UNIVERSIDAD NACIONAL DE LA AMAZONÍA PERUANA

FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

"PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACION, APLICADO AL HOSPITAL III-IQUITOS-ESSALUD-RED ASISTENCIAL LORETO (RALO), UTILIZANDO LA METODOLOGIA MAGERIT (V.3)"

INFORME PRÁCTICO DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO DE SISTEMAS E INFORMÁTICA

Presentado por el Bachiller:

BORIS GIOVANNI CARDENAS VELA

Asesor:

ING. JOSE EDGAR GARCIA DIAZ

IQUITOS – PERÚ

2014

Informe Técnico del examen de suficiencia previa Actualización Académica, aprobado en sustentación pública, por el jurado examinador designado por el Coordinador de la Facultad de Ingeniería de Sistemas e Informática, de la Universidad Nacional de la Amazonía Peruana.

Ing. Carlos Gonzáles Aspajo
PRESIDENTE

Ing. Juan Manuel Verme Insua
PRIMER MIEMBRO

Ing. José Edgar García Díaz
ASESOR

DEDICADO al Señor **Carlos Augusto Cárdenas Vilca** y a la Señora **Laura Vela Trigoso,** por brindarme una buena educación y el apoyo incondicional, para formarme como buen profesional, y a mi hijo Stephano Fabiano que es mi motor y mi motivo para lograr mis objetivos.

AGRADEZCO a Dios por iluminarme en mi camino cada día; por haberme dado una familia tan unida; y unos padres tan maravillosos como el Sr. Carlos y la Sra. Laura.

RESUMEN

Metodología MAGERIT con sus siglas que significan, "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información", fue creado por el CSAE (Consejo Superior de Administración Electrónica); y promueve su utilización como respuesta a la percepción de que la Administración y en general toda la sociedad, depende de forma creciente de las tecnologías de la información.

Debido a la carencia de una metodología en la USI (**U**nidad de **S**oporte **I**nformático), se optó por la utilización de MAGERIT; dicha metodología se aplicó en la sede del Hospital III- Iquitos, RALO (**R**ed **A**sistencial **Lo**reto), ubicado en la Av. La Marina s/n con calle Los Rosales (MASUSA) Km. 2.5. Esta investigación se inició el 01 de Setiembre del 2012 y finalizó el 23de Febrero del 2013.

MAGERIT nos da el alcance sobre un modelo de análisis y gestión de riesgos, que nos permitió formular un buen Plan de Contingencia, ante la carencia de éste, aplicado a los activos informáticos relevantes del Hospital III - Iquitos, teniendo en cuenta que toda Institución debería estar preparada ante un desastre.

Al formular el Plan de Contingencia se identificó **265 posibles prevenciones** en relación a los 118 existentes sin Plan de Contingencia, como también se identificó **266 posibles acciones** con Plan de Contingencia en relación a los 133 existentes sin Plan de Contingencia de todos los activos informáticos relevantes.

Así mismo, se **mejoró el tiempo de respuesta** a los problemas ocurridos:

Activo	Problema / riesgo/Contingencia	Sin Plan de Contingencia	Con Plan de Contingencia
CORREO ELECRONICO	Manipulación de la configuración	**1 hora**	**30 min**
SISTEMA DE GESTION HOSPITALARIA	Errores del administrador del SGH	**45 min**	**10 min**
	Manipulación de la configuración	**1 hora**	**20 min**
APLICACIONES	Manipulación de la configuración	**45 min**	**20 min**
	Vulnerabilidades de los programas (software)	**45 min**	**30 min**
	Errores de mantenimiento / actualización de programas (software)	**1 hora 1/2**	**30 min**
EQUIPOS	Difusión de software dañino	**1 hora**	**30 min**
	Abuso de privilegios de acceso	**30 min**	**10 min**
	Manipulación de programas	**45 min**	**20 min**
COMUNICACIONES	Análisis de tráfico	**20 min**	**10 min**
ADMINISTRADOR DE SISTEMAS Y BASE DE DATOS	Indisponibilidad del personal	**1 hora**	**30 min**
OPERADOR	Indisponibilidad del personal	**1 hora**	**30 min**

Palabras claves:

- Metodología.
- MAGERIT.
- Gestión de Riesgos.
- CSAE (Consejo Superior de Administración Electrónica).
- Percepción.
- USI (Unidad de Soporte Informático).
- RALO (Red Asistencial Loreto).
- Plan de Contingencia.
- Activos relevantes.
- Prevenciones.
- Acciones.

ABSTRACT

Methodology MAGERIT with acronyms mean, "Methodology for Analysis and Risk Management Information Systems", was created by the CSAE (eGovernment Council) and promotes its use as a response to the perception that the Administration and whole society in general, depends increasingly on information technologies.

Due to the lack of a methodology in USI (Computer Support Unit), we chose to use MAGERIT, this methodology was applied to the seat of Hospital III-Iquitos, THIN (Loreto Assistance Network), located at Av the Marina s / n and Street Los Rosales (Masusa) Km 2.5. This investigation was initiated on September 01, 2012 and ended on February 23de 2013.

MAGERIT gives us the scope on a model for risk analysis and management, which allowed us to formulate a good contingency plan, in the absence of this, applied to the relevant computing assets Hospital III - Iquitos, considering that every institution should be prepared for a disaster.

In formulating the Contingency Plan identified 265 possible precautions in relation to the existing 118 without Contingency Plan, as also identified 266 possible actions Contingency Plan in relation to the existing 133 without Contingency Plan all relevant information assets.

Likewise, improved response time problems occurred:

Active	Problem / Risk / Contingency	No Contingency Plan	With Contingency Plan
E-MAIL	Manipulation of the configuration	**1 time**	**30 min**
HOSPITAL MANAGEMENT SYSTEM	Errors SGH Administrator	**45 min**	**10 min**
	Manipulation of the configuration	**1 time**	**20 min**
APPLICATIONS	Manipulation of the configuration	**45 min**	**20 min**
	Vulnerabilities of programs (software)	**45 min**	**30 min**
	Errors maintenance / updating programs (software)	**1 time 1/2**	**30 min**
EQUIPMENT	**Dissemination of malware**	**1 time**	**30 min**
	Abuse of access privileges	**30 min**	**10 min**
	Program manipulation	**45 min**	**20 min**
COMMUNICATIONS	Traffic analysis	**20 min**	**10 min**
MANAGER SYSTEMS AND DATABASE	Unavailability of staff	**1 time**	**30 min**
OPERATOR	Unavailability of staff	**1 time**	**30 min**

Keywords:

- Methodology.
- MAGERIT.
- Risk Management.
- CSAE (EGovernment Council).
- Perception.
- USI-Computer Support Unit
- RALO (Red Asistencial Loreto
- Contingency Plan
- Relevant Assets
- Preventions
- Shares.

ÍNDICE GENERAL

ÍNDICE DE TABLAS Y CUADROS

ÍNDICE DE FIGURAS

SECCIÓN I: DATOS GENERALES

1. TÍTULO.

"PLAN DE CONTINGENCIA DE SISTEMAS DE INFORMACION, APLICADO AL HOSPITAL III-IQUITOS-ESSALUD-RED ASISTENCIAL LORETO (RALO) UTILIZANDO LA METODOLOGIA MAGERIT (V.3)"

2. AREA DE DESARROLLO.

- Seguridad de Sistemas de Información.

3. GENERALIDADES DE LA INSTITUCIÓN.

3.1. Razón Social.

- Hospital III – Iquitos – Red Loreto – EsSalud.

3.2. Ubicación de la Empresa.

El Hospital III – Iquitos – Red Loreto – EsSalud, está ubicada:

- ✓ País : Perú.
- ✓ Departamento : Loreto.
- ✓ Distrito : Punchana.
- ✓ Dirección : Av. La Marina s/n con calle Los Rosales (MASUSA) Km. 2.5

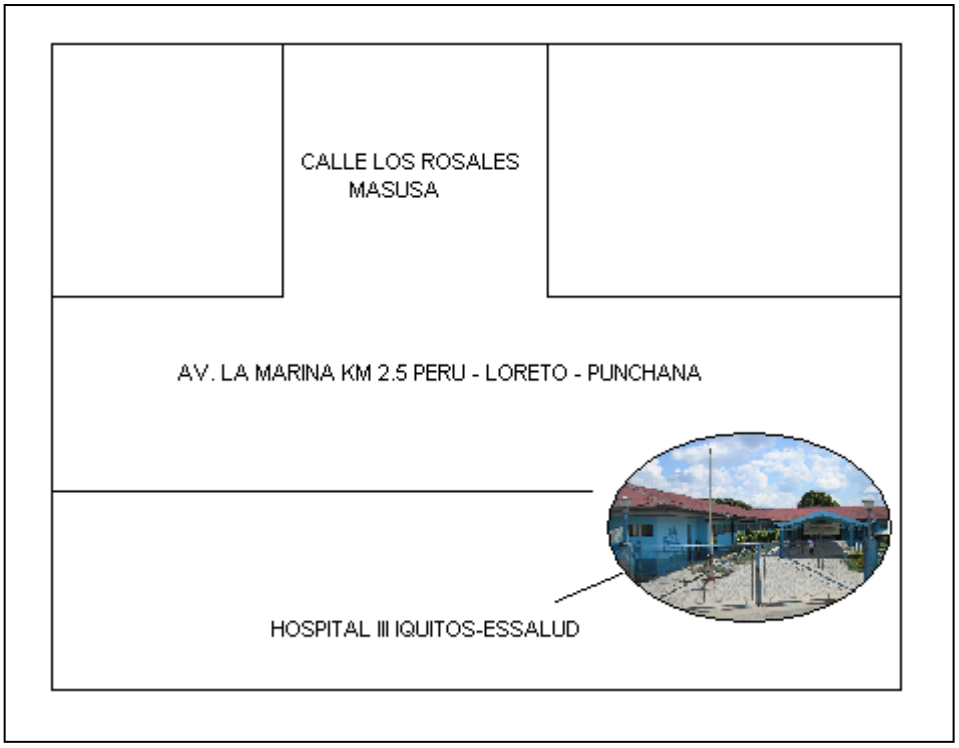


Figura 01: Hospital III-Iquitos

3.3. Organigrama Funcional

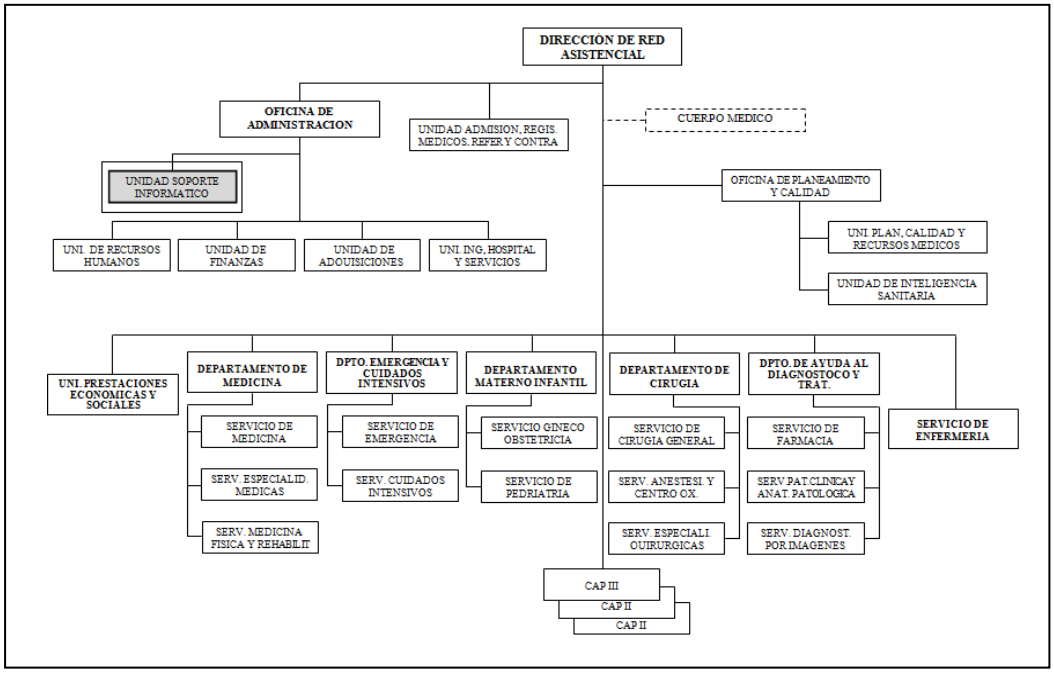


Figura 02: Organigrama Funcional

Leyenda: Área de Estudio.

3.4. Funciones Generales de la Oficina o Area.

Unidad de Soporte Informático (USI). Esta son algunas de las funciones que cumple dicha área

1. Identificar, coordinar, consolidar y sustentar las necesidades informáticas requeridas para el cumplimiento de sus funciones, a fin de que sean proveídos por las respectivas jefaturas, informando oportunamente al órgano central correspondiente a las acciones realizadas.
2. Facilitar, en coordinación con las unidades orgánicas correspondientes, la provisión y atención oportuna del soporte técnico para las áreas dentro de su entorno, informando oportunamente las acciones que permitan brindar una adecuada gestión informática a las áreas usuarias.
3. Proponer y ejecutar los planes de capacitación técnica necesarios para el personal de su área, así como para las áreas usuarias correspondientes, a fin de mejorar la gestión y operatividad de los sistemas de información implantados.
4. Garantizar el funcionamiento de los sistemas de información y/o aplicativos que están en explotación en las áreas usuarias dentro de su entorno, dotando los procedimientos necesarios de control y los procesos de copias de respaldo.
5. Establecer procedimientos de seguridad y control interno informáticos para las áreas dentro de su entorno, a fin de proteger los sistemas de información, base de datos y demás recursos informáticos involucrados.
6. Asegurar que la información que custodian referente a software, sistemas de información, bases de datos, usos de equipos de cómputo e insumos, es información reservada y exclusivamente de uso interno.
7. Mantener actualizada la documentación y los manuales técnicos necesarios para la gestión y explotación de los aplicativos y sistemas de información vigentes dentro de su ámbito, que hayan sido desarrollados con recursos propios y/o por terceros.

