"AÑO DEL FORTALECIMIENTO DE LA SOBERANIA NACIONAL"

FACULTAD DE CIENCIAS E INGENIERÍA

PROGRAMA ACADÉMICO DE INGENIERIA DE SISTEMAS DE INFORMACIÓN

PROGRAMA ACADÉMICO DE INGENIERIA INFORMÁTICA Y DE SISTEMAS

TRABAJO DE SUFICIENCIA PROFESIONAL

"EVALUACIÓN DEL NIVEL DE SEGURIDAD INFORMÁTICA DEL HOSPITAL III IQUITOS DE ESSALUD LORETO - 2022"

PARA OPTAR AL TÍTULO PROFESIONAL DE:

AUTORES : Bach. DAVILA VALERA, Willy Esteban.
INGENIERO DE SISTEMAS DE INFORMACIÓN

Bach. CHAVEZ BARDALES, Eduardo Adriam Benyamin
INGENIERO INFORMÁTICO Y SISTEMAS.

ASESOR: Dr. LEÓN VARGAS, Frank Romel

San Juan Bautista – Loreto – Maynas –Perú

2022

Dedicatoria

A Dios por brindarme la vida, salud y fuerza para seguir con mis metas y guiarme por el buen camino durante mi formación profesional.

A mis queridos padres por apoyarme de una forma incondicional durante todos estos tiempos para seguir adelante con mis proyectos.

A mis amigos, familiares y seres queridos que han estado conmigo apoyándome de una forma incondicional en el transcurso de los años de mi vida personal y profesional.

Willy Esteban

Dedicatoria

Dedico este logro académico, personal y profesional.

A Dios que es parte de mi vida que me dio la vocación hacia la Ingeniería de Sistemas de Información.

A mis queridos padres que siempre están apoyándome en cada aspecto y proyecto de la vida.

A mis queridos profesores que son parte de mi formación profesional, cada uno ha contribuido con su conocimiento y experiencia para lograr desempeñarme como un profesional competente y ante todo consciente del ambiente laboral en el que estoy.

Eduardo Adriam

Agradecimientos

A nuestro divino creador Dios por brindarnos la vida, alimentos y salud, porque siempre está con nosotros en lo bueno y malo.

A la Universidad Científica del Perú, por ayudarnos a formar de manera profesional en la carrera de Ingeniería de Sistemas de información y hacer que sigamos adelante aprendiendo cosas nuevas y ser personas de bien en la sociedad.

Al Hospital III Iquitos de Essalud, en especial a la Unidad de Soporte Informático por brindarnos todas las facilidades para poder realizar este presente proyecto, ya que sin su ayuda no hubiera sido posible realizar este proyecto.

A nuestras familias, amigos y a las personas que nos apoyaron en este trabajo, ya sea de forma directa o indirecta, agradecerles a todos ustedes, que fueron el motor y motivo seguir adelante, y que el resultado de todo nuestro esfuerzo brindado se refleja en la culminación exitosa de nuestro proyecto.

Los Autores

UNIVERSIDAD CIENTÍFICA DEL PERÚ

"Año del Fortalecimiento de la Soberanía Nacional"

CONSTANCIA DE ORIGINALIDAD DEL TRABAJO DE INVESTIGACIÓN DE LA UNIVERSIDAD CIENTÍFICA DEL PERÚ - UCP

El presidente del Comité de Ética de la Universidad Científica del Perú - UCP

Hace constar que:

El Trabajo de Suficiencia Profesional titulado:

"EVALUACIÓN DEL NIVEL DE SEGURIDAD INFORMÁTICA DEL HOSPITAL 111 IQUITOS DE ESSALUD LORETO - 2022"

De los alumnos: **DAVILA VALERA WILLY ESTEBAN Y CHAVEZ BARDALES EDUARDO ADRIAM BENYAMIN,** de la Facultad de Ciencias e Ingeniería, pasó satisfactoriamente la revisión por el Software Antiplagio, con un porcentaje de **4% de plagio**.

Se expide la presente, a solicitud de la parte interesada para los fines que estime conveniente.

San Juan, 07 de Junio del 2022.

Dr. César J. Ramal Asayag
Presidente del Comité de Ética – UCP

CJRA/ri-a
272-2022

Av. Abelardo Quiñones Km. 2.5 (065) 261088 www.ucp.edu.pe

UNIVERSIDAD CIENTÍFICA DEL PERÚ

"Año del Fortalecimiento de la Soberanía Nacional"

FACULTAD DE CIENCIAS E INGENIERÍA

ACTA DE SUSTENTACIÓN DE TRABAJO DE SUFICIENCIA PROFESIONAL

FACULTAD DE CIENCIAS E INGENIERÍA

Con Resolución Decanal N° 719-2022-UCP-FCEI del 25 de julio del 2022, la FACULTAD DE CIENCIAS E INGENIERÍA DE LA UNIVERSIDAD CIENTÍFICA DEL PERÚ - UCP designa como Jurado Evaluador de la sustentación del Trabajo de Suficiencia Profesional a los señores:

- Ing. Carmen Patricia Cerdeña del Águila, Dra. — Presidente
- Ing. Jimmy Max Ramírez Villacorta, Mgr. — Miembro
- Ing. Carlos Enrique Marthans Ruiz, Mgr. — Miembro

Como Asesor: al **Dr. Frank Romel Leon Vargas**

En la ciudad de Iquitos, siendo las 10:00 am del día lunes 01 de agosto del 2022, a través de la plataforma ZOOM supervisado en línea por el Secretario Académico del Programa Académico de Ingeniería de Sistemas de Información de la Facultad de Ciencias e Ingeniería de la Universidad Científica del Perú., se constituyó el Jurado para escuchar la sustentación y defensa del Trabajo de Suficiencia Profesional: **"EVALUACIÓN DEL NIVEL DE SEGURIDAD INFORMÁTICA DEL HOSPITAL III IQUITOS DE ESSALUD LORETO - 2022".**

Presentado por el sustentante: **EDUARDO ADRIAM BENYAMIN CHAVEZ BARDALES**
Como requisito para optar el título profesional de: ***INGENIERO INFORMÁTICA Y DE SISTEMAS***
Y por el sustentante: **WILLY ESTEBAN DAVILA VALERA**
Como requisito para optar el título profesional de: ***INGENIERO DE SISTEMAS* DE *INFORMACIÓN***

Luego de escuchar la sustentación y formuladas las preguntas las que fueron: **ABSUELTAS**

El Jurado después de la deliberación en privado llegó a la siguiente conclusión:

La sustentación es: **APROBADO POR MAYORIA**

En fe de lo cual los miembros del Jurado firman el acta.

Ing. Carmen Patricia Cerdeña del Águila, Dra.
Presidente

Ing. Jimmy Max Ramírez Villacorta, Mgr
Miembro

Ing. Carlos Enrique Marthans Ruiz, Mgr.
Miembro

Contáctanos:

Iquitos – Perú
065 - 26 1088 / 065 - 26 2240
Av. Abelardo Quiñones Km. 2.5

Filial Tarapoto – Perú
42 – 58 5638 / 42 – 58 5640
Leoncio Prado 1070 / Martines de Compagñon 933

Universidad Científica del Perú
www.ucp.edu.pe

INDICE GENERAL

DEDICATORIA II

AGRADECIMIENTOS IV

INDICE GENERAL VII

INDICE DE FIGURAS IX

RESUMEN XI

ABSTRACT XII

CAPÍTULO I

INTRODUCCIÓN 13

OBJETIVO GENERAL 13

OBJETIVOS ESPECÍFICOS 13

CAPÍTULO II

MARCO REFERENCIAL 14

ANTECEDENTE INTERNACIONAL 14

ANTECEDENTE NACIONAL 15

DEFINICIONES TEÓRICAS 16

- *Seguridad Informática 16*
- *Tipos de Seguridad 16*
- *Elementos de la seguridad informática 16*
- *Propiedades de un sistema de información seguro 16*
- *Políticas de seguridad informática 16*
- *Controles de seguridad informática 16*
- *Razones para la seguridad Informática 16*
- *NTP-ISO/IEC 27001: 2014 ..... 17*
- *Sistema de gestión de la seguridad de la Información 17*

DEFINICIONES CONCEPTUALES 17

- *Amenaza 17*

- *Vulnerabilidad* *17*
- *Riesgo* *17*
- *Confidencialidad* *18*
- *Integridad* *18*
- *Disponibilidad* *18*

CAPÍTULO III

METODOLOGÍA 18

A NIVEL DE CIENTÍFICO 18

A Nivel Practico *19*

A Nivel legal *19*

POBLACIÓN Y MUESTRA 19

Población *19*

Muestra *19*

Técnicas e Instrumentos de Recolección de Datos *20*

EVALUACIÓN DE LA SITUACIÓN ACTUAL 21

- *Organización* *21*
- *Estructura orgánica* *22*

DESCRIPCIÓN DE FUNCIONES DE LOS RESPONSABLES DEL ÁREA 23

INVENTARIO INFORMÁTICO 25

REALIDAD PROBLEMÁTICA O SITUACIÓN ACTUAL 33

CAPÍTULO IV

RESULTADOS 34

CAPÍTULO V

DISCUSIONES 54

CAPÍTULO VI

CONCLUSIONES 55

RECOMENDACIONES 56

REFERENCIAS BIBLIOGRÁFICAS 57

ANEXOS 58

INDICE DE FIGURAS

ILUSTRACIÓN 01: ORGANIGRAMA INSTITUCIONAL..... 22
ILUSTRACIÓN 02: PLANO DEL EDIFICIO A (PRIMER NIVEL) DEL HOSPITAL ESSALUD III – IQUITOS..... 28
ILUSTRACIÓN 03: PLANO DEL EDIFICIO A (SEGUNDO NIVEL) DEL HOSPITAL ESSALUD III – IQUITOS..... 29
ILUSTRACIÓN 04: PLANO DEL EDIFICIO A (TERCER NIVEL) DEL HOSPITAL ESSALUD III – IQUITOS..... 30
ILUSTRACIÓN 05: PLANO DEL EDIFICIO B (PRIMER NIVEL) DEL HOSPITAL ESSALUD III – IQUITOS..... 31
ILUSTRACIÓN 6: PLANO DEL EDIFICIO COMPLETO DEL HOSPITAL ESSALUD III – IQUITOS..... 32
ILUSTRACIÓN 07: HOSPITAL III IQUITOS ESSALUD..... 61
ILUSTRACIÓN 08: UNIDAD DE SOPORTE INFORMÁTICO..... 61

INDICE DE TABLAS

Tabla 01: Personal de la Unidad.....19
TABLA 02: COMPUTADORAS 25
TABLA 03: MONITORES 25
TABLA 04: SERVIDORES 26
TABLA 05: TECLADO 26
TABLA 06: RELOJ BIOMÉTRICO 26
TABLA 07: SWITCHER 27
TABLA 01 ¿LA INSTITUCIÓN INVIERTE PRESUPUESTO EN CIBERSEGURIDAD? 34
TABLA 02 ¿EL ÁREA CUENTA CON PERSONAL ESPECIALIZADO EN SEGURIDAD INFORMÁTICA? 35
TABLA 03 ¿EL ÁREA PROPENDE POR EL CORRECTO Y SEGURO FUNCIONAMIENTO DE LAS INSTALACIONES DE PROCESAMIENTO DE LA INFORMACIÓN Y MEDIOS DE COMUNICACIÓN? 36
TABLA 04 ¿EL ÁREA CUENTA CON PROCEDIMIENTOS ESTANDARIZADOS PARA ADQUISICIÓN, DESARROLLO Y/O MANTENIMIENTO DE SOFTWARE, QUE GARANTICEN NIVELES DE SEGURIDAD DE LA(S) APLICACIÓN(ES)? 37
TABLA 05 ¿EXISTE UNA POLÍTICA DE SEGURIDAD ADOPTADA INSTITUCIONALMENTE POR EL ÁREA? 38
TABLA 06 ¿EL ÁREA TIENE ESTABLECIDOS PROTOCOLOS PARA GARANTIZAR LA SEGURIDAD EN LA INFORMACIÓN ALMACENADA? 39
TABLA 07 ¿REALIZA PERIÓDICAMENTE BACKUP DE LA INFORMACIÓN? 40
TABLA 08 ¿USTED CONSIDERA QUE LOS DATOS QUE SE INGRESAN POR LOS SISTEMAS INFORMÁTICOS SON CORRECTOS? 41
TABLA 09 ¿LOS DATOS DE LOS SISTEMAS INFORMÁTICOS SE ALMACENAN EN UN EQUIPO SERVIDOR? 42
TABLA 10 ¿LOS SISTEMAS INFORMÁTICOS QUE CUENTAN, LES PERMITEN A LOS USUARIOS INGRESAR DATOS ERRÓNEOS? 43
TABLA 11 ¿CONSIDERA QUE LA RED DE DATOS EN LA QUE SE TRANSMITE LA INFORMACIÓN DE LOS SISTEMAS ES SEGURA? 44
TABLA 12 ¿REALIZA PERIÓDICAMENTE MANTENIMIENTO A SUS SERVIDORES? 45
TABLA 13 ¿EL ÁREA CONSIDERA TENER CONTROLADOS TODOS LOS INCIDENTES DE SEGURIDAD QUE HAN OCURRIDO EN LA RED DE DATOS? 46
TABLA 14 ¿EL ÁREA TIENE ESTABLECIDO UN PLAN DE RESPUESTA A INCIDENTES? 47
TABLA 15 ¿CUENTAN CON UN PLAN DE PREVENCIÓN DE RIESGOS INFORMÁTICOS? 48
TABLA 16 ¿LOS EMPLEADOS HACEN UN USO ADECUADO DE LAS CONTRASEÑAS Y DATOS PERSONALES? 49
TABLA 17 ¿EL MANEJO DE USUARIOS Y CONTRASEÑAS DE LOS SISTEMAS DE INFORMACIÓN SE ACTUALIZAN O CAMBIAN PERIÓDICAMENTE? 50
TABLA 18 ¿EXISTE ALGÚN DOCUMENTO DE REGISTRO DE USUARIOS Y CONTRASEÑAS DE ACCESO A LOS SISTEMAS INFORMÁTICOS? 51
TABLA 19 ¿EXISTE ALGUNA BITÁCORA DONDE SE REGISTRA LOS INCIDENTES DE ACCESOS NO AUTORIZADOS A LOS SISTEMAS? 52
TABLA 20 ¿DENTRO DEL ÁREA EXISTE UN RESPONSABLE QUE ASIGNE USUARIOS Y CONTRASEÑAS DE ACCESO A LOS SISTEMAS INFORMÁTICOS? 53

RESUMEN

En el presente trabajo de suficiencia profesional titulada “Evaluación del Nivel de Seguridad Informática del Hospital III Iquitos de Essalud Loreto – 2022”, se realiza un examen de las vulnerabilidades y amenazas existentes en la Unidad de Soporte Informático, se utilizó la metodología cuantitativa en donde se describe los criterios técnicos que determinan el mal o buen funcionamiento y calidad de los servicios que presta la mencionada unidad hacia los usuarios internos y externos, tomando en consideración los principios básicos de la información como es la Disponibilidad, Integridad y Confidencialidad, en este trabajo se tuvo como objetivo general evaluar los niveles de seguridad de la Información del Hospital III Iquitos Essalud, se logró establecer que no existen los protocolos y mecanismos necesarios para garantizar la exactitud de la información en su procesamiento, transporte y almacenamiento, no existen los criterios seguros y fiables para el acceso oportuno a los sistemas informáticos y por ultimo no existen los criterios y mecanismos de seguridad para garantizar la accesibilidad y control de ingreso autorizado a los sistemas informáticos de las personas que cuenten con las credenciales o autorización para el procesamiento de la información por parte del área usuaria, por lo tanto a la brevedad posible se debe implementar un Sistema de gestión de Seguridad Informática, en este caso en nuestro trabajo de suficiencia se recomienda la implementación de la “NTP ISO/IEC 27001:2014.

Palabras Claves: Seguridad Informática, Vulnerabilidad, Amenazas, Hospital.

