UNIVERSIDAD SAN PEDRO

FACULTAD DE INGENIERIA

PROGRAMA DE ESTUDIOS DE INGENIERÍA INFORMÁTICA Y DE SISTEMAS

Evaluación de la seguridad de la red de datos del Hospital Regional de Huacho

Tesis para obtener el título profesional de Ingeniera

en Informática y de Sistemas

Autoras

Marcos Susanibar, Kateryn Mirella

Tena Renteria, Fiorela Mishell

Asesor

Villarreal Torres, Henry Oswaldo

HUACHO – PERU

2020

Palabras Clave:

Tema	Red de Datos
Especialidad	Gestión

Keeywords

Theme	**Data network**
Specialty	**Management**

Línea de Investigación

Área	Ciencias sociales
Sub área	Economía y negocios
Disciplina	Negocios y Management

Titulo

Evaluación a la seguridad de la red de datos del Hospital Regional de Huacho

Resumen

El presente proyecto de investigación tuvo por objetivo realizar la evaluación de la seguridad de la red de datos del Hospital Regional de Huacho, utilizando herramientas y políticas de seguridad, fundamentada en las mejores prácticas y estándares internacionales para alcanzar ese fin.

Se utilizó el tipo de investigación tecnológico, con diseño de tipo no experimental con corte transversal. La investigación se fundamentó en el Marco de Trabajo MAIGTI, el cual estableció las herramientas para la evaluación del presente estudio.

Como resultados esperados se logró identificar las vulnerabilidades y amenazas para mitigar los riesgos en la seguridad de la red de datos del Hospital Regional de Huacho.

ABSTRACT

The objective of this research project was to evaluate the security of the data network of the Huacho Regional Hospital, using security tools and policies, based on best practices and international standards to achieve this end.

The type of technological research was used, with a non-experimental type design with a cross section. The research was based on the MAIGTI Framework, which established the tools for the evaluation of this study.

As expected results, vulnerabilities and threats were identified to mitigate risks in the security of the data network of the Huacho Regional Hospital.

INDICE

Palabras clave……i

Titulo……..……ii

Resumen……iii

Abstract…….iv

Índice……..…v

Introducción.....**1**

Metodología del Trabajo.....**28**

Resultados.....**30**

Análisis y Discusión **110**

Conclusiones y Recomendaciones **112**

Bibliografía.....**114**

1. Introducción

De los antecedentes encontrados se han abordado los trabajos más relevantes a esta investigación:

Ramírez (2015) realizó un estudio con el propósito de disminuir riesgos, así como limitar sus consecuencias en una dependencia universitaria, analizó los niveles de seguridad que se presentan, para luego, los administradores desarrollen políticas y mecanismos correctos para disminuir ataques de robo o daño de información relevante y/o confidencial. Aplicó la guía COBIT basada en objetivos de control de la información y tecnologías relacionadas para las buenas prácticas de seguridad y control. Como resultado se logró conservar la disponibilidad y integridad de los recursos informáticos según las necesidades y recursos financieros dispuestos para el análisis de seguridad.

Garcés **(**2015) implementó un mecanismo de seguridad informática que permite resguardar los datos que se transmiten e interactúan en la red de datos. Estableciendo recursos de red la cual no permita infringir las barreras de acceso que puedan generar pérdidas a la cooperativa y que los servicios prestados por la red se manejen de la mejor manera y se encuentre disponible por todos los usuarios. Aplicó la ISO 27001 y las recomendaciones NIST serie 800. Como resultado se obtuvo que la información se encuentre protegida y libre de intrusos, implantando políticas para la correcta utilización de los servicios de red, las cuales deben ser realizadas por los empleados de la cooperativa; también se estableció mecanismos de seguridad como un Firewall, servidor Proxy e IDS (Sistema de Detección de Intrusos) la cual que permitió que se realice la correcta administración, control y monitoreo de la red de la cooperativa.

Salazar (2016), aplicó políticas de seguridad informática como herramientas para la seguridad de la red de datos enfatizando la importancia de la información en sus trabajadores y obtengan

buenos resultados de productividad, salvaguardando correctamente los datos empresariales. Como resultado de obtuvo un informe de las amenazas en la red por elementos externos llamados hacker, así mismo orientaciones del funcionamiento de la red a fin de reducir riesgo que atenten a la integridad de la información.

Andrade (2016) evaluó el sistema de gestión de seguridad de la información para una gobernación autónoma, identificando las vulnerabilidades y oportunidades de mejora del mismo. Para la evaluación aplico la norma ISO 27001:2013, también se tomó como referencia al estándar COBIT para la elaboración del instrumento de evaluación del sistema de gestión seguridad de la información. Como resultado, esta investigación garantiza la continuidad de los servicios y permite gestionar el riesgo informático y llegar así al cumplimiento de los objetivos institucionales en beneficio del desarrollo provincial.

Bojaca (2016) implementó un sistema de gestión de seguridad de la información aplicando la Norma ISO/IEC 27001-27002 en el sector salud salvaguardando los 3 pilares de la información los cuales son disponibilidad, integridad confiabilidad de las historias clínicas. Así mismo utilizo la metodología MAGERIT que permitió identificar las causas de los daños que se generan respeto a la información financiera y administrativa al igual que la información de los pacientes. Como resultado se planteó un sistema de seguridad que mitigue riesgos y vulnerabilidades a los activos de información de la entidad hospitalaria.

Seguridad. Es importante en los negocios empresariales salvaguardar los datos, su integridad no sea susceptible a riesgos u otros elementos que atenten el normal desarrollo de sus actividades. Por tanto, nos indica que básicamente se refiere a los mecanismos con las que dispone el administrador o encargado de una red para realizar un monitorear los recursos, los

permisos de uso de estos recursos asignados a un usuario y el uso en sí que se les da a estos. (Villalón, 2002).

Red de Datos. Moro (2013), indica que la información se transfiere mediante medios de comunicación necesario para una correcta transferencia de datos bajo ciertos protocolos de red, emisores, receptores, nodos intermedios, conmutadores y enlaces. Las redes de datos permiten una comunicación rápida y eficiente.

Seguridad de la red de datos. Lo importante de los datos se caracteriza no solamente por lo útil que puede ser para una empresa, sino también crear diferentes mecanismos de seguridad de la misma que se mantenga la integridad, disponibilidad, privacidad, control y autenticidad de la información. (Bustamante, 2012).

Así mismo, el presente estudio brinda mejoras preventivas, correctivas para las redes de datos para el Hospital Regional de Huacho, que permita salvaguardar la información que generan todos los trabajadores de la institución, de igual manera prevenir ataques que puedan vulnerar la integridad de los datos que almacenan en sus sistemas informáticos.

A la vez puede servir de punto de inicio para otros investigadores que deseen investigar sobre el tema de la seguridad en las redes de datos.

La presente investigación tiene aportes científicos, porque busca conocimientos selectivos y sistematizados para explicar racionalmente los procesos de un plan de evaluación a la seguridad de la red de datos del Hospital Regional de Huacho, empleando el marco de trabajo MAIGTI. El aporte será elaborar un plan que ayudará a la evaluación de la seguridad de la red de datos, proponiendo las mejoras para la seguridad.

En estos tiempos las redes de datos se han transformado en una herramienta esencial que ayuda a los procesos de toda institución, al permitir el intercambio continuo de información. Esta situación se ha originado debido a la globalización, debido al alto desarrollo tecnológico que día a día va en creciendo, innovando y cambiando constante.

Cabe indicar que en la actualidad hay un número cuantioso de tareas y procesos automatizados de la institución, las cuales trabajan de manera primordial con las redes de datos, para así poder tener sus procesos como los sistemas contables, archivos, nómina del personal, inventarios entre otros; garantizando que los usuarios tengan a su disposición la información de forma inmediata. Además, las instituciones pueden ofrecer sus servicios e información vital para sus trabajadores, usuarios y proveedores el cual hace que tenga presencia en internet.

Toda institución anhela un entorno donde no exista fallas, vulnerabilidades, amenazas, o algún tipo accidentes que perjudicarían de manera negativa el desempeño de las redes de datos, pero en la actualidad, el entorno de toda institución está lejos de serlo.

El Hospital Regional de Huacho, posee una de red interna, permitiendo que todos los usuarios se conecten de manera simultánea a los servidores de datos con la finalidad de permitir todos los procesos de carácter administrativo y red asistencial.

En la actualidad muchas oficinas adquirieron el servicio de acceso a internet, lo cual ha ocasionado el incremento de puntos de redes a las establecidas, no siguiente la estructura primaria de la arquitectura de su red, ni la distribución de IP (Protocolo de Internet), generando así nuevos puntos vulnerables. También se evidencio que el cableado del área de informática se encuentra desordenado, a pesar de contar con dispositivos de red como switch, con el riesgo que el personal cometa algún error al momento del mantenimiento y se podría ocasionar interrupciones en el servicio para los usuarios de las redes de cómputo.

El Hospital Regional de Huacho contaba con servidor web y servidor de correo la cual eran muy vulnerables a ataques de software malicioso como por ejemplo el Ransomware, el cual encriptaba los archivos y para poder recuperar tu información exigía dinero, por tal motivo el hospital opto por contratar un Hosting.

Al estar los equipos conectados entre sí y con acceso a internet han recibido ataques informáticos, permitiendo que en algunos casos pueda introducirse a los equipos y colocando programas maliciosos, que permiten saltar hacia otros equipos de la red para causar daño, borrando información de mucho valor para la institución, uno de los factores que provoca tal vulnerabilidad es la falta de licencia del antivirus que poseen.

También se ha encontrado problemas con los permisos que poseen los usuarios en cuanto al acceso de internet, ya que en muchos casos algunos usuarios posen permisos totales en cuanto al acceso a correos y él envió y recepción información de manera externa, también se pudo observar que algunos usuarios poseen acceso a páginas, YouTube, buscadores, entre otros, pero no son conscientes del riesgo que esto conlleva a la institución, en el caso de ser mal utilizadas. Por tal razón se han implementado medidas como por ejemplo de firewall interno, también se han implementado un sistema proxy, la cual que actúa como intermediario entre el cliente y el servidor de aplicación.

Con los sucesos ya antes descritos se ha evidenciado que existe un problema de seguridad en el Hospital Regional de Huacho, que abarca ataques externos a los servicios y sistemas de información, así como de ataques internos, voluntarios o involuntarios, realizados por el personal de la institución, propagación de correos no autorizados, correos spam, virus, ingreso a páginas no autorizadas y ataques mediante el uso dispositivos no autorizados, entre otros.

La arquitectura de red es otro de los problemas que padece el Hospital Regional de Huacho, ya que no va a acorde con las necesidades de la institución provocando que la distribución de sus puntos no sea la más óptima y generando congestionamiento del tráfico de red

De seguir con los problemas mencionados en cuanto a la seguridad en la red informática pondrían en una situación vulnerable a toda la información que se encuentra almacenadas en los servidores de datos, información de los trabajadores, base de datos de todos los pacientes; con la posibilidad de ser eliminada, modificada o alterada.

Ante tal situación, las autoras nos planteamos la siguiente interrogante:

¿Cómo evaluar la seguridad de la red de datos del Hospital Regional de Huacho para detectar las vulnerabilidades y amenazas garantizando la operatividad de los servicios informáticos?

Asimismo, para dar soporte teórico a la solución de la problemática planteada, se han seleccionado las definiciones y conceptualizaciones siguientes:

1.1 Maigti

Alfaro Paredes (2008), nos indica que MAIGTI es una metodología la cual puede ser utilizada para realizar una auditoría o evaluación integral de la gestión de las tecnologías de la información, cuyo objetivo principal es evaluar la gestión de la tecnología de información en una institución, organización o lugar donde se requiera ser aplica, con el propósito de identificar la posible causa de pérdida de valor debido a fallas en los diversos procesos relacionados, se teniendo como base los estándares internacionales. COBIT, ISO/IEC 12207, ISO/IEC 17799, ISO/IEC 20000, ISO 27001 y PMBOK. (Alfaro Paredes, 2008)

Métodos de evaluación de MAIGTI. Señalaremos los métodos que forman parte de la metodología: (Alfaro Paredes, 2008)

- Método de evaluación de la planificación estratégica. (Se refiere al P002 de MAIGTI) (Alfaro Paredes, 2008)
- Método de evaluación de los planes operativos. (Se refiere al P003 de MAIGTI) (Alfaro Paredes, 2008)
- Método de evaluación de riesgos. (Se refiere al P004 de MAIGTI) (Alfaro Paredes, 2008)
- Método de evaluación para la planificación Estratégica de Tecnologías de Información. (Se refiere al P005 de MAIGTI) (Alfaro Paredes, 2008)
- Método de evaluación de planes de desarrollo de Sistemas de información. (Se refiere al P006 de MAIGTI) (Alfaro Paredes, 2008)
- Método de evaluación de los planes de proyecto de compra de sistemas de Información. (Se refiere al P007 de MAIGTI) (Alfaro Paredes, 2008)
- Método de evaluación del plan de contingencias de informática. (Se refiere al P008 de MAIGTI) (Alfaro Paredes, 2008)
- Método de evaluación para el Plan de continuidad de negocio. (Se refiere al P009 de MAIGTI) (Alfaro Paredes, 2008)
- Método de evaluación para el plan de seguridad de la información. (Se refiere al P010 de MAIGTI) (Alfaro Paredes, 2008)
- Método de evaluación para el plan de licenciamiento de software. (Se refiere al P011 de MAIGTI) (Alfaro Paredes, 2008)
- Método de evaluación para el plan de capacitación. (Se refiere al P012 de MAIGTI) (Alfaro Paredes, 2008)

- Método de evaluación para el plan de mantenimiento preventivo de hardware de computadoras, redes y equipos relacionados. (Se refiere al P013 de MAIGTI) (Alfaro Paredes, 2008)
- Método de evaluación para el plan de mantenimiento correctivo de hardware de computadoras, redes y equipos relacionados s. (Se refiere al P014 de MAIGTI) (Alfaro Paredes, 2008)
- Método de evaluación para la planificación de labores de rutina relacionadas con las tecnologías de información. (Se refiere al P015 de MAIGTI) (Alfaro Paredes, 2008)
- Método de evaluación del plan de calidad. (Se refiere al P016 de MAIGTI) (Alfaro Paredes, 2008)
- Método de evaluación para el plan de compras de tecnologías de información. (Se refiere al P017 de MAIGTI) (Alfaro Paredes, 2008)
- Método de evaluación para el reglamento de organización y funciones. (Se refiere al P018 de MAIGTI) (Alfaro Paredes, 2008)
- Método de evaluación para el manual de organización y funciones. (Se refiere al P019 de MAIGTI) (Alfaro Paredes, 2008)
- Método de evaluación para el currículum vitae del personal de tecnología de información. (Se refiere al P020 de MAIGTI) (Alfaro Paredes, 2008)
- Método de evaluación del inventario de hardware de tecnología de información. (Se refiere al P021 de MAIGTI) (Alfaro Paredes, 2008)
- Método de evaluación para el inventario de software de base. (Se refiere al P022 de MAIGTI) (Alfaro Paredes, 2008)

- Método de evaluación para el inventario de sistemas de información. (Se refiere al P023 de MAIGTI) (Alfaro Paredes, 2008)
- Método de evaluación para las solicitudes y evaluaciones de cotizaciones para las compras de hardware de computadoras, redes y equipos relacionados. (Se refiere al P024 de MAIGTI) (Alfaro Paredes, 2008)
- Método de evaluación para las solicitudes y evaluaciones de cotizaciones para las compras de software de base. (Se refiere al P025 de MAIGTI) (Alfaro Paredes, 2008)
- Método de evaluación para las solicitudes y evaluaciones de cotizaciones para las compras de sistemas de información. (Se refiere al P026 de MAIGTI) (Alfaro Paredes, 2008)
- Método de evaluación para los contratos de compra de bienes y servicios, de hardware de computadoras, redes y equipos relacionados. (Se refiere al P027 de MAIGTI) (Alfaro Paredes, 2008)
- Método de evaluación para los contratos para la compra de software de base. (Se refiere al P028 de MAIGTI) (Alfaro Paredes, 2008)
- Método de evaluación para los contratos para la compra de sistemas de información. (Se refiere al P029 de MAIGTI) (Alfaro Paredes, 2008)
- Método de evaluación para los contratos de seguros para las tecnologías de información. (Se refiere al P030 de MAIGTI) (Alfaro Paredes, 2008)
- Método de evaluación para la metodología de desarrollo de sistemas de información. (Se refiere al P031 de MAIGTI) (Alfaro Paredes, 2008)
- Método de evaluación para la metodología para la atención de requerimientos de soporte técnico. (Se refiere al P032 de MAIGTI) (Alfaro Paredes, 2008)

- Método de evaluación para la metodología para la atención de requerimientos de desarrollo de sistemas de información. (Se refiere al P033 de MAIGTI) (Alfaro Paredes, 2008)
- Método de evaluación para la documentación de los manuales técnicos de los sistemas de información. (Se refiere al P034 de MAIGTI) (Alfaro Paredes, 2008)
- Método de evaluación para la documentación de los manuales de usuario de los sistemas de información. (Se refiere al P035 de MAIGTI) (Alfaro Paredes, 2008)
- Método de evaluación para la arquitectura de la red de tecnologías de información. (Se refiere al P036 de MAIGTI) (Alfaro Paredes, 2008)
- Método de evaluación para la seguridad de acceso a los sistemas de información. (Se refiere al P037 de MAIGTI) (Alfaro Paredes, 2008)
- Método de evaluación para la seguridad de acceso a las carpetas en los servidores. (Se refiere al P038 de MAIGTI) (Alfaro Paredes, 2008)
- Método de evaluación para los manuales de procedimientos de soporte técnico. (Se refiere al P039 de MAIGTI) (Alfaro Paredes, 2008)
- Método de evaluación para los manuales de procedimientos de desarrollo de sistemas de información. (Se refiere al P040 de MAIGTI) (Alfaro Paredes, 2008)
- Método de evaluación para la revisión de los formularios de control de entregables de proyectos y requerimientos de desarrollo de sistemas de información. (Se refiere al P041 de MAIGTI) (Alfaro Paredes, 2008)
- Método de evaluación para el seguimiento de informes de auditoría interna. (Se refiere al P042 de MAIGTI) (Alfaro Paredes, 2008)

- Método de evaluación para el seguimiento de informes de auditoría externa. (Se refiere al P043 de MAIGTI) (Alfaro Paredes, 2008)
- Método de evaluación para de las certificaciones de calidad de tecnología de información. (Se refiere al P044 de MAIGTI) (Alfaro Paredes, 2008)
- Método de evaluación para la evaluación de desempeño del área de tecnología de información. (Se refiere al P045 de MAIGTI) (Alfaro Paredes, 2008)
- Método de evaluación para el Desempeño del Personal de Tecnología de Información. (Se refiere al P046 de MAIGTI) (Alfaro Paredes, 2008)
- Método de evaluación para la revisión de los formularios de control de cambios en proyectos de compra o desarrollo de sistemas de información. (Se refiere al P047 de MAIGTI) (Alfaro Paredes, 2008)
- Método de evaluación para la revisión de los formularios de control de riesgos en proyectos de compra o desarrollo de sistemas de información. (Se refiere al P048 de MAIGTI) (Alfaro Paredes, 2008)
- Método de evaluación para la revisión de los formularios de seguimiento de avances en proyectos de compra o desarrollo de sistemas de información. (Se refiere al P049 de MAIGTI) (Alfaro Paredes, 2008)
- Método de evaluación para el control de calidad de los requerimientos de compra o desarrollo de sistemas de información. (Se refiere al P050 de MAIGTI) (Alfaro Paredes, 2008)
- Método de evaluación para el control de calidad de los requerimientos de soporte técnico. (Se refiere al P051 de MAIGTI) (Alfaro Paredes, 2008)

