UNIVERSIDAD SAN PEDRO

FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA INFORMÁTICA Y DE SISTEMAS

Evaluación de la Seguridad Física del Centro de Datos del Hospital Regional de Huacho

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

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE INGENIERO EN INFORMÁTICA Y DE SISTEMAS

Autora

Laos Juan de Dios, Catherine Shirley

Coautora

Condori León, Lizbet Pamela

Asesor

Dr. Martínez Carrión, Javier

Huacho– Perú

2019

INDICE

PALABRAS CLAVE

Tema	Evaluación de la Seguridad
Especialidad	Gestión

KEYWORDS

Theme	**Security Assessment**
Management	Specialty

LINEA DE INVESTIGACION

Sub área	Disciplina
2.2 Ingeniería eléctrica, electrónica e informática	Ingeniería de Sistema y Comunicaciones.

EVALUACION DE LA SEGURIDAD FÍSICA DEL CENTRO DE DATOS DEL HOSPITAL REGIONAL DE HUACHO

RESUMEN

La presente investigación se planteó como propósito evaluar la seguridad física del centro de datos del Hospital Regional de Huacho para determinar el cumplimiento de las normas y estándares de seguridad en el desarrollo de sus actividades.

Para verificar la seguridad física en el centro de datos del Hospital Regional de Huacho, se evaluaron 10 Procesos seleccionados de la Metodología para la Auditoría Integral de la Gestión de Tecnología de Información (MAIGTI), ya que esta metodología es la integración de diversos estándares que interrelacionados encuentra las causas de los problemas de manera más eficiente y se podrá proponer soluciones concretas.

Al finalizar esta evaluación se dieron las recomendaciones para la seguridad física en el centro de datos y los cambios que se requieran en el Hospital para lograr mejores resultados.

ABSTRACT

The purpose of this research was to evaluate the physical security of the data center of the Regional Hospital of Huacho to determine compliance with the safety norms and standards in the development of its activities.

To verify the physical security in the data center of the Regional Hospital of Huacho, 10 Processes selected from the Methodology for the Integral Audit of Information Technology Management (MAIGTI) were evaluated, since this methodology is the integration of various standards that interrelated finds the causes of the problems more efficiently and concrete solutions can be proposed.

At the end of this evaluation, recommendations were given for physical security in the data center and the changes required in the Hospital to achieve better results.

I. INTRODUCCIÓN

El presente proyecto consiste en proponer una Evaluación de la seguridad física del Centro de Datos del Hospital Regional de Huacho, la cual al concluir ayudará al Hospital a conocer su actual condición y opte por corregir las deficiencias encontradas. De los antecedentes encontrados se han abordado los trabajos más relevantes a esta investigación:

Narváez y Sevilla (2012), en su tesis "Auditoria Informática Física y Lógica a la Empresa Almacenes Americanos S.A.", realizaron el estudio con el objetivo de Ejecutar un plan de auditoría informática lógica y física de los sistemas de información y tecnologías de comunicación de la empresa Almacenes Americanos S.A, utilizando la metodología COBIT 4.1 para poder evaluar de forma particular cada proceso del negocio y así identificar fortalezas y debilidades en la gestión de procesos informáticos de dicha empresa del cual emplearon dos de los dominios: Adquisición e implementación, Entrega de servicios y soporte, para el desarrollo de la auditoría también hicieron uso de la metodología MAI(Metodologías de auditorías informática) la cual plantea que toda auditoría informática debe realizarse en las Siguientes fases: Preliminar, Justificación, Adecuación, Formalización, Desarrollo. Como resultado se hizo entrega a la alta gerencia del plan de auditoría para evaluar los controles que se plantearon, enfocados al área de operaciones.

También, Anansi y Paspuel (2013), en su tesis "Evaluación de la Gestión Informática de la Unidad de TI de la Cooperativa de Ahorro y Crédito TEXTIL 14 DE MARZO usando COBIT 4.1", se propuso en realizar la Evaluación de la Gestión Informática de la Unidad de Tecnología de Información de la Cooperativa usando como marco de referencia COBIT 4.1(Objetivos de Control para Información y Tecnologías relacionadas) para medir el nivel de madurez de los procesos. Una vez realizado la evaluación se proponen mejoras en los procesos analizados para optimizar así la gestión de Tecnologías de información que realiza el departamento de Sistemas.

Nogueira (2013), en su tesis "Procedimientos para la auditoría física y medio ambiental de un Data Center basado en la clasificación y estándar internacional TIER",

realizó el estudio con el objetivo de Diseñar un procedimiento de auditoría física y medio ambiental para centros de datos (Data Center) basado en la clasificación y estándar internacional TIER, con la finalidad de verificar las condiciones de seguridad de información con las que cuentan dichas instalaciones. Para la realización de esta tesis, se hizo uso de dos metodologías para tener distintos enfoques uno de ellos es Plan-Do-Check-Act, también llamada Ciclo de Deming basado en la mejora de calidad, y la otra metodología es COBIT 5.0 para la seguridad de información. Una vez realizadas las pruebas y con los resultados que se indican en el apartado se concluyó que los procedimientos fueron correctamente aplicados en la auditoría, permitiendo obtener así los resultados que demuestran la efectividad o deficiencia de los controles que se han implantado y que perjudican la seguridad y continuidad de operación.

Así mismo Viteri (2013), en su tesis" Evaluación Técnica de la Seguridad Informática del Data Center de la Brigada De Fuerzas Especiales No. 9 Patria", tuvo como objetivo realizar una evaluación técnica informática de las seguridades del Data Center de la Brigada "Patria", Para la evaluación se consideró como referencia los estándares ISO 27001 e ISO 27002 para identificar los riesgos que soportan los sistemas de información y tomar medidas apropiadas para controlarlos; se concluyó con un plan de Seguridad Informática, el mismo que servirá para mantener la información disponible, confiable y oportuna.

Lala y López (2014), en su tesis "Modelo de Evaluación y monitoreo del Cumplimiento de Controles de gestión Tecnológico para el Municipio del Distrito Metropolitano de Quito", tuvo como propósito el diseño de un modelo que apoye a gestionar el control y mejora continua en las actividades de las dependencias del Municipio basado en los estándares ISO 27000 e ISO 27002. Se realizó el análisis de la información recopilada de las revisiones de campo y encuestas, para determinar las vulnerabilidades y amenazas que tiene el área de tecnología. Una vez identificada la situación actual se hizo entrega del modelo de Evaluación y Monitoreo del Cumplimiento de Controles de gestión Tecnológico

Desde el punto de vista social, la evaluación de la seguridad física del centro de datos del Hospital Regional de Huacho, permite tener un adecuado nivel de control de riesgos, agilizando los procesos y de esta manera ser una entidad capaz de garantizar la seguridad de los usuarios y mantener la confidencialidad, integridad y disponibilidad de su información.

La presente investigación se justifica científicamente, porque se evalúa la gestión de la tecnología de información usando la Metodología para la auditoría integral de la gestión de la tecnología de información (MAIGTI).

La principal problemática que presentó el Hospital Regional de Huacho es que en el centro de datos, no se lleva un correcto control de los equipos informáticos. No existen controles de acceso al Centro de datos, permitiéndose el ingreso constante de practicantes de ingeniería y de personas ajenas al área para tratar asuntos personales; haciendo así la información de diversas áreas importantes para la entidad pública vulnerable y de fácil manipulación ya que esta información se guarda en servidores dentro del centro de datos.

Además, no se cuenta con un adecuado cronograma de mantenimiento, como consecuencia los equipos de cómputo se deterioran mucho más rápido. El centro de datos no cuenta con una adecuada infraestructura ni políticas de seguridad, claro ejemplo de ello es que no maneja una adecuada ventilación, se comparte el área con el mantenimiento de las PCs, en el caso de algún desastre, no se cuenta con las medidas de seguridad necesarias (señalización, extinguidor, etc.).

Ante la problemática encontrada, nos planteamos la siguiente interrogante: ¿Cómo evaluarla seguridad física del Centro de Datos del Hospital Regional de Huacho utilizando la metodología MAIGTI?

Para dar respuesta a la interrogante planteada, presentamos las conceptualizaciones y operacionalización de las variables que intervienen en la presente investigación:

Seguridad Física

"Aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial" (Huerta, 2000).

MAIGTI

Metodología para la auditoría integral de la gestión de Tecnología de información, tiene como objetivo evaluar la gestión de la tecnología de información en una organización, con el fin de identificar la probable pérdida de valor debido a fallas en los diversos procesos relacionado. (Alfaro,2008)

La Metodología para la auditoría integral de la gestión de Tecnología de información enlaza diversos conceptos como:

- Las buenas prácticas del gobierno corporativo de la gestión de las tecnologías de información (COBIT Control Objectives for Information and related Technologies de ISACA Information Systems Audit and Control Association).
- La gestión de los procesos del ciclo de vida de desarrollo de software (ISO/IEC 12207),
- las buenas prácticas de la gestión de la seguridad de la información (ISO/IEC 17799).
- La gestión de servicios de tecnología de información (ISO/IEC 20000 o ITIL, Information Technology Infrastructure Library)
- La gestión de proyectos del Project Management Institute(PMBOK Project Management BodyOfKnowledge)
- El proceso general de auditoría descrito en la norma ISO19011:2002.

En la Tabla1 se muestra la relación de cada procedimiento de MAIGTI con los estándares internacionales de calidad.

Esta metodología al integrar los diversos estándares podrá encontrar las causas de los problemas de manera más eficiente y se podrá proponer soluciones concretas para que

se mejore la generación de valor de las organizaciones, eliminando o minimizando las causas de los problemas, lográndose así que la mejora de la gestión de la tecnología de información. (Alfaro,2008)

Tabla 1 - Relaciones de los procedimientos de MAIGTI con los estándares internacionales.