8. Brindar el soporte a los aplicativos para equipos informáticos, sólo preventivos.
9. Brindar soporte en software comerciales (Windows, Novell, Office y otros), e institucionales (Servicio de Gestión Hospitalaria, Vigilancia Perinatal, CITT y otros hospitalarios) a las diferentes áreas.
10. Organizar y mantener actualizado para la Red, un documento de registro descriptivo con la identificación, diagnósticos posibles y vías de solución a los problemas de hardware y software presentados durante la ejecución de los sistemas de información.
11. Mantener actualizado el inventario físico de contratos, licencias, hardware, sistemas operativos, software de oficina y otros instalados en los equipos de cómputo y de telecomunicaciones dentro de la Red.
12. Coordinar y mantener permanentemente informado al jefe inmediato sobre las actividades que desarrolla.
13. Ingresar y/o registrar en la computadora personal asignada, los datos e información necesaria para la correcta explotación de los aplicativos informáticos de su ámbito, guardando estricta confidencialidad de las claves de acceso y niveles de acceso que se le hayan autorizado.
14. Cumplir con las normas y procedimientos emitidos por la Gerencia Central de Organización e Informática.
15. Verificar la comunicación permanente entre el centro de cómputo del Hospital y la Sede Central, a través de los servicios de comunicaciones.
16. Efectuar las copias de respaldo y su restauración de la información y de software base de los servidores del centro de cómputo, así como almacenar los medios de almacenamiento, según procedimientos establecidos.
17. Brindar apoyo técnico especializado a los usuarios finales en la solución de problemas de hardware, software y de comunicaciones del Hospital.
18. Realizar la instalación de hardware y software; ejecutar la actualización respectiva de equipos de los usuarios finales. Así mismo, elaborar y presentar el informe técnico del mantenimiento de equipos realizado.
19. Mantener actualizado el inventario físico de contratos, licencias, hardware, sistemas operativos, software de oficina y otros instalados en los equipos de cómputo y de telecomunicaciones dentro de red.
20. Realizar el mantenimiento correctivo de los equipos de cómputo, de comunicaciones y del cableado estructurado, sin garantía o no cubiertos por el servicio de terceros, del Hospital. Además, de verificar e informar las necesidades de equipos informáticos y de comunicaciones del Hospital.

4. <u>BACHILLER</u>.

Boris Giovanni Cárdenas Vela. Bachiller de la Facultad de Ingeniería de Sistemas e Informática.

5. <u>ASESOR</u>.

Ing. José Edgar García Díaz. Docente de la Facultad de Ingeniería de Sistemas e Informática.

6. <u>COLABORADORES</u>.

- ✓ Técnico de Procesamiento Automático de Datos Sr. Roner Ruiz Utia.
- ✓ Jefe de Unidad de Soporte Informático (USI) Sr. Giancarlo Pinedo Picciotti**.**

7. <u>DURACIÓN ESTIMADA DE EJECUCIÓN DEL PROYECTO</u>.

5 Meses y 23 días (01 Setiembre del 2012 al 23de Febrero del 2013). ***Ver ANEXO Nº 01***

8. PRESUPUESTO ESTIMADO

Para el análisis y desarrollo del presente informe, se tendrá un presupuesto estimado de **S/.** 9,688.00 **nuevos soles**, donde se consideró los distintos materiales y requisitos que permitirán cumplir con el requerimiento solicitado, cabe mencionar que el coste total estará solventado por el ponente de dicho tema.

DESCRIPCIÓN	*CANTIDAD*	*COSTO UNITARIO*	*COSTO TOTAL*
BIENES			
Equipos de cómputo portátil			
Laptop TOSHIBA Core-i3	1	S/. 3000.00	S/. 3000.00
Impresora			
HP LaserJet 2055 dn	1	S/. 1000.00	S/. 1000.00
INSUMOS			
Licenciamiento de Software			
Microsoft Office 2010	1	S/. 200.00	S/. 200.00
Material procesamiento automático de datos			
Memoria USB KINGSTON 4 Gb	1	S/. 70.00	S/. 70.00
Módem Inalámbrico CLARO 4G	1	S/. 78.00	S/. 78.00
Material de escritorio			
Folder de Manila tamaño carta-docena	1	S/. 5.50	S/. 5.50
Papel Bond A-4 75 gr - millar	5	S/. 11.80	S/. 59.00
Faster-caja	1	S/. 3.50	S/. 3.50
Materiales de impresión			
Tóner LaserJet 2055 dn	1	S/. 300.00	S/. 300.00
Servicios			
Gasolina (veces)	5	S/. 10.00	S/. 50.00
SOFTWARE			
AUTOCAD	1	S/. 5000.00	S/. 5000.00
TOTAL			**S/.** 9,688.00

Tabla 01: Cuadro de Costos

- ✓ Los bienes son de propiedad del desarrollador del trabajo práctico.

SECCIÓN II: VISIÓN GENERAL DE LA SOLUCIÓN PROPUESTA DESARROLLO DEL TEMA

CAPITULO I: INTRODUCCION

1.1. CONTEXTO

La Unidad de Soporte Informático (USI) del Hospital II-Iquitos-Red Asistencial Loreto (RALO), se encuentra en la Av. La Marina s/n con calle Los Rosales (MASUSA) Km. 2.5, distrito de Punchana.

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 apropiados para brindar un servicio de calidad a sus asegurados, cumpliendo con los trabajos encomendados y solucionando de forma rápida los problemas suscitados.

El Hospital III-Iquitos-Red Asistencial Loreto, hoy y en día es un centro referencial de distintas especialidades, el cual acoge a los pacientes derivados de los distintos policlínicos, situados en los diferentes distritos de la Red Loreto, a la vez cuenta con las distintas áreas de Gerencia , Oficina de Planeamiento y Calidad (OPC) , Unidad de Soporte Informático (USI), Dpto.de Medicina, Dpto.de Emergencia y Cuidados Intensivos, Dpto. Materno Infantil , Dpto.de Cirugía, Dpto.de Ayuda al Diagnostico y Tto., Servicio de Enfermería – Unidad de Admisión Reg. Médicos Referencias y Contrarreferencias, entre otros.

Como toda institución, busca estar a la vanguardia con el uso de las Tecnologías de Información, para mejorar y optimizar procesos dentro de la Institución; y así permitir que los usuarios finales tengan una atención de su agrado.

1.2. PROBLEMÁTICA OBJETO DE LA APLICACIÓN

El área de seguridad de la información a nivel central de EsSalud, en la ciudad de Lima, no ha difundido una metodología necesaria a las sedes de las diferentes provincias, sobre cómo elaborar un plan de contingencia de los sistemas de información; por lo que cada jefatura de informática se vio obligado, a asumir las consecuencias de todos los niveles de impacto de riesgos y amenazas, trayendo consigo la inoperatividad de la contingencia, además de afectar con la evaluación del personal de informática, al no resolver los problemas en menor tiempo posible, por no tener en cuenta la identificación de los activos a proteger.

1.3. OBJETIVOS DEL PROYECTO.

1.3.1. Objetivo General.

- ✓ Elaboración del plan de contingencia del Hospital III-Iquitos Red Asistencial Loreto (RALO), para minimizar el impacto de los posibles riesgos.

1.3.2. Objetivos Específicos.

- ✓ Identificar la prevención de la amenaza.
- ✓ Identificar las salvaguardas o acciones después de activarse la Contingencia.
- ✓ Mejorar el tiempo de respuesta frente a las amenazas.

CAPÍTULO II: DESCRIPCIÓN DEL DISEÑO DE LA SOLUCIÓN

2.1. TÉCNICAS DE RECOLECCIÓN DE DATOS.

La técnica empleada para la recolección de datos en la institución fue:

- **Entrevista**
  Se eligió esta técnica, porque nos permitirá entablar una relación directa con el usuario final, llegando así a tocar el tema sobre la problemática actual, con la cuenta el Hospital III-Iquitos-Red Asistencial Loreto. ***VER ANEXO Nº 02***

La persona entrevistada fue:

- ✓ Técnico de Procesamiento Automático de Datos Sr. Roner Ruiz Utia.
- ✓ Jefe de Unidad de Soporte Informático (USI) Sr. Giancarlo Pinedo Picciotti.

2.2. METODOLOGÍA Y HERRAMIENTA A EMPLEAR

2.2.1. Metodología

La metodología MAGERIT se adecua al formato solicitado para la presentación de dicho informe.

MAGERIT responde a lo que se denomina, "Proceso de Gestión de los Riesgos". En otras palabras, MAGERIT implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo, para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información.

Hay varias aproximaciones al problema de analizar los riesgos soportados por los sistemas TIC: guías informales, aproximaciones metódicas y herramientas de soporte. El gran reto de todas estas aproximaciones, es la complejidad del problema al que se enfrentan; complejidad en el sentido de que hay muchos elementos que considerar y que no. Es por ello que en Magerit persigue una aproximación metódica que no deja lugar a la improvisación, ni dependa de la arbitrariedad del analista.

Magerit persigue los siguientes objetivos:
Directos:

1. Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.
2. Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC)
3. Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control

Indirectos:

4. Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

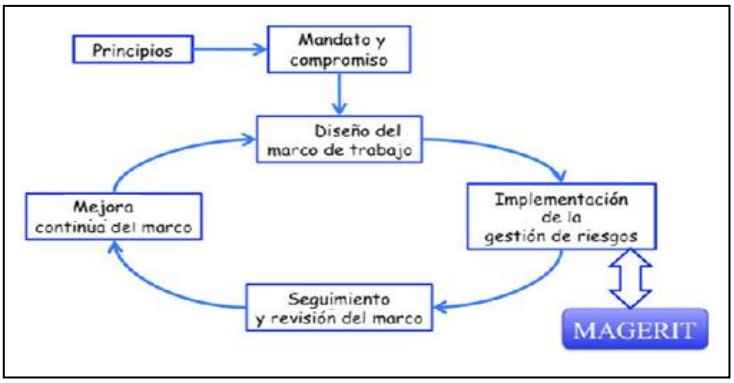


Figura 03: Metodología MAGERIT

2.2.1. Herramienta

La realización de un proyecto de análisis de riesgos supone trabajar con una cierta cantidad de activos, que rara vez baja de las decenas y que habitualmente son algunos centenares. El número de amenazas típicamente está del orden de las decenas, mientras que el número de salvaguardas está en los millares. Todo ello nos indica que hay que manejar multitud de datos y combinaciones entre ellos, lo que lleva lógicamente a buscar apoyo de herramientas automáticas.

Como requisitos generales, una herramienta de apoyo al análisis de riesgos debe:

- ✓ Permitir trabajar con un conjunto amplio de activos, amenazas y salvaguardas;
- ✓ Permitir un tratamiento flexible del conjunto de activos para acomodar un modelo cercano a la realidad de la Organización;
- ✓ No ocultar al analista el razonamiento que lleva a las conclusiones.

La herramienta soporta todas las fases del método Magerit:

- ✓ Caracterización de los activos: identificación, clasificación, dependencias y valoración
- ✓ Caracterización de las amenazas
- ✓ Evaluación de las salvaguardas

La herramienta incorpora los catálogos del "Catálogo de Elementos"(Libro II), permitiendo una homogeneidad en los resultados del análisis:

- ✓ Tipos de activos
- ✓ Dimensiones de valoración
- ✓ Criterios de valoración
- ✓ Catálogo de amenazas

2.3. DESCRIPCIÓN DEL DESARROLLO DE LA SOLUCIÓN.

El presente proyecto tiene como objetivo, la elaboración de un Plan de Contingencia, el cual está compuesta por las etapas o fases de la metodología MAGERIT *(Referencia bibliográfica pág. 87.)*, y según formato alcanzado para el desarrollo de éste informe, iniciando por un buen análisis de gestión de riesgos donde se identificarán los activos relevantes para el área, su interrelación y su valor, las amenazas a las que están expuestos los activos y las salvaguardas que existen y cuan eficaces son frente al riesgo.

Finalmente se presentará el respectivo plan de contingencia, teniendo en cuenta el análisis realizado.

