UNIVERSIDAD SAN PEDRO

FACULTAD DE INGENIERÍA

ESCUELA ACADÉMICO PROFESIONAL DE INGENIERÍA INFORMÁTICA Y DE SISTEMAS

Evaluación de la seguridad del centro de datos del Hospital de Apoyo II-2 Sullana

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

Autor

Bruno Pizarro, Eder Omar

Asesor

Arroyo Tirado, Jorge Luis

Piura – Perú

2019

PALABRAS CLAVES

TEMA	SEGURIDAD DE LA INFORMACIÓN
ESPECIALIDAD	GESTION

KEYWORDS

THEME	SECURITY OF THE INFORMATION
SPECIALTY	MANAGEMENT

LÍNEA DE INVESTIGACIÓN

LÍNEA	SISTEMAS DE GESTION
SUB LINEA	SEGURIDAD INFORMATICA
DISCIPLINA	NEGOCIOS Y MANAGEMENT

TÍTULO

Evaluación de la seguridad del centro de datos del Hospital de Apoyo II - 2 Sullana

RESUMEN

La presente investigación tuvo como objetivo la Evaluación de la Seguridad del Centro de Datos del Hospital de Apoyo II-2 Sullana. Así mismo nos permitirá identificar las condiciones en las que se encuentra el centro de datos, y conocer sus vulnerabilidades, amenazas y nivel de riesgo de cada activo de TI.

El diseño de la investigación es no experimental, respecto a la toma de datos para la construcción del sistema con corte transversal aplicándose técnicas e instrumentos de recolección de datos en el tiempo que dura el desarrollo de la evaluación, así mismo es propositiva, de innovación incremental, porque se trata de desarrollar una evaluación de la seguridad del centro de datos con la finalidad de reducir los niveles de riesgo que podría presentar.

Se aplicara la NTP ISO/IEC 27005:2009 para desarrollar dicha evaluación del riesgo de seguridad dado que dicha norma se refiere a las técnicas de seguridad y la gestión del riesgo en seguridad de información.

ABSTRACT

The objective of this research was the Safety Evaluation of the Data Center of Hospital de Apoyo II-2 Sullana. It will also allow us to identify the conditions in which the data center is located, and to know its vulnerabilities, threats and level of risk of each IT asset.

The design of the research is non-experimental, with respect to the data collection for the construction of the cross-sectional system, applying techniques and data collection instruments in the time that the development of the evaluation lasts, as well as proposing incremental innovation , because it is about developing an assessment of the data center's security in order to reduce the levels of risk it could present.

The NTP ISO / IEC 27005: 2009 will be applied to develop this security risk assessment given that this standard refers to security techniques and information security risk management.

ÍNDICE

INTRODUCCIÓN

Para la presente investigación se tomaron como antecedentes, la investigación de López (2011), en su Tesis titulada "Diseño de un Plan de Gestión de Seguridad de la Información. Caso: Dirección de Informática de la Alcaldía del Municipio Jiménez del Estado Lara", realizada en la Universidad Centroccidental Lisandro Alvarado, la investigación tuvo como objetivo fundamental diseñar un Plan de Gestión de Seguridad de la Información en la Alcaldía del Municipio Jiménez del Estado Lara. La investigación se enmarcó desde el punto de vista metodológico en la modalidad de proyecto factible, apoyado en la investigación monográfica 14 documental y de campo, el cual se dividió en tres fases: a). Una primera fase de diagnóstico de la situación actual de la Alcaldía del Municipio Jiménez en relación a la seguridad de la información; b) seguida por la evaluación de la factibilidad técnica, económica y financiera de la propuesta; c) y por último el diseño del Plan de Seguridad de la Información de acuerdo a la norma ISO/IEC 27001:2005 aprobada por la Organización Internacional de Estandarización y por la Comisión Internacional Electrotécnica de sus siglas en ingles ISO/IEC. En relación a la necesidad al diseño del Plan de Gestión de Seguridad de la Información se pudo observar que: un 65% del personal de la Alcaldía tiene conocimiento acerca del Plan de Seguridad de la Información mientras que el 35% manifiestan el desconocimiento de dicho Plan. Un 55% de los encuestados opina que no existe una estrategia de recuperación ante desastre, lo que significa que en la alcaldía no cuenta con un sistema o plan de contingencia en caso de desastre.

Por su parte Sánchez (2014), en su Tesis titulada "Diseño de Políticas de Seguridad de la Información para la Alcaldía Municipal de Rio de Oro, Cesar", realizada en Universidad Francisco de Paula Santander Ocaña, tiene como objetivo fundamental Diseñar las Políticas de Seguridad de la Información para la Alcaldía Municipal de Río de Oro (Cesar), así como también realizar un reconocimiento dela estructura organizacional, el direccionamiento estratégico y componente tecnológico de la Alcaldía Municipal de Río de Oro (Cesar), Evaluar las normas COBIT 4.1, ITIL v3 e ISO/IEC 27002 y mediante un cuadro comparativo determinar cuál es la más pertinente para el establecimiento de las Políticas de Seguridad de la Información en la Alcaldía Municipal de Río de Oro (Cesar), Proponer un Manual de las Políticas de Seguridad de la Información para la Alcaldía Municipal de Río de Oro (Cesar) con base a la norma seleccionada, Redactar un Artículo donde se expongan la tabulación de resultados de las encuestas aplicadas en la Alcaldía de Río de Oro (Cesar). Se tomó como base la ISO/IEC 27002. Tomando como base los resultados obtenidos de la investigación, se redactó un artículo donde se expuso la respectiva tabulación, enfocándose a la situación actual de la Alcaldía en cuanto a la seguridad de la información que allí se maneja. Reflejando la necesidad de aplicar políticas de seguridad de la información en todas sus secretarias, con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información.

Asimismo, se revisó la investigación de Patiño (2018), en su tema "Propuesta Metodológica de Gestión de Riesgos de Tecnología de Información y Comunicación

(TIC) para Entidades Públicas conforme Normativa NTE INEN ISO/IEC 27005", realizada en la Universidad de las Fuerzas Armadas, plantea como objetivo fundamental elaborar una guía metodológica para la gestión de riesgo de TIC en entidades del sector público conforme normativa NTE INEN ISO/IEC 27005 para mejorar la administración de la seguridad de la información. Así como también investigar las normas INEN ISO/IEC 27001:2013 e INEN ISO/IEC 27005:2008, determinar el grado con el cual se administran los riesgos tecnológicos en entidades del sector público, mediante la aplicación de una encuesta al responsable del área de tecnología, aplicar la guía metodológica de gestión de riesgos de TIC basada en la normativa ISO 27005 en una entidad del sector público. En conclusión se realizó la comprobación de la hipótesis, siendo positiva debido a que la elaboración e implementación de la guía metodológica permitió mejorar la administración de la seguridad de la información en la entidad del sector público, porque permitió la identificación de controles para que posteriormente serán implementados de acuerdo con los recursos disponibles en la institución.

También se revisó la investigación de Aquije y Jave (2012), en su tesis titulada "Metodología de Gestión de Seguridad de la Información para el Sector Financiero Peruano", realizada en la Universidad Nacional de Ingeniería, tiene como objetivo fundamental diseñar una metodología de gestión de seguridad de la información orientada al sector financiero peruano, que involucre desde la identificación de activos hasta el monitoreo y control de los riesgos. Para el desarrollo de la propuesta se toma como referencia estándares internacionales como la ISO 17799 y la 27001. La

implementación de un Sistema de Gestión de Seguridad de la Información permitirá asegurar los activos de información más importantes de la empresa y gestionar los riesgos existentes, es por ello que la propuesta metodológica brinda pautas para definir una metodología de gestión de riesgos consiste y alineada a la utilizada por riesgo operacional.

Así también se revisó la investigación de Ayala (2017), en su tesis titulada "Sistema de Gestión de seguridad de Información para Mejorar el Proceso de Gestión del Riesgo en un Hospital Nacional, 2017", realizada en la Universidad Cesar Vallejo, tiene como objetivo principal evaluar la manera en que la implementación del Sistema de Gestión de Seguridad de la Información influye en el proceso de gestión del riesgo en un Hospital Nacional, así como también evaluar la manera en que la implementación del sistema de Gestión de Seguridad de la Información influye en el número de controles aplicados en el proceso de gestión del riesgo en un Hospital Nacional. Se utilizó la norma ISO/IEC 27001. En conclusión Mediante la implementación de la metodología del sistema de gestión de seguridad de la información para mejorar el proceso de gestión del riesgo en el Hospital Nacional PNP "Luis N. Sáenz", el nivel del riesgo se consigue disminuir de 3.72 a 3.09, representando un 16.96%. Por tanto, se determina que el nivel de riesgo de los activos críticos identificados en la presente investigación ha disminuido.

Por su parte Huerta (2015), en sus tesis titulada "Procedimientos para la Auditoria en Seguridad Física del Data Center de la Municipalidad Provincial de Huamanga", en la Universidad Nacional de San Cristóbal de Huamanga, tiene como objetivo fundamental

Implementar un procedimiento de auditoría en seguridad física del Data Center de la Municipalidad Provincial de Huamanga de la ciudad de Ayacucho, 2014. Mediante la clasificación y estándar internacional TIER, marco de control COBIT 5.0 y la norma técnica peruana NTP-ISO/IEC 17799, Identificar los activos involucrados en la seguridad física del Data Center de la Municipalidad Provincial de Huamanga. Identificar los riesgos comunes en seguridad física del Data Center de la Municipalidad Provincial de Huamanga. Los procedimientos implementados, han sido aplicados en el Data Center de la Municipalidad, logrando resultados que demuestran la efectividad de su seguridad física en algunos aspectos y la deficiencia en otras, la sub gerencia de sistemas de la entidad evaluada mostró interés en querer poner en práctica las recomendaciones de la auditoría, para mejorar la infraestructura e instalaciones de su Data Center y hacerla más resistente ante eventuales riesgos, y para elevar el buen desempeño en sus servicios tecnológicos.

También Aliaga (2014), en sus tesis titulada "Análisis de Riesgo de TI para la Implementación de un Sistema de Seguridad de la Información en el Gobierno Regional de Cajamarca", en la Universidad Nacional de Cajamarca, como objetivo general es realizar un análisis de riesgos de TI que permita implementar un Sistema de Gestión de la Seguridad de la Información bajo la Norma Técnica Peruana NTP ISO/IEC 27001:2008, así como también Identificar y priorizar el(los) proceso(s) crítico(s) de negocio del Gobierno Regional de Cajamarca. Evaluar y elegir metodologías de análisis de riesgos de TI. Identificar Activos de Información basados en el(los) proceso (s}

críticos. Identificar y valorar las amenazas de los activos de información. Identificar y valorar las vulnerabilidades de los activos de información. Identificar los riesgos asociados a los activos de información. Identificar controles en función a la norma técnica peruana NTP-ISO/IEC 27001:2008 basándonos en los resultados del análisis de riesgos, que permitirá tomar como base para la implementación de un Sistema de Gestión de la seguridad de la información. Por tema normativo exigido por la Oficina Nacional de Gobierno Electrónico e Informática se ha utilizado la NTP ISO/IEC 27005: 2009. Se lograron identificar los controles a implementar para cada riesgo identificado con la ayuda de la NTP ISO/IEC 27001:2008 y NTP ISO/IEC 17799:2007. Finalmente se ha obtenido la lista de amenazas y vulnerabilidades; y sus valoraciones para cada activo de información (solo activos con valoración alta), y se ha identificado los controles a implementar por cada riesgo identificado, con el fin de proteger los activos de TI con el fin de asegurar la continuidad del negocio.

Otra investigación revisada fue De la Cruz (2016), en su tesis titulada "Propuesta de políticas, basadas en buenas practicas, para la gestión de seguridad de la información en la Municipalidad Provincial de Paita, 2016", realizada en la Universidad Católica Los Ángeles Chimbote, tuvo objetivo general realizar la propuesta de políticas basadas en buenas practicas, para la gestión de seguridad de la información en la Municipalidad Provincial de Paita; en el año 2016. La evaluación de la situación actual de los procesos de seguridad en la Municipalidad Provincial de Paita, en el año 2016; permitirá identificar las falencias de seguridad de la información. La inseguridad de la

información existente en la Municipalidad Provincial de Paita, en el año 2016; justificará la factibilidad técnica, la inversión económica y operativa para el desarrollo de la propuesta, basadas en buenas prácticas, para la gestión de seguridad de la información. La necesidad de una eficiente propuesta de políticas basadas, en buenas prácticas, para la gestión de seguridad de la información en la Municipalidad Provincial de Paita, en el año 2016; respalda el desarrollo e implementación de la propuesta. Para elaborar dicha propuesta se hizo uso de la NTP ISO/IEC 27001:2014. Según los resultados obtenidos en esta investigación, se concluye que: la Municipalidad Provincial de Paita carece de políticas y controles eficientes en cuanto a la protección de los activos de la información (los servidores públicos y/o contratistas, la creación de información, los procesos, las tecnologías de información incluido el hardware y el software y las instalaciones), por esta razón si resulta beneficioso el diseño e implementación de la propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la Municipalidad Provincial de Paita; 2016, el mismo que permitirá minimizar la pérdida de información, con lo que queda demostrado que la hipótesis general es aceptada.

Carrasco, S (2005) reseña como justificación teórica – científica en el que el resultado de la investigación podrá generalizarse e incorporarse al conocimiento científico, asimismo, complementar espacios cognoscitivos existentes.

La investigación aporta de manera científica porque aplica conocimientos selectivos y sistematizados para el desarrollo de la Evaluación de la Seguridad del Centro de Datos del Hospital de Apoyo II- 2 Sullana, para lo cual se hizo uso de la NTP ISO/IEC

27005:2009, esta norma es precisamente una guía que nos proporciona directrices para la gestión de riesgos en la seguridad de la información con la finalidad de lograr que las diferentes entidades reguladas optimicen sus inversiones de TI y administren de manera adecuada sus riesgos tecnológicos. Asimismo, la investigación científica desarrolla métodos tecnológicos y sistematizados para obtener resultados válidos y confiables de los procesos de desarrollo de la Evaluación de la Seguridad del Centro de Datos del Hospital de Apoyo II- 2 Sullana y contribuir a la mejora de la actualización de la información.

El Área de Informática del Hospital de Apoyo II- 2 Sullana, cuenta con un Sistema Informático de Gestión de Salud que administra la información de sus pacientes, durante el proceso de atención de salud y otros sistemas. Para ello el Área de Informática, cuenta con un centro de datos que opera los servidores, soporte que contiene las bases de datos de todos sus usuarios y demás procesos, en ambiente de producción que aún no cuenta con una buena política de seguridad de la información para sus procesos de gestión de riesgo, por lo tanto existe un gran peligro de seguridad, en mantener la confidencialidad del historial clínico de los pacientes y de los profesionales de la salud. La gestión de riesgo de un hospital implica los riesgos propiamente dichos de la seguridad de la información, las cuales abarcan el uso indebido de la data de los pacientes, ataque de terceros a los sistemas de información de salud, peligro a la integridad y confidencialidad de la información, perdida de información por robo o sustracción en el sistema de almacenamiento o algún desastre natural.

Después de realizar un análisis sobre los problemas que aquejan al Área de Informática, y en la búsqueda de una solución, se plantea la siguiente formulación:

¿Cómo desarrollar una Evaluación de la Seguridad del centro de Datos del Hospital de Apoyo II Sullana?

Asimismo, para dar respuesta a esta interrogante, en el desarrollo del proyecto se tomaron en cuenta las siguientes bases y fundamentos teóricas:

Activos.

Isaca (2011) conceptualiza que es un "activo", "un recurso o bien económico propiedad de una empresa, con el cual se obtienen beneficios. Los activos de las empresas varían de acuerdo con la naturaleza de la actividad desarrollada".

Para Areitio (2008) un activo es un componente o una parte de un sistema global al que la organización asigna un valor y, por tanto, que requiere protección. Posibles activos a identificar son: activos de TIC (Hardware, software, información), personal (empleados, invitados, usuarios de empresas de externalización), entorno (edificio, instalaciones), actividades (operaciones).

Según Bustos et. Al. (2009) un activo es un "recurso del sistema de información o relacionado con este, necesario para que la organización funcione correctamente y alcance los objetivos propuestos".

“los activos también son fundamentales para lograr los objetivos definidos por la organización y requieren de una especial protección: cualquier amenaza que pueda afectar a un activo puede poner en peligro la actividad de la organización y su servicio al cliente” (Chicano, 2015)

Para Tupia (2010) un activo “ es un elemento impreso o digital que contenga información, así como todo sistema - conformado por software, hardware y su documentación pertinente – que cree, maneje y procese información para una organización; también se puede incluir a la infraestructura tecnológica donde se desenvuelven dichos sistemas”

Vulnerabilidad.

Mantino (2013) define la vulnerabilidad como "grado de resistencia y/o exposición de un elemento o conjunto de elementos frente a la ocurrencia de un peligro".

Así mismo, Piattini y Del Peso (2001) conceptualiza a la vulnerabilidad como la situación creada, por la falta de uno o varios controles, con la que la amenaza pudiera acaecer y así afectar al entorno informático.