- Método de evaluación para entrevistar a los usuarios de tecnologías de información. (Se refiere al P052 de MAIGTI) (Alfaro Paredes, 2008)
- Método de evaluación para las instalaciones eléctricas de los equipos de cómputo y redes. (Se refiere al P053 de MAIGTI) (Alfaro Paredes, 2008)
- Método de evaluación para la seguridad de acceso al centro de cómputo principal. (Se refiere al P054 de MAIGTI) (Alfaro Paredes, 2008)
- Método de evaluación para las instalaciones del centro de cómputo principal. (Se refiere al P055 de MAIGTI) (Alfaro Paredes, 2008)
- Método de evaluación para la seguridad de acceso al centro de cómputo alterno (Se refiere al P056 de MAIGTI) (Alfaro Paredes, 2008)
- Método de evaluación para las instalaciones del centro de cómputo alterno. (Se refiere al P057 de MAIGTI) (Alfaro Paredes, 2008)
- Método de evaluación para el cableado de redes de datos. (Se refiere al P058 de MAIGTI) (Alfaro Paredes, 2008)
- Método de evaluación para el cálculo de la generación de valor de los proyectos. (Se refiere al P059 de MAIGTI) (Alfaro Paredes, 2008)
- Método de evaluación para la elaboración del informe preliminar. (Se refiere al P060de MAIGTI) (Alfaro Paredes, 2008)
- Método de evaluación para envío, sustentación y corrección del informe final. (Se refiere al P061 de MAIGTI) (Alfaro Paredes, 2008)
- Método de evaluación para la elaboración del plan de trabajo de la auditoría. (Se refiere al P062 de MAIGTI) (Alfaro Paredes, 2008)

- Método de evaluación para la medición de la resistencia de la puesta a tierra. (Se refiere al P063 de MAIGTI) (Alfaro Paredes, 2008)

Alcance

La metodología tiene como alcance los siguientes puntos:

A. Evaluación de la "planificación y organización", comprende lo siguiente:

- Se tiene que realizar la revisión de los diversos planes:
  - ✓ Plan estratégico de tecnología de información (PETI), es una herramienta reconocida para establecer políticas, uso y administración de los recursos Tecnológicos. Las estrategias del PETI continuamente sufren adaptación innovación y cambio de acuerdo a las necesidades de la institución. (Alfaro Paredes, 2008)
  - ✓ Plan de contingencias de informática, es el instrumento de gestión el cual permite mantener la contingencia operativa frente a un evento crítico de la institución y así poder disminuir el impacto negativo sobre los clientes, usuarios y la misma institución. (Alfaro Paredes, 2008)
  - ✓ Plan de continuidad de negocio, es un plan de emergencia ante como la institución debe restaurar y recuperar su funcionalidad de una manera aceptable y dentro de un tiempo estimado, ante cualquier interrupción parcial o total que ocurra o algún desastre. (Alfaro Paredes, 2008)
  - ✓ Plan de capacitación, es un proceso donde se podrá detectar y analizar las necesidades de la institución, para la cual se tiene que diseñar y ejecutar el plan de capacitación más adecuado para el personal y de ser necesario implementar acciones de mejora. (Alfaro Paredes, 2008)

- ✓ Plan de licenciamiento de software, su objetivo principal es garantizar que los programas de software que se utilicen en la institución cumplan con las disposiciones de legalidad de licencias correspondientes. (Alfaro Paredes, 2008)
- ✓ Plan de mantenimiento preventivo, consiste en realizar labores de verificación, limpieza, entre otras actividades, permitiendo alargar la vida útil orientado al equipo de cómputo, servidores de red, estaciones de trabajo, impresoras, y equipos de comunicaciones. De igual manera disminuir el deterioro y aumentando el rendimiento de los equipos. (Alfaro Paredes, 2008)
- ✓ Planes de proyectos, es un grupo de acciones estimadas para alcanzar un objetivo establecido. Por tal razón se debe, debe desarrollarse de una estrategia alineada con la institución. (Alfaro Paredes, 2008)
- ✓ Plan de seguridad, lo primero que se debe identificar son los activos de la institución los cuales incluyen el personal, software, hardware, sistemas, luego se tiene que evaluar los posibles riesgos a los están expuestos como por ejemplo los virus informáticos, hackers, daños físicos o errores del personal. Una vez de haber evaluado la probabilidad de que cada amenaza suceda, podemos decidir que amenaza es más importante para así empezar a protegerla. (Alfaro Paredes, 2008)
- ✓ Plan de calidad, en este documento se detallada los procesos, procedimientos y recursos que deben aplicarse, también indica el personal que debe aplicarlos y cuál es el momento para poder cumplir con los requisitos y la realización de un proyecto. (Alfaro Paredes, 2008)

- La organización del trabajo: este punto comprende lo siguiente:

- ✓ La estructura organizacional, es la manera en como un empresa e institución se organizan internamente y administrativa, basándose en sus objetivos trazados, utilizando sus recursos disponibles y aplicando metodologías de trabajo como procedimientos, entre otros. (Alfaro Paredes, 2008)

B. La evaluación de la "adquisición e implementación". Comprende lo siguiente:

- Dentro de las adquisiciones de tecnologías de información, se encuentra la compra de equipos de cómputo y red, licencias de software, sistemas de información, entre otros. Para el correcto proceso se debe revisar tanto las propuestas de alternativas como los contratos y anexos a los contratos. (Alfaro Paredes, 2008)
- En cuanto el desarrollo de tecnologías de información encontraremos el desarrollo de sistemas de información, y tecnologías de información de base, el cual se debe revisar la ejecución de la metodología y la documentación respectiva en cada caso. (Alfaro Paredes, 2008)

C. La evaluación de la "entrega de servicios y soporte". Comprende lo siguiente:

- La entrega de servicios de desarrollo e implantación de sistemas de información, en este punto se debe revisar la evaluación de todas las posibles soluciones, también debemos revisar detalladamente lo desarrollado, comprado e implantado, a la vez se deben verificar las medidas de seguridad y el nivel de satisfacción de los usuarios con respecto al servicio brindado. Otro punto importante es la entrega de servicios de soporte técnico e infraestructura de tecnologías de información, software base y hardware, así como servicios relacionados. (Alfaro Paredes, 2008)

D. Evaluación del “monitoreo y control”. Comprende lo siguiente:

- En el seguimiento de los planes debemos validar las diferentes acciones que son desarrolladas durante un tiempo establecido y de esta manera comprobar si los objetivos o metas trazadas en cada una de sus faces han sido cumplidas o se están cumpliendo. (Alfaro Paredes, 2008)
- La evaluación interna del desempeño es una herramienta que permite verificar si el personal está logrando los objetivos individuales en la institución. Con esta evaluación se puede medir el rendimiento, conducta, y la obtención de resultados manera integral y objetiva. (Alfaro Paredes, 2008)
- Las certificaciones o acreditaciones independientes de control y seguridad también serán tomadas para realizar una evaluación de monitoreo y control, a la vez la provisión de auditoría independiente. (Alfaro Paredes, 2008)

Cuando ya se ha establecido el alcance, lo cual significa que habremos evaluado lo que incluirá y lo cual no estará incluido, procederemos con la elaboración del plan de trabajo de la auditoría.

Entradas

Alfaro Paredes (2008), indica que las entradas de información están comprendidas por los documentos solicitados para el inicio de la evaluación, por lo que el personal encargado de la evaluación o auditoria debe requerir los documentos vigentes en el período en evaluación, el período anterior.

Procesos

A continuación, la siguiente figura sintetiza el método MAIGTI, en el cual muestra sus subprocesos con los métodos asociados:

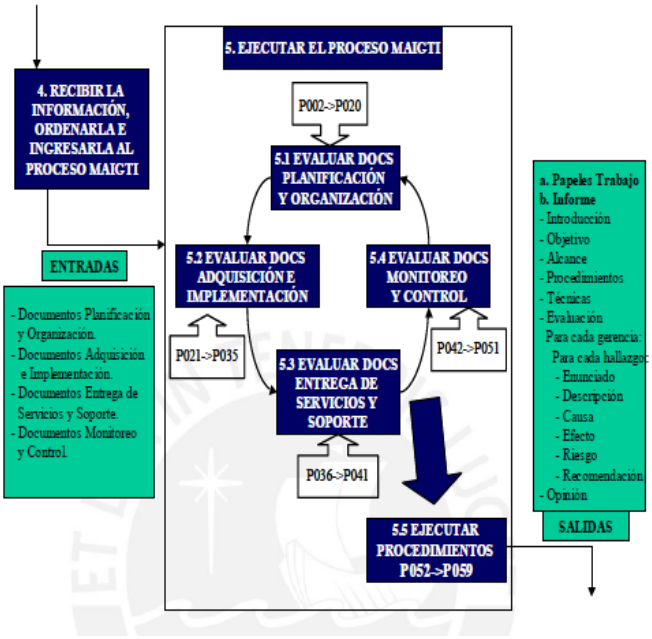


Figura N° 01. Proceso MAIGTI

Fuente. (Alfaro Paredes, 2008)

Los procesos que comprende MAIGTI son:

A. La información requerida debe estar documentada, para cumplir con esta tarea el área de auditoria o el equipo de auditoría asignado debe realizar sus solicitudes o requerimientos, la cual debe de realizar la revisión de documentos, por lo tanto, debe efectuarse por lo menos con 15 días de anticipación a la fecha proyectada. (Alfaro Paredes, 2008)
B. Se debe realizar la evaluación de la información recibida, los cuales deberán ser verificados por caso individual de acuerdo al siguiente orden: (Alfaro Paredes, 2008)
    - Examinar los documentos del período anterior con los del presente periodo.

- Examinar los documentos del actual periodo evaluado.
- Examinar los documentos que serán adaptados para el siguiente periodo en evaluación.

A continuación, se tiene que tomar el siguiente aspecto al verificar los documentos:

- Examinar los documentos de planificación y organización. Esto involucra que se debe de efectuar los procedimientos P002 al P020.
- Examinar los documentos de adquisición e implementación. Esto involucra que se debe de efectuar los procedimientos P021 al P035.
- Examinar los documentos de entrega de servicios y soporte". Esto involucra que se debe de efectuar los procedimientos P036 al P041.
- Examinar los documentos de monitoreo y control. Esto involucra que se debe de efectuar los procedimientos P042 al P051.

C. Se debe realizar una entrevista de manera personal y directa a todo el personal de las diferentes áreas de la institución, abarcando a todos directivos y personal administrativo. (Alfaro Paredes, 2008)
D. Realizar una entrevista y ejecutar la verificación de manera presencial con el personal o área encargada de gestión de tecnologías de información. (Alfaro Paredes, 2008)
E. Adquirir los datos del personal que trabaja en la gestión del desarrollo de sistemas de información tales correos, teléfonos, anexos y cargos. (Alfaro Paredes, 2008)
F. Realizar una entrevista al personal que dirige los proyectos, de igual manera los que desarrollan sistemas de información. Alfaro Paredes, 2008)
G. Realizar, revisar y corregir el informe preliminar, para la emisión del informe final. (Alfaro Paredes, 2008)

H. Expedir, sustentar y modificar el informe final. (Alfaro Paredes, 2008)

Salidas

A continuación, MAIGTI presenta sus salidas:

A. Archivos de trabajo.

B. El Informe final debe comprender la siguiente estructura:

- Introducción del informe.
- Objetivo del informe.
- Alcance del informe.
- Procedimientos y técnicas de la evaluación o auditoria.
- Evaluación, en este punto para cada hallazgo encontrado se debe realizar la descripción, la causa, efecto, riesgo y la recomendación para su solución.

Durante la aplicación de la metodología se obtendrá posibles hallazgos en gran cantidad. En el cual se detectará la carencia de documentación en planes, metodologías de desarrollo, información sobre datos de los proyectos, manuales de procedimientos, técnicos y manuales de usuario de los sistemas de información. (Alfaro Paredes, 2008)

Por lo general se observa que el usuario no se encuentra satisfecho con los servicios de soporte técnico y desarrollo de sistemas. La insatisfacción se debe primordialmente a la rapidez y efectividad de atención a requerimientos que por ende nunca fueron revisados. (Alfaro Paredes, 2008)

ISO/IEC 17799

Alfaro Paredes (2008), nos indica que la ISO/IEC 17799, es una norma técnica peruana, que al ser puesta en práctica o ejecutada nos brinda una progresión de objetivos de control, ayudando a implementar medidas de seguridad en las instituciones, organizaciones, la cual ayudara al mejorando del rendimiento.

Cobit

Es un marco de referencia, el cual integra todas las normas y estándares utilizando un conjunto de herramientas de soporte que ayudan a las organizaciones a tomar las decisiones apropiadas con respecto a los requerimientos de control, temas técnicos y riesgos de negocio, la cual ayudara a entender y administrar los riesgos y beneficios asociados con las tecnologías de información a las organizaciones, cabe indicar que COBIT a través del tiempo se actualiza y concuerda con otras normas (IT Governance Institute 2007).

Contiene 34 procesos de alta importancia clasificados en cuatro dominios: Planear y Organizar, Adquirir e Implementar, Entregar y Dar Soporte, y, Monitorear y Evaluar, tal y como se muestra en la siguiente Figura. (IT Governance Institute 2007)

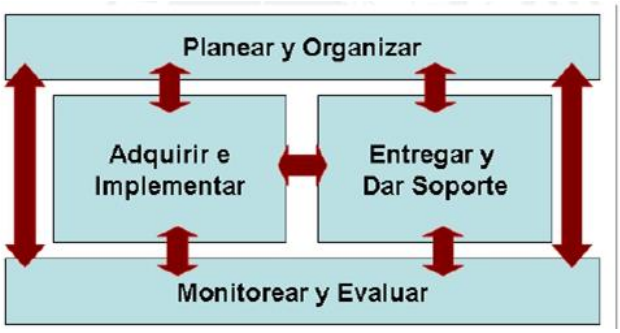


Figura N° 02: "Dominios de Cobit"

Fuente. (Alfaro Paredes, 2008)

El marco referencial de COBIT está constituido con 4 dominios, 34 procesos de TI, 210 objetivos de control y 40 guías de auditoría. Los 4 dominios de COBIT son: (IT Governance Institute 2007)

- **Planear y organizar**: Este dominio se enfoca en la manera de como direccionar a las tecnologías de información para cumplir los objetivos del negocio. Su objetivo es apoyar a que una organización tenga una adecuada infraestructura tecnológica apropiada. (IT Governance Institute 2007)

  Este dominio está constituido por los siguientes objetivos:

  - ✓ PO1 Definir un plan estratégico de tecnología de información.
  - ✓ PO2 Definir la arquitectura de Información.
  - ✓ PO3 Determinar la dirección tecnológica.
  - ✓ PO4 Definir la organización y de las relaciones de TI.
  - ✓ PO5 Manejar la inversión en Tecnología de Información.
  - ✓ PO6 Comunicar la dirección y aspiraciones de la gerencia.
  - ✓ PO7 Administrar recursos humanos.
  - ✓ PO8 Asegurar el cumplimiento de requerimientos externos.
  - ✓ PO9 Evaluar riesgos.
  - ✓ PO10 Administrar proyectos.
  - ✓ PO11 Administrar calidad.

- **Adquirir e implementar:** Todas las alternativas de solución deben ser identificadas, desarrolladas o adquiridas, de tal manera deben de ser aplicadas al proceso de negocio, esto servirá para elaborar una eficaz estrategia de TI. (IT Governance Institute 2007)

Este dominio cubre los cambios y el mantenimiento realizado a sistemas existentes.

A continuación, se presenta los objetivos de alto nivel:

- ✓ AI1 Identificar soluciones.
- ✓ AI2 Adquirir y mantener software de aplicación.
- ✓ AI3 Adquirir y mantener arquitectura de tecnología.
- ✓ AI4 Desarrollar y mantener procedimientos relacionados con TI.
- ✓ AI5 Instalar y acreditar sistemas.
- ✓ AI6 Administrar cambios.

- **Entregar y dar soporte:** Este dominio hace referencia a la entrega de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento procesamiento de los datos por sistemas de aplicación, clasificados frecuentemente como controles de aplicación. (IT Governance Institute 2007)

Este dominio considera los siguientes objetivos de alto nivel o procesos:

- ✓ DS1 Definir niveles de servicio.
- ✓ DS2 Administrar servicios prestados por terceros.
- ✓ DS3 Administrar desempeño y capacidad.
- ✓ DS4 Asegurar servicio continuo.
- ✓ DS5 Garantizar la seguridad de sistemas.
- ✓ DS6 Identificar y asignar costos.

- ✓ DS7 Educar y entrenar a los usuarios.
- ✓ DS8 Apoyar y asistir a los clientes de TI.
- ✓ DS9 Administrar la configuración.
- ✓ DS10 Administrar problemas e incidentes.
- ✓ DS11 Administrar datos.
- ✓ DS12 Administrar instalaciones.
- ✓ DS13 Administrar operaciones.

- **Monitorear y evaluar:** El presente dominio nos dice que los procesos tienen que ser previamente verificado a través del tiempo con el objetivo de revisar su calidad y suficiencia orientada a los requerimientos de control. (IT Governance Institute 2007)

  A continuación, se presenta los objetivos de alto nivel:

  - ✓ M1 Monitorear los procesos.
  - ✓ M2 Evaluar lo adecuado del control Interno.
  - ✓ M3 Obtener aseguramiento independiente.
  - ✓ M4 Proporcionar auditoría independiente.

Seguridad de la información

El 80% de los datos importantes de las organizaciones están almacenados en aplicaciones electrónicas, por tal motivo se tienen que tomar acciones que permitan reducir la perdida y alteración de información, provocando que dichos datos no se encuentren disponibles cuando se requiera. Estas posibles situaciones de amenazas pueden hacer colapsar en cualquier organización, por tal motivo es necesario plantear una buena estrategia de continuidad de

negocio que ayude a eliminar toda posibilidad de riesgo o por lo menos neutralizar cualquier tipo de ataque. (Alexander, 2007)

Sistemas De Información

Elementos interrelacionados que recaban, procesan, almacenan y distribuyen información, con el propósito de apoyar en la toma de decisiones y proporcionar todo tipo de control a las organizaciones. Además, los sistemas de información son de gran apoyo para el personal de alto rango como gerentes y también ayuda a trabajadores a que examinen problemas, tengan una visión de cómo tratar asuntos complejos y elaboren productos nuevos, comprendiendo por información los datos, la secuencia de hechos y eventos que suceden dentro de las organizaciones las cuales representan gran valor, y que se han adaptado de manera útil para los seres humanos. (Laudon, 2008)

Redes

Las redes de datos es una tecnología indispensable en las comunicaciones para la ejecución de los procesos de cualquier tipo de organización, por lo tanto, posibilitan a sus miembros contribuir entre sí, además de compartir todos los recursos informáticos disponibles dentro de una organización, lo cual implica compartir todo tipo de archivo en línea, la utilización de aplicaciones y todo tipo de servicios, entre otros. (Jimeno, 2008)

- **Tipo de redes**

Se divide en redes (privadas) esto quiere decir que se encuentran dentro de una misma organización, podemos clasificarlas por su capacidad, su rapidez de intercambiar datos y su alcance, la red se divide en tres categorías:

Redes LAN

Llamada Red de área local, conformada por un conjunto de equipos los cuales se encuentran ubicados en una misma organización, mediante una pequeña red dentro de un área geográfica. Comúnmente todos están conectadas con una misma tecnología (la más común es Ethernet). (Forouzan, 2002)

Redes MAN

Significa Red de área metropolitana, conecta diferentes LAN las que son más cercanas dentro de un área geográfica (su alcance está permitido dentro de cincuenta kilómetros) entre sí a una alta velocidad. De tal manera, que esta red permite que dos puntos remotos tengan una comunicación como si pertenecieran a misma red de área local.