ABSTRACT

In the present work of professional sufficiency entitled "Evaluation of the Level of Computer Security of the Hospital III Iquitos de Essalud Loreto - 2022", an examination of the vulnerabilities and threats existing in the Computer Support Unit is carried out, the quantitative methodology was used where The technical criteria that determine the poor or good functioning and quality of the services provided by the aforementioned unit to internal and external users are described, taking into consideration the basic principles of information such as Availability, Integrity and Confidentiality, in this work. The general objective was to evaluate the security levels of the Information of Hospital III Iquitos Essalud, it was possible to establish that there are no protocols and mechanisms necessary to guarantee the accuracy of the information in its processing, transport and storage, there are no safe criteria. and reliable for timely access to information systems and finally, there are no criteria and security mechanisms to guarantee accessibility and control of authorized entry to the computer systems of people who have the credentials or authorization for the processing of information by the user area, therefore As soon as possible, an Information Security Management System should be implemented, in this case, in our sufficiency work, the implementation of the “NTP ISO/IEC 27001:2014.

Keywords: Computer Security, Vulnerability, Threats, Hospital

CAPÍTULO I

Introducción

Actualmente la seguridad informática en las organizaciones se ha convertido en unos de los factores más importantes a considerar que debe estar muy bien organizada y aplicada, ya que de ella depende que la información cumpla sus reglas fundamentales como es la Integridad, Disponibilidad y Confidencialidad, por lo tanto, esto acarrea una serie de procesos y actividades que conllevan a los profesionales a tomar en consideración siguiendo estándares o normativas dependiendo del tipo de organización para cuidar o proteger el activo más importante de una organización que es la información.

La Unidad de Soporte Informático del Hospital III Iquitos de Essalud, es una de las áreas cuyos servicios son los más requeridos de manera diaria puesto que las actividades que desarrollan son evaluar las necesidades informáticas, soporte técnico informático, proponer y ejecutar planes de capacitación y lo más importante garantizar el buen funcionamiento de los sistemas de información que tiene la entidad durante las 24 horas del día y los 365 días del año sin parar alguna, tomando en consideración a la responsabilidad y alta demanda de los servicios y actividades que tiene esta unidad y a la falta de difusión y aplicación de medidas de seguridad informática a aplicar por parte de la Oficina Central de Organización e Informática de Essalud, hemos visto en la imperiosa necesidad de realizar una evaluación respecto a las vulnerabilidades y amenazas que existen en el entorno informático del Hospital III Iquitos de Essalud, situación que corresponde hacer un estudio minucioso de cada uno de los aspectos que conllevan a poner en riesgo la continuidad de los servicios informáticos y por lo tanto la disconformidad de los usuarios de estos servicios y también de los pacientes que se atienden es este hospital.

Objetivo General

Evaluar los niveles de seguridad de la Información del Hospital III Iquitos Essalud.

Objetivos Específicos

- Identificar las vulnerabilidades y amenazas respecto a la integridad de la información.
- Identificar las vulnerabilidades y amenazas relacionadas con la disponibilidad de la información.
- Identificar las vulnerabilidades y amenazas de la confidencialidad de la información.

CAPÍTULO II

Marco Referencial

Antecedente Internacional

Recalde, J. (2019). En su proyecto “Plan de implementación de un SGSI y aplicación de controles críticos en el centro de operaciones de seguridad en la empresa GMS”, Quito – Ecuador, Una empresa dedicada a brindar servicios para la gestión de seguridad de la información cuyo objetivo es la certificación en la norma ISO/IEC 27001:2013 desarrollando un plan de implementación de un SGSI en la empresa GMS, para el desarrollo del proyecto y considerando su alcance, se abarco de forma total la primera fase y de forma parcial la segunda fase del ciclo PDCA o ciclo de Deming: Planificación (Plan) y Ejecución (Do), durante la fase de planificación se realiza un análisis que son los requisitos dictados por la norma ISO 27001:2013 para la elaboración de los documentos requeridos, identificando los activos que forman parte del proceso evaluado, la metodología de gestión de riesgo, el detalle de los riesgos que enfrentan, el plan de tratamiento de riesgos con los controles a aplicarse para minimizar los riesgos, en la fase de ejecución se establecieron las políticas que fueron aprobadas por el comité de seguridad de la empresa y sus procedimientos fueron puestos en marcha en la gestión del SGSI dentro de su alcance, actuando sobre los activos comprometidos y siendo ejecutadas por los involucrados, para su implementación de controles se estableció un cronograma de implementación, en base a entrevistas con los responsables del proceso, dueños de activos, y gerente del área, una vez implementados se realizó un análisis de brecha de seguridad entre en estado actual y el estado deseado. Mediante la metodología de gestión de riesgos se pudo apreciar la brecha real de seguridad que tiene la Empresa GMS, los componentes vulnerables y la relación con otros activos de tecnología, y de esta forma enfocar especial atención a los más críticos, y una vez implementados los controles planteados en el SGSI, el resultado del análisis de brecha entre el estado de seguridad deseado y el estado de seguridad en ese momento sería notoriamente menor que el realizado inicialmente en este proyecto.

Antecedente Nacional

Poicon, J. (2020). En su tesis titulada “Propuesta de un sistema de gestión de seguridad de la información para la Municipalidad Distrital de Marcavelica, mediante la NTP-ISO/IEC 27001: 2014", Piura – Perú, tuvo como objetivo el diseñar una propuesta SGSI para la Municipalidad de Marcavelica, tomando como referencia el estándar NTP-ISO/IEC 27001:2014, Identificando los activos de información en la Municipalidad de Marcavelica, basado en la norma ISO 27001; determinando los riesgos de los activos de información para un Sistema de Gestión de Seguridad de la Municipalidad Distrital de Marcavelica, mediante la NTP-ISO/IEC 27001:201; determinar los indicadores seguridad para la protección de los activos de información en la Municipalidad de Marcavelica basado en la NTPISO/IEC 27001:2014 y proponer controles para el monitoreo y revisión de seguridad de los activos de información en la Municipalidad de Marcavelica, basado en la NTP-ISO/IEC 27001:2014, la metodología se basó en un diseño no experimental, pues solo se describieron las características de la variable del estudio sin intervenir en el proceso, clasificado en transeccionales y longitudinales.

La investigación transeccional, tiene como propósito la descripción de variables, analizando su incidencia en un momento determinado, mientras que la investigación longitudinal, recaba datos en distintos momentos o periodos de tiempo, para luego inferir en relación a los cambios que se suscitaron. Por lo definido la investigación se estableció como no experimental de corte transversal descriptivo simple.

La población estuvo conformada por todos los activos de información de la Municipalidad Distrital de Marcavelica, según la clasificación que indica la NTP-ISO/IEC 27001:2014, aplicando la encuesta y la observación, y de esta forma, se recopilaron los datos de cada activo de información, logrando determinar que el impacto del riesgo, los valores de criticidad de los activos de información fueron bajo y medio; y el nivel de los riesgos obtuvo un nivel significativo con un valor de 30%, en la denominación de riesgo dañino se encontró un 15% y para un riesgo serio fue del 4%, los cuales deberían ser controlados para evitar la materialización de las amenazas, proponiendo políticas y controles para el monitoreo y revisión de seguridad de los activos de información en la Municipalidad de Marcavelica, las que incluyen procedimientos e indicadores para la implementación del SGSI basado en el diagnóstico del nivel y el impacto del riesgo, cubriendo las brechas más representativas de acuerdo a las vulnerabilidades encontradas en los diversos activos de información evaluados

DEFINICIONES TEÓRICAS

- **Seguridad Informática**

Consiste en impedir la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan conllevar daños sobre la información, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema.

- **Tipos de Seguridad**

El tipo de seguridad depende del activo que se va a proteger, los recursos del sistema de información que son parte fundamental para el funcionamiento de la organización.

- **Elementos de la seguridad informática**

Son aquellas técnicas que se usan para resguardar datos y proteger la privacidad de las personas y del parque informático.

- **Propiedades de un sistema de información seguro**

Esto consiste que un sistema, se considere seguro, conformado Integridad, Confidencialidad, Disponibilidad de la información que se comparte en la organización.

- **Políticas de seguridad informática**

La política de seguridad informática es la forma de comunicarse con los usuarios, ya que las mismas establecen un canal formal de actuación del personal, en relación con los recursos y servicios informáticos de la organización.

- **Controles de seguridad informática**

Los controles de seguridad informático tienen por finalidad garantizar que todos los activos, sistemas, instalaciones, datos y archivos relacionados con el uso de la Tecnología de Información se encuentran protegidos contra accesos no autorizados, daños eventuales y uso indebido o ilegal que se encentran operables, seguros y protegidos en todo momento.

- **Razones para la seguridad Informática**

La razón para tener una seguridad informática es que esto se enfoca en la protección de la infraestructura computacional y todo lo relacionado con ello y, especialmente, la

información contenida, siendo algo de mucha importancia para la organización. El riesgo es ser vulnerables ante un robo de información y más cuando nuestros datos son de una empresa, uno de los aspectos con mayor importancia en toda organización es asegurar la privacidad de sus datos y la protección de sus sistemas.

- **NTP-ISO/IEC 27001: 2014**

Esto se adoptado entre los meses de abril a junio, también usa como antecedente a la ISO 27001:2013 que es difundida por el Instituto Nacional de la Calidad (INACAL), la Norma, especifica los requisitos de seguridad de la información a cumplir para poder implementar, establecer, mantener y mejorar un Sistema de Gestión de Seguridad de la Información. Puede ser en pequeñas, medianas y grandes organizaciones ya que cuenta con los controles del Anexo A, esto ayudara a identificar, analizar y eliminar posibles riesgos que afecten a los activos de información de la organización, esta Norma es certificable para las organizaciones y personas que quieran especializarse en seguridad informática.

- **Sistema de gestión de la seguridad de la Información**

Es el conjunto de políticas de administración de la información para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información dentro de la organización.

DEFINICIONES CONCEPTUALES

- **Amenaza**

Se entiende como acción o evento negativo en donde esto quede vulnerable ante algo y teniendo como resultado un impacto no deseado en un cierto periodo.

- **Vulnerabilidad**

Es el riesgo de sufrir frente a peligros inminentes, ya sean desastres naturales, desigualdades económicas, políticas, informáticas, sociales o culturales.

- **Riesgo**

Es la posibilidad de que ocurra un evento y sus consecuencias negativas. Los factores que lo componen son la amenaza y la vulnerabilidad.

- **Confidencialidad**

Es la propiedad de la seguridad que permite mantener en secreto la información y solo los usuarios autorizados pueden manipularla. Para evitar que nadie no autorizado pueda tener acceso a la información transferida y que recorre la Red se utilizan técnicas de encriptación o codificación de datos.

- **Integridad**

Esto consiste en lograr que la información transmitida entre dos entidades no sea modificada por un tercero, en donde mantener la integridad es importante para verificar que en el tiempo de viaje por la Red de la información entre el sitio emisor y receptor nadie no autorizado ha modificado el mensaje.

- **Disponibilidad**

Es la característica o capacidad de asegurar la fiabilidad y el acceso oportuno a los datos y recursos que los soportan por parte de los individuos autorizados, es decir, que lo necesitan para desenvolver sus actividades dentro de la organización.

CAPÍTULO III

Metodología

A Nivel de Científico:

Para el presente trabajo de suficiencia profesional se aplicó un diseño no experimental, ya que la variable independiente no se va a manipular de manera deliberada; es decir se observan hechos que ya se han presentado en el área del fenómeno estudiado.

El tipo de investigación que se aplicó es la transversal, porque se ha recopilado los datos para el desarrollo del trabajo en un solo tiempo o momento dado.

La investigación es descriptiva, porque se expondrán las vulnerabilidades y amenazas que abordan actualmente a los recursos informáticos del Hospital III Iquitos Essalud

Para desarrollar el trabajo de investigación se sigue el enfoque aplicado por que se busca de la aplicación de teorías, herramientas y conocimientos que pueda modificar, reformar o cambiar el aspecto de la realidad, el método es Cuantitativo, Porque se ponderaron de

manera cuantitativa los datos del cuestionario que se realizó a los trabajadores de la Unidad de Soporte Informático del Hospital III Iquitos de Essalud

A Nivel Practico:

Para desarrollar el presente trabajo de Investigación, se tuvo como referencia la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición".

A Nivel legal:

Resolución Ministerial N. º 004-2016-PCM, que Aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática.

POBLACIÓN Y MUESTRA

Población

La población, objeto del trabajo de suficiencia profesional está constituida por los trabajadores de la Unidad de Soporte Informático del Hospital III Iquitos de Essalud, que tienen acceso, control y seguridad de la información; siendo estas 9 personas.

Muestra

La muestra será igual a la población por ser finita.

Tabla 01: Personal de la Unidad

Cargo	Cantidad
Jefe	01
Soporte a Usuarios	05
Administrador de Sistemas	01
Administrador de Redes	01
Técnico Electrónico	01
Total	09

Fuente: *Unidad de Soporte Informático*

TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS.

Las técnicas que utilizaron para recopilar la información son:

La encuesta: Es una técnica que consiste en obtener información acerca de una parte de la población o muestra, mediante el uso del cuestionario o de la entrevista. (Pardinas, 2005)

La entrevista: consiste en obtención de información oral de parte de una persona, recabada por el entrevistador directamente. (Pardinas, 2005)

La entrevista, que se llevará a cabo a todo el personal de la Unidad de Soporte Técnico Informático del Hospital III Iquitos de Essalud

La Observación: Con el fin de recolectar datos suficientes para verificar las hipótesis formuladas se hace necesario, precisamente observar los fenómenos en cuestión con objeto de determinar si existe una adecuación entre ellos y las hipótesis. (Pardinas, 2005)

Con las técnicas antes mencionadas, la compañía ha encontrado la posible respuesta a algunos problemas encontrados y para prevenir algunos riesgos, que se puedan suscitar; en primera instancia utilizaron la entrevista hacia el gerente de la compañía Hospital III Iquitos Essalud, que de una manera empírica, comento el problema, el cual está teniendo el área operativa, también utilizaron la encuesta que le ayudo a descifrar en manera general algunos problemas que poseen el trabajador de la compañía y por último la observación que por ejemplos la aplicaron al haber encontrado el problema en sí y de haber encontrado algunos factores del porqué del problema.

Los instrumentos que se utilizar son:

Cuestionario: El cuestionario es un formato redactado en forma de interrogatorio en donde se obtiene información acerca de las variables que se va a investigar.
Guía de encuesta: Son anotaciones de preguntas previo a una encuesta claramente identificada.
Fichas de campo: Esta ficha es un gran auxiliar de la investigación para anotar todo cuanto observamos en el lugar de los hechos, lo que servirá luego para la construcción del conocimiento.

