital.	Identificar la cantidad de usuarios que tienen acceso a la red interna del hospital	**Norma ISO/IEC 27001:2013** En el punto 9.4. (Control de Acceso a la Red) refiere que hay que asegurarse que el acceso de los usuarios a las redes y sus servicios no comprometan la seguridad de dichos servicios	DOCUMENTO 1
2	Si hay un registro para la cantidad de usuarios creados con su contraseña	NOMINAL	En la revisión que se hizo en la seguridad lógica se pudo identificar que se implementó un registro de la cantidad de usuarios que existen y que tienen un equipo informático de disponibilidad en el hospital San Bartolomé	Identificar la cantidad de usuarios creados con su contraseña	**Norma ISO/IEC 27001:2013** En el punto 9.4. (Control de Acceso a la Red) refiere que hay que asegurarse que el acceso de los usuarios a las redes y sus servicios no comprometan la seguridad de dichos servicios	DOCUMENTO 2
3	Si hay un control para el nivel de seguridad de las contraseñas de los usuarios	NOMINAL	En la revisión que se hizo en la seguridad lógica se pudo identificar que se realizó un manual con la cantidad de caracteres para las contraseñas usuarios de red, correos y sistemas internos en el hospital San Bartolomé	Identificar el nivel seguridad que tienen las contraseñas de los usuarios	**Norma ISO/IEC 27001:2013** En el punto 9.4. (Control de Acceso a la Red) refiere que hay que asegurarse que el acceso de los usuarios a las redes y sus servicios no comprometan la seguridad de dichos servicios	DOCUMENTO 3
4	Si hay medidas adicionales para controlar los niveles de privilegios de acceso	NOMINAL	En la revisión que se hizo en la seguridad lógica se pudo identificar que se implementó un registro de control de los privilegios de acceso que tienen cada usuario para acceder a la red interna en el hospital San Bartolomé	Identificar los niveles de privilegios de acceso que tienen los usuarios	**Norma ISO/IEC 27001:2013** En el punto 9.4. (Control de Acceso a la Red) refiere que hay que asegurarse que el acceso de los usuarios a las redes y sus servicios no comprometan la seguridad de dichos servicios	DOCUMENTO 4

5	Si hay medidas adicionales para controlar el cambio de contraseña de los usuarios	NOMINAL	En la revisión que se hizo en la seguridad lógica se pudo identificar que se tiene un registro de los usuarios que deban de cambiar su contraseña por el tipo de información que manejan en su PC en el hospital San Bartolomé	Identificar el periodo de cambio de contraseñas de los usuarios	**Norma ISO/IEC 27001:2013** En el punto 9.4. (Control de Acceso a la Red) refiere que hay que asegurarse que el acceso de los usuarios a las redes y sus servicios no comprometan la seguridad de dichos servicios	DOCUMENTO 5
6	Si hay medidas adicionales para que el antivirus este activo	NOMINAL	En la revisión que se hizo en la seguridad física se pudo identificar qué el antivirus se mantiene activo y restringe implementó un usuario administrador al momento de instalar algún software interno o externo dentro de un usuario de red en el hospital San Bartolomé	Identificar si el antivirus está activo	**Norma ISO/IEC 27001:2013 En el punto 12.6.2 (Restricciones en la instalación de software)** se refiere que hay que tener permisos de la alta dirección para poder instalar un software ajeno a los requerimientos que tiene la organización y documentación del uso que se quiera dar al software	DOCUMENTO 6
7	Si hay un control para la restriccion de instalacion de software	NOMINAL	En la revisión que se hizo en la seguridad lógica se pudo identificar que el servidor del antivirus está activo y envía a cuarentena los posibles usuarios de red que están emitiendo virus, además se restringe el acceso de dispositivos de almacenamiento con la finalidad de no infectar con algún virus la información en el hospital San Bartolomé	Identificar si existe la restricción de instalación de software	**Norma ISO/IEC 27001:2013 En el punto 14 (Adquisición, desarrollo y mantenimiento de sistemas)** se refiere que hay que tener un plan preventivo y correctivo para los equipos informáticos, dado que no se tiene que perjudicar la operatividad de la red y las actividades de los usuarios.	DOCUMENTO 7
8	No hay un mantenimiento preventivo a los equipos informaticos	NOMINAL	En la revisión que se hizo en la seguridad física se pudo identificar que se tiene un plan preventivo de los equipos informáticos en el hospital San Bartolomé	Identificar si existe mantenimiento preventivo y correctivo de los equipos informáticos.	**Norma ISO/IEC 27001:2013 En el punto 12 (seguridad en las operaciones)** se refiere que hay que tener una operatividad correcta y eficaz de la red para no afectar a los procesos de información	DOCUMENTO 8

9	No hay un ordenamiento estructurado en los gabinetes	NOMINAL	En la revisión que se hizo en la seguridad física se pudo identificar que se tiene implementado los estándares de cableado estructurado en los gabinetes en el hospital San Bartolomé	Identificar si existe un ordenamiento estructurado en los gabinetes de la empresa para la supervisión de próximas auditorias.	**ANSI/TIA/EIA-569** El estándar provee especificaciones para el diseño de las instalaciones y la infraestructura edilicia necesaria para el cableado de telecomunicaciones en edificios.	DOCUMENTO 9
10	No hay un control de acceso de la situacion actual de la sala de servidores	NOMINAL	En la revisión que se hizo en la seguridad física se pudo identificar que se tienen los estándares para la sala de servidores ya sea en energía eléctrica, aire acondiciado, cableado estructurado y espacio en el hospital San Bartolomé	Identificar la situación actual de la sala de servidores	estándares **ANSI/TIA/EIA** exigen administrar las instalaciones, incluyendo el equipo de comunicaciones, está referido a las prácticas de diseños y construcción las cuales darán soporte a los medios de transmisión y al área de trabajo correcto. Estos estándares permitirán instalar una planta de cableado estructurado genérico que podrá hacer funcionar cualquier aplicación de datos y de voz, cumpliendo con la seguridad y ciertas restricciones. **ANSI/TIA/EIA-569** Determina los diferentes métodos para implementar el cableado estructurado. Respetando las reglas para las implementaciones y medidas que el estándar propone para la correcta implementación de un cableado estructurado.	DOCUMENTO 10
11	No cuenta con politicas y normas de seguridad de informacion	NOMINAL	En la revisión que se hizo en la seguridad de redes se identificó que la seguridad de redes cuenta con todas las políticas de seguridad por el motivo que no se tiene una documentación de políticas y normas de seguridad en el hospital San Bartolomé	Identificar si cuenta con políticas y normas de seguridad de información	**Norma ISO/IEC 27001:2013 En el punto 5 (Políticas de seguridad de la información)** se refiere que hay que tener un documento de las políticas de seguridad e implementarlas dentro de nuestra red interna	DOCUMENTO 11

11	No cuenta con politicas y normas de seguridad de informacion	NOMINAL	En la revisión que se hizo en la seguridad de redes se identificó que la seguridad de redes cuenta con todas las políticas de seguridad por el motivo que no se tiene una documentación de políticas y normas de seguridad en el hospital San Bartolomé	Identificar si cuenta con políticas y normas de seguridad de información	**Norma ISO/IEC 27001:2013 En el punto 5 (Políticas de seguridad de la información)** se refiere que hay que tener un documento de las políticas de seguridad e implementarlas dentro de nuestra red interna	DOCUMENTO 11
12	Administracion incorrecta de claves de los servdores	NOMINAL	En la revisión que se hizo en la seguridad de redes se identificó que no se tiene un registro de las contraseñas que se modifican en los servidores del área de servidores en el hospital San Bartolomé	Identificar las claves de los servidores	**Norma ISO/IEC 27001:2013 En el punto 9.4. (Control de Acceso a la Red)** refiere que hay que asegurarse que el acceso de los usuarios a las redes y sus servicios no comprometan la seguridad de dichos servicios	DOCUMENTO 12
13	No cuenta con procedimiento para fallas de red en la infraestrutura de red	NOMINAL	En la revisión que se hizo en la seguridad de redes se identificó que se tiene un plan personal y general para mitigar los riesgos de la red en el hospital San Bartolomé	Identificar planes para mitigar los riesgos de la red	**Norma ISO/IEC 27001:2013 En el punto 8 (Gestión de activos)** refiere que hay que tener documentado los activos de información para no depender de personas que falten a sus labores y poder administrar de una manera perfecta los equipos intermedios y administración de la red interna de la organización.	DOCUMENTO 13

SOLICITUDES

MATRIZ DE RIESGOS MAGERIT

SOLICITUD NUMERO 01: PERMISO DE AUDITORIA

SOLICITA: "PERMISO DE AUDITORIA"

SEÑOR: **ING. SISTEMAS. SPILCO LEON JARDY**

JEFE DEL AREA DE SISTEMA E INFORMATICA

Yo JERSON CALDERON ALVARADO, identificado con DNI No. 76034606, actualmente cursando el Décimo ciclo de la carrera de Ingeniería de Sistemas de la Universidad Cesar Vallejo, ante Ud., con el debido respeto me presento y expongo:

Se me brinde el permiso de auditoria de dicha institución para poder realizar mi tesis titulada "Herramienta de gestión de riesgos para la seguridad informatica" y poder beneficiar a dicha institución con la identificación de sus hallazgos y poder implementar mejoras.

POR LO TANTO:

Solicito a usted acceder a mi petición para alcanzar a dicha información solicitada

Los Olivos, 05 de Junio del 2017

MINISTERIO DE SALUD
HONADOMANI "SAN BARTOLOME"
Ing. JARDY L. ESPILCO LEON
JEFE DE LA UNIDAD DE INFORMATICA Y S.
C.P. N° 14713

JERSON CALDERON ALVARADO

DNI. Nro. 76034606

SOLICITUD NUMERO 02: CRONOGRAMA DE VISITAS A LA EMPRESA

SOLICITA: "CRONOGRAMA DE VISITA"

SEÑOR: **ING. SISTEMAS. SPILCO LEON JARDY**

JEFE DEL AREA DE SISTEMA E INFORMATICA

Yo, JERSON CALDERON ALVARADO, identificado con DNI No. 76034606, actualmente cursando el Décimo ciclo de Ingeniería de Sistemas de la Universidad Cesar Vallejo, ante Ud., con el debido respeto me presento y expongo:

Que, los días 06, 07, 08, 09, 10 y 12 de Junio del 2017 asistiré al hospital Nacional San Bartolomé en las horas de la mañana de 10:00 a 12:00 horas al área de Sistemas, para poder realizar la Auditoria de tecnologías de información.

POR LO TANTO:

Solicito a usted acceder a mi petición para alcanzar a dicha información solicitada

Los Olivos, 05 de Junio del 2017

JERSON CALDERON ALVARADO

DNI. Nro. 76034606

SOLICITUD NUMERO 03: RECOJO DE EVIDENCIAS PARA LA AUDITORIA INFORMATICA

SOLICITA: RECOJO DE EVIDENCIAS,

SEÑOR: **ING. SISTEMAS. SPILCO LEON JARDY**

JEFE DEL AREA DE SISTEMA E INFORMATICA

Yo JERSON CALDERON ALVARADO, identificado con DNI No. 76034606, actualmente cursando el Décimo ciclo de la carrera de Ingeniería de Sistemas de la Universidad Cesar Vallejo, ante Ud., con el debido respeto me presento y expongo:

Se me brinde el documento de plan de contingencia u otros y se me sellen las fotos para que tomen valides y credibilidad en esta Auditoria de tecnologías de información.

POR LO TANTO:

Solicito a usted acceder a mi petición para alcanzar a dicha información solicitada

Los Olivos, 06 de Junio del 2017

MINISTERIO DE SALUD
HONADOMANI "SAN BARTOLOME"
ING. JARDY R. SPILCO LEON
JEFE DE LA UNIDAD DE INFORMATICA Y S.
C.I.P. Nº 147113

JERSON CALDERON ALVARADO

DNI. Nro. 76034606

EVIDENCIAS

PROPUESTA DE PLAN DE ACCIÓN DE LISTAS DE USUARIOS CON ACCESO A LA RED

(Presentada por Jerson Calderón Alvarado)

Según la Auditoria,

Considerando los hallazgos que se encontraron en la Auditoria que se realizó el 26 de Octubre hasta el 02 de Noviembre del 2016, se pudo identificar una salvaguarda según la metodología magerit, que nos permitirá mitigar la amenaza “Mal control de accesos de red”

Objetivo Específico:

- Identificar la cantidad de usuarios que tienen acceso a la red interna del hospital.

Requerimiento de cada objetivo específico Según la ISO27001:2013

- En el punto 9.4. (Control de Acceso a la Red) refiere que hay que asegurarse que el acceso de los usuarios a las redes y sus servicios no comprometan la seguridad de dichos servicios

Actividades para cumplir con el Objetivo específico:

- Se debe de mantener actualizado cada 10 días el registro de cantidad de usuarios

PROPUESTA DE PLAN DE ACCIÓN DE LISTAS DE USUARIOS CON ACCESO A LA RED

CAPITULO I

PASOS PARA LA IMPLEMENTACION

1. Se establecerá perfiles de accesos según el usuario
2. Se clasificara los tipos de páginas por ancho de banda, con la finalidad que no se congestione la red
3. Se realizara un formato de accesos de red, para que el usuario pueda solicitar las páginas de acceso y fundamentar el porqué de dichos accesos
4. Se realizara un registro de las ip's para monitorear dichos accesos de red.
5. Cada vez que exista una configuración de red, se tendrá que identificar si las ip's de los usuarios de gerencia se han modificado, con la finalidad que no pierdan sus accesos de red.

CAPITULO II

PERFILES DE ACCESOS

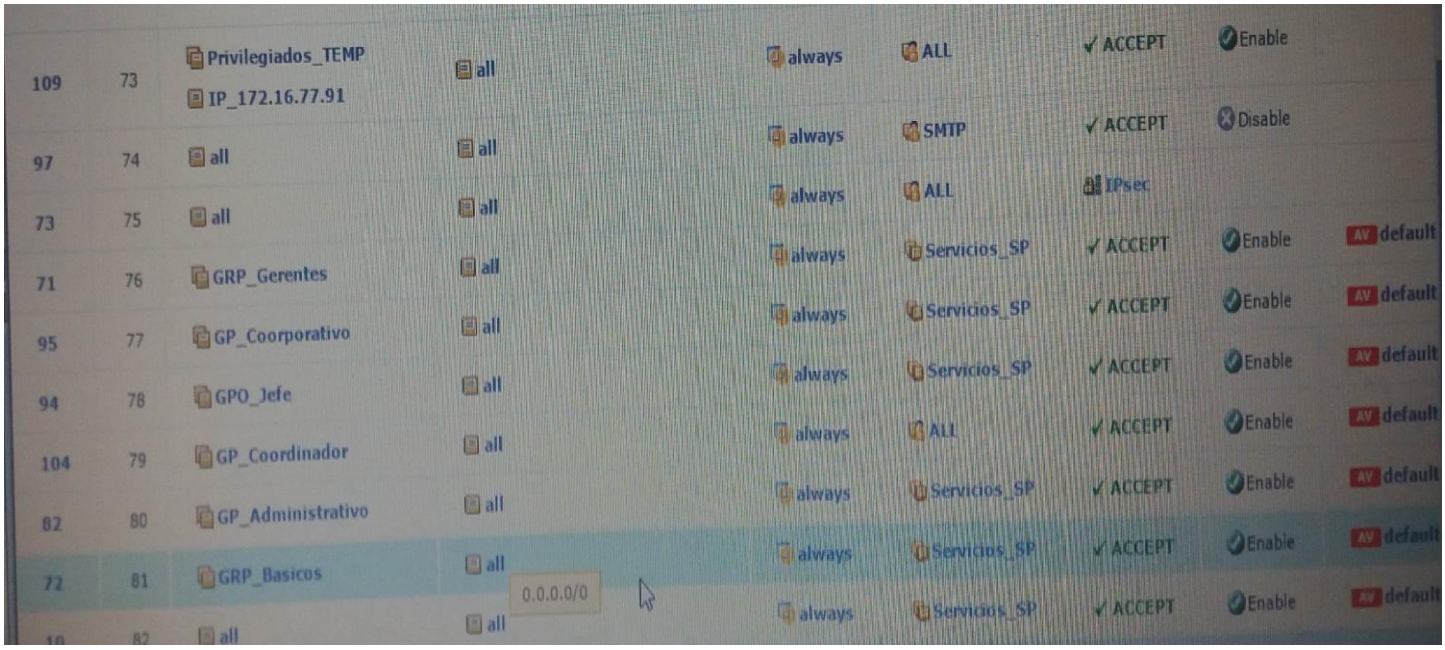
1. En la figura N°1 se muestra cómo se tiene distribuido los perfiles de accesos a la red

Figuera N°1

#	Nombre de Perfil	Permisos
1	Gerentes	TODO
2	Corporativos	TODO menos (Youtube)
3	Jefes	TODO menos (Youtube, Remoto)
4	Coordinadores	TODO menos (Streaming, Remoto, Redes Sociales)
5	Administrativos	TODO menos (Streaming, Remoto, Redes Sociales, Descarga de Archivos, Correos Personales)
6	Admisionistas	Solo traductor google, paginas aseguradoras, Sitecs.