Una MAN está constituida por conmutadores o routers conectados entre sí mediante cables de fibra óptica de alta velocidad. (Forouzan, 2002).

Redes WAN

Significa Red de área extensa que conecta múltiples LAN entre sí las cuales se encuentran geográficamente a grandes distancias. Las redes WAN tienen una velocidad disponible que puede variar según el costo de las conexiones (que aumenta con la distancia) y puede afectar brindando una señal muy baja.

Estas redes funcionan con routers, a través de estos se elige la ruta más adecuada para que la información llegue de manera segura a un nodo de la red. La WAN más conocida es Internet. (Olifer, 2009)

Conceptualización y Operacionalización De Variables

Tabla 1

Definición de Variables

Definición conceptual	Definición operacional
Seguridad de datos: el objetivo primordial es salvaguardar la integridad, disponibilidad, privacidad y a la vez su control y autenticidad de la información manejada a través de un equipo de cómputo, por medio de utilizar procedimientos basados en una política de seguridad y obtener los resultados adecuados para la organización. (Bustamante, 2012)	Nivel de satisfacción con respecto a la conectividad e instalaciones físicas de la actual red de datos

Nota: Realizado por las autoras

Por otro lado, la hipótesis planteada por las autoras es la siguiente:

La evaluacion de la seguridad de la red de datos del Hospital Regional de Huacho mediante la MAIGTI, permitirá el reconocimiento de vulnerabilidades y amenazas.

Asimismo, el objetivo principal trazado y que se buscó cumplir a cabalidad fue, evaluar la seguridad de la red de datos del Hospital Regional de Huacho para identificar las vulnerabilidades y amenazas; mientras que los objetivos específicos fueron:

- Planificar el proceso de evaluación de la seguridad de la red datos del Hospital Regional de Huacho.
- Desarrollar el proceso de evaluación de la seguridad de la red de datos empleando la metodología MAIGTI.
- Proponer las mejoras para la seguridad de la red de datos del hospital de Huacho.

2. Metodología del trabajo

El proceso realizado para la formulación de la presente propuesta tuvo un componente investigativo de tipo tecnológico, tomando en cuenta que se tuvo que realizar la recolección de información que tenga que ver con el tema de evaluar la seguridad de la red de datos del Hospital Regional de Huacho.

Además, el nivel de investigación: tiene un propósito de innovación incremental, porque se evaluó la seguridad de la red de datos del Hospital Regional de Huacho a un proceso ya existente y lo que se buscó fue, identificar las vulnerabilidades y amenazas existentes en la institución. Respecto al alcance temporal se trató de una investigación sincrónica porque se efectuó el estudio en un periodo a corto plazo. La investigación, respecto al tiempo del dato, es un estudio circunspectivo que analiza los factores que se presentan en Evaluación de Seguridad de la Red de Datos; y podríamos indicar que también es un estudio circunspectivo – prospectivo, ya que se utilizaron las opiniones de expertos y profesionales involucrados en la evaluación de Seguridad de la Red de Datos y sobre infraestructura tecnológica donde se ejecutó la solución.

Debido a que la investigación fue de tipo tecnológica, la población para la evaluación de Seguridad de la Red de Datos estuvo conformada por los trabajadores del área de informática y Trabajadores, cuya población del 100 % fue de dos personas, las cuales, a su vez, representaron la muestra tomada en forma de muestreo intencional por tratarse de solamente dos personas.

Las técnicas e instrumentos de recolección de datos que se emplearon para el presente proyecto de investigación fueron:

Tabla 2

Técnicas e instrumentos de recolección de datos

Técnicas	**Instrumentos**
Entrevistas	Guía de entrevista a personal especializado
Encuestas	Cuestionarios
Análisis documental	Textos, tesis, revistas y estudios previos

Nota: Realizado por las autoras

Con el fin de obtener mayor información y reforzar el tema de investigación, se realizaron preguntas abiertas y cerradas las cuales nos que brindaron información certera y directa en cuanto a los objetivos específicos planteados. Cabe indicar que se empleó la metodología MAIGTI para el desarrollo de la evaluación de Seguridad de la Red de Datos del Hospital Regional de Huacho.

3. Resultados

A continuación, pasamos a describir los resultados obtenidos luego de aplicar la metodología planteada:

Descripción de la institución

3.1. Reseña

El Hospital Regional de Huacho fue fundado el 02 de Octubre de 1970 como un Centro de Salud con servicio de hospitalización con 4 especialidades Básicas. En su desarrollo, en 1998 se transforma en un Hospital de Referencia, Centro de una red de Hospitales locales y establecimientos de Salud del Norte Chico, con influencia directa de las provincias del Sur del Departamento de Ancash, de la Sierra, de la Costa. Luego se convirtió en Hospital de Apoyo, a partir de 1990 fue considerado Hospital Regional, en la actualidad ha sido categorizado como Hospital II-2. Su estructura es horizontal, cuenta con 4 pisos, la primera planta está diseñada para los servicios de consulta externa, estrategias sanitarias, y unidades administrativas, en el segundo piso se encuentran los servicios de Pediatría y Medicina, en el tercero el servicio de Ginecobstetricia, centro obstétrico y Neonatología con su servicio de Cuidados Intensivos, y en el cuarto nivel el servicio de Cirugía, Centro Quirúrgico, y Central de Esterilización.

Desde el año 2000 se cuenta con módulos de emergencia, unidad de cuidado intensivos de adultos, y atención materna infantil. La estructura organizativa identifica 9 unidades, 14 departamentos, y la Oficina de control interno.

3.2. Visión

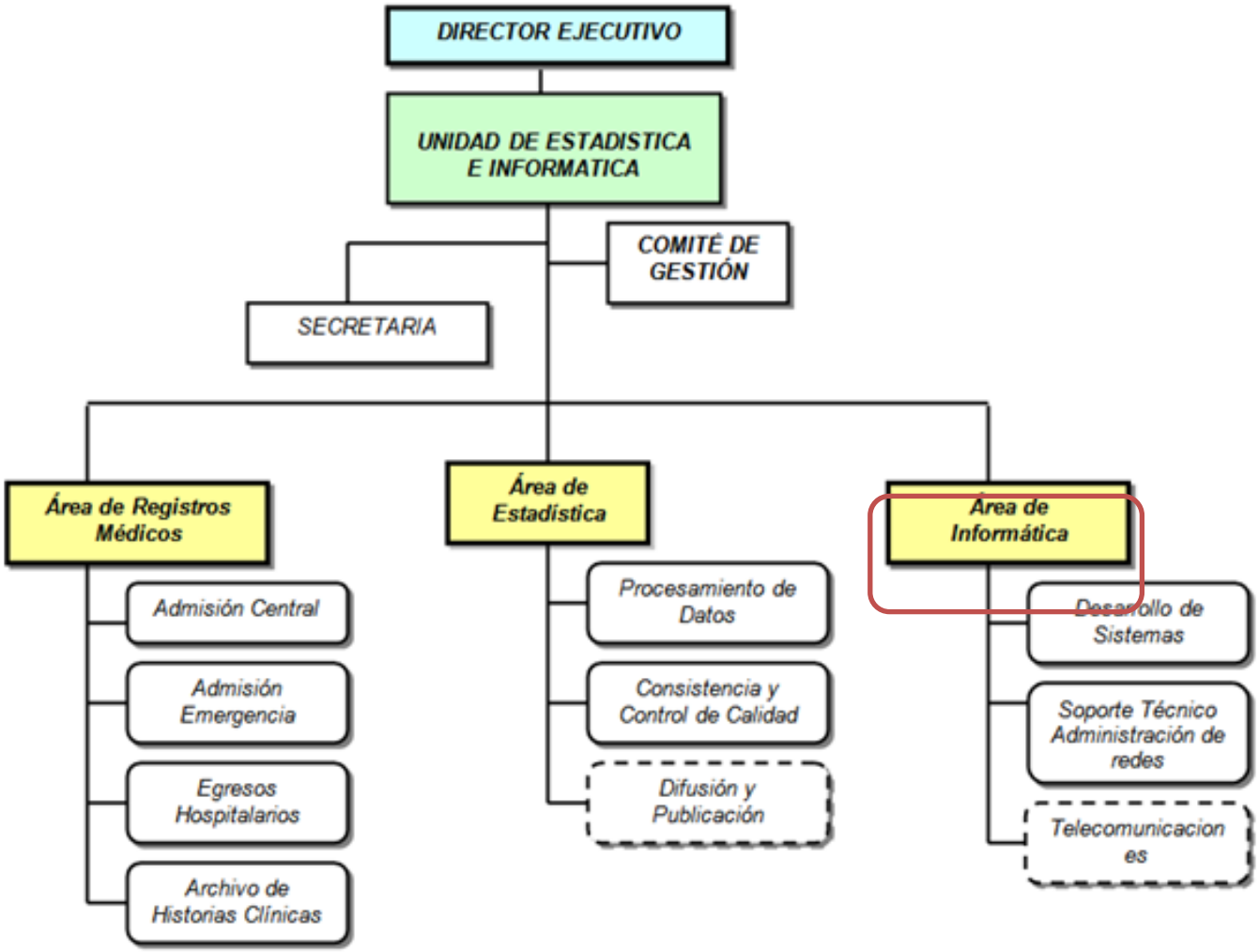
Red de salud acreditada, calificada y potenciada para asumir el nivel III-1; líder de modernidad y eficiencia en la atención de salud reconocida a nivel local y regional; con recursos humanos

capacitados según perfil epidemiológico y establecimientos de salud que cumplen con las políticas de salud y garantizan mayor accesibilidad a la población de menores recursos.

3.3. Misión

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

3.4. Organigrama



3.5. Proceso/ área a evaluar

El área a evaluar es la unidad Informática y Estadística y sub área de informática, y los procesos son los siguientes:

- Desarrollo de sistemas
- Soporte técnico y administración de redes
- Telecomunicaciones

3.6. Responsable de área

Responsable del Área Ingeniero, Jorge Sánchez.

3.7. Análisis FODA

3.7.1. Fortalezas

- El Hospital Regional cuenta con sistemas de información que permiten llevar a cabo sus procesos internos, favoreciendo la atención de los pacientes y la gestión interna.
- El Hospital Regional realiza el mantenimiento preventivo y el correctivo de equipos informáticos, garantizando la operatividad y funcionalidad de todas las áreas, lo cual se encuentra programado durante todo el año.
- El Hospital Regional cuenta con conexión simultánea entre todos sus ambientes (red de datos), esto implica los ambientes que se encuentran dentro y ambientes que se encuentran en los exteriores.
- Cuenta con un correo institucional, para la comunicación dentro y fuera del hospital.
- Todo el personal del área de estadística e informática conoce sus funciones y tiene experiencia.

3.7.2. Debilidades

- Se ha detectado la falta de un plan de capacitación en temas de especialización en tecnologías de información para promover las mejoras en el área.
- La infraestructura física del área de informática, donde se alojan los servidores, y equipos de cómputo es limitada y de alto riesgo, de igual manera es el espacio de los consultorios con respecto a los equipos de cómputo.
- No contar con un plan de contingencias frente a cualquier eventualidad o desastres naturales. Asimismo, se detectó la ausencia de un ambiente alterno donde realizar el almacenamiento de respaldo de backup.
- Ausencia de manuales o de documentación de los sistemas de información que fueron implementados en el Hospital Regional.
- Falta de licencias de software para algunos equipos informáticos.
- Deterioro de los equipos informáticos que se encuentran en desfase con más de 14 años.

3.7.3. Amenazas

- Las actualizaciones tecnológicas no son aprovechadas y puestos en práctica debido a la falta de presupuesto.
- El elevado costo de las capacitaciones relacionado a tecnologías de la información dificultando el desempeño en la administración y/o manejo de los equipos por parte del personal que labora en cada área.
- Cortafuego descontinuado en la seguridad perimetral.
- Peligro latente y constante de infecciones por virus informáticos o software malicioso.

- En la actualidad existe una creciente demanda por servicios informáticos que son brindados a través de la web, pero aún no han sido implementados por la falta de presupuesto y que comprenden una gran cantidad de consultas; por lo que, pueden provocar una baja en el rendimiento de la red.

3.7.4. Oportunidades

- Debido a la alta demanda de tecnologías, la disponibilidad de encontrar en el mercado es amplia, la cual ayudan a mejorar y actualizar la infraestructura de datos del Hospital Regional de Huacho.
- Los equipos informáticos tienen la predisposición de reducir sus precios debido al avance tecnológico.
- En la actualidad las tecnologías informáticas son consideradas como factor importante para desarrollar e implementar sistemas de información de la institución.
- Intercambio de experiencias con otras instituciones.
- Cumplir con normas publicadas por la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI).

3.7.5. Métodos de la metodología

- Método de evaluación para el Plan de Seguridad de la Información. (Se refiere al P010 de MAIGTI) (Alfaro Paredes, 2008)
- Método de evaluación para el plan de mantenimiento, preventivo de hardware de computadoras, redes y equipos relacionados. (Se refiere al P013 de MAIGTI) (Alfaro Paredes, 2008)

- Método de evaluación para el plan de mantenimiento correctivo de hardware de computadoras, redes y equipos relacionados. (Se refiere al P014 de MAIGTI) (Alfaro Paredes, 2008)
- Método de evaluación para el inventario de software de base. (Se refiere al P022 de MAIGTI) (Alfaro Paredes, 2008)
- Método de evaluación para la arquitectura de la red de tecnologías de información. (Se refiere al P036 de MAIGTI) (Alfaro Paredes, 2008)
- Método de evaluación para la seguridad de acceso a los sistemas de información. (Se refiere al P037 de MAIGTI) (Alfaro Paredes, 2008)
- Método de evaluación para la seguridad de acceso a las carpetas en los servidores. (Se refiere al P038 de MAIGTI) (Alfaro Paredes, 2008)
- Método de evaluación para la seguridad de acceso al centro de cómputo principal. (Se refiere al P054 de MAIGTI) (Alfaro Paredes, 2008)
- Método de evaluación para el cableado de redes de datos. (Se refiere al P054 de MAIGTI) (Alfaro Paredes, 2008)

Desarrollo de procesos

Método de evaluación para el plan de seguridad de la información

(Se refiere al P010 de MAIGTI)

Objetivo

Examinar y evaluar la realización y ejecución del plan de seguridad de la información del Hospital Regional de Huacho, con el fin de determinar la causa de la pérdida de datos, riesgos y poder identificar los posibles procesos involucrados que lo generarían.

Alcance

El alcance del método comprende lo siguiente:

A. Se verificó y revisó el proceso de conformación del equipo para la realización del plan de seguridad de la información.
B. Se verificó la alineación del plan de seguridad de la información a las necesidades y al plan estratégico de informática del Hospital Regional de Huacho.
C. Se revisó el documento del plan de seguridad de la información, y a la vez se verifico que se hayan implementado las acciones indicas en dicho plan.

El alcance del método no comprende lo siguiente:

A. Problemas de seguridad de la información o cualquier ataque informático que se hubieran suscitado durante el periodo de evaluación.

Entradas

Para ejecutar la evaluación del plan de seguridad, se requirió que el Hospital Regional de Huacho proporcione la información al período anterior en evaluación:

A. Se solicitó el plan de seguridad de la información para su revisión.
B. Listado de las personas que colaboraron o tuvieron participación en la realización del plan de seguridad de la información, dicho listado debe contener los datos básicos su contacto del personal.
C. Recepción de las actas de reuniones del equipo de elaboración del plan de seguridad de la información del Hospital Regional de Huacho.

Proceso

Las actividades que fueron realizadas en la evaluación al Hospital Regional Huacho fueron las siguientes:

A. Se recepcionó y revisó el plan de seguridad de información elaborado en el periodo 2019 en el Hospital Regional de Huacho, el cual fue solicitado, procediéndose a su revisión, donde se pudo observar que el equipo de elaboración del plan de seguridad de la información, está integrada solo por el jefe del área de informática, el mismo que realiza el plan de seguridad de la información.
B. Se verificó, si el plan de seguridad de la información está alineado a las necesidades del Hospital Regional de Huacho. También se verificó que priorice la seguridad de los procesos del hospital, empleando las medidas de seguridad máximas para salvaguardar la información, teniendo en cuenta los siguientes elementos:
    1. Seguridad lógica de la información.
        a. Se revisó los peligros de la seguridad por el uso incorrecto del equipo de cómputo.
            - Alfaro Paredes indica que es un peligro latente es compartir redes de Windows no protegidas, el usuario tampoco debe abrir extensiones de programas con archivo oculto. Por último, el manipular archivos adjuntos en

el correo electrónico, podría ocasionar la infección del computador con virus como troyanos, virus de programas, virus residentes entre otros.

b. Se revisó las políticas para control de accesos a:

- Se revisó si el usuario tiene permisos para acceder a las lectoras y grabadoras CD, DVD, o el uso de memorias USB.
- También se revisó si el usuario tiene permiso para realizar la instalación de programas en la computadora.
- Se revisó, si hay control en la visualización de los nombres de páginas web que se accede a través de internet.
- Se verificó que solo el personal autorizado tenga acceso al software de base y sistemas de información usados en el Hospital Regional de Huacho. También se debe realizar la revisión periódica de los registros de transacciones para comprobar si han sido manipulados sin alguna autorización.

c. Se revisó la configuración del "firewall".

- Se revisó si se cuenta con restricciones de accesos a sitios web no autorizados por su jefatura. También se verifico si han ocurrido intentos de ataque de intruso o se haya producido alguno y no pudo ser detectado en el momento oportuno.
- Se verificó si se cuenta con una revisión periódica del registro de transacciones del "firewall".

d. Con respecto a las copias de respaldo de información.

- Se verificó si el tiempo de elaboración para las copias de respaldo de información es el adecuado ante las necesidades del hospital.
- Se verificó si el uso de equipos para las copias de respaldo son los más adecuados, también se comprobó si el equipo para las copias de respaldo se

ubica en un ambiente físico del área de informática, y otra copia en un ambiente físico fuera del Hospital Regional. Por último, se revisó si el tiempo de demora en la restauración de la copia de respaldo es el adecuado y se realiza la verificación las tareas de los backups, para ver si se han realizado correctamente.

2. Seguridad física de la información:

a. Con respecto al acceso de personal en el área de informática:

- Se revisó la correcta identificación del personal que ingresan al área de informática, así como si las puertas de acceso al área de informática cuentan con claves de seguridad y el estado en el que se encuentran.

b. Con respecto al suministro de energía eléctrica de los equipos de cómputo.

- Se revisó que la línea de voltaje de los equipos de cómputo sea diferente de las líneas de voltaje que se usen para otros fines en la institución.
- Se verificó si el área de informática cuenta con un sistema de alimentación ininterrumpida (UPS) o uso de generadores de voltaje para el área de informática y si el personal cuenta con la capacitación de cómo actuar ante una caída del suministro de energía eléctrica.
- Se revisó la existencia y mantenimiento periódico del pozo de tierra.

c. Con respecto a la protección contra incendios.

- Se revisó si el hospital cuenta con extintores para incendios causados por equipos electrónicos, también si la vigencia de los extintores está actualizada y la cantidad es la suficiente para todos los equipos.
- Se revisó si el hospital realiza el correcto funcionamiento de las alarmas contra incendios a la vez si existe material inflamable en el área de informática, tales como ropa, material inflamable, etc.

d. Con respecto a las condiciones ambientales del área de informática.