EVALUACIÓN DE LA SITUACIÓN ACTUAL

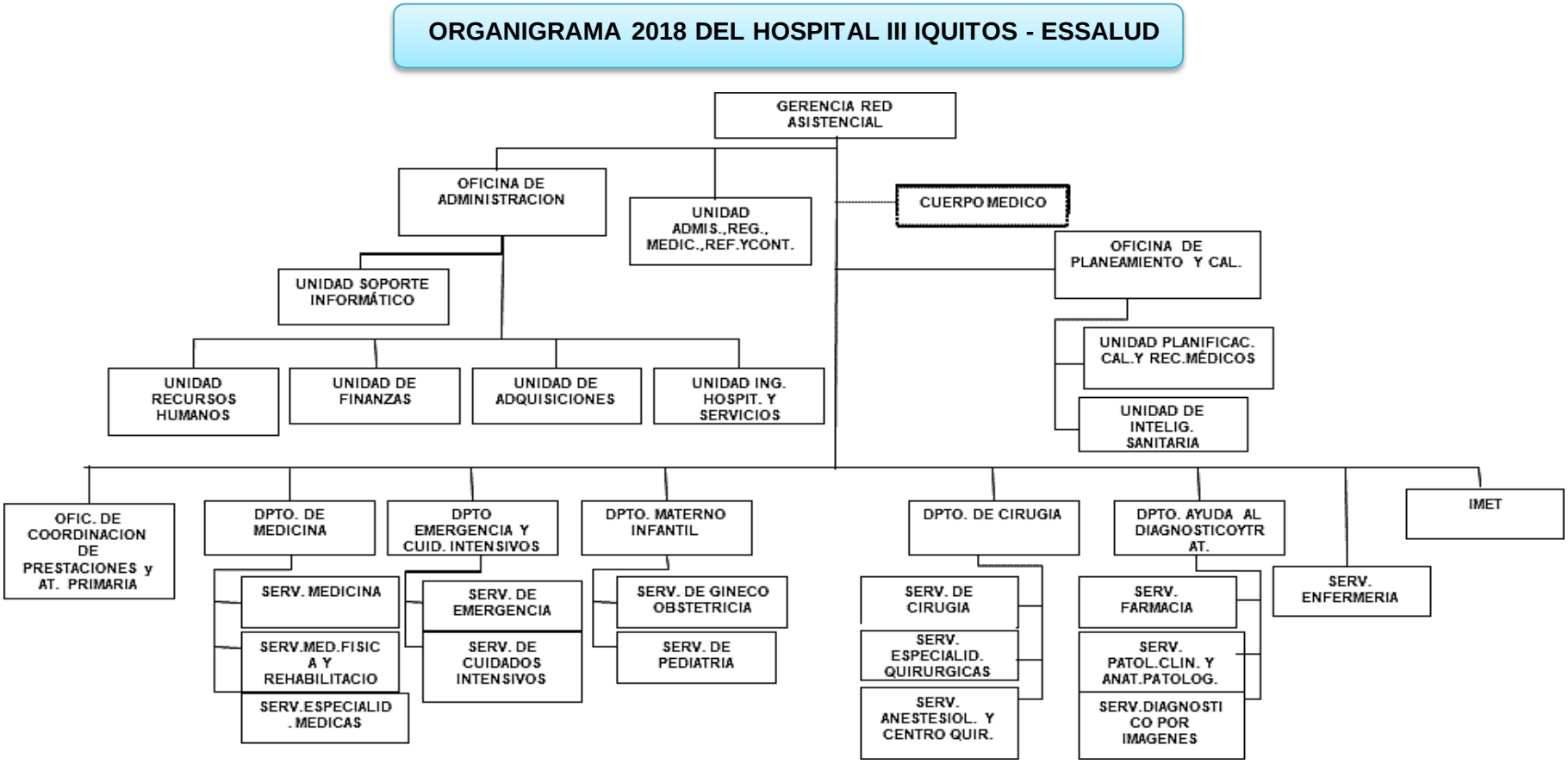
- **Organización**

  El Hospital III Iquitos de Essalud, está ubicado en la zona norte de la ciudad de Iquitos en la Av. La Marina s/n con calle Los Rosales (MASUSA) Km. 2.5, distrito de Punchana, este hospital cuenta con 4 módulos de un piso y atiende a más de 3,000 asegurados por día, diariamente se produce mucho flujo de información sobre las consultas, historias clínicas, farmacia, análisis de laboratorio entre otros.

  El Hospital, es un centro donde se referencia las distintas especialidades, el cual recibe a los pacientes que se derivan de los distintos policlínicos, situados en los diferentes distritos del departamento o red Loreto, el hospital cuenta con las áreas administrativas donde se destacan: Gerencia , Planeamiento y Calidad, Unidad de Soporte Informático, Departamento de Medicina, departamento de Emergencia y Cuidados Intensivos, departamento Materno Infantil , departamento de Cirugía, departamento de Ayuda al Diagnóstico y Tratamiento, Servicio de Enfermería – Unidad de Admisión, Registros Médicos, Referencias y Contrarreferencias, entre los otros.

- **Estructura orgánica**

Ilustración 01: Organigrama Institucional.



Fuente: *MOF - ESSALUD*

Descripción de funciones de los responsables del área.

a) **Gerencia de Red.**

Ejerce el cargo de administrar y otorgar prestaciones de salud, económicas y sociales en la Red Asistencial de Loreto. También programa, dirige, controla y evalúa la gestión de la Red Asistencial de Loreto e impartir las disposiciones pertinentes.

b) **Oficina de Administración.**

Cumple la función de organizar, dirigir y controlar las actividades de los procesos técnicos que conforman el sistema administrativo integrado por las unidades de Recursos Humanos, Finanzas, Adquisiciones y la Unidad de Ingeniería Hospitalaria y Servicios.

c) **Unidad de Prestación económico y sociales.**

Mejora el proceso de envejecimiento de las personas mayores, mediante el desarrollo de programas y proyectos que permitan la integración familiar, según normas y procedimientos establecidos por la Gerencia de Prestación Social.

d) **Oficina de Planeamiento y Calidad.**

Se encarga de organizar, dirigir y controlar las actividades de los procesos técnicos que conforman dicha oficina.

e) **Unidad de Inteligencia Sanitaria.**

Es el que ejecuta los procedimientos técnicos que conforman el sistema de inteligencia Sanitaria.

f) **Unidad de Recursos Humanos.**

Ejecuta actividades relacionadas con los procesos, procedimientos, proyectos y actividades relacionados a la selección, promoción, carrera, contrataciones y bienestar social.

g) **Unidad de Finanzas.**

Cumple la función de ejecutar los procesos técnicos que conforman los sistemas de: Contabilidad, Costos, Presupuesto, Tesorería y los que correspondan a la recuperación de las cuentas y deudas.

h) **Unidad de Adquisiciones.**

Ejecuta los procedimientos técnicos que conforman el sistema de Adquisiciones y almacenes relacionados a los procesos de compra local de la Red.

i) **Unidad de Soporte Informático.**

Cumple la función de planificar, coordinar, controlar y evaluar la gestión de la Unidad e impartir las disposiciones pertinentes.

j) **Oficina de Coordinación de Prestaciones y Atención Primaria.**

Se encarga de realizar permanentemente la evaluación del balance entre la oferta disponible en los centros asistenciales y hospitales de referencia que integran la Red Asistencial y la demanda de la población adscrita y poner el plan de ajustes.

k) **Dpto. Emergencia y Cuidado Intensivos.**

Cumple la función de planificar, organizar, y controlar el otorgamiento de las prestaciones asistenciales en el ámbito de responsabilidad del Dpto. Emergencia y Cuidado Intensivo.

l) **Dpto. de Medicina.**

Se encarga de planificar, organizar, ejecutar y controlar el otorgamiento de las prestaciones asistenciales en el ámbito del Depto. De Medicina.

m) **Servicio de Enfermería.**

Cumple la función de registrar y procesar datos del Servicio de Emergencia en los sistemas de información institucional autorizado.

n) **Departamento Materno Infantil.**

Se encarga de planificar, organizar, ejecutar y controlar el otorgamiento de las prestaciones de servicio de salud en el ámbito de del Departamento Materno Infantil.

o) **Servicio de Pediatría.**

Ejecuta actividad de promoción, prevención, recuperación y rehabilitación de la salud, según la capacidad resolutiva del servicio pediátrica.

Inventario Informático

- ✓ **Hardware**

El parque informático del hospital III Iquitos está conformado por: 127 computadoras, 126 monitores, 9 servidores operativos, 127 teclados, 62 impresoras, 2 relojes biométricos, 11 Switcher entre otros, en donde los usuarios puedan realizan distintos procesos en el transcurso del día, a continuación, le mostramos alguna de las características de cada hardware.

Tabla 02: Computadoras

MARCA	MODELO	PROCESADOR	MEMORIA RAM	CAPACIDAD DE ALMACENAR	CANTIDAD
DELL	OPTIPLEX 9020	INTEL I7	8 GB	1 TB	89
OTROS	S/M	INTEL CORE 2 DUO	512 MB	250 GB	1
LENOVO	M7303-A72	INTEL CORE 2 DUO	2 GB	160 GB	10
HP	DC7900	INTEL CORE 2 DUO	2 GB	250 GB	27

Fuente: *Elaboración Propia*

Tabla 03: Monitores

Marca	Modelo	Pulgadas	Cantidad
LENOVO	L197	19	8
DELL	E2016H	19	2
HP	LE1901w	19	28
AOC	I2080SW	19	2

Fuente: *Elaboración Propia*

Tabla 04:Servidores

Marca	Modelo	Procesador	Memoria	Capacidad de Disco	Sistema Operativo
DELL	POWEREDGE R370 T1	Intel Xeon 2.6 Ghz	128 GB	8.4 TB	Linux Red Hat Enterprise V.5.9
IBM	SYSTEM X3500	INTEL XEON	3 Gb.	300 Gb.	Linux Red Hat Enterprise V.5.4
HP	Proliant ML350	INTEL XEON 1.8Ghz	2 Gb.	144Gb	Linux Red Hat Enterprise V.5.1
IBM	SYSTEM X3650 N2	INTEL XEON 2.0Ghz	2 Gb.	146Gb	Linux Red Hat Enterprise V.5.4
DELL	POWEREDGE R370 T1	Intel Xeon 2.6 Ghz	128 GB	8.4 TB	Linux Red Hat Enterprise V.5.9
DELL	E31S	Intel Xeon 2.6 Ghz	128 GB	8.4 TB	Windows Server
DELL	E31S	Intel Xeon 2.6 Ghz	128 GB	8.4 TB	Tape backup
DELL	E31S	Intel Xeon 2.6 Ghz	129 GB	8.4 TB	Tape backup
HP	6300 Small	CORE i5	8 Gb	1 Tb	Linux RED HAT 5

Fuente: *Elaboración Propia*

Tabla 05: Teclado

Marca	Modelo	Cantidad
DELL	KB212-B	127

Fuente: *Elaboración Propia*

Tabla 06: Reloj Biométrico

Marca	Modelo	Cantidad
TOCTTEX	T6	2

Fuente: *Elaboración Propia*

Tabla 07: Switcher

Marca	Modelo	Puerto
Alcatel	OmniSwitch 6850-24	24

Fuente: *Elaboración Propia*

✓ **Software**

- **Ofimática.**

  Para la elaboración de documentación se utilizan los siguientes paquetes de MS Office H&E 2013, 2016, 2019. Todos estos softwares se encuentran licenciados.

- **Antivirus.**

  Con respecto al servicio del antivirus esto se encuentra en un servidor virtualizado que está dentro del Sistema Operativo Windows server 2012 R2, el antivirus que brinda servicio a la Unidad de soporte Informático es el Sophos que distribuye por todas las áreas del hospital III Iquitos Essalud.

✓ **Sistemas de Información**

- Sistemas operativos Servidores.

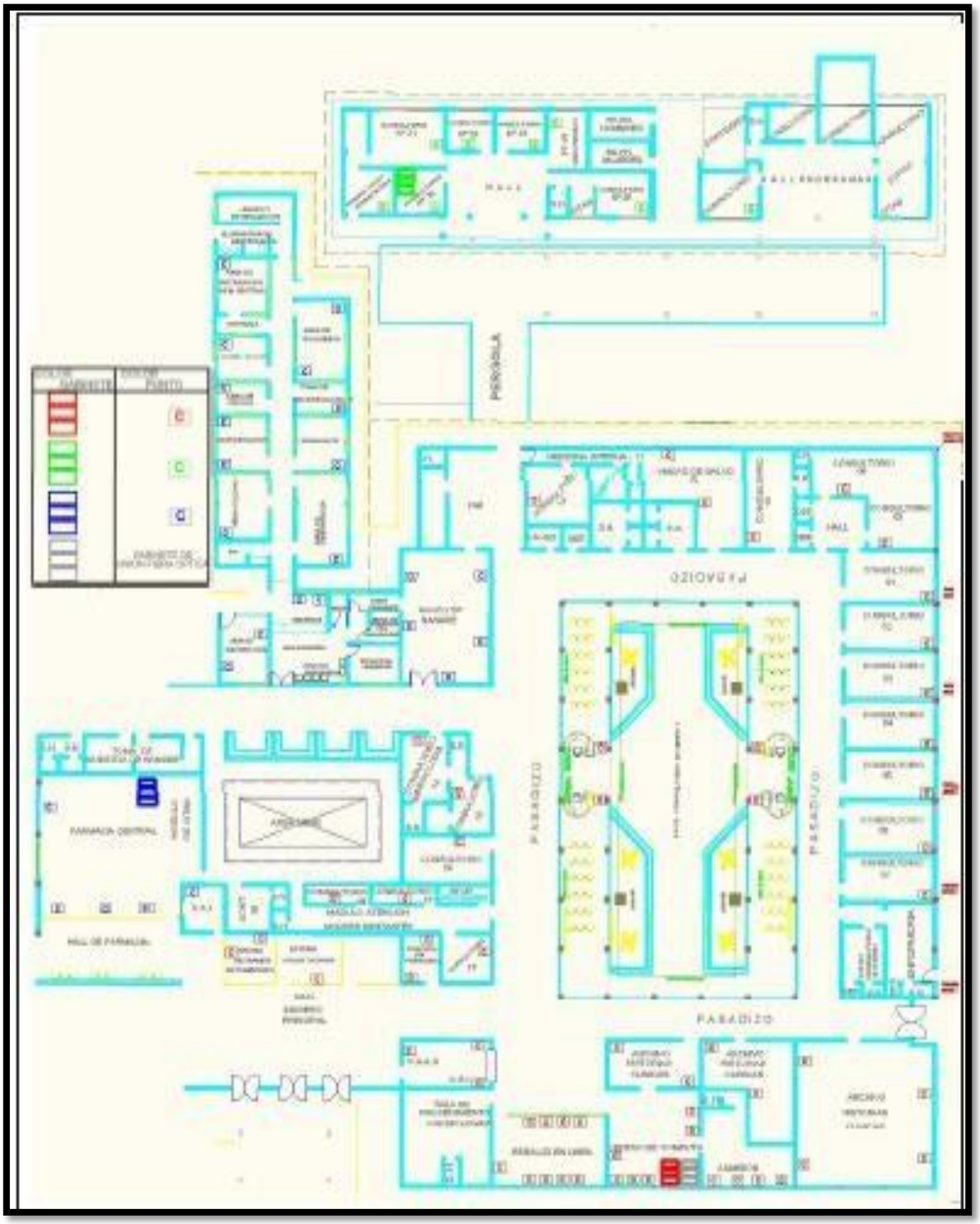
  Dentro del hospital III de Iquitos se utilizan los servidores, Linux Red Hat Enterprise V.5.9, Windows Server, Windows Server 2012 R2.

- Sistemas Operativos.

  El sistema operativo que utilizan las computadoras dentro del hospital III Iquitos son: Windows 7, 8.1 y 10, todos estos sistemas operativos cuentan con licencia original.