Nombres y descripción de los perfiles de acceso

Figura N°2



Perfiles de accesos creados en el firewall

CAPITULO III

MONITOREO Y MEJORA

1. Al momento que se incorpore un usuario, la lista se tendrá que modificar en ese mismo día, para poder entregar un informe cada 10 días.
2. Se tendrá que monitorear la lista de accesos a la red cada 10 días, con la finalidad de mantener un nivel de cumplimiento adecuado.
3. Al momento que se tenga la lista, se podrá identificar si la red no se congestionara si se siguen aumentando más usuarios.
4. Si existe el caso de poder mejorar esta salvaguarda se tendrá de realizar
5. Al momento que se mejore la salvaguarda, aumentará de versión para tenerlo como material histórico en una auditoria

CAPITULO IV

CONCLUSION

1. La salvaguarda ha ayudado al área de infraestructura a poder administrar y controlar de una mejor manera los perfiles de accesos del internet.
2. Este documento ha ayudado al área de infraestructura a tener material para presentar a la alta gerencia, de que están trabajando y que tienen mapeado de una manera correcta toda la información de la red de la organización

PROPUESTA DE PLAN DE ACCIÓN DE LISTAS DE CUENTAS ACTIVAS

(Presentada por Jerson Calderón Alvarado)

Según la Auditoria,

Considerando los hallazgos que se encontraron en la Auditoria que se realizó el 26 de Octubre hasta el 02 de Noviembre del 2016, se pudo identificar una salvaguarda según la metodología magerit, que nos permitirá mitigar la amenaza “Mal control de usuarios de red”

Objetivo Específico:

- Identificar la cantidad de usuarios creados con su contraseña

Requerimiento de cada objetivo específico Según la ISO27001:2013

- En el punto 9.4. (Control de Acceso a la Red) refiere que hay que asegurarse que el acceso de los usuarios a las redes y sus servicios no comprometan la seguridad de dichos servicios

Actividades para cumplir con el Objetivo específico:

- Se debe de mantener actualizado cada 30 días el registro de cantidad de usuarios que tienen una cuenta de acceso

PROPUESTA DE PLAN DE ACCIÓN DE LISTAS DE USUARIOS CON ACCESO A LA RED

CAPITULO I

PASOS PARA LA IMPLEMENTACION

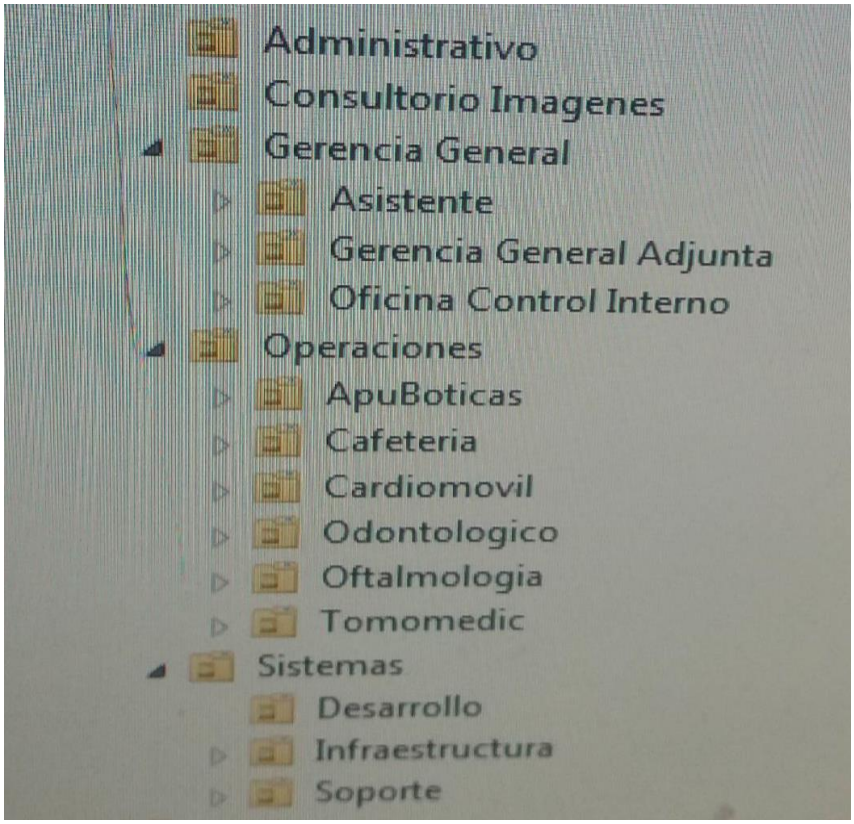
1. Se clasificara por área de trabajo en el active directory a cada usuario
2. Se tendrá que llenar un formato de creación de usuarios, firmada por el jefe del área y con la función que desempeñara el usuario
3. Se creara al usuario por inicial de nombre y apellido completo
4. Se tendrá un registro de los usuarios y el área donde pertenecen

CAPITULO II

PERFILES DE ACCESOS

1. En la figura N°1 se muestra cómo se tiene clasificado los usuarios en el active directory

Figura N°1



Estructura de usuarios de red en el Active Directory

CAPITULO III

FORMATO DE CREACION DE USUARIOS DE RED

Figura N°2

HOSPITAL SAN BARTOLOMÉ	FORMATO N°1 SOLICITUD DE CREACION DE USUARIOS DE RED	Código:	CSP.GTI.F.XX
		Versión:	V.01
		Vigencia:	XX/01/2017
		Página:	1 de 1

SOLICITUD DE CREACION DE USUARIOS DE RED	
NOMBRES Y APELLIDOS:	
CARGO:	
ÁREA:	
PERIODO DE CONTRATO	
IP :	. . .
SUSTENTO DE CREACION DE USUARIOS:	

V°B° JEFE DE INFRAESTRUCTURA TI

V°B° JEFE DE AREA

V°B° JEFE DE MESA DE AYUDA TI

CAPITULO IV

MONITOREO Y MEJORA

1. Al momento que se incorpore un usuario, la lista se tendrá que modificar en ese mismo día, para poder entregar un informe cada 30 días.
2. Se tendrá que monitorear la lista de usuarios de red cada 30 días, con la finalidad de mantener un nivel de cumplimiento adecuado.
3. Al momento que se tenga la lista, se podrá identificar si la red no se congestionara si se siguen aumentando más usuarios.
4. Si existe el caso de poder mejorar esta salvaguarda se tendrá de realizar
5. Al momento que se mejore la salvaguarda, aumentará de versión para tenerlo como material histórico en una auditoria

PROPUESTA DE PLAN DE ACCIÓN DE POLITICAS Y ADMINISTRACION DE CONTRASEÑAS

(Presentada por Jerson Calderón Alvarado)

Según la Auditoria,

Considerando los hallazgos que se encontraron en la Auditoria que se realizó el 26 de Octubre hasta el 02 de Noviembre del 2016, se pudo identificar una salvaguarda según la metodología magerit, que nos permitirá mitigar la amenaza “Error de acceso a la red”

Objetivo Específico:

- Identificar el nivel seguridad que tienen las contraseñas de los usuarios

Requerimiento de cada objetivo específico Según la ISO27001:2013

- En el punto 9.4. (Control de Acceso a la Red) refiere que hay que asegurarse que el acceso de los usuarios a las redes y sus servicios no comprometan la seguridad de dichos servicios

Actividades para cumplir con el Objetivo específico:

- Se debe de hacer seguimiento a la creación de contraseñas de los usuarios para mejorar y establecer una seguridad alta de cuenta

PROPUESTA DE PLAN DE ACCIÓN DE ESTABLECER POLITICAS Y ADMINISTRACION DE CONTRASEÑAS

CAPITULO I

PASOS PARA LA IMPLEMENTACION

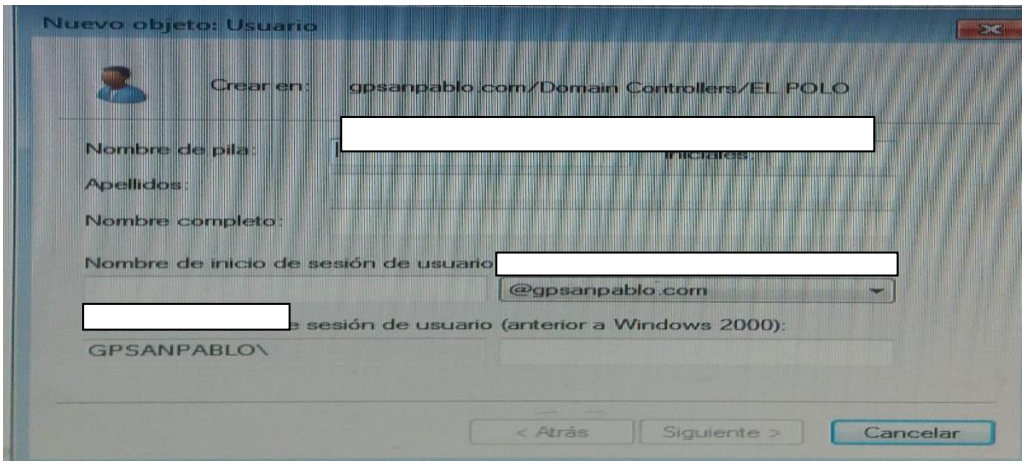
1. Se clasificara por usuario de red, correo y dispositivo intermedio.
2. En caso sea usuario de red se pondrá una palabra mayor a 5 caracteres
3. En caso sea correo se tendrán 8 caracteres con una concatenación de doble inicial de nombre en minúscula, doble inicial de apellido en mayúscula, doble carácter especial y doble numero
4. Se tendrá un registro de las contraseñas de los usuarios de red, en caso se puedan olvidar y requieran la contraseña.
5. En caso sea un dispositivo intermedio, el administrador de redes tendrá que manejar como mínimo 12 caracteres, para mantener seguridad de la red.
6. El administrador de redes deberá tener una concatenación en sus contraseñas
7. El administrador de redes tendrá que modificar sus contraseñas cada 7 días
8. El administrador de red tendrá que escribir su contraseña y ponerlo en un sobre, guardarlo en un cajón con llave, en caso falte por motivos personales o salud.
9. El área de infraestructura tiene la responsabilidad de las contraseñas de cada dispositivo intermedio.

CAPITULO II

PERFILES DE ACCESOS

1. En la figura N°1 se muestra cómo se tiene creado la contraseña de un usuario de red en el active directory

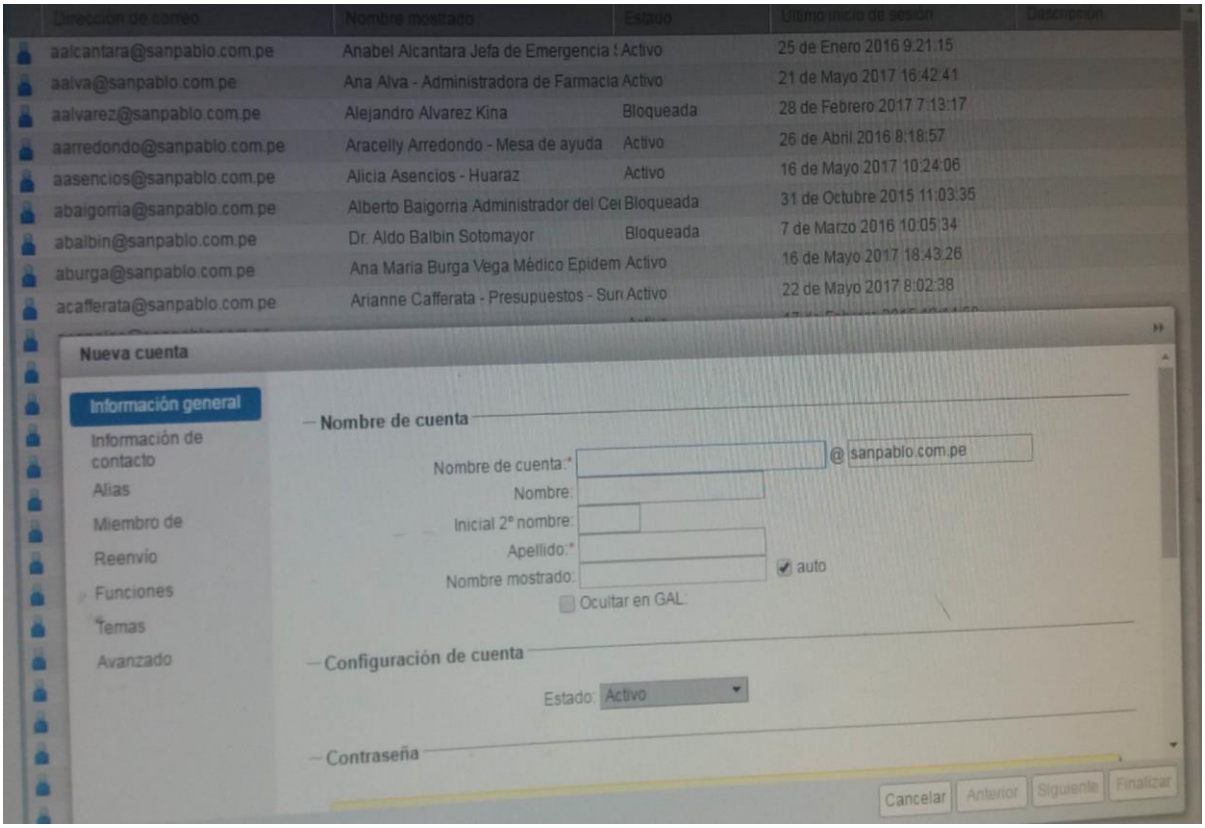
Figura N°1



CREACION DE USUARIOS DE RED EN EL ACTIVE DIRECTORY

2. En la figura N°2 se muestra como se tiene creado la contraseña de un correo en el servidor zimbra

FIGURA N°2.



Creación de correos electrónicos en el servidor ZIMBRA

CAPITULO III

MONITOREO Y MEJORA

1. Al momento que se genere una contraseña, esta se tendrá que poner en un registro para poder monitorearlas en caso el usuario lo requiera, la lista se tendrá que modificar en ese mismo día, para poder entregar un informe cada 30 días.
2. Se tendrá que monitorear la lista de contraseñas de usuarios cada 30 días, con la finalidad de mantener un nivel de cumplimiento adecuado.
3. Al momento que se tenga la lista, se podrá mantener la integridad de la información de los usuarios y de la organización
4. Si existe el caso de poder mejorar esta salvaguarda se tendrá de realizar
5. Al momento que se mejore la salvaguarda, aumentará de versión para tenerlo como material histórico en una auditoria

CAPITULO IV

CONCLUSIONES

1. Esta salvaguarda ayuda al área de infraestructura a tener un registro y control de los usuarios de red creado.
2. Esta salvaguarda ayuda al administrador de usuarios de red a poder tener una estructura adecuada un su trabajo
3. Esta salvaguarda ayuda al administrador de usuarios de red a poder tener
4. Esta salvaguarda ayuda a estar preparados a próximas auditorías internas o externas

PROPUESTA DE PLAN DE ACCIÓN DE GRUPOS DE ACCESO A INTERNET

(Presentada por Jerson Calderón Alvarado)

Según la Auditoria,

Considerando los hallazgos que se encontraron en la Auditoria que se realizó el 26 de Octubre hasta el 02 de Noviembre del 2016, se pudo identificar una salvaguarda según la metodología magerit, que nos permitirá mitigar la amenaza “Error de acceso a la red”

Objetivo Específico:

- Identificar los niveles de privilegios de acceso que tienen los usuarios

Requerimiento de cada objetivo específico Según la ISO27001:2013

- En el punto 9.4. (Control de Acceso a la Red) refiere que hay que asegurarse que el acceso de los usuarios a las redes y sus servicios no comprometan la seguridad de dichos servicios

Actividades para cumplir con el Objetivo específico:

- Se debe de controlar y mejorar el nivel de acceso que tiene cada usuario al acceso y privilegios que debe de tener a la red interna

PROPUESTA DE PLAN DE ACCIÓN DE GRUPOS DE ACCESO A INTERNET

CAPITULO I

PASOS PARA LA IMPLEMENTACION

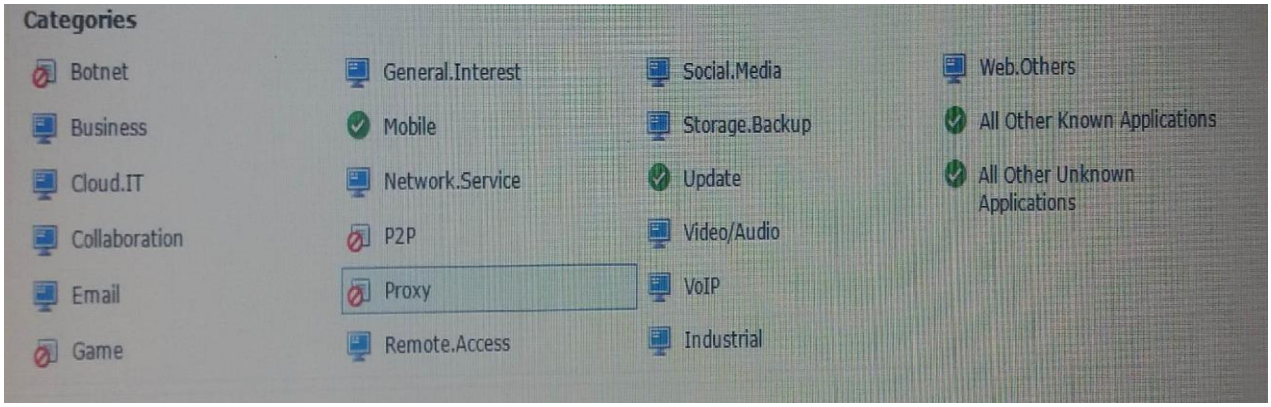
1. Teniendo en cuenta la salvaguarda 1, en establecer perfiles de accesos.
2. Cada perfil de usuario que se cree, tendrá accesos distintos
3. Cada acceso del perfil se distinguirá por velocidad de ancho de banda
4. Se tendrá en un registro los tipos de accesos que tendrán cada perfil de usuario
5. En caso el usuario requiere tener un acceso distinto a su perfil, su jefe de área tendrá que mandar un correo solicitando dicho acceso y el sustento del porque el acceso.
6. El administrador de redes deberá monitorear los accesos de perfiles de usuario para que no haya incidencias de accesos de red

CAPITULO II

PERFILES DE ACCESOS A INTERNET

1. En la figura N°1 se muestra cómo los accesos de cada perfil de usuario

Figura N°1



Tipos de servicios de un perfil de acceso a internet

3. En la figura N°2 se muestra el formato de accesos a la red

HOSPITAL SAN BARTOLOMÉ	FORMATO N°1 SOLICITUD DE ACCESOS: PAGINAS WEB -	Código:	CSP.GTI.F.XX
		Versión:	V.01
		Vigencia:	XX/01/2017
		Página:	1 de 1

SOLICITUD DE ACCESOS: PAGINAS WEB	
NOMBRES Y APELLIDOS:	
CARGO:	
ÁREA:	
USUARIO DE RED:	
IP :	. . .

PERFILES DE NAVEGACIÓN

Seleccione con un circulo, su perfil:

Ítem	Nombre de Perfil	Permisos
1	Gerentes	TODO
2	Corporativos	TODO menos (YouTube)
3	Jefes	TODO menos (YouTube, Remoto)
4	Coordinadores	TODO menos (Streaming, Remoto, Redes Sociales)
5	Administrativos	TODO menos (Streaming, Remoto, Redes Sociales, Descarga de Archivos, Correos Personales)
6	Admisionistas	Solo traductor google, paginas aseguradoras, Siteds.

SUSTENTO:	

_____
V°B° JEFE DE INFRAESTRUCTURA TI

_____
V°B° JEFE DE AREA

_____
V°B° JEFE DE MESA DE AYUDA TI

CAPITULO III

MONITOREO Y MEJORA

1. Al momento que se genere un nuevo acceso de red en el perfil de usuario, esta se tendrá que poner en un registro para poder monitorearlas en caso el usuario lo requiera, la lista se tendrá que modificar en ese mismo día, para poder entregar un informe cada 15 días.
2. Se tendrá que monitorear la lista de accesos a internet cada 30 días, con la finalidad de mantener un nivel de cumplimiento adecuado.
3. Al momento que se tenga la lista, se podrá mantener la disponibilidad de la información del internet
4. Si existe el caso de poder mejorar esta salvaguarda se tendrá de realizar
5. Al momento que se mejore la salvaguarda, aumentará de versión para tenerlo como material histórico en una auditoria

CAPITULO IV

MONITOREO Y MEJORA

1. Esta salvaguarda ha ayudado a poder administrar de una manera correcta los accesos al internet, teniendo como principal factor un formato de solicitud de accesos.
2. Este formato ayuda al área de infraestructura a poder tener material histórico respecto a los accesos de un usuario.
3. Esta salvaguarda muestra a la alta gerencia que el área de infraestructura tiene ganas de trabajar y de hacer las cosas sin perjudicar al usuario.
4. Esta salvaguarda concientiza al usuario que existen políticas de seguridad informatica, y que tienen que pedir dicho formato.

PROPUESTA DE PLAN DE ACCIÓN DE GUIA PARA MANTENIMIENTO DE CONTRASEÑAS

(Presentada por Jerson Calderón Alvarado)

Según la Auditoria,

Considerando los hallazgos que se encontraron en la Auditoria que se realizó el 26 de Octubre hasta el 02 de Noviembre del 2016, se pudo identificar una salvaguarda según la metodología magerit, que nos permitirá mitigar la amenaza "Error de accesos de usuarios"

Objetivo Específico:

- Identificar el periodo de cambio de contraseñas de los usuarios

Requerimiento de cada objetivo específico Según la ISO27001:2013

- En el punto 9.4. (Control de Acceso a la Red) refiere que hay que asegurarse que el acceso de los usuarios a las redes y sus servicios no comprometan la seguridad de dichos servicios

Actividades para cumplir con el Objetivo específico:

- Se debe de hacer un seguimiento, control y mejorar el nivel de seguridad de contraseñas para aquellos usuarios que lo requieran.