A la vez se estará proponiendo un presupuesto tentativo para la compra de equipos de respaldo visto el análisis de investigación. ***VER ANEXO Nº 03***

2.4. INDICADORES DE EVALUACIÓN DE LA SOLUCIÓN

INDICADORES	ÍNDICES	HERRAMIENTA
CANTIDAD DE PREVENCIÓN DE LAS AMENAZAS.	➢ > 10 - BUENO ➢ 5 - 10 - REGULAR ➢ < 5 - DEFICIENTE	➢ ENTREVISTA CON EL JEFE DE INFORMATICA ➢ OBSERVACION DIRECTA IN SITU AL HOSPITAL ➢ INVENTARIO DE ACIVOS
CANTIDAD DE SALVAGUARDAS O ACCIONES DESPUÉS DE ACTIVARSE LA CONTINGENCIA.	➢ > 10 – BUENO ➢ 5 - 10 - REGULAR ➢ < 5 - DEFICIENTE	➢ ENTREVISTA CON EL JEFE DE MANTENIMIENTO Y DE SOPORTE INFORMÁTICO
TIEMPO DE RESPUESTA FRENTE A ALAS AMENAZAS.	➢ <= 10 MIN - EFICIENTE ➢ 10 - 30 MIN – REGULAR ➢ > 30 – DEFICIENTE	➢ APLICACIÓN DEL PLAN DE CONTINGENCIA

Tabla 02: Indicadores

Fuente: Basado en el acta de conformidad de activos y salvaguardas firmado y validado por el jefe de informática ***VER ANEXO Nº 04***

2.5. RELACIÓN DE ENTREGABLES.

Los entregables que se van a otorgar forman parte de los requerimientos establecidos.

1. Planificación del Proyecto.
2. Análisis de riesgos que incluye lo siguiente:

    - Caracterización de activos (identificación, dependencia y valoración de activos)
    - Caracterización de las amenazas (identificación y valoración de las amenazas)
    - Caracterización de las salvaguardas (identificación y valoración de las salvaguardas)
    - Caracterización del Impacto (impacto acumulado e impacto repercutido)
    - Caracterización del Riesgo (riesgo acumulado y riesgo repercutido)
    - Gestión del Riesgo (Plan de contingencia)

3. Tratamiento de los riesgos.
4. Bitácora de Incidencias del Sistema de Gestión Hospitalaria ***VER ANEXO Nº 05***
5. Bitácora de Solicitud de Nuevo Usuario al Sistema de Información ***VER ANEXO Nº 06***
6. Eliminación y/o Inhabilitación de Usuario al Sistema de Gestión Hospitalaria ***VER ANEXO Nº 07***
7. Formato de control de backup y resguardo de la información. ***VER ANEXO Nº 08***
8. Formato de entrada y salida de personas al área restringida centro de cómputo ***VER ANEXO Nº 09***

CAPÍTULO III: DESARROLLO DE LA SOLUCIÓN PROPUESTA

3.1. Planificación

3.1.1. Dominio y Límites

Se tomaron las siguientes áreas a mencionar: Gerencia - Oficina de Planeamiento y Calidad (OPC) - Unidad de Soporte Informático (USI) - Dpto.de Medicina - Dpto.de Emergencia y Cuidados Intensivos - Dpto. Materno Infantil - Dpto.de Cirugía - Dpto.de Ayuda al Diagnostico y Tto. - Servicio de Enfermería – Unidad de Admisión Reg. Médicos Referencias y Contrarreferencias – CallCenter (EsSalud en línea) – Módulos de atención – Consultorios (cons02-cons33). ***VER ANEXO Nº10***

3.1.2. Estimación de dimensiones

Las dimensiones se utilizan para valorar las consecuencias de la materialización de una amenaza.

Un activo puede estimar diferentes dimensiones:

- [D] disponibilidad: ¿qué perjuicio causaría no tenerlo o no poder utilizarlo?
- [I] integridad: ¿qué perjuicio causaría que estuviera dañado o corrupto?
- [C] confidencialidad: ¿qué daño causaría que lo conociera quien no debe?
- [A] autenticidad de los usuarios y la información: ¿qué perjuicio causaría no saber exactamente quién hace o ha hecho cada cosa?
- [T] trazabilidad del servicio y de los datos: ¿qué daño causaría no saber a quién se le presta tal servicio? ¿qué daño causaría no saber quién accede a qué datos y qué hace con ellos?

3.2. Análisis de riesgos

Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización.

3.2.1 Caracterización de los activos

3.2.1.1. Activos a proteger

Los activos se agrupan según:

Servicios internos	Correo electrónico institucional.
	Intranet.
	Sistema de Gestión Hospitalaria.
Equipamiento	Aplicaciones
	Fox
	Linux Red Hat Enterprise 5.4.
	Centos 5
	Asterisk
	Equipos.
	Servidor de aplicaciones y Base de datos.
	Servidor de correo.
	Switch Core.
	Switch Alcatel.
	Servidor de backup.
	Radio enlaces.
	Comunicaciones.
	Red inalámbrica.
	Red LAN.
	Elementos auxiliares.
	UPS- Sistema de alimentación ininterrumpida.
	Cable UTP.
	Fibra óptica.
	Transformador de aislamiento
Personal	Administrador de sistemas y Base de datos.
	Operadores.

Instalación	Hospital III-Iquitos.
	CAP-Iquitos.
	CAP-Punchana.
	CAP-San Juan.

Cuadro 01. Activos

3.2.1.2. Dependencias

Los activos esenciales son la información y los servicios prestados; pero estos activos dependen de otros activos más prosaicos como pueden ser los equipos, las comunicaciones, las instalaciones y las frecuentemente olvidadas personas que trabajan con aquellos.

Servicios internos	**Correo electrónico institucional**.
	d – Red inalámbrica.
	d – Red LAN.
	Intranet.
	d – Red inalámbrica
	d – Red LAN.
	Sistema de Gestión Hospitalaria.
	d – FOX.
	d – Red LAN
Equipamiento	Aplicaciones
	Fox
	d – Servidor de aplicaciones y bases de datos.
	d **–** Switch Core.
	d **–** Administrador de sistemas y Base de datos.
	d **–** Hospital III-Iquitos.
	d - Administrador de sistemas y Base de datos
	Centos 5
	d – Servidor de back up
	d – Administrador de sistemas y Base de datos
	d **–** Hospital III-Iquitos
	d – Administrador de sistemas y Base de datos
	Linux 4.5
	d – Servidor de back up
	d – Administrador de sistemas y Base de datos
	d **–** Hospital III-Iquitos
	d – Administrador de sistemas y Base de datos
	Equipos.
	Servidor de aplicaciones y Base de datos.
	d **–** Switch Core.
	d **–** Administrador de sistemas y Base de datos.
	d **–** Hospital III-Iquitos
	Servidor de correo.
	d **–** Switch Core.
	d **–** Switch Alcatel.
	d **–** UPS- Sistema de alimentación ininterrumpida
	d **–** Transformador de aislamiento.
	d **–** Operador.
	d **–** Administrador de sistema de Base de datos.
	d **–** Hospital III-Iquitos.
	Switch Core.
	d **–** Switch Alcatel.
	d **–** UPS- Sistema de alimentación ininterrumpida
	d **–** Transformador de aislamiento.
	d **–** Operador.
	d **–** Hospital III-Iquitos.
	d **–** UPS- Sistema de alimentación ininterrumpida
	d **–** Transformador de aislamiento
	d **–** Operador.
	d **–** Hospital III-Iquitos.
	Switch Alcatel.
	d **–** UPS- Sistema de alimentación ininterrumpida
	d **–** Operador.

	d – Hospital III-Iquitos.
	Comunicaciones.
	Red inalámbrica.
	d – Switch Core
	d – Switch Alcatel
	d – UPS- Sistema de alimentación ininterrumpida
	d – Transformador de aislamiento.
	d – Operador.
	d – Hospital III-Iquitos.
	d – UPS- Sistema de alimentación ininterrumpida
	d – Transformador de aislamiento.
	d – Operador.
	d – Hospital III-Iquitos.
	d – Operador.
	d – Hospital III-Iquitos
	d – CAP-Iquitos
	d – CAP-Punchana.
	d – CAP-San Juan.
	Red LAN.
	d – Cable UTP.
	d – Operador.

Cuadro 02. Dependencias

3.2.1.3. Valor a los activos

El valor de un activo puede ser propio o acumulado. Se dice que los activos inferiores en un esquema de dependencias, acumulan el valor de los activos que se apoyan en ellos.

Para valorar los activos se tienen en cuenta el siguiente criterio de valoración **(***Referencia bibliográfica pág. 87 Magerit-I-Método***):**

VALORACIÓN:		
8-10	Alto	Daño grave al Hospital
5-7	Medio	Daño importante al Hospital
1-4	Bajo	Daño menor al Hospital
0	Despreciable	Irrelevantes a efectos prácticos

Tabla 03. Valor a los activos

Los activos son evaluados según:

- **Servicios internos**

Activo	[D]	[I]	[C]	[A]	[T]
Correo electrónico institucional	[5]	[7]	[4]	[6]	[6]
Intranet.	[6]	[5]	[2]	[6]	[6]
Sistema de gestión hospitalaria.	[7]	[7]	[6]	[7]	[7]

Tabla 04. Servicios internos

- **Equipamiento**

Activo	[D]	[I]	[C]	[A]	[T]
Aplicaciones					
Fox	[7]	[10]	[10]		
Linux Red Hat Enterprise 5.4	[7]	[9]	[7]		
Centos 5	[7]	[9]	[7]		

Asterisk	[6]	[9]	[6]		
Equipos					
Servidor de aplicaciones y Base de datos	[10]	[10]	[10]	[10]	[10]
Servidor de correo	[5]			[7]	
Switch Core	[10]				
Switch Alcatel			[10]	[10]	
Servidor de backup	[10]	[10]	[10]	[10]	[10]
Radioenlace	[5]				
Comunicaciones					
Red inalámbrica					
Red LAN	[3]				
Elementos Auxiliares					
UPS- Sistema de alimentación ininterrumpida	[5]				
Cable UTP	[5]				
Fibra óptica	[7]				

Tabla 05. Equipamiento

- **Personal**

Activo	[D]	[I]	[C]	[A]	[T]
Administrador de sistemas y Base de datos	[5]				
Operadores	[3]				

Tabla 06. Personal

3.2.2. Caracterización de las amenazas

3.2.2.1 Identifica las amenazas

Como parte de la identificación de las amenazas, estos deben categorizarse en función a las acciones de prevención o cuya ocurrencia no puede predecirse con anticipación. Así tenemos que los eventos pueden ser:

Eventos Controlables (C), si al identificarlos podemos tomar acciones que eviten su ocurrencia o minimicen el impacto en el servicio brindado. ***VER TABLA Nº 107***

Eventos No Controlables (NC), cuando su ocurrencia es impredecible y únicamente podemos tomar acciones que permitan minimizar el impacto en el servicio. ***VER TABLA Nº 108***

Algunas de las amenazas presentadas a continuación son las descritas en MAGERIT, identificadas en la USI. Los activos se asocian a las amenazas que, se cree, pueden sufrir (*Referencia bibliográfica pág. 87 Magerit-II- Catálogo de Elementos*).

Desastres Naturales	DN.1 Fuego
	DN.2 Daños por agua
	DN.3 Desastres naturales (terremotos, inundaciones, etc.)
De origen industrial	OI.1 Fuego
	OI.2 Daños por agua
	OI.3 Corte del suministro eléctrico
	OI.4 Condiciones inadecuadas de temperatura y/o humedad
	OI.5 Fallo de servicios de comunicaciones
Errores y fallos no intencionados	EFNI.1 Errores de los usuarios
	EFNI.2 Errores del administrador
	EFNI.3 Errores de monitorización
	EFNI.4 Errores de configuración
	EFNI.5 Difusión de software dañino
	EFNI.6 Errores de secuencia
	EFNI.7 Alteración accidental de la información
	EFNI.8 Introducción de falsa información
	EFNI.9 Degradación de la información
	EFNI.10 Destrucción de la información

Errores y fallos no intencionados	EFNI.11 Divulgación de la información
	EFNI.12Vulnerabilidades de los programas (software)
	EFNI.13 Errores de mantenimiento/actualización de programas (software)
	EFNI.14 Errores de mantenimiento/actualización de equipos (hardware)
	EFNI.15 Caída del sistema por agotamiento de recursos UPS
	EFNI.16 Indisponibilidad del personal
Ataque deliberados	AD.1 Manipulación de la configuración
	AD.2 Suplantación de la identidad del usuario
	AD.3 Abuso de privilegios de acceso
	AD.4 Difusión de software dañino
	AD.5 Alteración de la secuencia
	AD.6 Acceso no autorizado
	AD.7 Análisis de tráfico
	AD.8 Intercepción de información (escucha)
	AD.9 Modificación de información
	AD.10 Introducción de falsa información
	AD.11 Corrupción de la información
	AD.12 Destrucción de la información
	AD.13 Divulgación de la información
	AD.14 Manipulación de programas
	AD.15 Denegación de servicio
	AD.16 Robo de equipos
	EFNI.7 Alteración de la información

Cuadro 03. Amenazas

3.2.2.2 Valoración de las amenazas

Cuando un activo es víctima de una amenaza, no se ve afectado en todas sus dimensiones, ni en la misma cuantía.

Una vez determinado que una amenaza puede perjudicar a un activo, hay que estimar cuán vulnerable es el activo.