	ESTÁNDARES INTERNACIONALES DE CALIDAD					
PROCEDIMIENTO	**COBIT**	**ISO/IEC 12207**	**ISO/IEC 17799**	**ISO/IEC 20000**	**PMBOK**	**ISO 19011**
P001	X	X	X	X	X	X
P002	X				X	
P003	X				X	
P004	X				X	
P005	X				X	
P006	X	X			X	
P007	X	X			X	
P008	X		X		X	
P009	X		X		X	
P010	X		X		X	
P011	X		X		X	
P012	X	X			X	
P013	X		X		X	
P014	X		X		X	
P015	X		X		X	
P016	X	X	X		X	
P017	X	X	X		X	
P018	X	X	X		X	

P019	X	X	X		X	
P020	X	X			X	
P021	X		X	X		
P022	X	X	X	X		
P023	X	X	X	X		
P024	X	X			X	
P025	X	X			X	
P026	X	X			X	
P027	X			X	X	
P028	X			X	X	
P029	X			X	X	
P030	X		X			
P031	X	X	X	X		
P032	X		X	X		
P033	X	X	X	X		
P034	X	X				
P035	X	X				
P036	X		X			
P037	X		X			
P038	X		X			
P039	X		X			
P040	X	X	X			
P041	X	X				
P042	X					

P043	X					
P044	X					
P045	X					
P046	X	X	X			
P047	X	X		X		
P048	X	X			X	
P049	X	X			X	
P050	X	X			X	
P051	X		X	X		
P052	X					
P053	X		X			
P054	X		X			
P055	X		X			
P056	X		X			
P057	X		X			
P058	X		X			
P059	X					
P060						X
P061						X
P062						X
P063	X		X			

Fuente: Alfaro Paredes

La metodología para la auditoría integral de la gestión de Tecnología de información comprende los siguientes elementos:

- Objetivo (la finalidad)
- Alcance (detalla lo que está incluido y lo que no está incluido)
- Entradas (requerimientos de información).
- Proceso de MAIGTI (evaluaciones a realizar)
- Salidas (Informe).

Asimismo, cada uno de los procedimientos para la evaluación de los principales objetivos de control dentro de los subprocesos de MAIGTI, comprende la siguiente estructura:

- Objetivo (la finalidad del procedimiento)
- Alcance (detalla lo que está incluido y lo que no está incluido en el procedimiento a realizarse)
- Entradas (requerimientos de información para ejecutar el procedimiento).
- Proceso (detalle de los pasos a seguir en el procedimiento).
- Salidas (hallazgos evidenciados como resultado de la ejecución del proceso).

Las actividades que comprenden el proceso de la metodología para la auditoría integral de la gestión de Tecnología de información, son las siguientes:

- Solicitar la documentación requerida.
- Evaluar los documentos recibidos.

Las ventajas de la aplicación de la metodología para la auditoría integral de la gestión de Tecnología de información son las siguientes: (Alfaro, 2008)

- Reduce la subjetividad al momento de determinar las observaciones a la gestión de las tecnologías de información, dado que se tienen listas de verificación concretas, las cuales no son tan dispersas o no se presentan en tanta cantidad como los objetivos de control de los estándares internacionales de la gestión de la tecnología de información.

- Permite identificar claramente las causas de los problemas relacionados a la gestión informática, dado que se puede analizar las interrelaciones de los diversos entes involucrados.

- Permite cuantificar los impactos de los problemas y sus causas, así como cuantificar los riesgos asociados a las ineficiencias en la gestión de las tecnologías de información.

- Dado que se enfoca en identificar las causas de manera más precisa, se puede realizar un adecuado diagnóstico y recomendaciones concretas para que se eliminen o mitiguen las causas.

- Luego de su aplicación, la gerencia de las tecnologías de información, se enfoca mejor hacia los puntos que requieren su atención.

Procedimientos de la Metodología para la Auditoria de la gestión Informática (Alfaro,2008)

- P002: Procedimiento para la auditoría de la Planificación Estratégica.

- P003: Procedimiento para la auditoría de los Planes Operativos.

- P004: Procedimiento para la auditoría de la Evaluación de Riesgos.

- P005: Procedimiento para la auditoría de la Planificación Estratégica de Tecnologías de Información.

- P006: Procedimiento para la auditoría de los Planes de Proyecto de Desarrollo de Sistemas de Información.
- P007: Procedimiento para la auditoría de los Planes de Proyecto de Compra de Sistemas de Información.
- P008: Procedimiento para la auditoría del Plan de Contingencias de Informática.
- P009: Procedimiento para la auditoría del Plan de Continuidad de Negocio.
- P010: Procedimiento para la auditoría del Plan de Seguridad de la Información.
- P011: Procedimiento para la auditoría del Plan de Licenciamiento de Software.
- P012: Procedimiento para la auditoría del Plan de Capacitación.
- P013: Procedimiento para la auditoría del Plan de Mantenimiento Preventivo de Hardware de Computadoras, Redes y Equipos Relacionados.
- P014: Procedimiento para la auditoría del Plan de Mantenimiento Correctivo de Hardware de Computadoras, Redes y Equipos Relacionados.
- P015: Procedimiento para la auditoría de la Planificación de Labores de Rutina relacionadas con las Tecnologías de Información.
- P016: Procedimiento para la auditoría del Plan de Calidad.
- P017: Procedimiento para la auditoría del Plan de Compras de Tecnologías de Información.
- P018: Procedimiento para la auditoría del Reglamento de Organización y Funciones.
- P019: Procedimiento para la auditoría del Manual de Organización y Funciones.

- P020: Procedimiento para la Evaluación del Currículum Vitae del personal de Tecnología de Información.

- P021: Procedimiento para la auditoría del Inventario de Hardware de Tecnología de Información.

- P022: Procedimiento para la auditoría del Inventario de Software de Base.

- P023: Procedimiento para la auditoría del Inventario de Sistemas de Información.

- P024: Procedimiento para la auditoría de las Solicitudes y Evaluaciones de Cotizaciones para las compras de hardware de computadoras, redes y equipos relacionados.

- P025: Procedimiento para la auditoría de las Solicitudes y Evaluaciones de Cotizaciones para las compras de software de base.

- P026: Procedimiento para la auditoría de las Solicitudes y Evaluaciones de Cotizaciones para las compras de sistemas de información.

- P027: Procedimiento para la auditoría de los contratos de compra de bienes y servicios, de hardware de computadoras, redes y equipos relacionados.

- P028: Procedimiento para la auditoría de los contratos para la compra de software de base.

- P029: Procedimiento para la auditoría de los contratos para la compra de sistemas de información.

- P030: Procedimiento para la auditoría de los contratos de seguros para las tecnologías de información.

- P031: Procedimiento para la auditoría de la metodología de desarrollo de sistemas de información.

- P032: Procedimiento para la auditoría de la metodología para la atención de requerimientos de soporte técnico.

- P033: Procedimiento para la auditoría de la metodología para la atención de requerimientos de desarrollo de sistemas de información.

- P034: Procedimiento para la auditoría de la documentación de los manuales técnicos de los sistemas de información.

- P035: Procedimiento para la auditoría de la documentación de los manuales de usuario de los sistemas de información.

- P036: Procedimiento para la auditoría de la arquitectura de la red de tecnologías de información.

- P037: Procedimiento para la auditoría de la seguridad de acceso a los sistemas de información.

- P038: Procedimiento para la auditoría de la seguridad de acceso a las carpetas en los servidores.

- P039: Procedimiento para la auditoría de los manuales de procedimientos de soporte técnico.

- P040: Procedimiento para la auditoría de los manuales de procedimientos de desarrollo de sistemas de información.

- P041: Procedimiento para la Revisión de los Formularios de Control de Entregables de Proyectos y Requerimientos de Desarrollo de Sistemas de información.

- P042: Procedimiento para el Seguimiento de Informes de Auditoría Interna.

- P043: Procedimiento para el Seguimiento de Informes de Auditoría Externa.

- P044: Procedimiento para la auditoría de las Certificaciones de Calidad de Tecnología de Información.

- P045: Procedimiento para la auditoría de la Evaluación de Desempeño del Área de Tecnología de Información.

- P046: Procedimiento para la auditoría de la Evaluación de Desempeño del Personal de Tecnología de Información.

- P047: Procedimiento para la Revisión de los Formularios de Control de Cambios en Proyectos de Compra o Desarrollo de Sistemas de Información.

- P048: Procedimiento para la Revisión de los Formularios de Control de Riesgos en Proyectos de Compra o Desarrollo de Sistemas de Información.

- P049: Procedimiento para la Revisión de los Formularios de Seguimiento de Avances en Proyectos de Compra o Desarrollo de Sistemas de Información.

- P050: Procedimiento para la auditoría del Control de Calidad de los Requerimientos de Compra o Desarrollo de Sistemas de Información.

- P051: Procedimiento para la auditoría del Control de Calidad de los Requerimientos de Soporte Técnico.

- P052: Procedimiento para Entrevistar a los usuarios de Tecnologías de Información.

- P053: Procedimiento para la auditoría de las Instalaciones Eléctricas de Equipos de Cómputo y Redes.

- P054: Procedimiento para la auditoría de la Seguridad de Acceso al Centro de Cómputo Principal.

- P055: Procedimiento para la auditoría de las Instalaciones del Centro de Cómputo Principal.

- P056: Procedimiento para la auditoría de la Seguridad de Acceso al Centro de Cómputo Alterno.

- P057: Procedimiento para la auditoría de las Instalaciones del Centro de Cómputo Alterno.

- P058: Procedimiento para la auditoría del Cableado de Redes de Datos.

- P059: Procedimiento para la auditoría del Cálculo de la Generación de Valor de los Proyectos.

- P060: Procedimiento para la Elaboración del Informe Preliminar.

- P061: Procedimiento para el Envío, Sustentación y Corrección del Informe Final.

- P062: Procedimiento para la Elaboración del Plan de Trabajo de la Auditoría.

- P063: Procedimiento para la Medición de la resistencia de la Puesta a tierra

La investigación tiene un alcance de carácter descriptivo, no es posible plantear una hipótesis debido a que no se intenta correlacionar o explicar casualidad de variables, por tal razón la hipótesis es implícita.

Entre los objetivos que buscamos en la presente investigación tenemos:

Como objetivo general, Evaluar la seguridad física del centro de datos del Hospital Regional de Huacho utilizando la metodología MAIGTI; y como objetivos específicos:

- Identificar la situación actual de la infraestructura tecnológica del centro de datos del Hospital Regional de Huacho.

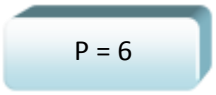
- Aplicar los procedimientos de evaluación para la seguridad física del centro de datos del Hospital Regional de Huacho en base a la metodología MAIGTI

- Realizar la documentación de los resultados de la evaluación para la seguridad física del centro de datos del Hospital Regional de Huacho

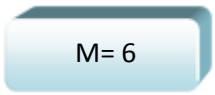
II. METODOLOGÍA DE TRABAJO

La presente investigación es de tipo descriptivo y de diseño no experimental, ya que los datos son obtenidos a través de técnicas de investigación para desarrollar la evaluación del centro de datos del Hospital Regional de Huacho.