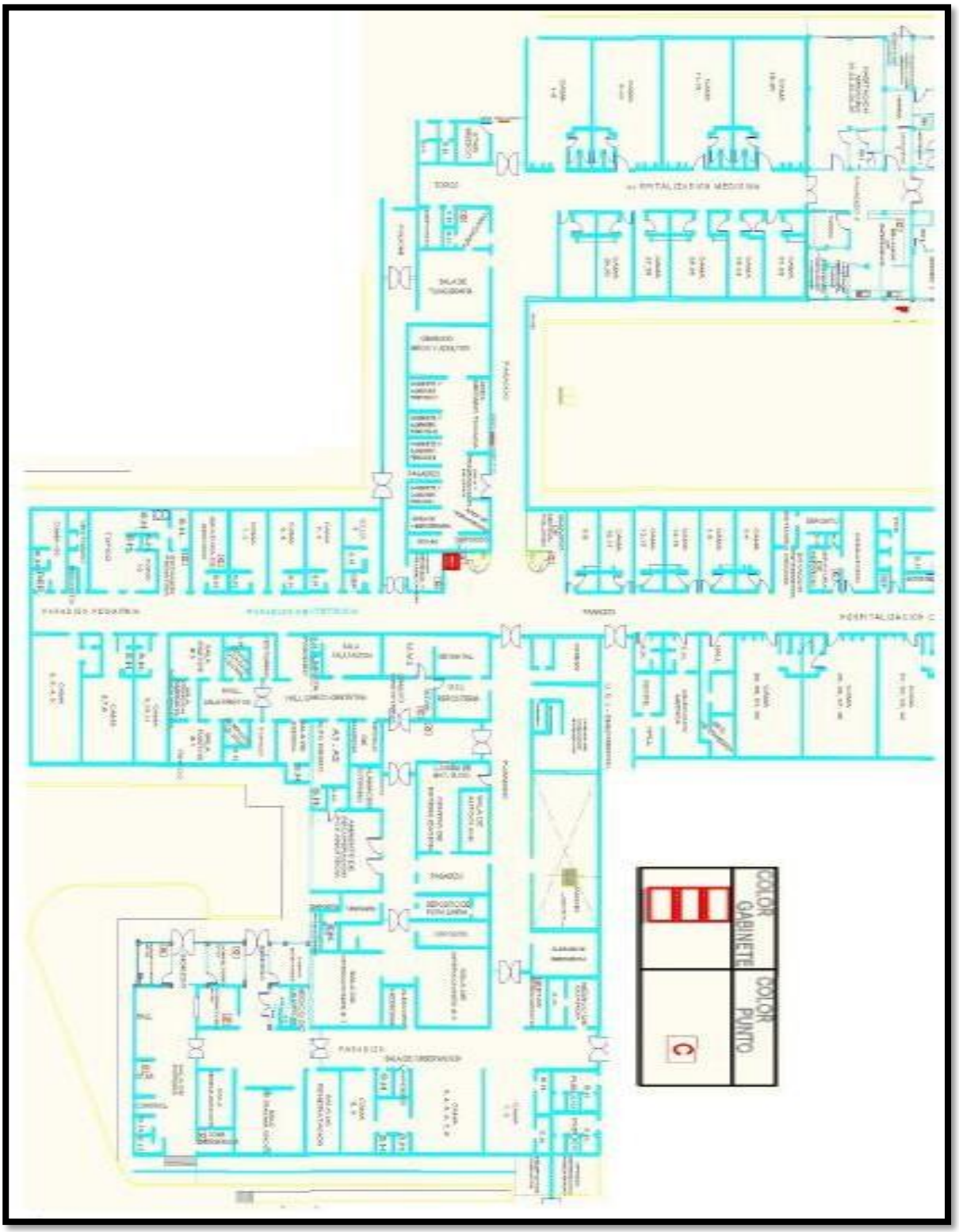
✓ **Plano de Distribución de la red de datos**

Ilustración 02: Plano del Edificio A (Primer Nivel) del Hospital Essalud III – Iquitos



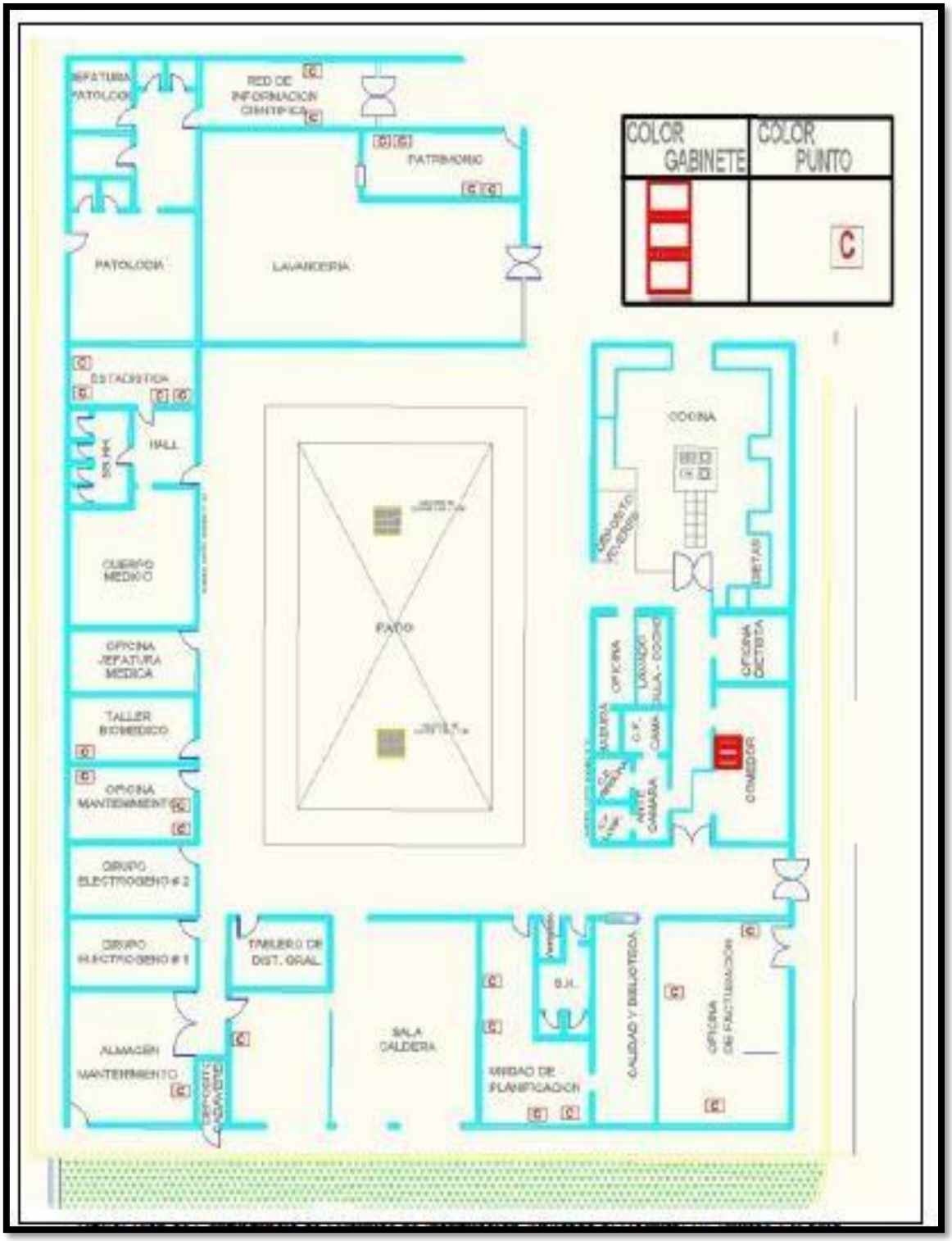
Fuente: Unidad de Soporte Técnico

Ilustración 03: Plano del Edificio A (Segundo Nivel) del Hospital Essalud III – Iquitos



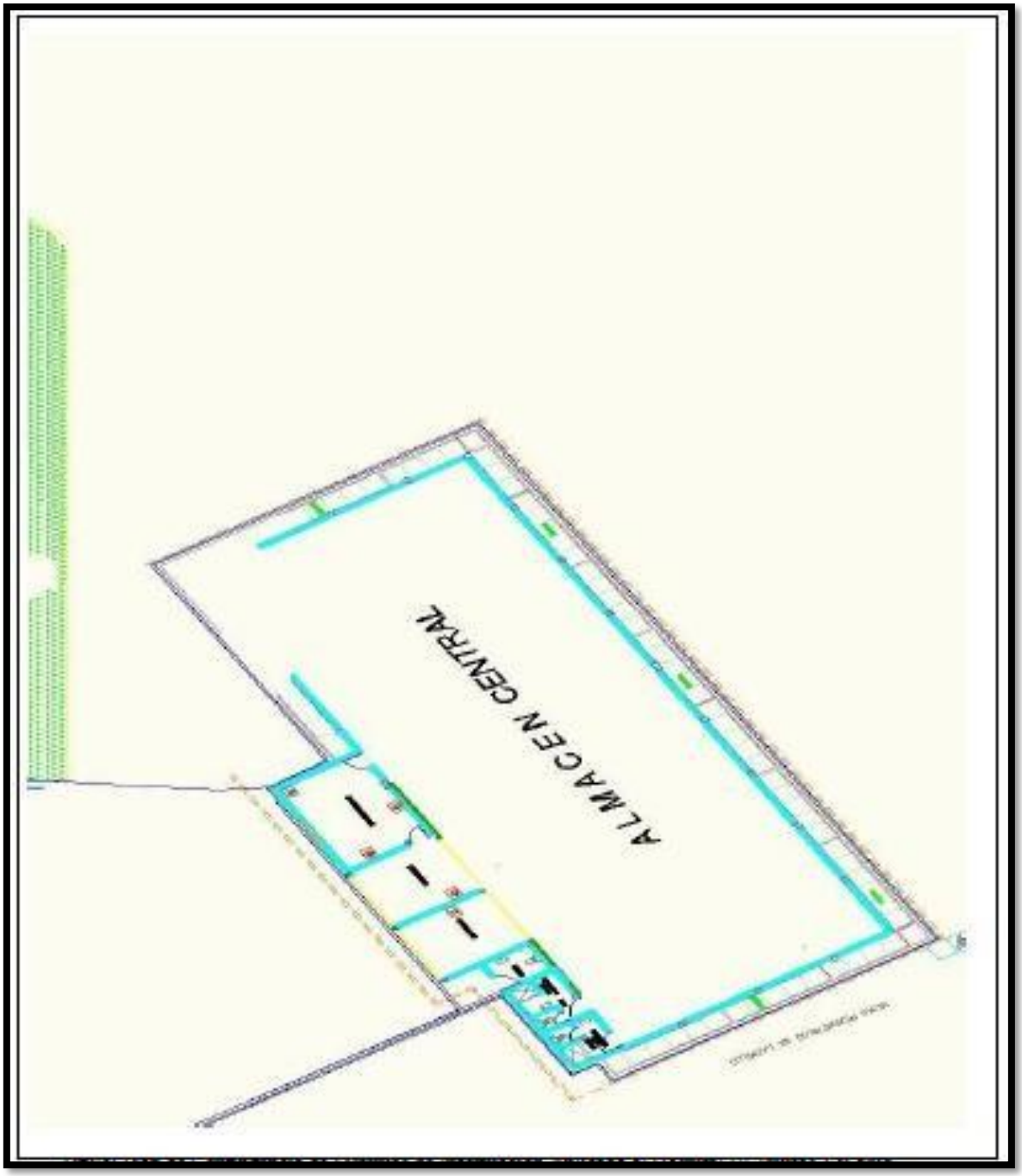
Fuente: Unidad de Soporte Técnico

Ilustración 04: Plano del Edificio A (Tercer Nivel) del Hospital Essalud III – Iquitos



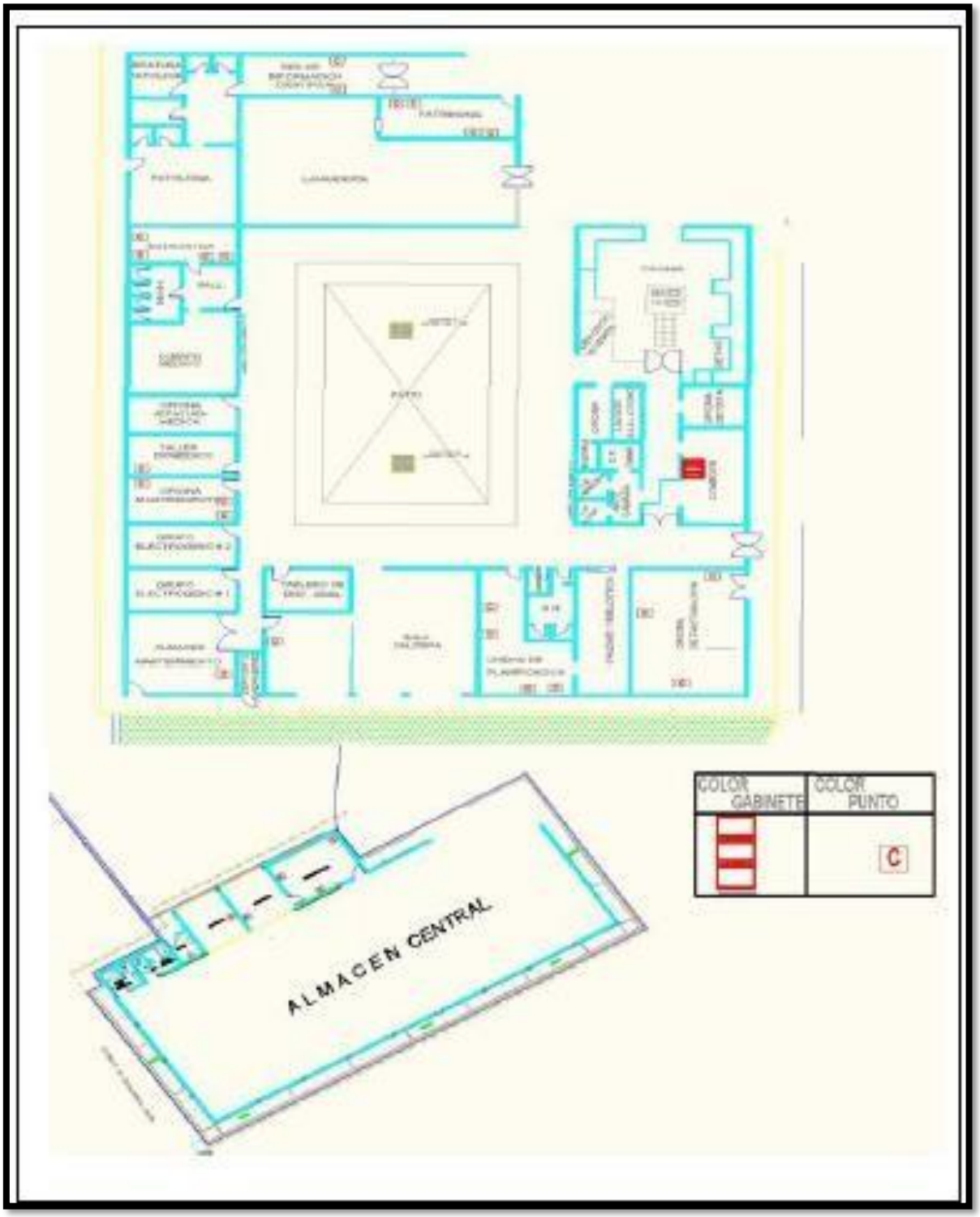
Fuente: Unidad de Soporte Técnico

Ilustración 05: Plano del Edificio B (Primer Nivel) del Hospital Essalud III – Iquitos



Fuente: Unidad de Soporte Técnico

Ilustración 6: Plano del Edificio Completo del Hospital Essalud III – Iquitos



Fuente: Unidad de Soporte Técnico

REALIDAD PROBLEMÁTICA O SITUACIÓN ACTUAL

El problema que nos aborda en este trabajo de suficiencia profesional es la Unidad de Soporte Informático del Hospital II-Iquitos, que se encuentra en una oficina dentro del Hospital III de Essalud Iquitos, cito en la Av. La Marina s/n con calle Los Rosales (MASUSA) Km. 2.5, distrito de Punchana, donde se va evaluar el nivel de seguridad en el que se encuentra la unidad de soporte informático y todo lo que tiene a su cargo como los equipos de cómputo, redes y comunicaciones, servidores, etc.

La Unidad de Soporte Informático, es la encargada de controlar, monitorear y verificar el uso apropiado de las Tecnologías de Información; para ello cuenta con los equipos y sistemas informáticos apropiados para brindar un servicio de calidad a los usuarios y asegurados.

Es por ello que mediante este estudio vamos a evaluar el riesgo y el nivel de seguridad informática que tiene para poder brindar los servicios de manera continua, cumpliendo con los estándares exigidos por las normas y directivas del estado respecto a la seguridad de la información, ya que de acuerdo a estos estándares la información que maneja y custodia la unidad de soporte informático debería conservar las características principales de la integridad, disponibilidad y confidencialidad de la información, esto se logrará.

Para la elaboración del Plan de seguridad informática aplicaremos una encuesta para valorar los niveles de seguridad implementados a la fecha y también se pueda describir las vulnerabilidades y amenazas con que está expuesta los procesos de

CAPÍTULO IV

Resultados

- Análisis Descriptivo de la Evaluación respecto a la Seguridad de la Información Institucional

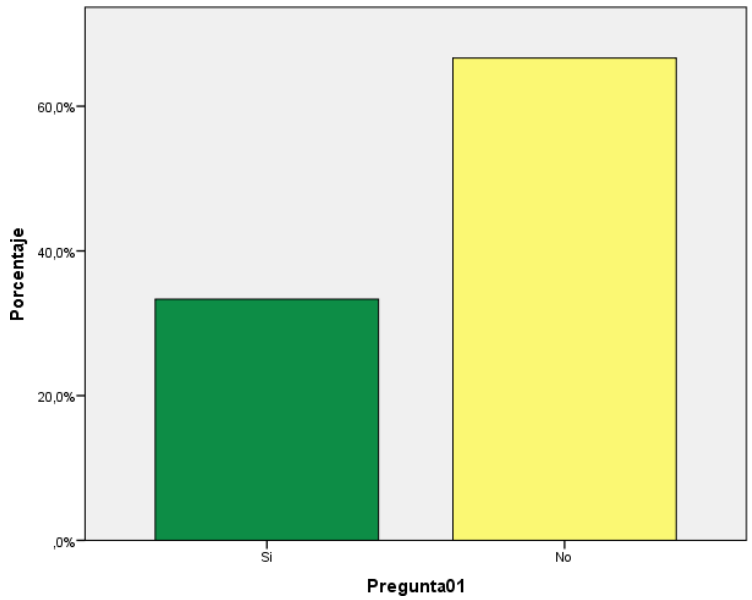
Tabla 01

Pregunta 01: ¿La Institución invierte presupuesto en ciberseguridad?