Para valorar las amenazas se tienen en cuenta el siguiente criterio de valoración *(Referencia bibliográfica pág. 87 Magerit-III-Guía de Técnicas)*

Probabilidad de ocurrencia	Descripción
4%	Ocasional (Sucede alguna vez)
3%	Probable (Incidentes aislados)
2%	Frecuente (Incidentes repetidos)
1%	Remoto (Improbable que suceda)

Tabla 07. Probabilidad de ocurrencia

A continuación se muestra el resumen de valoración de las amenazas por activos:

- **Servicios internos**

Amenaza	Probabilidad
EFNI.1 Errores de los usuarios	2%
EFNI.2 Errores del administrador	2%
EFNI.3 Errores de monitorización	2%
EFNI.4 Errores de configuración	2%
EFNI.6 Errores de secuencia	2%
EFNI.15 Caída del sistema por agotamiento de recursos UPS	3%
AD.1 Manipulación de la configuración	3%
AD.2 Suplantación de la identidad del usuario	3%
AD.3 Abuso de privilegios de acceso	3%
AD.5 Alteración de secuencia	2%
AD.6 Acceso no autorizado	3%
AD.15 Denegación de servicio	3%

Tabla 08. Valoración de amenazas - Correo electrónico

Amenaza	*Probabilidad*
EFNI.1 Errores de los usuarios	1%
EFNI.2 Errores del administrador	2%
EFNI.3 Errores de monitorización	1%
EFNI.4 Errores de configuración	1%
EFNI.6 Errores de secuencia	1%
EFNI.15 Caída del sistema por agotamiento de recursos UPS	3%
AD.1 Manipulación de la configuración	1%
AD.2 Suplantación de la identidad del usuario	1%
AD.3 Abuso de privilegios de acceso	3%
AD.5 Alteración de secuencia	1%
AD.6 Acceso no autorizado	1%
AD.15 Denegación de servicio	1%

Tabla 09. Valoración de amenazas – Intranet

Amenaza	Probabilidad
EFNI.1 Errores de los usuarios	3%
EFNI.2 Errores del administrador	3%
EFNI.3 Errores de monitorización	2%
EFNI.4 Errores de configuración	3%
EFNI.6 Errores de secuencia	2%
EFNI.15 Caída del sistema por agotamiento de recursos UPS	3%
AD.1 Manipulación de la configuración	3%
AD.2 Suplantación de la identidad del usuario	3%
AD.3 Abuso de privilegios de acceso	3%
AD.5 Alteración de secuencia	2%
AD.6 Acceso no autorizado	3%
AD.15 Denegación de servicio	3%

Tabla 10. Valoración de amenazas – Sistema de Gestión Hospitalaria

- **Equipamiento**

Amenaza	Probabilidad
EFNI.1 Errores de los usuarios	2%
EFNI.2 Errores del administrador	2%
EFNI.3 Errores de monitorización	2%
EFNI.4 Errores de configuración	2%
EFNI.6 Errores de secuencia	2%
EFNI.15 Caída del sistema por agotamiento de recursos UPS	3%
AD.1 Manipulación de la configuración	3%
AD.2 Suplantación de la identidad del usuario	3%
AD.3 Abuso de privilegios de acceso	3%
AD.5 Alteración de secuencia	2%
AD.6 Acceso no autorizado	3%
AD.15 Denegación de servicio	3%
EFNI.7 Alteración de la información	4%
AD.10 Introducción de falsa información	4%
AD.12 Destrucción de la información	4%
AD.13 Divulgación de información	4%
EFNI.12 Vulnerabilidades de los programas (software)	4%
EFNI.13 Errores de mantenimiento / actualización de programas (software)	4%

Tabla 11. Valoración de amenazas – Aplicaciones

Amenaza	Probabilidad
DN.1 Fuego	4%
DN.2 Daños por agua	4%
DN.3 Desastres naturales	4%
OI.3 Corte del suministro eléctrico	3%
OI.4 Condiciones inadecuadas de temperatura o humedad	3%
EFNI.1 Errores de los usuarios	2%
EFNI.2 Errores del administrador	2%
EFNI.3 Errores de monitorización	2%
EFNI.4 Errores de configuración	2%
EFNI.5 Difusión de software dañino	3%
EFNI.6 Errores de secuencia	2%
EFNI.12 Vulnerabilidades de los programas (software)	4%
EFNI.13 Errores de mantenimiento / actualización de programas (software)	4%
EFNI.14 Errores de mantenimiento / actualización de equipos (hardware)	4%
EFNI.15 Caída del sistema por agotamiento de recursos UPS	3%
AD.16 Robo de equipos	4%
AD.1 Manipulación de la configuración	3%
AD.2 Suplantación de la identidad del usuario	3%
AD.3 Abuso de privilegios de acceso	3%
AD.5 Alteración de secuencia	2%
AD.6 Acceso no autorizado	3%
AD.8 Interceptación de información (escucha)	3%
AD.14 Manipulación de programas	3%
AD.15 Denegación de servicio	3%

Tabla 12. Valoración de amenazas – Equipos

Amenaza	Probabilidad
DN.1 Fuego	4%
DN.2 Daños por agua	4%
DN.3 Desastres naturales	4%
OI.3 Corte del suministro eléctrico	3%
OI.4 Condiciones inadecuadas de temperatura o humedad	3%
EFNI.17 Fallo de servicios de comunicaciones	3%
EFNI.2 Errores del administrador	2%
EFNI.4 Errores de configuración	2%
EFNI.6 Errores de secuencia	2%
EFNI.15 Caída del sistema por agotamiento de recursos UPS	3%
AD.1 Manipulación de la configuración	3%
AD.2 Suplantación de la identidad del usuario	3%
AD.3 Abuso de privilegios de acceso	3%
AD.5 Alteración de secuencia	2%
AD.6 Acceso no autorizado	3%
AD.8 Interceptación de información (escucha)	3%
AD.15 Denegación de servicio	3%
AD.16 Robo de equipos	4%

Tabla 13. Valoración de amenazas – Comunicaciones

Amenaza	Probabilidad
DN.1 Fuego	4%
DN.2 Daños por agua	4%
DN.3 Desastres naturales	4%
OI.3 Corte del suministro eléctrico	3%
OI.4 Condiciones inadecuadas de temperatura o humedad	3%
AD.16 Robo de equipos	4%

Tabla 14. Valoración de amenazas – Elementos auxiliares

- **Personal**

Amenaza	Probabilidad
AD.13 Divulgación de información	3%
EFNI.16 Indisponibilidad del personal	1%

Tabla 15. Valoración de amenazas – Administrador de sistemas y Base de datos

Amenaza	Probabilidad
AD.13 Divulgación de información	3%
EFNI.16 Indisponibilidad del personal	1%

Tabla 16. Valoración de amenazas – Operador

- **Instalación**

Amenaza	Probabilidad
DN.1 Fuego	4%
DN.2 Daños por agua	4%
DN.3 Desastres naturales	4%
AD.6 Acceso no autorizado	3%

Tabla 17. Valoración de amenazas – Hospital III-Iquitos

3.2.3. Caracterización de las salvaguardas

3.2.3.1 Identifica las salvaguardas

Se definen las salvaguardas o contra medidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo. Hay amenazas que se conjuran simplemente organizándose adecuadamente, otras requieren elementos técnicos; programas o equipos, (*Referencia bibliográfica pág. 87 Magerit-II-Catálogo).*

Las salvaguardas se clasifican según:

Protecciones generales	Identificación y autenticación.
	Mecanismo de autenticación.
	Gestión de incidencias (TIC) post implementación.
	Registro y auditoría post implementación.
Protección de los servicios	Aseguramiento de la disponibilidad de los sistemas.
	Aceptación de los usuarios (funcionamiento)
	Aplicación de perfiles de seguridad (SGH)
	Definición del proceso
	Registro de toda actualización de servicios
	Protección del correo electrónico
	Identificación de los usuarios
	Acuerdo de seguridad post implementación.
Protección de la información	Inventario de activos de información post implementación
	Aseguramiento de la disponibilidad
	Aseguramiento de la integridad de datos (SGH-CORREO)
Protección de las aplicaciones informáticas (SW)	Normativa sobre el uso correcto de las aplicaciones post implementación.
	Procedimientos de uso de las aplicaciones
	Inventario de aplicaciones
	Copias de seguridad (backup) (SW)
	Adquisición de aplicaciones SW
	Aplicación de perfiles de seguridad (SW)
	Cambios (actualizaciones y mantenimiento) ligados a nivel central
Protección de los equipos informáticos	Normativa sobre el uso correcto de los equipos
	Procedimientos de uso del equipamiento
	Inventario de equipos

	Aseguramiento de la disponibilidad
	Adquisición de HW ligado a nivel central
	Aplicación de perfiles de seguridad (HW) post implementación
	Instalación
	Operación
	Cambios (actualizaciones y mantenimiento)
	Protección de los cortafuegos (firewall) en Sistema Operativo
Protección de las comunicaciones	Normativa sobre el uso correcto del internet
	Procedimientos de uso del internet
	Inventario de equipos de comunicación
	Aseguramiento de la disponibilidad
	Adquisición o contratación (sujeto a nivel central)
	Operatividad
	Cambios (sujeto a nivel central)
Protección de las instalaciones del Data Center	Cumplimiento de las normas
	Procedimientos de seguridad
	Diseño de las instalaciones
	Control de los accesos físicos
	Protección del perímetro
	Vigilancia (cámaras IP)
	Protección frente a desastres
Gestión del Personal	Política de gestión de personal (en materia de seguridad) post implementación.
	Relación de personal autorizado
	Ubicación de personal interno (Data Center)
	Contratación de personal capacitado
	Formación y concienciación post implementación

Cuadro 04. Salvaguardas

3.2.3.2 Valoración de las salvaguardas

Para evaluar las salvaguardas se utiliza como parámetros los niveles de madurez y fase (*Referencia bibliográfica pág. 87 Magerit-II-Catálogo)*

Nivel de madurez

- ✓ 0 – inexistente (post implementación)
- ✓ 1 - inicial / ad hoc
- ✓ 2 - reproducible, pero intuitivo
- ✓ 3 - proceso definido (actualidad)
- ✓ 4 - gestionado y medible
- ✓ 5 – optimizado

Fases

- ✓ [f1] situación actual
- ✓ [f2] situación objetivo

A continuación se muestra la valoración de las salvaguardas:

Salvaguarda	[f1]	[f2]
Aseguramiento de la disponibilidad de los sistemas	3	4
Aceptación de los usuarios (funcionamiento)	3	4
Aplicación de perfiles de seguridad (SGH)	3	4
Definición del proceso	3	4
Registro de toda actualización de servicios	4	4
Protección del correo electrónico	4	4
Identificación de los usuarios	4	4
Acuerdo de seguridad post implementación	0	4

Tabla 18. Protecciones generales

Salvaguarda	[f1]	[f2]
Inventario de activos de información post implementación	3	4
Aseguramiento de la disponibilidad	3	4
Aseguramiento de la integridad de datos (SGH-CORREO)	3	4

Tabla 19. Protección de los servicios

Salvaguarda	[f1]	[f2]
Identificación y autenticación	3	4
Mecanismo de autenticación	4	4
Gestión de incidencias (TIC)post implementación	0	4
Registro y auditoría post implementación	0	4

Tabla 20. Protección de la información

Salvaguarda	[f1]	[f2]
Normativa sobre el uso correcto de las aplicaciones post implementación	0	4
Procedimientos de uso de las aplicaciones	3	4
Inventario de aplicaciones	3	4
Copias de seguridad (backup) (SW)	3	4
Adquisición de aplicaciones SW	3	4
Aplicación de perfiles de seguridad (SW)	3	4
Cambios (actualizaciones y mantenimiento)ligados a nivel central	5	5

Tabla 21. Protección de las aplicaciones informáticas (SW)

Salvaguarda	[f1]	[f2]
Normativa sobre el uso correcto de los equipos	3	4
Procedimientos de uso del equipamiento	3	4
Inventario de equipos	4	4
Aseguramiento de la disponibilidad	3	4
Adquisición de HW ligados a nivel central	5	5
Aplicación de perfiles de seguridad (HW) post implementación	0	4
Instalación	4	4
Operación	4	4
Cambios (actualizaciones y mantenimiento)	4	4
Protección de los cortafuegos (firewall) en Sistema Operativo	4	4

Tabla 22. Protección de los equipos informáticos

Salvaguarda	[f1]	[f2]
Normativa sobre el uso correcto del internet	3	4
Procedimientos de uso del internet	3	4
Inventario de servicios de comunicación	3	3
Aseguramiento de la disponibilidad	3	3
Adquisición o contratación (sujeto a nivel central)	5	5
Operatividad	4	4
Cambios (sujeto a nivel central)	5	5

Tabla 23. Protección de las comunicaciones

Salvaguarda	[f1]	[f2]
Cumplimiento de las normas	3	4
Procedimientos de seguridad	4	4
Diseño de las instalaciones	3	4
Control de los accesos físicos	3	4
Protección del perímetro	4	4
Vigilancia (cámaras IP)	0	4
Protección frente a desastres	3	4

Tabla 24. Protección de las instalaciones del Data Center

Salvaguarda	[f1]	[f2]
Política de gestión de personal (en materia de seguridad)post implementación	0	4
Relación de personal autorizado	3	4
Ubicación de personal interno (Data Center)	3	4
Contratación de personal capacitado	3	4
Formación y concienciación post implementación	4	4

Tabla 25. . Gestión del Personal

3.2.4. Caracterización del impacto

- Impacto acumulado

El impacto acumulado es el calculado sobre un activo teniendo en cuenta:

- ✓ El impacto acumulado se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo el resultado final, el valor del activo por el impacto de la amenaza. *(Referencia bibliográfica pág.87 Magerit-III-Guía de Técnicas).*

VALORACIÓN:		
8-10	Alto	Daño grave al Hospital
5-7	Medio	Daño importante al Hospital
1-4	Bajo	Daño menor al Hospital
0	Despreciable	Irrelevantes a efectos prácticos

Referencia (Tabla 3-Valor a los activos)

Nivel	Descripción	Impacto
Poco Impacto	Pérdida de Información y/o equipamiento	1
Bajo Impacto	Pérdida de información de poca importancia	2
Alto Impacto	Retraso o interrupción del sistema	3
Gran Impacto	Información crítica, daño serio, patrimonial	4