CAPITULO I

PASOS PARA LA IMPLEMENTACION

1. Establecer una guía para que el usuario pueda cambiar su contraseña, según periodos determinados que establezca el administrador de usuarios de red.
2. La contraseña debe de tener como mínimo 5 caracteres, entre letras y números
3. Al momento que el usuario cambia su contraseña debe de mandar un correo al área de mesa de ayuda que hizo una actualización de su contraseña.
4. El usuario tiene toda la responsabilidad de mantener en secreto su contraseña.
5. El usuario tiene toda la responsabilidad de mantener en privacidad la información de su PC.

CAPITULO II

MONITOREO Y MEJORA

1. El registro que se haga respecto a la actualización de contraseñas, se monitorearan cada 30 días.
2. Si existe la posibilidad de mejorar la salvaguarda se procederá con la versión 2.

PROPUESTA DE PLAN DE ACCIÓN DE DESARROLLO E IMPLEMENTACION DE DIRECTRICES Y CONTROLES PAEA LA DETECCION Y TRATAMIENTO DE SOFTWARE

(Presentada por Jerson Calderón Alvarado)

Según la Auditoria,

Considerando los hallazgos que se encontraron en la Auditoria que se realizó el 26 de Octubre hasta el 02 de Noviembre del 2016, se pudo identificar una salvaguarda según la metodología magerit, que nos permitirá mitigar la amenaza “Daño de información”

Objetivo Específico:

- Identificar si el antivirus está activo

Requerimiento de cada objetivo específico Según la ISO27001:2013

- En el punto 12 (seguridad en las operaciones) se refiere que hay que tener una operatividad correcta y eficaz de la red para no afectar a los procesos de información

Actividades para cumplir con el Objetivo específico:

- Se debe de tener un registro de aquellos equipos informáticos que están con el antivirus actualizado y un manual de la forma correcta de eliminar un archivo infectado en un usuario de red

PROPUESTA DE PLAN DE ACCIÓN DE DESARROLLO E IMPLEMENTACION DE DIRECTRICES Y CONTROLES PAEA LA DETECCION Y TRATAMIENTO DE SOFTWARE

CAPITULO I

PASOS PARA LA IMPLEMENTACION

1. Se verificara si la maquina tiene virus.
2. Se procederá con la eliminación del virus, a través del análisis del antivirus.
3. Luego se eliminaran los archivos temporales.
4. Luego se habilitaran los archivos ocultos y dentro de la carpeta app se eliminaran los archivos temporales que quedan.
5. Luego se tendrá que pasar el ccleaner para eliminar algunos archivos temporales que no se hayan borrado.
6. En caso no se elimine el virus, se procederá con formatear la pc y luego hacer todos los pasos anteriores.

CAPITULO IV

MONITOREO Y MEJORA

1. Si existe algún método mejor en eliminar un virus se añadirá a los pasos para la implementación.
2. Se tendrá que hacer un seguimiento a esta salvaguarda para prevenir las vulnerabilidades que pueda sufrir un activo de información.

PROPUESTA DE PLAN DE ACCIÓN DE IMPLEMENTACION DE CONTROLES DE SEGURIDAD PARA LA INSTALACION DE CUALQUIER SOFTWARE EN UN EQUIPO INFORMATICO

(Presentada por Jerson Calderón Alvarado)

Según la Auditoria,

Considerando los hallazgos que se encontraron en la Auditoria que se realizó el 26 de Octubre hasta el 02 de Noviembre del 2016, se pudo identificar una salvaguarda según la metodología magerit, que nos permitirá mitigar la amenaza “Infección de virus en el equipo”

Objetivo Específico:

- Identificar si existe la restricción de instalación de software

Requerimiento de cada objetivo específico Según la ISO27001:2013

- En el punto 12.6.2 (Restricciones en la instalación de software) se refiere que hay que tener permisos de la alta dirección para poder instalar un software ajeno a los requerimientos que tiene la organización y documentación del uso que se quiera dar al software

Actividades para cumplir con el Objetivo específico:

- Se debe de tener normas de seguridad respecto a software instalables para que se pueda restringir esas instalaciones

PROPUESTA DE PLAN DE ACCIÓN DE IMPLEMENTACION DE CONTROLES DE SEGURIDAD PARA LA INSTALACION DE CUALQUIER SOFTWARE EN UN EQUIPO INFORMATICO

CAPITULO I

PASOS PARA LA IMPLEMENTACION

1. Se creada un usuario local administrador
2. Se pondrá una contraseña que solo el área de soporte debe de conocer.
3. Se crearan usuarios de red administradores ya sea por el perfil de usuario
4. Se tendrá que mantener el antivirus activo en todo momento.
5. Todo usuario que quiera algún software para su ayuda persona, su jefe directo tiene que enviar un correo y el jefe de mesa de ayuda tiene que dar la aprobación
6. Aquellos usuarios que tengan software extras, se tendrán que hacer un seguimiento para ver si lo utilizan en sus actividades de trabajo.

CAPITULO IV

MONITOREO Y MEJORA

1. Si existe algún software de monitoreo para identificar que software tiene cada usuario en su PC se implementara.
2. Se tendrá que hacer un seguimiento a esta salvaguarda para prevenir las vulnerabilidades que pueda sufrir un activo de información.

PROPUESTA DE PLAN DE ACCIÓN DE DESARROLLO E IMPLEMENTACION DE CONTROLES PARA EL MANTENIMIENTO PREVENTIVO Y CORRECTIVO DE LOS EQUIPOS INFORMATICOS

(Presentada por Jerson Calderón Alvarado)

Según la Auditoria,

Considerando los hallazgos que se encontraron en la Auditoria que se realizó el 26 de Octubre hasta el 02 de Noviembre del 2016, se pudo identificar una salvaguarda según la metodología magerit, que nos permitirá mitigar la amenaza “Perdida de equipos informáticos”

Objetivo Específico:

- Identificar si existe mantenimiento preventivo y correctivo de los equipos informáticos

Requerimiento de cada objetivo específico Según la ISO27001:2013

- En el punto 14 (Adquisición, desarrollo y mantenimiento de sistemas) se refiere que hay que tener un plan preventivo y correctivo para los equipos informáticos, dado que no se tiene que perjudicar la operatividad de la red y las actividades de los usuarios.

Actividades para cumplir con el Objetivo específico:

- Se debe de tener un plan preventivo y correctivo de los equipos informáticos para evitar equipos en estado de inoperatividad.

PROPUESTA DE PLAN DE ACCIÓN DE DESARROLLO E IMPLEMENTACION DE CONTROLES PARA EL MANTENIMIENTO PREVENTIVO Y CORRECTIVO DE LOS EQUIPOS INFORMATICOS

CAPITULO I

PASOS PARA LA IMPLEMENTACION

1. Identificar cuáles son las área que tienen contacto directo con el publico
2. Se procederá a hacer un inventario de equipos informáticos
3. Si las características son inferiores a lo que se estima, se procederá con el cambio de PC.
4. Si las características son las correctas y aun así persiste en lentitud, se procederá con el formateo de la PC.
5. Se le entregara una PC de backups hasta que se formatee su PC del usuario
6. En caso luego del formateo de PC; vuelve a recaer en lentitud, se procederá con el cambio de PC
7. Se hará un mantenimiento a las PC's nuevas con la finalidad que puedan durar un tiempo determinado.
8. Se tendrá un inventario de las PC's nuevas en cada área.

CAPITULO IV

MONITOREO Y MEJORA

1. Si existe algún método mejor en mantenimiento preventivo de equipos se podrá implementar, pero con previo análisis.
2. Se tendrá que hacer un seguimiento a esta salvaguarda para prevenir las vulnerabilidades que pueda sufrir un activo de información.

PROPUESTA DE PLAN DE ACCIÓN DE ORDENAMIENTO DE LOS GABINETES DE RED

(Presentada por Jerson Calderón Alvarado)

Según la Auditoria,

Considerando los hallazgos que se encontraron en la Auditoria que se realizó el 26 de Octubre hasta el 02 de Noviembre del 2016, se pudo identificar una salvaguarda según la metodología magerit, que nos permitirá mitigar la amenaza “Mal control de puertos de red”

Objetivo Específico:

- Identificar si existe un ordenamiento estructurado en los gabinetes de la empresa para la supervisión de próximas auditorias

Requerimiento de cada objetivo específico Según la ISO27001:2013

- ANSI/TIA/EIA-569
  El estándar provee especificaciones para el diseño de las instalaciones y la infraestructura edilicia necesaria para el cableado de telecomunicaciones en edificios.

Actividades para cumplir con el Objetivo específico:

- Se debe de implementar los estándares de cableado estructurado para tener un mejor control de los puertos de acceso de los switch.

PROPUESTA DE PLAN DE ACCIÓN DE ORDENAMIENTO DE LOS GABINETES DE RED

CAPITULO I

PASOS PARA LA IMPLEMENTACION

1. Se verificara cuantos gabinetes hay
2. Se identificara el estado, y se procederá con el mas critico
3. Se establecerá fechas no laborales para poder proceder con el ordenamiento de cableado estructurado
4. Se procederá aponer etiquetas a los cables de red, para poder identificar su ubicación.
5. Si hay algún proveedor de servicios, luego de hacer el cableado debe de entregar un certificado.

CAPITULO IV

MONITOREO Y MEJORA

1. Si existe algún método mejor en eliminar un virus se añadirá a los pasos para la implementación.
2. Se tendrá que hacer un seguimiento a esta salvaguarda para prevenir las vulnerabilidades que pueda sufrir un activo de información.

PROPUESTA DE PLAN DE ACCIÓN DE IMPLEMENTACION DE UN LIBRO DE CONTROL DE ACCESO

(Presentada por Jerson Calderón Alvarado)

Según la Auditoria,

Considerando los hallazgos que se encontraron en la Auditoria que se realizó el 26 de Octubre hasta el 02 de Noviembre del 2016, se pudo identificar una salvaguarda según la metodología magerit, que nos permitirá mitigar la amenaza “Mal control de equipos intermedios”

Objetivo Específico:

- Identificar la operatividad de la red en el hospital

Requerimiento de cada objetivo específico Según la ISO27001:2013

- En el punto 12 (seguridad en las operaciones) se refiere que hay que tener una operatividad correcta y eficaz de la red para no afectar a los procesos de información

Actividades para cumplir con el Objetivo específico:

- Se debe de identificar cuáles son los recursos que inestabilizan la red y poder administrarla de una mejor manera.

PROPUESTA DE PLAN DE ACCIÓN DE IMPLEMENTACION DE UN LIBRO DE CONTROL DE ACCESO

CAPITULO I

PASOS PARA LA IMPLEMENTACION

1. Se identificara cuantos equipos intermedios habrá.
2. Se procederá a poner contraseñas de 10 caracteres como mínimo.
3. Se procederá a cambiar cada 7 días la contraseña
4. Se guardaran en un sobre sellado dichas contraseñas
5. Se guardarán toda la información de los equipos intermedios en un servidor FTP
6. Si no hay un servidor FTP, se procederá a copiar toda la configuración en un notepad.
7. Esta información se guardara y solo se mostrará al jefe de área de infraestructura

CAPITULO IV

MONITOREO Y MEJORA

1. Si existe algún método mejor en guardar toda la data de los equipos intermedios se añadirá a los pasos para la implementación.
2. Se tendrá que hacer un seguimiento a esta salvaguarda para prevenir las vulnerabilidades que pueda sufrir un activo de información.

PROPUESTA DE PLAN DE ACCIÓN DE IMPLEMENTACION DEL PLAN DE POLITICAS Y NORMAS DE SEGURIDAD

(Presentada por Jerson Calderón Alvarado)

Según la Auditoria,

Considerando los hallazgos que se encontraron en la Auditoria que se realizó el 26 de Octubre hasta el 02 de Noviembre del 2016, se pudo identificar una salvaguarda según la metodología magerit, que nos permitirá mitigar la amenaza “Mal control de red y acceso de los usuarios”

Objetivo Específico:

- Identificar si cuenta con políticas y normas de seguridad de información

Requerimiento de cada objetivo específico Según la ISO27001:2013

- En el punto 5 (Políticas de seguridad de la información) se refiere que hay que tener un documento de las políticas de seguridad e implementarlas dentro de nuestra red interna

Actividades para cumplir con el Objetivo específico:

- Se debe de crear y aprobar una documentación de políticas y normas de seguridad informática.

PROPUESTA DE PLAN DE ACCIÓN DE IMPLEMENTACION DEL PLAN DE POLITICAS Y NORMAS DE SEGURIDAD

CAPITULO I

PASOS PARA LA IMPLEMENTACION

1. Se verificara cuales con las normas que el usuario debe de aprender
2. Se plasmara en un documento las políticas de seguridad
3. Se realizara una documentación y en esta se incluirá las salvaguardas anteriores, para poder llevar un mejor control de ello.
4. Se tendrá que mejorar este documento cada 4 meses y ver el nivel de cumplimiento.

CAPITULO IV

MONITOREO Y MEJORA

1. Si existe algún método mejor de políticas y normas de seguridad se añadirá a los pasos para la implementación.
2. Se tendrá que hacer un seguimiento a esta salvaguarda para prevenir las vulnerabilidades que pueda sufrir un activo de información.

Políticas y normas de seguridad Del Hospital

MATRIZ DE RIESGOS MAGERIT

INTRODUCCIÓN

En una organización la gestión de riesgos para la seguridad informatica es de suma importancia porque ayuda clasificar los niveles de seguridad de un activo, para que no pueda ser vulnerado y capaz afectado por una amenaza. Esto permite organizar y coordinar todos los esfuerzos encaminados para lograr una seguridad informatica y poder consolidar a la organización.

El documento que se presenta integra las políticas de seguridad que deberá tener el HADOMANI San Bartolomé, esto permitirá poder adecuarse a las reglas, normas y procedimientos para proteger los riesgos de seguridad.

Estas normas que se presentan en este documento sirven como un marco de referencia mas no como normas absolutas, donde estas políticas que se plantean pueden ser modificadas con el objetivo de mejorar el nivel de seguridad de la información y los servicios que se brindan a los usuarios por la red.

Toda persona que esté utilizando la red deberá conocer las políticas y normas de seguridad que se plantean en este documento, en caso no esté de acuerdo deberá conversar con la alta dirección mas no con el área de informatica o el administrador de redes.

Seguridad Lógica

La seguridad lógica se encarga de los controles de acceso que están diseñados para salvaguardar la integridad de la información almacenada de un dispositivo intermedio o final. La seguridad lógica se encarga de controlar y salvaguardar la información generada por los sistemas, por el software de desarrollo y por los programas en aplicación, identifica a cada usuario y sus actividades en el sistema, y restringe el acceso a datos, a los programas de uso general, de uso específico, de las redes y terminales

Seguridad Física

La seguridad física se refiere a los controles y mecanismos de la seguridad dentro y alrededor del centro de cómputo así como los medios de acceso remoto del mismo, implementados para proteger el hardware y medios de almacenamiento de datos. Es muy importante, que por más que nuestra organización sea la más segura desde el punto de vista de ataques externos, hackers, virus, etc.; la seguridad de la misma será nula si no se ha previsto como combatir un incendio

Seguridad de redes

La definición y el objetico de la seguridad en redes es mantener la integridad, disponibilidad, privacidad, control y autenticidad de la información manejada por computadoras, a través de procedimientos basados en una política de seguridad tales que permitan el control de lo adecuado

GENERALIDADES

MATRIZ DE RIESGOS MAGERIT

INSTRUCCIONES DE INTERPRETACION

La información que se ha planteado en este documento trata de ser el más sencillo para su posible interpretación por el usuario e implementación en el HOADOMANI San Bartolomé.

El presente documento trata de 2 capítulos en donde, la primera trata específicamente de las normas de seguridad

El segundo capítulo trata de un enfoque objetivo de la situación real del HONADOMANI San Bartolomé, creando cada política se seguridad para proteger un activo, nos guiaremos respecto a la norma ISO/IEC 27001:2013 (Sistema de gestión de seguridad de información)

Seguridad Lógica

- Control de acceso
- Administración del acceso de usuarios
- Control de acceso a la red
- Monitoreo de acceso

Seguridad Física

- Seguridad física
- Seguridad de los equipos

Seguridad de redes

- Copias de seguridad
- Antivirus
- Documentación de scripts

MATRIZ DE RIESGOS MAGERIT

DEFINICION DE NORMAS Y POLITICAS DE SEGURIDAD INFORMATICA

¿Qué son las normas de seguridad?

Las normas de seguridad son un conjunto de reglas, recomendaciones y controles en donde estos dan un respaldo a las políticas de seguridad, esto tiene como objetivo principal tener claro las necesidades de la seguridad en el entorno administrativo de la red

¿Qué son las políticas de seguridad?

Las políticas de seguridad están orientadas al personal, donde tienen que acatar estas políticas para poder utilizar los servicios de la red que emplea la organización, que nos ayude a proteger los riesgos de diferentes activos.

ORGANIZACIÓN DE LA SEGURIDAD INFORMATICA

DIRECCION

Es la autoridad de nivel superior que permite la aceptación y seguimiento de las políticas y normas de seguridad.

COORDINADOR DE SISTEMAS

Persona encargada de establecer la seguridad de la información. Realiza auditorias y elabora documentos de seguridad, tales como políticas y normas para tener un control de los servicios según los niveles de seguridad

UNIDAD DE SISTEMAS

Es la unidad de la organización que vela por los sistemas de información, equipos informáticos, redes informáticas y el procesamiento de datos e información.

RESPONSABLE DE ACTIVOS

Es el personal de cada área que se encargara de velar por la seguridad y correcto funcionamiento de los activos de información.

MATRIZ DE RIESGOS MAGERIT

MARCO LEGAL

La elaboración de las políticas y normas de seguridad está fundamentado bajo la norma ISO/IEC 27001:2013 donde es un estándar internacional para el sistema de gestión y seguridad de información.

VIGENCIA

La documentación que se establece en este informe entrara en vigencia desde el día que se apruebe por la dirección de la HONADOMANI San Bartolomé. Esta normativa deberá ser revidad y actualizada cada cierto tiempo para mejorar los niveles de seguridad de cada activo de información.

POLITICA DE SEGURIDAD INFORMÁTICA

NIVEL 1: SEGURIDAD LÓGICA

1. SEGURIDAD LÓGICA

1.1. CONTROL DE ACCESO

- El administrador de redes proporcionara toda la documentación necesaria para poder agilizar la utilización de los sistemas de información.
- Se establecerá canales de gestión para que cuando un usuario quiera pedir información o servicio proveniente, lo haga a través de pautas.

1.1.1. ADMINISTRACION DEL ACCESO DE USUARIOS

- Se establecerá usuarios con nivel de privilegio alto, para aquellos que sean jefes de áreas y/o secretarios que utilicen servicios de red en el HONADOMANI San Bartolomé
- Se establecerá cuentas de acceso a la red de la institución para todos los usuarios que tengan acceso a los sistemas de información y/o actividades diarias que sumen a al HONADOMANI San Bartolomé.
- Los usuarios externos solo tendrán acceso a los servicios de internet que tengan que ver con su actividad diarias, a ellos se les restringe página alternas.

- Se considera usuario externo a cualquier persona o instituciones que brindaran servicios
- Para que un usuario quiera tener los privilegios de acceso a la red, tiene que presentar previa documentación de autorización de la alta dirección del HONADOMANI San Bartolomé, especificando el motivo y los accesos que quiera tener a la red.
- Se creara una cuenta temporal para cada usuario en caso el usuario se olvide su contraseña o pierda su información
- La contraseña de cada usuario tendrá como mínimo 6 caracteres que tendrán combinación alfanumérica y caracteres especiales.
- La contraseña de cada usuario tendrá máximo 12 caracteres que tendrán combinación alfanumérica y caracteres especiales.
- La contraseña tiene que ser cambiada en un periodo máximo de 30 días, con la finalidad de proteger la información del usuario.