Respuesta	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Si	3	33,3	33,3	33,3
No	6	66,7	66,7	100,0
Total	**9**	**100**	**100**	

Fuente: *Elaboración Propia*

Gráfico N°01



Fuente: *Elaboración Propia*

Interpretación: De la Tabla 01 y Gráfico 01 se puede determinar que de las 9 personas que trabajan en la Unidad de Soporte Informático del Hospital III Iquitos de Essalud el 33,3% respondió que su Institución si invierte presupuesto en ciberseguridad y el 66,7% respondió que no.

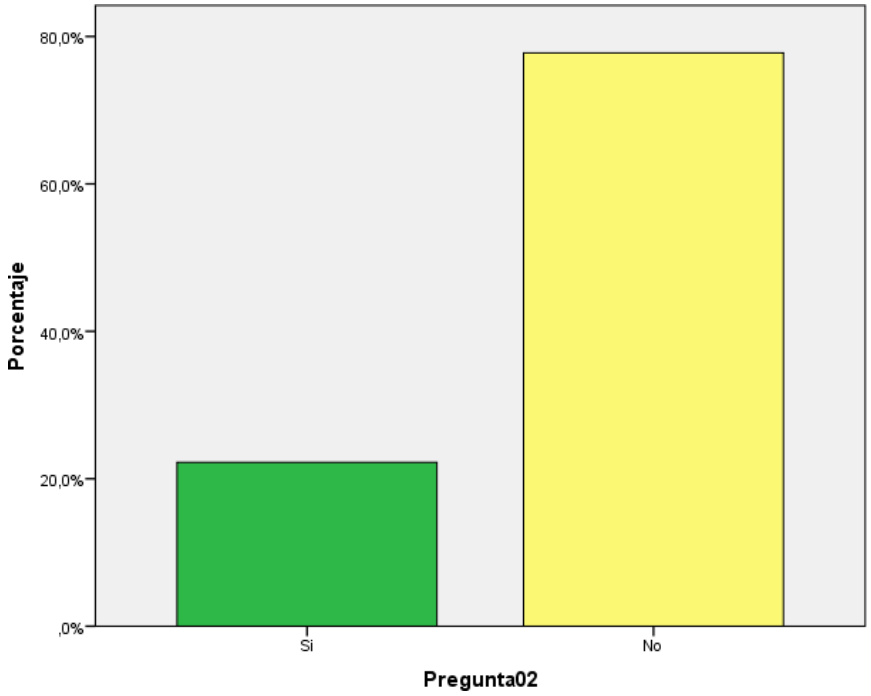
Tabla 02

Pregunta 02: ¿El área cuenta con personal especializado en seguridad informática?

Respuesta	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Si	2	22,2	22,2	22,2
No	7	77,8	77,8	100
Total	**9**	**100**	**100**	

Fuente: *Elaboración Propia*

Gráfico N°02



Fuente: *Elaboración Propia*

Interpretación: De la Tabla 02 y Gráfico 02 se puede determinar que de las 9 personas que trabajan en la Unidad de Soporte Informático del Hospital III Iquitos de Essalud el 22,2% respondió que el área cuenta con personal especializado en seguridad informática y el 77,8% respondió que no.

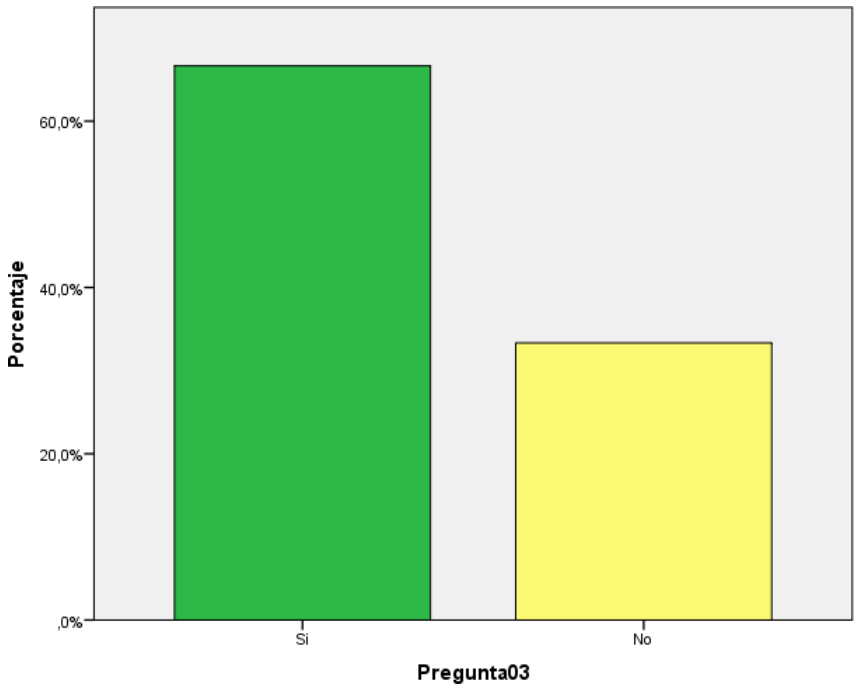
Tabla 03

Pregunta 03: ¿El área propende por el correcto y seguro funcionamiento de las instalaciones de procesamiento de la información y medios de comunicación?

Respuesta	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Si	6	66,7	66,7	66,7
No	3	33,3	33,3	100,0
Total	**9**	**100**	**100**	

Fuente: *Elaboración Propia*

Gráfico N°03



Fuente: *Elaboración Propia*

Interpretación: De la Tabla 03 y Gráfico 03 se puede determinar que de las 9 personas que trabajan en la Unidad de Soporte Informático del Hospital III Iquitos de Essalud el 66,7% respondió que el área si propende por el correcto y seguro funcionamiento de las instalaciones de procesamiento de la información y medios de comunicación y el 33,3% respondió que no.

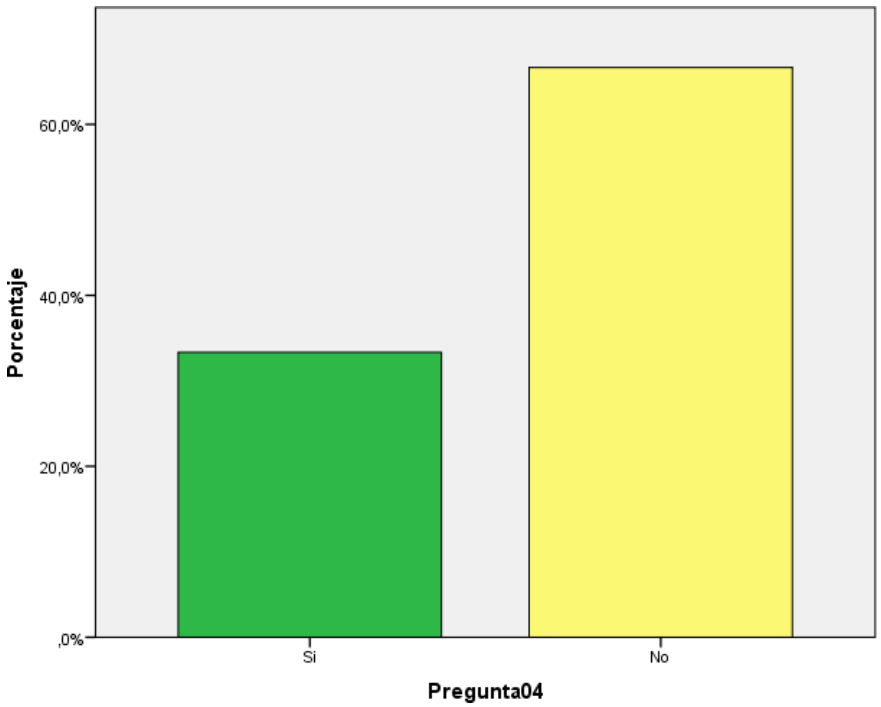
Tabla 04

Pregunta 04: ¿El área cuenta con procedimientos estandarizados para adquisición, desarrollo y/o mantenimiento de software, que garanticen niveles de seguridad de la(s) aplicación(es)?

Respuesta	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Si	3	33,3	33,3	33,3
No	6	66,7	66,7	100,0
Total	**9**	**100,0**	**100,0**	

Fuente: *Elaboración Propia*

Gráfico N°04



Fuente: *Elaboración Propia*

Interpretación: De la Tabla 04 y Gráfico 04 se puede determinar que de las 9 personas que trabajan en la Unidad de Soporte Informático del Hospital III Iquitos de Essalud el 33,7% respondió que el área si cuenta con procedimientos estandarizados para adquisición, desarrollo y/o mantenimiento de software, que garanticen niveles de seguridad de la(s) aplicación(es) y el 66,7% respondió que no.

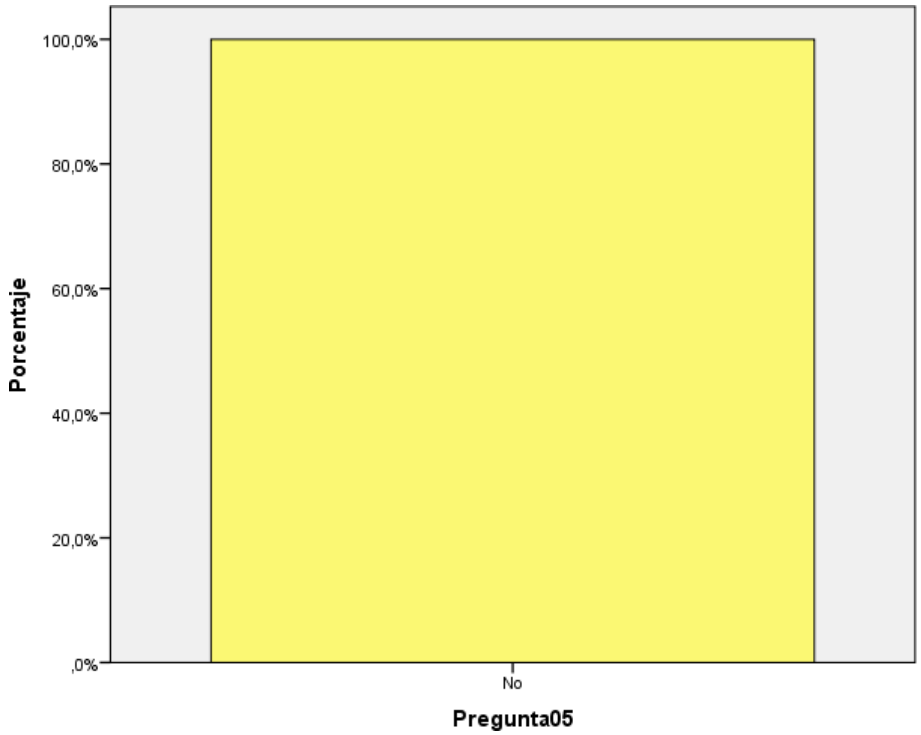
Tabla 05

Pregunta 05: ¿Existe una Política de seguridad adoptada institucionalmente por el área?

Respuesta	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
No	9	100,0	100,0	100,0

Fuente: *Elaboración Propia*

Gráfico N°05



Fuente: *Elaboración Propia*

Interpretación: De la Tabla 05 y Gráfico 05 se puede determinar que de las 9 personas que trabajan en la Unidad de Soporte Informático del Hospital III Iquitos de Essalud el 100% respondió que no existe una Política de seguridad adoptada institucionalmente por el área

- Análisis Descriptivo de la Evaluación de las vulnerabilidades y amenazas respecto a la integridad de la información por el área de Soporte Técnico.

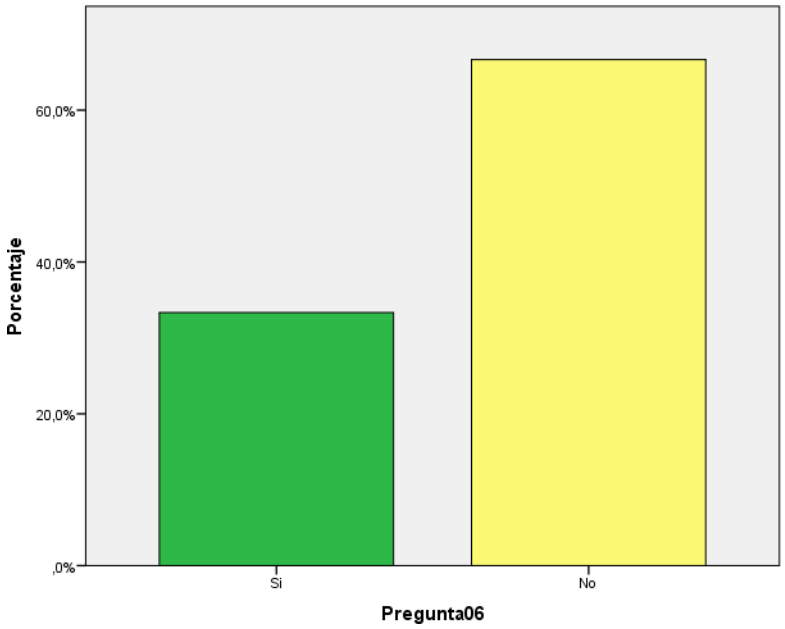
Tabla 06

Pregunta 06: ¿El área tiene establecidos protocolos para garantizar la seguridad en la información almacenada?

Respuesta	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Si	3	33,3	33,3	33,3
No	6	66,7	66,7	100,0
Total	**9**	**100,0**	**100,0**	

Fuente: *Elaboración Propia*

Gráfico N°06



Fuente: *Elaboración Propia*

Interpretación: De la Tabla 06 y Gráfico 06 se puede determinar que de las 9 personas que trabajan en la Unidad de Soporte Informático del Hospital III Iquitos de Essalud el 33,3% respondió que el área si tiene establecidos protocolos para garantizar la seguridad en la información almacenada y el 66,7% dijo que no

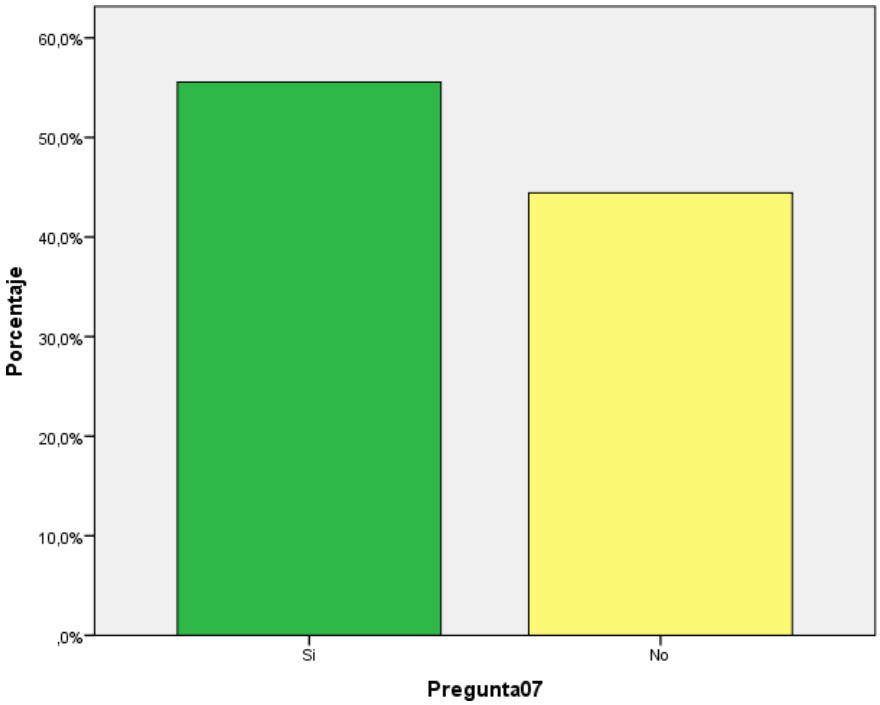
Tabla 07

Pregunta 07: ¿Realiza periódicamente Backup de la Información?