- En cuanto al equipo de aire acondicionado se revisó que su funcionamiento se encuentra de manera correcta, también si el área de informática cuenta con detectores de humedad y medidor de temperatura del ambiente.
- Se revisó si en el área de informática los cables de red se encuentran desordenado y expuesto ocasionando un mayor riesgo de manipulación y algún tipo de accidente.

e. Con respecto fallas en hardware.

- Se revisó cuáles son las fallas más comunes pudieron ser fallas en disco duro, fuente de voltaje del equipo, en la tarjeta principal entre otras.

Salidas

Al desarrollar esta evaluación en el Hospital Regional de Huacho se encontraron las siguientes observaciones:

A. Se evidenció que el Hospital Regional de Huacho no cuenta con un Plan estratégico de información, la cual se debe estar alineado al plan de seguridad de la información.
B. Se evidenció que la institución cuenta con un plan de seguridad de la información, el cual permite conservar la información de atención al cliente, información institucional como son el Sistema Integrado Administración Financiera (SIAF), Sistema Informático de Gestión Administrativa (SIGA), planillas, control de asistencia los cuales son de vital importancia para la continuidad del hospital.
C. En la evaluación se encontró lo siguiente con respecto a la seguridad lógica:

- Se evidenció que el Hospital Regional de Huacho contaba con servidor web y servidor de correo la cual eran muy vulnerables a ataques de software malicioso como por ejemplo el Ransomware, el cual actuaba encriptando los archivos y te exigía dinero

para poder recuperar tu información, por tal motivo el hospital opto por contratar un Hosting, se trabaja con HostiGator, la capacidad con la se cuenta es ilimitada y el contrato se realizó por el periodo de junio del 2019 a junio 2021.

D. Se encontró lo siguiente con respecto a políticas de control accesos:

- Se puedo verificar que solo el área de informática, se brinda lo siguiente.
  - ✓ Registrar usuarios
  - ✓ Registrar privilegios
  - ✓ Gestionar contraseñas
- El jefe de cada área envía un informe con los accesos que se otorga a cada usuario, y el cual es enviado al área de informática para su respectiva atención.
- También se evidencia que existe personal que cuenta con accesos para utilizar exploradores de internet de manera libre, pero se a la vez se ha identificado que no es utilizada de la mejor manera y hasta con fines no institucionales.
- Algo alertador es que todos los usuarios de las áreas administrativas tienen permisos para realizar envíos de correos electrónicos a otras direcciones y a la vez recepción de correos externos, el cual incrementa el margen de vulnerabilidad, si bien es cierto se trabaja con un hosting llamado HostGator el cual tiene centrado el plan Básico, pero esto no es indicador que pudiera estar libre de ataques informáticos

E. Se encontró lo siguiente con respecto a la administración de Firewall:

- Si bien cierto en la evaluación se encontró que se trabaja Mikrotik, el cual permite controlar los accesos a internet de los usuarios, se halló que existen restricciones para sitios web no autorizados como, por ejemplo: redes sociales, pornografía, YouTube.
- Se evidencio que en varias oportunidades se ha logrado bloqueado el intento de ataques de virus, troyanos como por ejemplo D-Stop, virus oculta archivos, pero también han ocurrido ataques a los programas instalados como fue el caso del ataque

de software malicioso llamado Ransomware, cual bloqueaba los archivos de tu computadora hasta que pagues.

- Se verifico que se realizan revisiones periódicas a las transacciones del firewall.

F. Se encontró lo siguiente con respecto a las copias de respaldo de la información en el Hospital Regional de Huacho:

- Se evidencio que se cuenta con servidor backup de marca IBM, modelo: 7158 y con capacidad de un 1 Terabyte, la condición en la que se encuentra dicho servidor no es la adecuada, más un con la información que se resguarda. Por tal motivo se recomienda la adquisición un nuevo servidor con la siguiente característica Servidor HPE ProLiant ML350 Gen10, Xeon Silver 4110 2.1GHz.
- Se evidencio que se realiza un backup de aplicativos hospitalarios de atención al cliente:
  - ✓ Se realiza cada 6 horas en disco duro con aplicativo desarrollado en el hospital; en 2 equipos de cómputo y uno en pc dedicada como servidor de backup, programado a distintas horas con la finalidad de disminuir la pérdida de información conservando las 10 últimas copias anteriores por seguridad; esta copia de seguridad se realiza en forma automática con Aplicativo System Scheduler Free.
- Se evidencio que se realiza un backup de aplicativo SIAF:
  - ✓ Se realiza cada 24 horas en 1 pc dedicada como servidor de backup, el tiempo de realización es de 10 min aproximadamente.
- Se evidencio que se realiza un backup de pcs de áreas administrativas.
  - ✓ Se realiza cada 4 horas en disco duro con aplicativo desarrollado en el hospital con la finalidad de proteger la información de los servicios de Economía,

Epidemiología, Estadística, Logística, Personal, Servicios Generales; esta copia de seguridad se realiza en forma automática con Aplicativo System Scheduler Free.

- Se evidenció que el Hosting HostGator contratado realiza sus copias de backup cada 24 horas.
- La copia de respaldo se aloja en un ambiente del área de informática, considerando que la ubicación no cuenta con las condiciones adecuadas para ello. Otra copia se encuentra en la nube la cual se trabaja con el Google Drive de manera gratuita.
- La restauración de las copias de respaldo se realiza en un tiempo estimado de 30 minutos.
- Se encontró que diariamente se realiza la verificación de backup que se completen correctamente.

G. Se encontró lo siguiente con respecto a la seguridad física del Hospital Regional de Huacho:

a. Se revisó el acceso de personas en el área de informática:

- Se permite el ingreso de personas al área de informática como personal administrativo de otras áreas por cualquier consulta o problema que hayan tenido con sus equipos, ya que el área de informática se ubica en el mismo ambiente de servidores, donde se encuentren los equipos informáticos; si otras personan ingresan debe ser con autorización y coordinación de la jefatura inmediata y en los tiempos establecidos y/o coordinados.
- No se cuenta con claves de seguridad para el ingreso de la puerta de acceso a la oficina, solo cuenta con una llave para el ingreso.
- Si bien es cierto el hospital regional cuenta con cámaras de seguridad para sus consultorios y el área de emergencia, también se evidencio que no se cuentan con cámaras seguridad para el área de informática, y deja vulnerable al área pudiendo

producirse robos o manipulación de información, o de algún equipos de cómputo, por tal motivo se recomienda realizar la adquisición de una cámara de seguridad Marca: Yale, Modelo: CCTV V720P 8C y unirla al sistema CCTV con la que cuenta el hospital que permite tener controlada una zona específica y solamente ciertos usuarios pueden tener acceso a las imágenes.

b. Se revisó el suministro de energía eléctrica de los equipos de cómputo del Hospital Regional de Huacho:

- El área de informática cuenta con un solo equipo UPS de Marca: FORZA Power Technologies, Modelo: FDC-010K con trasformador de aislamiento, el cual funciona las 24 horas, permite conserva el voltaje de energía adecuado por 1 hora ante un corte de energía.
- El UPS FORZA, si bien protege un tiempo suficiente como para soportar la carga de todos los servidores ante un corte de energía eléctrica, solo es para el área de cómputo, este es un problema de alta importancia, ya que se utiliza una misma línea de voltaje para equipos de salud (instrumentos quirúrgicos), para los equipos de cómputo de los consultorios y área de emergencia, colapsando el hospital ante esta ocurrencia.
- El Hospital Regional de Huacho cuenta con 20 pozos a tierra, a los cuales no se les brinda mantenimiento en los últimos 2 años.

c. Se evidencio que en el área de informática cuenta con extintores contra incendios de Marca TISCHER, pero los cuales cuentan con una última revisión de junio del 2018, también se encontró la existencia de material inflamable como ropa, cartones entre otros, poniendo en riesgo ante cualquier incidencia que ocurra en el área.

d. Se evidencio que no se cuenta con detectores de humo, no cuenta con alarma contra incendios, y el personal del área no tiene la capacitación adecuada para actuar ante cualquier incidente.

e. Con respecto a las condiciones ambientales de la sala de cómputo se evidencio lo siguiente:

   - El cableado de red se encuentra muy desordenado, con el riesgo que el personal cometa algún error al momento de realizar algún tipo de mantenimiento y lo cual generaría interrupciones en el servicio para todos los usuarios de la red.
   - El espacio del área de informática es pequeño, para albergar a los servidores, dar mantenimiento a los sistemas informáticos y realizar soporte informático a todo el hospital.
   - El equipo de aire acondicionado es de Marca: CIAC, se encuentra funcionando, pero se encuentra deteriorado y sin mantenimiento preventivo, no cumple con su función el cual es mantener la zona de servidores una temperatura adecuada. Por tal se recomienda la adquisición de un nuevo equipo de aire acondicionado VM122C6 Split Inverter de 12.000 BTUs de acuerdo al presupuesto del hospital.

f. Se evidencio las diversas fallas de hardware en los equipos del Hospital Regional de Huacho:

   - Se encontró fallas en hardware son muy comunes en el hospital, las más comunes son fallas en el disco duro, fallas en la tarjeta principal, fallas en la memoria RAM.

Método de evaluación para el plan de mantenimiento preventivo de equipos de cómputo, redes y equipos relacionados (se refiere al P013 de Maigti)

Objetivo

Examinar y evaluar la realización y ejecución del plan de mantenimiento preventivo del equipo de cómputo, redes y otros equipos relacionados en el Hospital Regional de Huacho, con el fin de determinar la causa de la pérdida de datos, riesgos y poder identificar los posibles procesos involucrados que lo generarían.

Alcance

El alcance del método comprende lo siguiente:

A. Se revisó el proceso de elaboración del plan de mantenimiento preventivo de equipos de cómputo, redes y otros equipos relacionados.
B. Se revisó el documento del plan de mantenimiento preventivo de equipos de cómputo, redes y otros equipos relacionados.
C. Se verificó los cronogramas y responsabilidades para la ejecución del plan del mantenimiento preventivo de equipos de cómputo, redes y otros equipos relaciones.

El alcance del método no comprendió lo siguiente:

A. El plan de mantenimiento correctivo de equipos de cómputo, redes y otros equipos relaciones no se incluirán en la evaluación.

Entradas

Para ejecutar la evaluación se requirió que el Hospital Regional de Huacho proporcione la información al período anterior en evaluación:

A. Se solicitó el inventario de los equipos de cómputos, redes y equipos relacionados. Y también el listado de equipos que requieran mantenimiento preventivo.
B. Se solicitó los últimos mantenimientos preventivos que se haya realizado sobre los equipos con las fechas e informes correspondientes.
C. Se solicitó el cronograma de actividades del plan de mantenimiento preventivo con el personal asignado para su atención.

Proceso

Las actividades que fueron realizadas en la evaluación al Hospital Regional de Huacho fueron las siguientes:

A. Se recepciono y revisó el plan de mantenimiento preventivo del Hospital Regional de Huacho elaborado en el periodo 2019 el cual fue solicitado.
B. Se revisó que en la lista de equipos para el mantenimiento preventivo trabaje en alineación en el inventario de total de equipos, dicha lista de equipos debe incluir lo siguiente:
    - Equipos de cómputo en su totalidad o están directamente conectados a ella.
    - Equipos de servidores, equipos de red.
    - Equipos relacionados a la energía eléctrica.
    - Equipos relacionados a las condiciones ambientales y protección contra incendios.
    - Equipos relacionados a la seguridad.
C. Se solicitó los últimos informes sobre mantenimientos preventivos que se haya realizado en los equipos del Hospital Regional de Huacho.

D. Se logró revisar el proceso del plan de mantenimiento preventivo para los equipos informáticos, también se puedo evaluar cuáles son los criterios utilizados para priorizar dicho mantenimiento.

E. Se logró revisar los cronogramas y responsabilidades asignadas para la realización del plan de mantenimiento preventivo.

Salidas

Al desarrollar esta evaluación en el Hospital Regional de Huacho se encontraron las siguientes observaciones:

A. El Hospital Regional de Huacho, si cuenta con un plan preventivo de equipos de cómputos, el cual es elaborado por el jefe del área de informática Jorge Sánchez.

B. El Hospital Regional de Huacho, no realiza un inventario detallado por áreas de equipos de cómputo (por ejemplo, piezas internas del computador), equipos redes, equipos eléctricos, equipos de medios ambientales, pero se trabajó un detalle de toda la información recaudada:

Tabla 3

Detalle de Servidores

Servidores					
Nº	**Descripcion**	**Marca-Modelo**	**Capacidad**	**Procesador**	**Cantidad**
1	Servidor De Siaf	Del Power Edge 2950	1 Tb	Intel Zeon 3.2	1
2	Servidor Atención Al Cliente	Hp Intel Xeon	80 Gb	Intel Zeon 3.2	1

4	Servidor De Siga	Hp Proliant Dl380e Gen8	1 Tb	Intel Zeon 3.2	1
5	Servidor De Backup	Ibm 7158_Serie: Kc8wt17	1 Tb	Intel Zeon 3.2	2
6	Servidor De Laboratorio	Hp Proliant Ml 110 Gen10	1 Tb	Intel Zeon 3.2	1
7	Servidor Robot_Sunat	Hp Proliant Ml110 Gen9	1 Tb	Intel Zeon 3.2	1

Nota: Realizado por las autoras

Tabla 4

Detalle de Equipos personales

Computadoras Personales		
Nº	**Hardware**	**Cantidad**
1	Compatibles - Core I 3	43
2	Hp- Core I 5	24
3	Halion - Core I 7	46
5	Compatibles-Intel Celeron	10
6	Compatibles - Pentium Iv	81

Nota: Realizado por las autoras

Tabla 5

Detalle de UPS

Ups		
Nº	**Hardware**	**Cantidad**
1	Forza Power Technologies	1

Nota: Realizado por las autoras

Tabla 6

Detalle de Routers

Routers		
N°	**Marca_Modelo**	**Cantidad**
1	Tp-Link Telefónica (Administrativos)	1
2	Tp-Link Telefónica (Asistenciales)	1
3	Tp-Link Telefónica (Sis)	1
4	Nucon Telefónica	6

Nota: Realizado por las autoras

Tabla 7

Detalle de Conputadoras Portatil

Computadoras Portatiles			
Nº	**Hardware**	**Capacidad**	**Cantidad**
1	N-Computer	1 Tb	32

Nota: Realizado por las autoras

Tabla 8

Detalle de Switches

Switchers			
Nº	**Marca_Modelo**	**Puertos**	**Cantidad**
1	D-Link	16 Puertos	3
2	D-Link	24 Puertos	10
4	D-Link	8 Puertos	5
5	Cisco	48 Puertos	2
6	Cisco	24 Puertos	2
7	HP	24 Puertos	1

Nota: Realizado por las autoras

Tabla 9

Detalle de otros equipos que se encuentran en el Área de Informática

Nº	**Otros**	**Cantidad**
1	Pozos a tierra.	20
2	Caja de control de suministro de energía eléctrica.	01
3	Aire Acondicionado –Ciac.	01
4	Extintor – Tischer.	02

Nota: Realizado por las autoras

C. Se realiza el mantenimiento preventivo a los equipos de cómputo cada 3 meses, el último mantenimiento registrado empezó en el mes de octubre, equipos de servidores y equipos de red se realiza el mantenimiento cada 2 años, sin embargo, no se realiza ningún mantenimiento a los pozos a tierra, a los equipos de condiciones ambientales, ni equipos de seguridad.

D. El personal del área de informática realiza informes de los mantenimientos preventivos, contando con formatos propios en el cual detallan el área, usuario y el problema.
E. En cuanto a los últimos mantenimientos preventivos, no se logró obtener de manera física los informes que se haya realizado sobre los equipos.
F. También se evidencio que el mantenimiento está asignado a un solo personal del área de informática, pero debido a la falta de personal es difícil cumplir con los tiempos estimados según los cronogramas establecidos.

Método de evaluación para el plan de mantenimiento correctivo de equipos de cómputo, redes y equipos relacionados (se refiere al P014 de Maigti)

Objetivo

Examinar y evaluar la realización y ejecución del plan de mantenimiento correctivo de los equipos de cómputo, redes y otros equipos relacionados en el Hospital Regional de Huacho, con el fin de determinar la causa de la pérdida de datos, riesgos y poder identificar los posibles procesos involucrados que lo generarían.

Alcance

El alcance del método comprendió lo siguiente:

A. Se revisó el proceso de elaboración del plan de mantenimiento correctivo de equipos de cómputo, redes y otros equipos relacionados.
B. Se revisó el documento del plan de mantenimiento correctivo de equipos de cómputo, redes y otros equipos relacionados.

C. Se verificó los cronogramas y responsabilidades para la ejecución del plan del mantenimiento correctivo de equipos de cómputo, redes y otros equipos relaciones.

El alcance del método no comprendió lo siguiente:

A. El plan de mantenimiento preventivo de los equipos de cómputo, redes y otros equipos relaciones no se incluirán en la evaluación.

Entradas

Para ejecutar la evaluación se requirió que el Hospital Regional de Huacho proporcione la información al período anterior en evaluación:

A. Se solicitó el inventario de los equipos de cómputos, redes y equipos relacionados. Y también el listado de equipos que requieran mantenimiento correctivo.
B. Se solicitó los últimos mantenimientos correctivos ejecutados sobre los equipos con las fechas e informes correspondientes.
C. Se solicitó el cronograma de actividades del plan de mantenimiento correctivo de cómputos, redes y equipos relacionados con el personal asignado para su atención.

Proceso

Las actividades que fueron realizadas en la evaluación al Hospital Regional de Huacho fueron las siguientes:

A. Se recepcionó y revisó el plan de mantenimiento correctivo del Hospital Regional elaborado en el periodo 2019 que fue solicitado.
B. Se revisó la lista de equipos para el mantenimiento correctivo, los cuales son: equipos de servidores, equipos de red.

C. Se logró revisar el proceso del plan mantenimiento correctivo para los equipos informáticos, también se puedo evaluar cuáles son los criterios utilizados para priorizar dicho mantenimiento.
D. Se solicitó los últimos informes sobre últimos mantenimientos correctivos que se haya realizado sobre los equipos del Hospital Regional de Huacho.
E. Se logró revisar la asignación de cronogramas y responsabilidades para la realización del plan de mantenimiento correctivo.

Salidas

Al desarrollar esta evaluación en el Hospital Regional de Huacho se encontraron las siguientes observaciones:

A. El Hospital Regional de Huacho cuenta con un plan de mantenimiento correctivo de equipos informáticos, elaborado por el propio personal del área de informática, el cual consiste en dar una solución inmediata por alguna circunstancia no prevista, reparación y/o cambio de las piezas defectuosas, comprende el diagnóstico, realizar la reparación y suministrar el repuesto necesario.
B. Como se tiene de conocimiento el Hospital Regional de Huacho no realiza un inventario detallado por áreas de equipos de cómputo, equipos redes, equipos eléctricos, equipos de medios ambientales, esto es debido a la falta de tiempo y falta de persona en el área de informática.
C. El Hospital Regional de Huacho elabora al término de cada atención un reporte de mantenimiento correctivo, donde se registran los datos de los equipos de cómputo revisados, detalle del diagnóstico encontrado durante el mantenimiento efectuado.

D. Los criterios utilizados para determinar y priorizar las necesidades de los mantenimientos, son mayormente por las áreas que tienen interacción con el público, ya que ellos son los que reportan mayores averías en el trascurso del año.
E. No se logró obtener los informes sobre últimos mantenimientos correctivos que se haya realizado sobre los equipos.
F. En el mantenimiento de servidores en algunas ocasiones se realiza en caliente, pudiendo provocar problemas. En el caso de la electricidad cuando es un problema leve lo ve el mismo personal de informática, si fuera grave un especialista en electricidad.
G. El mantenimiento está asignado a un solo personal del área de informática, pero debido a la falta de personal es un difícil cumplir tiempos estimados según los cronogramas establecidos para cada equipo que presente alguna falla.