La población es de 6 personas entre el personal técnico y administrativo, que laboran en el centro de datos del Hospital Regional de Huacho.



Para la muestra se tomará el 100% de la población.



La técnica e instrumento utilizado en la investigación es la siguiente:

Tabla2:técnica e instrumento de evaluación

Técnica	Instrumento
Encuesta	Cuestionario de Preguntas.
Observación	Visitas Presenciales

Fuente Propia

METODOLOGIA MAIGTI

FASES DE LA METODOLOGIA

Tabla3: Fases de la Metodología

FASES	**RESULTADOS**
Fase I: Planificación de la Evaluación	1.1. Plan de evaluación preliminar 1.2 Conocimiento del negocio 1.3 Identificación de área a evaluar 1.4 Estimación de tiempo para realizar la evaluación
Fase II: Ejecución de la evaluación	2.1Aplicación de herramienta e instrumento de evaluación. 2.2 Selección de los procesos MAIGTI aplicables a la evaluación 2.2 Ejecutar los procesos MAIGTI
Fase III: Comunicación de Resultados.	3.1 Informe de Evaluación (Anexo 2)

Fuente Propia

III. APLICACIÓN DE LA METODOLOGIA

FASE I: PLANIFICACIÓN DE LA EVALUACIÓN

1.1 Plan de evaluación preliminar

Antecedentes

El Hospital Regional de Huacho para el desarrollo de sus actividades utiliza herramientas informáticas y cuenta con un plan de seguridad con respecto a sus equipos, debido a la magnitud de sus actividades.

Objetivos de la evaluación

- Realizar una evaluación al centro de datos para identificar la situación actual.

- Realizar la ejecución del procedimiento de la seguridad física en el centro de datos.

- Elabora un informe de evaluación de la seguridad física del centro de datos.

Alcance

El alcance de la presente auditoria se enfoca a la evaluación del centro de datos**,** en las cuales se verificará la vulnerabilidad de los equipos y la información.

Recursos

Se realizarán las labores de investigación en el Hospital Regional de Huacho y en el domicilio de los investigadores.

- **Humanos**

Personal investigador:

Bach. Laos Juan de Dios, Catherine Shirley (Autora)

Bach. Condori León, Lizbet Pamela (Co Autora)

- **Materiales y equipos**

  Materiales:

01 Millar de papel bond A4 80gr

01 kit de útiles de escritorio

01 USB 16GB

Equipos:

01 Computadora Portátil LENOVO

01 Impresora Canon 2700

1.2 Conocimiento del negocio

Los requerimientos de información que maneja el Hospital Regional de Huacho han aumentado considerablemente desde sus inicios, debido a ello cada unidad usa y requiere tener tecnologías de la información.

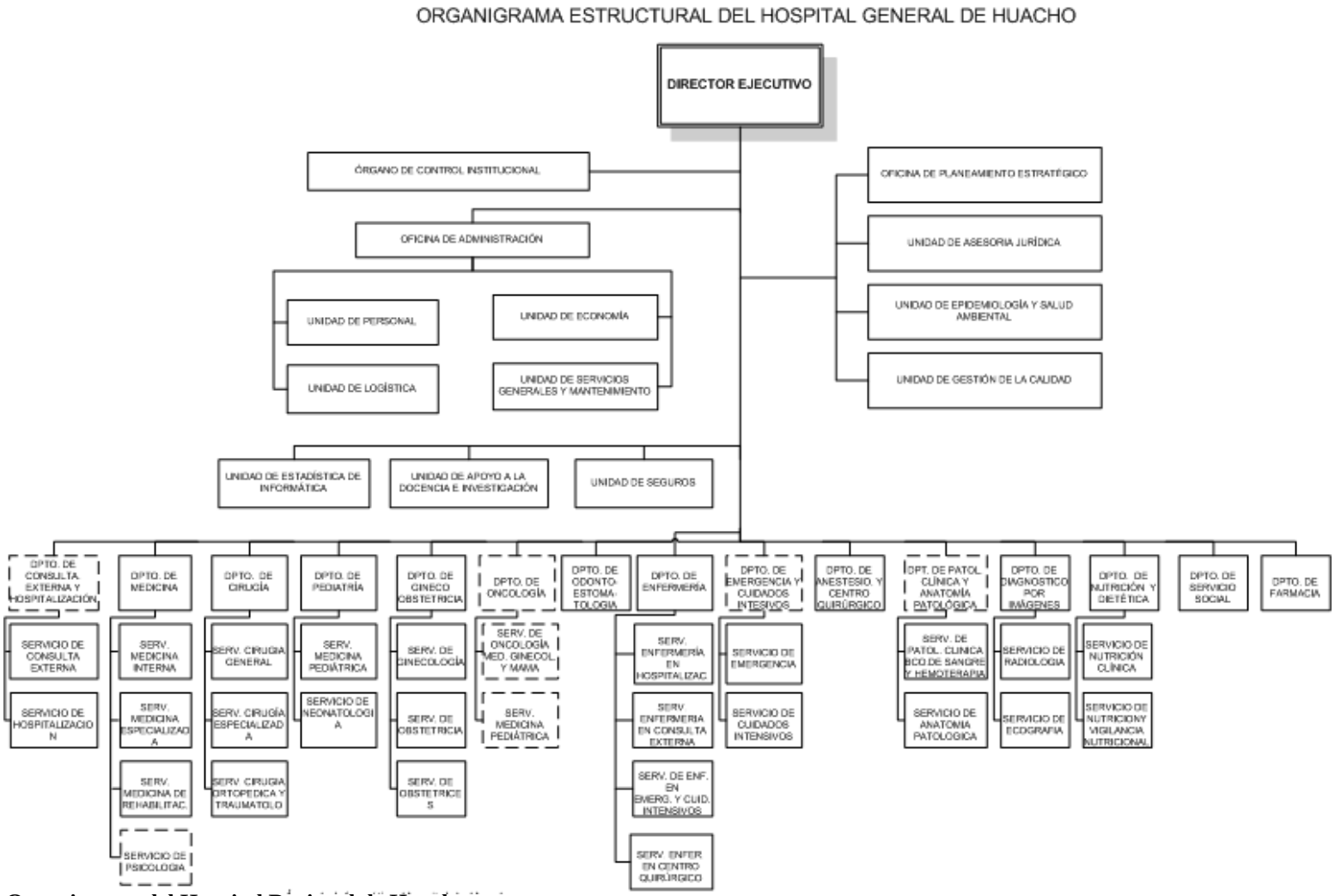


Figura 12: Organigrama del Hospital Regional de Huacho

Fuente: Hospital Regional De Huacho

1.3 Identificación de área a evaluar

Dado que toda la información de todas las unidades es almacenada en los servidores, hemos evaluado la seguridad física en el centro de datos del Hospital Regional de Huacho.

Toda la información recopilada se toma del área responsable, que en este caso es el área de Informática