Respuesta	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Si	5	55,6	55,6	55,6
No	4	44,4	44,4	100,0
Total	**9**	**100,0**	**100,0**	

Fuente: *Elaboración Propia*

Gráfico N°07



Fuente: *Elaboración Propia*

Interpretación: De la Tabla 07 y Gráfico 07 se puede determinar que de las 9 personas que trabajan en la Unidad de Soporte Informático del Hospital III Iquitos de Essalud el 55,6% respondió que el área si realiza periódicamente Backup de la Información y el 44,4% dijo que no

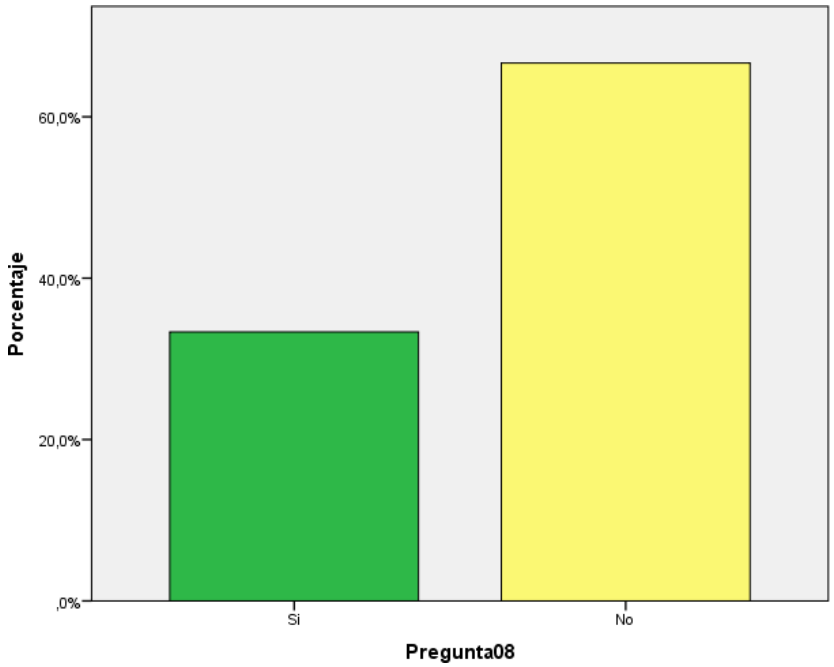
Tabla 08

Pregunta 08: ¿Usted considera que los datos que se ingresan por los sistemas informáticos son correctos?

Respuesta	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Si	3	33,3	33,3	33,3
No	6	66,7	66,7	100,0
Total	**9**	**100,0**	**100,0**	

Fuente: *Elaboración Propia*

Gráfico N°08



Fuente: *Elaboración Propia*

Interpretación: De la Tabla 08 y Gráfico 08 se puede determinar que de las 9 personas que trabajan en la Unidad de Soporte Informático del Hospital III Iquitos de Essalud el 33,3% respondió que si considera que los datos que se ingresan por los sistemas informáticos son correctos y el 66,7% dijo que no.

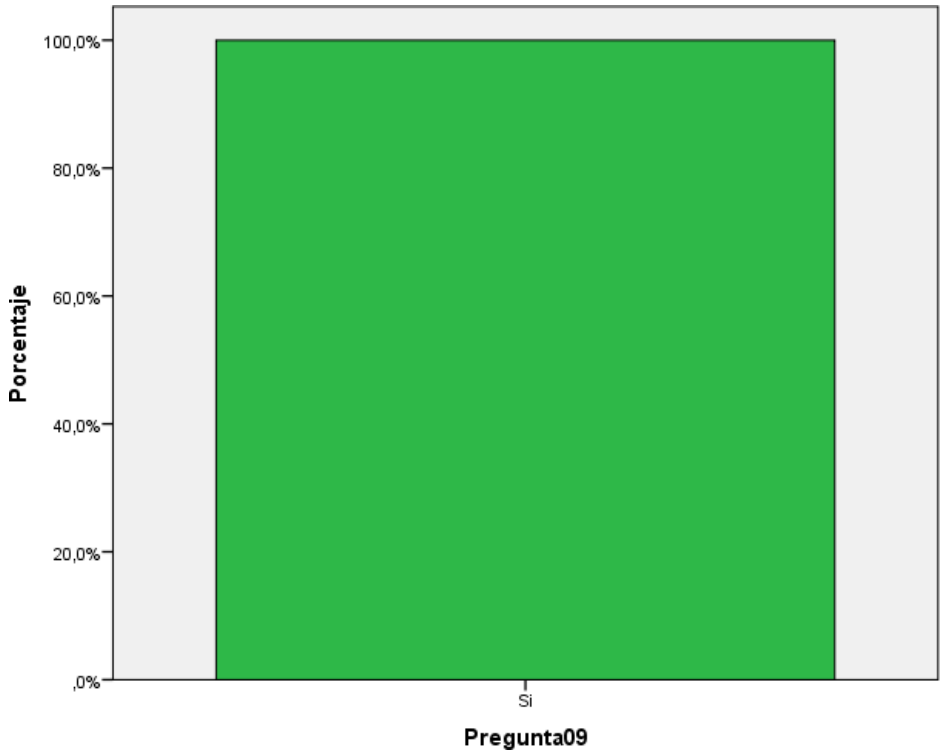
Tabla 09

Pregunta 09: ¿Los datos de los sistemas informáticos se almacenan en un equipo servidor?

Respuesta	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Si	9	100,0	100,0	100,0

Fuente: *Elaboración Propia*

Gráfico N°09



Fuente: *Elaboración Propia*

Interpretación: De la Tabla 09 y Gráfico 09 se puede determinar que de las 9 personas que trabajan en la Unidad de Soporte Informático del Hospital III Iquitos de Essalud el 100% respondió que los datos de los sistemas informáticos si se almacenan en un equipo servidor.

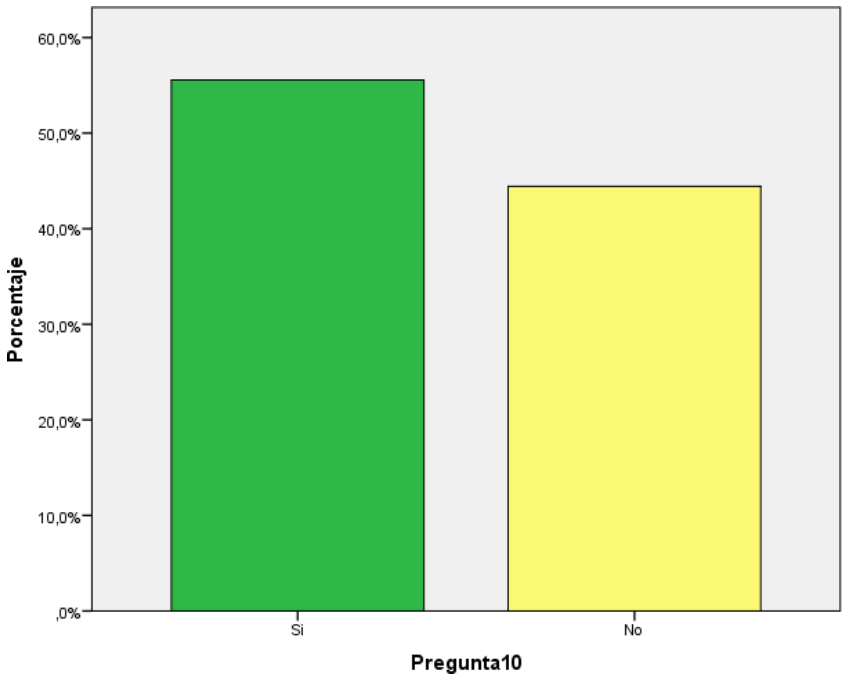
Tabla 10

Pregunta 10: ¿Los sistemas informáticos que cuentan, les permiten a los usuarios ingresar datos erróneos?

Respuesta	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Si	5	55,6	55,6	55,6
No	4	44,4	44,4	100,0
Total	**9**	**100,0**	**100,0**	

Fuente: *Elaboración Propia*

Gráfico N°10



Fuente: *Elaboración Propia*

Interpretación: De la Tabla 10 y Gráfico 10 se puede determinar que de las 9 personas que trabajan en la Unidad de Soporte Informático del Hospital III Iquitos de Essalud el 55,6% respondió que Los sistemas informáticos que cuentan si les permiten a los usuarios ingresar datos erróneos, y el 44,4% respondió que no.

- Análisis Descriptivo de la Evaluación de las vulnerabilidades y amenazas respecto a la disponibilidad de la información por el área de Soporte técnico.

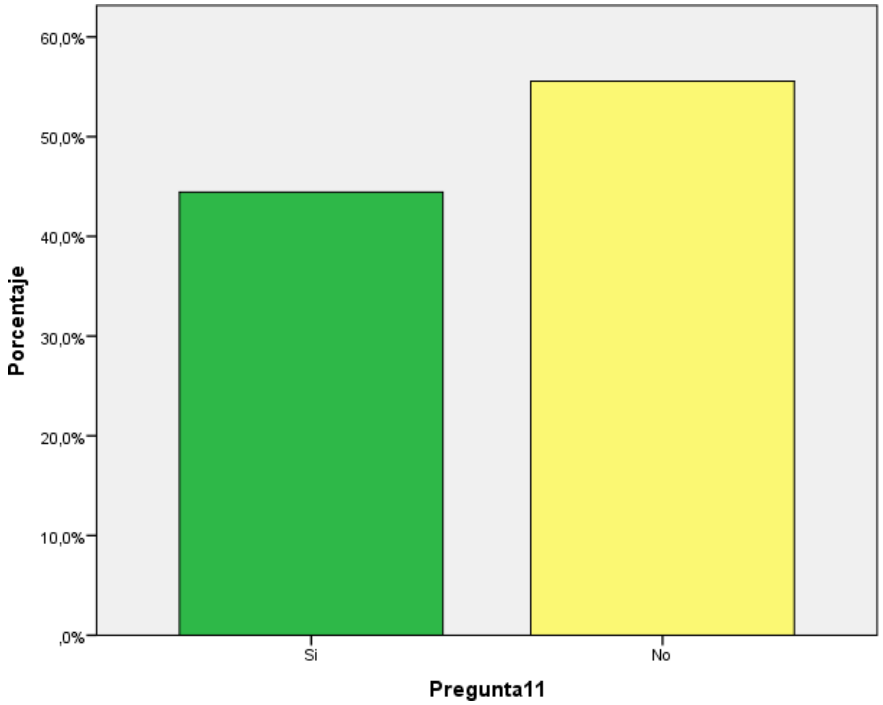
Tabla 11

Pregunta 11: ¿Considera que la red de datos en la que se transmite la información de los sistemas es segura?

Respuesta	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Si	4	44,4	44,4	44,4
No	5	55,6	55,6	100,0
Total	**9**	**100,0**	**100,0**	

Fuente: *Elaboración Propia*

Gráfico N°11



Fuente: *Elaboración Propia*

Interpretación: De la Tabla 11 y Gráfico 11 se puede determinar que de las 9 personas que trabajan en la Unidad de Soporte Informático del Hospital III Iquitos de Essalud el 44,4% respondió que, si considera que la red de datos en la que se transmite la información de los sistemas es segura, y el 55,6% respondió que no.

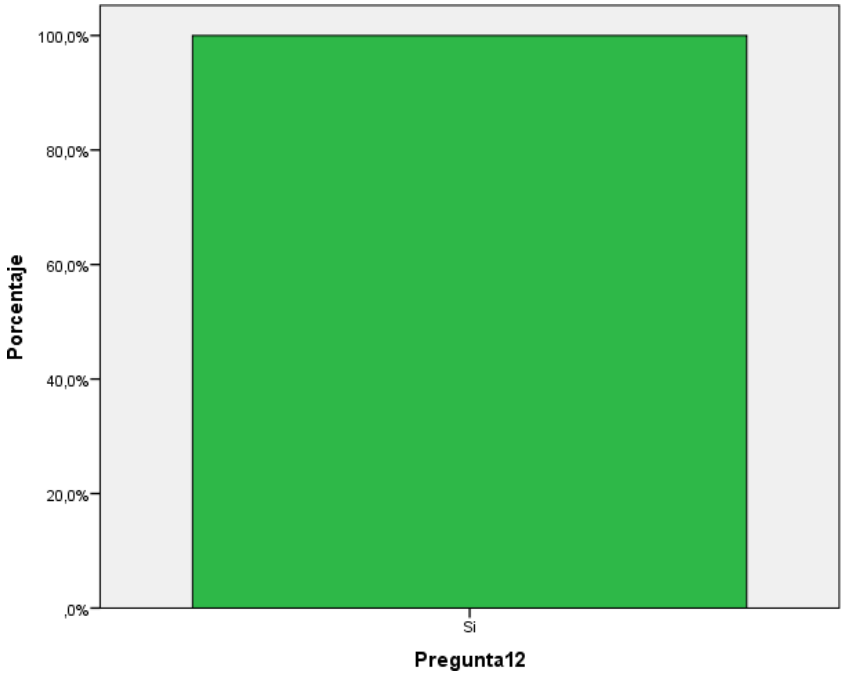
Tabla 12

Pregunta 12: ¿Realiza periódicamente mantenimiento a sus servidores?

Respuesta	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Si	9	100,0	100,0	100,0

Fuente: *Elaboración Propia*

Gráfico N°12



Fuente: *Elaboración Propia*

Interpretación: De la Tabla 12 y Gráfico 12 se puede determinar que de las 9 personas que trabajan en la Unidad de Soporte Informático del Hospital III Iquitos de Essalud el 100 respondió que, si se realiza periódicamente mantenimiento a sus servidores.

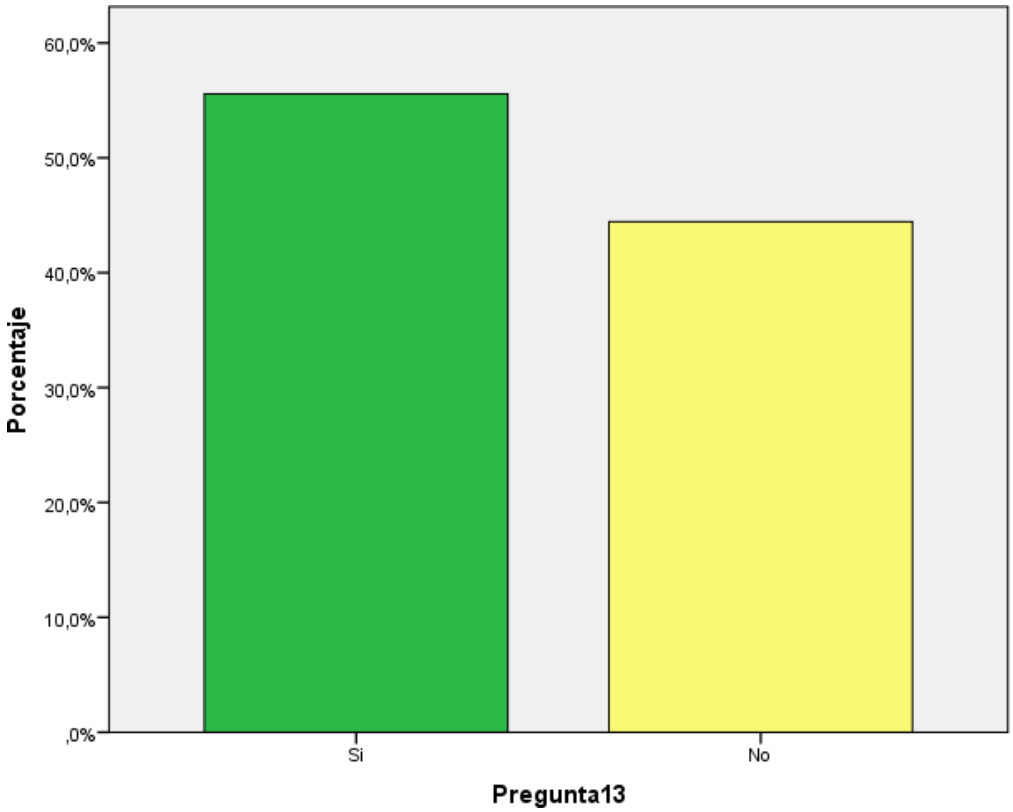
Tabla 13

Pregunta 13: ¿El área considera tener controlados todos los incidentes de seguridad que han ocurrido en la red de datos?