Tabla 26. Nivel de Impacto

Dimensiones:

[D] disponibilidad
[I] integridad de los datos
[C] confidencialidad de los datos
[A] autenticidad de los usuarios y de la información
[T] trazabilidad del servicio y de los datos

a) [D] disponibilidad (dimensión)

- **Servicios Internos**

Activo	Amenazas	Valor del Activo	Impacto	Impacto Acumulado
CORREO ELECTRONICO	EFNI.1 Errores de los usuarios	[4]	[2]	[8]
	EFNI.2 Errores del administrador	[4]	[2]	[8]
	EFNI.3 Errores de monitorización	[4]		[4]
	EFNI.4 Errores de configuración	[4]	[2]	[8]
	EFNI.6 Errores de secuencia	[4]	[2]	[8]
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[4]	[3]	[12]

CORREO ELECTRONICO	AD.1 Manipulación de la configuración	[4]	[3]	[12]
	AD.2 Suplantación de la identidad del usuario	[4]	[3]	[12]
	AD.3 Abuso de privilegios de acceso	[4]	[2]	[8]
	AD.5 Alteración de secuencia	[4]	[3]	[12]
	AD.6 Acceso no autorizado	[4]	[3]	[12]
	AD.15 Denegación de servicio	[4]	[2]	[8]
SISTEMA DE GESTION HOSPITALARIA	AD.15 Denegación de servicio	[5]	[3]	[15]
	EFNI.1 Errores de los usuarios	[5]	[3]	[15]
	EFNI.2 Errores del administrador	[5]	[3]	[15]
	EFNI.3 Errores de monitorización	[5]		[5]
	EFNI.4 Errores de configuración	[5]	[2]	[10]
	EFNI.6 Errores de secuencia	[5]	[3]	[15]
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[5]	[3]	[15]
	AD.1 Manipulación de la configuración	[5]	[3]	[15]
	AD.2 Suplantación de la identidad del usuario	[5]	[3]	[15]
	AD.3 Abuso de privilegios de acceso	[5]	[2]	[10]
	AD.5 Alteración de secuencia	[5]	[3]	[15]
	AD.6 Acceso no autorizado	[5]	[3]	[15]
	AD.15 Denegación de servicio	[5]	[2]	[10]

Tabla 27. Impacto acumulado: Disponibilidad - Servicios internos (activo)

- **Equipamiento**

Activos	Amenazas	Valor del Activo	Impacto	Impacto Acumulado
APLICACIONES (Fox, Linux R.H 5.4,Cenos 5, Asterisk)	EFNI.1 Errores de los usuarios	[6]	[2]	[12]
	EFNI.2 Errores del administrador	[6]	[2]	[12]
	EFNI.3 Errores de monitorización	[6]		[6]
	EFNI.4 Errores de configuración	[6]	[2]	[12]
	EFNI.6 Errores de secuencia	[6]	[2]	[12]
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[6]	[3]	[18]
APLICACIONES (Fox, Linux R.H 5.4,Cenos 5, Asterisk)	AD.1 Manipulación de la configuración	[6]	[3]	[18]
	AD.2 Suplantación de la identidad del usuario	[6]	[3]	[18]
	AD.3 Abuso de privilegios de acceso	[6]	[2]	[12]
	AD.5 Alteración de secuencia	[6]	[3]	[18]
	AD.6 Acceso no autorizado	[6]	[3]	[18]
	AD.15 Denegación de servicio	[6]	[2]	[12]
	AD.19 Alteración de la información	[6]	[4]	[24]
	AD.10 Introducción de falsa información	[6]	[4]	[24]
	AD.12 Destrucción de la información	[6]	[4]	[24]
	AD.13 Divulgación de información	[6]	[4]	[24]
	EFNI.12 Vulnerabilidades de los programas (software)	[6]	[4]	[24]
	EFNI.13 Errores de mantenimiento / actualización de programas (software)	[6]	[3]	[18]
EQUIPOS (Servidor de aplicaciones y Base de datos, Servidor de Correo, Switch Core, Switch Alcatel, Servidor de Backup, Radio enlace)	DN.1 Fuego	[10]	[4]	[40]
	DN.2 Daños por agua	[10]	[4]	[40]
	DN.3 Desastres naturales	[10]	[4]	[40]
	OI.3 Corte del suministro eléctrico	[10]	[3]	[30]
	OI.4 Condiciones inadecuadas de temperatura o humedad	[10]	[4]	[40]
	EFNI.1 Errores de los usuarios	[10]	[3]	[30]
	EFNI.2 Errores del administrador	[10]	[3]	[30]
	EFNI.3 Errores de monitorización	[10]		[10]
	EFNI.4 Errores de configuración	[10]	[3]	[30]
	EFNI.5 Difusión de software dañino	[10]	[3]	[30]
	EFNI.6 Errores de secuencia	[10]	[3]	[30]
	EFNI.12 Vulnerabilidades de los programas (software)	[10]	[4]	[40]
	EFNI.13 Errores de mantenimiento / actualización de programas (software)	[10]	[3]	[30]

	EFNI.14 Errores de mantenimiento / actualización de equipos (hardware)	[10]	[4]	[40]
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[10]	[3]	[30]
	AD.16 Robo de equipos	[10]	[4]	[40]
	AD.1 Manipulación de la configuración	[10]	[3]	[30]
	AD.2 Suplantación de la identidad del usuario	[10]	[4]	[40]
	AD.3 Abuso de privilegios de acceso	[10]	[3]	[30]
	AD.5 Alteración de secuencia	[10]	[3]	[30]
	AD.6 Acceso no autorizado	[10]	[4]	[40]
	AD.8 Interceptación de información (escucha)	[10]	[4]	[40]
	AD.14 Manipulación de programas	[10]	[4]	[40]
	AD.15 Denegación de servicio	[10]	[3]	[30]
COMUNICACIÓN (Red inalámbrica, Red LAN)	DN.1 Fuego	[10]	[4]	[40]
	DN.2 Daños por agua	[10]	[4]	[40]
	DN.3 Desastres naturales	[10]	[4]	[40]
	OI.3 Corte del suministro eléctrico	[10]	[3]	[30]
	OI.4 Condiciones inadecuadas de temperatura o humedad	[10]	[4]	[40]
	EFNI.17 Fallo de servicios de comunicaciones	[10]	[4]	[40]
	EFNI.2 Errores del administrador	[10]	[3]	[30]
	EFNI.4 Errores de configuración	[10]	[3]	[30]
	EFNI.6 Errores de secuencia	[10]	[3]	[30]
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[10]	[3]	[30]
	AD.1 Manipulación de la configuración	[10]	[3]	[30]
	AD.2 Suplantación de la identidad del usuario	[10]	[4]	[40]
	AD.3 Abuso de privilegios de acceso	[10]	[3]	[30]
	AD.5 Alteración de secuencia	[10]	[3]	[30]
	AD.6 Acceso no autorizado	[10]	[4]	[40]
	AD.7 Análisis de tráfico	[10]	[2]	[20]
	AD.8 Interceptación de información (escucha)	[10]	[4]	[40]
	AD.16 Robo de equipos	[10]	[4]	[40]
ELEMENTOS AUXILIARES UPS, Cable UTP, Fibra óptica, Transformador de aislamiento)	DN.1 Fuego	[7]	[4]	[28]
	DN.2 Daños por agua	[7]	[4]	[28]
	DN.3 Desastres naturales	[7]	[4]	[28]
	OI.3 Corte del suministro eléctrico	[7]	[3]	[21]
	OI.4 Condiciones inadecuadas de temperatura o humedad	[7]	[4]	[28]
	AD.16 Robo de equipos	[7]	[4]	[28]

Tabla 28. Impacto acumulado: Disponibilidad – Equipamiento (activo)

- **Personal**

Activo	Amenazas	Valor del Activo	Impacto	Impacto Acumulado
ADMINISTRADOR DE SISTEMAS Y BASE DE DATOS	AD.13 Divulgación de información	[7]	[4]	[28]
	EFNI.16 Indisponibilidad del personal	[7]	[3]	[21]
OPERADOR	AD.13 Divulgación de información	[7]	[4]	[28]
	EFNI.16 Indisponibilidad del personal	[7]	[3]	[21]

Tabla 29. Impacto acumulado: Disponibilidad – Personal (activo)

- **Instalación**

Activo	Amenazas	Valor del Activo	Impacto	Impacto Acumulado
HOSPITAL III-IQUITOS	DN.1 Fuego	[10]	[4]	[40]
	DN.2 Daños por agua	[10]	[4]	[40]
	DN.3 Desastres naturales	[10]	[4]	[40]
	AD.6 Acceso no autorizado	[10]	[4]	[40]

Tabla 30. Impacto acumulado: Disponibilidad – Instalación (activo)

b) [I] integridad (dimensión)

- **Servicios Internos**

Activo	Amenazas	Valor del Activo	Impacto	Impacto Acumulado
CORREO ELECTRONICO	EFNI.1 Errores de los usuarios	[4]	[2]	[8]
	EFNI.2 Errores del administrador	[4]	[2]	[8]
	EFNI.3 Errores de monitorización	[4]		[4]
	EFNI.4 Errores de configuración	[4]	[2]	[8]
	EFNI.6 Errores de secuencia	[4]	[2]	[8]
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[4]	[3]	[12]
	AD.1 Manipulación de la configuración	[4]	[3]	[12]
	AD.2 Suplantación de la identidad del usuario	[4]	[3]	[12]
	AD.3 Abuso de privilegios de acceso	[4]	[2]	[8]
	AD.5 Alteración de secuencia	[4]	[3]	[12]
	AD.6 Acceso no autorizado	[4]	[3]	[12]
	AD.15 Denegación de servicio	[4]	[2]	[8]
SISTEMA DE GESTION HOSPITALARIA	EFNI.1 Errores de los usuarios	[5]	[3]	[15]
	EFNI.2 Errores del administrador	[5]	[3]	[15]
	EFNI.3 Errores de monitorización	[5]	[3]	[15]
	EFNI.4 Errores de configuración	[5]		[5]
	EFNI.6 Errores de secuencia	[5]	[2]	[10]
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[5]	[3]	[15]
	AD.1 Manipulación de la configuración	[5]	[3]	[15]
	AD.2 Suplantación de la identidad del usuario	[5]	[3]	[15]
	AD.3 Abuso de privilegios de acceso	[5]	[3]	[15]
	AD.5 Alteración de secuencia	[5]	[2]	[10]
	AD.6 Acceso no autorizado	[5]	[3]	[15]
	AD.15 Denegación de servicio	[5]	[3]	[15]

Tabla 31. Impacto acumulado: Integridad - Servicios internos (activo)

- **Equipamiento**

Activos	Amenazas	Valor del Activo	Impacto	Impacto Acumulado
APLICACIONES (Fox, Linux R.H 5.4,Cenos 5, Asterisk)	EFNI.1 Errores de los usuarios	[6]	[2]	[12]
	EFNI.2 Errores del administrador	[6]	[2]	[12]
	EFNI.3 Errores de monitorización	[6]		[6]
	EFNI.4 Errores de configuración	[6]	[2]	[12]
	EFNI.6 Errores de secuencia	[6]	[2]	[12]
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[6]	[3]	[18]
	AD.1 Manipulación de la configuración	[6]	[3]	[18]
	AD.2 Suplantación de la identidad del usuario	[6]	[3]	[18]
	AD.3 Abuso de privilegios de acceso	[6]	[2]	[12]
	AD.5 Alteración de secuencia	[6]	[3]	[18]
	AD.6 Acceso no autorizado	[6]	[3]	[18]
	AD.15 Denegación de servicio	[6]	[2]	[12]
	AD.19 Alteración de la información	[6]	[4]	[24]
	AD.10 Introducción de falsa información	[6]	[4]	[24]
	AD.12 Destrucción de la información	[6]	[4]	[24]
	AD.13 Divulgación de información	[6]	[4]	[24]
	EFNI.12 Vulnerabilidades de los programas (software)	[6]	[4]	[24]
	EFNI.13 Errores de mantenimiento / actualización de programas (software)	[6]	[3]	[18]
EQUIPOS (Servidor de aplicaciones y Base de datos, Servidor de Correo, Switch Core, Switch Alcatel, Servidor de Backup, Radio enlace)	DN.1 Fuego	[10]	[4]	[40]
	DN.2 Daños por agua	[10]	[4]	[40]
	DN.3 Desastres naturales	[10]	[4]	[40]
	OI.3 Corte del suministro eléctrico	[10]	[3]	[30]
	OI.4 Condiciones inadecuadas de temperatura o humedad	[10]	[4]	[40]
	EFNI.1 Errores de los usuarios	[10]	[3]	[30]
	EFNI.2 Errores del administrador	[10]	[3]	[30]
	EFNI.3 Errores de monitorización	[10]		[10]
	EFNI.4 Errores de configuración	[10]	[3]	[30]
	EFNI.5 Difusión de software dañino	[10]	[3]	[30]
	EFNI.6 Errores de secuencia	[10]	[3]	[30]