Por su parte Aguilera (2010) define como la probabilidad que existe de que una amenaza se materialice contra un activo. No todos los activos son vulnerables a las mismas amenazas. Por ejemplo, los datos son vulnerables a la acción del hackers, mientras que una instalación eléctrica es vulnerable a un cortocircuito. Al hacer el análisis de riesgo hay que tener en cuenta la vulnerabilidad de cada activo.

"Una vulnerabilidad, por sí misma, no causa daño alguno; es, simplemente, una condición o conjunto de condiciones que pueden permitir que una amenaza afecte a un activo. Las vulnerabilidades pueden ser permanentes, a no ser que se produzcan cambios en el activo, de forma que lo haga insensible a la vulnerabilidad" (Areitio, 2008)

Amenaza.

Según Piattini y Del Peso (2001) una amenaza es una(s) persona(s) o cosa(s) vista(s) como posible fuente de peligro o catástrofe. Ejemplos: inundación, robo de datos, sabotaje, agujeros publicados, falta de procedimientos de emergencia, divulgación de datos, implicaciones con la ley, aplicaciones mal diseñadas, gastos incontrolados, etc.

"Son todas las actividades, eventos o circunstancias que pueden afectar el buen uso de un activo de información dañándolo y no permitiendo que brinde soporte a algún proceso, perjudicando directamente la consecución de los objetivos de negocio" (Tupia, 2010).

Guagalango y Moscoso (20 11) "una amenaza es cualquier cosa que puede suceder y que, cuando ocurre, tiene consecuencias negativas sobre el valor de nuestros activos".

Una amenaza necesita explotar una vulnerabilidad del activo para producir un daño. El daño causado por una amenaza puede ser temporal o permanente y se puede asociar con una escala de severidad como otros fenómenos. Entre las características más relevantes de una amenaza se encuentra las siguientes: El origen (puede ser interno o externo), la motivación (como son las ventajas competitivas, los beneficios económicos,

etc.), la frecuencia o periodicidad de los ataques, la severidad (dependiendo de si es o irreversible). Al tratar las amenazas, se deben considerar los de tipo medioambientales y también culturales (Areitio, 2008).

Según Del Peso E., Ramos, Del Peso M. y Del Peso M. (2011) "las amenazas pueden ser muy diversas: sabotaje, vandalismo, terrorismo accidentes de distinto tipo, incendios, inundaciones, averías importantes, derrumbamientos, explosiones, así como otros que afectan a las personas y pueden impactar el funcionamiento de los centros, tales como errores, negligencias, huelgas, epidemias o intoxicaciones".

Mantino (2013) enumera distintas amenazas físicas con relación a la seguridad física: “Desastres naturales, incendios accidentales, tormentas e inundaciones, amenazas ocasionadas por el hombre, disturbios, sabotajes internos y externos deliberados”

Para Aguilera (2010) las amenazas físicas pueden ser desde cortes eléctricos, fallos del hardware o riesgos ambientales: y menciona dos tipos de amenazas a nivel físico:

> **Interrupción.** El objetivo de la amenaza es deshabilitar el acceso a la información; por ejemplo, destruyendo componentes físicos como el disco duro, bloqueando el acceso a los datos, o cortando o saturando los canales de comunicación.
>
> **Accidentales.** Accidentes meteorológicos, incendios, inundaciones, fallos en los equipos, en las redes, en los sistemas operativos o en el software, errores humanos.

Riesgo

Según Guagalango y Moscoso (2011) un riesgo es “estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización”

De la misma manera, Según Chaparro, Pérez y Tenjo (2010) “el riesgo se refiere a la incertidumbre o probabilidad de que una amenaza se materialice utilizando la vulnerabilidad existente de un activo o grupo de activos, generándole pérdidas o daños."

Para Piattini y Del Peso (2001) el riesgo es "la probabilidad de que una amenaza llegue a acaecer por una vulnerabilidad. Ejemplo: los datos estadísticos de cada evento de una base de datos de incidentes".

“El riesgo es la probabilidad de que una amenaza explote una vulnerabilidad. En los sistemas de la información se pueden asumir riesgos si el coste de la pérdida es bajo, pero existen entornos en los que el riesgo es muy alto y se han de implantar medidas para mitigarlo" (Cilleros, 2012).

Aguilera (201 0), afirma: No constituye riesgo una amenaza cuando no hay vulnerabilidad ni una vulnerabilidad cuando no existe amenaza para la misma. Ante un determinado riesgo, una organización puede optar por tres alternativas distintas: Asumirlo sin hacer nada, esto solamente resulta lógico cuando el perjuicio esperado no tiene valor alguno o cuando el coste de aplicación de medidas superaría de la reparación

del daño; aplicar medidas para disminuirlo o anularlo y tb 5mransferirlo (por ejemplo, contratando un seguro).

Para identificar los posibles riesgos dentro de un Data Center es necesario realizar un análisis de riesgo.

Análisis de riesgo. El análisis de riesgo, es el estudio de las causas de las posibles amenazas y probables eventos no deseados y los daños y consecuencias que éstas puedan producir.

Dais-ujat (2006) "El análisis de riesgo puede ser considerado como, la identificación, el análisis, la evaluación, el control y la minimización de las pérdidas asociadas con eventos de riesgo, es una revisión constante y permanente debido a que se trata de un proceso continuo"

El análisis de riesgos introduce un enfoque riguroso y consecuente para la investigación de los factores que contribuyen a los riesgos. En general implica la evaluación del impacto que una violación de la seguridad tendría en la empresa; señala los riesgos existentes, identificando las amenazas y la determinación de la vulnerabilidad a dichas amenazas. (*De* Pablos, López-Hermoso, Martín-Romo, Medina, Montero y Nájera, 2006).

FAMILIA DE NORMAS DE SEGURIDAD DE LA INFORMACIÓN ISO 27000

Portal de ISO 27001 en Español, La información es un activo vital para el éxito y la continuidad en el mercado de cualquier organización. El aseguramiento de la información y de los sistemas que la procesan es un objetivo de primer nivel para la organización.

Para la adecuada gestión de la seguridad de la información, es necesario implantar un sistema que aborde esta tarea de una forma metódica, documentada y basada en objetivos claros de seguridad y en una evaluación de los riesgos a los que está sometida la información de la organización.

La familia de normas ISO 27000 es un conjunto de estándares desarrollados por la ISO e IEC, que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

El conjunto de normas ISO/IEC 27000 tiene su origen en la norma BS 7799 de la BSI que apareció por primera vez en 1995, con objeto de proporcionar a cualquier empresa un conjunto de buenas prácticas para la gestión de la seguridad de su información.

La primera parte de la norma (BS 7799-1) fue una guía de buenas prácticas, para la que no se establecía un esquema de certificación. Es la segunda parte (BS 7799-2), publicada por primera vez en 1998, la que estableció los requisitos de un SGSI para ser certificable por una entidad independiente.

Las dos partes de las norma BS 7799 se revisaron en 1999 y la primera parte se adoptó por ISO, sin cambios sustanciales, como ISO 17799 en el año 2000.

En 2002, se revisó la BS 7799-2 para adecuarse a la filosofía de normas ISO de sistemas de gestión.

En 2005, con más de 1700 empresas certificadas en BS 7799-2, esta norma se publicó por ISO, con algunos cambios, como estándar ISO 27001. Al tiempo se revisó y actualizo la ISO 17799. Esta última norma se renombro como ISO 27002:2005 el 1 de julio del 2007, manteniendo el contenido así como el año de publicación formal de la revisión.

Figura 01: Evolución ISO/IEC 27000
Fuente: www.iso27000.es

La familia ISO/IEC 27000 está conformada por una serie de normas que permiten ser un guía para mejorar la seguridad de la información en cualquier organización independientemente del rubro y tamaño.

Varias de las normas de la familia ISO/IEC 27000 son aplicadas en el Perú bajo las iniciales NTP. Las normas técnicas peruanas publicadas por INDECOPI son la NTP-ISO/IEC 27001:2008, NTP-ISO/IEC 17799:2007, NTP-ISO/IEC 27003:2012 y NTP-ISO/IEC 27005:2009.

DESCRIPCIÓN GENERAL NTP ISO/IEC 27001:2008

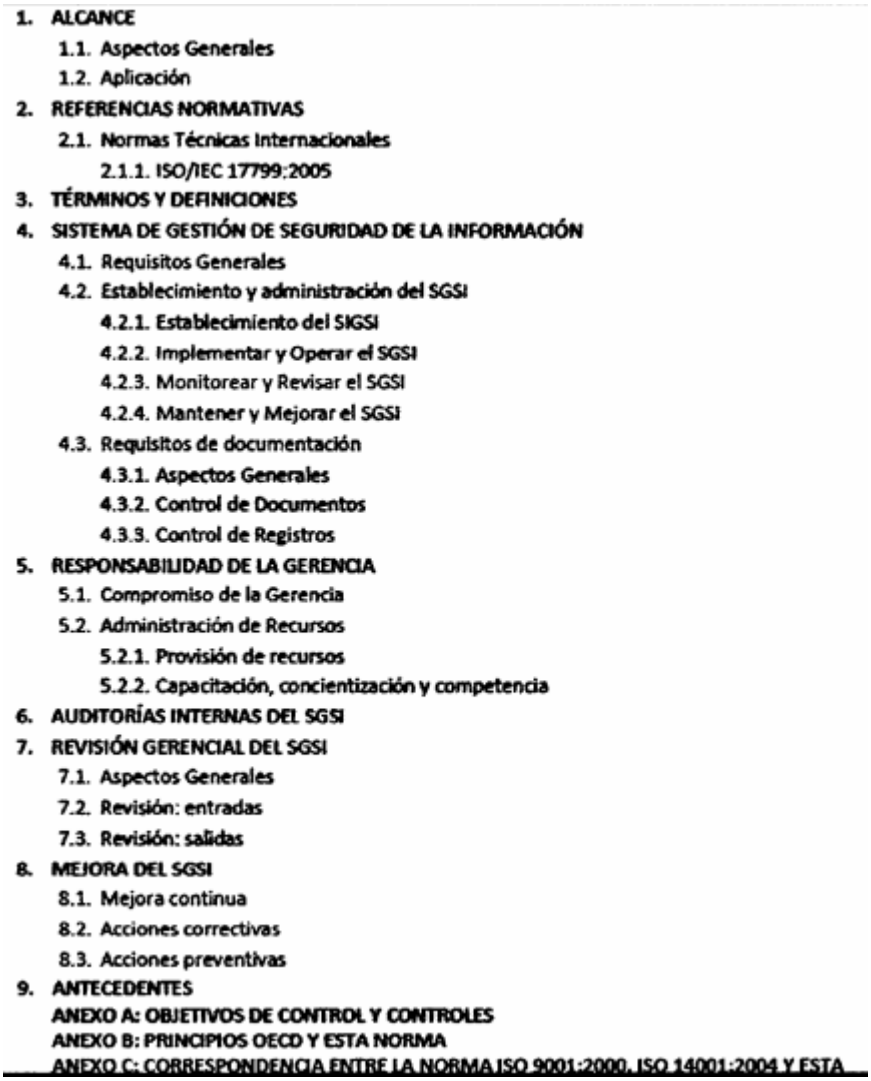
Norma técnica peruana elaborada por el Comité Técnico Permanente de Codificación e Intercambio Electrónico de Datos en el año 2008 donde se especifica los requerimientos obligatorios para establecer, implementar, operar, monitorear, mantener y mejorar un SGSI dentro de una organización. Cabe recalcar que esta norma es una transcripción de la norma internacional ISO/IEC 27001 del idioma inglés al español, al igual que sucede con las demás normas técnicas peruanas relacionadas a seguridad de la información.

Esta norma tiene como fin asegurar una adecuada selección de controles de seguridad para proteger los activos de información.

El 23 de mayo del 2012se publica la Resolución Ministerial N° 129-2012-PCM para aprobar el uso obligatorio de la "NTP-ISO/IEC 27001:2008 EDI: Tecnología de la Información. Requisitos" para entidades integrantes del Sistema Nacional de Información. Esta resolución también especifica que la certificación no es obligatoria y será decisión de cada entidad pública asumiendo los costos que implique dicha certificación.

La ISO 27001 es la única certificable de toda la familia; además existen certificaciones para profesionales en relación a su implementación y auditoria principalmente

En la siguiente figura se muestra todos los puntos que detalla esta norma técnica peruana:



1. ALCANCE
   - 1.1. Aspectos Generales
   - 1.2. Aplicación
2. REFERENCIAS NORMATIVAS
   - 2.1. Normas Técnicas Internacionales
     - 2.1.1. ISO/IEC 17799:2005
3. TÉRMINOS Y DEFINICIONES
4. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN
   - 4.1. Requisitos Generales
   - 4.2. Establecimiento y administración del SGSI
     - 4.2.1. Establecimiento del SIGSI
     - 4.2.2. Implementar y Operar el SGSI
     - 4.2.3. Monitorear y Revisar el SGSI
     - 4.2.4. Mantener y Mejorar el SGSI
   - 4.3. Requisitos de documentación
     - 4.3.1. Aspectos Generales
     - 4.3.2. Control de Documentos
     - 4.3.3. Control de Registros
5. RESPONSABILIDAD DE LA GERENCIA
   - 5.1. Compromiso de la Gerencia
   - 5.2. Administración de Recursos
     - 5.2.1. Provisión de recursos
     - 5.2.2. Capacitación, concientización y competencia
6. AUDITORÍAS INTERNAS DEL SGSI
7. REVISIÓN GERENCIAL DEL SGSI
   - 7.1. Aspectos Generales
   - 7.2. Revisión: entradas
   - 7.3. Revisión: salidas
8. MEJORA DEL SGSI
   - 8.1. Mejora continua
   - 8.2. Acciones correctivas
   - 8.3. Acciones preventivas
9. ANTECEDENTES

ANEXO A: OBJETIVOS DE CONTROL Y CONTROLES
ANEXO B: PRINCIPIOS OECD Y ESTA NORMA
ANEXO C: CORRESPONDENCIA ENTRE LA NORMA ISO 9001:2000, ISO 14001:2004 Y ESTA

Figura 02: Estructura NTP ISO/IEC 27001:2008

Fuente: NTP ISO/IEC 27001:2008

GESTIÓN DE RIESGO EN SEGURIDAD DE LA INFORMACIÓN (NTP ISO/IEC 27005:2009)

Comité Técnico de Normalización de Codificación e Intercambio Electrónico de Datos (2009) denomina que la gestión del riesgo en seguridad de la información debe ser un proceso continuo. El proceso debe establecer el contexto, evaluar los riesgos y tratarlos utilizando un plan de tratamiento de riesgos para implementar las recomendaciones y decisiones. La gestión del riesgo analiza lo que puede ocurrir y cuáles serían las consecuencias posibles antes de decidir qué debe hacerse y cuando para reducir el riesgo a un nivel aceptable.

La gestión del riesgo en seguridad de la información debe contribuir a lo siguiente:

Identificar los riesgos

- Evaluar los riesgos en términos de sus consecuencias para la empresa y la posibilidad de su ocurrencia
- La comunicación y comprensión de la posibilidad y consecuencias de estos riesgos.
- El establecimiento de un orden para el tratamiento del riesgo.
- Priorización de acciones para reducir la ocurrencia de riesgo.
- Participación de los interesados cuando se toman las decisiones de gestión del riesgo e información sobre la situación de la gestión del riesgo.
- Monitoreo y revisión regulares de los riesgos y del proceso de gestión del riesgo.

- Captación de información para mejorar el enfoque de gestión del riesgo.
- Educación a gerentes y personal respecto a los riesgos y acciones que se toman para mitigarlos.

El proceso de gestión del riesgo en seguridad de la información puede aplicarse a la organización en su conjunto, a cualquier parte especifica de la organización (por ejemplo: un departamento, una ubicación física, un servicio), a cualquier sistema de información, existente o planeado, o a aspectos particulares del control (por ejemplo: planeamiento de la continuidad del negocio).

Vista panorámica del proceso de gestión del riesgo en seguridad de la información

El proceso de gestión del riesgo en seguridad de la información consiste en establecer el contexto, evaluar el riesgo, tratar el riesgo, aceptar el riesgo, comunicar el riesgo y monitorear y revisar el riesgo.