Respuesta	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Si	5	55,6	55,6	55,6
No	4	44,4	44,4	100,0
Total	**9**	**100,0**	**100,0**	

Fuente: *Elaboración Propia*

Gráfico N°13



Fuente: *Elaboración Propia*

Interpretación: De la Tabla 13 y Gráfico 13 se puede determinar que de las 9 personas que trabajan en la Unidad de Soporte Informático del Hospital III Iquitos de Essalud el 55,6% respondió que, si considera que el área tiene controlados todos los incidentes de seguridad que han ocurrido en la red de datos, y el 44,4% respondió que no.

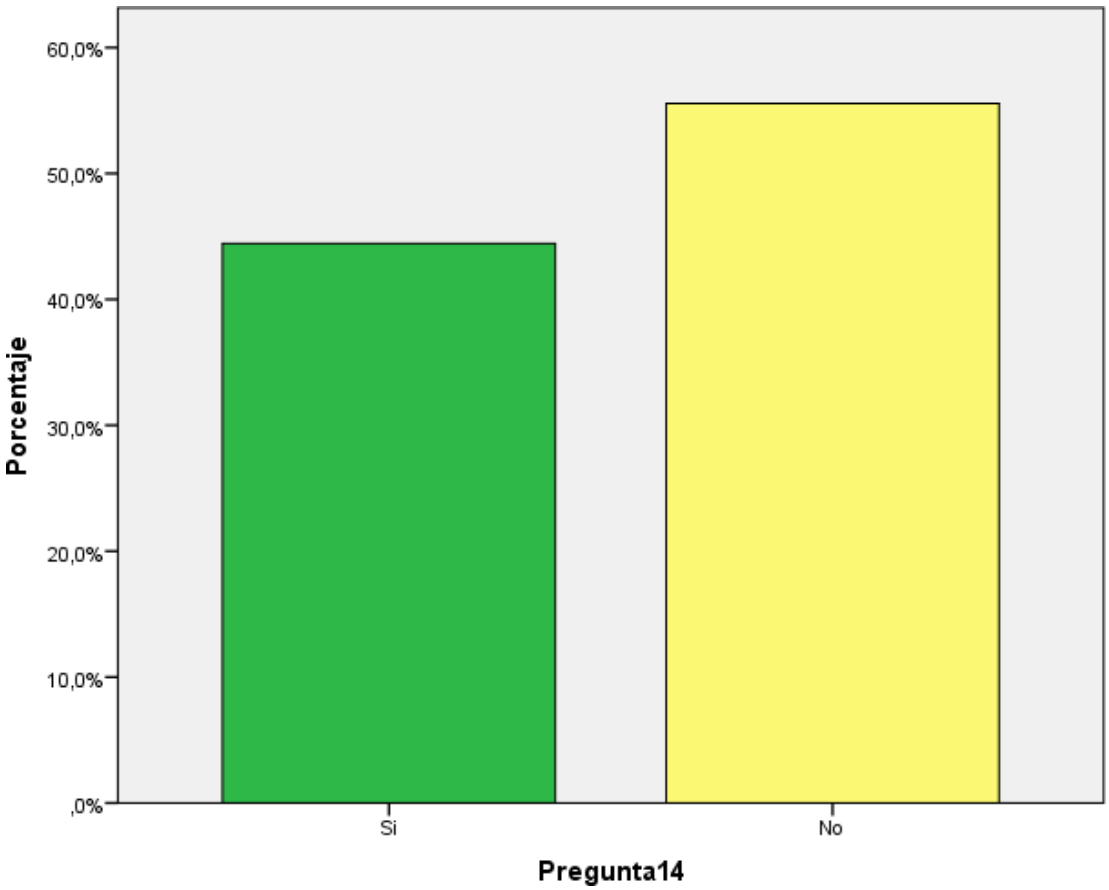
Tabla 14

Pregunta 14: ¿El área tiene establecido un Plan de respuesta a incidentes?

Respuesta	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Si	4	44,4	44,4	44,4
No	5	55,6	55,6	100,0
Total	**9**	**100**	**100**	

Fuente: *Elaboración Propia*

Gráfico N°14



Fuente: *Elaboración Propia*

Interpretación: De la Tabla 14 y Gráfico 14 se puede determinar que de las 9 personas que trabajan en la Unidad de Soporte Informático del Hospital III Iquitos de Essalud el 44,4% respondió que, si considera que el área tiene establecido un Plan de respuesta a incidentes, y el 55,6% respondió que no.

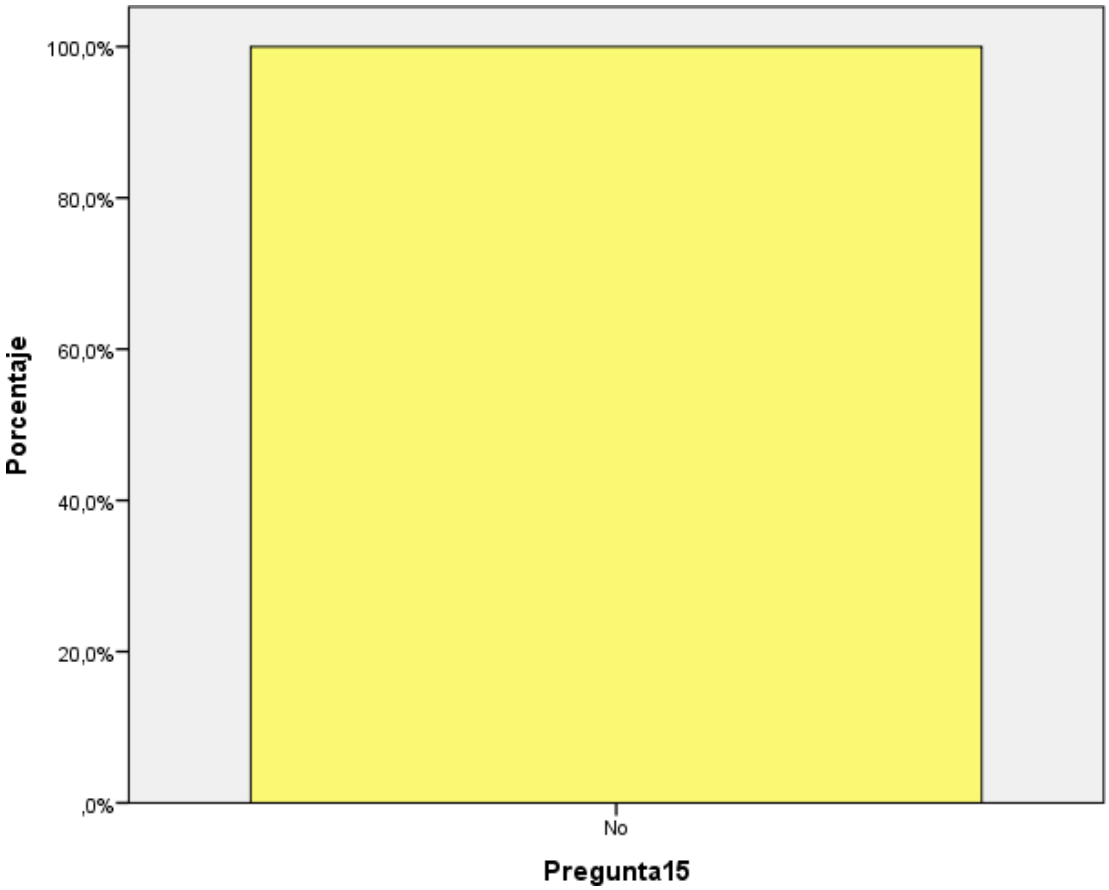
Tabla 15

Pregunta 15: ¿Cuentan con un plan de prevención de riesgos informáticos?

Respuesta	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
No	9	100	100	100

Fuente: *Elaboración Propia*

Gráfico N°15



Fuente: *Elaboración Propia*

Interpretación: De la Tabla 15 y Gráfico 15 se puede determinar que de las 9 personas que trabajan en la Unidad de Soporte Informático del Hospital III Iquitos de Essalud el 100% respondió que, no considera que el área tiene Cuentan con un plan de prevención de riesgos informáticos

- Análisis Descriptivo de la Evaluación de las vulnerabilidades y amenazas respecto a la confidencialidad de la información por el área de soporte técnico.

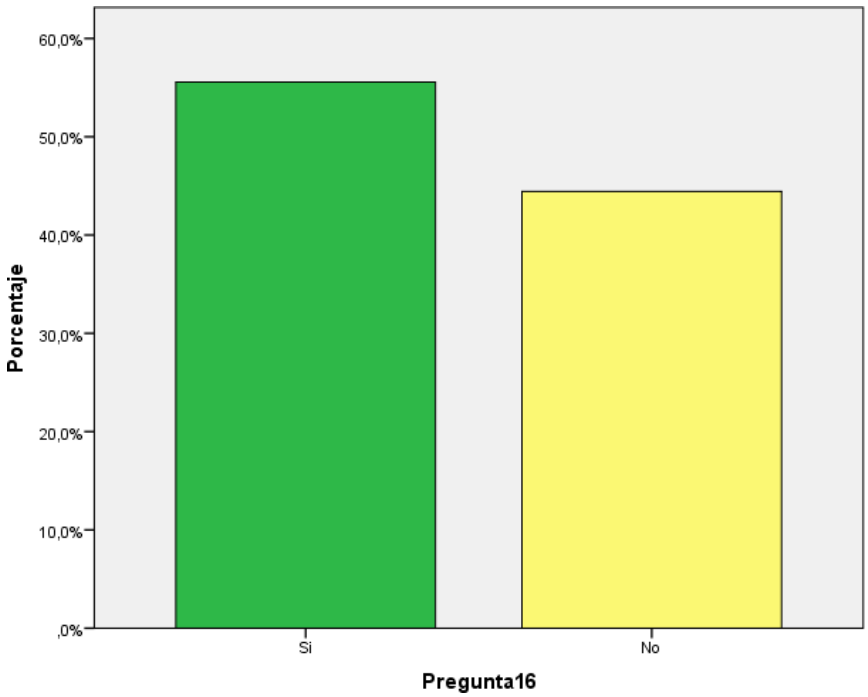
Tabla 16

Pregunta 16: ¿Los empleados hacen un uso adecuado de las contraseñas y datos personales?

Respuesta	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Si	5	55,6	55,6	55,6
No	4	44,4	44,4	100,0
Total	**9**	**100**	**100**	

Fuente: *Elaboración Propia*

Gráfico N°16



Fuente: *Elaboración Propia*

Interpretación: De la Tabla 16 y Gráfico 16 se puede determinar que de las 9 personas que trabajan en la Unidad de Soporte Informático del Hospital III Iquitos de Essalud el 55,6% respondió que, si considera que los empleados hacen un uso adecuado de las contraseñas y datos personales, y el 44,4% respondió que no.

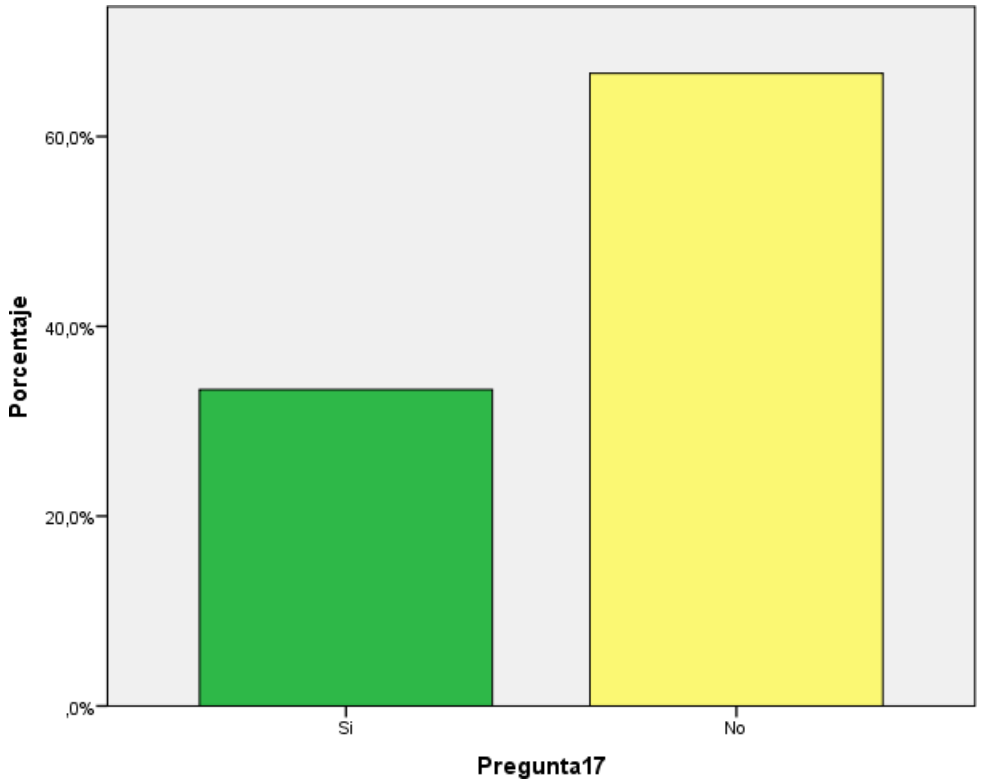
Tabla 17

Pregunta 17: ¿El manejo de usuarios y contraseñas de los sistemas de información se actualizan o cambian periódicamente?

Respuesta	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Si	3	33,3	33,3	33,3
No	6	66,7	66,7	100,0
Total	**9**	**100**	**100**	

Fuente: *Elaboración Propia*

Gráfico N°17



Fuente: *Elaboración Propia*

Interpretación: De la Tabla 17 y Gráfico 17 se puede determinar que de las 9 personas que trabajan en la Unidad de Soporte Informático del Hospital III Iquitos de Essalud el 33,3% respondió que en el manejo de usuarios y contraseñas de los sistemas de información si se actualizan o cambian periódicamente, y el 66,7% respondió que no.

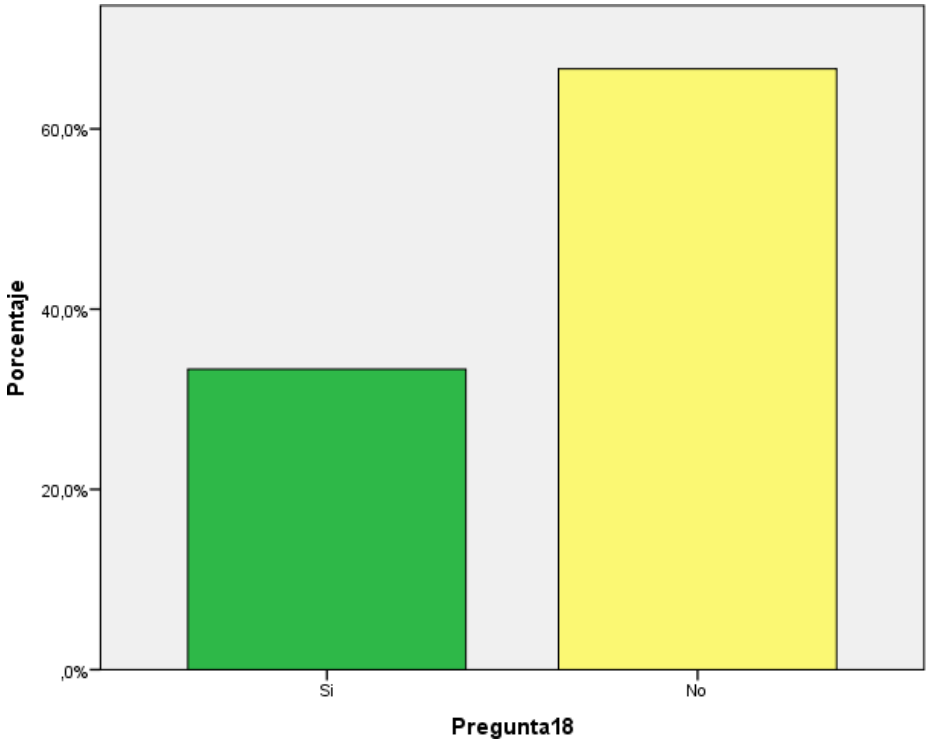
Tabla 18

Pregunta 18: ¿Existe algún documento de registro de usuarios y contraseñas de acceso a los sistemas informáticos?