1.1.2. RESPONSABILIDADES DEL USUARIO

- El usuario es el único responsable para tener el control de su contraseña
- El usuario debe de evitar poner su contraseña en un papel, al menos que esté en un lugar seguro que este considere.
- Cualquier usuario que identifique alguna falla de red o cambios de privilegios en su ordenador, está obligado a reportarlo con el área de informatica o con el coordinador de sistemas

USO DE CORREO ELECTRONICO

- El servicio de correo electrónico es gratuito, pero se tiene que tener un control de ello.
- El correo electrónico es de uso exclusivo de los empleados, en caso el usuario no cumpla con esto, el área de informatica no se hace responsable de la perdida de información que este podría tener.
- El usuario es responsable de la información que envía

- El administrador de la red monitoreará las cuentas de los usuarios, y si en caso haya un comportamiento sospechoso tiene toda la autoridad de reportar al usuario con la alta dirección.

1.1.3. SEGURIDAD EN ACCESO DE TERCEROS

- El acceso de terceros será permitido siempre y cuando este respetando las normas de seguridad que se planteen.
- El usuario externo solo tiene que utilizar el acceso a la red para su función que le ha asignado su institución.

1.1.4. CONTROL DE ACCESO A LA RED

UNIDAD DE SISTEMAS Y AFINES A ELLA

- El acceso a la red interna se permitirá si se cumple los requisitos de autentificación de seguridad necesarios.
- Se debe de eliminar cualquier acceso a la red sin autentificación.
- El área de informatica debe de emplear el bloqueo de red para el filtrado de información no autorizado.
- Se registrara todo acceso a los dispositivos de red, mediante archivos de log.
- Se revisara el log de los dispositivos de acceso a la red en un tiempo de 48 horas.

1.1.5. CONTROL DE ACCESO AL SISTEMA OPERATIVO

- Se eliminaran las cuentas creadas por aplicaciones no autorizadas
- Al culminar la hora de trabajo del usuario, este tiene la obligación de apagar su equipo.

SERVIDORES

- Solo el usuario administrador tiene acceso al sistema operativo de los servidores
- Toda configuración que el usuario administrador haga, lo tendrá que hacer bajo cuentas restrictivas.
- Las cuentas restrictivas que el usuario administrador haga, se deberá de eliminar cada 15 a 20 días y crear una nueva, y se tendrá que repetir el proceso

1.1.6. CONTROL DE ACCESO A LAS APLICACIONES

- Se deberá definir y estructurar el nivel de permiso sobre las aplicaciones que el usuario solicite.
- Se deberá revisar cada aplicación que el usuario este utilizando.
- La salida de la información de las aplicaciones deberán ser documentadas

1.1.7. MONITOREO DEL ACCESO Y USO DEL SISTEMA

- Se debe de registrar y archivar toda actividad de log.
- Los archivos de log almacenaran los nombres de usuarios, niveles de privilegios, ir de terminal, fecha y hora de utilización y archivos a los que tuvo acceso.
- Se efectuara una copia automática de los archivos de log.

1.2. GESTION DE OPERACIONES Y COMUNICACIONES

1.2.1. RESPONSABILIDADES Y PROCEDIMIENTOS OPERATIVOS

- El personal encargado de un área, tiene toda la responsabilidad de velar por la seguridad de información del servicio.
- El personal encargado de un área, revisara los archivos de forma frecuente y también después de la falla.

1.2.2. PLANIFICACION Y ACEPTACION DE SISTEMAS

- El personal de programación, redes y planificaciones que pertenecen al área de sistemas, tendrán la obligación de documentar todo lo relacionado con sus actividades
- La alta dirección aprobara la ejecución de un software, previo análisis y pruebas por el área de informatica.
- Se ejecutaran software licencias o desarrollados por el área de informatica.
- Los programadores deberán realizar las pruebas respecto a los siguientes puntos:
    - Caracteres inválidos en los campos de datos
    - Datos incompletos
    - Datos no autorizados
    - Validación de errores
    - Validación de caracteres

- Validación de la integridad de los datos
- Validación e integridad de las salidas

1.2.3. PROTECCION CONTRA SOFTWARE MALICIOSO

- Se utilizara software de fuentes confiables
- Los servidores y equipos informáticos deberán tener el antivirus instalados

1.2.4. MANTENIMIENTO

- El mantenimiento de los sistemas de información y equipos informáticos es responsabilidad del área de informatica
- Se tendrá que registrar todo tipo de mantenimiento que se haga a un sistema de información o equipo informático

1.2.5. MANEJO Y SEGURIDAD DE MEDIOS DE ALMACENAMIENTO

- Los medios de almacenamiento que guarden copias de seguridad tendrán que ser etiquetados con la información que lleva y del área a donde pertenece
- Los medios de almacenamiento que guarden copias de seguridad solo serán manipuladas por el área el área de informatica
- Los medios de almacenamiento que guarden copias de seguridad de usuarios privilegiados tendrán que ser guardados en una caja con llave.
- Se llevara un control de la cantidad de medios de almacenamiento se tiene en el área de informatica

NIVEL 2: SEGURIDAD FISICA

2. SEGURIDAD FISICA

2.1. Seguridad de los equipos

- Se tendrá que identificar el tipo de cacle que se use, sea cable de red o eléctrico
- Los servidores se tendrán que reparar localmente
- En caso haya una falla en los servidores se tendrá que retirar su medio de almacenamiento.

- Los equipos con estado crítico deberán de ser guardados en un lugar con espacio y en buenas condiciones.

2.2. Controles generales

- Las estaciones o lugares propensos a sufrir daños deben de ser descartados para almacenar equipos informáticos
- Debe de haber una mantenimiento preventivo y correctivo de los equipos
- Toda oficina debe de tener herramientas auxiliares (extintores o alarmas contra incendios) para salvaguardar los equipos informáticos.
- La sala de servidores debe de estar separada del área de informatica o cualquier unidad.
- La sala de servidores se debe adecuar o parecer a los estándares internacionales
- Las instalaciones en el área de servidores debe de tener una adecuada instalación eléctrica.
- Las salas deben de tener un cartel con el nombre que identifique a ello.

NIVEL 3: SEGURIDAD DE REDES

3. SEGURIDAD DE REDES

3.1. Internet

- Está prohibida la publicación de material de pornografía y de cualquier otra índole que atente contra la integridad de los usuarios de la organización.
- No está permitido publicar o usar juegos en redes internas de trabajo.
- No está permitido publicar, transmitir, almacenar o copiar música desde ni hacia componentes de redes, unidades publicar o unidades internas de la organización
- No está permitido publicar, transmitir, almacenar o copiar software corporativo u otros.

3.2. Copias de seguridad

- Debe existir un procedimiento que determine actividades, periodicidad, responsables y mecanismos de almacenamiento de las copias de respaldo de todos los sistemas de información
- Debe existir una definición formal de las políticas y procedimientos de generación, retención y rotación de copias de respaldo.
- Cada vez que se cambien los servidores o el Software, los procedimientos para realizar las Copias de Respaldo y el Plan de Contingencia deben ser actualizados.
- Con el objetivo de garantizar la continuidad del negocio, se determina como de carácter obligatorio, la ejecución de políticas y procedimientos relacionados con copias de respaldo
- Todas las copias de respaldo deben estar encriptado
- El acceso al registro de ubicación y contenido de los medios debe estar restringido.
- Se debe contar con un registro, el cual permita identificar la ubicación y el contenido de cada medio

NORMAS DE SEGURIDAD INFORMATICA

1. SEGURIDAD LÓGICA

1.1. Control del acceso de usuarios a la red institucional

- La documentación de seguridad será realizada por el administrador.

1.1.1. Administración del acceso de usuarios a los servicios informáticos de la corporación

- Se consideran usuarios de la red a todos trabajadores del HONADOMANI San Bartolomé que se encuentran denotado en la política de administración de acceso de usuarios
- Los usuarios que tengan los permisos necesarios podrán acceder a los sistemas y servicios de información.
- Las necesidades y/o informaciones de los usuarios deberán de ser documentada y actualizadas.

- El administrador brindara la identificación hacia la red al usuario, y se autentificara con una firma del usuario.
- Cualquier persona ajena a la institución que quiera tener un usuario, deberá de ser aprobado en la política de acceso.
- Toda cuenta nula u olvidada se tendrá que eliminar de los sistemas
- El sistema no aceptara contraseñas menores a la longitud que se establece en la política de creación de contraseñas
- El usuario se responsabiliza en crear una contraseña fuerte y difícil de olvidar

1.1.2. Responsabilidades del usuario

- El usuario debe de estar consciente de la magnitud de daño que causaría dar su contraseña a otro usuario
- El usuario será sancionado si pone su contraseña en un papel o en cualquier parte del escritorio que note su visibilidad, porque estaría generando una amenaza a los archivos temporales.
- El servidor de dominio deberá bloquear de forma inmediata cualquier estación de trabajo con un protector de pantalla que tenga un tiempo de inactividad mayor a un (1) minuto.
- Toda falla en el equipo informático deberá de ser documentada por el usuario e informada inmediatamente al área de soporte técnico.
- El usuario que revise la falla del equipo informático y lo malogre, quedara sancionado y tendrá que reponer dicho equipo y/o parte afectada.

  <u>NORMATIVA DEL USO DE CORREO ELECTRONICO</u>
- El correo electrónico es una comunicación directa y de tipo confidencial, donde el usuario que tenga o reciba un correo ajeno deberá de información de forma inmediata al área de informatica o su jefe inmediato, si en caso no lo haga quedara sancionado.

- El servidor de correo bloqueara archivos adjuntos o información como archivos .exe o de ejecución de comandos como applets java, JavaScript o archivos de tipo ActiveX o IFrame
- Ningún usuario externo deberá tener acceso al correo electrónico proporcionado por la red institucional
- Cualquier actividad que se considere en esos ítems se considerara como mala:
  - El no mandar ni contestar cadenas de correo
  - El uso de su cuenta con fines académicos y/o investigación
  - Depurar correos de largos periodos en la bandeja de entrada
  - Respetar las cuentas de otros usuarios
  - Respetar los términos en el contrato de trabajo sobre normativas y políticas de seguridad.
- La cuenta de usuario que almacene un software de forma ilegal será inhabilitado temporalmente.
- La organización no se responsabiliza por el uso de correo electrónico de parte de sus empleados violentando la ley de derechos de autor

1.1.3. Seguridad en acceso de terceros

- El administrador de sistemas tomara las medidas necesarias para asignar los servicios a los usuarios externos.
- El no cumplimiento de las disposiciones de la seguridad y responsabilidad sobre sus acciones por parte de los usuarios de la red institucional, se obliga a la suspensión de su cuenta de usuario de los servicios.

1.1.4. Control de acceso a la red

- El administrador de sistemas diseñara las maneras necesarias para proveer el acceso a los servicios de la red institucional.
- Los mecanismos de autentificación y permisos de la red deberán ser revisados y aprobados por el administrador de la red
- El administrador hará evaluaciones periódica a los sistemas de red
- El personal que haga conexión remota será desde su máquina propia que este dentro de la red de la institución.

- Los dispositivos de red siempre estarán activos y configurados correctamente para evitar anomalías en el tráfico y seguridad de información.

1.1.5. Monitoreo del acceso y uso del sistema

PERSONAL DE INFORMATICA

- El administrador de sistemas deberá tener el cuidado suficiente al momento que instale aplicaciones en los servidores, y configurando cada permiso de ejecución.
- La finalización de la jornada laboral, termina con cualquier actividad desarrollada en ese momento, lo cual implica apagar los equipos informáticos.
- El servidor de dominios, verificara y desactivara cualquier estación de trabajo que este uso después de la hora de salida.
- El administrador de redes no se responsabiliza si el equipo se apaga por el servidor de dominios con algún documento sin guardar por parte del usuario.
- El servidor deberá estar correctamente configurado, con la finalidad de evitar el abuso extraño a la administración.
- La cuenta administrativa solo es propiedad exclusiva del administrador de sistemas
- Las aplicaciones prestadoras de servicios correrán con cuentas restrictivas y jamás con privilegios tan altos como los de la cuenta administrativa.

1.1.6. Control de acceso a las aplicaciones

- Las aplicaciones deberán contar con su respectiva documentación.
- Los usuarios tendrán los permisos necesarios para ejercer su trabajo
- Los niveles de seguridad son definidos por el comité de seguridad del área de informatica y la alta dirección.
- Se llevara un seguimiento en limpio sobre que terminales es posible efectuar las salidas de información desde el servidor.

- Se verificara constantemente la operatividad de los registros de logs, que no sean alterados de forma fraudulenta.

1.1.7. Monitoreo del acceso y uso del sistema

- Es necesario efectuar un respaldo de los archivos de registro o logs, fuera de los dispositivos que les creen.
- Los archivos de logs deben ser respaldados en tiempo real, sus nombres deben contener la hora y la fecha en la que fueron creados sus originales.

1.2. GESTION DE OPERACIONES Y COMUNICACIONES

1.2.1. Responsabilidades del usuario sobre los procedimientos operativos

- La unidad de sistemas es la única encargada para la ejecución de algún servicio
- Los sistemas son configurados para responder de forma automática, con la presentación de un informe que denote las características propias de un error en el sistema.

1.2.2. Planificación y aceptación de sistemas

- Ninguna persona ajena a la institución podrá instalar un software en los equipos informáticos sin autorización previa.
- Antes de realizar el análisis y pruebas de los sistemas de información, se tendrá que hacer un back-up de información

1.2.3. Protección contra software malicioso

- El administrador supervisara la instalación y correcta configuración del software de antivirus para todos los equipos informáticos.

1.2.4. Mantenimiento de sistemas y equipo de computo

- El usuario no puede intervenir física o lógicamente en ningún equipo informático.
- El usuario no podrá modificar los archivos de las carpetas compartidas
- Se deberá tener en una bitácora las versiones de actualización del software.

1.2.5. Seguridad en el manejo de los medios de almacenamiento

- La clasificación e identificación de los medios de almacenamiento, es acorde al propósito u objetivo por el cual se respalda.
- Bajo ninguna circunstancia se dejaron desatendidos los medios de almacenamiento, o copias de seguridad de los sistemas.
- Todo medio de almacenamiento deberá ser documentado e inventariado en un registro específico y único sobre medios de almacenamiento.
- La ubicación de los medios de almacenamiento deberá estar alejada del polvo, humedad, o cualquier contacto con material o químicos corrosibles.
- La llave de seguridad que da acceso a los medios de almacenamiento resguardados bajo supervisión de la gerencia, ser mantenida bajo estricta seguridad por cualquiera de las dos entidades encargadas de mantener la seguridad de los medios.
- La documentación de seguridad deberá tener un control para la clasificación y resguardo de los medios de almacenamiento.

2. SEGURIDAD FISICA

2.1. LA SEGURIDAD EN LOS DIFERENTES DEPARTAMENTOS

2.1.1. RESGUARDO DE LOS EQUIPOS DE COMPUTO

Usuarios comunes y administrativos

- El área de sistemas diseñara toda la red del HONADOMANI, siguiente los estándares internacionales de cableado estructurado.
- Está totalmente prohibido que un usuario intervenga en la manipulación del cableado estructurado

Personal de informática

- El soporte técnico de la sala se servidores es responsabilidad del área de informatica
- Se deberá proteger la sala de servidores.

- El centro de procesamiento de datos tiene que tener acceso restringido para los usuarios.
- El personal de informatica debe de contar con su identificación para el ingreso de las área restringidas

Controles físicos generales

- Las unidades USB y CD se debe de deshabilitar en las maquinas que no se necesiten
- Cada empleado de la organización se responsabiliza de su información personal.
- El administrador deberá de tener los registros de las maquinas que reciban actualizaciones de sistemas operativos
- No se permitirá la instalación de programas de procesos críticos
- Los UPS son de uso obligatorio en la organización
- El administrador de redes debe de brindar los materiales administrativos de cada configuración que se implemente en los dispositivos intermedios y finales.
- El material informativo debe de ser entendible para los usuarios.

2.1.2. ACTIVIDADES PROHIBIDAS

- Está prohibido el ingreso de alimentos y/o bebidas a las área en donde se manejen medios de almacenamiento o equipos informáticos
- Esta prohíbo realizar actividades ajenas en el horario de trabajo por parte de los usuarios.
- Se prohíbe el ingreso de usuario en estado de ebriedad a la hora de trabajo

3. SEGURIDAD DE REDES

3.1. Internet

- El servicio de Internet debe ser utilizado para facilitar el cumplimiento de las funciones asignadas a los empleados y contratistas del HONADOMANI San Bartolomé.
- Debe existir un procedimiento de administración de la intranet, en especial el mantenimiento y depuración de la información publicada,

que garantice el buen uso de este y de las herramientas disponibles para su gestión.

- La información de Intranet debe ser únicamente utilizada por personal autorizado. Los usuarios no deben re-direccionar información que aparezca en Intranet a terceros sin autorización de la Organización.
- La información que se publique en la Intranet de la Organización, debe contar con la aprobación del responsable de cada Área y bajo la coordinación del Área de Servicio Regional de Información, encargada de la administración de la página web, y la del propietario de la información involucrada

3.2. Copias de seguridad

- Deben usarse medios que permitan almacenar la información apropiadamente, no utilizar CD o DVD ya que dichos medios se degradan y la información se pierde.
- Los medios deben ser almacenados en un sitio que posea las condiciones ambientales correctas (Temperatura y Humedad), el cual asegure el adecuado funcionamiento de los mismos.
- Los medios deben contar con un periodo de vida (registro de fecha de inicio del uso de los mismos y una fecha de descarte).
- Los medios descartados no se deben usar ya que existe el riesgo de pérdida de la información en ellos almacenada.
- Todos los medios se deben mantener en un área restringida y bajo llave.
- El acceso a los medios será autorizado únicamente al Área de Sistemas y T.I. o al personal que sea autorizado por dicha área.
- Los medios deben estar adecuadamente etiquetados de tal forma que sean fácilmente identificables.
- El contrato de los medios almacenados en instalaciones externas, debe contar con una cláusula de Confidencialidad la cual asegure que la información no pueda ser copiada o divulgada en forma no autorizada.
- Se debe tener un registro de los medios enviados a sitio externo, firmado por el tercero que reciba dichos medios o su representante.

MATRIZ DE RIESGOS MAGERIT

RECOMENDACIONES

- Crear una gestión de riesgos para la seguridad informatica que nos permita poder identificar las vulnerabilidades de los activos y las amenazas que afecten a ello.
- Aprobar y poner en marcha las políticas y normas de seguridad
- Actualizar de forma constante las políticas y normas de seguridad
- Asignar un personal encargado a la gestión de riesgos para la seguridad informatica.
- Fijar las salvaguardas para las amenazas
- Dar seguimiento a los estándares internaciones
- Contratar a terceros para que ejecuten una etical hacking
- Capacitar a los empleados para la seguridad informatica

PROPUESTA DE PLAN DE ACCIÓN DE IMPLEMENTACION DE UN PROCEDIMIENTO DE RESGUARDO DE SOBRES SELLADOS

(Presentada por Jerson Calderón Alvarado)

Según la Auditoria,

Considerando los hallazgos que se encontraron en la Auditoria que se realizó el 26 de Octubre hasta el 02 de Noviembre del 2016, se pudo identificar una salvaguarda según la metodología magerit, que nos permitirá mitigar la amenaza “Claves de los servidores”

Objetivo Específico:

- Identificar las claves de los servidores

Requerimiento de cada objetivo específico Según la ISO27001:2013

- En el punto 9.4. (Control de Acceso a la Red) refiere que hay que asegurarse que el acceso de los usuarios a las redes y sus servicios no comprometan la seguridad de dichos servicios

Actividades para cumplir con el Objetivo específico:

- Se debe de implementar un procedimiento de resguardo de sobres sellados donde solo lo tenga el jefe de informatica en su escritorio mediante llaves.