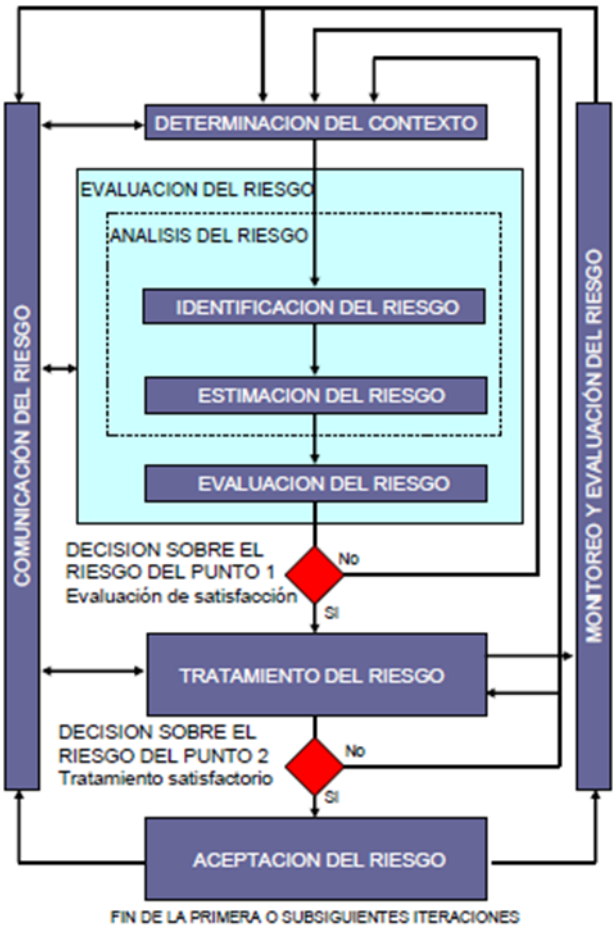


Figura 03: Proceso de gestión del riesgo de seguridad de la información.

Fuente: NTP ISO/IEC 27005:2009

El proceso de gestión de seguridad de la información puede ser iterativo para la evaluación del riesgo y/o para las actividades de tratamiento del riesgo. Un enfoque iterativo para la conducción de la evaluación del riesgo puede incrementar la profundidad y detalle de la evaluación en cada iteración. El enfoque iterativo provee un buen balance entre minimizar el tiempo y el esfuerzo que se emplea en identificar los controles y a la vez asegurar que se evalué apropiadamente los altos riesgos.

Primero se determina el contexto. Luego se realiza una evaluación del riesgo. Si esto provee suficiente información para determinar efectivamente las acciones requeridas para modificar los riesgos a un nivel aceptable, entonces la tarea está completa y sigue el tratamiento del riesgo. Si la información es suficiente, se conducirá otra iteración del riesgo con el contexto revisado (por ejemplo: criterios de evaluación del riesgo, criterios de aceptación del riesgo o criterios de impacto) posiblemente en partes limitadas del alcance total.

La eficacia en el tratamiento del riesgo depende de los resultados de la evaluación del riesgo. Es posible que el tratamiento del riesgo no conduzca inmediatamente a un nivel aceptable del riesgo residual. En esta situación, podría requerirse otra iteración de la evaluación del riesgo con parámetros de contexto cambiados (por ejemplo: la evaluación del riesgo, aceptación del riesgo o criterios de impacto), si fuera necesario, seguido de otro tratamiento del riesgo.

La actividad de aceptación del riesgo tiene que asegurar que los gerentes de la organización acepten explícitamente los riesgos residuales. Esto es especialmente importante en una situación donde la implementación de controles se omite o pospone, por ejemplo debido al costo.

Durante todo el proceso de gestión del riesgo en seguridad de la información es importante que los riesgos y su tratamiento se comuniquen a los gerentes apropiados y al personal operativo. Incluso antes del tratamiento de los riesgos puede ser muy valioso contar con información sobre los riesgos identificados para administrar los incidentes y puede ayudar a reducir el daño potencial. La conciencia de los gerentes y el personal

respecto de los riesgos, la naturaleza de los controles empleados para mitigar los riesgos y las áreas de preocupación para la organización ayudan a tratar los incidentes y los eventos inesperados de la manera más eficaz. Deben documentarse los resultados detallados de los dos puntos de decisión sobre el riesgo.

La norma ISO/IEC 27001 especifica que los controles implementados dentro del alcance, límites y contexto del ISMS deben basarse en el riesgo. La aplicación de un proceso de gestión del riesgo en seguridad de la información puede satisfacer este requisito. Existen muchos enfoques por medio de los cuales se puede implementar exitosamente el proceso en una organización. La organización debe utilizar el enfoque que mejor se acomode a sus circunstancias para cada aplicación específica del proceso.

En un ISMS, determinar el contexto, evaluar el riesgo, desarrollar un plan de tratamiento del riesgo y aceptar el riesgo son parte de la fase del "plan". En la fase de "hacer" del ISMS, se implementan las acciones y controles requeridos para reducir el riesgo a un nivel aceptable de acuerdo con el plan de tratamiento del riesgo. En la fase de "verificar" del ISMS, los gerentes determinan la necesidad de revisiones de la evaluación del riesgo y el tratamiento del riesgo a la luz de los incidentes y cambios en las circunstancias. En la fase de "actuar", se realizan todas las acciones requeridas, incluyendo la aplicación adicional del proceso de gestión del riesgo en seguridad de la información.

La siguiente figura resume las actividades de gestión del riesgo en seguridad de la información relevantes a las cuatro fases del proceso del ISMS.

Proceso ISMS	Proceso de Gestión del Riesgo en Seguridad de la Información
	Determinar el contexto
Plan	Evaluar el riesgo
	Desarrollar el plan de tratamiento del riesgo
	Aceptar el riesgo
Hacer	Implementar el plan de tratamiento del riesgo
	Monitoreo y revisión continuos de los riesgos
Revisar	
Hacer	Mantener y mejorar el Proceso de Gestión del Riesgo en Seguridad de la Información

Figura 04: Alineamiento del ISMS y del Proceso de Gestión del Riesgo en Seguridad de la Información. Fuente: NTP ISO/IEC 270005:2009

Centro de datos.

Galván (2013) denomina Centro de Proceso de Datos o Datacenter a aquella ubicación donde se concentran todos los recursos necesarios para el procesamiento de la información de una organización.

Dichos recursos consisten esencialmente en unas dependencias, debidamente acondicionadas, de computadoras y redes de comunicaciones.

Se suelen denominar por su acrónimo: CD o Datacenter (en inglés), Centro de Cómputo o Centro de Datos.

"El Centro de Procesamiento de Datos (CPD) es un cuarto, espacio físico o ubicación donde se concentran todos los recursos necesarios para el procesamiento de la información de una organización. Se le conoce también como centro de cálculo en España, centro de cómputo en Iberoamérica, o centro de datos (data center). En dicho espacio se encuentran los equipos de una red, además de los servidores" (Gómez, 2011)

Por su lado Mario G. Piattini y Emilio del Peso (2001), Un data center sigue un modelo organizativo más o menos estándar, aunque debido a diferentes causas, como puedes ser el tipo de empresa al que pertenece, situación económica, disponibilidades de espacio, actitud de la Dirección, etc. Haces que, en realidad los centros de proceso de datos difieran bastante uno de los otros.

Mientras que la empresa IBM (2012), en un artículo publicado define que: El entorno del Data Center es una compilación de servidores, almacenamiento, sistemas de redes, sistemas mecánicos/eléctricos, aplicaciones y herramientas, procedimientos de gobernanza y personal. El único medio efectivo para medir la eficiencia de las operaciones del Data Center es incorporar un enfoque global que considere múltiples medidas en todos los elementos.

Se señalan a continuación algunas Fuentes que deben estar accesibles en todo Centro de Proceso de Datos: Políticas, Normas y Planes sobre Seguridad emitidos y distribuidos tanto por la Dirección de la empresa en términos generales como por el Departamento de Seguridad siguiendo un enfoque más detallado; Auditorías anteriores, generales y parciales, referentes a la Seguridad física o cualquier otro tipo de auditoría que, de una u otra manera, esté relacionada con la Seguridad Física; Contratos de seguros, de proveedores y de mantenimiento; Entrevistas con el personal de seguridad, personal informático y de otras actividades; Actas e informes de técnicos y consultores; Plan de contingencia y valoración de las pruebas; Informes sobre accesos y visitas. Existencia de una sistema de control de entradas y salidas diferenciando entre áreas Perimetral, interna y restringida; Informes sobre pruebas de evacuación ante diferentes tipos de amenaza:

incendio, catástrofe natural, terrorismo, etc.; Informe sobre evacuaciones reales; Políticas de personal e Inventarios de soportes.

Respecto de la operacionalización de las variables son las siguientes:

Tabla 01

Operacionalización de variables.

VARIABLE	DEFINICION CONCEPTUAL	DEFINICIÓN OPERACIONAL
NTP ISO/IEC 27005:2009	La gestión del riesgo en la seguridad de la información debería ser una parte integral de todas las actividades de gestión de seguridad de la información y se deberían aplicar tanto a la implementación como al funcionamiento continuo de un SGSI.	Proporciona directrices para la gestión de riesgos de seguridad de la información en una organización, dando particular soporte a los requisitos de un SGSI de acuerdo a la norma NTP ISO/IEC 27005 :2009,
CENTRO DE DATOS	Galván (2013) denomina Centro de Proceso de Datos o Datacenter a aquella ubicación donde se concentran todos los recursos necesarios para el procesamiento de la información de una organización. Dichos recursos consisten esencialmente en unas dependencias, debidamente acondicionadas, de computadoras y redes de comunicaciones. Se suelen denominar por su acrónimo: CD o Datacenter (en inglés), Centro de Cómputo o Centro de Datos.	Es hacer las tareas más rápidas, flexibles y cómodas para los usuarios del mismo.

La hipótesis de la presente investigación es implícita por ser un estudio de alcance descriptivo, en el cual determino los procesos y se aplicaron herramientas informáticas para el desarrollo de la evaluación.

La presente investigación tiene como objetivo General, Evaluar la seguridad del centro de datos del Hospital de Apoyo II – Sullana y como objetivo específicos: a) Realizar el proceso de evaluación utilizando el marco de trabajo para la medición de seguridad del centro de datos, b) Aplicar la NTP ISO/IEC 27005:2009, para la evaluación de la seguridad del centro de datos.

METODOLOGÍA

El proceso llevado a cabo en la formulación de la presente investigación tiene componente Investigativo de nivel descriptivo, teniendo en cuenta que fue necesaria la recolección de información para desarrollar una "Evaluación de la Seguridad del Centro de Datos del Hospital de Apoyo II- 2 Sullana"

El diseño de Investigación es no experimental, respecto a la toma de datos para el desarrollo de la evaluación con corte transversal aplicándose técnicas e instrumentos de recolección de datos en el tiempo que dura el desarrollo de la evaluación, así mismo es propositiva, de innovación incremental.

Debido a que la investigación es de tipo descriptivo, la muestra a considerar será la misma que la población, para el desarrollo de la evaluación de la seguridad del centro de datos del Hospital de Apoyo II-2 Sullana, la cual son aquellos colaboradores del Área de Informática con un total de (3 personas).

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

Tabla 02

Técnicas e instrumentos de recolección de datos

Técnicas	**Instrumentos**	**Uso**
Encuesta	Ficha de encuesta	Se aplicaron encuesta al personal involucrado
Análisis documental	Textos, tesis, revistas y estudios previos	Se analizó la documentación para fundamentar la investigación

RESULTADOS

DISEÑO METODOLÓGICO DE LA NORMA TÉCNICA PERUANA ISO /IEC 27005:2009

La investigación se basa en el desarrollo de la Norma Técnica Peruana ISO/IEC 27005: 2009, es por ello que se presenta los siguientes alcances.

Para la consideración del proyecto de investigación se realizara de la siguiente manera.

Tabla 03

Desarrollo del diseño metodológico NTP ISO/IEC 27005:2009

Etapa	**Consideración**
Identificación de procesos críticos	Generalidades del Hospital de Apoyo II-2 Sullana
Análisis de Riesgo de TI	Alcance y Limites Requisitos Normativos y regulatorios Evaluación del estado actual de la seguridad de la información Identificación de Activos de la Información Identificación Valoración de Activos Identificación de Vulnerabilidades Identificación de Amenazas Valoración de Riesgo

IDENTIFICACION DE PROCESOS CRÍTICOS

GENERALIDADES DEL HOSPITAL DE APOYO II- 2 SULLANA

Sector del Hospital de Apoyo II- 2 Sullana

Pertenece al Sector de Salud Pública en general.

Misión del Hospital de Apoyo II-2 Sullana

Es un establecimiento referencial de las Regiones Piura y Tumbes, con ámbito binacional de la Cuenca Catamayo – Chira, que promociona salud, previene los riesgos, protege del daño; con énfasis en la recuperación de la salud, rehabilitación de las capacidades de los pacientes; en condiciones de plena accesibilidad, para la atención de la persona, familia, la comunidad y medio ambiente, desde su concepción hasta su muerte natural; con enfoque de derechos humanos, equidad de género e interculturalidad en salud.

Visión del Hospital de Apoyo II- 2 Sullana

Constituirse en un hospital de alta complejidad en la atención de salud, con infraestructura moderna y equipos con tecnología de punta, de excelencia y liderazgo en la atención hospitalaria integral a la población en condiciones de legalidad, calidad y plena accesibilidad, fortalecido en la docencia e investigación para la salud, de acuerdo a la modernidad, integrándose al sistema de referencia y contra referencia, con enfoque de derechos humanos, equidad de género e interculturalidad en salud.

Organigrama del Hospital de Apoyo II- 2 Sullana

El organigrama del Hospital de Apoyo II- 2 Sullana se puede visualizar en la siguiente figura:

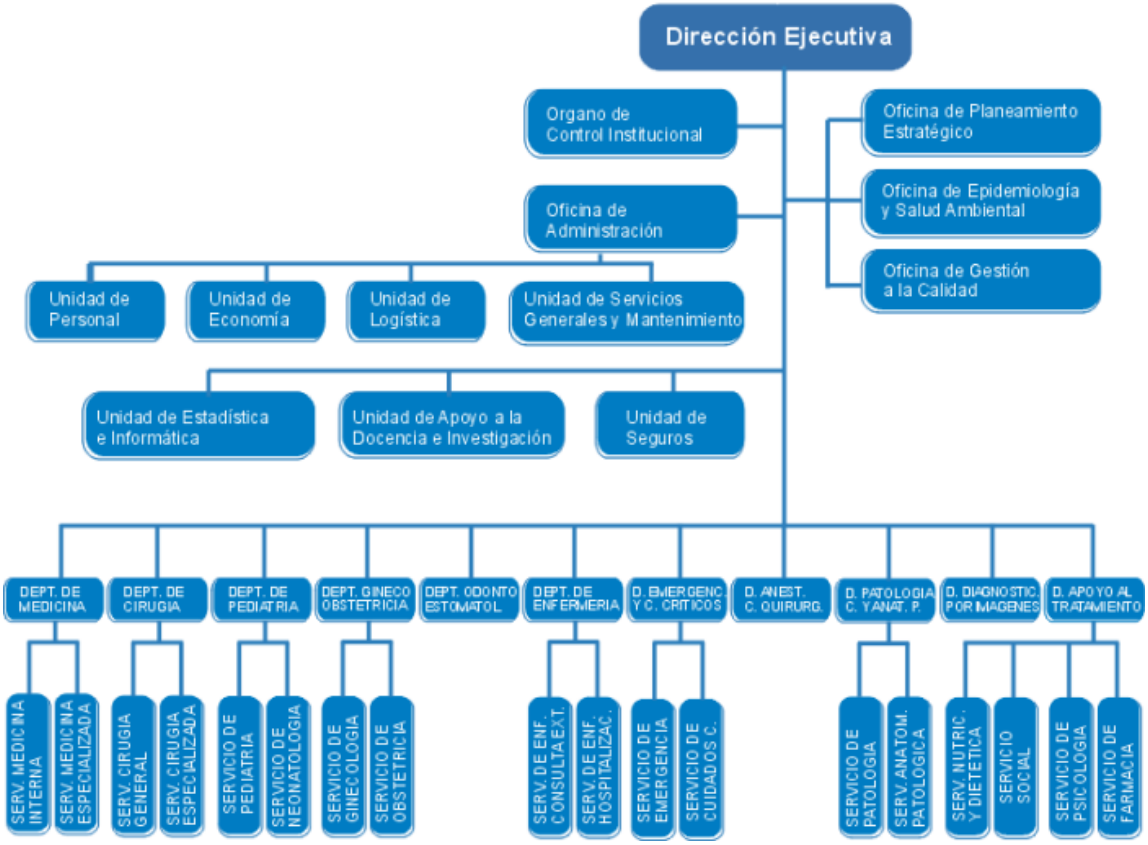


Figura 05: Organigrama del Hospital de Apoyo II-2 Sullana

Fuente: Portal Institucional del Hospital de Apoyo II- 2 Sullana (http://www.hospitalsullana.gob.pe/)

ANALISIS DE RIESGO DE TI

El análisis de riesgos de TI tiene sustento en la NTP ISO/IEC 27005:2009.

La gestión de riesgos es un aspecto muy importante para dar soporte a un Sistema de Gestión de la Seguridad de la Información uno de los puntos importantes que especifica

la norma NTP ISO/IEC 27005:2009 es tener en cuenta los objetivos estratégicos, políticas y estrategias de la organización, los procesos del negocio, entre otra más.

La NTP ISO/IEC 27005: 2009 nos sugiere definir los siguientes puntos:

- Identificación del riesgo
- Identificación de activos
- Identificación de amenazas
- Identificación de controles existentes
- Identificación de vulnerabilidades
- Identificación de las consecuencias
- Estimación del riesgo.

A continuación se define los siguientes puntos.