Método de evaluación para el inventario de software de base

(se refiere al P022 de Maigti)

Objetivo

Examinar y evaluar el inventario de software de base del Hospital Regional de Huacho, con el fin de determinar la causa de la pérdida de datos, riesgos y poder identificar los posibles procesos involucrados que lo generarían.

Alcance

El alcance del método comprende lo siguiente:

A. Se realizó la revisión detallada del documento del inventario de software del Hospital Regional de Huacho

B. Revisión y verificación de los procedimientos y los documentos físico funcionamiento en el software de base del Hospital Regional de Huacho.
C. Revisión física del inventario de software.

El alcance del método no comprendió lo siguiente:

A. Realizar la evaluación del listado de los sistemas de información con que cuenta el Hospital Regional de Huacho.

Entradas

Para ejecutar la evaluación se requirió que el Hospital Regional de Huacho proporcione la información al período anterior en evaluación:

A. Inventario de software en unidades de todas las oficinas del Hospital Regional de Huacho.

Proceso

Las actividades realizadas en el Hospital Regional Huacho para esta evaluación fueron las siguientes:

A. Se logró recepcionar y revisar información sobre el inventario de software del Hospital Regional del periodo 2019 que fue solicitada.
B. Se logró revi sar detalladamente el documento del inventario de software, verificando la existencia de los siguientes tipos de software:
    - Sistemas operativos.
    - Servidor de bases de datos.
    - Software de protección contra intrusos.
    - Servidores web y correo.
    - Servidor backup.

- Software de oficina.

C. Se logró obtener el número de licencias que se ha comprado, para poder contrastar con lo que realmente utilizan y necesitan los usuarios.

Salidas

Al desarrollar esta evaluación en el Hospital Regional de Huacho se encontró las siguientes observaciones:

A. El Hospital Regional de Huacho tiene un inventario de software. El cual se detalló a continuación los siguientes tipos de software:

   Tabla 10

   Detalle de inventario de Software

Nº	Software		
	Servidores	**Sistema Operativo**	**Cantidad**
01	Servidor Backup	Windows 2012 Server	1
02	Servidor De Laboratorio	Linux - Centos	1
03	Servidor Robot - Sunat	Windows 2012 Server	1
04	Servidor SIAF	Windows 2012 Server	1
05	Servidor SIGA	Windows 2016 Server	1
06	Servidor Atención Al Cliente	Novell 5.1	1
07	Servidor Web	Hostgator	1
	Sistemas operativos- Equipos de Cómputos		
	Sistemas Operativos		**Cantidad**
08	Novell 5.1		100
09	Widows Xp Started		1
10	Windows Xp Profesional OEM		9
11	Windows 7		47
12	Windows 8		46
	Herramientas de Desarrollo		
13	Visual Estudio 6		2
14	Visual Estudio Pro 2008		1
15	Visual Fox Pro 25		1
	De oficina		
16	Microsoft Office 2007 For LATAM		2
17	Microsoft Office Basic 2007 OEM		9
18	Microsoft Office Bassic Edicion 2003		4
19	Microsoft Office Pro 2003		4
20	Microsoft Office Sbe 2003		106
22	Microsoft Visio 2007		1
23	Microsoft Office 2007		10
24	Microsoft Office 2010		10
25	Win RAR		-
26	Lector De PDF		-
	Antivirus		

25	Esetnod Antivirus	0

Nota: Realizado por las autoras

B. Se logró evidenciar que se utiliza software original Novell 5.1 para el 30% de máquinas, para el resto de equipos no utilizan software original solo craqueado, esto generaría una problemática de detectarse la utilización de software ilegal, en primera instancia se asumiría una denuncia, pudiendo incluir virus, troyanos o software espía lo cual supones un grave peligro para la seguridad en la información.

C. Se trabaja con sistemas operativos Windows XP, Windows 7, Windows 8 y Windows 10, teniendo en cuenta que el hospital tiene 370 equipos de cómputo según el inventario.

D. También se logró evidenciar que no se cuenta con licencia original de ESET NOD32 Antivirus, solo se utiliza el antivirus craqueado para las todas las máquinas que se registran en el hospital el cual son de 370 según el inventario de los equipos. Esto es de alto riesgo ya que las probabilidades de infectar un equipo con virus, serán mucho mayores, si esto llegara a suceder se perderá toda la información e incluso quitarle utilidad al computador.

E. Se evidenció que el software de escritorio con las que cuenta los computadores en el Hospital Regional no son original y se trabaja con software craqueado, se cuenta con Office Profesional 2003, 2010, 2019, Win RAR, lector de pdf.

F. Se manejan dos redes, dentro de las cuales se manejan programas originales provenientes del ministerio de salud.

- Red administrativa (SIGA, SIAF)
- Red asistencial

G. Se logró evidenciar que el Hospital Regional de Huacho no cuenta con el apoyo de la alta dirección para comprar las licencias originales, hacen caso omiso a sus requerimientos.

Método de evaluación para la arquitectura de la red de tecnologías de información.

(se refiere al P036 de Maigti)

Objetivo

Examinar y evaluar la arquitectura de la red de tecnologías de información del Hospital Regional de Huacho, con el fin de determinar la causa de la pérdida de datos, riesgos y poder identificar los posibles procesos involucrados que lo generarían.

Alcance

El alcance del método comprende lo siguiente:

A. Verificación detallada del documento de la arquitectura de la red de tecnologías de información.
B. Revisión física de la arquitectura de la red de tecnologías de información.
C. Evaluar la probabilidad que se generaría por errores en la arquitectura de la red de tecnologías de información.

El alcance del método no comprendió lo siguiente:

A. Realizar la evaluación de los sistemas de información que operan sobre la arquitectura de la red.

Entradas

Para ejecutar la evaluación se requirió que el Hospital Regional de Huacho proporcione la información al período anterior en evaluación:

A. Documento de la arquitectura de la red de tecnologías de información.

Proceso

Las actividades realizadas en el Hospital Regional de Huacho para esta evaluación fueron las siguientes:

A. Se logró examinar y verificar la documentación solicitada sobre la arquitectura de la red de tecnologías de información del Hospital Regional de Huacho del periodo 2019.
    - Revisar los siguientes tipos de hardware en el área de informática:
        - ✓ Equipos de red: routers, firewalls, switches, hubs, cableado, la cual se logró verificar que el cableado se encuentre instalado estructuralmente en "racks" y cubiertos por falsos pisos.
        - ✓ En cuanto a los puntos de la red de datos, se pudo examinar si dichos puntos se encuentran cerca de medios de red de energía eléctrica como motores.
        - ✓ Se logró revisar equipos de servidores.
    - Revisar los siguientes tipos de software en el área de informática

B. Se logró verificar físicamente la arquitectura de la red de tecnologías de información. A la vez se logró comprobar la velocidad de transmisión de datos en la red interna, como en internet.

C. Se logró identificar la probabilidad que se generaría por errores en la arquitectura de la red de tecnologías de información.

Salidas

Al desarrollar esta evaluación en el Hospital Regional de Huacho se encontró las siguientes observaciones:

A. El Hospital Regional de Huacho elabora un documento no formal sobre la arquitectura de la red, lo tienen un libro de Excel donde se detalla el tipo de arquitectura que se emplea, el cual es de tipo estrella y la distribución IP para cada área.

B. A continuación, se indica los detalles sobre la arquitectura de la red de tecnologías de información.

Tabla 11

Detalle de equipos de red

Routers		
N°	**Marca_Modelo**	**Cantidad**
1	Tp-Link Telefónica (Administrativos)	1
2	Tp-Link Telefónica (Asistenciales)	1
3	Tp-Link Telefónica (Sis)	1
4	Nucon Telefónica	6

Switchers			
Nº	**Marca_Modelo**	**Puertos**	**Cantidad**
1	D-LINK	16 PUERTOS	3
2	D-LINK	24 PUERTOS	10
3	D-LINK	48 PUERTOS	3
4	D-LINK	8 PUERTOS	5
5	CISCO	48 PUERTOS	2
6	CISCO	24 PUERTOS	2
7	HP	24 PUERTOS	1

Nota: Realizado por las autoras

- El cableado de red no se encuentra correctamente ordenado, en algunos casos se encuentra empotrados y otros por canaletas, tampoco cuentan con falsos pisos, en el

lugar donde están ubicados los servidores, switches, routers los cuales a la vez se encuentra muy desordenado.

- Los puntos de la red de datos, en algunos casos no cumplen con la normativa de cercanía a motores y puntos de conectores a la red de energía eléctrica, lo cual se observó en áreas administrativas y consultorios.
- El hospital cuenta con 2 líneas en las cuales la velocidad de conexión a servicios internet es de 20 megabytes como línea dedicada, se trabaja una línea con movistar y otra con claro.
- Tipos de software en el hospital son los siguientes.

Tabla 12

Detalle de software que se encuentra en el Hospital Regional de Huacho

Nº	SOFTWARE	CANTIDAD
	SISTEMAS OPERATIVOS	
1	NOVELL 5.1	100
2	WINDOWS XP STARTED	1
3	WINDOWS XP PROFESIONAL OEM	9
4	WINDOWS 7	47
5	WINDOWS 8	46

Nota: Realizado por las autoras

C. La red interna del hospital regional tiene una buena velocidad en la transmisión de datos es de 10 Mbps, 100 Mbps, 1000 Mbps.

D. Se evidencio que se cuenta con un bajo presupuesto en base a la arquitectura de red, de no realizarse la adecuada organización, el impacto de no tener una arquitectura de red debidamente instalada tendría consecuencias muy graves para la institución, no se podría

compartir de forma eficiente la información a las áreas del Hospital, se encontró una mala distribución de la red generaría una conexión a internet más lenta, lo cual se ha venido presentando en el área de admisión y caja generando malestar en el personal y en los pacientes al realizar su atención, también se encontró mucho desorden de cables dentro del área de informática, pudiendo ocasionar errores al momento de realizar mantenimiento o cualquier procedimiento en la red.

Método de evaluación para la seguridad de acceso a los sistemas de información.

(se refiere al P037 de Maigti)

Objetivo

Examinar y evaluar la seguridad de acceso a los sistemas de información del Hospital Regional de Huacho, con el fin de determinar la causa de la pérdida de datos, riesgos y poder identificar los posibles procesos involucrados que lo generarían.

Alcance

El alcance del método comprendió lo siguiente:

A. Verificación de todos los permisos al sistema que tiene el personal en referencia a las opciones de acceso a sistemas de información.
B. Verificación del método para el otorgar permisos al personal.
C. Revisión alterna en cuanto a los permisos exclusivos que se le concede al usuario.
D. Análisis e identificación de la probabilidad que pudiera ocasionar si la seguridad de acceso a los sistemas de información fuera vulnerada o se concediera un permiso indebido.

El alcance del método no comprendió:

A. Realizar la evaluación de la seguridad en cuanto al acceso a las carpetas de los servidores.

Entradas

Para ejecutar la evaluación se requirió que el Hospital Regional de Huacho proporcione la información al período anterior en evaluación:

A. Listado de todos los accesos que se otorgan a los usuarios sobre los sistemas de información.
B. Los criterios que se toman para otorgar permisos a los usuarios.
C. Los permisos que se otorgan a los accesos de los sistemas de información dentro del hospital, en modo lectura; es decir, que los usuarios solo deben de tener la opción de consulta y reportes.

Proceso

Las actividades realizadas en el Hospital Regional de Huacho para esta evaluación fueron las siguientes:

A. Se logró revisar la documentación solicitada de seguridad de acceso a los sistemas de información del Hospital Regional de Huacho del periodo 2019.
B. Se logró revisar los permisos que se otorgan al personal en referencia a las opciones de los diferentes sistemas de información con los que se cuentan y también se constató si el personal verdaderamente tiene la necesidad de acceder a un sistema de información u otra opción, también se logró ver si el usuario necesita la autorización del gerente o jefe de área.
C. Se revisó de modo alterno el acceso exclusivo que se le concede al personal en referencia a las opciones que se les ha otorgado acceso.

D. Se logró identificación de la probabilidad que pudiera ocasionar si la seguridad de acceso a los sistemas de información fuera vulnerada o se concediera un permiso indebido.

Salidas

Al desarrollar esta evaluación en el Hospital Regional de Huacho se encontraron las siguientes observaciones:

A. Se evidenció que no se cuenta con ninguna documentación formal de acceso a los sistemas de información del Hospital Regional de Huacho en el periodo 2019.
B. Se evidenció que los usuarios no pueden acceder a los sistemas de información y otras opciones a los cuales no tienen permisos, designados por el jefe de su área, ya que para cada área y puesto de trabajo cuentan con un perfil determinado.
C. Solo el jefe del área de informática, tiene el permiso de manipular directamente la base de datos.
D. Si bien solo el personal del área de informática tiene el permiso de asignar usuarios y privilegios, esto se realiza con una coordinación del área del usuario, mediante un documento donde se detalla sus accesos a tener.
E. No cuentan con un programa para la administración de usuario como por ejemplo el Active Directory.
F. No se permite que se ingrese con claves vacías o con nombres similares a los del usuario a los sistemas de información.
G. Dado que es un hospital la información que posee es de suma importancia ya que se guarda en su base de datos los registros de cada persona, por el cual todos los accesos tienen que ser otorgados por el jefe del área de informática ya que si hubiera alguna perdida de información debido a una deficiente seguridad o a un acceso indebido, causaría una gran pérdida de datos en el historial de cada persona, dinero por los

módulos de atención al cliente, y el tiempo que se tomaría para solucionar el problema sería demasiado ya que en todo momento el hospital necesita seguir funcionando.

Método de la evaluación de la seguridad de acceso a las carpetas en los servidores (Se refiere al P038 de Maigti)

Objetivo

Examinar y evaluar la seguridad de acceso a las carpetas en los servidores del Hospital Regional de Huacho, con el fin de determinar la causa de la pérdida de datos, riesgos y poder identificar los posibles procesos involucrados que lo generarían.

Alcance

El alcance de método comprende lo siguiente:

A. Verificación a todos los accesos del personal en cuanto a las carpetas que se encuentran en los servidores.
B. Verificación de los permisos que se otorgan al personal.
C. Revisión aleatoria en cuanto al permiso exclusivo del personal en referencia al acceso de carpetas en los servidores que se les ha dado permiso
D. Análisis e identificación de la probabilidad que pudiera ocasionar si la seguridad de acceso de la carpeta en los servidores fuera vulnerada o se concediera un permiso indebido.

El alcance del método no comprendió lo siguiente:

A. Realizar la revisión de la seguridad en cuanto al acceso a los sistemas de información.

Entradas

Para ejecutar la evaluación se requirió que el Hospital Regional de Huacho proporcione la información al período anterior en evaluación:

A. La lista de permisos de todos los accesos de cada usuario, en el cual debe de estar registrada la ruta de red por cada carpeta del servidor.
B. Criterios para conceder accesos al usuario con respecto a las carpetas que se encuentran en los servidores.

Proceso

Las actividades realizadas en el Hospital Regional de Huacho para esta evaluación fueron las siguientes:

A. Se logró revisar la documentación solicitada sobre la seguridad de acceso a las carpetas en los servidores del Hospital Regional de Huacho del periodo 2019.
B. Se logró verificar cuidadosamente los accesos del personal en cuanto a las carpetas de los servidores. Se revisó la relación de carpetas a las cuales se puede acceder, además se revisó si el personal verdaderamente necesita acceso.
C. Se revisó el proceso de otorgar permisos sobre las carpetas de los servidores. El cual se verifico que incluya por lo menos la autorización del jefe de área del usuario.
D. Se logró identificar la pérdida de valor que se podría originar en caso sea vulnerable la seguridad de acceso a las carpetas de los servidores o se concediera un acceso indebido.

Salidas

Al desarrollar esta evaluación en el Hospital Regional de Huacho se encontraron las siguientes observaciones:

A. Cada usuario tiene asignado sus accesos de acuerdo a sus perfiles y cargos para un mejor desempeño en sus labores.

- El usuario que tenga un requerimiento de acceso a un software adicional al pre instalado en su equipo debe solicitarlo, por medio de un formato de requerimiento a la unidad de estadística e informática.
- El usuario que realice una instalación de manera intencional de software en su equipo de cómputo es el único responsable del mal funcionamiento del mismo, conjuntamente las dificultades que se podrían presentar en los demás equipos conectados a la red.
- El usuario no debe realizar ninguna manipulación en el hardware, ni del software que se encuentra a su disposición, de igual manera no debe de alterar la configuración de los equipos de cómputo instalada por el área de informática.

B. El jefe del área de informática es el único en dar accesos a las carpetas de servidores, controla los permisos a todos los servicios informáticos, tomando la decisión de negar a cualquiera que infrinja las políticas o cause problemas a los demás usuarios.
C. Se ha verificado que los accesos a las carpetas de servidores son utilizados únicamente por el personal del área de informática
D. Dada la importancia de los servidores y la cantidad de datos que almacenan en él, es necesario obtener un sistema completamente seguro y resistente frente a cualquier tipo de amenaza o vulnerabilidad. El impacto que produciría sería muy serio, ya que se vería involucrada información muy sensible del hospital al quedar expuesta, las pérdidas económicas también se harían visibles, ya que se trabaja con modulo caja, los empleados estarían impedidos en sus actividades labores, también ocasionara retraso en toda la

atención a los clientes, a ello habría que añadir aquellos daños incuantificables que afectan a la imagen del hospital.

Método de evaluación para la seguridad de acceso al centro de cómputo principal (Se refiere al P054 de Maigti)

Objetivo

Examinar y evaluar la seguridad de acceso al ingreso al área de informática del Hospital Regional de Huacho, con el fin de determinar la causa de la pérdida de datos, riesgos y poder identificar los posibles procesos involucrados que lo generarían.

Alcance

El alcance del método comprende lo siguiente:

A. Verificación de acceso en la puerta principal al área de informática.
B. Revisión del acceso donde se encuentra de área de informática.
C. Control del acceso en la entrada de área de informática.
D. Análisis e identificación de la probabilidad que pudiera ocasionar si la seguridad de acceso al área de informática fuera vulnerada o se concediera un permiso indebido.

El alcance del método no comprende:

Realizar la revisión técnica de los equipos que sirven de apoyo para la seguridad de acceso.

Entrada

Para ejecutar la evaluación se requirió que el Hospital Regional de Huacho proporcione la información al período anterior en evaluación:

A. Se solicitó la lista de personas que están involucradas con el permiso de acceso al área de informática, iniciando con el personal de seguridad que resguarda el acceso del hospital hasta la puerta del área de informática.
B. Capacitación para el personal, con los temas de seguridad de acceso a las instalaciones, como también a personas no autorizadas.
C. Reporte de incidentes relacionados a la seguridad de acceso en el área de informática.

Proceso

Las actividades realizadas en el Hospital Regional de Huacho para esta evaluación fueron las siguientes:

A. Se logró revisar la documentación solicitada sobre la seguridad de acceso al área de informática del Hospital Regional de Huacho del periodo 2019.
B. Se logró observar cómo se realiza el acceso a la puerta que permite el ingreso al área de informática. A la vez se ha verifico lo siguiente:
    - El hospital cuenta con un personal encargado de vigilar el acceso.
    - Indicaciones impartidas al personal encargado de vigilar el acceso y poder decidir si permite el acceso a una persona.
    - Registro de ingreso y salida de cada persona que sea ajena al área de informática.
C. Se logró identificación de la probabilidad que pudiera ocasionar si la seguridad de acceso al área de informática fuera vulnerada o se concediera un permiso indebido.