Jefe del Área de Informática Bach. Jorge Alberto Sánchez Marcos

ORGANIGRAMA ESTRUCTURAL

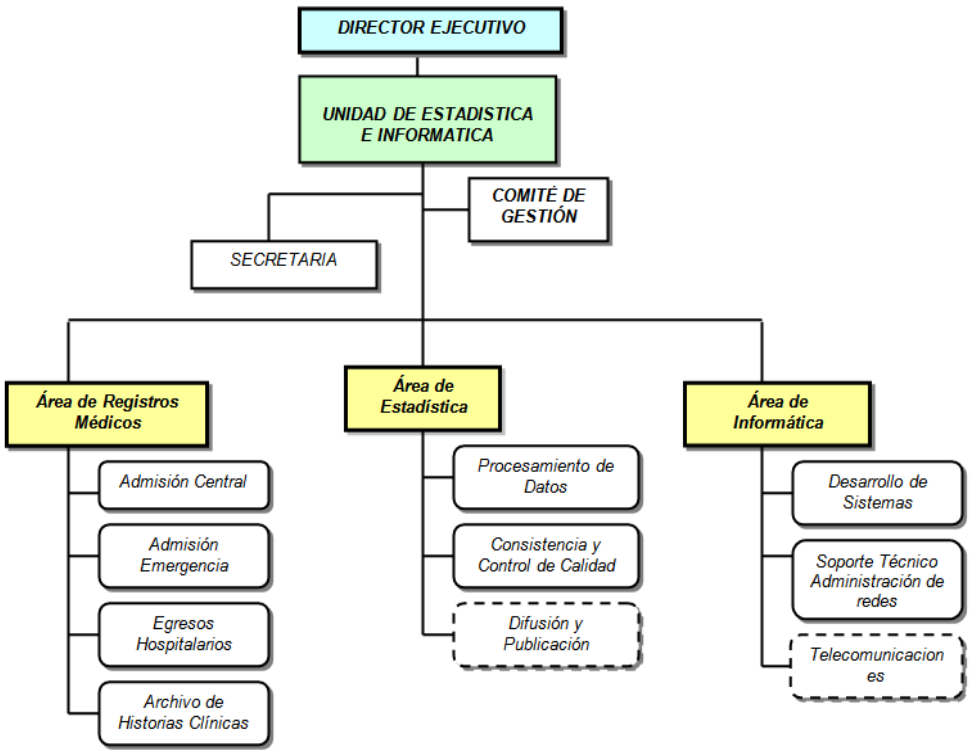


Figura 13: Organigrama Estructural

Fuente: Hospital Regional de Huacho

ORGANIGRAMA FUNCIONAL

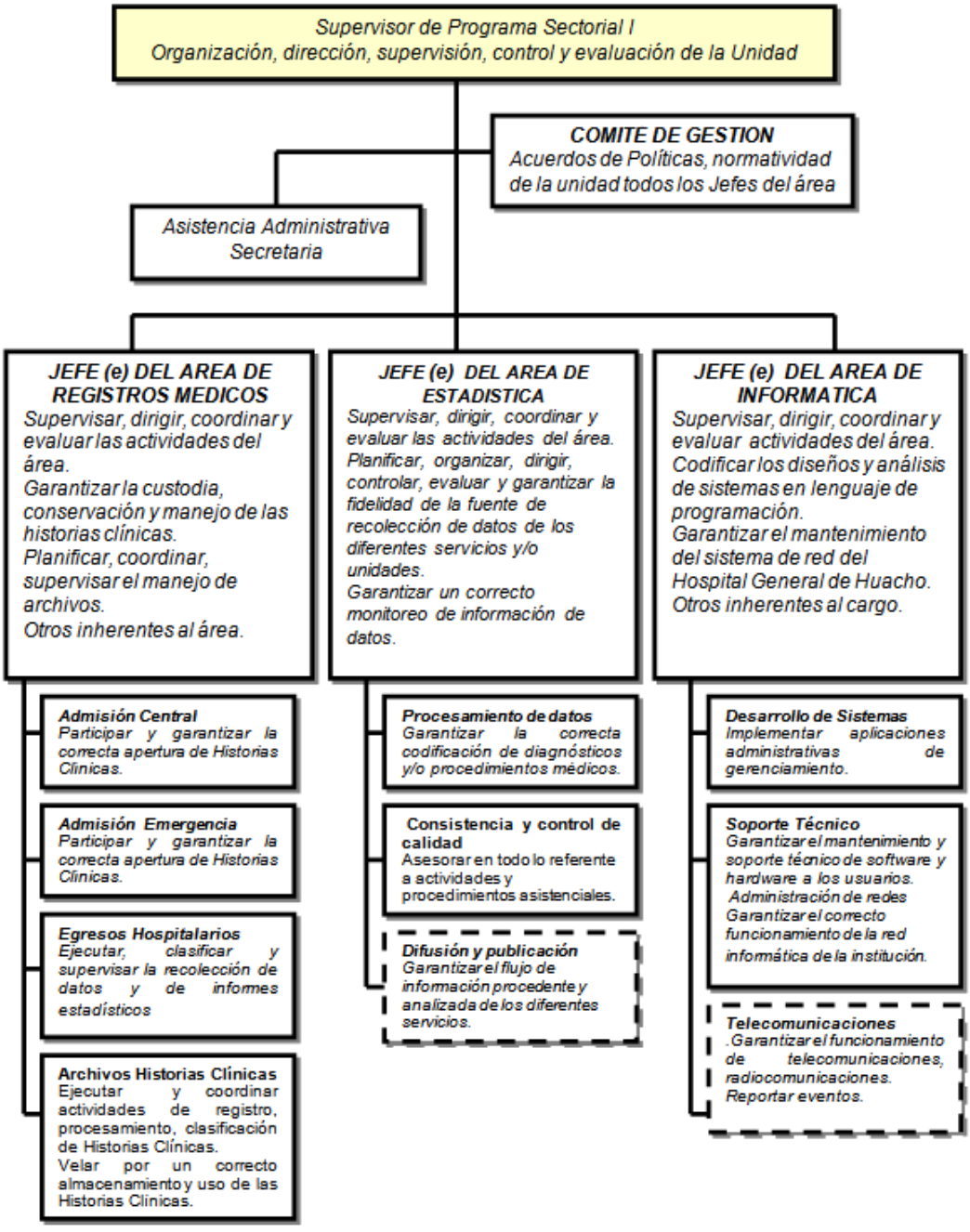


Figura 14: Organigrama Funcional

Fuente: Hospital Regional de Huacho

1.4 Estimación de tiempo para realizarla evaluación

El tiempo para el desarrollo de la evaluación fue de 4 meses:

Inicio: 4 de febrero del 2018

Término: 27 de mayo del 2018

Tabla4: Cronograma de la evaluación.

ACTIVIDADES	**Febrero**	**Marzo**	**Abril**	**Mayo**
Presentación	X			
Solicitar información	X			
Revisión y ejecución de los procedimientos de la evaluación		X	X	
Elaboración del informe final				X
Sustentación del informe final				X

Fuente Propia

FASE II: EJECUCION DE LA EVALUACION

2.1 Aplicación de herramienta e instrumento de evaluación

En esta etapa evaluamos todo lo referente al uso de las tecnologías de información dentro del hospital, lo cual nos ayudó a identificar la situación actual; a continuación, describimos los instrumentos utilizados:

Cuestionario

El Cuestionario aplicado a los trabajadores del área de informática y estadística, se detalla en el Anexo 1 y Anexo 2.

Visita Presenciales

A través de las visitas presenciales pudimos observar las condiciones en que se labora, como prueba tomamos fotografías que se adjuntan en el Anexo 4.

2.2 Selección de los procedimientos MAIGTI a aplicar

Resultaría demasiado extenso el aplicar la evaluación en todos los procedimientos que abarca la metodología MAIGTI, por lo que se seleccionaron los siguientes procedimientos tomando como referencia resultados de nuestras observaciones y cuestionario.

P010: Procedimiento para la auditoría del Plan de Seguridad de la Información.

P013: Procedimiento para la auditoría del Plan de Mantenimiento Preventivo de Hardware de Computadoras, Redes y Equipos Relacionados.

P014: Procedimiento para la auditoría del Plan de Mantenimiento Correctivo de Hardware de Computadoras, Redes y Equipos Relacionados.

P021: Procedimiento para la auditoría del Inventario de Hardware de Tecnología de Información.

P032: Procedimiento para la auditoría de la metodología para la atención de requerimientos de soporte técnico.

P036: Procedimiento para la auditoría de la arquitectura de la red de tecnologías de información.

P053: Procedimiento para la auditoría de las Instalaciones Eléctricas de los Equipos de Cómputo y Redes.

P054: Procedimiento para la auditoría de la Seguridad de Acceso al Centro de Cómputo Principal.

P055: Procedimiento para la auditoría de las Instalaciones del Centro de Cómputo Principal.

P058: Procedimiento para la auditoría del Cableado de Redes de Datos.

2.2 Ejecutar los procesos MAIGTI:

P010: PROCEDIMIENTO PARA LA AUDITORIA DEL PLAN DE SEGURIDAD DE LA SEGURIDAD DE LA INFORMACIÓN

OBJETIVO

El objetivo de este procedimiento fue analizar y evaluar el proceso de ejecución del Plan de Seguridad de la Información del Hospital Regional de Huacho, con el fin de identificar fallas en los diversos procesos involucrados.

ALCANCE

En el alcance del procedimiento se incluyó:

- La revisión del documento del Plan de Seguridad de la Información.
- La verificación de la asignación de presupuesto, cronogramas y responsabilidades para la ejecución del Plan de Seguridad de la Información.

En el alcance del procedimiento no se incluyó:

La evaluación de los ataques de intrusos u otros problemas de seguridad de la información que hubieran ocurrido durante el período en evaluación.

ENTRADAS

Para realizar esta evaluación, se solicitó la siguiente información:

- Plan de Seguridad de la Información.
- Cronogramas para la ejecución del Plan de Seguridad de la Información, con su respectiva asignación de responsabilidades.
- Presupuesto detallado para la ejecución del Plan de Seguridad de la Información.

PROCESO

Se reviso el documento de Plan de Seguridad de la Información, verificando que se haya detallado acciones para proteger al Hospital de lo siguiente:

- Acceso de Personas:
  - Identificación de las personas que ingresan al centro de datos.
  - Claves de seguridad en las puertas de acceso del centro de datos.
  - Correcto estado de las puertas de acceso del centro de datos.
- Suministro de energía eléctrica de los equipos.
  - Estabilización de la línea de voltaje de los equipos.
  - Uso de equipos UPS en el centro de datos.
  - Existencia de un pozo de tierra.
  - Mantenimiento periódico del pozo de tierra.
- Protección contra incendios.
  - Extinguidores para incendios.
  - Vigencia de los extinguidores de incendios.
  - Suficiencia en cantidad de extinguidores de incendios.
  - Detectores de humo.
  - Correcto funcionamiento de las alarmas contra incendios.
  - Inexistencia de material inflamable en los centros de datos, tales como madera, ropa, cuadernos, etc.
- Condiciones ambientales de las salas de cómputo.
  - Correcto funcionamiento de los equipos de aire acondicionado.
  - Correcto funcionamiento de los medidores de humedad y temperatura.
  - Cableado desordenado con riesgo que lo pisen y se retiren los cables de los “switches”.

- Fallas en el hardware.
  - Fallas en disco.
  - Fallas en la tarjeta principal.
- Traslado de Información.
  - Normas sobre el traslado de documentos físicos fuera de los locales de la organización.
  - Normas para el ingreso de dispositivos de memoria dentro de la organización.
  - Normas para la salida de dispositivos de memoria fuera de la organización.

Verificamos la asignación de presupuesto, cronogramas y responsabilidades para la ejecución del Plan de Seguridad de la Información.

SALIDAS

Al desarrollar esta evaluación encontramos las siguientes observaciones:

- El Hospital tiene un Plan de Seguridad de la Información, pero no esta especificado el presupuesto y el cronograma.
- Errores en la seguridad física:
  - No se tiene ningún control de las personas que ingresan al centro de datos.
  - La Puerta del centro de datos no cuenta con clave de seguridad.
  - No existe mantenimiento periódico al pozo a tierra.
  - No hay extinguidores de incendios
  - No existe detectores de humo.
  - Las alarmas contra incendios no funcionan.
  - Dentro del centro de datos existe material inflamable.
  - El equipo de aire acondicionado no es el adecuado. Cada cierto tiempo los operadores apagan el aire acondicionado cuando trabajan en el mismo ambiente.
  - No existe medidores de humedad y temperatura.

- El cableado se encuentra muy desordenado, con riesgo que lo pisen y se salgan los cables de red de los switches y ocurra interrupciones en el sistema para algunos usuarios.
- No existe piso técnico o "falso piso" para el cableado.
- Los operadores trabajan en el mismo ambiente físico donde se encuentran los equipos del centro de datos.
- En el plan no se especifica normas sobre el traslado de documentos, el ingreso y salida de dispositivos de memoria.

P013: PROCEDIMIENTO PARA LA AUDITORÍA DEL PLAN DE MANTENIMIENTO PREVENTIVO DE HARDWARE DE COMPUTADORAS, REDES Y EQUIPOS RELACIONADOS

OBJETIVO

El objetivo de este procedimiento fue analizar y evaluar el proceso de ejecución del Plan de Mantenimiento Preventivo de Hardware de Computadoras, Redes y Equipos Relacionados en el Hospital Regional de Huacho, con el fin de identificar fallas en los diversos procesos involucrados.

ALCANCE

El alcance del procedimiento incluyó:

La revisión del Plan de Mantenimiento Preventivo del Hardware de Computadoras, Redes y Equipos Relacionados.