ALCANCE Y LÍMITES

En todo SGSI se debe establecer su alcance y límites. La presente investigación únicamente se concentrará en los activos de TI (Centro de Datos del Área de Informática), excluyendo cualquier activo que no tenga referencia a la tecnología. Este alcance es obligatorio tenerlo en cuenta, a partir de este la gestión de riesgos (la cual incluye el análisis respectivo de riesgo) debe estar alineada al SGSI.

La definición del alcance del análisis de riesgo es muy importante para el desarrollo del presente proyecto, dado que aplicar mucho implicaría costos muy elevados que ocasionaría desechar las propuestas de mejora, y abarcar poco podría afectar la continuidad del negocio.

REQUISITOS NORMATIVOS Y REGULATORIOS

Es importante tener en cuenta los requisitos normativos relacionados con la seguridad de la información, los cuales se detallan a continuación:

- ***Resolución Ministerial N° 129-2012-PCM:*** aprueban el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2008 EDI Tecnología de la Información. Técnicas de Seguridad. "Requisitos" en todas las entidades integrantes del Sistema Nacional de Informática".
- ***Ley N° 27291:*** ley que permite el uso de medios electrónicos para la manifestación de voluntad y la utilización de la firma electrónica.
- ***Ley N° 27269:*** ley de Firmas y Certificados Digitales.
- ***Ley N° 27309:*** ley que incorpora los delitos informáticos al Código Penal.
- ***Código Penal, Artículo 154:*** delito de violación a la intimidad.
- ***Ley N° 28493:*** ley que regula el uso del correo electrónico comercial no solicitado (SPAM).
- ***Decreto Supremo N°043-2003-PCM:*** texto único ordenado de la ley N° 27806, Ley de Transparencia y Acceso a la Información Pública.
- ***Resolución Jefatural N°088-2003-INEI:*** directiva sobre "Normas para el uso del servicio de correo electrónico en las entidades de la Administración Publica"
- ***Ley N° 28612:*** ley que norma el uso, adquisición y adecuación del software en la administración pública.

- ***Decreto Supremo N° 013-2003-PCM y sus modificaciones***: medidas para garantizar la legalidad de la adquisición de software en entidades y dependencias del sector público.
- ***Ley N° 29733:*** ley de protección de los datos (LOPD) y privacidad de la información personal (artículo 2 numeral 6 de la Constitución Política del Perú).

EVALUACION DEL ESTADO ACTUAL DE LA SEGURIDAD DE LA INFORMACION

La Resolución Ministerial N° 129-2012-PCM indica el uso obligatorio de la Norma Técnica Peruana NTP ISO/IEC 27001:2008, por lo cual todas las instituciones están en la obligación de implementar un Sistema de Gestión de Seguridad de la Información.

Actualmente el Hospital de Apoyo II- 2 Sullana no cuenta con un Sistema de Gestión de Seguridad de la Información por lo cual se ha realizado esta evaluación para determinar los riesgos que existen en el Centro de Datos para una posterior implementación de un SGSI.

IDENTIFICACION DE ACTIVOS DE LA INFORMACION

IDENTIFICACION

Para el Análisis de Riesgos, la NTP ISO/IEC 27005:2009 recomienda iniciar identificando los activos de información, luego valorarlos y priorizarlos; esto para evitar incluir activos de poca relevancia para un futuro SGSI.

El presente proyecto solo se centrara en los activos TI que existen en el Centro de Datos, ya que es muy probable que se identifique información (documentación), personas, ambientes físicos, etc., que deberán ser protegidos.

De acuerdo a la información que el Jefe de la Unidad de Estadística e Informática brindó para este proyecto se determinó elaborar en una tabla.

Tabla 04

Fase preliminar de identificación de activos de información

TIPO	NOMBRE DE ACTIVO	DESCRIPCION DEL ACTIVO DE INFORMACIÓN
INFORMACIÓN	Certificación Presupuestal	Acto de administración, cuya finalidad es garantizar que se cuente con el crédito presupuestario disponible y libre de afectación, autorizada para el año fiscal.
	Pedido de Servicio	Documento creado por un centro de costo (en este caso el Área de Logística del HAS) mediante el cual se solicita al área de Abastecimiento la adquisición de un bien o servicio).
	Orden de Servicio	Luego finalizada la etapa de cotización, se genera la orden del servicio mediante el sistema SIGA.
SOFTWARE	Sistema Integrado de Información de Salud	Tipo de implementación por compra a terceros.
	SIGA – SIAF	Sistema Integrado del Ministerio de Economía y Finanzas, es empleada para la administración del Hospital de Apoyo II- 2 Sullana.
	Sistema Integrado de Salud	Se utiliza para el ingreso de información estadística.
	PIH - Sistema de Recursos Humanos	Se utiliza para el ingreso de información de planillas del HAS.
	Sistema Integrado de Farmacia	Ingreso de la información del movimiento de Farmacia.
	Sistema Información Perinatal	Se registra la información perinatal del HAS.
	Sistema de Trámite Documentario	Ingreso de expedientes internos del HAS - Gobierno Regional de Piura.

	Sistema de Transporte (Movimiento de Vehículos)	Ingreso de información vehicular del HAS.
	SEM - Sistema de Emergencia	Sistema Integrado para el ingreso de información de emergencias del HAS.

Ya identificados los principales activos de información, procedemos a identificar los activos de información de los que depende cada activo de TI detallados en la tabla anterior. Para que un documento, un servicio, o un software existan es muy probable que dependa de otros activos, por lo cual se detalla en la siguiente tabla:

Tabla 05

Dependencia de activos de información.

CLASE DE ACTIVO	NOMBRE	ACTIVO DE INFORMACIÓN DEL QUE DEPENDE
ACTIVOS PRIMARIOS	Certificación presupuestal	Impresora SIAF Sistema Operativo Windows 7 PC Escritorio Servicio de Directorio Activo
	Pedido de Servicio	Impresora SIGA Sistema Operativo Windows 7 PC Escritorio Servicio de Directorio Activo
	Orden de Servicio	Impresora SIGA Sistema Operativo Windows 7 PC Escritorio Servicio de Directorio Activo

ACTIVOS DE SOPORTE	Sistema Integrado de Información de Salud	Base de Datos Gestor de Base de Datos Servidor Base de Datos Sistema Operativo Windows Server 2008 R2 Antivirus Datacenter Aire acondicionado Sistema contra incendios UPS para datacenter Firewall Cableado estructurado Administrador de Base de datos Administrador de Redes y Servidores
	SIGA – SIAF	Base de Datos SIGA/ SIAF Gestor de Base de Datos Servidor Base de Datos SIGA /SIAF Sistema Operativo Windows Server 2012 R2 Antivirus Datacenter Aire acondicionado Sistema contra incendios UPS para datacenter Firewall Cableado estructurado Administrador de Base de datos Administrador de Redes y Servidores
	Sistema Integrado de Salud	Base de Datos Gestor de Base de Datos Servidor Base de Datos Sistema Operativo Windows Server 2008 R2 Antivirus Datacenter Aire acondicionado Sistema contra incendios UPS para datacenter Firewall Cableado estructurado Administrador de Base de datos Administrador de Redes y Servidores

PIH - Sistema de Recursos Humanos	Base de Datos Gestor de Base de Datos Servidor Base de Datos Sistema Operativo Windows Server 2012 R2 Antivirus Datacenter Aire acondicionado Sistema contra incendios UPS para datacenter Firewall Cableado estructurado Administrador de Base de datos Administrador de Redes y Servidores
Sistema Integrado de Farmacia	Base de Datos Gestor de Base de Datos Servidor Base de Datos Sistema Operativo Windows Server 2008 R2 Antivirus Datacenter Aire acondicionado Sistema contra incendios UPS para datacenter Firewall Cableado estructurado Administrador de Base de datos Administrador de Redes y Servidores
Sistema Información Perinatal	Base de Datos Gestor de Base de Datos Servidor Base de Datos Sistema Operativo Windows Server 2008 R2 Antivirus Datacenter Aire acondicionado Sistema contra incendios UPS para datacenter Firewall Cableado estructurado Administrador de Base de datos Administrador de Redes y Servidores

Sistema de Trámite Documentario	Base de Datos Gestor de Base de Datos Servidor Base de Datos Sistema Operativo Windows Server 2012 R2 Antivirus Datacenter Aire acondicionado Sistema contra incendios UPS para datacenter Firewall Cableado estructurado Administrador de Base de datos Administrador de Redes y Servidores
Sistema de Transporte (Movimiento de Vehículos)	Base de Datos Gestor de Base de Datos Servidor Base de Datos Sistema Operativo Windows Server 2008 R2 Antivirus Datacenter Aire acondicionado Sistema contra incendios UPS para datacenter Firewall Cableado estructurado Administrador de Base de datos Administrador de Redes y Servidores
SEM - Sistema de Emergencia	Base de Datos Gestor de Base de Datos Servidor Base de Datos Sistema Operativo Windows Server 2008 R2 Antivirus Datacenter Aire acondicionado Sistema contra incendios UPS para datacenter Firewall Cableado estructurado Administrador de Base de datos Administrador de Redes y Servidores

Es obligatorio identificar al dueño de cada activo de información, para que posteriormente se le asigne la responsabilidad de velar por la integridad, disponibilidad y confidencialidad de sus activos de información. La categorización de activos (clase de activo) se basa

también en lo que nos especifica la NTP ISO/IEC 27005: 2009; activos primarios y activos de soporte (Anexo B de la norma antes mencionada). Luego de detallar cada uno de estos activos solo se hablara de los activos de soporte relacionado a las Tecnologias de Información específicamente.

Tabla 06

Consolidado de Activos de Información de TI

CLASE DE ACTIVO	TIPO	NOMBRE DE ACTIVO	Encargado
ACTIVOS PRIMARIOS	INFORMACIÓN	Certificación presupuestal	Logística
		Pedido de servicio	Dirección de administración
		Orden de Servicio	Dirección de administración
ACTIVOS DE SOPORTE	SOFTWARE	Antivirus	Área de Informática
		Gestor de Base de Datos	Área de Informática
		Microsoft Word	Área de Informática
		Servicio de Directorio Activo	Área de Informática
		Servicio de DNS	Área de Informática
		Sistema operativo Windows 7	Área de Informática
		Sistema Operativo Windows server 2008 r2	Área de Informática
		Sistema Operativo Windows server 2012 r2	Área de Informática
		Sistema SIAF	Ministerio de Economía y Finanzas
		Sistema SIGA	Ministerio de Economía y Finanzas
		Sistema Integrado de Información de Salud	Compra de terceros
		Sistema Integrado de Salud	Ministerio de Salud
		PIH - Sistema de RR.HH.	Ministerio de Salud
		Sistema Integrado de Farmacia	Ministerio de Salud
		Sistema Información Perinatal	Ministerio de Salud
		Sistema de Trámite Documentario	Gobierno Regional de Piura
		Sistema de Transporte (Moví. Vehicular)	Área de Informática
		SEM - Sistema de Emergencia	Área de Informática
	HARDWARE	Impresora	Logística

		Pc Escritorio	Área de Informática
		Servidor Base de Datos	Área de Informática
		Servidor de Directorio Activo y DNS	Área de Informática
		UPS para Datacenter	Área de Informática
	REDES	Cableado Estructurado	Área de Informática
		Firewall	Área de Informática
		Router ISP	Área de Informática
		Servicio de Internet	Área de Informática
		Switch Acceso	Área de Informática
	PERSONAL	Administrador de Base de Datos	Área de Informática
		Administrador de Redes y Servidores	Área de Informática
	SITIO	Aire acondicionado	Área de Informática
		Datacenter	Área de Informática
		Sistema contra incendios del datacenter	Área de Informática

VALORACION DE ACTIVOS

Teniendo en cuenta la NTP ISO/IEC 27005:2009, la valoración de los activos puede ser mediante una estimación cualitativa o cuantitativa. En este proyecto se ha optado tener la estimación cualitativa, basándome en los tres pilares de un SGSI que son confidencialidad, integridad y disponibilidad; también se podría realizar la combinación de ambas, la norma no la restringe; es decisión de la organización que tipo de estimación aplicar. Para iniciar la valoración se define los siguientes parámetros que permitirán determinar si es un activo crítico o no.

Tabla 07

Leyenda valoración de activos desde el punto de vista de confidencialidad.

CONFIDENCIALIDAD		
C	Confidencial	Activo restringido para el Jefe de la UEI
I	Uso interno	Activo dispuesto para el Jefe de la UEI

P	Uso Publico	Activo dispuestos para el personal de la UEI

Tabla 08

Leyenda valoración desde el punto de vista de integridad.

INTEGRIDAD		
S	Sensible	Activo que requiere controles estrictos para su protección
I	Normal	Activo que requiere controles habituales para su protección
P	Baja	Activo que requiere controles mínimos para su protección

Tabla 08

Leyenda valoración desde el punto de vista de disponibilidad.

DISPONIBILIDAD		
MA	Muy alta	Tiempo tolerable de interrupción menor a 2 horas
A	Alta	Tiempo tolerable mayor a 2 horas y menos a 4 horas
M	Media	Tiempo tolerable mayor a 4 horas y menor a 1 día
B	Baja	Tiempo tolerable mayor a 1 día y menor a 2 días
MB	Muy baja	Tiempo tolerable mayor a 2 días y menor a 7 días

Tabla 10

Posible valor de un activo

VALORACION DEL ACTIVO		
CODIGO	**VALOR**	**DESCRIPCION**
A	Alto	Nivel confidencialidad: confidencial
		Nivel integridad: sensible
		Nivel disponibilidad: muy alta, alta
M	Medio	Nivel confidencialidad: uso interno
		Nivel integridad: normal
		Nivel disponibilidad: media
B	Bajo	Nivel confidencialidad: uso publico
		Nivel integridad: baja
		Nivel disponibilidad: baja, muy baja

Teniendo en cuenta los valores de las tablas 10, 11, 12 y 13, se ha elaborado en Microsoft Office Excel donde permite determinar el valor de los activos de TI identificados mostrados a continuación:

ID	ACTIVO	TIPO DE ACTIVO	CLASIFICACION DE INFORMACION			VALORACION DEL ACTIVO	
			ONFIDENCIALID	INTEGRIDAD	DISPONIBILIDAD	NIVEL	VALOR
INF01	base de datos SIAF	INF	confidencial	SENSIBLE	ALTA	ALTO	3
INF02	base de datos SIGA	INF	confidencial	sensible	muy alta	alto	3
SW01	gestor de base de datos	SW	confidencial	sensible	muy alta	alto	3
SW02	microsoft word	SW	uso interno	baja	muy baja	medio	2
SW03	serviicio de directorio activo	SW	uso interno	normal	muy alta	alto	3
SW04	servicio de DNS	SW	uso interno	normal	muy alta	alto	3
SW05	sistema SIAF	SW	confidencial	sensible	muy alta	alto	3
SW06	sistema SIGA	SW	confidencial	sensible	muy alta	alto	3
SW07	sistema operativo windows 7	SW	uso interno	baja	baja	medio	2
SW08	Sistema operativo windows server 2008 R2	SW	uso interno	normal	muy alta	alto	3
SW09	antivirus	SW	uso interno	sensible	muy alta	alto	3
HW01	impresora	HW	uso interno	baja	muy baja	medio	2
HW02	PC escritorio	HW	uso interno	normal	baja	medio	2
HW03	servidor base de datos SIGa	HW	confidencial	sensible	muy alta	alto	3
HW04	servidor de directorio activo y DNS	HW	confidencial	sensible	muy alta	alto	3
HW05	servidor SIAF	HW	confidencial	sensible	muy alta	alto	3
HW06	UPS para datacenter	HW	uso interno	normal	muy alta	alto	3
RED01	cableado estructurado	REDES	uso interno	normal	muy alta	alto	3
RED02	firewall	REDES	uso interno	sensible	muy alta	alto	3
RED03	router ISP	REDES	uso interno	baja	muy alta	alto	3
RED04	servicio de internet	REDES	uso interno	normal	muy alta	alto	3
RED05	switch acceso	REDES	uso interno	normal	alta	alto	3
PER01	administrador de base de datos	PERSONAL	confidencial	sensible	muy alta	alto	3
PER02	administrador de redes y servidores	PERSONAL	confidencial	sensible	muy alta	alto	3
AMB01	aire acondicionado	AMBIENTE	uso intenro	normal	muy alta	alto	3
AMB02	datacenter	AMBIENTE	confidencial	normal	muy alta	alto	3
AMB03	sistema contra incendios del datacenter	AMBIENTE	uso interno	normal	muy alta	alto	3

Figura 06: Fase preliminar valoración de activos de la información.

Luego de haber determinado la valoración de activos, solo tomaremos los activos más críticos (Valor Alto-3), y con ellos continuaremos el análisis de riesgos. No tendría sentido incluir todos los activos de información identificados, debido a que el análisis se volvería muy complejo, y la implementación de controles a todos los activos probablemente sería innecesaria, costosa y el Hospital de Apoyo II – 2 Sullana es muy probable que no opte por una futura implementación de un SGSI.

Teniendo en cuenta lo anterior dicho de los 27 activos de información de TI identificados; solo 23 pasaran por el análisis de riesgos.