	EFNI.12 Vulnerabilidades de los programas (software)	[10]	[4]	[40]
	EFNI.13 Errores de mantenimiento / actualización de programas (software)	[10]	[3]	[30]
	EFNI.14 Errores de mantenimiento / actualización de equipos (hardware)	[10]	[4]	[40]
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[10]	[3]	[30]
	AD.16 Robo de equipos	[10]	[4]	[40]
	AD.1 Manipulación de la configuración	[10]	[3]	[30]
	AD.2 Suplantación de la identidad del usuario	[10]	[4]	[40]
	AD.3 Abuso de privilegios de acceso	[10]	[3]	[30]
	AD.5 Alteración de secuencia	[10]	[3]	[30]
	AD.6 Acceso no autorizado	[10]	[4]	[40]
	AD.8 Interceptación de información (escucha)	[10]	[4]	[40]
	AD.14 Manipulación de programas	[10]	[4]	[40]
	AD.15 Denegación de servicio	[10]	[3]	[30]
COMUNICACIÓN (Red inalámbrica, Red LAN)	DN.1 Fuego	[10]	[4]	[40]
	DN.2 Daños por agua	[10]	[4]	[40]
	DN.3 Desastres naturales	[10]	[4]	[40]
	OI.3 Corte del suministro eléctrico	[10]	[3]	[30]
	OI.4 Condiciones inadecuadas de temperatura o humedad	[10]	[4]	[40]
	EFNI.17 Fallo de servicios de comunicaciones	[10]	[4]	[40]
	EFNI.2 Errores del administrador	[10]	[3]	[30]
	EFNI.4 Errores de configuración	[10]	[3]	[30]
	EFNI.6 Errores de secuencia	[10]	[3]	[30]
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[10]	[3]	[30]
	AD.1 Manipulación de la configuración	[10]	[3]	[30]
	AD.2 Suplantación de la identidad del usuario	[10]	[4]	[40]
	AD.3 Abuso de privilegios de acceso	[10]	[3]	[30]
	AD.5 Alteración de secuencia	[10]	[3]	[30]
	AD.6 Acceso no autorizado	[10]	[4]	[40]
	AD.7 Análisis de tráfico	[10]	[2]	[20]
	AD.8 Interceptación de información (escucha)	[10]	[4]	[40]
	AD.16 Robo de equipos	[10]	[4]	[40]
ELEMENTOS AUXILIARES (UPS, Cable UTP, Fibra óptica, Transformador de aislamiento)	DN.1 Fuego	[7]	[4]	[28]
	DN.2 Daños por agua	[7]	[4]	[28]
	DN.3 Desastres naturales	[7]	[4]	[28]
	OI.3 Corte del suministro eléctrico	[7]	[3]	[21]
	OI.4 Condiciones inadecuadas de temperatura o humedad	[7]	[4]	[28]
	AD.16 Robo de equipos	[7]	[4]	[28]

Tabla 32. Impacto acumulado: Integridad – Equipamiento (activo)

- **Personal**

Activo	Amenazas	Valor del Activo	Impacto	Impacto Acumulado
ADMINISTRADOR DE SISTEMAS Y BASE DE DATOS	AD.13 Divulgación de información	[7]	[4]	[28]
	EFNI.16 Indisponibilidad del personal	[7]	[3]	[21]
OPERADOR	AD.13 Divulgación de información	[7]	[4]	[28]
	EFNI.16 Indisponibilidad del personal	[7]	[3]	[21]

Tabla 33. Impacto acumulado: Integridad – Personal (activo)

- **Instalación**

Activo	Amenazas	Valor del Activo	Impacto	Impacto Acumulado
HOSPITAL III-IQUITOS	DN.1 Fuego	[10]	[4]	[40]
	DN.2 Daños por agua	[10]	[4]	[40]
	DN.3 Desastres naturales	[10]	[4]	[40]
	AD.6 Acceso no autorizado	[10]	[4]	[40]

Tabla 34. Impacto acumulado: Integridad – Instalación (activo)

c) [C] confidencialidad (dimensión)

- **Servicios Internos**

Activo	Amenazas	Valor del Activo	Impacto	Impacto Acumulado
CORREO ELECTRONICO	EFNI.1 Errores de los usuarios	[4]	[2]	[8]
	EFNI.2 Errores del administrador	[4]	[2]	[8]
	EFNI.3 Errores de monitorización	[4]		[4]
	EFNI.4 Errores de configuración	[4]	[2]	[8]
	EFNI.6 Errores de secuencia	[4]	[2]	[8]
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[4]	[3]	[12]
	AD.1 Manipulación de la configuración	[4]	[3]	[12]
	AD.2 Suplantación de la identidad del usuario	[4]	[3]	[12]
	AD.3 Abuso de privilegios de acceso	[4]	[2]	[8]
	AD.5 Alteración de secuencia	[4]	[3]	[12]
	AD.6 Acceso no autorizado	[4]	[3]	[12]
	AD.15 Denegación de servicio	[4]	[2]	[8]
SISTEMA DE GESTION HOSPITALARIA	EFNI.1 Errores de los usuarios	[5]	[3]	[15]
	EFNI.2 Errores del administrador	[5]	[3]	[15]
	EFNI.3 Errores de monitorización	[5]	[3]	[15]
	EFNI.4 Errores de configuración	[5]		[5]
	EFNI.6 Errores de secuencia	[5]	[2]	[10]
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[5]	[3]	[15]
	AD.1 Manipulación de la configuración	[5]	[3]	[15]
	AD.2 Suplantación de la identidad del usuario	[5]	[3]	[15]
	AD.3 Abuso de privilegios de acceso	[5]	[3]	[15]
	AD.5 Alteración de secuencia	[5]	[2]	[10]
	AD.6 Acceso no autorizado	[5]	[3]	[15]
	AD.15 Denegación de servicio	[5]	[3]	[15]

Tabla 35. Impacto acumulado: Confidencialidad - Servicios internos (activo)

- **Equipamiento**

Activos	Amenazas	Valor del Activo	Impacto	Impacto Acumulado
APLICACIONES (Fox, Linux R.H 5.4,Cenos 5, Asterisk)	EFNI.1 Errores de los usuarios	[6]	[2]	[12]
	EFNI.2 Errores del administrador	[6]	[2]	[12]
	EFNI.3 Errores de monitorización	[6]		[6]
	EFNI.4 Errores de configuración	[6]	[2]	[12]
	EFNI.6 Errores de secuencia	[6]	[2]	[12]
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[6]	[3]	[18]
	AD.1 Manipulación de la configuración	[6]	[3]	[18]
	AD.2 Suplantación de la identidad del usuario	[6]	[3]	[18]
	AD.3 Abuso de privilegios de acceso	[6]	[2]	[12]
	AD.5 Alteración de secuencia	[6]	[3]	[18]
	AD.6 Acceso no autorizado	[6]	[3]	[18]
	AD.15 Denegación de servicio	[6]	[2]	[12]
	AD.19 Alteración de la información	[6]	[4]	[24]
	AD.10 Introducción de falsa información	[6]	[4]	[24]
	AD.12 Destrucción de la información	[6]	[4]	[24]
	AD.13 Divulgación de información	[6]	[4]	[24]
	EFNI.12 Vulnerabilidades de los programas (software)	[6]	[4]	[24]
	EFNI.13 Errores de mantenimiento / actualización de programas (software)	[6]	[3]	[18]
EQUIPOS (Servidor de aplicaciones y Base de datos, Servidor de Correo, Switch Core, Switch Alcatel, Servidor de Backup, Radio enlace)	DN.1 Fuego	[10]	[4]	[40]
	DN.2 Daños por agua	[10]	[4]	[40]
	DN.3 Desastres naturales	[10]	[4]	[40]
	OI.3 Corte del suministro eléctrico	[10]	[3]	[30]
	OI.4 Condiciones inadecuadas de temperatura o humedad	[10]	[4]	[40]
	EFNI.1 Errores de los usuarios	[10]	[3]	[30]
	EFNI.2 Errores del administrador	[10]	[3]	[30]
	EFNI.3 Errores de monitorización	[10]		[10]
	EFNI.4 Errores de configuración	[10]	[3]	[30]
	EFNI.5 Difusión de software dañino	[10]	[3]	[30]
	EFNI.6 Errores de secuencia	[10]	[3]	[30]

	EFNI.12 Vulnerabilidades de los programas (software)	[10]	[4]	[40]
	EFNI.13 Errores de mantenimiento / actualización de programas (software)	[10]	[3]	[30]
	EFNI.14 Errores de mantenimiento / actualización de equipos (hardware)	[10]	[4]	[40]
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[10]	[3]	[30]
	AD.16 Robo de equipos	[10]	[4]	[40]
	AD.1 Manipulación de la configuración	[10]	[3]	[30]
	AD.2 Suplantación de la identidad del usuario	[10]	[4]	[40]
	AD.3 Abuso de privilegios de acceso	[10]	[3]	[30]
	AD.5 Alteración de secuencia	[10]	[3]	[30]
	AD.6 Acceso no autorizado	[10]	[4]	[40]
	AD.8 Interceptación de información (escucha)	[10]	[4]	[40]
	AD.14 Manipulación de programas	[10]	[4]	[40]
	AD.15 Denegación de servicio	[10]	[3]	[30]
COMUNICACIÓN (Red inalámbrica, Red LAN)	DN.1 Fuego	[10]	[4]	[40]
	DN.2 Daños por agua	[10]	[4]	[40]
	DN.3 Desastres naturales	[10]	[4]	[40]
	OI.3 Corte del suministro eléctrico	[10]	[3]	[30]
	OI.4 Condiciones inadecuadas de temperatura o humedad	[10]	[4]	[40]
	EFNI.17 Fallo de servicios de comunicaciones	[10]	[4]	[40]
	EFNI.2 Errores del administrador	[10]	[3]	[30]
	EFNI.4 Errores de configuración	[10]	[3]	[30]
	EFNI.6 Errores de secuencia	[10]	[3]	[30]
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[10]	[3]	[30]
	AD.1 Manipulación de la configuración	[10]	[3]	[30]
	AD.2 Suplantación de la identidad del usuario	[10]	[4]	[40]
	AD.3 Abuso de privilegios de acceso	[10]	[3]	[30]
	AD.5 Alteración de secuencia	[10]	[3]	[30]
	AD.6 Acceso no autorizado	[10]	[4]	[40]
	AD.7 Análisis de tráfico	[10]	[2]	[20]
	AD.8 Interceptación de información (escucha)	[10]	[4]	[40]
	AD.16 Robo de equipos	[10]	[4]	[40]
ELEMENTOS AUXILIARES (UPS, Cable UTP, Fibra óptica, Transformador de aislamiento)	DN.1 Fuego	[7]	[4]	[28]
	DN.2 Daños por agua	[7]	[4]	[28]
	DN.3 Desastres naturales	[7]	[4]	[28]
	OI.3 Corte del suministro eléctrico	[7]	[3]	[21]
	OI.4 Condiciones inadecuadas de temperatura o humedad	[7]	[4]	[28]
	AD.16 Robo de equipos	[7]	[4]	[28]

Tabla 36. Impacto acumulado: Confidencialidad – Equipamiento (activo)

- **Personal**

Activo	Amenazas	Valor del Activo	Impacto	Impacto Acumulado
ADMINISTRADOR DE SISTEMAS Y BASE DE DATOS	AD.13 Divulgación de información	[7]	[4]	[28]
	EFNI.16 Indisponibilidad del personal	[7]	[3]	[21]
OPERADOR	AD.13 Divulgación de información	[7]	[4]	[28]
	EFNI.16 Indisponibilidad del personal	[7]	[3]	[21]

Tabla 37. Impacto acumulado: Confidencialidad – Personal (activo)

- **Instalación**

Activo	Amenazas	Valor del Activo	Impacto	Impacto Acumulado
HOSPITAL III-IQUITOS	DN.1 Fuego	[10]	[4]	[40]
	DN.2 Daños por agua	[10]	[4]	[40]
	DN.3 Desastres naturales	[10]	[4]	[40]
	AD.6 Acceso no autorizado	[10]	[4]	[40]

Tabla 38. Impacto acumulado: Confidencialidad – Instalación (activo)

d) [A] autenticidad de los usuarios y la información (dimensión)

- **Servicios internos**

Activo	Amenazas	Valor del Activo	Impacto	Impacto Acumulado
CORREO ELECTRONICO	EFNI.1 Errores de los usuarios	[4]	[2]	[8]
	EFNI.2 Errores del administrador	[4]	[2]	[8]
	EFNI.3 Errores de monitorización	[4]		[4]
	EFNI.4 Errores de configuración	[4]	[2]	[8]
	EFNI.6 Errores de secuencia	[4]	[2]	[8]
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[4]	[3]	[12]
	AD.1 Manipulación de la configuración	[4]	[3]	[12]
	AD.2 Suplantación de la identidad del usuario	[4]	[3]	[12]
	AD.3 Abuso de privilegios de acceso	[4]	[2]	[8]
	AD.5 Alteración de secuencia	[4]	[3]	[12]
	AD.6 Acceso no autorizado	[4]	[3]	[12]
	AD.15 Denegación de servicio	[4]	[2]	[8]
SISTEMA DE GESTION HOSPITALARIA	EFNI.1 Errores de los usuarios	[5]	[3]	[15]
	EFNI.2 Errores del administrador	[5]	[3]	[15]
	EFNI.3 Errores de monitorización	[5]	[3]	[15]
	EFNI.4 Errores de configuración	[5]		[5]
	EFNI.6 Errores de secuencia	[5]	[2]	[10]
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[5]	[3]	[15]
	AD.1 Manipulación de la configuración	[5]	[3]	[15]
	AD.2 Suplantación de la identidad del usuario	[5]	[3]	[15]
	AD.3 Abuso de privilegios de acceso	[5]	[3]	[15]
	AD.5 Alteración de secuencia	[5]	[2]	[10]
	AD.6 Acceso no autorizado	[5]	[3]	[15]
	AD.15 Denegación de servicio	[5]	[3]	[15]