PROPUESTA DE PLAN DE ACCIÓN DE IMPLEMENTACION DE UN PROCEDIMIENTO DE RESGUARDO DE SOBRES SELLADOS

CAPITULO I

PASOS PARA LA IMPLEMENTACION DE UN PROCEDIMIENTO DE RESGUARDO DE SOBRES SELLADOS

1. Se procederá a poner contraseñas no menores a 10 caracteres
2. Se procederá a poner en sobres sellados
3. Estos sobres se pondrán dentro de un cajón con llave.
4. En caso el administrador de redes o de servidores, falte por algunas razones, el personal que queda en segundo plano, podrá realizar las configuraciones correspondientes con el objetivo de no retrasar el trabajo de los usuarios.
5. El jefe del área de infraestructura solo podrá dar el acceso de configuración al personal de segundo plano.

CAPITULO IV

MONITOREO Y MEJORA

1. Si existe algún método mejor en resguardo de sobres sellados se añadirá a los pasos para la implementación.
2. Se tendrá que hacer un seguimiento a esta salvaguarda para prevenir las vulnerabilidades que pueda sufrir un activo de información.

PROPUESTA DE PLAN DE IMPLEMENTACION DE DOCUMENTOS POR CADA SERVIDOR DE PROCEDIMIENTO DE FALLAS

(Presentada por Jerson Calderón Alvarado)

Según la Auditoria,

Considerando los hallazgos que se encontraron en la Auditoria que se realizó el 26 de Octubre hasta el 02 de Noviembre del 2016, se pudo identificar una salvaguarda según la metodología magerit, que nos permitirá mitigar la amenaza “No saber mitigar el riesgo de la falla de red”

Objetivo Específico:

- Identificar planes para mitigar los riesgos de la red

Requerimiento de cada objetivo específico Según la ISO27001:2013

- En el punto 8 (Gestión de activos) refiere que hay que tener documentado los activos de información para no depender de personas que falten a sus labores y poder administrar de una manera perfecta los equipos intermedios y administración de la red interna de la organización.

Actividades para cumplir con el Objetivo específico:

- Se debe documentar por cada servidor unos procedimientos de fallas para poder resolver dichas fallas.

PROPUESTA DE PLAN DE IMPLEMENTACION DE DOCUMENTOS POR CADA SERVIDOR DE PROCEDIMIENTO DE FALLAS

CAPITULO I

PASOS PARA LA IMPLEMENTACION

6. Se verificara la operatividad de los servidores
7. Se establecerá fechas no laborales para cualquier implementación nueva
8. Se tendrá un plan de contingencia para el servidor de correos
9. El servidor de antivirus siempre tiene que estar activo
10. El servidor de DHCP tiene que estar en monitoreo constante
11. Se debe tener un servidor FTP para guardar toda la información posible

CAPITULO IV

MONITOREO Y MEJORA

5. Si existe algún método mejor en procedimiento de fallas se añadirá a los pasos para la implementación.
6. Se tendrá que hacer un seguimiento a esta salvaguarda para prevenir las vulnerabilidades que pueda sufrir un activo de información.

ANEXO 13:

CRONOGRAMA DE TRABAJO

VI. ASPECTOS ADMINISTRATIVOS

RECURSOS Y PRESUPUESTO

- Recursos humanos - Auditoria Pre - test

  En la primera Auditoria que se desarrolló para poder tener una línea base de la situación actual del hospital nacional San Bartolomé, se genera un costo por ejecutar dicha auditoria.

  Mediante el diagrama de Gantt se pudo identificar el cronograma y además las tareas que se realizó, para ello se fijó el monto según el cuadro de estadística de proyecto que ofrece el diagrama de Gantt.

  - El auditor líder recibirá una remuneración de S/.480.00 Nuevos Soles
  - El auditor líder de seguridad informatica recibirá una remuneración de S/.240.00 Nuevos Soles
  - El auditor líder de seguridad lógica y física recibirá una remuneración de S/.240.00 Nuevos Soles
  - El auditor líder de seguridad de redes recibirá una remuneración de S/.240.00 Nuevos Soles
  - El costo total por la auditoria que se realizo es de S/. 1200.00 Nuevos soles
  -

Tabla N° 4

No	Personal	Cantidad	Costo Unitario (S/.)	Dias	Costo toral (S/.)
1	Auditor lider	1	S/.480.00	6	S/.480.00
2	Auditor Líder de Seguridad informática	1	S/.240.00	6	S/.240.00
3	Auditor Interno de seguridad Lógica y física	1	S/.240.00	6	S/.240.00
4	Auditor interno de seguridad de redes	1	S/.240.00	6	S/.240.00
TOTAL					S/.1,200.00

Fuente: Elaboración propia

Recursos humanos - Auditoria Pre-test

- Materiales Auditoria Pre – test

  En la primera Auditoria que se desarrolló para poder tener una línea base de la situación actual del hospital nacional San Bartolomé, se generó una documentación y utilización de diversos materiales, donde se toma como referencia lo siguiente.

Tabla N° 5

Fuente: Elaboración propia

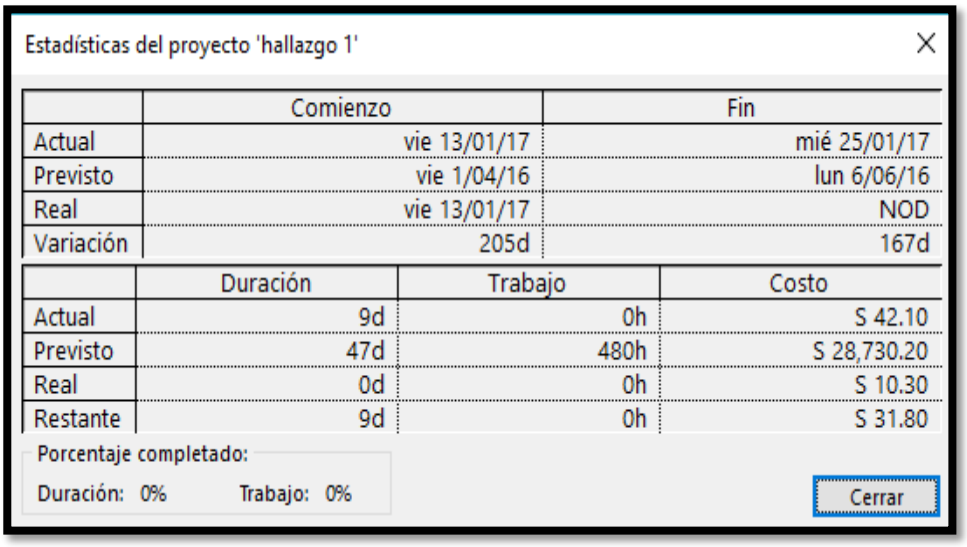
No	Personal	Cantidad	Costo Unitario (S/.)	Dias	Costo toral (S/.)
1	Camara digital	1		6	
2	Impresión	200	S/.0.30	6	S/.60.00
3	Material Bibliografico	1	S/.15.00	6	S/.9.90
4	Internet	1		6	
5	Laptop	1		6	
6	USB	1		6	
7	Utiles de oficina	8	S/.30.00	6	S/.15.00
TOTAL					S/.84.90

Materiales Auditoria Pre – test

- Salvaguarda 1: “Establecer una lista de usuario con acceso a la red” En esta figura se observa el costo de implementar el hallazgo final seleccionado N°1, donde genera un costo de S/. 42.10 Nuevos soles.

Figura N°14

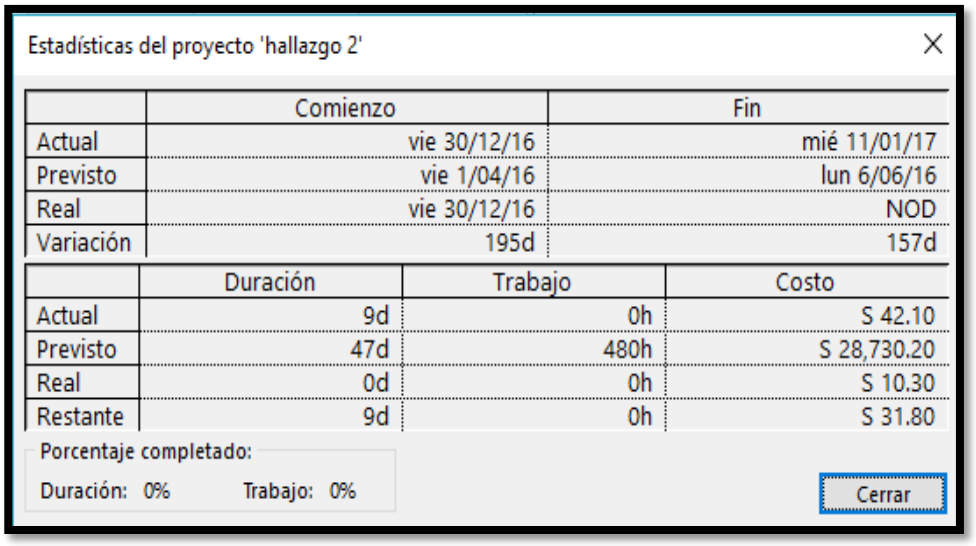
Fuente: Elaboración propia



Hallazgo N°1

- Salvaguarda 2 “Establecer una lista de cuentas activas” En esta figura se observa el costo de implementar el hallazgo final seleccionado N°2, donde genera un costo de S/. 42.10 Nuevos soles.

Figura N°15

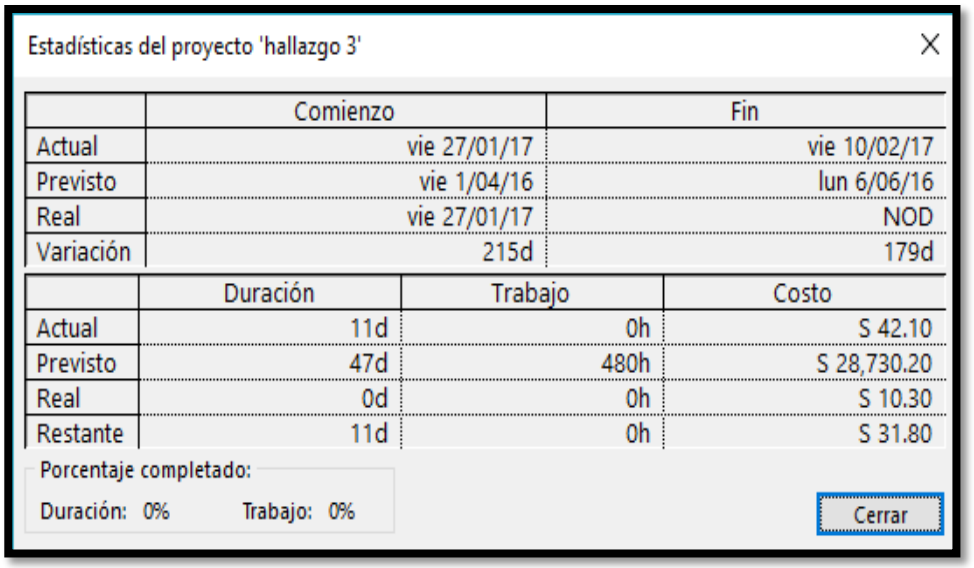


Fuente: Elaboración propia

Hallazgo N°2

- Salvaguarda 3: “Establecer políticas y administración de contraseñas” En esta figura se observa el costo de implementar el hallazgo final seleccionado N°3, donde genera un costo de S/. 42.10 Nuevos soles.

Figura N°16



Fuente: Elaboración propia

Hallazgo N°3

- Salvaguarda 4 “Realizar grupos de acceso a internet” En esta figura se observa el costo de implementar el hallazgo final seleccionado N°4, donde genera un costo de S/. 42.10 Nuevos soles.

Figura N°17

Fuente: Elaboración propia

Estadísticas del proyecto 'hallazgo 4'

	Comienzo	Fin
Actual	lun 13/02/17	vie 17/02/17
Previsto	vie 1/04/16	lun 6/06/16
Real	lun 13/02/17	NOD
Variación	226d	184d

	Duración	Trabajo	Costo
Actual	5d	0h	S 42.10
Previsto	47d	480h	S 28,730.20
Real	0d	0h	S 10.30
Restante	5d	0h	S 31.80

Porcentaje completado:
Duración: 0% Trabajo: 0%
Cerrar

Hallazgo N°4

- Salvaguarda 5 “Establecer una guía para que el usuario seleccione y realice el mantenimiento de contraseñas seguras” En esta figura se observa el costo de implementar el hallazgo final seleccionado N°5, donde genera un costo de S/. 42.10 Nuevos soles.

Figura N°18

Fuente: Elaboración propia

Estadísticas del proyecto 'hallazgo 5'

	Comienzo	Fin
Actual	lun 20/02/17	mié 1/03/17
Previsto	vie 1/04/16	lun 6/06/16
Real	lun 20/02/17	NOD
Variación	231d	192d

	Duración	Trabajo	Costo
Actual	8d	0h	S 42.10
Previsto	47d	480h	S 28,730.20
Real	0d	0h	S 10.30
Restante	8d	0h	S 31.80

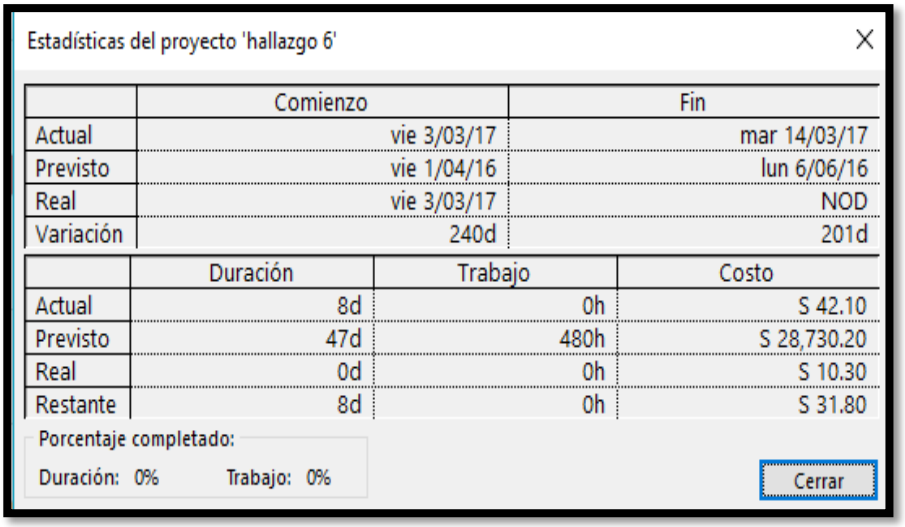
Porcentaje completado:
Duración: 0% Trabajo: 0%
Cerrar

Hallazgo N°5

- Salvaguarda 6“Desarrollar e implementar directrices y controles para la detección, prevención y tratamiento de software malicioso” En esta figura se observa el costo de implementar el hallazgo final seleccionado N°6, donde genera un costo de S/. 42.10 Nuevos soles.

Figura N°19

Fuente: Elaboración propia

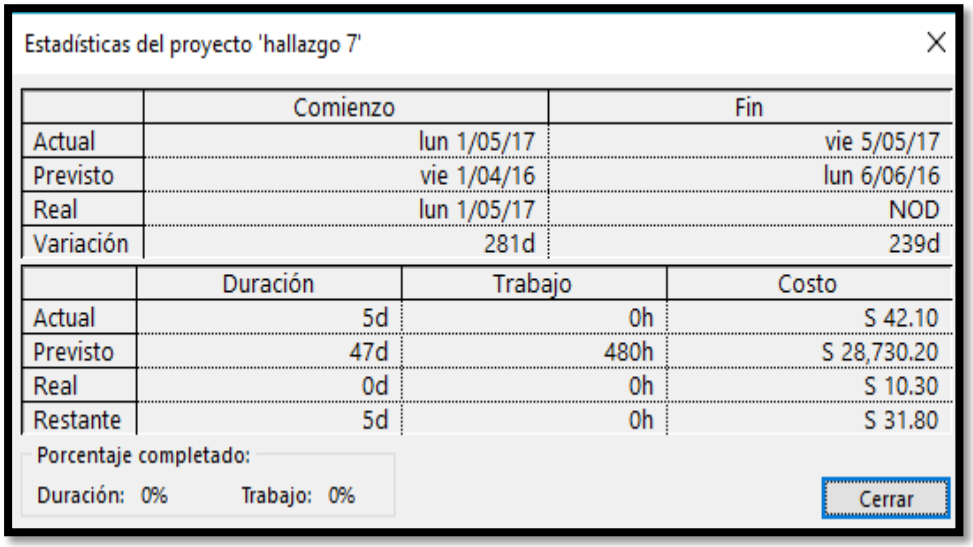


Hallazgo N°6

- Salvaguarda 7“Implementar controles de seguridad para la instalación de cualquier software en un equipo informático En esta figura se observa el costo de implementar el hallazgo final seleccionado N°7, donde genera un costo de S/. 42.10 Nuevos soles.

Figura N°20

Fuente: Elaboración propia

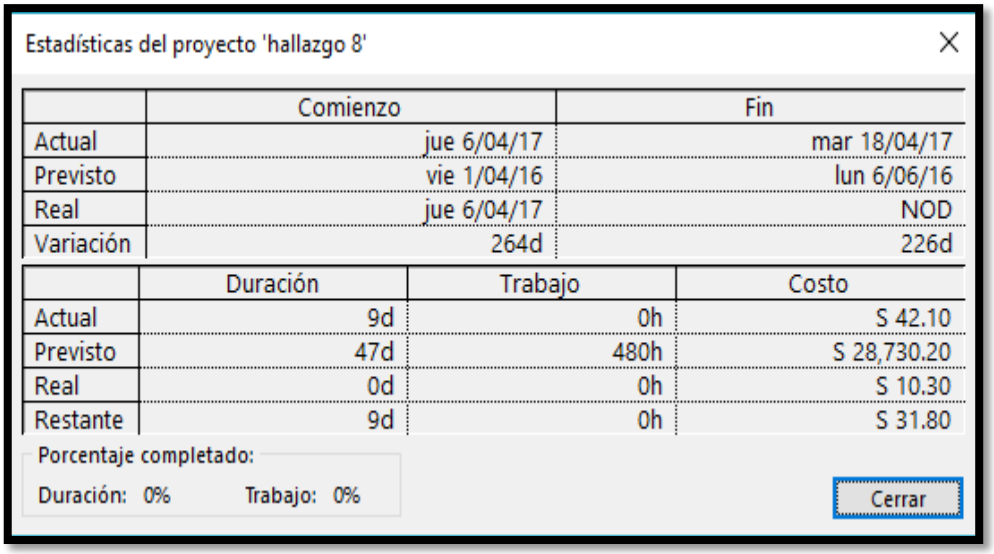


Hallazgo N°7

- Salvaguarda 8 “Desarrollar e implementar controles para el mantenimiento preventivo de los equipos informáticos”, en esta figura se observa el costo de implementar el hallazgo final seleccionado N°8, donde genera un costo de S/. 42.10 Nuevos soles.