Como se puede observar en la siguiente figura, cada activo está debidamente codificado, clasificado por un tipo (como puede ser información, software, hardware, etc.). Clasificación basada en los pilares de la seguridad de la información y la valoración de activos. Esto permite tener el inventario de los activos de información que serán actualizados periódicamente, algunos de ellos ya no figuraran, otros continuaran y nuevos surgirán.

ID	ACTIVO	TIPO DE ACTIVO	CLASIFICACION DE INFORMACION			VALORACION DEL ACTIVO	
			)NFIDENCIALID	INTEGRIDAD	DISPONIBILIDAD	NIVEL	VALOR
INF01	base de datos SIAF	INF	confidencial	SENSIBLE	ALTA	ALTO	3
INF02	base de datos SIGA	INF	confidencial	sensible	muy alta	alto	3
SW01	gestor de base de datos	SW	confidencial	sensible	muy alta	alto	3
SW03	serviicio de directorio activo	SW	uso interno	normal	muy alta	alto	3
SW04	servicio de DNS	SW	uso interno	normal	muy alta	alto	3
SW05	sistema SIAF	SW	confidencial	sensible	muy alta	alto	3
SW06	sistema SIGA	SW	confidencial	sensible	muy alta	alto	3
SW08	Sistema operativo windows server 2008 R2	SW	uso interno	normal	muy alta	alto	3
SW09	antivirus	SW	uso interno	sensible	muy alta	alto	3
HW03	servidor base de datos SIGa	HW	confidencial	sensible	muy alta	alto	3
HW04	servidor de directorio activo y DNS	HW	confidencial	sensible	muy alta	alto	3
HW05	servidor SIAF	HW	confidencial	sensible	muy alta	alto	3
HW06	UPS para datacenter	HW	uso interno	normal	muy alta	alto	3
RED01	cableado estructurado	REDES	uso interno	normal	muy alta	alto	3
RED02	firewall	REDES	uso interno	sensible	muy alta	alto	3
RED03	router ISP	REDES	uso interno	baja	muy alta	alto	3
RED04	servicio de internet	REDES	uso interno	normal	muy alta	alto	3
RED05	switch acceso	REDES	uso interno	normal	alta	alto	3
PER01	administrador de base de datos	PERSONAL	confidencial	sensible	muy alta	alto	3
PER02	administrador de redes y servidores	PERSONAL	confidencial	sensible	muy alta	alto	3
AMB01	aire acondicionado	AMBIENTE	uso intenro	normal	muy alta	alto	3
AMB02	datacenter	AMBIENTE	confidencial	normal	muy alta	alto	3
AMB03	sistema contra incendios del datacenter	AMBIENTE	uso interno	normal	muy alta	alto	3

Figura 07: Activos de Información de TI para análisis de riesgo.

IDENTIFICACIÓN Y VALORACIÓN DE AMENAZAS

Como se ha mencionado en las bases teóricas sobre la decisión de amenazas por diferentes autores, en la NTP ISO/IEC 27005:2009 también se hace referencia a ello:

Una amenaza tiene el potencial de causar daños a activos tales como información, procesos y sistemas y, por lo tanto, a las organizaciones. Las amenazas pueden ser de origen natural o humano y podrían ser accidentales o deliberadas. Es recomendable identificar tanto los orígenes de las amenazas accidentales como de las deliberadas. Una amenaza puede tener su origen dentro o fuera de la organización. Las amenazas se deberían identificar genéricamente y por tipo (por ejemplo; acciones no autorizadas, daño físico, fallas técnicas) y, cuando sea adecuado, las amenazas individuales dentro de la clase generia identificada. Esto significa que ninguna amenaza se pasa por alto, incluidas las inesperadas, pero teniendo en cuenta que el volumen de trabajo requerido es limitado.

La identificación de las amenazas y la estimación de la probabilidad de ocurrencia puede ser obtenida de los propietarios o de los usuarios del activo, del personal de recursos humanos, del administrador de las instalaciones y de especialistas en seguridad de la información, expertos en seguridad física, área jurídica y otras organizaciones que incluyen organismos legales, bien sea autoridades, compañías de seguros y autoridades del Hospital de Apoyo II – 2 Sullana.

Teniendo en cuenta las indicaciones obtenidas de la NTP ISO/IEC 27005:2009 y que han sido mencionadas en el párrafo anterior, se han identificado las amenazas como se muestran en las siguientes tablas:

Tabla 11

Origen de amenazas

ORIGEN DE AMENAZAS	
A	Accidentales
D	Deliberadas
E	Ambientales

Tabla 12

Lista de amenazas identificadas

ID	AMENAZA	ORIGEN
A01	Abuso de privilegios	A; D
A02	Acceso al sistema por parte de usuarios que no deberían tener acceso a determinados perfiles de acceso al sistema	A,D
A03	Acceso de personas ajenas a la institución quienes podrían robar información	A,D
A04	Acceso no autorizado a la red	D
A05	Acceso no autorizado al datacenter	A,D
A06	Accidentes del personal	A,D
A07	Ataque de hackers a las vulnerabilidades de las aplicaciones	D
A08	Caída del servicio	A,D,E
A09	Cambio de configuraciones no autorizadas en las aplicaciones o servicios	A,D
A10	Corrupción de datos	A,D,E
A11	Deterioro / Obsolencia de equipamiento	A,D,E
A12	Deterioro de infraestructura física	A,D,E
A13	Deterioro del cableado de red	A,D,E
A14	Errores de operación de los usuarios	A,D
A15	Fácil descifrado de las contraseñas de los usuarios por parte de personas inescrupulosos	D
A16	Falla / corte del servicio de internet	A,D,E

A17	Falla / corte de suministro eléctrico	A,D,E
A18	Falla de equipo	A, D,E
A19	Falla equipo de aire acondicionado	A, D, E
A20	Fallo del sistema contra incendios	A, D, E
A21	Fallo UPS principal del datacenter	A, D, E
A22	Filtraciones de información y accesos no autorizados al sistema	
A23	Incendios	A, D
A24	Infección de software malicioso	A
A25	Interferencia electromagnética	A, D, E
A26	Inundaciones	A, D, E
A27	Mal funcionamiento del sistema	
A28	Manipulación de hardware	A, D
A29	Penetración y propagación de virus en la intranet por mal uso de internet / o memorias extraíbles	A, D
A30	Renuncia / ausentismo del personal de la UEI	A, D
A31	Robo de equipamiento	D
A32	Robo de información	D
A33	Saturación del servicio	A, D

Luego de haber identificado las amenazas, las relacionaremos con los activos de información de TI vinculados al análisis de riesgos; procedemos a valorar cada una de las amenazas teniendo en cuenta la probabilidad de ocurrencias y que es descrita en la siguiente tabla:

Tabla 13

Leyenda valoración de amenazas

PROB. DE OCURRENCIA	**DEFINICION**
Muy alta=4	Una vez al mes
Alta=3	Trimestral
Media=2	Semestral

Baja=1	Una vez cada 1 año o mas

Tabla 14

Vinculación de activos y amenazas, valoración de amenazas

ID	ACTIVO	AMENAZAS	VALORACION
INF01	DB SIAF	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	1
		Filtraciones de información y accesos no autorizados al sistema	2
		Corrupción de datos	3
		Robo de información	1
		Abuso de privilegios	2
INF02	BASE DE DATOS SIGA	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	1
		Filtraciones de información y accesos no autorizados al sistema	2
		Corrupción de datos	1
		Robo de información	1
		Abuso de privilegios	1
SW01	GESTOR DE BASE DE DATOS	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3
		Caída del servicio	4
		Saturación del servicio	2
		Ataque de hackers a las vulnerabilidades de las aplicaciones	1
		Mal funcionamiento del sistema	1
SW02	SERVICIO DE DIRECTORIO ACTIVO	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	1
		Caída del servicio	3
		Saturación del servicio	2
		Ataque de hackers a las vulnerabilidades de las aplicaciones	1
		Acceso no autorizado a la red	1
		Mal funcionamiento del sistema	1
		Penetración y propagación de virus en la intranet por mal uso de internet / o	1

		memorias extraíbles	
		Abuso de privilegios	1
SW03	SERVICIO DE DNS	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	1
		Caída del servicio	3
		Saturación del servicio	2
		Ataque de hackers a las vulnerabilidades de las aplicaciones	1
		Acceso no autorizado a la red	1
		Mal funcionamiento del sistema	1
		Penetración y propagación de virus en la intranet por mal uso de internet / o memorias extraíbles	1
		Abuso de privilegios	1
SW04	SISTEMA SIAF	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	4
		Caída del servicio	4
		Saturación del servicio	4
		Ataque de hackers a las vulnerabilidades de las aplicaciones	1
		Errores de operación de los usuarios	2
		Filtraciones de información y accesos no autorizados al sistema	4
		Robo de información	1
		Mal funcionamiento del sistema	4
		Fácil descifrado de las contraseñas de los usuarios por parte de personas inescrupulosas	4
		Acceso de personas ajenas a la institución quienes podría robar información	2
		Abuso de privilegios	4
SW05	SISTEMA SIGA	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3
		Caída del servicio	3
		Saturación del servicio	3
		Ataque de hackers a las vulnerabilidades de las aplicaciones	1
		Errores de operación de los usuarios	4
		Filtraciones de información y accesos no autorizados al sistema	2
		Robo de información	1
		Mal funcionamiento del sistema	3
		Fácil descifrado de las contraseñas de los	4

		usuarios por parte de personas inescrupulosas	
		Acceso de personas ajenas a la institución quienes podría robar información	4
		Abuso de privilegios	1
SW06	SISTEMA OPERATIVO WINDOWS SERVER 2008 R2	Acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	1
		Caída del servicio	3
		Saturación del servicio	2
		Ataque de hackers a las vulnerabilidades de las aplicaciones	1
		Acceso no autorizado a la red	1
		Mal funcionamiento del sistema	2
		Infección de software malicioso	1
		Penetración y propagación de virus en la intranet por mal uso de internet / o memorias extraíbles	1
		Abuso de privilegios	1
SW07	ANTIVIRUS	Infección de software malicioso	3
		Penetración y propagación de virus en la intranet por mal uso de internet / o memorias extraíbles	3
		Abuso de privilegios	1
HW03	SERVIDOR DE BASE DE DATOS SIGA	Incendios	1
		Falla / corte de suministro eléctrico	3
		Robo de equipamiento	1
		Falla de equipo	1
		Deterioro / obsolescencia de equipamiento	2
		Manipulación de hardware	2
HW04	SERVIDOR DE DIRECTORIO ACTIVO Y DNS	Incendios	1
		Falla / corte de suministro eléctrico	3
		Robo de equipamiento	1
		Falla de equipo	1
		Deterioro / obsolescencia de equipamiento	2
		Manipulación de hardware	2
HW05	SERVIDOR SIAF	Incendios	1
		Falla / corte de suministro eléctrico	3
		Robo de equipamiento	1
		Falla de equipo	1
		Deterioro / obsolescencia de equipamiento	4
		Manipulación de hardware	2
HW06	UPS PARA DATACENTER	Incendios	1
		Fallo UPS principal del datacenter	1
		Deterioro / obsolescencia	4

		Manipulación de hardware	1
RED01	CABLEADO ESTRUCTURADO	Interferencia electromagnética	1
		Deterioro del cableado de red	2
		Acceso no autorizado a la red	2
RED02	FIREWALL	Incendios	1
		Saturación del servicio	2
		Falla / corte de suministro eléctrico	3
		Robo de equipamiento	1
		Ataque de hackers a las vulnerabilidades de las aplicaciones	1
		Falla de equipo	1
		Deterioro / obsolescencia de equipamiento	1
		Acceso no autorizado a la red	1
		Manipulación de hardware	2
		Abuso de privilegios	4
RED03	ROUTER ISP	Incendios	1
		Falla / corte de suministro eléctrico	3
		Robo de equipamiento	1
		Ataque de hackers a las vulnerabilidades de las aplicaciones	1
		Falla de equipo	1
		Deterioro / obsolescencia de equipamiento	1
		Acceso no autorizado a la red	1
		Manipulación de hardware	1
RED04	SERVICIO DE INTERNET	Falla / corte del servicio de internet	2
RED05	SWITCH DE ACCESO	Incendios	1
		Saturación del servicio	1
		Falla / corte de suministro eléctrico	3
		Robo de equipamiento	1
		Ataque de hackers a las vulnerabilidades de las aplicaciones	1
		Falla de equipo	1
		Deterioro / obsolescencia de equipamiento	4
		Acceso no autorizado a la red	1
		Manipulación de hardware	3
PER01	ADMINISTRADOR DE BASE DE DATOS	Renuncia / ausentismo del personal al centro de labores	1
		Accidentes del personal	1
PER02	ADMINISTRADOR DE REDES Y SERVIDORES	Renuncia / ausentismo del personal al centro de labores	1
		Accidentes del personal	1
AMB01	AIRE ACONDICIONADO	Incendios	1
		Inundaciones	1
		Falla equipo de aire acondicionado	2
		Falla / corte de suministro eléctrico	3

		Deterioro / obsolescencia de equipamiento	2
AMB02	DATACENTER	Incendios	1
		Acceso no autorizado al datacenter	4
		Inundaciones	1
		Falla / corte de suministro eléctrico	3
		Deterioro de la infraestructura física	2
AMB03	SISTEMA CONTRA INCENDIOS DEL DATACENTER	Incendios	1
		Inundaciones	1
		Fallo del sistema contra incendios	1
		Deterioro / obsolescencia de equipamiento	2

La valoración de amenazas nos servirá posteriormente para sacar el nivel de riesgo al que está expuesto un activo de información. Pero antes de ellos procederemos con identificar y valorar las vulnerabilidades de cada uno de los activos de información ya identificados.

IDENTIFICACIÓN Y VALORACIÓN DE VULNERABILIDADES

Basándome en la norma NTP ISO/IEC 27005:2009, tenemos como entradas la lista de amenazas, los activos de información.

La sola presencia de una vulnerabilidad no causa daño por sí misma, dado que es necesario que exista una amenaza presente para explotarla. Una vulnerabilidad que no tiene amenaza puede no requerir de la implementación de un control, pero es recomendable reconocerla y monitorearla para determinar los cambios.

A continuación se detallan las vulnerabilidades encontradas en base a entrevista al personal responsable y a los hallazgos previa inspección visual:

Tabla 15

Lista de vulnerabilidades identificadas

ID	VULNERABILIDAD
V01	Aplicación desactualizada o parchada deficientemente
V02	Ausencia de bitácoras de los sistemas
V03	Ausencia de capacitación en la manipulación de hardware
V04	Ausencia de código fuente
V05	Ausencia de documento de la implementación y configuración de los servicios que están en producción
V06	Ausencia de equipos de comunicación de respaldo
V07	Ausencia de grupo electrógeno
V08	Ausencia de mantenimiento a la instalaciones
V09	Ausencia de mantenimiento periódico a los equipos de comunicaciones
V10	Ausencia de mantenimiento periódico del UPS
V11	Ausencia de mantenimiento y pruebas periódicas al sistema contra incendios del datacenter
V12	Ausencia de mapeo de red / mapeo de puntos de red
V13	Ausencia de monitoreo de servicios
V14	Ausencia de políticas de confidencialidad de información
V15	ausencia de política y procedimientos para la gestión de cuentas de usuarios
V16	ausencia de política y procedimientos para realizar mantenimientos preventivos periódicos de HW
V17	Ausencia de procedimientos estandarizados para actualización de parches de seguridad del software
V18	Ausencia de registros de los ingresos al datacenter
V19	Ausencia de segregación de funciones
V20	Cables de red sin protección, sin etiquetas y desordenadas
V21	Contraseñas de cuentas de usuarios sencilla
V22	Controles de acceso al sistema deficiente
V23	Cuentas de acceso activas de personas cuyo vinculo laborar con HAS ha concluido
V24	Deficiente control de acceso a la red
V25	Deficiente control de acceso a las instalaciones
V26	Deficiente proceso de copias de seguridad o de respaldo de información (backups)
V27	Falta de políticas para el uso adecuado de aplicativos
V28	Políticas de firewall inadecuadas

V29	Presencia de material inflamable en el ambiente contiguo al datacenter
V30	Servicio no configurado en alta disponibilidad
V31	Servidores ubicados en mesa
V32	Puertos de red sin uso y habilitados
V33	Dependencia de un solo personal para estas funciones

Luego de identificar e inventariar las vulnerabilidades, estas deben de ser valoradas en relación a la probabilidad de que una amenaza explote la vulnerabilidad o debilidad que se identificó para cada activo de información. Es por ello que las siguientes dos tablas muestran primero el criterio de valoración y la relación entre activos de información, amenazas y vulnerabilidades. Luego de ello determinaremos los niveles de riesgo a los que están expuestos los activos de información.