Salidas

Al desarrollar esta evaluación en el Hospital Regional de Huacho se encontraron las siguientes observaciones:

A. Se evidencio que no cuenta con ningún documento sobre la seguridad de acceso al área de informática del Hospital Regional de Huacho.
B. Se permite el ingreso de personas al área de informática como personal administrativo de otras áreas por cualquier consulta o problema que hayan tenido con sus equipos y personas que vienen a realizar gestiones al hospital, tomando en cuenta que el área de informática se encuentra ubicado cerca de las áreas de atención al cliente.
C. El personal que se encuentra ubicado en recepción cumple la función de entregar un ticket de visitante y realiza la interrogante hacia donde se dirige, a la cual le entrega el ticket. normalmente sólo se pregunta el piso a donde va a visitar.
D. La puerta de acceso al área de informática no cuenta con un dispositivo para colocar clave de seguridad, solo cuenta con una llave de acceso. Tampoco existen cámaras de vigilancia ante cualquier hecho que pueda suscitar, se recomienda la adquisición de cámara de seguridad Marca: Yale, Modelo: CCTV V720P 8C y unirla al sistema CCTV con la cuenta el hospital que permite tener controlada una zona específica y solamente ciertos usuarios pueden tener acceso a las imágenes.
E. El personal de vigilancia no elabora un adecuado registro de las personas que ingresan o salen del área de informática, tampoco se registra la hora en que produjo la entrada o la salida.
F. Al producirse una violación a la seguridad de accesos al área de informática, ocasionaría que personas malintencionadas, puede realizar manipulación en los equipos de cómputos, redes, así como manipulación de datos sensibles y perdida de documentación que se tiene en el área, a ello habría que añadir aquellos daños que afectan a la imagen de la empresa al ser utilizado dicha información con otros fines.

Método de evaluación para el cableado de redes de datos

(Se refiere al P058 de Maigti)

Objetivo

Examinar y evaluar el cableado de la red datos del área de informática del Hospital Regional de Huacho, con el fin de determinar la causa de la pérdida de datos, riesgos y poder identificar los posibles procesos involucrados que lo generarían.

Alcance

El alcance del método comprendió lo siguiente incluye:

A. Observar la ubicación y las condiciones en las que se encuentra el cableado de red de datos.
B. Verificación de la velocidad que transcurre por el cableado de red de datos.
C. Identificar de la probabilidad que pudiera ocasionar si la seguridad de acceso al área de informática fuera vulnerada o se concediera un permiso indebido.

El alcance del método no comprende lo siguiente:

A. La revisión técnica a los equipos que se encuentran conectados a los cables de redes de datos.

Entradas

Para ejecutar la evaluación se requirió que el Hospital Regional de Huacho proporcione la información al período anterior en evaluación:

A. Se solicitó el plano del cableado de redes de datos del Hospital Regional de Huacho.

B. Se solicitó los reportes de los mantenimientos preventivos y correctivos anteriores.

Proceso

Las actividades realizadas en Hospital Regional de Huacho para esta evaluación fueron las siguientes:

A. Se revisó la información solicitada al Hospital Regional de Huacho de lo cual fue la siguiente:
   - Plano del cableado de la red de datos del Hospital Regional de Huacho, que fue elaborado en el 2019. También se solicitó adicionalmente los puntos de red detalladamente por áreas.

B. Se logró observar y revisar la ubicación y en qué condiciones se encuentra el cableado de red de datos:
   - Según la evaluación se pudo observar sobre la ubicación del cableado estructurado:
     - ✓ El cableado no debe encontrarse expuesto a altas temperaturas.
     - ✓ El cableado no debe encontrarse cerca de motores, mucho menos de cables de corriente eléctrica.
   - El cableado debe encontrarse en las siguientes condiciones:
     - ✓ El cableado debe encontrarse en perfectas condiciones, sin daños.
     - ✓ El cableado se debe encontrar ordenadamente estructurado en canaletas.
     - ✓ El cableado tiene que estar ordenado y estructurado en los “racks”.

C. Se logró revisar la velocidad de la transmisión que pasa por el cableado de red de datos. Verificando que la velocidad sea satisfactoria.

D. Se logró identificar y analizar la probabilidad que pudiera ocasionarse por distintos factores tales como la velocidad o ubicación, o en condiciones inadecuadas para cableado de red de datos.

Salidas

Al desarrollar esta evaluación en el Hospital Regional de Huacho se encontraron las siguientes observaciones:

A. El cableado del área de informática se encuentra desordenado, con el riesgo que el personal cometa algún error al momento del mantenimiento y se genere alguna interrupción en el servicio, generando pérdida de tiempo para los usuarios que se encuentran conectados a la red.
B. Los “racks” no tienen un adecuado uso, sin embargo, se encuentran disponibles.
C. Se logró verificar que el cableado de red de datos se encuentra muy cerca de la corriente de energía eléctrica y del área de servidores. El cableado no se encuentra ordenado a través de canaletas, todos estos puntos ocasionan daño y deterioro más rápido.
D. El cableado está expuesto ante cualquier personal que ingrese al área de informática.
E. La velocidad de transmisión que transita por el cableado de red de datos es de 10mbps/100mbps/1000mbps. Comúnmente sucede algunos errores en la trasmisión porque las tarjetas de red no han sido actualizadas en referencia con la velocidad que soporta el cableado, debido a los años de antigüedad.
F. El impacto que se generaría si produjera algún error sería muy significativo, ya que, debido al desorden y la mala ubicación de los cables de redes de datos, sumado a la velocidad de la trasmisión de datos, generara una lentitud en la atención a los clientes, en el área administrativa, hasta en la misma área de informática.

Informe de propuesta de mejoras para la seguridad de la red de datos del Hospital Regional De Huacho

Al finalizar el proceso de evaluación se puede realizar una propuesta de mejoramiento soportada en los siguientes aspectos:

Método de evaluación para el plan de seguridad de la información (Se refiere al P010 de Maigti)

Hallazgos 1:

A. Se evidencio que el Hospital Regional de Huacho, no cuenta con un Plan estratégico de seguridad de la información.

Recomendación

A. Se recomienda elaborar y realizar seguimiento al plan estratégico de seguridad de la información el cual debe estar alineado al plan de seguridad de la información del Hospital Regional de Huacho, este plan debe ser compartido con todo el personal del área para que conjuntamente se logre alcanzar la meta trazada o específica, se debe tener presente realizar un monitorio y seguimiento periódico para verificar el logo de la meta y la alineación del personal con la misma.

   El principal objetivo es proteger la información que se maneja en el Hospital utilizando herramientas para el procesamiento de la información, los cuales nos ayudaran a combatir vulnerabilidades internas, externas, intencionales o accidentales, y así poder garantizar la seguridad cumpliendo con los 3 pilares de la información que son la integridad, disponibilidad y confiabilidad.

Hallazgo 2:

A. Si bien se cumple con este proceso, se está bridando esta recomendación con respecto a las políticas de control accesos de usuarios, la cual se evidencio que el jefe de cada área envía un informe con los accesos que se otorga a cada usuario, y el cual es enviado al área de informática para su respectiva atención. Pero también se han detectado que en muchos usuarios poseen permisos al acceso a internet de manera libre y no están realizando el correcto uso, descargando archivos no autorizados y visitando portales de internet que no van acorde para el cumplimiento de sus respectivas funciones, a la vez también se identificó que existen usuarios que tienen permisos para acceder lectoras y memorias USB, pero no realizan la correcta desinfección ocasionando la infección del equipo de cómputo con software maliciosos, o virus informáticos.

Recomendaciones:

A. Se recomienda crear un formato de perfil de usuario en el cual agrupe las necesidades de software según se requiera. Este perfil debe de contener el listado de software que puede utilizar para el desempeño de su función.

   Por ejemplo:

   Perfil de Usuario 1: En este perfil se puede agrupar a todos los usuarios que utilicen la red asistencial, como por ejemplo sistema de farmacia, atención al cliente.

   Perfil de Usuario 2: En este perfil se puede agrupar a todos los usuarios que utilicen el software de oficina, antivirus, utilitario PDF, entre otros, como ejemplos las áreas administrativas.

B. También el área de informática debe realizar una evaluación minuciosa sobre los permisos y accesos con los que cuenta cada personal, ya que como se mencionó anteriormente algunos usuarios están utilizando esos permisos para fines no

institucionales, y al realizar dicha evaluación se podrá otorgar los permisos y accesos necesarios, evitar que el usuario realiza acciones que no están relacionadas a sus funciones.

C. Asimismo, la ISO/IEC 27002 la cual anteriormente denominada estándar 17799:2005, nos indica que es suma importancia realizar un control de accesos a la información en base a las necesidades de institución, organización y/o empresa.

Por tal razón nos indica que se puede realizar las siguientes actividades para el control del riesgo:

1. Se debe establecer, documentar y revisar la política de control de acceso según las necesidades de la institución.
2. Se debe proveer el acceso a redes y servicios de red a los usuarios para los cuales han sido autorizados.
3. Implementar un procedimiento formal para la creación y así poder habilitar todos sus accesos correspondientes y también realizar eliminación de un usuario según sea el caso.
4. Implementar un procedimiento formal para asignar o anular los derechos de acceso para todos los usuarios, sistemas de información y servicios.
5. En el caso de acceso con privilegios especiales, debe ser otorgado de una controlada y restringida.
6. El área encargada de realizar otorgar los accesos tiene que revisar periódicamente los derechos de acceso de todos los usuarios.
7. En el caso de realizar contrataciones o con trabajadores externos, es necesario retirar los derechos de acceso a la información una vez finalizado el trabajo o contrato.
8. Todos los usuarios deben ser conscientes de la responsabilidad en el control de sus accesos, un punto importante es al momento de emplear sus contraseñas y la

seguridad en los equipos que se les asigna, por tal razón es necesario que los usuarios utilicen buenas prácticas de seguridad en el uso de la información asignada.

9. En cuanto al control de acceso a sistemas y aplicaciones se debe establecer procedimientos seguros el cual restrinjan los accesos de los usuarios y el personal de soporte a la información., además se debe implementar un sistema de gestión de contraseñas para asegurar contraseñas de calidad.
10. Solo el personal autorizado debe tener acceso al código fuente de los sistemas y aplicaciones del software, debiendo ser necesario un acceso restringido a lo demás usuarios.

Hallazgo 3:

1. En la evaluación realizada se evidenció que se realizan las copias de respaldo de la información de las diferentes áreas con las cuentas del Hospital Regional de Huacho de la manera más oportuna para salvaguardar la información, pero también se evidencio que las copias se alojan en un ambiente del área de informática, considerando que la ubicación no cuenta con las condiciones adecuadas para ello. Otra copia se encuentra en la nube la cual se trabaja con el Google Drive de manera gratuita.
2. También se encontró que el Hospital Regional de Huacho no cuenta con medios de respaldo de su información fuera de sus instalaciones provocando que se encuentre vulnerable ante cualquier siniestro que pueda ocurrir.

Recomendaciones:

A. La ISO/IEC 17799 en su control 10.5 Respaldo o Back-Up nos indica los siguiente:

- La institución debe determinar un nivel adecuado de respaldo de la información, en el

caso del Hospital Regional de Huacho, es de suma importancia ya que la información que se maneja en ella es primordial para el funcionamiento de sus áreas administrativas y de atención a los pacientes.

La institución debe generar registros puntuales e íntegros de las copias de respaldo y métodos documentados de restauración, ya que un reporte incompleto puede generar retrasos en la atención de requerimientos en las distintas áreas del Hospital Regional de Huacho. A la vez se debe generar copias de respaldo, las cuales se deben almacenar en un sitio seguro, a una distancia recomendable ante cualquier daño por un desastre ocasionado en el hospital, como una recomendación todos los dispositivos de respaldo deben de probados constantemente para poder asegurar confiablemente la información y poder utilizarla cuando se requiera en caso de una emergencia.

B. En Cobit 4.1. en su dominio DS4.9 Almacenamiento de Respaldos Fuera de las Instalaciones, indica que, para cumplir con medidas necesarias, se debe de almacenar un lugar externo todos los medios de respaldo, quiere decir fuera de las instalaciones incluyendo documentación y otros recursos de tecnología de la información críticos, indispensable para restablecer los planes de continuidad del Hospital Regional de Huacho.

Para realizar el almacenamiento externo se debe de seguir una política de clasificación de datos y prácticas de almacenamiento de datos del Hospital Regional de Huacho. El cual debe de asegurar que los lugares externos destinado para almacenar los respaldos sean evaluados periódicamente, como mínimo de manera anual, respecto al contenido, a la protección ambiental y a la seguridad.

También se debe asegurar de la compatibilidad del hardware y software con la finalidad de recuperar datos archivados, los cuales deben de ser probados y renovados periódicamente.

Hallazgo 4:

A. En cuanto a la seguridad física se encontró, no se cuenta con claves de seguridad para el ingreso de la puerta de acceso a la oficina, solo cuenta con una llave para el ingreso.
B. Si bien es cierto el Hospital Regional de Huacho cuenta con cámaras de seguridad para sus consultorios y el área de emergencia, también se evidencio que no se cuentan con cámaras seguridad para el área de informática, y deja vulnerable al área pudiendo producirse robos o manipulación de información, o de algunos equipos de cómputo.

Recomendaciones:

A. Por tal motivo se recomienda realizar la adquisición de una cámara de seguridad Marca: Yale, Modelo: CCTV V720P 8C y unirla al sistema CCTV con la cuenta el hospital que permite tener controlada una zona específica y solamente ciertos usuarios pueden tener acceso a las imágenes.

B. En **NTP-ISO-IEC-17799** en su control 9**. Seguridad física y del entorno** indica en su control **9.1.2 Controles físicos de entradas**:

   A continuación, se presentan las siguientes pautas:

   - Las visitas al área de informática siempre deben supervisar, a menos que el acceso sea autorizado por el Jefe del área y se debe registrar la fecha de entrada y salida, al personal sólo se le permitirá el acceso siempre y cuando tenga propósitos específicos

y autorizados, como ejemplo el mantenimiento de algún equipo de cómputo o algún inconveniente que se presente en el trascurso del día.

- Se recomienda controlar el acceso al personal que manipula información de alto nivel de importancia como también el uso de recursos. Una recomendación es usar controles de autenticación, por ejemplo, tarjetas con número de identificación personal (PIN), para autorizar y validar el acceso.

Hallazgo 5:

A. Se encontró con extintores contra incendios de Marca TISCHER pero los cuales cuentan con su revisión de junio del 2018, también se encontró la existencia de material inflamable como ropa, cuadernos, entre otros, poniendo en riesgo ante cualquier incidencia que ocurra en el área. También se evidencio que no se cuenta con detectores de humo, no cuenta con alarma contra incendios, y el personal del hospital no tiene la capacitación adecuada para actuar ante cualquier incidente.

Recomendaciones:

A. En **COBIT 4.1.** en su dominio **DS12.5. Administración de Instalaciones Físicas,** el cual recomienda extraer cualquier tipo de material inflamable (papeles, cartones, etc.) del piso del área de informática y de la sala de servidores pues incrementan los riesgos de que exista algún incendio en los interiores del área.

Se recomienda lo siguiente:

Extintor a base de polvo químico, este extintor está compuesto a base de polvo químico el cual es adecuado para combatir situaciones de peligro tales como combatir fuegos de clase A, B y C, lo que hace es cortar la reacción en cadena y sofocar el fuego, al fundirse con el calor, formando una barrera entre el oxígeno y el material en llamas.

Detectores de humo

- En cuenta a los detectores de humo, se debe colocar en la parte más alta del área donde se instalará y de preferentemente, en el medio, como el hospital tiene más pisos se recomienda instalar el detector en el lugar donde las escaleras se comunican al piso siguiente.
- También se recomienda que la instalación de los detectores a una distancia mínima de 50 cm de otros objetos y deben colocarse sobre el techo, no sobre la pared, tampoco deben colocarse cerca de aberturas para ventilación o cerca de quemadores o en baños, donde pueden hacer sonar falsas alarmas.

Método De Evaluación Para El Plan De Mantenimiento Preventivo De Equipos De Cómputo, Redes Y Equipos Relacionados (Se Refiere Al P013 De Maigti)

Hallazgo 1:

A. En la evaluación realizada al Hospital Regional de Huacho se evidencio que no se realiza un inventario detallado de todos sus equipos informáticos, tampoco cuenta con reportes de últimos mantenimientos preventivos realizados, a pesar de contar con un formato impreso.

Recomendación:

A. Se recomienda realizar un inventario de todos los equipos de cómputo con los que cuenta en forma anual. Este inventario debe de incluir servidores, estaciones de trabajo, computadoras portátiles, n-computer, UPS, routers, switch. Cada equipo debe de ser detallado sus características principales como modelo, marca, tarjeta madre, microprocesador, disco duro, memoria, tarjeta de video, tarjeta de red, etc.

B. Toda esta información debe de quedar registrada en una base de datos detallada con todas las características ya antes señaladas, así como el usuario y área donde está ubicado el bien.

C. Se debe elaborar un reporto de manera digital de los mantenimientos preventivos, para llevar un control y registro detallado de las operaciones que se han realizan y el motivo del mantenimiento.

D. También en la **NTP-ISO-IEC-17799** señala en su objetivo de control **7.1. Responsabilidad por los activos**, indica en su control **7.1.1. Inventario de Activos**, la elaboración de un inventario de todos los activos incluyendo las instalaciones donde se procesa la información, las cuales deben ser identificados y elaborados en un formato de reporte de inventario el cual debe de ser actualizada periódicamente.

Hallazgo 2:

A. En el Hospital Regional de Huacho se observó que se realiza un mantenimiento preventivo a todos los equipos de cómputo cada 3 meses, el ultimo mantenimiento registro empezó en el mes de octubre, equipos de servidores y equipos de red cada 2 años. Además, se observó que a los pozos a tierra no se les realiza ninguna clase de mantenimiento, mucho menos a los equipos de condiciones ambientales, ni equipos de seguridad.

Recomendación:

A. Se propone que partiendo del ultimo inventario realizado de equipos de cómputo que posee el Hospital Regional de Huacho se realice un cronograma en el cual se detalle las fecha y hora del mantenimiento, esta actividad debe de ser previamente coordinada entre

el personal del área de informática con todos los usuarios, con el objetivo de tener a disposición de los equipos, sin afectar las actividades cotidianas.

El personal de soporte técnico debe de seguir los siguientes lineamientos durante los mantenimientos preventivos:

- Revisar que todos los equipos se mantengan en buen estado y su funcionamiento sea optimo, realizar el diagnostico, limpieza interna y externa.
- Realizar una revisión a los servidores de red, estaciones de trabajo, impresoras, equipo de cómputo y comunicaciones en concordancia con el inventario del Hospital Regional de Huacho. En caso el equipo no se encuentre en el listado, se procede a informar a la jefatura del área para poder actualizar el inventario.
- Realizar una prueba a los componentes del equipo, y si fuera necesario se realizaría una reparación.
- Al finalizar cada atención de mantenimiento se deberá entregar un reporte con los detalles correspondientes del servicio.

Se debe de realizar el mantenimiento de pozo a tierra como mínimo una vez al año, existen varias empresas que prestan servicios una de ellas es INGELCI PERU SAC.