En el alcance del procedimiento no se incluyó:

La evaluación del Plan de Mantenimiento Correctivo de Hardware de Computadoras, Redes y Equipos Relacionados.

ENTRADAS

Para realizar esta evaluación, se solicitó la siguiente información:

- Inventario del hardware de computadoras, redes y equipos relacionados.
- Listado del hardware de computadoras, redes y equipos relacionados, que requieran mantenimiento preventivo.
- Informes de los últimos mantenimientos preventivos que se haya realizado sobre los equipos.
- Cronograma para la ejecución de las actividades del Plan de Mantenimiento Preventivo del Hardware de Computadoras, Redes y Equipos Relacionados.
- Presupuesto detallado para la ejecución de las actividades del Plan de Mantenimiento Preventivo del Hardware de Computadoras, Redes y Equipos Relacionados.

PROCESO

- Revisamos el documento del Plan de Mantenimiento Preventivo del Hardware de Computadoras, Redes y Equipos Relacionados Verificamos que contenga:
  - Listado de equipos que necesitan mantenimiento preventivo.
  - Criterios para evaluar y priorizar las necesidades de mantenimiento preventivo.
  - Presupuesto, Cronograma y Asignación de Responsabilidades.
- Verificamos que las listas de equipos para el mantenimiento preventivo estén incluidas en el inventario de equipos total. En la lista de equipos debe estar detallado:
  - Equipos que forman parte de la computadora o están directamente conectados a ella.
  - Equipos de red.
  - Equipos relacionados a la energía eléctrica

- Equipos relacionados a las condiciones ambientales.
- Equipos relacionados a la protección contra incendios.
- Equipos relacionados a la seguridad.

❖ Verificamos que se haya determinado los criterios para la evaluación y priorización de las necesidades de mantenimiento preventivo.

❖ Verificamos que se haya determinado el personal que realizara los mantenimientos preventivos.

❖ Verificamos la asignación del presupuesto, cronogramas y responsabilidades para la ejecución de Plan de Mantenimiento Preventivo del Hardware de Computadoras, Redes y Equipos Relacionados.

SALIDAS

Al desarrollar esta evaluación encontramos las siguientes observaciones:

❖ El Hospital si cuenta con un Plan de Mantenimiento Preventivo del Hardware de Computadoras, Redes y Equipos Relacionados, de la cual no se encuentra bien estructurado y no se cumple con el lineamiento propuesto en el Plan.
❖ El Hospital omite realizar mantenimiento preventivo de algunos equipos críticos (cajas de cuchillas, pozo a tierra, ups, ventiladores, alarmas contra incendio).
❖ No existe un cronograma para realización del mantenimiento preventivo de los equipos del centro de datos.
❖ En el plan no se detalla la asignación del personal encargado para el mantenimiento preventivo.

P014: PROCEDIMIENTO PARA LA AUDITORÍA DEL PLAN DE MANTENIMIENTO CORRECTIVO DE HARDWARE DE COMPUTADORAS, REDES Y EQUIPOS RELACIONADOS

OBJETIVO

El objetivo de este procedimiento fue analizar y evaluar la ejecución del Plan de Mantenimiento Correctivo de Hardware de Computadoras, Redes y Equipos Relacionados en el Hospital Regional de Huacho, con el fin de identificar fallas en los diversos procesos involucrados.

ALCANCE

En el alcance del procedimiento se incluyó:

La revisión del documento del Plan de Mantenimiento Correctivo de Hardware de Computadoras, Redes y Equipos Relacionados

En el alcance del procedimiento no se incluyó:

La evaluación del Plan de Mantenimiento Preventivo de Hardware de Computadoras, Redes y Equipos Relacionados.

ENTRADAS

Para realizar esta evaluación, se solicitó la siguiente información:

- Inventario del hardware de computadoras, redes y equipos relacionados.
- Listado del hardware de computadoras, redes y equipos relacionados, que requieran mantenimiento correctivo, clasificado de acuerdo a quién le debe realizar dicho mantenimiento.
- Informes de los últimos mantenimientos correctivos que se haya realizado sobre los equipos.
- Cronogramas para la ejecución de las actividades del Plan de Mantenimiento Correctivo de Hardware de Computadoras, Redes y Equipos Relacionados.

- Presupuesto detallado para la ejecución de las actividades del Plan de Mantenimiento Preventivo de Hardware de Computadoras, Redes y Equipos Relacionados.

PROCESO

Verificamos que las listas de equipos para el mantenimiento correctivo estén incluidas en el inventario de equipos total.

En la lista de equipos debe estar detallado:

- Equipos que forman parte de la computadora o están directamente conectados a ella.
- Equipos de red.
- Equipos relacionados a la energía eléctrica
- Equipos relacionados a las condiciones ambientales.
- Equipos relacionados a la protección contra incendios.
- Equipos relacionados a la seguridad.

Revisamos que el documento del Plan de Mantenimiento Correctivo de Hardware de Computadoras, Redes y Equipos Relacionados contenga lo siguiente:

- Listado de equipos que necesitan mantenimiento correctivo.
- Criterios para la priorización de las necesidades de mantenimiento preventivo.
- Priorización de las necesidades de mantenimiento correctivo.
- Presupuesto, Cronograma y Asignación de Responsabilidades.

SALIDAS

Al desarrollar esta evaluación encontramos las siguientes observaciones:

- El Hospital Regional de Huacho cuenta con un Plan de Mantenimiento Correctivo del Hardware de Computadoras, Redes y Equipos Relacionados, pero dentro de ella no se encuentra una lista de equipos que necesitan mantenimiento correctivo, ni un cronograma de ejecución, por lo tanto, se omite realizar mantenimiento de algunos equipos críticos; los cuales terminan malográndose por esta negligencia.
- No se realizan informes del mantenimiento correctivo realizado.

P021: PROCEDIMIENTO PARA LA AUDITORIA DEL INVENTARIO DE HARDWARE DE TECNOLOGIA DE INFORMACIÓN.

OBJETIVO

El objetivo de este procedimiento fue analizar y evaluar el Inventario de Hardware de Tecnología de la Información del Hospital Regional de Huacho, con el fin de identificar fallas en los diversos procesos involucrados.

ALCANCE

En el alcance del procedimiento se incluyó:

La revisión del documento del Inventario de Hardware de Tecnología de la Información.

La revisión de procedimientos relativos a altas, bajas y mejoras en el hardware de Tecnología de la Información.

La revisión y Evaluación de la correcta contabilización del Inventario de Hardware de Tecnología de información.

En el alcance del procedimiento no se incluyó:

La evaluación del inventario de software.

ENTRADAS

Inventario de hardware de tecnología de información

PROCESO

- Revisamos detalladamente el documento de Inventario de hardware de tecnología de información y verificamos se encuentren los siguientes tipos de hardware:
  - Equipos que forman parte de la computadora o están directamente conectados a ella.
  - Equipos de red.
  - Equipos relacionados a la energía eléctrica
- Revisamos los procedimientos relativos a altas, bajas y transferencias en el hardware de Tecnología de Información.

SALIDAS

Al desarrollar esta evaluación encontramos las siguientes observaciones:

- El Hospital Regional de Huacho no tiene un Inventario de hardware de tecnología de información completo.
- No existen procedimientos establecidos relativos a altas, bajas y transferencias de hardware, por tanto, no se conserva adecuadamente los equipos fuera de uso, provocando que se deterioren y ya no sirvan.

P032: PROCEDIMIENTO PARA LA AUDITORIA DE LA METODOLOGIA DE ATENCIÓN DE REQUERIMIENTOS DE SOPORTE TECNICO.

OBJETIVO

El objetivo de este procedimiento fue analizar y evaluar la metodología para la atención de requerimientos de soporte técnico del Hospital Regional de Huacho, con el fin de identificar fallas en los diversos procesos involucrados.

ALCANCE

En el alcance del procedimiento se incluyó:

- La revisión de la metodología de atención de requerimientos de soporte técnico del Hospital Regional de Huacho.

En el alcance del procedimiento no se incluyó:

- La evaluación de la metodología de atención de requerimientos de desarrollo de sistemas de información.

ENTRADAS

- Metodología de atención de requerimientos de soporte técnico.

PROCESO

- Revisamos detalladamente la metodología de atención de requerimientos de soporte técnico la cual debe incluir los siguientes procesos:
  - Recibir del requerimiento.
  - Clasificar el requerimiento.
  - Definición de criterios para priorizar la atención de requerimientos.
  - Definir procesos para la atención de requerimientos de cada tipo.
  - Verificar la correcta ejecución de los procesos para la atención de requerimientos de cada tipo.
  - Registrar los procesos en la atención de requerimientos de cada tipo.
  - Consultar al usuario acerca de la calidad de la atención recibida.

SALIDAS

Al desarrollar esta evaluación encontramos las siguientes observaciones:

- No existe un proceso definido para la recepción de los requerimientos.
- No existen criterios claramente definidos para priorizar la atención de los requerimientos de soporte técnico.
- No existe un registro de la atención ni verificación de la calidad de la atención brindada.

P036: PROCEDIMIENTO PARA LA AUDITORIA DE LA ARQUITECTURA DE LA RED DE TECNOLOGIAS DE INFORMACIÓN

OBJETIVO

El objetivo de este procedimiento fue analizar y evaluar la Arquitectura de la Red de Tecnologías de Información del Hospital Regional de Huacho, con el fin de identificar fallas en los diversos procesos involucrados.

ALCANCE

En el alcance del procedimiento se incluyó:

- La revisión detallada del documento de la Arquitectura de la Red de Tecnologías de Información.

- La verificación física de la Arquitectura de la Red de Tecnologías de Información.

En el alcance del procedimiento no se incluyó:

- La evaluación de los sistemas de información que operan sobre la Arquitectura de la Red de Tecnologías de Información.

ENTRADAS

Para la ejecución de esta evaluación, se solicitó la siguiente información:

- Documento de la Arquitectura de la Red de Tecnologías de Información.

PROCESO

- Revisamos detalladamente el documento de la Arquitectura de la Red de Tecnologías de Información.
  - Revisamos los siguientes tipos de hardware en el centro de datos:
    - Equipos de red: routers, firewalls, switches, hubs, cableado, etc. Ej.: que el cableado este colocado ordenadamente en estantes y en pisos técnicos (falsos pisos).
    - Puntos de la Red de Datos. Ej: cercanías a motores y puntos conectores a la red de energía eléctrica.
    - Equipos Servidores.
    - Equipos Clientes.
- Se verificó físicamente que se encuentren todos los componentes descritos en el documento de la Arquitectura de la Red de Tecnologías de Información.