Tabla 16

Valores que puede tomar la vulnerabilidad

VALOR	VULNERABILIDAD	DESCRIPCIÓN
3	ALTA	Fácil de ser explotar / para protección
2	MEDIA	Posibilidad de ser explotada
1	BAJA	Difícil de explotar / existen buenos controles implementados

Tabla 17

Valoración de vulnerabilidades

ACTIVOS	VULNERABILIDADES	AMENAZAS	FACILIDAD DE EXPLOTACION

BASE DE DATOS SIAF	ausencia de bitácoras de los sistemas	acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3
	ausencia de políticas de confidencialidad de información	acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	2
	cuenta de acceso activas de persona cuyo vínculo laboral con el HAS ha concluido	acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3

	ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3
	controles de acceso al sistema deficientes	acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	2
	ausencia de bitácoras de los sistemas	filtraciones de información y acceso no autorizados al sistema	2
	ausencia de políticas de confidencialidad de información	filtraciones de información y accesos no autorizados al sistema	3

	cuenta de acceso activas de persona cuyo vínculo laboral con el HAS ha concluido	filtraciones de información y accesos no autorizados al sistema	3
	ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	filtraciones de información y accesos no autorizados al sistema	3
	controles de acceso al sistema deficientes	filtraciones de información y accesos no autorizados al sistema	3
	deficiente proceso de copias de seguridad o de respaldo de información (backups)	corrupción de datos	2
	ausencia de políticas y procedimientos para la gestión de respaldo de información (backups)	corrupción de datos	2
	ausencia de bitácoras de los sistemas	robo de información	2

	ausencia de políticas de procedimientos para la gestión de cuentas de usuarios	robo de información	3
	controles de acceso al sistema deficientes	robo de información	3
	ausencia de bitácoras de los sistemas	abuso de privilegios	2
	ausencia de políticas de confidencialidad de información	abuso de privilegios	3
	cuentas de acceso activas de persona cuyo vínculo laboral con el HAS ha concluido	abuso de privilegios	3
	ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	abuso de privilegios	3
	controles de acceso al sistema deficientes	abuso de privilegios	3
BASE DE DATOS SIGA	ausencia de bitácoras de los sistemas	acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	2

	ausencia de políticas de confidencialidad de información	acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	2
	cuenta de acceso activas de persona cuyo vínculo laboral con el HAS ha concluido	acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3
	ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	2
	controles de acceso al sistema deficientes	acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	2
	ausencia de bitácoras de los sistemas	filtraciones de información y acceso no autorizados al sistema	2
	ausencia de políticas de confidencialidad de información	filtraciones de información y accesos no autorizados al sistema	3

	cuenta de acceso activas de persona cuyo vínculo laboral con el HAS ha concluido	filtraciones de información y accesos no autorizados al sistema	3
	ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	filtraciones de información y accesos no autorizados al sistema	3
	controles de acceso al sistema deficientes	filtraciones de información y accesos no autorizados al sistema	3
	deficiente proceso de copias de seguridad o de respaldo de información (backups)	corrupción de datos	2
	ausencia de políticas y procedimientos para la gestión de respaldo de información (backups)	corrupción de datos	2
	ausencia de bitácoras de los sistemas	robo de información	2
	ausencia de políticas de confidencialidad de información	robo de información	3
	cuentas de acceso activas de persona cuyo vínculo laboral con el HAS ha concluido	robo de información	3

	ausencia de bitácoras de los sistemas	abuso de privilegios	2
	ausencia de políticas de confidencialidad de información	abuso de privilegios	3
	cuentas de acceso activas de persona cuyo vínculo laboral con el HAS ha concluido	abuso de privilegios	3
	ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	abuso de privilegios	3
	controles de acceso al sistema deficientes	abuso de privilegios	3
GESTOR DE BASE DE DATOS	ausencia de bitácoras de los sistemas	acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	2
	ausencia de políticas de confidencialidad de información	acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	2

	cuenta de acceso activas de persona cuyo vínculo laboral con el HAS ha concluido	acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3
	ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	2
	controles de acceso al sistema deficientes	acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	2
	servicio no configurado en alta disponibilidad	caída del servicio	3
	ausencia de documentación de implementación y configuración de los servicios que están en producción	caída del servicio	3
	ausencia de monitoreo de servicios	caída del servicio	3
	aplicación desactualizada o parchada deficientemente	caída del servicio	3

	ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	caída del servicio	3
	ausencia de bitácoras de los sistemas	ataque de hackers a las vulnerabilidades de las aplicaciones	2
	ausencia de monitoreo de servicios	ataque de hackers a las vulnerabilidades de las aplicaciones	2
	aplicación desactualizada o parchada deficientemente	ataque de hackers a las vulnerabilidades de las aplicaciones	3
	ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	ataque de hackers a las vulnerabilidades de las aplicaciones	2
	ausencia de bitácoras de los sistemas	saturación del servicio	2
	servicio no configurado en alta disponibilidad	saturación del servicio	3
	aplicación desactualizada o parchada deficientemente	saturación del servicio	3

	ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	saturación del servicio	3
	ausencia de documentación de implementación y configuración de los servicios que están en producción	mal funcionamiento del sistema	3
	ausencia de monitoreo de servicios	mal funcionamiento del sistema	2
	aplicación desactualizada o parchada deficientemente	mal funcionamiento del sistema	2
	ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	mal funcionamiento del sistema	3
SERVICIO DE DIRECTORIO ACTIVO	ausencia de bitácoras de los sistemas	acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	2

	ausencia de políticas de confidencialidad de información	acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	2
	cuenta de acceso activas de persona cuyo vínculo laboral con el HAS ha concluido	acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3
	ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	2
	controles de acceso al sistema deficientes	acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	2
	Ausencia de bitácoras de los sistemas	caída del servicio	1
	servicio no configurado en alta disponibilidad	caída del servicio	3

	ausencia de documentación de implementación y configuración de los servicios que están en producción	caída del servicio	3
	ausencia de monitoreo de servicios	caída del servicio	3
	aplicación desactualizada o parchada deficientemente	caída del servicio	3
	ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	caída del servicio	3
	ausencia de bitácoras de los sistemas	saturación del servicio	2
	servicio no configurado en alta disponibilidad	saturación del servicio	3
	ausencia de documentación de implementación y configuración de los servicios que están en producción	saturación del servicio	3
	ausencia de monitoreo de servicios	saturación del servicio	3
	aplicación desactualizada o parchada deficientemente	saturación del servicio	2

	ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	saturación del servicio	2
	ausencia de bitácoras de los sistemas	ataque de hackers a las vulnerabilidades de las aplicaciones	2
	ausencia de monitoreo de servicios	ataque de hackers a las vulnerabilidades de las aplicaciones	2
	aplicación desactualizada o parchada deficientemente	ataque de hackers a las vulnerabilidades de las aplicaciones	3
	ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	ataque de hackers a las vulnerabilidades de las aplicaciones	2
	ausencia de bitácoras de acceso a la red	acceso no autorizado a la red	2
	deficiente control de acceso a la red	acceso no autorizado a la red	3
	ausencia de monitoreo de servicios	acceso no autorizado a la red	2
	ausencia de bitácoras de los sistemas	mal funcionamiento del sistema	2

	ausencia de documentación de implementación y configuración de los servicios que están en producción	mal funcionamiento del sistema	3
	ausencia de monitoreo de servicios	mal funcionamiento del sistema	2
	aplicación desactualizada o parchada deficientemente	mal funcionamiento del sistema	2
	ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	mal funcionamiento del sistema	3
	ausencia de bitácoras de los sistemas	Penetración y propagación de virus en la intranet por mal uso de internet / o memorias extraíbles	1
	ausencia de monitoreo de servicios	Penetración y propagación de virus en la intranet por mal uso de internet / o memorias extraíbles	2
	ausencia de bitácoras de los sistemas	abuso de privilegios	2
	ausencia de políticas de confidencialidad de información	abuso de privilegios	3

	cuentas de acceso activas de persona cuyo vínculo laboral con el HAS ha concluido	abuso de privilegios	3
	ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	abuso de privilegios	3
	controles de acceso al sistema deficientes	abuso de privilegios	3
SERVICIO DE DNS	ausencia de bitácoras de los sistemas	acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	2
	ausencia de políticas de confidencialidad de información	acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	2
	cuenta de acceso activas de persona cuyo vínculo laboral con el HAS ha concluido	acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3

	ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	2
	controles de acceso al sistema deficientes	acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	2
	Ausencia de bitácoras de los sistemas	caída del servicio	1
	servicio no configurado en alta disponibilidad	caída del servicio	3
	ausencia de documentación de implementación y configuración de los servicios que están en producción	caída del servicio	3
	ausencia de monitoreo de servicios	caída del servicio	3
	aplicación desactualizada o parchada deficientemente	caída del servicio	3

	ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	caída del servicio	3
	ausencia de bitácoras de los sistemas	saturación del servicio	2
	servicio no configurado en alta disponibilidad	saturación del servicio	3
	ausencia de documentación de implementación y configuración de los servicios que están en producción	saturación del servicio	3
	ausencia de monitoreo de servicios	saturación del servicio	3
	aplicación desactualizada o parchada deficientemente	saturación del servicio	2
	ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	saturación del servicio	2
	ausencia de bitácoras de los sistemas	ataque de hackers a las vulnerabilidades de las aplicaciones	2

	ausencia de monitoreo de servicios	ataque de hackers a las vulnerabilidades de las aplicaciones	2
	aplicación desactualizada o parchada deficientemente	ataque de hackers a las vulnerabilidades de las aplicaciones	3
	ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	ataque de hackers a las vulnerabilidades de las aplicaciones	2
	ausencia de bitácoras de acceso a la red	acceso no autorizado a la red	2
	deficiente control de acceso a la red	acceso no autorizado a la red	3
	ausencia de monitoreo de servicios	acceso no autorizado a la red	2
	ausencia de bitácoras de los sistemas	mal funcionamiento del sistema	2
	ausencia de documentación de implementación y configuración de los servicios que están en producción	mal funcionamiento del sistema	3
	ausencia de monitoreo de servicios	mal funcionamiento del sistema	2

	ausencia de procedimientos estandarizados para actualización de parches de seguridad del software	mal funcionamiento del sistema	3
	ausencia de bitácoras de los sistemas	Penetración y propagación de virus en la intranet por mal uso de internet / o memorias extraíbles	1
	ausencia de monitoreo de servicios	Penetración y propagación de virus en la intranet por mal uso de internet / o memorias extraíbles	2
	ausencia de bitácoras de los sistemas	abuso de privilegios	2
	ausencia de políticas de confidencialidad de información	abuso de privilegios	3
	cuentas de acceso activas de persona cuyo vínculo laboral con el HAS ha concluido	abuso de privilegios	3
	ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	abuso de privilegios	3
	controles de acceso al sistema deficientes	abuso de privilegios	3

ANTIVIRUS	ausencia de bitácoras de los sistemas	infección de software malicioso	2
	ausencia de monitoreo de servicios	infección de software malicioso	3
	ausencia de bitácoras de los sistemas	Penetración y propagación de virus en la intranet por mal uso de internet / o memorias extraíbles	1
	ausencia de monitoreo de servicios	Penetración y propagación de virus en la intranet por mal uso de internet / o memorias extraíbles	2
	ausencia de bitácoras de los sistemas	abuso de privilegios	2
	ausencia de políticas de confidencialidad de información	abuso de privilegios	3
	cuentas de acceso activas de persona cuyo vínculo laboral con el HAS ha concluido	abuso de privilegios	3
	ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	abuso de privilegios	3
	controles de acceso al sistema deficientes	abuso de privilegios	3

UPS PARA DATACENTER	presencia de material inflamable en el ambiente contiguo al datacenter	incendios	3
	ausencia de mantenimiento y pruebas periódicas al sistemas contra incendios del datacenter	incendios	3
	ausencia de mantenimiento periódico del UPS	fallo UPS principal del datacenter	3
	ausencia de mantenimiento periódico del UPS	deterioro / obsolescencia de equipamiento	3
	ausencia de mantenimiento a las instalaciones	deterioro / obsolescencia de equipamiento	1
	ausencia de capacitación en la manipulación de hardware	manipulación de hardware	2
	ausencia de políticas y procedimientos preventivos periódicos de HW	manipulación de hardware	2
CABLEADO ESTRUCTURADO	cables de red sin protección, sin etiquetas y desordenados	interferencia electromagnética	1
	ausencia de mantenimiento periódico a los equipos de comunicaciones	deterioro del cableado de red	2

	cables de red sin protección, sin etiquetas y desordenados	deterioro del cableado de red	3
	ausencia de mapeo de red / mapeo de puntos de red	acceso no autorizado a la red	2
	cables de red sin protección, sin etiquetas y desordenados	acceso no autorizado a la red	2
	deficiente control de acceso a la red	acceso no autorizado a la red	3
	puertos de red sin uso y habilitados	acceso no autorizado a la red	3
SERVICIO DE INTERNET	ausencia de Grupo Electrógeno	falla / corte del servicio de internet	3

Valoración de riesgo

Todo el proceso realizado para identificar y valorar los activo de información, amenazas y vulnerabilidades nos permitirán determinar / identificar los niveles de riesgos a los cuales está expuesto cada activo de información, para que posteriormente se realice el proceso de tratamiento de los riesgos que para el presente proyecto no se realizara, ya que será decisión de la institución implementar los salvaguardas necesarios para reducir el riesgos de los activos de información.

Para determinar el riesgo de los activos de información (Anexo E de la NTP ISO/IEC 27005: 2009) nos basaremos en la siguiente tabla, teniendo en cuenta los valores de las amenazas Baja (1), Media (2), Alta (3), Muy Alta (4), los

valores adoptadas por las vulnerabilidades Baja (1), Media (2), Alta (3); adicional a ello el impacto determinado por la valoración de cada uno de los activos de información.

Tabla 18

Valorización de los niveles de riesgo de un activo de información.

TABLA DE VALORACION DEL RIESGO													
AMENAZA		BAJA (1)			MEDIA (2)			ALTA (3)			MUY ALTA (4)		
VULNERABILIDAD		B(1)	M(2)	A(3)	B(1)	M(2)	A(3)	B(1)	M(2)	A(3)	B(1)	M(2)	A(3)
IMPACTO	1	1	2	3	2	3	4	3	4	5	4	5	6
	2	2	3	4	3	4	5	4	5	6	5	6	7
	3	3	4	5	4	5	6	5	6	7	6	7	8

En la tabla siguiente se muestra los resultados del nivel de riesgo por cada activo de información, relacionando sus amenazas y vulnerabilidades, hay que tener en cuenta en la identificación y valoración de activos de información ya se realizó un filtro previo donde solo se consideró los activos con una valor 3.

Tabla 19

Riesgos depurados

ACTIVO	VULNERABILIDADES	AMENAZAS	VAL ACT	VAL AM	VAL VUL	NIVEL RIESGO
GESTOR DE BASE DE DATOS	ausencia de bitácoras de los sistemas	acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	3	2	6

	ausencia de políticas de confidencialidad de información	acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	3	2	6
	cuentas de acceso activas de personas cuyo vínculo laboral con el HAS ha concluido	acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	3	2	7
	ausencia de políticas y procedimientos para la gestión de cuentas de usuarios	acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	3	2	6
	controles de acceso al sistema deficientes	acceso al sistema por parte de usuarios que no deberían tener acceso o determinados perfiles de acceso al sistema	3	4	3	8
	servicio no configurado en alta disponibilidad	caída del servicio	3	4	3	8
ANTIVIRUS	ausencia de bitácoras de los sistemas	infección de software malicioso	3	3	2	6

	ausencia de monitoreo de servicios	infección de software malicioso	3	3	3	7
	ausencia de bitácoras de los servicios	penetración y propagación de virus en la intranet por mal uso de internet / o memorias extraíbles	3	3	2	6
	ausencia de grupo electrógeno	falla / corte de suministro eléctrico	3	3	3	7
SERVIDOR DE BASE DE DATOS SIGA	ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	deterioro / obsolescencia de equipamiento	3	2	3	6
	ausencia de grupo electrógeno	falla / corte de suministro eléctrico	3	3	3	7
SERVIDOR DE DIRECTORIO ACTIVO Y DNS	ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	deterioro / obsolescencia de equipamiento	3	2	3	6
SERVIDOR SIAF	ausencia de grupo electrógeno	falla / corte de suministro eléctrico	3	3	3	7
	ausencia de mantenimiento periódico de servidores	deterioro / obsolescencia de equipamiento	3	4	1	7
	ausencia de mantenimiento a las instalaciones	deterioro / obsolescencia de equipamiento	3	4	1	6
UPS PARA DATACENTER	ausencia de políticas y procedimientos para realizar mantenimientos preventivos periódicos de HW	deterioro / obsolescencia de equipamiento	3	4	3	8

	ausencia de mantenimiento a las instalaciones	deterioro / obsolescencia de equipamiento	3	4	3	8
CABLEADO ESTRUCTURADO	deficiente control de acceso a la red	acceso no autorizado a la red	3	2	3	6

ANÁLISIS Y DISCUSIÓN

Después de haber trabajado los resultados detalladamente haciendo uso de los instrumentos que apoyaron para la recolección de información, se puede afirmar que el 100 % de la población que fue evaluada confirma que los procesos que se desarrollan en el Centro de Datos no son documentados, lo cual resulta alarmante para esta área ya que para la evaluación se necesitará conocer los procesos más importantes que se desarrollan en ella.