Tabla 39. Impacto acumulado: Autenticidad de los usuarios y la información - Servicios internos (activo)

- **Equipamiento**

Activos	Amenazas	Valor del Activo	Impacto	Impacto Acumulado
APLICACIONES (Fox, Linux R.H 5.4,Cenos 5, Asterisk)	EFNI.1 Errores de los usuarios	[6]	[2]	[12]
	EFNI.2 Errores del administrador	[6]	[2]	[12]
	EFNI.3 Errores de monitorización	[6]		[6]
	EFNI.4 Errores de configuración	[6]	[2]	[12]
	EFNI.6 Errores de secuencia	[6]	[2]	[12]
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[6]	[3]	[18]
	AD.1 Manipulación de la configuración	[6]	[3]	[18]
	AD.2 Suplantación de la identidad del usuario	[6]	[3]	[18]
	AD.3 Abuso de privilegios de acceso	[6]	[2]	[12]
	AD.5 Alteración de secuencia	[6]	[3]	[18]
	AD.6 Acceso no autorizado	[6]	[3]	[18]
	AD.15 Denegación de servicio	[6]	[2]	[12]
	AD.19 Alteración de la información	[6]	[4]	[24]
	AD.10 Introducción de falsa información	[6]	[4]	[24]
	AD.12 Destrucción de la información	[6]	[4]	[24]
	AD.13 Divulgación de información	[6]	[4]	[24]
	EFNI.12 Vulnerabilidades de los programas (software)	[6]	[4]	[24]
	EFNI.13 Errores de mantenimiento / actualización de programas (software)	[6]	[3]	[18]
EQUIPOS (Servidor de aplicaciones y Base de datos, Servidor de Correo, Switch Core, Switch Alcatel, Servidor de Backup, Radio enlace)	DN.1 Fuego	[10]	[4]	[40]
	DN.2 Daños por agua	[10]	[4]	[40]
	DN.3 Desastres naturales	[10]	[4]	[40]
	OI.3 Corte del suministro eléctrico	[10]	[3]	[30]
	OI.4 Condiciones inadecuadas de temperatura o humedad	[10]	[4]	[40]
	EFNI.1 Errores de los usuarios	[10]	[3]	[30]
	EFNI.2 Errores del administrador	[10]	[3]	[30]
	EFNI.3 Errores de monitorización	[10]		[10]
	EFNI.4 Errores de configuración	[10]	[3]	[30]
	EFNI.5 Difusión de software dañino	[10]	[3]	[30]
	EFNI.6 Errores de secuencia	[10]	[3]	[30]
	EFNI.12 Vulnerabilidades de los programas (software)	[10]	[4]	[40]

	EFNI.13 Errores de mantenimiento / actualización de programas (software)	[10]	[3]	[30]
	EFNI.14 Errores de mantenimiento / actualización de equipos (hardware)	[10]	[4]	[40]
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[10]	[3]	[30]
	AD.16 Robo de equipos	[10]	[4]	[40]
	AD.1 Manipulación de la configuración	[10]	[3]	[30]
	AD.2 Suplantación de la identidad del usuario	[10]	[4]	[40]
	AD.3 Abuso de privilegios de acceso	[10]	[3]	[30]
	AD.5 Alteración de secuencia	[10]	[3]	[30]
	AD.6 Acceso no autorizado	[10]	[4]	[40]
	AD.8 Interceptación de información (escucha)	[10]	[4]	[40]
	AD.14 Manipulación de programas	[10]	[4]	[40]
	AD.15 Denegación de servicio	[10]	[3]	[30]
COMUNICACIÓN (Red inalámbrica, Red LAN)	DN.1 Fuego	[10]	[4]	[40]
	DN.2 Daños por agua	[10]	[4]	[40]
	DN.3 Desastres naturales	[10]	[4]	[40]
	OI.3 Corte del suministro eléctrico	[10]	[3]	[30]
	OI.4 Condiciones inadecuadas de temperatura o humedad	[10]	[4]	[40]
	EFNI.17 Fallo de servicios de comunicaciones	[10]	[4]	[40]
	EFNI.2 Errores del administrador	[10]	[3]	[30]
	EFNI.4 Errores de configuración	[10]	[3]	[30]
	EFNI.6 Errores de secuencia	[10]	[3]	[30]
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[10]	[3]	[30]
	AD.1 Manipulación de la configuración	[10]	[3]	[30]
	AD.2 Suplantación de la identidad del usuario	[10]	[4]	[40]
	AD.3 Abuso de privilegios de acceso	[10]	[3]	[30]
	AD.5 Alteración de secuencia	[10]	[3]	[30]
	AD.6 Acceso no autorizado	[10]	[4]	[40]
	AD.7 Análisis de tráfico	[10]	[2]	[20]
	AD.8 Interceptación de información (escucha)	[10]	[4]	[40]
	AD.16 Robo de equipos	[10]	[4]	[40]
ELEMENTOS AUXILIARES (UPS, Cable UTP, Fibra óptica, Transformador de aislamiento)	DN.1 Fuego	[7]	[4]	[28]
	DN.2 Daños por agua	[7]	[4]	[28]
	DN.3 Desastres naturales	[7]	[4]	[28]
	OI.3 Corte del suministro eléctrico	[7]	[3]	[21]
	OI.4 Condiciones inadecuadas de temperatura o humedad	[7]	[4]	[28]
	AD.16 Robo de equipos	[7]	[4]	[28]

Tabla 40. Impacto acumulado: Autenticidad de los usuarios y la información – Equipamiento (activo)

- **Personal**

Activo	Amenazas	Valor del Activo	Impacto	Impacto Acumulado
ADMINISTRADOR DE SISTEMAS Y BASE DE DATOS	AD.13 Divulgación de información	[7]	[4]	[28]
	EFNI.16 Indisponibilidad del personal	[7]	[3]	[21]
OPERADOR	AD.13 Divulgación de información	[7]	[4]	[28]
	EFNI.16 Indisponibilidad del personal	[7]	[3]	[21]

Tabla 41. Impacto acumulado: Autenticidad de los usuarios y la información – Personal (activo)

- **Instalación**

Activo	Amenazas	Valor del Activo	Impacto	Impacto Acumulado
HOSPITAL III-IQUITOS	DN.1 Fuego	[10]	[4]	[40]
	DN.2 Daños por agua	[10]	[4]	[40]
	DN.3 Desastres naturales	[10]	[4]	[40]
	AD.6 Acceso no autorizado	[10]	[4]	[40]

Tabla 42. Impacto acumulado: Autenticidad de los usuarios y la información – Instalación (activo)

e) [T] trazabilidad del servicio y de los datos (dimensión)

- **Servicios internos**

Activo	Amenazas	Valor del Activo	Impacto	Impacto Acumulado
CORREO ELECTRONICO	EFNI.1 Errores de los usuarios	[4]	[2]	[8]
	EFNI.2 Errores del administrador	[4]	[2]	[8]
	EFNI.3 Errores de monitorización	[4]		[4]
	EFNI.4 Errores de configuración	[4]	[2]	[8]
	EFNI.6 Errores de secuencia	[4]	[2]	[8]
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[4]	[3]	[12]
	AD.1 Manipulación de la configuración	[4]	[3]	[12]
	AD.2 Suplantación de la identidad del usuario	[4]	[3]	[12]
	AD.3 Abuso de privilegios de acceso	[4]	[2]	[8]
	AD.5 Alteración de secuencia	[4]	[3]	[12]
	AD.6 Acceso no autorizado	[4]	[3]	[12]
	AD.15 Denegación de servicio	[4]	[2]	[8]
SISTEMA DE GESTION HOSPITALARIA	EFNI.1 Errores de los usuarios	[5]	[3]	[15]
	EFNI.2 Errores del administrador	[5]	[3]	[15]
	EFNI.3 Errores de monitorización	[5]	[3]	[15]
	EFNI.4 Errores de configuración	[5]		[5]
	EFNI.6 Errores de secuencia	[5]	[2]	[10]
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[5]	[3]	[15]
	AD.1 Manipulación de la configuración	[5]	[3]	[15]
	AD.2 Suplantación de la identidad del usuario	[5]	[3]	[15]
	AD.3 Abuso de privilegios de acceso	[5]	[3]	[15]
	AD.5 Alteración de secuencia	[5]	[2]	[10]
	AD.6 Acceso no autorizado	[5]	[3]	[15]
	AD.15 Denegación de servicio	[5]	[3]	[15]

Tabla 43. Impacto acumulado: Trazabilidad del servicio y de los datos - Servicios internos (activo)

- **Equipamiento**

Activos	Amenazas	Valor del Activo	Impacto	Impacto Acumulado
APLICACIONES (Fox, Linux R.H 5.4,Cenos 5, Asterisk)	EFNI.1 Errores de los usuarios	[6]	[2]	[12]
	EFNI.2 Errores del administrador	[6]	[2]	[12]
	EFNI.3 Errores de monitorización	[6]		[6]
	EFNI.4 Errores de configuración	[6]	[2]	[12]
	EFNI.6 Errores de secuencia	[6]	[2]	[12]
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[6]	[3]	[18]
	AD.1 Manipulación de la configuración	[6]	[3]	[18]
	AD.2 Suplantación de la identidad del usuario	[6]	[3]	[18]
	AD.3 Abuso de privilegios de acceso	[6]	[2]	[12]
	AD.5 Alteración de secuencia	[6]	[3]	[18]
	AD.6 Acceso no autorizado	[6]	[3]	[18]
	AD.15 Denegación de servicio	[6]	[2]	[12]
	AD.19 Alteración de la información	[6]	[4]	[24]
	AD.10 Introducción de falsa información	[6]	[4]	[24]
	AD.12 Destrucción de la información	[6]	[4]	[24]
	AD.13 Divulgación de información	[6]	[4]	[24]
	EFNI.12 Vulnerabilidades de los programas (software)	[6]	[4]	[24]
	EFNI.13 Errores de mantenimiento / actualización de programas (software)	[6]	[3]	[18]
EQUIPOS (Servidor de aplicaciones y Base de datos, Servidor de Correo, Switch Core, Switch Alcatel, Servidor de Backup, Radio enlace)	DN.1 Fuego	[10]	[4]	[40]
	DN.2 Daños por agua	[10]	[4]	[40]
	DN.3 Desastres naturales	[10]	[4]	[40]
	OI.3 Corte del suministro eléctrico	[10]	[3]	[30]
	OI.4 Condiciones inadecuadas de temperatura o humedad	[10]	[4]	[40]
	EFNI.1 Errores de los usuarios	[10]	[3]	[30]
	EFNI.2 Errores del administrador	[10]	[3]	[30]
	EFNI.3 Errores de monitorización	[10]		[10]
	EFNI.4 Errores de configuración	[10]	[3]	[30]
	EFNI.5 Difusión de software dañino	[10]	[3]	[30]
	EFNI.6 Errores de secuencia	[10]	[3]	[30]

	EFNI.12 Vulnerabilidades de los programas (software)	[10]	[4]	[40]
	EFNI.13 Errores de mantenimiento / actualización de programas (software)	[10]	[3]	[30]
	EFNI.14 Errores de mantenimiento / actualización de equipos (hardware)	[10]	[4]	[40]
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[10]	[3]	[30]
	AD.16 Robo de equipos	[10]	[4]	[40]
	AD.1 Manipulación de la configuración	[10]	[3]	[30]
	AD.2 Suplantación de la identidad del usuario	[10]	[4]	[40]
	AD.3 Abuso de privilegios de acceso	[10]	[3]	[30]
	AD.5 Alteración de secuencia	[10]	[3]	[30]
	AD.6 Acceso no autorizado	[10]	[4]	[40]
	AD.8 Interceptación de información (escucha)	[10]	[4]	[40]
	AD.14 Manipulación de programas	[10]	[4]	[40]
	AD.15 Denegación de servicio	[10]	[3]	[30]
COMUNICACIÓN (Red inalámbrica, Red LAN)	DN.1 Fuego	[10]	[4]	[40]
	DN.2 Daños por agua	[10]	[4]	[40]
	DN.3 Desastres naturales	[10]	[4]	[40]
	OI.3 Corte del suministro eléctrico	[10]	[3]	[30]
	OI.4 Condiciones inadecuadas de temperatura o humedad	[10]	[4]	[40]
	EFNI.17 Fallo de servicios de comunicaciones	[10]	[4]	[40]
	EFNI.2 Errores del administrador	[10]	[3]	[30]
	EFNI.4 Errores de configuración	[10]	[3]	[30]
	EFNI.6 Errores de secuencia	[10]	[3]	[30]
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[10]	[3]	[30]
	AD.1 Manipulación de la configuración	[10]	[3]	[30]
	AD.2 Suplantación de la identidad del usuario	[10]	[4]	[40]
	AD.3 Abuso de privilegios de acceso	[10]	[3]	[30]
	AD.5 Alteración de secuencia	[10]	[3]	[30]
	AD.6 Acceso no autorizado	[10]	[4]	[40]
	AD.7 Análisis de tráfico	[10]	[2]	[20]
	AD.8 Interceptación de información (escucha)	[10]	[4]	[40]
	AD.16 Robo de equipos	[10]	[4]	[40]
ELEMENTOS AUXILIARES (UPS, Cable UTP, Fibra óptica, Transformador de aislamiento)	DN.1 Fuego	[7]	[4]	[28]
	DN.2 Daños por agua	[7]	[4]	[28]
	DN.3 Desastres naturales	[7]	[4]	[28]
	OI.3 Corte del suministro eléctrico	[7]	[3]	[21]
	OI.4 Condiciones inadecuadas de temperatura o humedad	[7]	[4]	[28]
	AD.16 Robo de equipos	[7]	[4]	[28]

Tabla 44. Impacto acumulado: Trazabilidad del servicio y de los datos – Equipamiento (activo)

- **Personal**

Activo	Amenazas	Valor del Activo	Impacto	Impacto Acumulado
ADMINISTRADOR DE SISTEMAS Y BASE DE DATOS	AD.13 Divulgación de información	[7]	[4]	[28]
	EFNI.16 Indisponibilidad del personal	[7]	[3]	[21]
OPERADOR	AD.13 Divulgación de información	[7]	[4]	[28]
	EFNI.16 Indisponibilidad del personal	[7]	[3]	[21]

Tabla 45. Impacto acumulado: Trazabilidad del servicio y de los datos – Personal (activo)

- **Instalación**

Activo	Amenazas	Valor del Activo	Impacto	Impacto Acumulado
HOSPITAL III-IQUITOS	DN.1 Fuego	[10]	[4]	[40]
	DN.2 Daños por agua	[10]	[4]	[40]
	DN.3 Desastres naturales	[10]	[4]	[40]
	AD.6 Acceso no autorizado	[10]	[4]	[40]

Tabla 46. Impacto acumulado: Trazabilidad del servicio y de los datos – Instalación (activo)

- Impacto repercutido

El impacto repercutido es el calculado sobre un activo teniendo en cuenta:
Su valor propio.