SALIDAS

Al desarrollarse esta evaluación encontramos las siguientes observaciones:

- El Hospital no cuenta con un documento formal sobre la Arquitectura de la Red de Tecnologías de Información.
- El cableado no está colocado ordenadamente en estantes (“racks”)

P053: PROCEDIMIENTO PARA LA AUDITORIA DE LAS INSTALACIONES ELECTRICAS DE LOS EQUIPOS DE COMPUTO Y REDES.

OBJETIVO

El objetivo de este procedimiento fue analizar y evaluar las instalaciones eléctricas de los equipos de cómputo y redes del Hospital Regional de Huacho, con el fin de identificar fallas en los diversos procesos involucrados.

ALCANCE

En el alcance del procedimiento se incluyó:

- La revisión de condiciones de tomacorrientes de equipos de cómputo.
- La revisión de condiciones de equipos de suministro de energía eléctrica: UPS y generador.
- La revisión de la frecuencia de los mantenimientos a las instalaciones de puesta a tierra.

En el alcance del procedimiento no se incluyó:

La revisión técnica detallada de las instalaciones eléctricas.

ENTRADAS

Para la realización de esta evaluación el Hospital Regional de Huacho se solicitó la siguiente información:

- Plano de instalaciones eléctricas de equipos de cómputo. Considerar: pozo de tierra, caja de control de la corriente eléctrica, tomacorrientes de equipos de cómputo y equipos de suministro de energía eléctrica (UPS y generador).
- Informes técnicos de mantenimientos preventivos y correctivos anteriores.

PROCESO

Las actividades que se realizaron en la evaluación fueron las siguientes:

- Se revisó de las condiciones de los tomacorrientes de los equipos de cómputo:

- Los tomacorrientes de los equipos de cómputo deben tener línea a tierra.
- Los tomacorrientes deben encontrarse sin deterioros físicos.

❖ Se revisó de las condiciones de equipos de suministro de energía eléctrica. Verificar:

- Estado del UPS.
- Estado del generador de corriente eléctrica.
- Cableado no dañado.
- Cableado aislado de manera que no se afecte con las condiciones del entorno.
- Debe estar empotrado con canaletas.

❖ Se revisó la frecuencia de los mantenimientos a las instalaciones de puesta a tierra.

SALIDAS

Al desarrollar esta evaluación encontramos las siguientes observaciones:

❖ El Hospital no realiza mantenimiento al pozo de tierra.

❖ Los tomacorrientes se encuentran con deterioros físicos.

❖ El cableado se encuentra disperso debe estar empotrado con canaletas.

P054: PROCEDIMIENTO PARA LA AUDITORÍA DE LA SEGURIDAD DE ACCESO AL CENTRO DE CÓMPUTO PRINCIPAL

OBJETIVO

El objetivo de este procedimiento fue analizar y evaluar la seguridad de acceso al centro de datos del Hospital Regional de Huacho, con el fin de identificar fallas en los diversos procesos involucrados.

ALCANCE

En el alcance del procedimiento se incluyó:

- La revisión del acceso por la puerta principal del piso donde se encuentra el centro de datos.

- La revisión del acceso de la entrada al centro de datos.

En el alcance del procedimiento no se incluyó:

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

ENTRADAS

Para esta evaluación se solicitó la siguiente información:

- Listado de personas que tienen relación con el permiso de acceso a las instalaciones del centro de datos.

- Capacitación otorgada al personal de seguridad en la puerta principal del Hospital, referente a los criterios para decidir si se permite o no el ingreso de una persona.

- Informes sobre incidentes relativos a la seguridad de acceso.

PROCESO

- Se reviso el acceso al piso donde se encuentra el centro de datos, verificando lo siguiente:

  - Existencia de personal encargado de recepción en el piso.
  - Criterios impartidos al personal de recepción del piso para permitir el acceso a las instalaciones.
  - Existencia de dispositivo para colocar clave de seguridad para el ingreso.
  - Estado de la puerta que permite el acceso al piso (abierta o cerrada).

- Revisamos el acceso por la entrada al centro de datos.

  - Existencia de personal encargado de controlar el acceso.

- Criterios impartidos al personal encargado para decidir si una persona ingresa o no al centro de datos.
- Estado de la puerta que permite acceso al centro de datos (abierta o cerrada).
- Registro de entrada y salida en el centro de datos.

SALIDAS

- Al Verificar el acceso al piso donde se encuentra el centro de datos encontramos lo siguiente:
  - Dado que es un Hospital continuamente se permite el ingreso al piso donde se encuentra el centro de datos ya sea por alguna atención o tramite.
  - No existe un personal encargado en la recepción de piso donde se encuentra el centro de datos.
  - No existe ningún dispositivo para colocar clave de seguridad para el ingreso al piso donde se encuentra el centro de datos.

- Se revisó el acceso de la entrada al centro de datos y se encontró lo siguiente:

  - La puerta de acceso al centro de datos no tiene ningún dispositivo para colocar clave de seguridad.
  - No se lleva un registro de quiénes ingresan o salen del centro de datos, así como la hora en que se produjo la entrada o la salida.

P055: **PROCEDIMIENTO PARA LA AUDITORIA DE LAS INSTALACIONES DEL CENTRO DE COMPUTO PRINCIPAL**

OBJETIVO

El objetivo de este procedimiento fue analizar y evaluar el estado de las instalaciones del centro de datos del Hospital Regional de Huacho, con el fin de identificar fallas en los diversos procesos involucrados.

ALCANCE

En el alcance del procedimiento se incluyó:

- La verificación de la existencia de los equipos de acuerdo al inventario actualizado.
- La verificación del funcionamiento de los equipos de cada tipo.
- La verificación del cumplimiento de las medidas de seguridad del centro de datos.

En el alcance del procedimiento no se incluyó:

La revisión técnica de los equipos del centro de datos.

ENTRADAS

Al momento de la evaluación se solicitó la siguiente información:

- Inventario actualizado de los equipos del centro de cómputo principal.
- Reportes de mantenimientos realizados sobre los equipos.

PROCESO

- Verificamos la existencia de los equipos del centro de datos, de acuerdo al inventario.
- Verificamos el funcionamiento de los equipos de cada tipo: routers, switches, hubs, cableado, racks, computadoras servidores, equipo de aire acondicionado, alarma contra incendios, equipos de aire acondicionado, UPS, estabilizadores, supresores de picos, etc.
- Verificamos el cumplimiento de las medidas de seguridad del centro de datos. Seguir el procedimiento relativo a la seguridad física que se detalla en el documento P010: "Procedimiento para la Auditoría del Plan de Seguridad de la Información".

SALIDAS

Al desarrollar esta evaluación encontramos las siguientes observaciones:

- Dado que el inventario no se encuentra completo existen muchos equipos que no figuran en el documento.
- El funcionamiento del equipo de aire acondicionado no es el adecuado, y la alarma contraincendios no se encuentra en funcionamiento.
- El Hospital tiene equipos que no usa en el centro de datos, además de material inflamable como cajas, bolsas, cuadernos, etc.
- Existen problemas de seguridad de la información diversos. Ver sección "Salidas", en el documento P010: "Procedimiento para la Auditoría del Plan de Seguridad de la Información".

P058: PROCEDIMIENTO PARA LA AUDITORIA DEL CABLEADO DE REDES DE DATOS

OBJETIVO

El objetivo de este procedimiento fue analizar y evaluar el cableado de redes de datos del Hospital Regional de Huacho, con el fin de identificar fallas en los diversos procesos involucrados.

ALCANCE

En el alcance del procedimiento se incluyó:

La revisión de la ubicación y condiciones del cableado de redes de datos.

En el alcance del procedimiento no se incluye:

La revisión técnica de los equipos a los cuales se conectan los cables de redes de datos.

ENTRADAS

Para la realización de esta evaluación se solicitaron la siguiente información:

- Plano del cableado de redes de datos de la organización.
- Informes técnicos de mantenimientos preventivos y correctivos anteriores.

PROCESO

- Se verificó la ubicación del Cableado.
  - El cableado no puede estar expuesto a altas temperaturas. Evitar que esté expuesto al sol.
  - El cableado no puede estar cerca de motores ni cables de corriente eléctrica.
- Se verificó las condiciones del Cableado:
  - El cableado no debe estar dañado.
  - El cableado debe estar colocado ordenadamente en canaletas.
  - El cableado debe conectarse ordenadamente a los "racks",

SALIDAS

Al desarrollar la evaluación encontramos las siguientes observaciones:

- El cableado del centro de cómputo se encuentra disperso sin ningún orden, con el consecuente riesgo que el personal lo pise y se puedan generar interrupciones en el servicio para los usuarios de las redes de cómputo.
- No se usa adecuadamente los "racks", pese a estar disponibles.
- El cableado de redes de datos se coloca de manera muy cercana a los cables de corriente eléctrica.
- El cableado de redes de datos no se encuentra ubicado apropiadamente dentro de canaletas.
- El cableado está expuesto al sol.

IV. ANÁLISIS Y DISCUSIÓN

Se realizó el análisis de la información recopilada mediante los instrumentos de investigación, al igual que Lala y López (2014), para identificar la situación actual del centro de datos del Hospital, determinándose las vulnerabilidades y amenazas que presenta.

Por otra parte, en forma concordante con Viteri (2013), se realizó una evaluación al centro de datos de una entidad del estado, para tomar medidas apropiadas para controlar los riesgos que tiene, y de esta manera mantener la información disponible confiable y oportuna**.**

Al igual que Narváez y Sevilla (2012), se evaluó la seguridad física, ya que es un aspecto muchas veces olvidado, estableciendo las amenazas y determinaron la urgencia de proteger los activos de información manejados en la empresa.

En concordancia con Nogueira (2013), no se tomó en cuenta la seguridad lógica del centro de datos, ya que se estableció como punto de evaluación la seguridad física, para que la información esté disponible y resguardada de la mejor manera.

Al igual que Anansi y Paspuel (2013), primero se identificó la situación actual de la organización, luego se seleccionaron los procesos para la ejecución de la evaluación, en nuestro caso se usaron los procedimientos de la metodología MAIGTI, para finalmente analizar los resultados y dar las respectivas conclusiones y recomendaciones

V. CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES:

1. Al identificar la situación actual se determinó que no se han tomado acciones referentes a la seguridad física en el Centro de Datos del Hospital Regional de Huacho.