Asimismo también se indica que el 100 % de la población estima que se realizan inventarios de los equipos en el Centro de Datos; esto nos indica que la aplicación de la NTP ISO/IEC 27005 será de gran relevancia para poder hacer el diagnostico enfocados en criterios tales como efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad; es por esto que sirvió de base la investigación de Aliaga (2014) dado que aplica la NTP ISO/IEC 27001: 2008, NTP ISO/IEC 27005:2009; así como también la investigación de López (2011) y Aquije y Jave (2012) quienes utilizan la norma estándar; y Ayala (2017), De la Cruz (2016), quienes utilizan la Norma Técnica Peruana; al tener como marco de referencia para el análisis y diseño de Plan de Seguridad de Seguridad de Información.

También resulta interesante el trabajo de Sánchez (2014) quien utiliza el Estándar Internacional 27002 incluyendo con esto modelos de madurez que le apoyaron reflejar la necesidad de aplicar políticas de seguridad de la información, con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información.

Otra investigación que se consideró importante fue la realizada por Patiño (2018), al hacer uso de la NTE INEN ISO/IEC 27005, al elaborar una guía metodológica para la gestión de riesgo de TIC permitiendo así la identificación de controles para su posterior implementación,

Por último y no menos importante consideramos de gran apoyo el trabajo de Huerta (2015), porque mediante la clasificación y estándar internacional TIER, marco de control COBIT 5.0 y la NTP-ISO/IEC 17799, logró demostrar la efectividad de su seguridad física, coincidiendo con nuestros resultados a pesar de utilizar diferentes normas.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

El proceso metodológico utilizado en el presente proyecto se ha basado en la norma técnica peruana NTP ISO/IEC 27005: 2009, la cual es contemplada por la oficina nacional de Gobierno Electrónico e Informática.

Durante el desarrollo del proyecto se ha identificado los activos de información de TI más importantes con el centro de datos, permitiendo tener un inventario actualizado de activos de TI que dan soporte al proceso. Adicional a ello se ha realizado la valoración de cada uno de ellos teniendo en cuenta características como integridad, confidencialidad y disponibilidad (pilares de la seguridad de la información).

Se ha obtenido la lista de amenazas y vulnerabilidades; y sus valoraciones para activo de información (solo activos con valoración alta)

En función a la combinación de activos de TI, amenazas y vulnerabilidades se ha identificado los riesgos de cada activo de TI

RECOMENDACIONES

En el presente proyecto se tomó como alcance el Hospital de Apoyo II – 2 Sullana, y se recomienda que para próximos trabajos se considere a los demás hospitales, clínicas del sector.

Para iniciar con la implementación de un SGSI, es necesario concientizar a la alta dirección en la importancia y la exigencia por parte de la ONGEI en la implementación del SGSI en el Hospital de Apoyo II-2 Sullana, haciendo prevalecer los beneficios de contar con una SGSI.

Es importante conformar un comité de Seguridad de la Información el cual debe ser multidisciplinario, dentro de este comité se debe incluir a miembros clave de la alta gerencia (tomadores de decisiones) que apoyen en la implementación de un SGSI

AGRADECIMIENTOS

Gracias a Dios por permitirme tener y disfrutar a mi familia, gracias a mi familia por apoyarme en cada decisión y proyecto, gracias a la vida porque cada día me demuestra lo hermoso que es la vida y lo justa que puede llegar a ser; gracias a mi familia, a mi asesor y docentes que gracias a sus conocimientos me permiten cumplir el desarrollo del presente proyecto. Gracias por creer en mí y gracias a Dios por permitirme vivir y disfrutar de cada día.

No ha sido sencillo el camino hasta ahora, pero gracias al aporte de cada uno de ellos, a su amor, a su inmensa bondad y apoyo. Les agradezco y hago presente mi gran afecto hacia ustedes, mi hermosa familia.

REFERENCIAS BIBLIOGRÁFICAS

Aguilera, P. (201 0). *Seguridad Informática.* Madrid, España: Edifex, S.A

Aliaga Infante R.J. (2014). *Análisis de Riesgos de TI para la Implementación de un Sistema de Seguridad de la Información en el Gobierno Regional de Cajamarca.* Universidad Nacional de Cajamarca, Cajamarca, Perú. Disponible en: http://repositorio.unc.edu.pe/bitstream/handle/UNC/523/T%20620.7%20A398%202014.pdf?sequence=1&isAllowed=y

Aquije Quijandra J.G. y Jave Bobadilla L.L. (2012). *Metodología de Gestión de Seguridad de la Información para el Sector Financiero Peruano*. Universidad Nacional de Ingeniería, Lima, Perú. Disponible en: http://cybertesis.uni.edu.pe/bitstream/uni/3355/1/aquije_jg.pdf

Areitio, J. (2008). *Seguridad de la Información. Redes, informática y Sistemas de Información.* Madrid, España: Paraninfo

Ayala Medrano M.A. (2017). *Sistema de Gestión de Seguridad de Información para Mejorar el Proceso de Gestión del Riesgo en un Hospital Nacional, 2017*. Universidad Cesar Vallejo, Lima, Perú. Disponible en: http://repositorio.ucv.edu.pe/bitstream/handle/UCV/13753/Ayala_MMA.pdf?sequence=1&isAllowed=y

Bustos, F.A., Chávez, J.F., Gonzales, L.A., Millán, A. y Gómez, A. (2009). *Metodología para evaluar y calificar la seguridad física de un centro de procesamiento de datos.* Tesina, Instituto Politécnico Nacional, México D.F. Disponible en: https://tesis.ipn.mx/bitstream/handle/123456789/2869/C7.1373.pdf?sequence=1&isAllowed=y

Carrasco Sergio. *Metodología de la Investigación Científica*. Lima: Editorial San Marcos (2005)

Chaparro, N., Pérez, D. y Tenjo N. (2010). Riesgo Informático.Disponible en: https://www.cabinas.net/informatica/analisis_riesgos_informaticos.asp

Chicano, E. (2015). *Auditoria de Seguridad Informática IFCTO109.* Antequera, Málaga: IC Editorial

Cilleros, D. (2012). *Seguridad en Data Centers: infraestructura y prevención.* Proyecto de Fin de Carrera, Universidad Carlos III, Madrid, España. Disponible en: https://e-archivo.uc3m.es/handle/10016/16735

Comité Técnico de Normalización de Codificación e Intercambio Electrónico de Datos, "EDI. Tecnología de la Información. Técnicas de Seguridad. Gestión del riesgo en seguridad de la información NTP-ISO/IEC 27005:2009", Lima, 2009 Comité Técnico de Normalización de Codificación e Intercambio Electrónico de Datos, "EDI. Tecnología de la Información. Técnicas de

Seguridad. Sistemas de gestión de seguridad de la información. Requisitos NTP-ISO/IEC 27001:2008", Lima, 2008

Dais-ujat (2006). *Avances en Informática y Sistema Computacionales. Tomo I (CONAIS 2006).* Tabasco, México: Univ. J. Autónoma de Tabasco

De la Cruz Vargas R. (2016). *Propuestas de Políticas, Basadas en Buenas Practicas, para la Gestión de Seguridad de la Información en la Municipalidad Provincial de Paita.* Universidad Católica Los Ángeles de Chimbote, Paita, Perú. Disponible en: http://repositorio.uladech.edu.pe/bitstream/handle/123456789/885/ACTIVO_SEGURIDAD%20DE%20LA%20INFORMACION_DE%20LA%20CRUZ_VARGAS_RONALD%20_EDUARDO%20.pdf?sequence=1

De Pablos, C., López-Hermoso, J.J., Martín-Romo, S., Medina, S., Montero, A. y Nájera, J.J. (2006). *Dirección y gestión de los sistemas de información en la empresa (2° Ed).* Madrid, España: ESIC.

Del Peso E., Ramos, M.A., Del Peso M. y Del Peso M. (2011). *Nuevo Reglamento de Protección de datos de carácter personal: Medidas de Seguridad.* Madrid, España: Díaz de Santos, S.A.

Galván V. G. (2013) DATACENTER: Una mirada por dentro (1ª ed.), SM de Tucumán: Ediciones Índigo.

Gómez, A.J. (2011). *Redes locales.* Madrid, España: Editex

Guagalango, R.N. y Moscoso, P.E. (2011). Evaluación Técnica de la Seguridad Física del Data Center de la Escuela Politécnica del Ejército. Tesis, Escuela Politécnica del Ejército, Sangolqui, Ecuador. Disponible en: https://repositorio.espe.edu.ec/bitstream/21000/4279/1/T-ESPE-032634.pdf

Hospital de Apoyo II-2 Sullana. Disponible en: http://www.hospitalsullana.gob.pe/

Huerta Aranda M. (2014). *Procedimientos para la Auditoria en Seguridad Física del Data Center de la Municipalidad Provincial de Huamanga.* Universidad Nacional de San Cristóbal de Huamanga, Ayacucho, Perú. Disponible en: http://repositorio.unsch.edu.pe/bitstream/handle/UNSCH/1064/Tesis%20Sis23_Hue.pdf?sequence=1&isAllowed=y

Isaca (2011). *Auditoria de Sistemas*. Disponible en: http://www.isaca.org/Blogs/282270/archive/2011/04/27/Protecci%C3%B3ndeActivosdeInformaci%C3%B3n.aspx

López A. (2011). *Diseño de un Plan de Gestión de Seguridad de la Información. Caso: Dirección de Informática de la Alcaldía del Municipio Jiménez del Estado Lara*. Tesis Post-grado. Barquisimeto: Universidad Centroccidental "Lisandro Alvarado" – Venezuela. Disponible en: https://docplayer.es/5605349-Universidad-centroccidental-lisandro-alvarado-decanato-de-ciencias-y-tecnologias-maestria-en-ciencias-de-la-computacion.html

Mantino, I. (2013). Auditoria de la Seguridad Física y Ambiental. Auditoria. Trabajo de campo. Disponible en: https://es.slideshare.net/isabelmantino/auditoria-seguridadfisica-y-del-entorno-isoiec-270022005

Patiño Rosado S.G. (2018). *Propuesta Metodológica de Gestión de Riesgos de Tecnología de Información u Comunicación (TIC) para Entidades Públicas conforme Normativa NTE INEN ISO/IEC 27005*. Tesis de Postgrado. Universidad de las Fuerzas Armadas. Ecuador. Disponible en: http://repositorio.espe.edu.ec/xmlui/bitstream/handle/21000/13994/T-ESPE-057835.pdf?sequence=1&isAllowed=y

Piattini, M.G. y Del Peso, E. (2001). Auditoria Informática: Un enfoque práctico (2° Ed). México D.F: Alfa omega grupo editor S.A.

Sánchez Arias K. (2014). *Diseño de Políticas de Seguridad de Información para la Alcaldía Municipal de Rio de Oro, Cesar*. Tesis de Grado. Ocaña: Universidad Francisco de Paula Santander Ocaña, Ecuador. Disponible en: http://repositorio.ufpso.edu.co:8080/dspaceufpso/bitstream/123456789/444/1/25791.pdf

Tupia, M. (2010). Administración de la Seguridad de Información. Perú: Graficar.

ANEXOS

ANEXO 1: MATRIZ DE CONSISTENCIA

Tabla 20

Matriz de consistencia

PROBLEMA	OBJETIVOS	VARIABLES
¿Cómo desarrollar una evaluación de la seguridad del centro de datos del Hospital de Apoyo II – 2 Sullana?	**General:** Evaluar el centro de datos del Hospital de Apoyo II – 2 Sullana. **Específicos:** • Realizar el proceso de evaluación utilizando el marco de trabajo para la medición de seguridad del centro de datos. • Aplicar la NTP ISO/IEC 27005: 2009, para la evaluación de la seguridad del centro de datos.	• Centro de Datos • NTP ISO/IEC 27005:2009

ANEXO 2: CUESTIONARIO

UNIVERSIDAD SAN PEDRO

FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERIA INFORMATICA Y DE SISTEMAS

ENCUESTA AL PERSONAL DE LA UNIDAD DE ESTADÍSTICA E INFORMÁTICA DEL HOSPITAL DE APOYO II - SULLANA

PROYECTO: EVALUACIÓN DE LA SEGURIDAD DEL CENTRO DE DATOS DEL HOSPITAL DE APOYO II – SULLANA

OBJETIVO: Recolectar información confiable y confidencial del personal de la Unidad de Estadística e Informática del Hospital de Apoyo II – Sullana que permita el desarrollo de la evaluación de la seguridad del centro de datos del Hospital de Apoyo II - Sullana.

CUESTIONARIO

Instrucción: Sírvase por favor responder con sinceridad a cada pregunta formulada para el estudio, marcando con una (X) la alternativa de la pregunta que Usted considere conveniente. En tal sentido, agradecemos su colaboración y le invocamos ser objetivo y honesto en sus apreciaciones, la encuesta es anónima.

N°	PREGUNTAS	RESPUESTA	
		SI	NO
1	¿Los procesos que se desarrollan en el Centro de Datos son documentados?		
2	¿Se realizan inventarios de los equipos en el Centro de Datos?		
3	¿Se cuenta con manuales por cada Sistema Implantado o software que se utiliza?		
4	¿Existe un reglamento para el personal de sistemas sobre el acceso al Centro de Datos?		
5	¿Se cuenta con un plan operativo?		
6	¿Se ha realizado anteriormente una evaluación al Centro de datos?		
7	¿La infraestructura del Centro de Datos está construido con un material confiable?		
8	¿El lugar en donde se encuentran los equipos es seguro?		

9	¿Existe algún tipo de material que sea inflamable o pueda resultar peligroso para los equipos?
10	¿Existe algún tipo de mantenimiento preventivo para los equipos del Centro de Datos?
11	¿Está conforme con la infraestructura del Centro de Datos?
12	¿Considera importante las salidas de emergencia en el lugar en donde se encuentran los equipos?
13	¿Está conforme con la seguridad física y tecnológica del Centro de Datos?
14	¿Cómo considera el cableado y las vías del cuarto de equipo en relación con los estándares generales?
15	¿Está conforme con los etiquetados de cada uno de los equipos dentro del Centro de Datos?
16	¿El control de humedad es efectivo dentro del lugar de los equipos?

ANEXO 3: RESULTADOS DEL CUESTIONARIO

1. ¿Los procesos que se desarrollan en el Centro de Datos son documentados?

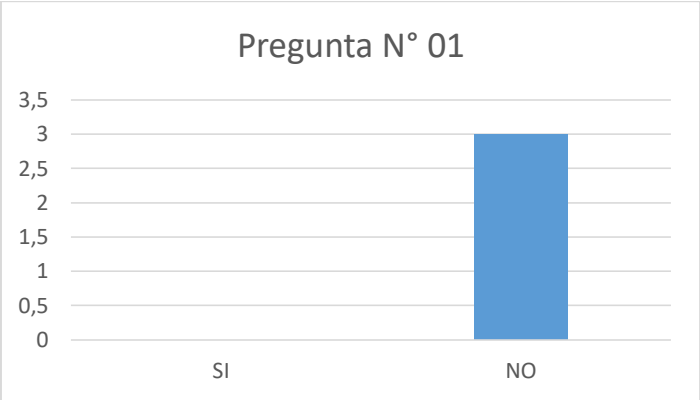


Figura 08: Gráfico procesos documentados.
Fuente: Elaboración propia

Interpretación: El 100% de la población encuestada respondió que los procesos que se desarrollan en el Centro de datos no son documentados.

2. ¿Se realizan inventarios de los equipos en el Centro de Datos?

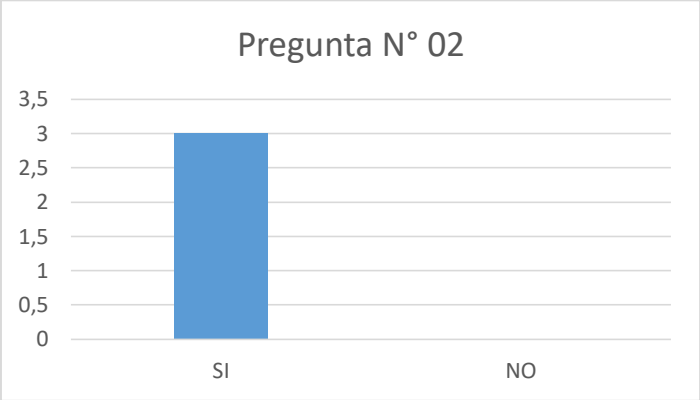


Figura 09: Gráfico inventario de equipos del Centro de Datos.
Fuente: Elaboración propia

Interpretación: El 100% de la población encuestada respondió que si se realizan inventarios de los equipos en el Centro de Datos.

3. ¿Se cuenta con manuales por cada sistema implantado o software que se utiliza?