Figura N°21

Fuente: Elaboración propia

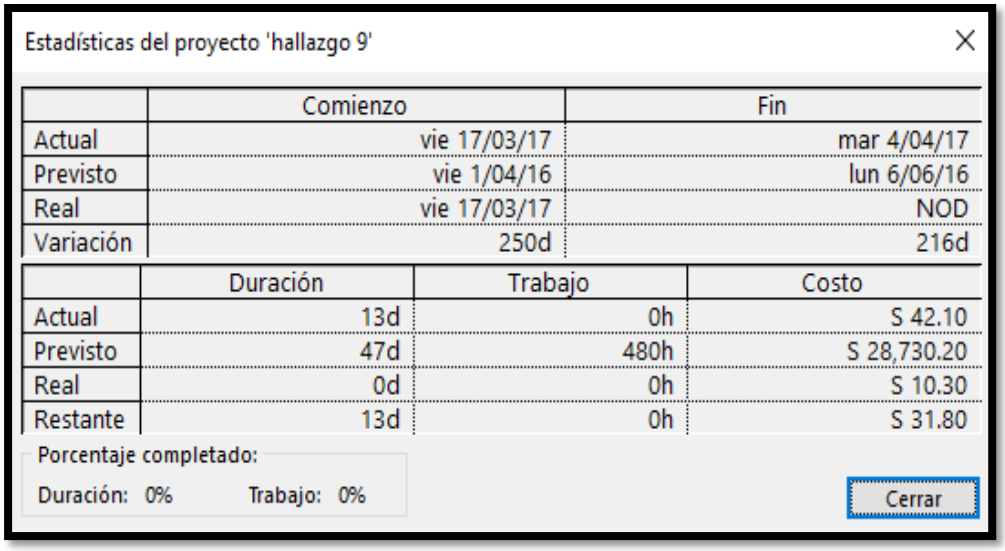


Hallazgo N°8

- Salvaguarda 9“Ordenamiento de los gabinetes de red” En esta figura se observa el costo de implementar el hallazgo final seleccionado N°9, donde genera un costo de S/. 42.10 Nuevos soles.

Figura N°22

Fuente: Elaboración propia



Hallazgo N°9

- Hallazgo 10 “Implementar un libro de control de acceso” En esta figura se observa el costo de implementar el hallazgo final seleccionado N°10, donde genera un costo de S/. 42.10 Nuevos soles.

Figura N°23

Fuente: Elaboración propia

Estadísticas del proyecto 'hallazgo 10'

	Comienzo	Fin
Actual	jue 20/04/17	vie 28/04/17
Previsto	vie 1/04/16	lun 6/06/16
Real	jue 20/04/17	NOD
Variación	274d	234d

	Duración	Trabajo	Costo
Actual	7d	0h	S 42.10
Previsto	47d	480h	S 28,730.20
Real	0d	0h	S 10.30
Restante	7d	0h	S 31.80

Porcentaje completado:

Duración: 0% Trabajo: 0%

Cerrar

Hallazgo N°10

- Hallazgo 11“Implementar el plan de políticas y normas de seguridad” En esta figura se observa el costo de implementar el hallazgo final seleccionado N°11, donde genera un costo de S/. 42.10 Nuevos soles.

Figura N°24

Fuente: Elaboración propia

Estadísticas del proyecto 'hallazgo 11'

	Comienzo	Fin
Actual	lun 8/05/17	vie 19/05/17
Previsto	vie 1/04/16	lun 6/06/16
Real	lun 8/05/17	NOD
Variación	286d	249d

	Duración	Trabajo	Costo
Actual	10d	0h	S 42.10
Previsto	47d	480h	S 28,730.20
Real	0d	0h	S 10.30
Restante	10d	0h	S 31.80

Porcentaje completado:

Duración: 0% Trabajo: 0%

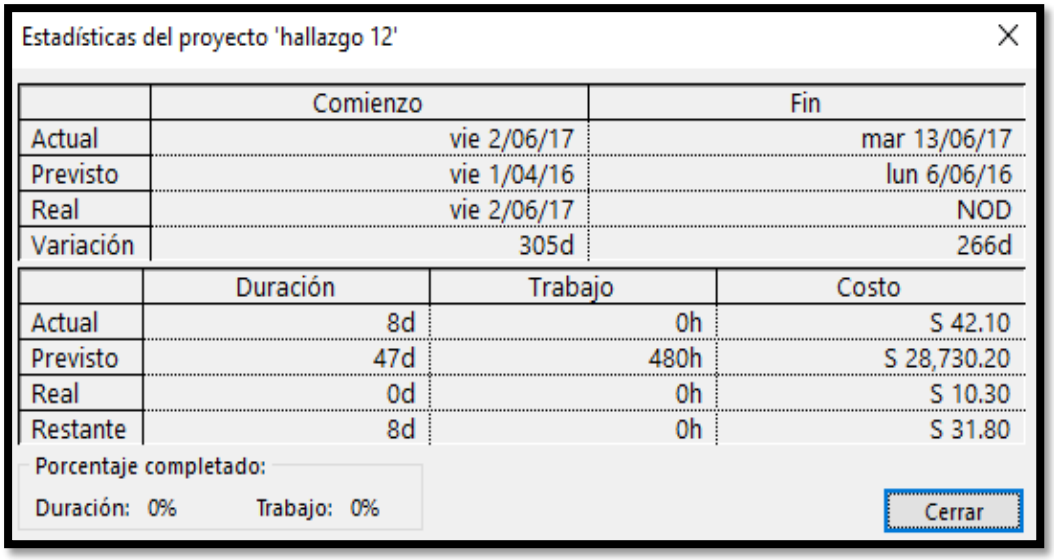
Cerrar

Hallazgo N°11

- Hallazgo 12 “Implementar un procedimiento de resguardo de sobres sellados” En esta figura se observa el costo de implementar el hallazgo final seleccionado N°12, donde genera un costo de S/. 42.10 Nuevos soles.

Figura N°25

Fuente: Elaboración propia

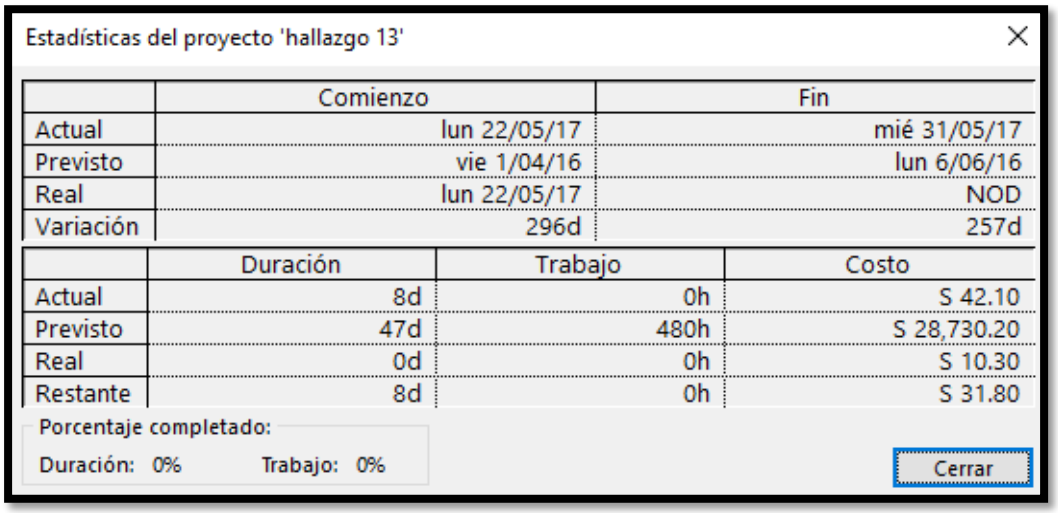


Hallazgo N°12

- Hallazgo 13“Implementar un procedimiento de resguardo de sobres sellados” En esta figura se observa el costo de implementar el hallazgo final seleccionado N°13, donde genera un costo de S/. 42.10 Nuevos soles.

Figura N°26

Fuente: Elaboración propia



Hallazgo N°13

- Costo total de Salvaguardas: En la tabla N°6 se observa el costo total que se generara por implementar las 13 salvaguardas que se van a implementar, donde muestra un costo total de S/. 547.30 Nuevos Soles.

Tabla N°6

Salvaguardas	Dias	Costo (S/.)
Salvaguarda 1	9	S/.42.10
Salvaguarda 2	9	S/.42.10
Salvaguarda 3	5	S/.42.10
Salvaguarda 4	11	S/.42.10
Salvaguarda 5	8	S/.42.10
Salvaguarda 6	8	S/.42.10
Salvaguarda 7	5	S/.42.10
Salvaguarda 8	9	S/.42.10
Salvaguarda 9	13	S/.42.10
Salvaguarda 10	7	S/.42.10
Salvaguarda 11	10	S/.42.10
Salvaguarda 12	8	S/.42.10
Salvaguarda 13	8	S/.42.10
TOTAL	110	S/.547.30

Fuente: Elaboración propia

Costo total de Salvaguardas

- Auditoria Post-test: En la tabla N°7 se muestra el costo que se empleara por ejecutar la segunda Auditoria de post-test en el hospital de San Bartolomé, donde se calcular un monto de S/. 1,420.00 Nuevos Soles.

Tabla N°7

No	Personal	Cantidad	Costo Unitario (S/.)	Dias	Costo toral (S/.)
1	Auditor lider	1	S/.580.00	9	S/.580.00
2	Auditor Líder de Seguridad informática	1	S/.280.00	3	S/.280.00
3	Auditor Interno de seguridad Lógica y física	1	S/.280.00	3	S/.280.00
4	Auditor interno de seguridad de redes	1	S/.280.00	3	S/.280.00
TOTAL					S/.1,420.00

Fuente: Elaboración propia

Recursos humanos - Auditoria Post-test

- Materiales Auditoria Post – test

  En la primera Auditoria que se desarrolló para poder medir las salvaguardas implementadas en el post-test del hospital nacional San Bartolomé, se generó una documentación y utilización de diversos materiales, donde se calculó el gasto de materiales en S/. 104.90 Nuevos Soles.

Tabla N° 8

Fuente: Elaboración propia

No	Personal	Cantidad	Costo Unitario (S/.)	Dias	Costo toral (S/.)
1	Camara digital	1		9	
2	Impresión	200	S/.0.30	9	S/.36.00
3	Material Bibliografico	1	S/.2.00	9	S/.8.60
4	Pasajes	1	S/.5.00	9	S/.50.00
5	Laptop	1		9	
6	USB	1		9	
7	Utiles de oficina	8	S/.2.60	9	S/.10.30
TOTAL					S/.104.90

Materiales Auditoria Pre – test

- Costo total del proyecto: En la tabla N°9 se observa el costo total que costara este proyecto de investigación, donde se muestra al costo de la Auditoria del Post-test y al costo total de salvaguardas, donde muestra un costo total de S/. 3,357.10 Nuevos Soles.

Tabla N°9

Fuente: Elaboración propia

Trabajos	Costo
Auditoria Pre-test	S/.1,284.90
Auditoria Post-test	S/.1,524.90
Salvaguardas	S/.547.30
Costo Total	S/.3,357.10

Costo total del proyecto

3.2. CRONOGRAMA DE EJECUCION

- Recursos humanos - Auditoria Pre – test

  En la figura N°26 se puede observar el cronograma de ejecución del inicio y planeación de la auditoria informatica.

Figura N°27

	Modo de	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras	Nombres de los recursos
1		**INICIO**	**2 días**	**mié 26/10/16**	**jue 27/10/16**		
2		Identificacion de la empresa	1 día	mié 26/10/16	mié 26/10/16		Encargado de Proyecto ;Material Bibliografo[1
3		Reunion de la empresa	1 día	mié 26/10/16	mié 26/10/16	2	Material Bibliografo[1 UNIDADES]
4		Solicitud de cronograma de visita	0 días	mié 26/10/16	mié 26/10/16	3	Laptop[0 UNIDADES];Impresión[0
5		Solicitud de documentos	0 días	jue 27/10/16	jue 27/10/16	4	Impresión[0 UNIDADES]
6		Recopilacion de informacion de la empresa	1 día	jue 27/10/16	jue 27/10/16	5	USB[1 UNIDADES];Laptop[1 UNIDADES]
7		**PLANEACION**	**2 días**	**jue 27/10/16**	**vie 28/10/16**	**6**	
8		Recopilacion de informacion del area de informatica	1 día	jue 27/10/16	jue 27/10/16		USB[1 UNIDADES];Laptop[1 UNIDADES]
9		Asiganacion de roles	1 día	vie 28/10/16	vie 28/10/16	8	Impresión[1 UNIDADES]
10		Elaboracion del programa de	1 día	vie 28/10/16	vie 28/10/16	9	Impresión[1 UNIDADES];Laptop[1
11		Establacer los objetivos generales y	1 día	vie 28/10/16	vie 28/10/16	10	Impresión[1 UNIDADES];Laptop[1
12		Elaboracion del primer entregable	1 día	vie 28/10/16	vie 28/10/16	11	Impresión[1 UNIDADES];Laptop[1
13		**EJECUCION**	**2 días**	**lun 31/10/16**	**mar 01/11/16**	**12**	**Material Bibliografo[2 UI**
21		**CIERRE**	**2 días**	**mar 01/11/16**	**mié 02/11/16**	**20**	**Material Bibliografo[1 UI**

Fuente: Elaboración propia

Diagrama de Gantt – Auditoria Pre – test

En la figura N°27 se puede observar el cronograma de la ejecución y cierre de la auditoria informatica

Figura N°28

	Modo de	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras	Nombres de los recursos
1		**INICIO**	**2 días**	**mié 26/10/16**	**jue 27/10/16**		
7		**PLANEACION**	**2 días**	**jue 27/10/16**	**vie 28/10/16**	**6**	
13		**EJECUCION**	**2 días**	**lun 31/10/16**	**mar 01/11/16**	**12**	**Material Bibliografo[2 UNI**
14		Analisis de datos recopilados	0 días	lun 31/10/16	lun 31/10/16		Impresión[0 UNIDADES];USB[0
15		Aplicación de estandar de apoyo	0 días	lun 31/10/16	lun 31/10/16	14	Impresión[0 UNIDADES];Material
16		Entrevista al personal	0 días	lun 31/10/16	lun 31/10/16	15	Impresión[0 UNIDADES];Ca
17		Evidencias	0 días	lun 31/10/16	lun 31/10/16	16	Camara Digital[0 UNIDADES
18		Elaboracion de lista final de hallazgos	0 días	lun 31/10/16	lun 31/10/16	17	Impresión[0 UNIDADES];Material
19		Elaboracion de matriz de hallazgos	0 días	mar 01/11/16	mar 01/11/16	18	Impresión[0 UNIDADES];Material
20		Elaboracion del segundo entregable	1 día	lun 31/10/16	mar 01/11/16	19	USB[0 UNIDADES];Material Bibliografo[0
21		**CIERRE**	**2 días**	**mar 01/11/16**	**mié 02/11/16**	**20**	**Material Bibliografo[1 UNI**
22		Entrega y sustentacion del plan de Auditoria	2 días	mar 01/11/16	mié 02/11/16		Utiles de Oficina[1 UNIDADES];Material Bibliografo[1

Fuente: Elaboración propia

Diagrama de Gantt – Auditoria Pre – test

- Salvaguarda 1: “Establecer una lista de usuarios con acceso a la red” En la figura N°28 se observa el cronograma para implementar la salvaguarda en el hospital San Bartolomé

Figura N°29

	Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
1		**INICIO**	**1 día**	**vie 13/01/17**	**vie 13/01/17**	
2		Reunion con la empresa	0 días	vie 13/01/17	vie 13/01/17	
3		Solicitud de cronograma de ejecucion	0 días	vie 13/01/17	vie 13/01/17	2
4		**PLANEACION**	**5 días**	**lun 16/01/17**	**vie 20/01/17**	
5		Recopilacion de informacion del area de informatica	0 días	lun 16/01/17	lun 16/01/17	
6		Establacer los objetivos generales y especificos	0 días	mar 17/01/17	mar 17/01/17	
7		Elaboracion del primer entregable	3 días	mié 18/01/17	vie 20/01/17	6
8		**EJECUCION**	**2 días**	**vie 20/01/17**	**lun 23/01/17**	**7**
9		Analisis de datos recopilados	1 día	vie 20/01/17	vie 20/01/17	
10		Elaboracion del segundo entregable	2 días	vie 20/01/17	lun 23/01/17	
11		**CIERRE**	**3 días**	**lun 23/01/17**	**mié 25/01/17**	**10**
12		Entrega y sustentacion de la lista de usuarios con acceso a la red	3 días	lun 23/01/17	mié 25/01/17	

Fuente: Elaboración propia

Diagrama de Gantt: Salvaguarda 1

- Salvaguarda 2“Establecer una lista de cuentas activas” En la figura N°29 se observa el cronograma para implementar la salvaguarda en el hospital San Bartolomé

Figura N°30

Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
	INICIO	**1 día**	**vie 30/12/16**	**vie 30/12/16**	
	Reunion con la empresa	0 días	vie 30/12/16	vie 30/12/16	
	Solicitud de cronograma de ejecucion	0 días	vie 30/12/16	vie 30/12/16	2
	PLANEACION	**5 días**	**lun 2/01/17**	**vie 6/01/17**	
	Recopilacion de informacion del area de informatica	0 días	lun 2/01/17	lun 2/01/17	
	Establacer los objetivos generales y especificos	0 días	mar 3/01/17	mar 3/01/17	
	Elaboracion del primer entregable	0 días	jue 5/01/17	jue 5/01/17	6
	EJECUCION	**2 días**	**vie 6/01/17**	**lun 9/01/17**	**7**
	Analisis de datos recopilados	0 días	vie 6/01/17	vie 6/01/17	
	Elaboracion del segundo entregable	0 días	vie 6/01/17	vie 6/01/17	
	CIERRE	**3 días**	**lun 9/01/17**	**mié 11/01/17**	**10**
	Entrega y sustentacion de la lista de ucuentas activas	3 días	lun 9/01/17	mié 11/01/17	

Fuente: Elaboración propia

Diagrama de Gantt: Salvaguarda 2

- Salvaguarda 3“Establecer políticas y administración de contraseñas” En la figura N°30 se observa el cronograma para implementar la salvaguarda en el hospital San Bartolomé

Figura N°31

	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
1	**INICIO**	**1 día**	**vie 27/01/17**	**vie 27/01/17**	
2	Reunion con la empresa	0 días	vie 27/01/17	vie 27/01/17	
3	Solicitud de cronograma de ejecucion	0 días	vie 27/01/17	vie 27/01/17	2
4	**PLANEACION**	**6 días**	**lun 30/01/17**	**dom 5/02/17**	
5	Recopilacion de informacion del area de informatica	0 días	lun 30/01/17	lun 30/01/17	
6	Establacer los objetivos generales y especificos	0 días	mar 31/01/17	mar 31/01/17	
7	Elaboracion del primer entregable	4 días	mié 1/02/17	dom 5/02/17	6
8	**EJECUCION**	**4 días**	**lun 6/02/17**	**jue 9/02/17**	**7**
9	Analisis de datos recopilados	1 día	lun 6/02/17	lun 6/02/17	
10	Elaboracion del segundo entregable	3 días	mar 7/02/17	jue 9/02/17	
11	**CIERRE**	**2 días**	**jue 9/02/17**	**vie 10/02/17**	**10**
12	Entrega y sustentacion de politicas y administracion de contraseñas	2 días	jue 9/02/17	vie 10/02/17	

Fuente: Elaboración propia

Diagrama de Gantt: Salvaguarda 3

- Salvaguarda 4 “Realizar grupos de acceso a internet” En la figura N°31 se observa el cronograma para implementar la salvaguarda en el hospital San Bartolomé

Figura N°32

Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
	INICIO	**1 día**	**lun 13/02/17**	**lun 13/02/17**	
	Reunion con la empresa	0 días	lun 13/02/17	lun 13/02/17	
	Solicitud de cronograma de ejecucion	0 días	lun 13/02/17	lun 13/02/17	2
	PLANEACION	**2 días**	**lun 13/02/17**	**mar 14/02/17**	
	Recopilacion de informacion del area de informatica	0 días	lun 13/02/17	lun 13/02/17	
	Establacer los objetivos generales y especificos	0 días	lun 13/02/17	lun 13/02/17	
	Elaboracion del primer entregable	2 días	lun 13/02/17	mar 14/02/17	6
	EJECUCION	**3 días**	**mar 14/02/17**	**jue 16/02/17**	**7**
	Analisis de datos recopilados	1 día	mar 14/02/17	mar 14/02/17	
	Elaboracion del segundo entregable	3 días	mar 14/02/17	jue 16/02/17	
	CIERRE	**2 días**	**jue 16/02/17**	**vie 17/02/17**	**10**
	Entrega y sustentacion de grupos de acceso a internet	2 días	jue 16/02/17	vie 17/02/17	