2. Al evaluar los 10 procedimientos de la metodología MAIGTI, se encontraron fallas en los diversos procesos involucrados.

3. Por último se concluye que no existe un claro plan para la seguridad física del centro de datos del Hospital Regional de Huacho.

RECOMENDACIONES:

1. Se propone la verificación, corrección y actualización de los procesos donde se presenta vulnerabilidad de acuerdo a la evaluación desarrollada.

2. El hospital debe considerar establecer evaluaciones periódicas al centro de datos, ya que después de haber aplicado la Metodología MAIGTI, los resultados no fueron favorables, comprobándose que la infraestructura tecnológica no es segura y la información en ella es vulnerable.

3. El Hospital debe de estar preparado para cualquier riesgo que ocurra, por ello se debe monitorear el cumplimiento de los procedimientos y emprender acción donde los procesos no funcionan efectivamente, de esta manera buscamos soluciones y mejoras para mantener la seguridad física del centro de datos.

REFERENCIAS BIBLIOGRÁFICAS

Alfaro(2008).Metodología para la auditoría integral de la gestión de la tecnología de información Recuperado de: http://tesis.pucp.edu.pe/repositorio/handle/123456789/1048

Anansi y Paspuel (2013), en su tesis "Evaluación de la Gestión Informática de la Unidad de TI de la Cooperativa de Ahorro y Crédito TEXTIL 14 DE MARZO usando COBIT 4.1". Recuperado de: http://bibdigital.epn.edu.ec/handle/15000/6672

Lala y López (2014)." Modelo de Evaluación y monitoreo del Cumplimiento de Controles de gestión Tecnológico para el Municipio del Distrito Metropolitano de Quito" Recuperado de: http://repositorio.espe.edu.ec/xmlui/handle/21000/9755?show=full

Narváez y Sevilla (2012).Auditoria Informática Física y Lógica a la Empresa Almacenes Americanos S.A. Tesis de Titulo. Universidad Centroamericana, Managua, Nicaragua. Recuperado de:http://165.98.12.83/556/1/UCANI3501.PDF

Nogueira (2013). Procedimientos para la auditoría física y medio ambiental de un Data Center basado en la clasificación y estándar internacional TIER. Tesis de Titulo. Pontificia Universidad católica del Perú, Lima, Perú. Recuperado de: http://tesis.pucp.edu.pe/repositorio/bitstream/handle/123456789/4978/nogueira_jocelyne_procedimientos_auditoria_fisica_medio_ambiental_data_center_clasificacion_estandar_internacional_tier.pdf?sequence=1

Rodríguez (2017). Evaluación de la seguridad del Centro de datos del Poder Judicial del Santa, Chimbote. Recuperado de: Universidad San Pedro, Lima, Perú.

Viteri (2013), en su tesis" Evaluación Técnica de la Seguridad Informática del Data Center de la Brigada De Fuerzas Especiales No. 9 Patria". Recuperado de: http://repositorio.espe.edu.ec/xmlui/handle/21000/6811

Wail (2004). **Auditoria de Seguridad Física Lógica en el Sistema de Información del Departamento de Sistemas de la Honorable Alcaldía Municipal de Oruro. Tesis de título. Universidad Técnica de Oruro, Oruro, Bolivia.** Recuperado de:http://postgrado.uto.edu.bo/tesis/facultad-de-ciencias-economicas-financieras-y-administrativas/carrera-de-contaduria-publica/875-auditoria-de-seguridad-fisica-logica-en-el-sistema-de-informacion-del-departamento-de-sistemas-de-la-honorable-alcaldia-municipal-de-oruro.html

ANEXO 1: ENTREVISTA
ENTREVISTA A LOS USUARIOS DEL CENTRO DE DATOS DEL HOSPITAL REGIONAL DE HUACHO

UNIVERSIDAD PRIVADA SAN PEDRO

FACULTAD DE INGENIERIA

ESCUELA DE INGENIERIA DE INFORMATICA Y SISTEMAS

INTRODUCCION:

La siguiente encuesta está elaborada con la finalidad de recopilar información sobre la seguridad fisca en el centro de datos del hospital regional de huacho.

Preguntas:

1. ¿Existe un documento donde se especifique las políticas de seguridad de la información?

   Si ( ) No ( )

2. ¿Existe un plan de mantenimiento preventivo y correctivo de los equipos?

   Si ( ) No ( )

3. ¿Se registran los accesos de personas a las áreas donde se encuentran los equipos servidores?

   Si ( ) No ( )

4. ¿A usted se le brinda capacitación por parte del Hospital Regional de Huacho acerca de seguridad de la información?

   Si ( ) No ( )

5. ¿Puede identificar a las personas que no trabajan en el Hospital Regional de Huacho?

   Si ( ) No ( )

6. ¿Has observado que algún compañero ha ingerido algún alimento cuando se encuentra en el centro de datos del Hospital Regional de Huacho?

   Si ( ) No ( )

7. ¿Todos los empleados portan su identificación visible durante su permanencia en el centro de datos?

   Si ( ) No ( )

8. ¿Se cuenta con servicio de vigilancia, personas y/o videocámara en el centro de datos?

   Vigilancia( ) Video Cámara ( ) Ninguno ( )

9. En el centro de datos existe alarma para:

   Robot ( ) Fuego ( ) Ninguno ( )

10. ¿Existen extintores en el Centro de Datos?

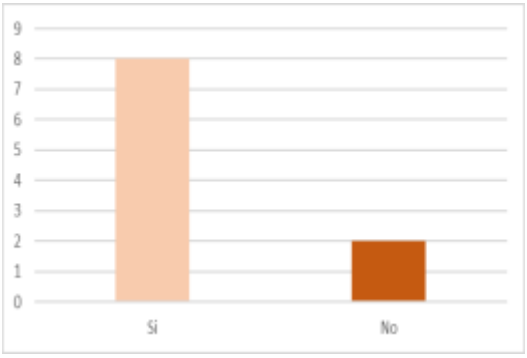
    Si ( ) No ( )

11. ¿Existen material inflamable dentro del Centro de Datos?

    Si ( ) No ( )

ANEXO 2: RESULTADOS DE LAS ENCUESTAS

1. ¿Existe un documento donde se especifique las políticas de seguridad de la información?

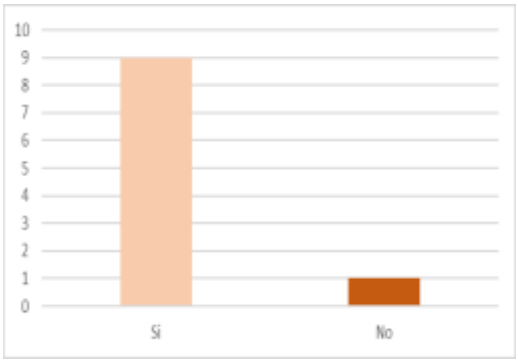


Análisis: En el grafico podemos apreciar que del 100% de la encuesta el 80% de los trabajadores saben que el Hospital Regional de Huacho cuenta con un documento de políticas de seguridad de la información y el 20% desconoce de este documento.

Figura 1: Grafico Documento de Políticas de Seguridad

Fuente: Elaboración Propia

2. ¿Existe un plan de mantenimiento preventivo y correctivo de los equipos?

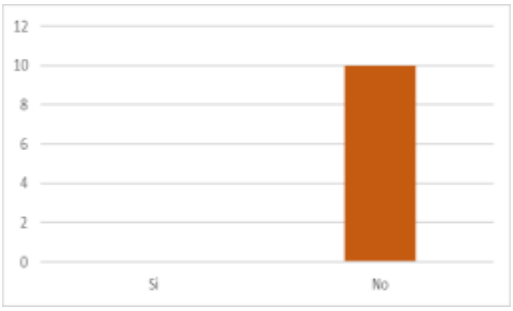


Análisis: En el grafico podemos apreciar que del 100% de la encuesta el 90% de los trabajadores saben que el Hospital Regional de Huacho cuenta con un plan de mantenimiento preventivo y correctivo de los equipos y el 10% desconoce este plan.

Figura 2: Grafico Plan Mantenimiento Preventivo y Correctivo

Fuente: Elaboración Propia

3. ¿Se registran los accesos de personas a las áreas donde se encuentran los equipos servidores?

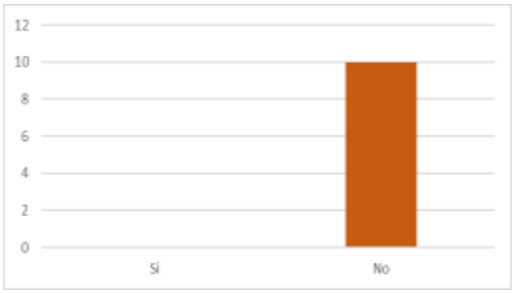


Análisis: En el grafico podemos apreciar que el 100% de la encuesta afirma que no existe un control de accesos.

Figura 3: Grafico Registro de Accesos

Fuente: Elaboración Propia

4. ¿A usted se le brinda capacitación por parte del Hospital Regional de Huacho acerca de seguridad de la información?

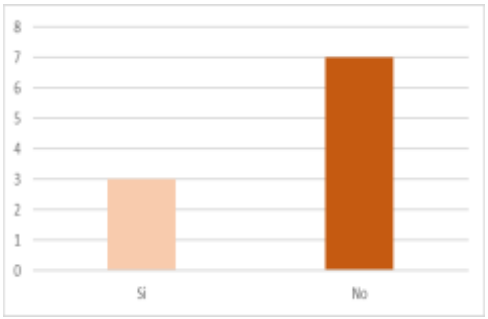


Análisis: En el grafico podemos apreciar que el 100% de la encuesta afirma que no se realiza capacitaciones por parte del hospital.

Figura 4: Grafico Capacitación de Seguridad de la Información

Fuente: Elaboración Propia

5. ¿Puede identificar a las personas que no trabajan en el Hospital Regional de Huacho?