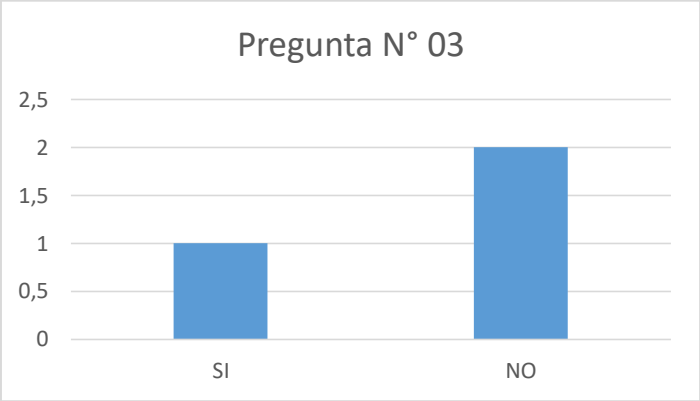


Figura 10: Gráfico manuales de software.
Fuente: Elaboración propia

Interpretación: El 33.33% de la población encuestada respondió que sí se cuenta con manuales por cada sistema implantado o software que se utiliza mientras el 66.67% de la población entrevistada respondió que no se cuenta con manuales por cada sistema implantado o software que se utiliza.

4. ¿Existe un reglamento para el personal de sistemas sobre el acceso al Centro de Datos?

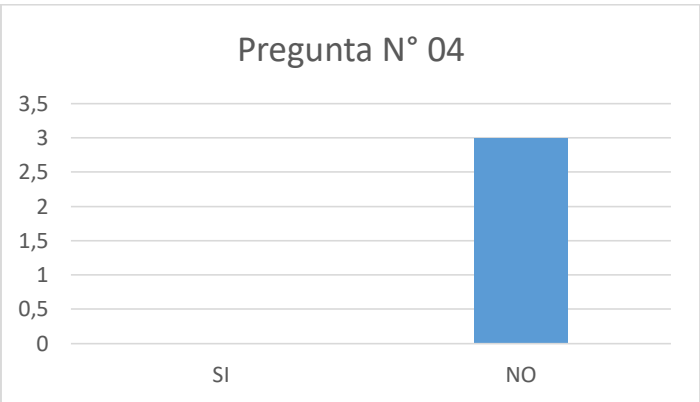


Figura 11: Gráfico reglamento para el acceso al Centro de Datos.
Fuente: Elaboración propia

Interpretación: El 100% de la población encuestada respondió que no existe un reglamento para el personal de sistemas sobre el acceso al Centro de Datos.

5. ¿Se cuenta con un plan operativo?

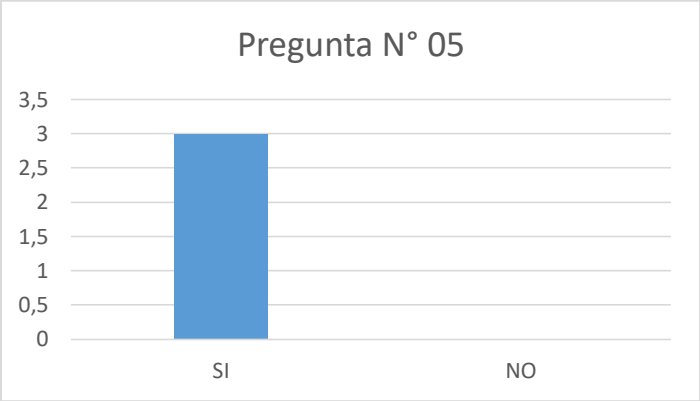


Figura 12: Gráfico plan operativo.
Fuente: Elaboración propia

Interpretación: El 100% de la población encuestada respondió que sí se cuenta con un plan operativo.

6. ¿Se ha realizado anteriormente una evaluación al Centro de Datos?

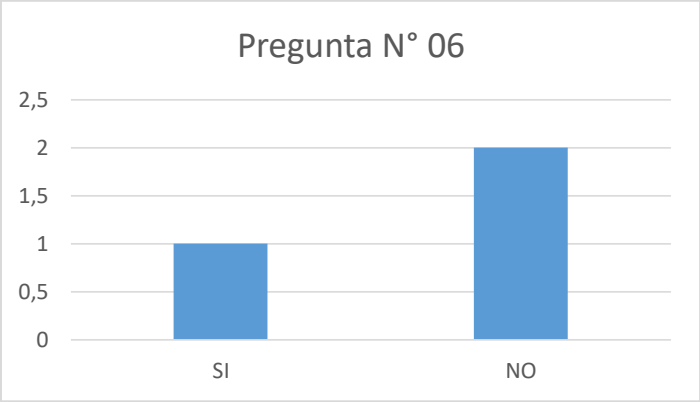


Figura 13: Gráfico evaluación al Centro de Datos.
Fuente: Elaboración propia

Interpretación: El 33.33% de la población encuestada respondió que sí se ha realizado anteriormente una evaluación al Centro de Datos mientras que el 66.67% de la población encuestada respondió que no se ha realizado una evaluación al Centro de Datos.

7. ¿La infraestructura del Centro de Datos está construido con un material confiable?

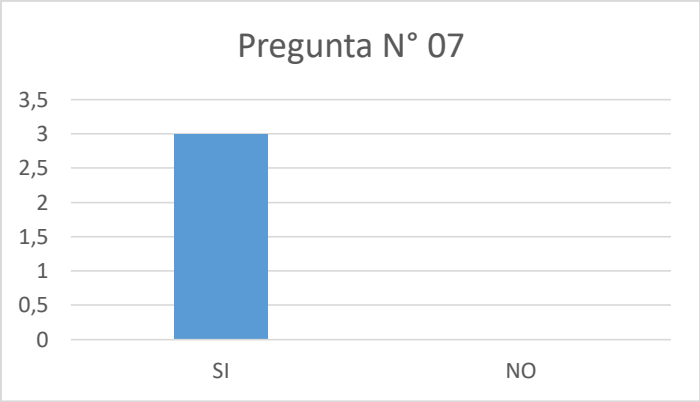


Figura 14: Gráfico infraestructura del Centro de Datos.
Fuente: Elaboración propia

Interpretación: El 100% de la población encuestada respondió que la infraestructura del Centro de Datos si está construido con un material confiable.

8. ¿El lugar donde se encuentran los equipos es seguro?

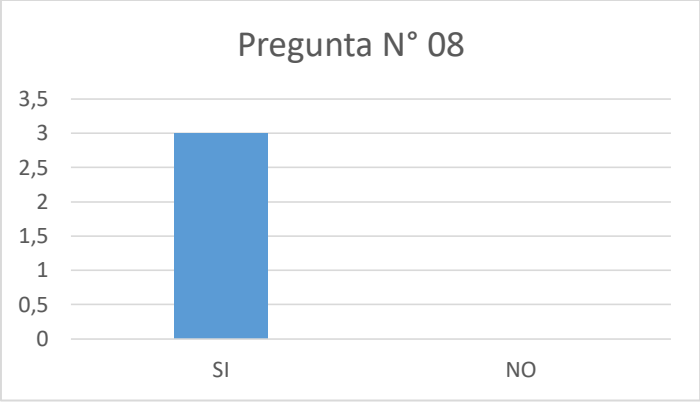


Figura 15: Gráfico seguridad de los equipos.
Fuente: Elaboración propia

Interpretación: El 100% de la población encuestada respondió que el lugar donde se encuentran los equipos sí es seguro.

9. ¿Existe algún tipo de mantenimiento preventivo para los equipos del Centro de Datos?

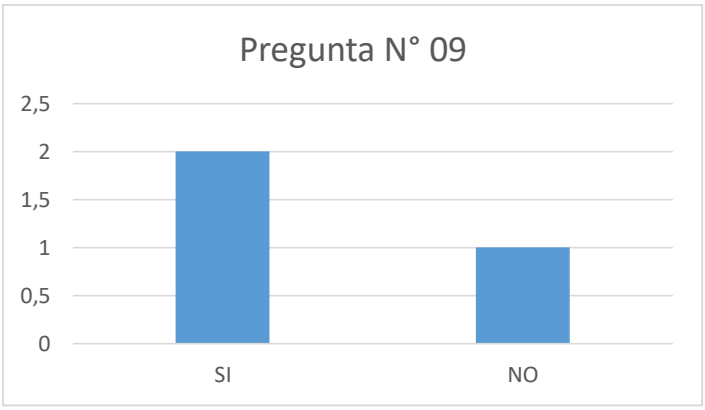


Figura 16: Gráfico mantenimiento preventivo.
Fuente: Elaboración propia

Interpretación: El 66.67% de la población encuestada respondió que si existe algún tipo de mantenimiento preventivo para los equipos del Centro de Datos mientras que el 33.33 % respondió que no existe algún tipo de mantenimiento para los equipos del Centro de Datos.

10. ¿Está conforme con la infraestructura del Centro de Datos?

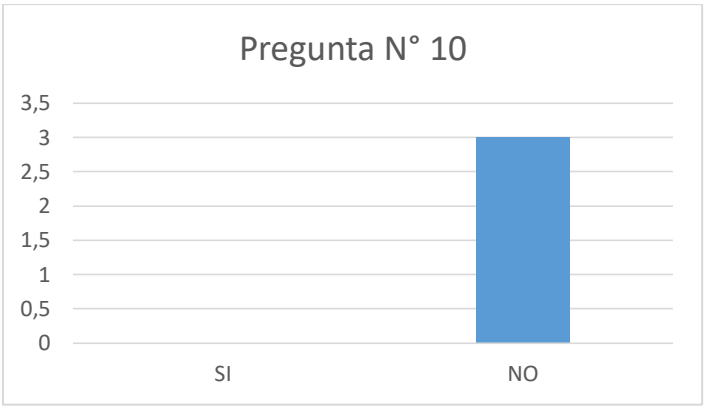


Figura 17: Gráfico conformidad de infraestructura del Centro de Datos.
Fuente: Elaboración propia

Interpretación: El 100 % de la población encuestada respondió que no está conforme con la infraestructura del Centro de Datos.

11. ¿Existe algún tipo de material que sea inflamable o pueda resultar peligroso para los equipos?

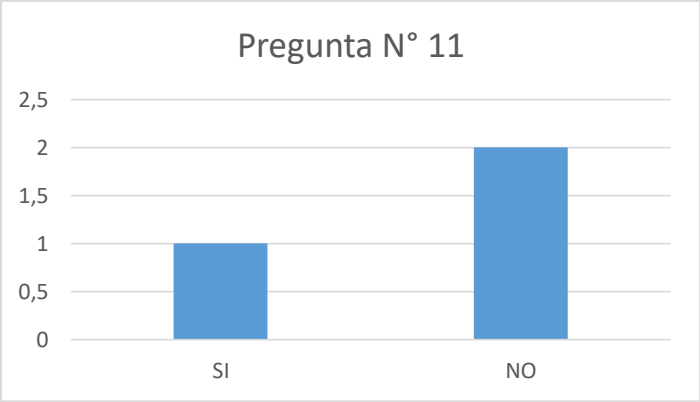


Figura 18: Gráfico material inflamable.
Fuente: Elaboración propia

Interpretación: El 33.33 % de la población encuestada respondió que si existe algún tipo de material inflamable mientras el 66.67 % respondió que no existe algún tipo de material que sea inflamable o pueda resultar peligroso para los equipos.

12. ¿Considera importante las salidas de emergencia en el lugar en donde se encuentran los equipos?

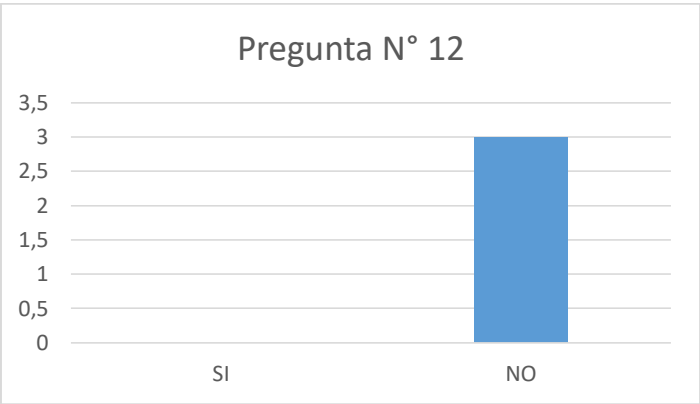


Figura 19: Gráfico salida de emergencia.
Fuente: Elaboración propia

Interpretación: El 100 % de la población encuestada respondió que no consideran importante las salidas de emergencia en el lugar donde se encuentran los equipos.

13. ¿Está conforme con la seguridad física y tecnológica del Centro de Datos?

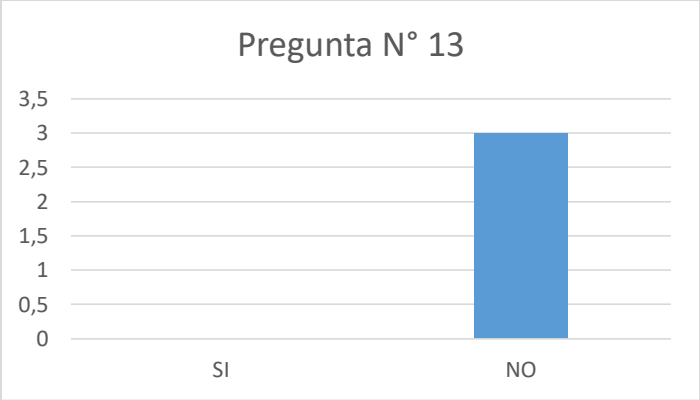


Figura 20: seguridad física y tecnológica del Centro de Datos.
Fuente: Elaboración propia

Interpretación: El 100 % de la población encuestada respondió que no está conforme con la seguridad física y tecnológica del Centro de Datos.

14. ¿Cómo considera el cableado y las vías del cuarto de equipo en relación con los estándares generales?

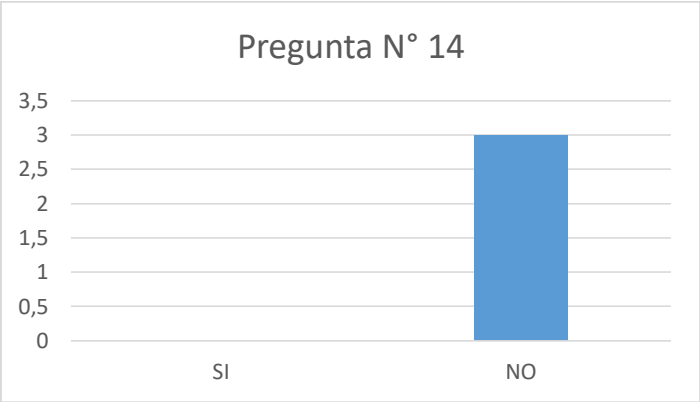


Figura 21: cableado en relación con estándares generales.
Fuente: Elaboración propia

Interpretación: El 100 % de la población encuestada respondió que no considera el cableado y las vías del cuarto de equipos en relación con los estándares generales.

15. ¿Está conforme con los etiquetados de cada uno de los equipos dentro del Centro de Datos?

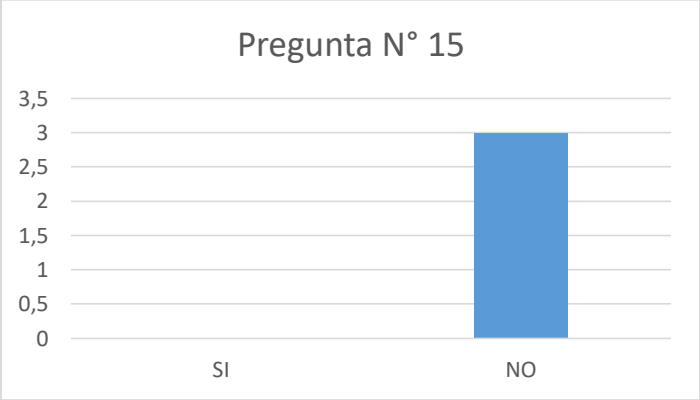


*Figura 22: E*etiquetado del Centro de Datos.
Fuente: Elaboración propia

Interpretación: El 100 % de la población encuestada respondió que no está conforme con los etiquetados de cada uno de los equipos dentro del Centro de Datos.

16. ¿El control de humedad es efectivo dentro del lugar de los equipos?

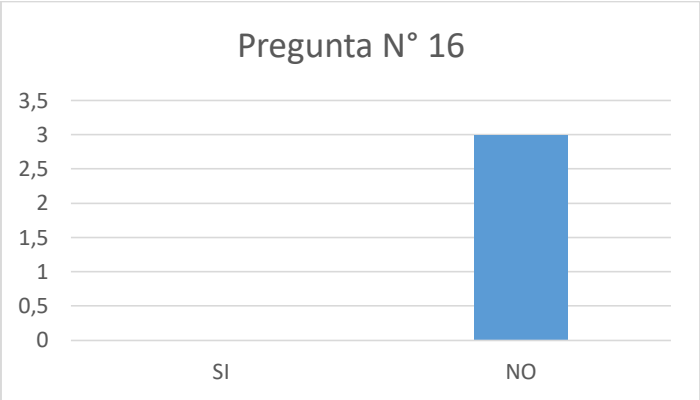


Figura 23: efectividad del control de humedad.

Fuente: Elaboración propia

Interpretación: El 100 % de la población encuestada respondió que el control de humedad no es efectivo dentro del lugar de los equipos.

ANEXO 4: EVIDENCIA FOTOGRÁFICA