Fuente: Elaboración propia

Diagrama de Gantt: Salvaguarda 4

- Salvaguarda 5 “Establecer una guía para que el usuario seleccione y realice el mantenimiento de contraseñas seguras” En la figura N°32 se observa el cronograma para implementar la salvaguarda en el hospital San Bartolomé

Figura N°33

Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
	INICIO	**1 día**	**lun 20/02/17**	**lun 20/02/17**	
	Reunion con la empresa	0 días	lun 20/02/17	lun 20/02/17	
	Solicitud de cronograma de ejecucion	0 días	lun 20/02/17	lun 20/02/17	2
	PLANEACION	**3 días**	**mar 21/02/17**	**jue 23/02/17**	
	Recopilacion de informacion del area de informatica	0 días	mar 21/02/17	mar 21/02/17	
	Establacer los objetivos generales y especificos	0 días	mar 21/02/17	mar 21/02/17	
	Elaboracion del primer entregable	2 días	mar 21/02/17	mié 22/02/17	6
	EJECUCION	**4 días**	**mié 22/02/17**	**lun 27/02/17**	**7**
	Analisis de datos recopilados	1 día	mié 22/02/17	mié 22/02/17	
	Elaboracion del segundo entregable	4 días	mié 22/02/17	lun 27/02/17	
	CIERRE	**2 días**	**mar 28/02/17**	**mié 1/03/17**	**10**
	Entrega y sustentacion de la guia de mantenimiento de contraseñas	2 días	mar 28/02/17	mié 1/03/17	

Fuente: Elaboración propia

Diagrama de Gantt: Salvaguarda 5

- Salvaguarda 6“Desarrollar e implementar directrices y controles para la detección, prevención y tratamiento de software malicioso” En la figura N°33 se observa el cronograma para implementar la salvaguarda en el hospital San Bartolomé

Figura N°34

Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
	INICIO	**1 día**	**vie 3/03/17**	**vie 3/03/17**	
	Reunion con la empresa	0 días	vie 3/03/17	vie 3/03/17	
	Solicitud de cronograma de ejecucion	0 días	vie 3/03/17	vie 3/03/17	2
	PLANEACION	**5 días**	**sáb 4/03/17**	**jue 9/03/17**	
	Recopilacion de informacion del area de informatica	0 días	sáb 4/03/17	sáb 4/03/17	
	Establacer los objetivos generales y especificos	0 días	dom 5/03/17	dom 5/03/17	
	Elaboracion del primer entregable	4 días	lun 6/03/17	jue 9/03/17	6
	EJECUCION	**2 días**	**vie 10/03/17**	**lun 13/03/17**	**7**
	Analisis de datos recopilados	1 día	vie 10/03/17	vie 10/03/17	
	Elaboracion del segundo entregable	2 días	vie 10/03/17	lun 13/03/17	
	CIERRE	**2 días**	**lun 13/03/17**	**mar 14/03/17**	**10**
	Entrega y sustentacion de directrices y controles para la deteccion, prevencion y tratamiento de software malicioso	2 días	lun 13/03/17	mar 14/03/17	

Fuente: Elaboración propia

Diagrama de Gantt: Salvaguarda 6

- Salvaguarda 7“Implementar controles de seguridad para la instalación de cualquier software en un equipo informático” En la figura N°34 se observa el cronograma para implementar la salvaguarda en el hospital San Bartolomé

Figura N°35

Fuente: Elaboración propia

Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin	Predecesor
	INICIO	**1 día**	**lun 1/05/17**	**lun 1/05/17**	
	Reunion con la empresa	0 días	lun 1/05/17	lun 1/05/17	
	Solicitud de cronograma de ejecucion	0 días	lun 1/05/17	lun 1/05/17	2
	PLANEACION	**2 días**	**mar 2/05/17**	**mié 3/05/17**	
	Recopilacion de informacion del area de informatica	0 días	mar 2/05/17	mar 2/05/17	
	Establacer los objetivos generales y especificos	0 días	mar 2/05/17	mar 2/05/17	
	identificar que programas son instalados por los mismos usuarios	2 días	mar 2/05/17	mié 3/05/17	6
	EJECUCION	**2 días**	**mié 3/05/17**	**jue 4/05/17**	**7**
	Implementar medidas de control de instalacion de software	1 día	mié 3/05/17	mié 3/05/17	
	Elaboracion del primer entregable	1 día	jue 4/05/17	jue 4/05/17	
	CIERRE	**1 día**	**vie 5/05/17**	**vie 5/05/17**	**10**
	Entrega y sustentacion de controles de seguridad para la instalacion de cualquier software en un equipo informatico	1 día	vie 5/05/17	vie 5/05/17	

Diagrama de Gantt: Salvaguarda 7

- Salvaguarda 8“Desarrollar e implementar controles para el mantenimiento preventivo de los equipos informáticos” En la figura N°35 se observa el cronograma para implementar la salvaguarda en el hospital San Bartolomé

Figura N°36

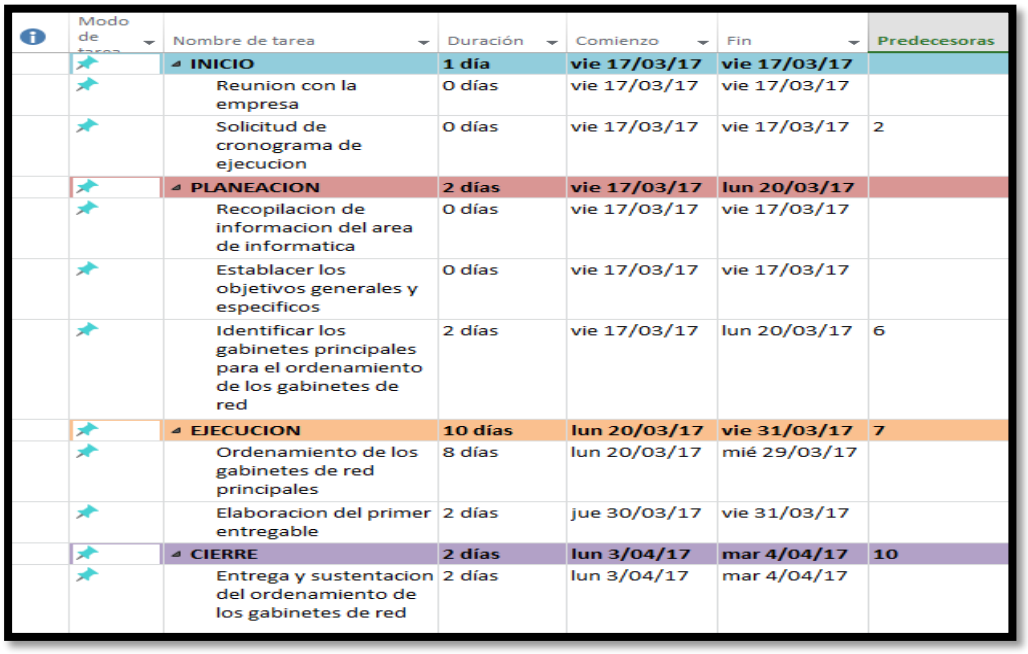
Fuente: Elaboración propia

Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
	INICIO	**1 día**	**jue 6/04/17**	**jue 6/04/17**	
	Reunion con la empresa	0 días	jue 6/04/17	jue 6/04/17	
	Solicitud de cronograma de ejecucion	0 días	jue 6/04/17	jue 6/04/17	2
	PLANEACION	**2 días**	**vie 7/04/17**	**lun 10/04/17**	
	Recopilacion de informacion del area de informatica	0 días	vie 7/04/17	vie 7/04/17	
	Establacer los objetivos generales y especificos	0 días	vie 7/04/17	vie 7/04/17	
	identificar los problemas mas propensos que tienen los equipos informaticos	2 días	sáb 8/04/17	lun 10/04/17	6
	EJECUCION	**5 días**	**mar 11/04/17**	**sáb 15/04/17**	**7**
	Elaboracion de controles de prevencion de los equipos informaticos	1 día	mar 11/04/17	mar 11/04/17	
	Elaboracion del primer entregable	4 días	mié 12/04/17	sáb 15/04/17	
	CIERRE	**2 días**	**lun 17/04/17**	**mar 18/04/17**	**10**
	Entrega y sustentacion de los controles para el mantenimiento preventivo de los equipos informaticos	2 días	lun 17/04/17	mar 18/04/17	

Diagrama de Gantt: Salvaguarda 8

- Hallazgo 9“Ordenamiento de los gabinetes de red” En la figura N°36 se observa el cronograma para implementar la salvaguarda en el hospital San Bartolomé

Figura N°37



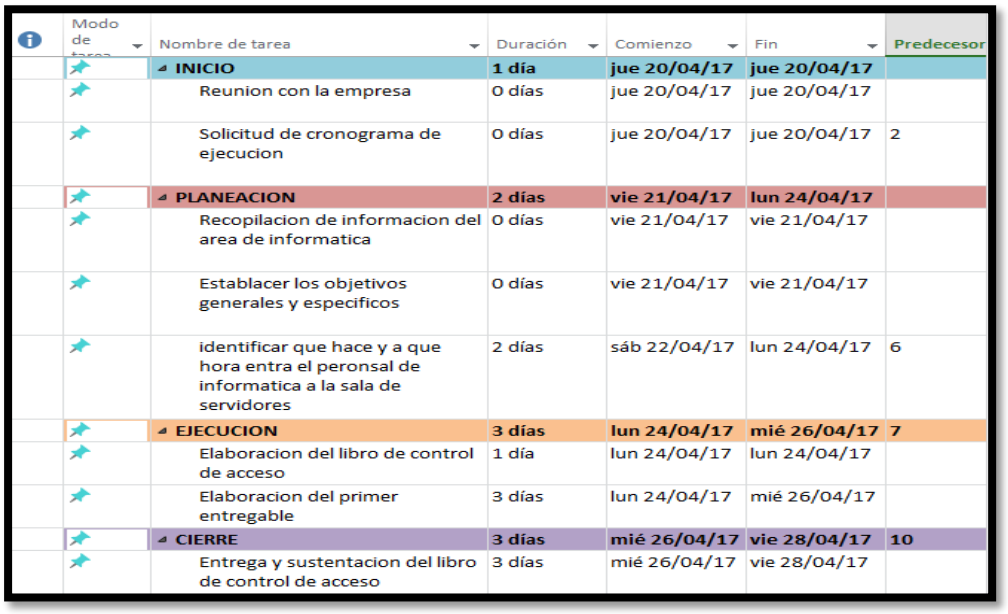
Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
	INICIO	**1 día**	**vie 17/03/17**	**vie 17/03/17**	
	Reunion con la empresa	0 días	vie 17/03/17	vie 17/03/17	
	Solicitud de cronograma de ejecucion	0 días	vie 17/03/17	vie 17/03/17	2
	PLANEACION	**2 días**	**vie 17/03/17**	**lun 20/03/17**	
	Recopilacion de informacion del area de informatica	0 días	vie 17/03/17	vie 17/03/17	
	Establacer los objetivos generales y especificos	0 días	vie 17/03/17	vie 17/03/17	
	Identificar los gabinetes principales para el ordenamiento de los gabinetes de red	2 días	vie 17/03/17	lun 20/03/17	6
	EJECUCION	**10 días**	**lun 20/03/17**	**vie 31/03/17**	**7**
	Ordenamiento de los gabinetes de red principales	8 días	lun 20/03/17	mié 29/03/17	
	Elaboracion del primer entregable	2 días	jue 30/03/17	vie 31/03/17	
	CIERRE	**2 días**	**lun 3/04/17**	**mar 4/04/17**	**10**
	Entrega y sustentacion del ordenamiento de los gabinetes de red	2 días	lun 3/04/17	mar 4/04/17	

Fuente: Elaboración propia

Diagrama de Gantt: Salvaguarda 9

- Hallazgo 10“Implementar un libro de control de acceso” En la figura N°37se observa el cronograma para implementar la salvaguarda en el hospital San Bartolomé

Figura N°38



Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin	Predecesor
	INICIO	**1 día**	**jue 20/04/17**	**jue 20/04/17**	
	Reunion con la empresa	0 días	jue 20/04/17	jue 20/04/17	
	Solicitud de cronograma de ejecucion	0 días	jue 20/04/17	jue 20/04/17	2
	PLANEACION	**2 días**	**vie 21/04/17**	**lun 24/04/17**	
	Recopilacion de informacion del area de informatica	0 días	vie 21/04/17	vie 21/04/17	
	Establacer los objetivos generales y especificos	0 días	vie 21/04/17	vie 21/04/17	
	identificar que hace y a que hora entra el peronsal de informatica a la sala de servidores	2 días	sáb 22/04/17	lun 24/04/17	6
	EJECUCION	**3 días**	**lun 24/04/17**	**mié 26/04/17**	**7**
	Elaboracion del libro de control de acceso	1 día	lun 24/04/17	lun 24/04/17	
	Elaboracion del primer entregable	3 días	lun 24/04/17	mié 26/04/17	
	CIERRE	**3 días**	**mié 26/04/17**	**vie 28/04/17**	**10**
	Entrega y sustentacion del libro de control de acceso	3 días	mié 26/04/17	vie 28/04/17	

Fuente: Elaboración propia

Diagrama de Gantt: Salvaguarda 10

- Hallazgo 11“Implementar el plan de políticas y normas de seguridad” En la figura N°38 se observa el cronograma para implementar la salvaguarda en el hospital San Bartolomé

Figura N°39

Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
	INICIO	**1 día**	**lun 8/05/17**	**lun 8/05/17**	
	Reunion con la empresa	0 días	lun 8/05/17	lun 8/05/17	
	Solicitud de cronograma de ejecucion	0 días	lun 8/05/17	lun 8/05/17	2
	PLANEACION	**4 días**	**mar 9/05/17**	**vie 12/05/17**	
	Recopilacion de informacion del area de informatica	0 días	mar 9/05/17	mar 9/05/17	
	Establacer los objetivos generales y especificos	0 días	mar 9/05/17	mar 9/05/17	
	identificar las medidas de control que tiene la seguridad informatica	3 días	mié 10/05/17	vie 12/05/17	6
	EJECUCION	**4 días**	**vie 12/05/17**	**mié 17/05/17**	**7**
	Implementar el plan de politicas de seguridad	1 día	vie 12/05/17	vie 12/05/17	
	Elaboracion del primer entregable	4 días	vie 12/05/17	mié 17/05/17	
	CIERRE	**2 días**	**jue 18/05/17**	**vie 19/05/17**	**10**
	Entrega y sustentacion del plan de politicas y normas de seguridad	2 días	jue 18/05/17	vie 19/05/17	

Fuente: Elaboración propia

Diagrama de Gantt: Salvaguarda 11

- Hallazgo 12“Implementar un procedimiento de resguardo de sobres sellados” En la figura N°38 se observa el cronograma para implementar la salvaguarda en el hospital San Bartolomé

Figura N°40

Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
	INICIO	**1 día**	**vie 2/06/17**	**vie 2/06/17**	
	Reunion con la empresa	0 días	vie 2/06/17	vie 2/06/17	
	Solicitud de cronograma de ejecucion	0 días	vie 2/06/17	vie 2/06/17	2
	PLANEACION	**5 días**	**lun 5/06/17**	**vie 9/06/17**	
	Recopilacion de informacion del area de informatica	0 días	lun 5/06/17	lun 5/06/17	
	Establacer los objetivos generales y especificos	0 días	lun 5/06/17	lun 5/06/17	
	identificar los cambios que hace el administrador de redes en las contraseñas de los servidores	4 días	mar 6/06/17	vie 9/06/17	6
	EJECUCION	**2 días**	**vie 9/06/17**	**lun 12/06/17**	**7**
	Implementar esobres sellados para las contraseñas de los servidores	1 día	vie 9/06/17	vie 9/06/17	
	Elaboracion del primer entregable	2 días	vie 9/06/17	lun 12/06/17	
	CIERRE	**2 días**	**lun 12/06/17**	**mar 13/06/17**	**10**
	Entrega y sustentacion del resguardo de sobres sellados	2 días	lun 12/06/17	mar 13/06/17	

Fuente: Elaboración propia

Diagrama de Gantt: Salvaguarda 12

- Hallazgo 13 ”Implementación de documentación por cada servidor de procedimiento de fallas” En la figura N°40 se observa el cronograma para implementar la salvaguarda en el hospital San Bartolomé

Figura N°41

Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
	INICIO	**1 día**	**lun 22/05/17**	**lun 22/05/17**	
	Reunion con la empresa	0 días	lun 22/05/17	lun 22/05/17	
	Solicitud de cronograma de ejecucion	0 días	lun 22/05/17	lun 22/05/17	2
	PLANEACION	**5 días**	**mar 23/05/17**	**lun 29/05/17**	
	Recopilacion de informacion del area de informatica	0 días	mar 23/05/17	mar 23/05/17	
	Establacer los objetivos generales y especificos	0 días	mié 24/05/17	mié 24/05/17	
	identificar las medidas de control que tiene el personal de informatica para mitigar los riesgos	4 días	mié 24/05/17	lun 29/05/17	6
	EJECUCION	**2 días**	**lun 29/05/17**	**mar 30/05/17**	**7**
	Implementar el documento por cada servidor	1 día	lun 29/05/17	lun 29/05/17	
	Elaboracion del primer entregable	2 días	lun 29/05/17	mar 30/05/17	
	CIERRE	**1 día**	**mié 31/05/17**	**mié 31/05/17**	**10**
	Entrega y sustentacion del documento por cada servidor de procedimiento de fallas	1 día	mié 31/05/17	mié 31/05/17	

Fuente: Elaboración propia

Diagrama de Gantt: Salvaguarda 13

- Auditoria Post-test

En la figura N°41 se puede observar el cronograma de ejecución del inicio y planeación de la auditoria informatica.

Figura N°42

Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras	Nombres de los recursos
	INICIO	**3 días**	**mar 20/06/17**	**jue 22/06/17**		
	Identificacion de la empresa	1 día	mar 20/06/17	mar 20/06/17		Encargado de Proyecto ; Material Bibliografo[0
	Reunion de la empresa	0 días	mar 20/06/17	mar 20/06/17	2	Material Bibliografo[0 UNIDADES]
	Solicitud de cronograma de visita	1 día	mar 20/06/17	mar 20/06/17	3	Laptop[1 UNIDADES]; Impresión[1 UNIDADES]
	Solicitud de documentos	0 días	mié 21/06/17	mié 21/06/17	4	Impresión[0 UNIDADES]
	Recopilacion de informacion de la empresa	0 días	jue 22/06/17	jue 22/06/17	5	USB[0 UNIDADES]; Laptop[0 UNIDADES]
	PLANEACION	**2 días**	**jue 22/06/17**	**vie 23/06/17**	**6**	
	Recopilacion de informacion del area de informatica	0 días	jue 22/06/17	jue 22/06/17		USB[0 UNIDADES]; Laptop[0 UNIDADES]
	Asiganacion de roles	0 días	jue 22/06/17	jue 22/06/17	8	Impresión[0 UNIDADES]
	Elaboracion del programa de Auditoria	0 días	jue 22/06/17	jue 22/06/17	9	Impresión[0 UNIDADES]; Laptop[0 UNIDADES];USB[(
	Establacer los objetivos generales y especificos	0 días	vie 23/06/17	vie 23/06/17	10	Impresión[0 UNIDADES]; Laptop[0 UNIDADES]; USB[0 UNIDADES];Material
	Elaboracion del primer entregable	0 días	vie 23/06/17	vie 23/06/17	11	Impresión[0 UNIDADES]; Laptop[0 UNIDADES];USB[(
	EJECUCION	**3 días**	**lun 26/06/17**	**mié 28/06/17**	**12**	**Material Bibliografo[2 UNI**
	CIERRE	**2 días**	**mié 28/06/17**	**jue 29/06/17**	**20**	**Material Bibliografo[1 UNI**

Fuente: Elaboración propia

Cronograma de Auditoria Post-test inicio y planificación

En la figura N°42 se puede observar el cronograma de ejecución del inicio y planeación de la auditoria informatica.