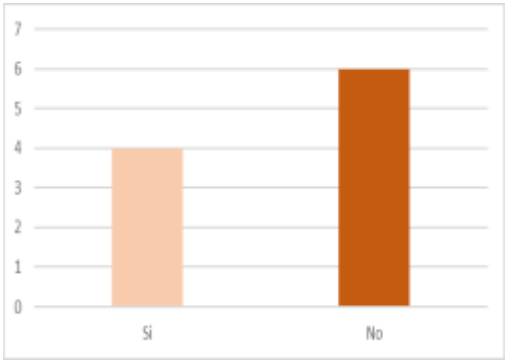


Análisis: En el grafico podemos apreciar que del 100% de la encuesta el 70% de los trabajadores no pueden identificar a las personas que no trabajan en el Hospital Regional de Huacho y el 30% afirma si identificarlos.

Figura 5: Grafico Identificación de Personas

Fuente: Elaboración Propia

6. ¿Has observado que algún compañero ha ingerido algún alimento cuando se encuentra en el centro de datos del Hospital Regional de Huacho?

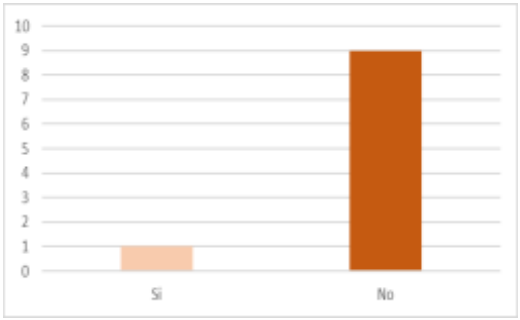


Análisis: En el grafico podemos apreciar que del 100% de la encuesta el 60% de los trabajadores afirma no haber visto ingerir alimento alguno dentro del centro de datos y el 40% afirma si haber observado la ingesta de alimentos en esta área.

Figura 6: Grafico Ingesta de Alimentos

Fuente: Elaboración Propia

7. ¿Todos los empleados portan su identificación visible durante su permanencia en el centro de datos?

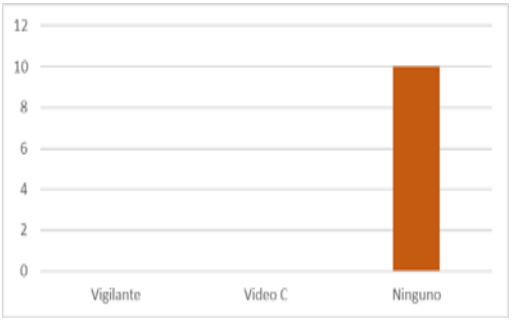


Análisis: En el grafico podemos apreciar que del 100% de la encuesta el 90% de los encuestados afirma no visualizar el carnet de identificación de los trabajadores y el 10% afirma si haber observado el uso de ello.

Figura 7: Grafico Identificación Visible

Fuente: Elaboración Propia

8. ¿Se cuenta con servicio de vigilancia, personas y/o videocámara en el centro de datos?



Análisis: En el grafico podemos apreciar que el 100% de los encuestados afirman que no existe ningún servicio de vigilancia en el centro de datos.

Figura 8: Grafico Servicio de Vigilancia

Fuente: Elaboración Propia

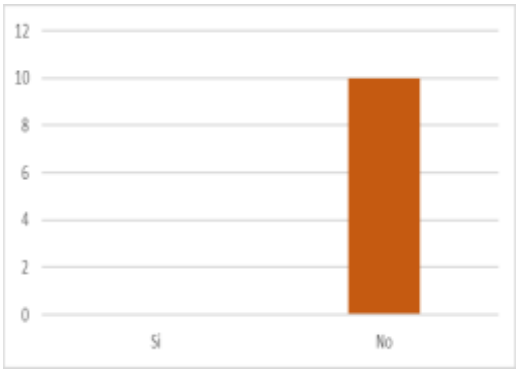
9. En el centro de datos existe alarma para:

Análisis: En el grafico podemos apreciar que el 100% de los encuestados afirman que no existe ningún tipo alarma.

Figura 9: Grafico de Alarmas

Fuente: Elaboración Propia

10. ¿Existen extintores en el Centro de Datos?

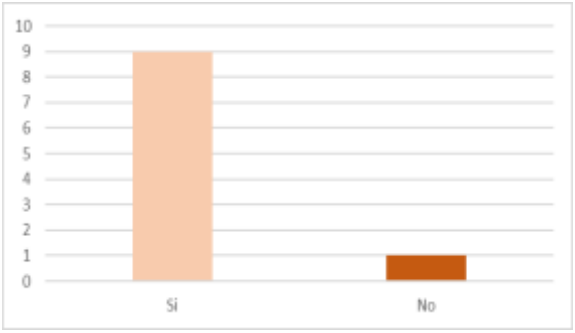


Análisis: En el grafico podemos apreciar que el 100% de los encuestados afirman que no existe ningún extintor.

Figura 1: Grafico de Existencia de Extintores

Fuente: Elaboración Propia

11. ¿Existen material inflamable dentro del Centro de Datos?



Análisis: En el grafico podemos apreciar que del 100% de los encuestados el 90% afirma que existe material inflamable dentro del Centro de Datos, mientras que el 10% afirma que no existe.

Figura 1: Grafico de Existencia de Material Inflamable

Fuente: Elaboración Propia

ANEXO 3: INFORME FINAL

1. Objetivo

Evaluar la seguridad física del centro de datos del hospital regional de huacho

2. Alcance

El periodo de la evaluación abarco del 4 de febrero a 27 de mayo

3. Responsable

Jefe del área: Bach. Jorge Alberto Sánchez Marcos

4. Equipo de Evaluación:

Laos Juan de Dios, Catherine Shirley

Condori León, Lizbet Pamela

5. Hallazgos Potenciales

- No se tiene ningún control de las personas que ingresan al centro de datos.
- Los operadores trabajan en el mismo ambiente físico donde se encuentran los equipos del centro de datos.
- El inventario de hardware se encuentra desactualizado.
- No existen procedimientos establecidos relativos a altas, bajas y transferencias de hardware, por tanto, no se conserva adecuadamente los equipos fuera de uso, provocando que se deterioren y ya no sirvan
- El cableado del centro de cómputo se encuentra disperso sin ningún orden, con el consecuente riesgo que el personal lo pise y se puedan generar interrupciones en el servicio para los usuarios de las redes de cómputo.

- No se realiza periódicamente los mantenimientos preventivos y correctivos a los equipos informáticos.

6. Conclusiones:

- Como resultado de la evaluación podemos manifestar que hemos cumplido con evaluar la seguridad física del centro de datos del Hospital Regional de Huacho.
- El Centro de datos presenta deficiencias sobre el cumplimiento de los estándares de seguridad física.
- El personal no está debidamente capacitado.
- Existe un plan de seguridad de información incompleto, el cual no lo usan ni como referencia a sus procedimientos.

7. Recomendaciones:

N° PROC.	NORMA DE VERIFICACIÓN	RECOMENDACIÓN
10	ISO/IEC 17799 PMBOK	Se debe tener un plan de seguridad donde se especifique todos los procesos a realizar con su respectivo cronograma y asignación de responsabilidades, ya que este proporciona dirección y soporte a la seguridad de información. Realizar constantes capacitación sobre la seguridad de información.
13	COBIT ISO/IEC 17799 PMBOK	Debe existir un inventario actualizado para identificar los equipos a los que se les va realizar un mantenimiento preventivo. El Plan de mantenimiento preventivo debe tener claros criterios de priorización para su ejecución. El Plan de mantenimiento preventivo debe contar con presupuesto, cronograma y asignación de responsabilidades.
14	COBIT ISO/IEC 17799 PMBOK	Debe existir un inventario actualizado para identificar los equipos a los que se les va realizar un mantenimiento correctivo. El Plan de mantenimiento correctivo debe tener claros criterios de priorización para su ejecución. El Plan de mantenimiento correctivo debe contar con presupuesto, cronograma y asignación de responsabilidades.

21	COBIT ISO/IEC 17799 ISO/IEC 20000	Verificar que el inventario este totalmente actualizado e incluya todos los equipos. Definir los procesos de bajas y altas de los equipos de tecnología información.
32	COBIT ISO/IEC 17799 ISO/IEC 20000	Se debe implementar la metodología de atención de requerimientos de soporte técnico, donde se incluya sus principales procesos (recepción, clasificación, priorización, ejecución y control de calidad).
36	COBIT ISO/IEC 17799	El hospital debe contar con un documento formal sobre la arquitectura de la red de tecnología de información.
53	COBIT ISO/IEC 17799	El hospital debe contar con un plano de instalaciones eléctricas donde se considere el pozo a tierra, cajas de control, tomacorrientes, ups entre otros. Realizar un mantenimiento preventivo y correctivo para su óptimo funcionamiento.
54	COBIT ISO/IEC 17799	Definir e implementar procedimientos para otorgar, limitar y revocar el acceso al centro de datos. El acceso debe justificarse, autorizarse, registrase y monitorearse. Esto aplica para todas las personas, incluyendo personal, visitantes o cualquier tercera persona.
55	COBIT ISO/IEC 17799	Se debe mejorar la infraestructura del centro de datos. El hospital debe implementar un lugar específico donde se realice el mantenimiento de los equipos, así como para guardar los equipos en desuso. Se debe tener actualizado el inventario de hardware, para poder evaluar el estado y funcionamiento de cada equipo dentro de las instalaciones del centro de datos.
58	COBIT ISO/IEC 17799	Tomar las medidas necesarias para la ubicación del cableado, con esto se contribuirá a mejorar su condición. Algunos de los puntos a tomar en cuenta son que el cableado no puede estar expuesto al sol, debe estar ordenado en canaletas, no debe estar cerca a otros cables de corriente eléctrica, entre otros.

27 de mayo de 2018

_____ _____

Condori León Lizbet Pamela Laos de Juan Dios Catherine Shirley

ANEXO4: FOTOS DEL CENTRO DE DATOS

SEGURIDAD DE LA INFORMACION

AIRE ACONDICIONADO

EXTINGUIDORES DE INCENDIO MAL UBICADOS

PUERTA DE INGRESO AL PISO DONDE SE ENCUENTRA EL CENTRO DE DATOS

PUERTA DE INGRESO AL CENTRO DE DATOS

DIRECTIVA

PLAN DE MANTENIMIENTO PREVENTIVO Y CORRECTIVO DE EQUIPOS DE CÓMPUTO DEL HOSPITAL HUACHO HUAURA OYON

2018

PLAN DE MANTENIMIENTO PREVENTIVO Y CORRECTIVO

SOPORTE TECNICO

SERVIDORES

AREAS DE TRABAJO

MATERIAL INFLAMABLE

CABLEADO