Respuesta	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Si	3	33,3	33,3	33,3
No	6	66,7	66,7	100,0
Total	**9**	**100,0**	**100,0**	

Fuente: *Elaboración Propia*

Gráfico N°18



Fuente: *Elaboración Propia*

Interpretación: De la Tabla 18 y Gráfico 18 se puede determinar que de las 9 personas que trabajan en la Unidad de Soporte Informático del Hospital III Iquitos de Essalud el 33,3% considera que, si existe algún documento de registro de usuarios y contraseñas de acceso a los sistemas informáticos, y el 66,7% respondió que no.

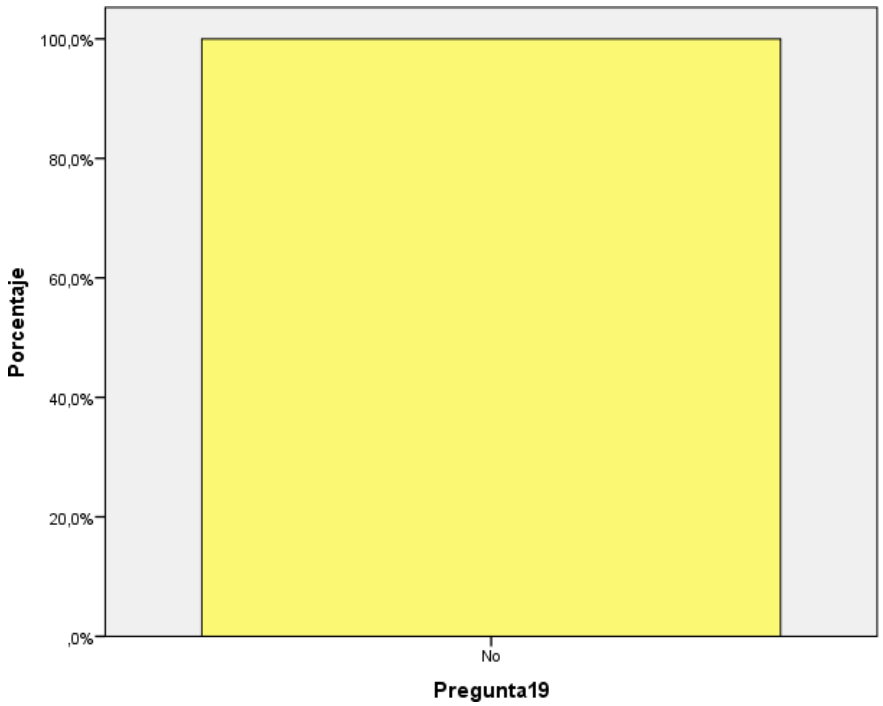
Tabla 19

Pregunta 19: ¿Existe alguna bitácora donde se registra los incidentes de accesos no autorizados a los sistemas?

Respuesta	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
No	9	100	100	100

Fuente: *Elaboración Propia*

Gráfico N°19



Fuente: *Elaboración Propia*

Interpretación: De la Tabla 19 y Gráfico 19 se puede determinar que de las 9 personas que trabajan en la Unidad de Soporte Informático del Hospital III Iquitos de Essalud el 100% considera que, no existe una bitácora donde se registra los incidentes de accesos no autorizados a los sistemas.

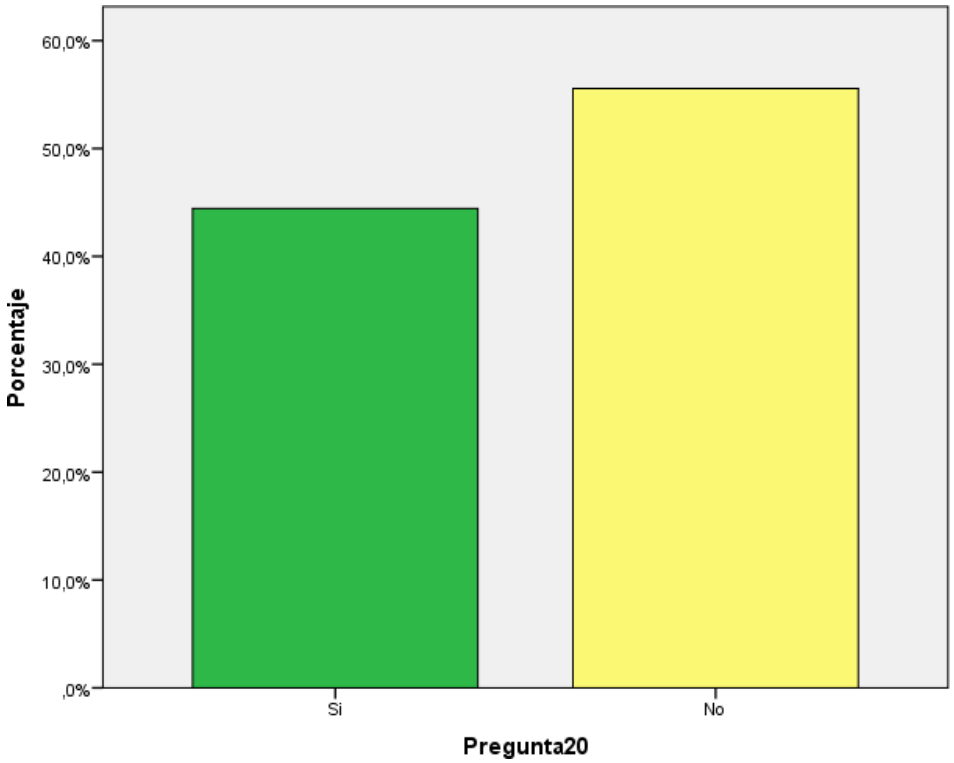
Tabla 20

Pregunta 20: ¿Dentro del área existe un responsable que asigne usuarios y contraseñas de acceso a los sistemas informáticos?

Respuesta	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Si	4	44,4	44,4	44,4
No	5	55,6	55,6	100
Total	**9**	**100**	**100**	

Fuente: *Elaboración Propia*

Gráfico N°20



Fuente: *Elaboración Propia*

Interpretación: De la Tabla 20 y Gráfico 20 se puede determinar que de las 9 personas que trabajan en la Unidad de Soporte Informático del Hospital III Iquitos de Essalud el 44,4% considera que dentro del área si existe un responsable que asigne usuarios y contraseñas de acceso a los sistemas informáticos y el 55,6% considera que no.

CAPÍTULO V

Discusiones

Para Castro (2018), en su trabajo de investigación titulada Implementación de la NTP ISO/IEC 27001:2014, para mejorar la Gestión de la Seguridad en Los Sistemas De Información De La Autoridad Portuaria Nacional, Callao – 2017, realiza un diagnóstico de las vulnerabilidades y amenazas existentes en el área de tecnologías de la información, donde se describe los riesgos existentes en los principios fundamentales a considerar en la información como es la integridad, disponibilidad y confiabilidad y al final determina que se debe aplicar la NTP que establece los criterios necesarios para asegurar y mantener los principios antes descritos, del mismo modo en nuestro trabajo de suficiencia pudimos determinar que existe un bajo nivel de aseguramiento de la información por lo tanto se debe aplicar de manera urgente un Sistema de gestión de seguridad, establecidos y normados por el estado.

Para Angulo (2017), en su trabajo de investigación titulada Plan de Seguridad Informática para mejorar la calidad en el servicio de Call Center de la Empresa TELSAT Perú SAC, antes de la elaboración del Plan, realiza un estudio donde se describe los niveles de vulnerabilidades existentes al momento de brindar los servicios de Call Center, y de acuerdo a los hallazgos sobre la Integridad, Disponibilidad y Confidencialidad de la información se logró determinar la necesidad de implementar un mecanismo para asegurar a la información que maneja y así poder atender de manera óptima, continua y de calidad a sus clientes en caso de que se suscite alguna catástrofe, del mismo modo en nuestro trabajo de investigación se logró determinar la necesidad de contar con un Plan de Seguridad que permita asegurar a la información utilizando un estándar o metodología regida por el estado.

CAPÍTULO VI

Conclusiones

- Se logró identificar las vulnerabilidades y amenazas respecto a la integridad de la información, donde se estableció que la información que se maneja en la Unidad de Soporte Informático del Hospital III Iquitos de Essalud, no existen los protocolos y mecanismos necesarios para garantizar la exactitud de la información en su procesamiento, transporte y almacenamiento.

- Se logró identificar las vulnerabilidades y amenazas respecto a la disponibilidad de la información, donde se estableció que la información que se maneja en la Unidad de Soporte Informático del Hospital III Iquitos de Essalud, no existen los criterios seguros y fiables para el acceso oportuno a los sistemas informáticos.

- Se logró identificar las vulnerabilidades y amenazas respecto a la confidencialidad de la información, donde se estableció que la información que se maneja en la Unidad de Soporte Informático del Hospital III Iquitos de Essalud, no existen los criterios y mecanismos de seguridad para garantizar la accesibilidad y control de ingreso autorizado a los sistemas informáticos de las personas que cuenten con las credenciales o autorización para el procesamiento de la información por parte del área usuaria.

Recomendaciones

- Se recomienda la implementación de la NTP-ISO/IEC 27001: 2014, para lograr la Seguridad Informática en el Hospital III Iquitos Essalud, ya que esto está establecido en el Decreto Supremo Nº004-2016-PCM, donde señala que toda entidad del estado que está inmerso en el Sistema Nacional de Informática debe implementar un sistema de gestión de seguridad aplicando la NTP-ISO/IEC 27001: 2014.

- Se recomienda la contratación de un experto en seguridad informática para que haga la evaluación más detallada de las amenazas y vulnerabilidades de la seguridad informática siguiendo la metodología MAGERIT, que es la que más se acopla a este tipo de entidades.

- Se recomienda la elaboración de un plan de contingencia que permita la recuperación inmediata de un desastre informático, y así poder mantener la continuidad de los servicios que presta la Unidad de Soporte Informático del Hospital III Iquitos de Essalud.

- Se recomienda la capacitación continua al personal de la Unidad de Soporte Informático del Hospital III Iquitos de Essalud, en temas de seguridad informática.

Referencias Bibliográficas

Aguilera Lopez, P. (2010). *Seguridad Informatica.* Editorial Editex.

Laudon , K. C., & Laudon , J. P. (2012). *SIstemas de Información Gerencial .* Mexico: Pearson Educación.

Alfaro Viana, I. A., & Vargas León, E. (2016). *Diseño del plan de seguridad informática del sistema de información misional de la procuraduría de la nación.* Bogotá: Universidad Piloto de Colombia.

Baca Urbina, G. (2016). *Introducción a la Seguridad Informatica.* Grupo Editorial Patria.

PCM. (2016). *Norma Tecnica Peruana "NTP ISO/IEC 27001: 2014 Tecnologia de la Información. Tecnicas de Seguridad. Sistema de Gestión de Seguridad de la Información. Requisitos.2aEdición ".* Lima.

SISTEMAS, S. G. (2016). *Plan de Contingencia y Seguridad de la Información .* Sicuani - Perú: Municipalidad Provincial de Chanchis.

Coqueña, E. W. (2018). *Plan de Seguridad Informática en la Municipalidad provincial de San Roman (Sistema Web).* juliaca - Perú: Universidad Andina Nestor Caceres Velasquez.

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.

Triana Acevedo, H. R. Diagnóstico y planeación del modelo de seguridad y privacidad de la información en el Hospital San José de Ortega, Tolima, ESE.

Pizarro, B., & Omar, E. (2019). Evaluación de la seguridad del Centro de Datos del Hospital de Apoyo II-2 Sullana.

Vegas Varona, I. A. (2019). Diseño de un sistema de gestión de seguridad de la información para los procesos académicos de la Universidad Nacional de Piura según la NTP ISO/IEC 27001.

Poicon Zapata, J. M. Á., & Ramírez Merino, O. (2020). Propuesta de un sistema de gestión de seguridad de la información para la Municipalidad Distrital de Marcavelica, mediante la NTP-ISO/IEC 27001: 2014.

Castro Siguas, J. J. (2018). Implementación de la NTP ISO/IEC 27001: 2014 para mejorar la gestión de la seguridad en los sistemas de información de la Autoridad Portuaria Nacional, Callao-2017.

Cueva Araujo, P. O., & Ríos Mercado, J. A. (2018). Gestión de la historia clínica y la seguridad de la información del Hospital II Cajamarca-ESSALUD bajo la NTP-ISO/IEC 27001: 2014.

ANEXOS

Anexo 01

CUESTIONARIO

TRABAJO DE SUFICIENCIA PROFESIONAL TITULADA "EVALUCIÓN DEL NIVEL DE SEGURIDAD INFORMÁTICA DEL HOSPITAL III IQUITOS DE ESSALUD LORETO - 2022"

Marque con un X la respuesta que considere, de acuerdo a su experiencia dentro del área:

NIVEL DE SEGURIDAD INFORMÁTICA INSTITUCIONAL

N°	Pregunta	Si	No
01	¿La Institución invierte presupuesto en ciberseguridad?		
02	¿El área cuenta con personal especializado en seguridad informática?		
03	¿El área propende por el correcto y seguro funcionamiento de las instalaciones de procesamiento de la información y medios de comunicación?		
04	¿El área cuenta con procedimientos estandarizados para adquisición, desarrollo y/o mantenimiento de software, que garanticen niveles de seguridad de la(s) aplicación(es)?		
05	¿Existe una Política de seguridad adoptada institucionalmente por el área?		

INTEGRIDAD DE LA INFORMACIÓN POR EL ÁREA

N°	Pregunta	Si	No
06	¿El área tiene establecidos protocolos para garantizar la seguridad en la información almacenada?		
07	¿Realiza periódicamente Backup de la Información?		
08	¿Usted considera que los datos que se ingresan por los sistemas informáticos son correctos?		
09	¿Los datos de los sistemas informáticos se almacenan en un equipo servidor?		
10	¿Los sistemas informáticos que cuentan, les permiten a los usuarios ingresar datos erróneos?		

DISPONIBILIDAD DE LA INFORMACIÓN POR EL ÁREA

N°	Pregunta	Si	No
11	¿Considera que la red de datos en la que se transmite la información de los sistemas es segura?		
12	¿Realiza periódicamente mantenimiento a sus servidores?		
13	¿El área considera tener controlados todos los incidentes de seguridad que han ocurrido en la red de datos?		
14	¿El área tiene establecido un Plan de respuesta a incidentes?		
15	¿Cuentan con un plan de prevención de riesgos informáticos?		

CONFIDENCIALIDAD DE LA INFORMACIÓN POR EL ÁREA

N°	Pregunta	Si	No
16	¿Los empleados hacen un uso adecuado de las contraseñas y datos personales?		
17	¿El manejo de usuarios y contraseñas de los sistemas de información de actualizan o cambian periódicamente?		
18	¿Existe algún documento de registro de usuarios y contraseñas de acceso a los sistemas informáticos?		
19	¿Existe alguna bitácora donde se registra los incidentes de accesos no autorizados a los sistemas?		
20	¿Dentro del área existe un responsable que asigne usuarios y contraseñas de acceso a los sistemas informáticos?		

Anexo 02

VALIDACIÓN DEL INSTRUMENTO

CUESTIONARIO

TRABAJO DE SUFICIENCIA PROFESIONAL TITULADA "EVALUCIÓN DEL NIVEL DE SEGURIDAD INFORMÁTICA DEL HOSPITAL III IQUITOS DE ESSALUD LORETO - 2022"

Nombre y Apellido del Experto: Jimmy Max Ramírez Villacorta

Título Profesional del Evaluador: Ingeniero de Sistemas e Informática

N°	Ítems a Evaluar	Cumple	No Cumple	Observaciones
1	Es Claro y Preciso	x		
2	Hace referencia al título de la investigación	x		
3	Utiliza un lenguaje sencillo y fácil de entender por el encuestado	x		
4	Recopila información reservando la identidad del encuestado	x		
5	Existe relación entre las preguntas formuladas	x		

Opinión de Aplicabilidad:

Aplicable [X] Aplicable después de corregir [ ] No aplicable [ ]

Iquitos, 14 de mayo del 2022

Ing. Jimmy Max Ramírez Villacorta
Ingeniero de Sistemas e Informática
Reg. CIP N° 145066

Anexo 03

Evidencia Fotográfica

Ilustración 07: Hospital III Iquitos Essalud

Fuente: *Elaboración Propia*

Ilustración 08: Unidad de soporte Informático

Fuente: *Elaboración Propia*