Figura N°43

Fuente: Elaboración propia

Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras	Nombres de los recursos
	INICIO	**3 días**	**mar 20/06/17**	**jue 22/06/17**		
	PLANEACION	**2 días**	**jue 22/06/17**	**vie 23/06/17**	**6**	
	EJECUCION	**3 días**	**lun 26/06/17**	**mié 28/06/17**	**12**	**Material Bibliografo[2 UNI**
	Analisis de datos recopilados	0 días	lun 26/06/17	lun 26/06/17		Impresión[0 UNIDADES]; USB[0 UNIDADES];Laptop[(
	Aplicación de estandar de apoyo	0 días	lun 26/06/17	lun 26/06/17	14	Impresión[0 UNIDADES]; Material Bibliografo[0
	Entrevista al personal	0 días	lun 26/06/17	lun 26/06/17	15	Impresión[0 UNIDADES];Ca
	Evidencias	0 días	lun 26/06/17	lun 26/06/17	16	Camara Digital[0 UNIDADES
	Elaboracion de lista final de hallazgos	0 días	lun 26/06/17	lun 26/06/17	17	Impresión[0 UNIDADES]; Material Bibliografo[0
	Elaboracion de matriz de hallazgos	0 días	mar 27/06/17	mar 27/06/17	18	Impresión[0 UNIDADES]; Material Bibliografo[0
	Elaboracion del segundo entregable	2 días	mar 27/06/17	mié 28/06/17	19	USB[0 UNIDADES]; Material Bibliografo[0
	CIERRE	**2 días**	**mié 28/06/17**	**jue 29/06/17**	**20**	**Material Bibliografo[1 UNI**
	Entrega y sustentacion del plan de Auditoria	0 días	mié 28/06/17	jue 29/06/17		Utiles de Oficina[0 UNIDADES] Material Bibliografo[0

Cronograma de Auditoria Post-test ejecución y cierre

ANEXO 14: VALIDACION DE INSTRUMENTO

EXPERTO 1

VALIDACIÓN DE INSTRUMENTO

I. DATOS GENERALES

1.1. Apellidos y Nombres:

1.2. Cargo e institución donde Labora:

Universidad César Vallejo, Escuela Academica de Ingeniería de Sistemas

1.3. Nombre del instrumento motivo de Evaluación:

Ficha de Registro – NIVEL DE CUMPLIMIENTO DE SEGURIDAD FISICA

1.4. Título de la investigación:

APLICACIÓN DE LA HERRAMIENTA DE GESTION DE RIESGOS PARA LA SEGURIDAD INFORMAATICA DEL HONADOMANI SAN BARTOLOMI

1.5. Autor: Jerson Joseph, Calderón Alvarado

II. ASPECTOS DE VALIDACIÓN

INDICADORES	CRITERIOS	DEFICIENTE 0 – 20%	REGULAR 21 – 50%	BUENO 51 – 70%	MUY BUENO 71 – 90%	EXCELENTE 91 – 100%
1.CLARIDAD	Esta formulado con el lenguaje apropiado				76%	
2.OBJETIVIDAD	Esta expresado en conducta observable				77%	
3.ACTUALIDAD	Es adecuado al avance de la ciencia y tecnología					85%
4.ORGANIZACIÓN	Existe una organización lógica				77%	
5.SUFICIENCIA	Comprende los aspectos de cantidad y calidad					83%
6.INTENCIONALIDAD	Adecuado para valorar aspectos del sistema metodológico y científico					87%
7.CONSISTENCIA	Esta basado en aspectos teóricos, científicos acordes a la tecnología educativa					85%
8.COHERENCIA	Entre los índices, indicadores, dimensiones					82%
9.METODOLOGIA	Responde al propósito del trabajo bajo los objetivos a lograr				78%	
10.PERTINENCIA	El instrumento es adecuado al tipo de investigación					84%
PROMEDIO DE VALIDACIÓN					77%	83%

III. PROMEDIO DE VALORACION: 80%

IV. OPCIÓN DE APLICABILIDAD:

(X) El instrumento puede ser aplicado, tal como está elaborado.

( ) El instrumento debe ser mejorado, antes de ser aplicado.

Considera las recomendaciones y aplicar al trabajo

Fecha:

FIRMA DEL EXPERTO

MATRIZ DE RIESGOS MAGERIT

VALIDACIÓN DE INSTRUMENTO

I. DATOS GENERALES

1.1. Apellidos y Nombres:

1.2. Cargo e Institución donde Labora:
Universidad César Vallejo, Escuela Académica de Ingeniería de Sistemas.

1.3. Nombre del Instrumento motivo de Evaluación:
Ficha de Registro – NIVEL DE CUMPLIMIENTO DE SEGURIDAD DE REDES

1.4. Título de la Investigación:
APLICACIÓN DE LA HERRAMIENTA DE GESTION DE RIESGOS PARA LA SEGURIDAD INFORMATICA DEL HONADOMANI SAN BARTOLOME

1.5. Autor: Jerson Joseph, Calderón Alvarado

II. ASPECTOS DE VALIDACIÓN

INDICADORES	CRITERIOS	DEFICIENTE 0 – 20%	REGULAR 21 – 50%	BUENO 51 – 70%	MUY BUENO 71 – 80%	EXCELENTE 81 – 100%
1.CLARIDAD	Esta formulado con el lenguaje apropiado				75%	
2.OBJETIVIDAD	Esta expresado en conducta observable				79%	
3.ACTUALIDAD	Es adecuado al avance de la ciencia y tecnología					85%
4.ORGANIZACIÓN	Existe una organización lógica				79%	
5.SUFICIENCIA	Comprende los aspectos de cantidad y calidad					89%
6.INTENCIONALIDAD	Adecuado para valorar aspectos del sistema metodológico y científico					89%
7.CONSISTENCIA	Está basado en aspectos teóricos, científicos acordes a la tecnología educativa					85%
8.COHERENCIA	Entre los índices, indicadores, dimensiones					89%
9.METODOLOGIA	Responde al propósito del trabajo bajo los objetivos a lograr				78%	
10.PERTINENCIA	El instrumento es adecuado al tipo de investigación					87%
PROMEDIO DE VALIDACIÓN					77%	83%

III. PROMEDIO DE VALORACION: 80%

IV. OPCIÓN DE APLICABILIDAD:

(X) El instrumento puede ser aplicado, tal como está elaborado.

( ) El instrumento debe ser mejorado, antes de ser aplicado.

Considera las recomendaciones y aplicar al trabajo

Fecha:

FIRMA DEL EXPERTO

MATRIZ DE RIESGOS MAGERIT

VALIDACIÓN DE INSTRUMENTO

I. DATOS GENERALES

1.1. Apellidos y Nombres:

1.2. Cargo e Institución donde Labora:

Universidad César Vallejo, Escuela Académica de Ingeniería de Sistemas.

1.3. Nombre del Instrumento motivo de Evaluación:

Ficha de Registro – NIVEL DE CUMPLIMIENTO DE SEGURIDAD LOGICA

1.4. Título de la Investigación:

APLICACIÓN DE LA HERRAMIENTA DE GESTION DE RIESGOS PARA LA SEGURIDAD INFORMATICA DEL HONADOMANI SAN BARTOLOME

1.5. Autor: Jerson Joseph, Calderón Alvarado

II. ASPECTOS DE VALIDACIÓN

INDICADORES	CRITERIOS	DEFICIENTE 0 – 20%	REGULAR 21 – 50%	BUENO 51 – 70%	MUY BUENO 71 – 80%	EXCELENTE 81 – 100%
1.CLARIDAD	Esta formulado con el lenguaje apropiado				75%	
2.OBJETIVIDAD	Esta expresado en conducta observable				77%	
3.ACTUALIDAD	Es adecuado al avance de la ciencia y tecnología					85%
4.ORGANIZACIÓN	Existe una organización lógica				77%	
5.SUFICIENCIA	Comprende los aspectos de cantidad y claridad					82%
6.INTENCIONALIDAD	Adecuado para valorar aspectos del sistema metodológico y científico					82%
7.CONSISTENCIA	Está basado en aspectos teóricos, científicos acordes a la tecnología educativa					85%
8.COHERENCIA	Entre los índices, indicadores, dimensiones					87%
9.METODOLOGÍA	Responde al propósito del trabajo bajo los objetivos a lograr				78%	
10.PERTINENCIA	El instrumento es adecuado al tipo de investigación					82%
PROMEDIO DE VALIDACIÓN					74%	83%

III. PROMEDIO DE VALORACIÓN: 79%

IV. OPCIÓN DE APLICABILIDAD:

(X) El instrumento puede ser aplicado, tal como está elaborado.

( ) El instrumento debe ser mejorado, antes de ser aplicado.

Considera las recomendaciones y aplicar al trabajo

Fecha:

FIRMA DEL EXPERTO

MATRIZ DE RIESGOS MAGERIT

EXPERTO 2

VALIDACIÓN DE INSTRUMENTO

I. DATOS GENERALES

1.1. Apellidos y Nombres:

1.2. Cargo e Institución donde Labora:

Universidad Cesar Vallejo, Escuela Academica de Ingeniería de Sistemas

1.3. Nombre del Instrumento motivo de Evaluación:

Ficha de Registro – NIVEL DE CUMPLIMIENTO DE SEGURIDAD FISICA

1.4. Título de la Investigación:

APLICACIÓN DE LA HERRAMIENTA DE GESTION DE RIESGOS PARA LA SEGURIDAD INFORMATICA DEL HONADOMANI SAN BARTOLOME

1.5. Autor: Jerson Joseph, Calderón Alvarado

II. ASPECTOS DE VALIDACIÓN

INDICADORES	CRITERIOS	DEFICIENTE 0 – 20%	REGULAR 21 – 50%	BUENO 51 – 70%	MUY BUENO 71 – 80%	EXCELENTE 81 – 100%
1.CLARIDAD	Esta formulado con el lenguaje apropiado				76%	
2.OBJETIVIDAD	Esta expresado en conducta observable				76%	
3.ACTUALIDAD	Es adecuado al avance de la ciencia y tecnologia					84%
4.ORGANIZACIÓN	Existe una organización lógica				76%	
5.SUFICIENCIA	Comprende los aspectos de cantidad y claridad					84%
6.INTENCIONALIDAD	Adecuado para valorar aspectos del sistema metodológico y científico					84%
7.CONSISTENCIA	Está basado en aspectos teóricos, científicos acordes a la tecnología educativa					84%
8.COHERENCIA	Entre los indices, indicadores, dimensiones				76%	
9.METODOLOGIA	Responde al propósito del trabajo bajo los objetivos a lograr				76%	
10.PERTINENCIA	El instrumento es adecuado al tipo de investigación				80%	
PROMEDIO DE VALIDACIÓN					77%	84%

III. PROMEDIO DE VALORACION: 81%

IV. OPCIÓN DE APLICABILIDAD:

(X) El instrumento puede ser aplicado, tal como está elaborado.

( ) El instrumento debe ser mejorado, antes de ser aplicado.

Considera las recomendaciones y aplicar al trabajo

Fecha:

FIRMA DEL EXPERTO

MATRIZ DE RIESGOS MAGERIT

VALIDACIÓN DE INSTRUMENTO

I. DATOS GENERALES

1.1. Apellidos y Nombres:

1.2. Cargo e Institución donde Labora:

Universidad César Vallejo, Escuela Académica de Ingeniería de Sistemas.

1.3. Nombre del Instrumento motivo de Evaluación:

Ficha de Registro – NIVEL DE CUMPLIMIENTO DE SEGURIDAD DE REDES

1.4. Título de la Investigación:

APLICACIÓN DE LA HERRAMIENTA DE GESTION DE RIESGOS PARA LA SEGURIDAD INFORMATICA DEL HOSPITAL HONADOMANI SAN BARTOLOME

1.5. Autor: Jerson Joseph, Calderón Alcarado

II. ASPECTOS DE VALIDACIÓN

INDICADORES	CRITERIOS	DEFICIENTE 0 – 30%	REGULAR 31 – 50%	BUENO 51 – 70%	MUY BUENO 71 – 80%	EXCELENTE 81 – 100%
1.CLARIDAD	Está formulado con el lenguaje apropiado				74%	
2.OBJETIVIDAD	Está expresado en conducta observable				76%	
3.ACTUALIDAD	Es adecuado al avance de la ciencia y tecnología					84%
4.ORGANIZACIÓN	Existe una organización lógica				76%	
5.SUFICIENCIA	Comprende los aspectos de cantidad y calidad					84%
6.INTENCIONALIDAD	Adecuado para valorar aspectos del sistema metodológico y científico					84%
7.CONSISTENCIA	Está basado en aspectos teóricos, científicos acordes a la tecnología educativa					84%
8.COHERENCIA	Entre los índices, indicadores, dimensiones				74%	
9.METODOLOGÍA	Responde al propósito del trabajo bajo los objetivos a lograr				76%	
10.PERTINENCIA	El instrumento es adecuado al tipo de investigación				76%	
PROMEDIO DE VALIDACIÓN					76%	84%

III. PROMEDIO DE VALORACION: 80%

IV. OPCIÓN DE APLICABILIDAD:

(X) El Instrumento puede ser aplicado, tal como está elaborado.

( ) El Instrumento debe ser mejorado, antes de ser aplicado.

Considera las recomendaciones y aplicar al trabajo

Fecha:

FIRMA DEL EXPERTO

VALIDACIÓN DE INSTRUMENTO

I. DATOS GENERALES

1.1. Apellidos y Nombres:

1.2. Cargo e institución donde Labora:

Universidad Cesar Vallejo, Escuela Academico de Ingeniería de Sistemas

1.3. Nombre del Instrumento motivo de Evaluación:

Ficha de Registro - NIVEL DE CUMPLIMIENTO DE SEGURIDAD LOGICA

1.4. Título de la investigación:

APLICACIÓN DE LA HERRAMIENTA DE GESTION DE RIESGOS PARA LA SEGURIDAD INFORMATICA DEL HONADOMAAI SAN BARTOLOMÉ

1.5. Autor: Jerson Joseph, Calderón Alvarado

II. ASPECTOS DE VALIDACIÓN

INDICADORES	CRITERIOS	DEFICIENTE 0 - 30%	REGULAR 31 - 50%	BUENO 51 - 70%	MUY BUENO 71 - 80%	EXCELENTE 81 - 100%
1.CLARIDAD	Esta formulado con el lenguaje apropiado				75%	
2.OBJETIVIDAD	Esta expresado en conducta observable				75%	
3.ACTUALIDAD	Es adecuado al avance de la ciencia y tecnología					84%
4.ORGANIZACIÓN	Existe una organización lógica				75%	
5.SUFICIENCIA	Comprende los aspectos de cantidad y calidad					84%
6.INTENCIONALIDAD	Adecuado para valorar aspectos del sistema metodológico y científico					84%
7.CONSISTENCIA	Esta basado en aspectos teóricos, científicos acordes a la tecnología educativa					84%
8.COHERENCIA	Entre los índices, indicadores, dimensiones				75%	
9.METODOLOGÍA	Responde al propósito del trabajo bajo los objetivos a lograr				75%	
10.PERTINENCIA	El instrumento es adecuado al tipo de investigación					84%
PROMEDIO DE VALIDACIÓN					75%	84%

III. PROMEDIO DE VALORACIÓN: 80%

IV. OPCIÓN DE APLICABILIDAD:

(X) El instrumento puede ser aplicado, tal como está elaborado.

( ) El instrumento debe ser mejorado, antes de ser aplicado.

Considera las recomendaciones y aplicar al trabajo

Fecha:

FIRMA DEL EXPERTO

ANEXO 15: HOJA DE VIDA DEL AUDITOR INTERNO

ALEXANDER CLAUDE GARCIA PALACIOS

Fecha de Nacimiento: 21 de Febrero de 1994

Dirección: **Psj 3 de octubre #135 San Ramón la Balanza Comas-Lima**

Teléfono: **957281145/ 633-9391**

E-mail: **alexcgp94@gmail.com**

RESUMEN

Estudiante de Ingeniería de Sistemas. Investigador y proponente de nuevas metodologías, participando en implementaciones de Agile Testing, soy una persona dinámica y respetuosa, habilidad para desarrollar trabajos en equipo y para relacionarme a todo nivel.

FORMACIÓN ACADÉMICA

- **UNIVERSIDAD CÉSAR VALLEJO**

  Estudiante de Ingeniería de Sistemas (9no ciclo)

EXPERIENCIA PROFESIONAL / LABORAL

Q SYSTEM S.A.C **(2016 - Actualidad)**

Q SYSTEM S.A.C es una empresa de tecnología especializada en brindar servicios de Desarrollo de Software y QA en sus diferentes modalidades (Consultoría, Asistencia Técnica/Provisión de personal especializado

ANALISTA DE CONTROL DE CALIDAD

Contribuyente en proyectos de automatización de pruebas, logrando automatizar más de 50% de pruebas de regresión.

Ejecución del ciclo de pruebas de software, desde la planificación, diseño, ejecución en aplicaciones web, desarrolladas en Java, Oracle, SQL y Testing de Apps para Android.

Ejecución de pruebas funcionales, integradas, reporte de incidencia y pruebas de carga (estrés) en aplicaciones web, desarrolladas en Java con Oracle, .Net con SQL Server.

Participe en el Proyecto de "Apertura de Cuenta de Ahorros" del Banco de Crédito (BCP) realizando lo siguiente:

- Planificación de Pruebas
- Pruebas de Regresión
- Diseño de Pruebas
- Ejecución de los casos de pruebas
- Testing Funcional (Manual y Automatizado) y no Funcional
- Mantis / Bugzilla (gestión de defectos)

CURSOS

- **DIPLOMADO: "**Sistema de Gestión de Seguridad de la Información**"** – BS GRUPO
- **CERTIFICADO: "**Desarrollador de Base de Datos con SQL Server**"** – CEPS UNI
- **CERTIFICADO: "**Asistente Help Desk**"** – Universidad César Vallejo
- **CONFERENCIA: "**Buenas Practicas en Gestión de Proyectos**"** – SEDIPRO PUCP
- **CONFERENCIA: "**Nuevas tecnologías de información**"** – Universidad César Vallejo
- **CERTIFICADO: "**Asistente Help Desk**"** – Universidad César Vallejo
- **CERTIFICADO: "**CCNA1, CCNA2, CCNA3**"**

IDIOMAS

- **INGLÉS:**

  Conocimientos Básicos – Intermedio
  Centro de Idiomas de la Universidad Cesar Vallejo.

COMPUTACIÓN

MS Office Profesional (Excel, Word, Access, Power Point, Ms Project)
Conocimiento en Java, Php, MS Sql server avanzado, Html 5, Oracle, UML, Erwin y Rational Rose. Dominio en Windows server 2008 R2, VmWare, Hyper-V

INFORMACIÓN ADICIONAL

- Facilidad de Comunicación, Creatividad e Iniciativa.
- Rapidez en aprendizaje.

REFERENCIAS PERSONALES

Sr. Rómulo Fernando Lomparte Alvarado Teléfono: 99638080

Gerente de tecnología del GRUPO EPENSA, Consultor en Gobierno de TI, Auditoria de Sistemas y Seguridad de la Información.

-*