A. En la **NTP-ISO-IEC-27001** señala en su objetivo de control **A.11.2 Equipos**, indica en su control **A. 11.2.4. Mantenimiento de Equipos**, nos indica que para realizar un mantenimiento preventivo es necesario observar el ambiente y el estado de los componentes ya que dependiendo de estas indicaciones se tomara en cuenta la frecuencia que debe ser efectuado, cada 3 meses siempre y cuando el ambiente sea extremadamente sucio o por lo contrario dos veces al año. Para asegurar el correcto funcionamiento y la

continua disponibilidad de los equipos, estos deben de mantenerse en buen estado y teniendo como objetivo la integridad de la información.

Esta norma nos recomienda una opción que es contratar servicios de terceros para el mantenimiento de equipos, solo cuando la organización no cuente con un área de TI. Una sugerencia es seguir las recomendaciones del fabricante ya que cada equipo cuenta con una garantía dentro de un cierto plazo de vencimiento, solo el personal autorizado debe de realizar el mantenimiento a los equipos críticos cumpliendo con las indicaciones que se tiene establecido.

Método De Evaluación Para El Plan De Mantenimiento Correctivo De Equipos De Cómputo, Redes Y Equipos Relacionados (Se Refiere Al P014 De Maigti)

Hallazgo 1:

A. En la evaluación realizada al Hospital Regional de Huacho no se logró obtener los últimos informes sobre últimos mantenimientos correctivos que se haya realizado sobre los equipos.
B. En lo que respecta al mantenimiento de servidores en algunas ocasiones se realiza en caliente, pudiendo provocar problemas. En el caso de la electricidad cuando es un problema leve lo ve el mismo personal de informática, si fuera grave un especialista en electricidad.
C. El mantenimiento está asignado a un solo personal del área de informática, pero debido a la falta de personal es un difícil cumplir tiempos estimados según los cronogramas establecidos.

Recomendación:

A. Se debe elaborar un reporto de manera digital de los mantenimientos correctivos, para llevar un control y registro detallado de las operaciones que se han realizan y el motivo del mantenimiento.

B. Se propone una solución inmediata para este tipo de mantenimiento ya que es una circunstancia no prevista por el usuario, el cual debe de consistir en un cambio de piezas y si fuese posible la reparación del componente, el cual incluye un diagnóstico, el tiempo de mano de obra de reparación y el presupuesto.

C. El tiempo de respuesta ante un mantenimiento correctivo no debe de exceder más de 4 días, ya que son tiempos establecidos por el área de informática.

D. En el caso que no se dé una solución rápida al usuario se tomara la decisión de asignar un equipo alternativo con características semejantes o mejores, con el propósito de no causar pérdida de tiempo a los usuarios y continúen con su trabajo.

E. Al finalizar cada atención de mantenimiento se debe de elaborar un informe detallado y especifico del mantenimiento correctivo realizado, adicionalmente se debe de elaborar un reporte de incidencias en el cual especifique los datos del equipo y todos los detalles encontrados durante la inspección efectuada.

F. En la **NTP-ISO-IEC-27001** señala en su objetivo de control **A.11.2 Equipos**, indica en su control **A.11.2.4. Mantenimiento de Equipos**, nos define que un mantenimiento correctivo requiere dar solución inmediata y consiste en la reparación y/o cambio de piezas defectuosas o reparación del sistema operativo. Tras recibir una solicitud de manteniendo correctivo se tomarán en cuenta los siguientes puntos:

    - Verificar si se cuenta con los repuestos y herramientas apropiadas para realizar el mantenimiento.

- Evaluar la opción de reparar o actualizar el equipo, el cual de no ser factible se le considerará como obsoleto, todo este proceso debe de estar plasmado en un informe técnico.
- Examinar que el equipo haya mejorado su rendimiento después de la actualización y recupere su operatividad.
- De deben de elaborar formatos para registrar todos los detalles de incidencias de cada equipo.

Método De Evaluación Para El Inventario De Software De Base

(Se Refiere Al P022 De Maigti)

Hallazgo 1:

A. Se logró evidenciar que se utiliza software original Novell 5.1 para el 30% de máquinas, para el resto de equipos no utilizan software original solo craqueado, esto generaría una problemática, ya que de detectarse un software ilegal en primer lugar se generaría problemas legales y a la vez este tipo de programas pudieran incluir virus, troyanos o algún software espía y dejaría con vulnerabilidad la seguridad de su información

Recomendaciones:

A. Se recomienda que el Hospital Regional de Huacho realice una previa evaluación para que determinar el tipo de licencia de software más conveniente para atender los requerimientos de adquisición de licencias. En esta evaluación debe de contener el análisis comparativo de valores de mercado, los costos y beneficios a obtener; ya que todo equipo de cómputo que se adquiera debe de contar con el software y las licencias necesarias para su funcionamiento incluyendo el sistema operativo y antivirus.

B. De la misma manera siempre se debe estar supervisando el funcionamiento y actualización de estos tipos de software, así como la elaboración de un inventario de las licencias con las que se cuentan ya que la detección temprana de un fallo en un software de base permite al usuario salvar hasta la integridad de las partes físicas del equipo.

C. También en la NTP-ISO-IEC-27001 señala en su objetivo de control **A.12.5 Control del software operacional**, y en su control **A. 12.5.1. Instalación de software en sistemas operacionales,** se indica que se deben realizar procedimientos implementados para controlar la instalación de software en sistemas operacionales.

Es importante mantener procedimientos para las instalaciones de software en cualquier dispositivo que se encuentre dentro de una organización. A continuación, deben de tomarse en cuenta los siguientes controles:

Antes de realizar cualquier instalación de un software se deben de realizar pruebas en entornos aislados.

Verificar la compatibilidad del programa a instalar con el hardware.

Establecer métodos o herramientas de monitoreo para detectar cambios no autorizados.

D. También en la NTP-ISO-IEC-17799 señala en su objetivo de control **A.12.4 Seguridad de Archivos del Sistema**, y en su control **A. 12.4.1. Control del Software en Producción,** nos indica que un software adquirido que se utilice en sistemas operativos se debería mantener en el nivel de soporte de proveedor. Ya que existen proveedores que venden software con versiones antiguas. Se debe de considerar la propuesta de solo adquirir software que cuenten con soporte.

Cuando se tome la decisión de actualizar un sistema operativo también se debe de considerar los requerimientos de negocio para dicho cambio y la seguridad, ya que una nueva versión puede ser menos segura y difícil de familiarizar con el usuario. Otra opción son los parches, pero estos solo de deben de utilizar cuando ayuden a reducir

vulnerabilidades.

Solo se debe de permitir el acceso físico o lógico a proveedores cuando estén autorizados y sea necesario por temas de soporte.

Método De Evaluación Para La Arquitectura De La Red De Tecnologías De Información (Se Refiere Al P036 De Maigti)

Hallazgo 1:

A. El Hospital Regional de Huacho elabora un documento no formal sobre la arquitectura de la red, lo tienen un libro de Excel donde se detalla el tipo de arquitectura que se emplea, el cual es de tipo estrella y la distribución IP para cada área.

- El cableado de red no se encuentra correctamente ordenado, en algunos casos se encuentra empotrados y otros por canaletas, tampoco cuentan con falsos pisos, en el lugar donde están ubicados los servidores, switches, routers los cuales a la vez se encuentra muy desordenado.
- Los puntos de la red de datos, en algunos casos no cumplen con la normativa de cercanía a motores y puntos de conectores a la red de energía eléctrica, lo cual se observó en áreas administrativas y consultorios.

Recomendaciones:

A. Se debe realizar un documento formal donde se pueda apreciar la topología utilizada por el Hospital Regional de Huacho, también podría ser incluido en el plan se seguridad de la información.

El Hospital Regional de Huacho utiliza la topología de red en estrella, la cual en primera instancia es óptima, teniendo en cuenta los recursos con la cual va ser construida. A continuación, se detalla las ventajas y desventajas de esta topología:

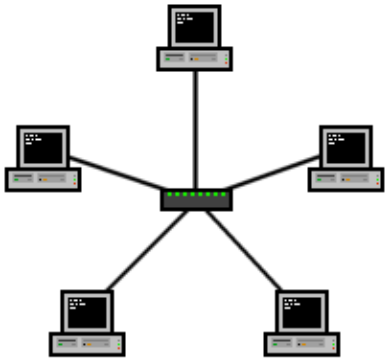


Figura N° 13. Topología Estrella

Fuente. (https://www.lifeder.com/topologia-en-estrella/)

Ventajas

- Una de sus principales ventajas y por la cual fue optada la topología por la institución fue principalmente es que limita el impacto de una falla, por ejemplo, si un equipo de cómputo no funciona correctamente en la red no va afectar al resto de la red la cual seguirá funcionando con normalidad
- Esta topología permite una estructura simple.
- Facilita poder agregar, reemplazar o eliminar cualquier componente que esté conectada a la red. Por tal motivo la red es fácil de extender sin tener que interrumpir su funcionamiento.
- En cuanto a la administrar y mantener la red es mucho fácil de realizar, porque cada equipo o nodo solo requiere un cable independiente, así mismo ante cualquier

inconveniente o problema es fácil de identificar y darle solucionar oportuna sin afectar a los demás usuarios.

- En tanto a la seguridad y rendimiento los paquetes de datos no viajan a través de varios nodos, por tal motivo garantiza que los datos estén seguros y transferencia de datos sea considerablemente más rápida.

Desventajas

- El principal problema de la topología de red en estrella es en cuanto a su funcionamiento, ya que depende en gran medida del servidor o dispositivo central, con esto nos referimos a que si falla el servidor central se caerá toda la red y todas las computadoras quedarán desconectadas de la red, lo que en el hospital significaría que todo el proceso de atención en los pacientes y procesamiento de información en los sistemas se vería gravemente afectado.
- En cuanto a su implementación puede tener mayor costo debido que se usa adicionalmente un hub (repetidor) o switch como dispositivo central de conexión de la red, por tal razón para conectarse se necesitan más cables en comparación con la topología de anillo y bus.
- En cuanto a su funcionamiento depende del servidor central o centrador directamente, si el servidor es lento, hará que toda la red se funcione igual. Así mismo si el servidor central se ve afectado de alguna manera dejará a toda la red vulnerable.

B. En cuanto a su cableado estructura se recomienda seguir con la utilización del cableado horizontal.

Estructura del cableado horizontal

Los cableados horizontales son aquellos que van a integrar todos los ambientes que están en el centro de datos de todas las áreas del hospital. Se sugiere que se debe de canalizar los tipos de cableados que manda la norma TIA-568.

En un primer lugar se recomienda que se debe utilizar una fibra óptica, pero según los usuarios de la institución no requiere tal ancho de banda: por lo tanto, se debe de tener lo siguiente:

- ✓ Debe tenerse presente que todo el canal de comunicación debe estar apto para soportar velocidades en las aplicaciones.
- ✓ Cuando se menciona a todo el canal se debe tener presente y claro que es todo lo que forma parte de la conectividad desde el gabinete hasta cada área en el Hospital.

Identificación y administración de equipos

Así mismo es esencial que se determine las configuraciones IP para cada equipo que se realiza la conectividad.

Es recomendable utilizar IP fijas o estáticas ya que ofrecen conexiones más estables y mayores velocidades, así como un control exclusivo al no ser utilizada por nadie más, sin embargo, también tienen algunos inconvenientes, como que al tener siempre la misma dirección quedas más expuesto en cuanto a seguridad online se refiere.

Condiciones de instalación del cableado horizontal

Por lo general, en cuarto de servidores, existe uno o varios Switch o hub para conectar cada área de trabajo a la red de área local mediante cableado horizontal.

Para adaptarse a las necesidades cambiantes de los usuarios en las oficinas, se recomienda instalar por lo menos un cable horizontal extra por cada área de trabajo, de lo contrario el área de trabajo podría ser poco eficiente ante posibles modificaciones.

En cuanto a las longitudes máximas de estos cables se tienen que tener en cuenta lo siguiente:

- La longitud máxima del cable horizontal debe ser de 90 m.
- La longitud máxima de los cables de parcheo es 6 m.

Método De Evaluación Para La Seguridad De Acceso A Los Sistemas De Información (Se Refiere Al P037 De Maigti)

Hallazgo 1:

A. Se evidencio que en el Hospital Regional de Huacho no cuenta con ninguna documentación de acceso a los sistemas de información en el periodo 2019.
B. Con respecto al acceso a los sistemas de información se observó que el personal tiene restringido ingresar a los sistemas de información u opciones a las cuales no tienen permisos, designados por el jefe de su área.

Recomendación:

A. Se sugiere realizar un manual documentado donde se pueda especificar los accesos a los sistemas de información, también se debe supervisar la asignación de privilegios por un método formal de autorización para la cual se deberían considerar los pasos siguientes:
    - El perfil de usuario y la contraseña de acceso a la red de datos, correo, sistemas administrativos y asistenciales, SIGA, SIAF entre otros que son creados por el área de informática, pertenecen al Hospital Regional de Huacho y son para uso únicamente

personal quedando bajo la responsabilidad del usuario al que se le asigna dicha cuenta. Para pertenecer a una red datos y a todos los servicios de información debe de ejecutarse desde un equipo debidamente registrado y autorizado por el área de informática, el cual debe contar una dirección IP dentro del rango de números IP legítimos definidos por el área de informática y debe contener un nombre de máquina.

- Existen criterios para establecer cuentas y contraseñas asignadas por el personal del área. De igual manera cada usuario no debe compartir ni facilitar a ningún otro su cuenta y su contraseña personal, lo cual puede producir una sustracción de información o manipulación de los documentos electrónicos en los equipos informáticos, está prohibido imprimir información reservada y trasladarla fuera de los ambientes del Hospital Regional de Huacho con la finalidad de utilizarla a beneficio propio. Esto genera la divulgación o manipulación de información reservada del usuario afectando el funcionamiento.
- Si se tiene el caso de reparación personal el área de informática debe de reconstruir un nuevo perfil con una nueva contraseña que por derecho el usuario puede solicitar.
- El usuario no puede realizar ningún tipo de descargas, ni compartir archivos de música, videos, juegos y similares con fines no institucionales.
- Para un mejor control de acceso se recomienda ACTIVE DIRECTORY ya que divide a los usuarios en grupos y les proporciona permisos de inicio de sesión.

Método De Evaluación Para La Seguridad De Acceso Al Centro De Cómputo Principal (Se Refiere Al P054 De Maigti)

Hallazgo 1:

A. Se evidencio que no cuenta con ningún documento sobre la seguridad de acceso al área de informática del Hospital Regional de Huacho.
B. Se permite el ingreso de personas al área de informática como personal administrativo de otras áreas por cualquier consulta o problema que hayan tenido con sus equipos y personas que vienen a realizar gestiones al Hospital, tomando en cuenta que el área de informática se encuentra ubicado cerca de las áreas de atención al cliente.
A. La puerta de acceso al área de informática no tiene dispositivo para colocar clave de seguridad, solo cuenta con una llave de acceso. Tampoco existen cámaras de vigilancia ante cualquier hecho que pueda suscitar.

Recomendación:

A. En la **NTP-ISO-IEC-27001** señala **9. Seguridad Física y del Entorno indica en su control 9.1.2 Controles físicos de entradas.**

Deberían considerarse las siguientes pautas:

- El personal que ingresa al área de informática tiene que ser supervisado y registrado con la fecha y hora de entrada y salida. De igual manera el personal debe ingresar acceso para propósitos específicos y autorizados.
- Se debería vigilar y limitar el acceso al personal que no está autorizado para la manipulación de información sensible y a los recursos de su tratamiento. Se deberían usar controles de autenticación, por ejemplo, tarjetas con número de identificación personal (PIN), para autorizar y validar el acceso.

- Como una recomendación se debería de exigir a todo personal que labora lleve identificación visible como por ejemplo un fotocheck.
- Cuando se presente el caso de apoyo de terceros se debe de garantizar la seguridad de acceso restringido hacia áreas de seguridad o a los recursos de procesamiento de información sensibles, estas visitas deben de ser autorizados y monitoreadas.
- Se deberían revisar y actualizar regularmente los derechos de acceso a las áreas de seguridad.

Método De Evaluación Para El Cableado De Redes De Datos

(Se Refiere Al P058 De Maigti)

Hallazgo 1:

A. Se evidencio que el cableado del área de informática se encuentra desordenado, con el riesgo que el personal cometa algún error al momento del mantenimiento y se genere alguna interrupción en el servicio, generando pérdida de tiempo para los usuarios que se encuentran conectados a la red, se pudo observar que los "racks" no tienen un adecuado uso, sin embargo, se encuentran disponibles.
B. También se evidenció que el cableado de red se encuentra ubicado muy cerca a los cables de corriente de energía eléctrica, cerca al área de servidores, el cableado no está ordenado estructuralmente dentro de canaletas, ocasionando el daño y deterioro más rápido.

Recomendaciones:

A. En la **NTP-ISO-IEC-17799** en control **10.6.1 Controles de redes** indica que se debe garantizar la protección de la información en redes y fortalecer la infraestructura de soporte.

- La responsabilidad operacional para las redes no solo debe recaer sobre el área de informática, el personal debe comprometerse para el funcionamiento correcto de la misma.
- Se deben implantar controles definidos para proteger la confidencialidad y la integridad de la información que transita a través de las redes; adicionalmente también se puede tener la necesidad de controles especiales para conservar la disponibilidad de los servicios de la red y las computadoras conectadas.

B. Adicionalmente se citan algunas normas para una mejor estructura del cableado.

1. Norma Eia/Tia 568a - 568b

Esta norma surge de la revisión de la EIA/TIA 568A. La TIA/EIA-568-B intenta precisar políticas de implantar un diseño de sistema de cableado estructurado ideales para centros comerciales y edificios en entornos de campus. FAUBLA, VELEZ, MORAN (2011).

Esta norma se subdivida en:

- ANSI/TIA/EIA-568-B1: Esta norma nos indica el cableado que se debe utilizar de telecomunicaciones en edificios Comerciales. Esta norma nos indica los requerimientos y sugerencias en estructura, configuración, interfaces, instalación, parámetros de desempeño y verificación.
- TIA/EIA 568-B2: Esta norma nos ofrece requisitos generales para componentes de par tranzado balanceados.
- TIA/EIA 568-B3: Esta norma nos indica los componentes que se debe tener para un cableado, también la fibra óptica (cable, conectores, hardware de conexión, cordones, jumpers y equipo de prueba)

1.1.Servicio del área de trabajo

Es conveniente utilizar cables de conexión ya que cuando ocurra alguna variación en la conectividad, será mucho más sencillo realizar la conexión desde el área de trabajo a una nueva posición en sala de servidores. (FAUBLA, VELEZ, MORAN, 2011)

FAUBLA, VELEZ, MORAN (2001), nos indica que es recomendable cuando se va a utilizar un panel de conexión aplicar cables de par trenzado no blindado, par trenzado blindado, o, si se montan en lugares cerrados, conexiones de fibra óptica. Los UTP son los paneles de conexión más comunes (par trenzado no blindado). También se ha evidenciado que en las instalaciones comúnmente suceden casos que no se supervisan al personal de mantenimiento cuando realiza una conexión no autorizada como instalar un hub o hacer alguna conexión de cables en el circuito.

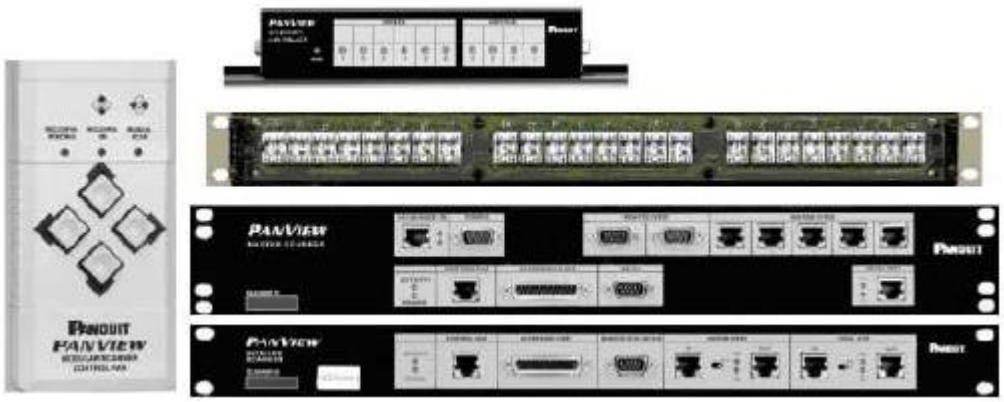


Figura N° 03. Panel de conexión

Fuente. (Faubla, Velez, Moran, 2011)

1.2.Cable de conexión UTP

Este cable es utilizado para conectar PC´s a la red, o switch. Generalmente un dispositivo de comunicaciones por ejemplo un hub o switch adyacente se conecta mediante un cable de interconexión cruzada. Los cables de interconexión cruzada utilizan

el plan de cableado T568-A en un extremo y el T568-B en el otro. FAUBLA, VELEZ, MORAN (2001)

Figura N° 04. Cable UTP para conexiones de red

Fuente. (Faubla, Velez, Moran, 2011)

1.3.Administración de cables

FAUBLA, VELEZ, MORAN (2001), indica que los dispositivos de administración de cables tienen como propósito tener un cableado ordenado a lo largo de su trayectoria, garantizando así la ausencia de daños y retorcimientos de los cables, reduciendo la cantidad de cables y cambiando al sistema de cableado.

Figura N° 05. Administración de cables tipo PANDUIT

Fuente. (Faubla, Velez, Moran, 2011)

1.4.Tipos de conexión cruzada

Por diversos motivos, regularmente las redes se encuentran en diversas salas de telecomunicaciones, de acuerdo a su distribución una red se encuentra dividida en varios pisos o edificios, teniendo en cuenta que la señal es débil cuando la distancia del área es mayor. En consecuencia, las salas de comunicaciones se encuentran ubicadas a distancias apropiadas dentro de la LAN para brindar interconexiones y conexiones cruzadas a los hub y switches, con el propósito de asegurar el rendimiento deseado de la red. (Faubla, Velez, Moran, 2011)

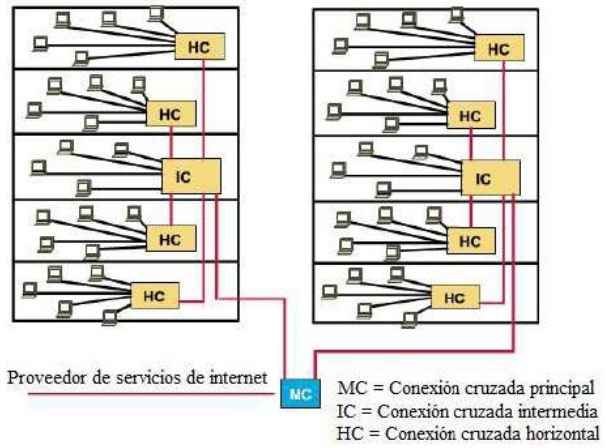


Figura N° 06. Administración de cables tipo PANDUIT

Fuente. (Faubla, Velez, Moran, 2011)

1.5.Conexiones

Faubla, Velez, Moran, (2011), nos indica que las conexiones más comunes son Cat 5e y Cat3. Para el Cat5e no es más que un jack el cual se conectará al cable; permitiendo el paso de la información, asimismo es considerada la opción más eficaz de todas, considerando que tiene un bajo costo y proporciona una velocidad de 1 Gb/s y un índice de transmisión de 100 MHz. Para cat3 simplemente es un conector RJ45 comúnmente

utilizado en telefonía, diseñado para transportar datos de hasta 10 Mbit/s, con un factible ancho de banda de 16 MHz. De igual manera todos los cables que se utilizan en todas áreas, estos deben de finalizar en un conector que cumpla con las necesidades específicas dentro de la norma con la terminación 568-a, y opcionalmente 568-B. (Faubla, Velez, Moran, 2011)

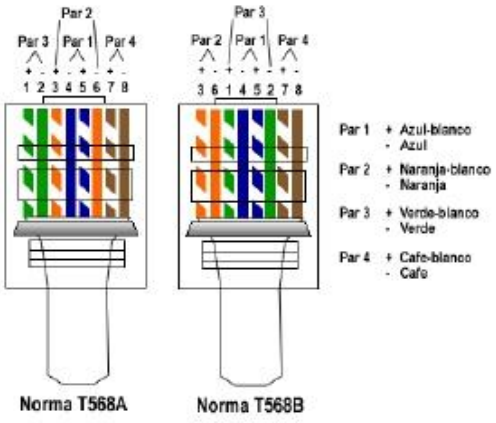


Figura N° 07. Configuración de la norma T568A y T568B

Fuente. (Faubla, Velez, Moran, 2011)

1.5.1. Cable

Es un medio de transporte para la información que viaja desde un punto emisor hasta un punto destinatario. (Faubla, Velez, Moran, 2011)

Los cables de cobre son el mejor conductor para transmitir señales eléctricas y los del tipo de fibra óptica se utilizan para la luz, ambos conductores son igual de buenos para transmitir energía. (Faubla, Velez, Moran, 2011)

1.5.1.1.Cable De Cobre

A continuación, los medios de transmisión más recomendados por el Instituto Americano Nacional de Estándares (ANSI), la Asociación de Industria de

Telecomunicaciones (TIA), y la Asociación de Industrias Electrónicas (EIA) (Faubla, Velez, Moran, 2011):

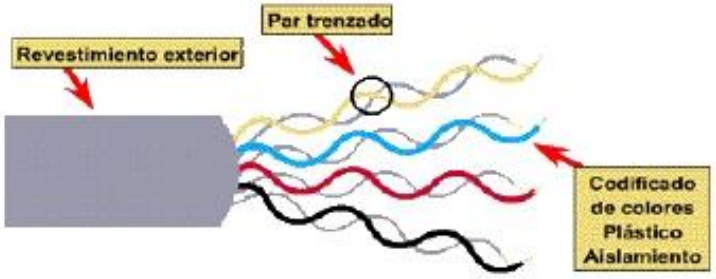


Figura N° 08. Par trenzado sin blindaje

Fuente. (Faubla, Velez, Moran, 2011)

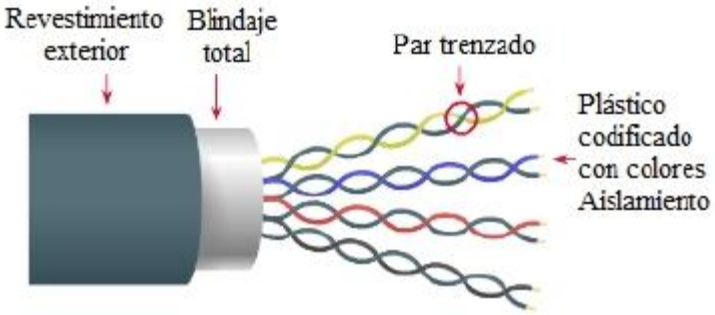


Figura N° 09. Par trenzado con blindaje

Fuente. (Faubla, Velez, Moran, 2011)

1.5.1.2.Fibra Óptica

Es un filamento de vidrio el cual contiene 125 micras de diámetro, que comparado con un cabello humano es mucho más delgado, este material tiene ciertas ventajas comparado con el cobre, cuenta con impulsos luminosos para una buena transmisión, ya que tiene un mejor soporte en tasas de transmisión altas, un mayor alcance en metros de

distancia y un mejor ancho de banda. (Faubla, Velez, Moran, 2011)

El material de fibra óptica está compuesto por lo siguiente:

- Núcleo: Es una hebra de vidrio que se encuentra en el centro de la fibra, por aquí viajan los pulsos de luz.
- Revestimiento: Es el vidrio que rodea el núcleo y previene que la luz escape del mismo.
- Cubierta: Es una capa de material plástico que cubre y protege la fibra.

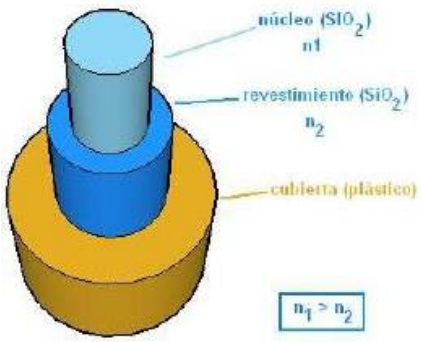


Figura N° 10. Composición de la fibra óptica.

Fuente. (Faubla, Velez, Moran, 2011)

1.6.Patch Cords

Llamados también con el nombre de latiguillos, son cables de distribución, conformados por un cable de cuatro pares trenzados y dos conectores RJ45 uno en cada extremo. Para que el conector RJ45 no pierda sus parámetros de capacidad debe contener cincuenta micrones de oro, estos patch cords se conectan al panel de parcheo o distribución funcionando como una interconexión dentro de la información, su principal función es la interconexión de toda la información, también utilizada para conectar de la salida de telecomunicaciones a la PC. (Faubla, Velez, Moran, 2011)

Figura N° 11. Conector RJ45.

Fuente. (Faubla, Velez, Moran, 2011)

Los servicios de los sistemas de telecomunicaciones se encuentran disponibles y ubicados en un rack, (telefonía, informática y otros servicios). Igualmente existen patch cord de material de cobre y de fibra óptica. (Faubla, Velez, Moran, 2011)

Figura N° 12. Patch cord de cobre.

Fuente. (Faubla, Velez, Moran, 2011)

Figura N° 13. Patch cord de fibra óptica.

Fuente. (Faubla, Velez, Moran, 2011)

1.7.Piso Falso

Conocido también como piso con acceso, con la forma de un piso elevado, está compuesto por una serie de placas que reposan en soportes de acero o aluminio fijados al piso del edificio. Usualmente las placas son de acero con madera laminada adherida, cubierta por vinilo o alfombra, estas pueden ser removibles dependiendo en el lugar donde se encuentran para poder alcanzar los cables del interior. Se debe de considerar que depende de la marca con la que se trabaje contiene concreto inyectado. (Faubla, Velez, Moran, 2011)

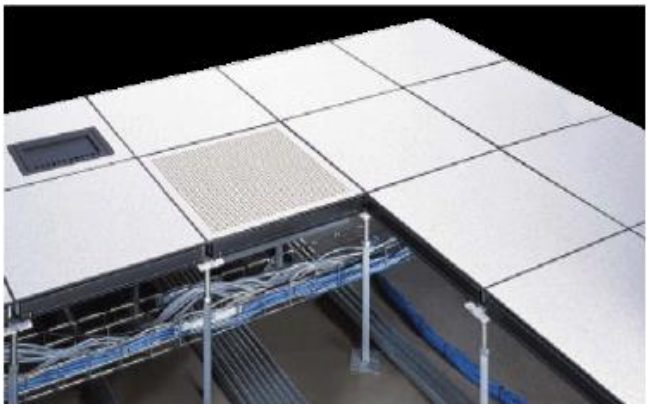


Figura N° 13. Canalización piso falso.

Fuente. (Faubla, Velez, Moran, 2011)

1.8.Bandejas Para Cables

Son de metal y existen diferentes tipos como: Ventilada, Cerrada, Abierta, Estacionaria, con fuente de poder etc. Su principal uso es ubicar equipos de gran tamaño incluyendo cualquier tipo de teclado, además sirve para acondicionar y tener un mejor orden con los cables. Es característico por ser de color negro ya que se encuentra ubicado dentro de un gabinete o en un rack, según el tipo de bandeja que se utilice dependerá su ubicación. (Faubla, Velez, Moran, 2011)

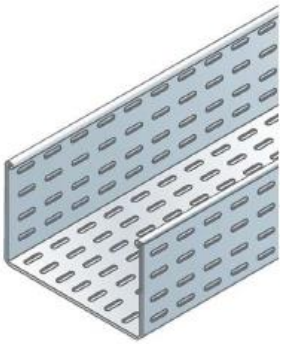


Figura N° 14. Bandeja ventilada para cables.

Fuente. (Faubla, Velez, Moran, 2011)

1.9.Ventajas

El cableado estructurado tiene los siguientes beneficios:

- Disminuye el costo de horas muertas, cuando ocurren problemas en un sistema. Un sistema de cableado estructurado ante un problema nos permite encontrar una solución rápidamente, ya que se encuentran ordenados y no es necesario utilizar cables adicionales. Como consecuencia no se produce dificultades en la continuidad de trabajo y un valor adicional.

- En un sistema de cableado no estructurado necesita que se actualice continuamente el cual provoca costos escalares. A diferencia de un sistema de cableado estructurado necesitará menos actualizaciones lo cual es beneficioso ya que mantendrá los costos controlados.
- Un sistema de cableado estructurado está diseñado para no depender del proveedor y de la aplicación a la vez, ya que para cualquier cambio en la red y equipamiento puede trabajarse con los mismos cables existentes. En conclusión, para un diseño adecuado de cableado estructurado es necesario utilizar un sistema normalizado y apropiado para una red, esto prolonga la vida útil más que otro componente ya que se promedia unos 10 de años de utilización.

4. Análisis y Discusión

De los antecedentes considerados para contrastar nuestros resultados obtenidos con los resultados de los mismos, se encontró gran coincidencia con el trabajo realizado por **Ramírez (2015),** quién al igual que con nuestro trabajó, logró eliminar o atenuar riesgos, luego de un análisis de los niveles de seguridad que se presentaban, para el desarrollo de políticas y mecanismos correctivos para disminuir cualquier tipo de incidentes de robo o perjuicio de información reservada y/o confidencial. También existe coincidencia en el uso del marco normativo COBIT basada en objetivos de control de la información y tecnologías relacionadas para las buenas prácticas de seguridad y control. Asimismo, se logró mantener la integridad y disponibilidad de los recursos informáticos de acuerdo a las necesidades y recursos financieros dispuestos para el análisis de seguridad.

Otro de los aportes, es el recibido por **Andrade (2016),** quien logró efectuar el cumplimiento de las políticas de seguridad de la información luego de haber sido elaboradas, definidas, documentadas y socializadas dentro de la institución, al igual que en nuestro caso, las cuales ayudan a la protección y salvaguardar la confidencialidad, integridad y disponibilidad de la información. El contraste radica en el uso de la norma ISO 27001:2013, pero también se coincide en el uso como referencia al estándar COBIT para la elaboración del instrumento de evaluación del sistema de gestión seguridad de la información. Como consecuencia, ambos trabajos, garantizan la continuidad de los servicios y permite gestionar el riesgo informático, llegándose a cumplir con los objetivos trazados.

Otro de los trabajos que dieron soporte a la presente investigación y, de paso al marco de gestión utilizado, fue el realizado por **Bojaca (2016), c**oncluyendo ambos, con una propuesta de sistema de gestión de seguridad de la información aplicando la Norma ISO/IEC 27001-27002 y Cobit respectivamente, que permitieron en ambos casos,

identificar las causas de los daños que se generan respecto a la manipulación inadecuada de la información, llegando a proponer un sistema de seguridad que mitigue riesgos y vulnerabilidades a los activos de información de las entidades respectivas.

En los antecedentes citados que se describe en este informe de tesis los autores narran que los proyectos de investigación que realizaron les sirvió de gran ayuda para empresas e instituciones, siendo su trabajo de investigación de gran apoyo para esta evaluación de seguridad de la red de datos el cual nos permitió evidenciar las diferentes debilidades y amenazas informáticas a las que se ven expuestas los activos de información del área de informática del Hospital Regional de Huacho por lo que es importante las medidas de seguridad para proteger los activos de información y garantizar el normal funcionamiento del Hospital. Aplicando la metodología MAIGTI se identificó deficiencias en la seguridad de hardware y software, estructura física de cableado y las condiciones en las que se encuentra el área de informática acceso no autorizado que son recurrentes por parte de los usuarios del hospital por lo que es necesario implementar las mejoras de políticas de seguridad propuestas en el presente proyecto.

5. Conclusiones y Recomendaciones

Conclusiones

1. Se logró planificar el proceso de evaluación de la seguridad de la red de datos del Hospital Regional de Huacho, llegando a evidenciar deficiencias de seguridad en las redes de datos de dicho hospital, presenta debilidades desde el punto de vista organizacional, primordialmente no tiene un Área específica de redes, del mismo modo no se realizan auditorías de sistemas, por lo que la obligación de la seguridad reincide en el personal del área de informática.
2. Se aplicó la metodología MAIGTI, bajo entorno Cobit en el proceso de evaluación de la seguridad de la red de datos, realizando una evaluación integral y detectando que no se ha implantado políticas, estándares y procedimientos adecuados ante cualquier tipo de incidentes de seguridad, lo que ocasiona dificultades al comenzar los procesos de recuperación luego de algún percance.
3. Se logró desarrollar las respectivas propuestas de mejora en relación a la seguridad de las redes de datos, garantizando la continuidad de los servicios, con la implantación de nuevos y eficientes métodos de control, teniendo un adecuado registro de datos de los usuarios, así como los antecedentes de cada usuario en el cual se podrá verificar el historial y los accesos otorgados al sistema.
4. Es importante hacer énfasis que siendo MAIGTI la metodología para una evaluación integral de la gestión de las tecnologías de la información fue utilizada como punto de partida para la elaboración de la presente investigación, se debe entender claramente las interrelaciones existentes entre los diversos objetivos de control para su correcta aplicación.

Recomendaciones

1. Se recomienda, una planificación periódica de auditoría a las redes de datos y la seguridad de los sistemas en forma anual, con formulación de objetivos, políticas, normas y procedimientos que permitan fortalecer el tema de la seguridad de la información identificando las debilidades de la organización y que procedimientos se van aplicar para la mejora continua.
2. Como sugerencia, recomendamos la metodología MAIGTI ya que trata temas específicos de seguridad, tales como seguridad en las redes de datos, seguridad en los equipos servidores o en las bases de datos, deben ser tratados sólo cuando se tenga la certeza que exista un marco de seguridad global, previamente establecido, que la sustente.
3. Se recomienda, evaluar nuevamente las recomendaciones planteadas acorde a los avances de tecnología y seguridad de la institución, capacitando al personal en la ejecución de las políticas establecidas y de las nuevas políticas a implementarse.

6. Referencias bibliográficas

Aceituno, V. (2007). Seguridad de la Información. México. Limusa Noriega Editores.

Alfaro, P (2008). Metodología para la Auditoría Integral de la Gestión de la Tecnología de Información.

Ampuero, C. (2011). Diseño de un Sistema de Seguridad de la Red de Datos para una compañía de seguros.

Bolívar, M. (2007). Seguridad de la Información dentro de la Banca Universal Venezolana. Trabajo de grado de Maestría no publicado. Universidad Metropolitana. Caracas. Venezuela.

Cardozo Arteada, C. y Zuluaga Contreras, M. (2010, Marzo,11) Aplicaciones de los estados financieros ISO 17799 27001 para el diagnóstico de la seguridad física y lógica en laboratorios de informática.

COBIT 4.1 (2007, IT Governance Institute)

Cueva Córdova, D. (2010, Marzo, 09) Estándar ISO 27001 Auditoria de sistemas.

Forouzan, B. (2002). Transmisión de Datos y Redes de Comunicaciones. (2ª Ed.).

Faubla, V.M. (2011) Implementación De Elementos Para Prácticas de Cableado Estructurado para el Laboratorio de Telecomunicaciones

Herrera, J. (2006). Auditoria a la Gestión de Seguridad de la Red de Datos del Swissotel basada en Cobit.

Instituto Nacional de Estadística e Informática, Colección de Seguridad de la Información.