- ✓ Las amenazas a las que están expuestos los activos de los que depende.
- ✓ El impacto repercutido se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo el resultado final la degradación del valor del activo con el impacto de la amenaza. **(*Referencia bibliográfica pág.87 Magerit-III-Guía de Técnicas***

VALORACIÓN:		
8-10	Alto	Daño grave al Hospital
5-7	Medio	Daño importante al Hospital
1-4	Bajo	Daño menor al Hospital
0	Despreciable	Irrelevantes a efectos prácticos

Referencia (Tabla 3-Valor a los activos)

Nivel	Descripción	Impacto
Poco Impacto	Pérdida de Información y/o equipamiento	1
Bajo Impacto	Pérdida de información de poca importancia	2
Alto Impacto	Retraso o interrupción del sistema	3
Gran Impacto	Información crítica, daño serio, patrimonial	4

Referencia (Tabla 26. Cuadro de Impacto)

Dimensiones:
[D] disponibilidad
[I] integridad de los datos
[C] confidencialidad de los datos
[A] autenticidad de los usuarios y de la información
[T] trazabilidad del servicio y de los datos

a) [D] disponibilidad (dimensión)

- **Servicios Internos**

Activo	Amenazas	Valor del Activo	Impacto	Impacto Repercutido
CORREO ELECTRONICO	EFNI.1 Errores de los usuarios	[4]	[2]	[2]
	EFNI.2 Errores del administrador	[4]	[2]	[2]
	EFNI.3 Errores de monitorización	[4]		[4]
	EFNI.4 Errores de configuración	[4]	[2]	[2]
	EFNI.6 Errores de secuencia	[4]	[2]	[2]
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[4]	[3]	[1]
	AD.1 Manipulación de la configuración	[4]	[3]	[1]
	AD.2 Suplantación de la identidad del usuario	[4]	[3]	[1]
	AD.3 Abuso de privilegios de acceso	[4]	[2]	[2]
	AD.5 Alteración de secuencia	[4]	[3]	[1]
	AD.6 Acceso no autorizado	[4]	[3]	[1]

	AD.15 Denegación de servicio	[4]	[2]	[2]
SISTEMA DE GESTION HOSPITALARIA	EFNI.1 Errores de los usuarios	[5]	[3]	[2]
	EFNI.2 Errores del administrador	[5]	[3]	[2]
	EFNI.3 Errores de monitorización	[5]	[3]	[2]
	EFNI.4 Errores de configuración	[5]		[5]
	EFNI.6 Errores de secuencia	[5]	[2]	[3]
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[5]	[3]	[2]
	AD.1 Manipulación de la configuración	[5]	[3]	[2]
	AD.2 Suplantación de la identidad del usuario	[5]	[3]	[2]
	AD.3 Abuso de privilegios de acceso	[5]	[3]	[2]
	AD.5 Alteración de secuencia	[5]	[2]	[3]
	AD.6 Acceso no autorizado	[5]	[3]	[2]
	AD.15 Denegación de servicio	[5]	[3]	[2]

Tabla 47. Impacto repercutido: Disponibilidad - Servicios internos (activo)

- **Equipamiento**

Activos	Amenazas	Valor del Activo	Impacto	Impacto Repercutido
APLICACIONES (Fox, Linux R.H 5.4,Cenos 5, Asterisk)	EFNI.1 Errores de los usuarios	[6]	[2]	[4]
	EFNI.2 Errores del administrador	[6]	[2]	[4]
	EFNI.3 Errores de monitorización	[6]		[6]
	EFNI.4 Errores de configuración	[6]	[2]	[4]
	EFNI.6 Errores de secuencia	[6]	[2]	[4]
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[6]	[3]	[3]
	AD.1 Manipulación de la configuración	[6]	[3]	[3]
	AD.2 Suplantación de la identidad del usuario	[6]	[3]	[3]
	AD.3 Abuso de privilegios de acceso	[6]	[2]	[4]
	AD.5 Alteración de secuencia	[6]	[3]	[3]
	AD.6 Acceso no autorizado	[6]	[3]	[3]
	AD.15 Denegación de servicio	[6]	[2]	[4]
	AD.19 Alteración de la información	[6]	[4]	[2]
	AD.10 Introducción de falsa información	[6]	[4]	[2]
	AD.12 Destrucción de la información	[6]	[4]	[2]
	AD.13 Divulgación de información	[6]	[4]	[2]
	EFNI.12 Vulnerabilidades de los programas (software)	[6]	[4]	[2]
	EFNI.13 Errores de mantenimiento / actualización de programas (software)	[6]	[3]	[3]
EQUIPOS (Servidor de aplicaciones y Base de datos, Servidor de Correo, Switch Core, Switch Alcatel, Servidor de Backup, Radio enlace)	DN.1 Fuego	[10]	[4]	[6]
	DN.2 Daños por agua	[10]	[4]	[6]
	DN.3 Desastres naturales	[10]	[4]	[6]
	OI.3 Corte del suministro eléctrico	[10]	[3]	[30]
	OI.4 Condiciones inadecuadas de temperatura o humedad	[10]	[4]	[6]
	EFNI.1 Errores de los usuarios	[10]	[3]	[7]
	EFNI.2 Errores del administrador	[10]	[3]	[7]
	EFNI.3 Errores de monitorización	[10]		[10]
	EFNI.4 Errores de configuración	[10]	[3]	[7]
	EFNI.5 Difusión de software dañino	[10]	[3]	[7]
	EFNI.6 Errores de secuencia	[10]	[3]	[7]
	EFNI.12 Vulnerabilidades de los programas (software)	[10]	[4]	[6]
	EFNI.13 Errores de mantenimiento / actualización de programas (software)	[10]	[3]	[7]
	EFNI.14 Errores de mantenimiento / actualización de equipos (hardware)	[10]	[4]	[6]
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[10]	[3]	[7]
	AD.16 Robo de equipos	[10]	[4]	[6]
	AD.1 Manipulación de la configuración	[10]	[3]	[7]
	AD.2 Suplantación de la identidad del usuario	[10]	[4]	[6]
	AD.3 Abuso de privilegios de acceso	[10]	[3]	[7]
	AD.5 Alteración de secuencia	[10]	[3]	[7]
	AD.6 Acceso no autorizado	[10]	[4]	[6]
	AD.8 Interceptación de información (escucha)	[10]	[4]	[6]
	AD.14 Manipulación de programas	[10]	[4]	[6]
	AD.15 Denegación de servicio	[10]	[3]	[7]
	DN.1 Fuego	[10]	[4]	[6]
	DN.2 Daños por agua	[10]	[4]	[6]
	DN.3 Desastres naturales	[10]	[4]	[6]
	OI.3 Corte del suministro eléctrico	[10]	[3]	[7]

COMUNICACIÓN (Red inalámbrica, Red LAN)	OI.4 Condiciones inadecuadas de temperatura o humedad	[10]	[4]	[6]
	EFNI.17 Fallo de servicios de comunicaciones	[10]	[4]	[6]
	EFNI.2 Errores del administrador	[10]	[3]	[7]
	EFNI.4 Errores de configuración	[10]	[3]	[7]
	EFNI.6 Errores de secuencia	[10]	[3]	[7]
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[10]	[3]	[7]
	AD.1 Manipulación de la configuración	[10]	[3]	[7]
	AD.2 Suplantación de la identidad del usuario	[10]	[4]	[6]
	AD.3 Abuso de privilegios de acceso	[10]	[3]	[7]
	AD.5 Alteración de secuencia	[10]	[3]	[7]
	AD.6 Acceso no autorizado	[10]	[4]	[6]
	AD.7 Análisis de tráfico	[10]	[2]	[8]
	AD.8 Interceptación de información (escucha)	[10]	[4]	[6]
	AD.16 Robo de equipos	[10]	[4]	[6]
ELEMENTOS AUXILIARES (UPS, Cable UTP, Fibra óptica, Transformador de aislamiento)	DN.1 Fuego	[7]	[4]	[3]
	DN.2 Daños por agua	[7]	[4]	[3]
	DN.3 Desastres naturales	[7]	[4]	[3]
	OI.3 Corte del suministro eléctrico	[7]	[3]	[4]
	OI.4 Condiciones inadecuadas de temperatura o humedad	[7]	[4]	[3]
	AD.16 Robo de equipos	[7]	[4]	[3]

Tabla 48. Impacto repercutido: Disponibilidad – Equipamiento (activo)

- **Personal**

Activo	Amenazas	Valor del Activo	Impacto	Impacto Repercutido
ADMINISTRADOR DE SISTEMAS Y BASE DE DATOS	AD.13 Divulgación de información	[7]	[4]	[3]
	EFNI.16 Indisponibilidad del personal	[7]	[3]	[4]
OPERADOR	AD.13 Divulgación de información	[7]	[4]	[3]
	EFNI.16 Indisponibilidad del personal	[7]	[3]	[4]

Tabla 49. Impacto repercutido: Disponibilidad – Personal (activo)

- **Instalación**

Activo	Amenazas	Valor del Activo	Impacto	Impacto Repercutido
HOSPITAL III-IQUITOS	DN.1 Fuego	[10]	[4]	[6]
	DN.2 Daños por agua	[10]	[4]	[6]
	DN.3 Desastres naturales	[10]	[4]	[6]
	AD.6 Acceso no autorizado	[10]	[4]	[6]

Tabla 50. Impacto repercutido: Disponibilidad – Instalación (activo)

b) [I] integridad (dimensión)

- **Servicios internos**

Activo	Amenazas	Valor del Activo	Impacto	Impacto Repercutido
CORREO ELECTRONICO	EFNI.1 Errores de los usuarios	[4]	[2]	[2]
	EFNI.2 Errores del administrador	[4]	[2]	[2]
	EFNI.3 Errores de monitorización	[4]		[4]
	EFNI.4 Errores de configuración	[4]	[2]	[2]
	EFNI.6 Errores de secuencia	[4]	[2]	[2]
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[4]	[3]	[1]
	AD.1 Manipulación de la configuración	[4]	[3]	[1]
	AD.2 Suplantación de la identidad del usuario	[4]	[3]	[1]
	AD.3 Abuso de privilegios de acceso	[4]	[2]	[2]
	AD.5 Alteración de secuencia	[4]	[3]	[1]
	AD.6 Acceso no autorizado	[4]	[3]	[1]

	AD.15 Denegación de servicio	[4]	[2]	[2]
SISTEMA DE GESTION HOSPITALARIA	EFNI.1 Errores de los usuarios	[5]	[3]	[2]
	EFNI.2 Errores del administrador	[5]	[3]	[2]
	EFNI.3 Errores de monitorización	[5]	[3]	[2]
	EFNI.4 Errores de configuración	[5]		[5]
	EFNI.6 Errores de secuencia	[5]	[2]	[3]
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[5]	[3]	[2]
	AD.1 Manipulación de la configuración	[5]	[3]	[2]
	AD.2 Suplantación de la identidad del usuario	[5]	[3]	[2]
	AD.3 Abuso de privilegios de acceso	[5]	[3]	[2]
	AD.5 Alteración de secuencia	[5]	[2]	[3]
	AD.6 Acceso no autorizado	[5]	[3]	[2]
	AD.15 Denegación de servicio	[5]	[3]	[2]

Tabla 51. Impacto repercutido: Integridad - Servicios internos (activo)

- **Equipamiento**

Activos	Amenazas	Valor del Activo	Impacto	Impacto Repercutido
APLICACIONES (Fox, Linux R.H 5.4,Cenos 5, Asterisk)	EFNI.1 Errores de los usuarios	[6]	[2]	[4]
	EFNI.2 Errores del administrador	[6]	[2]	[4]
	EFNI.3 Errores de monitorización	[6]		[6]
	EFNI.4 Errores de configuración	[6]	[2]	[4]
	EFNI.6 Errores de secuencia	[6]	[2]	[4]
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[6]	[3]	[3]
	AD.1 Manipulación de la configuración	[6]	[3]	[3]
	AD.2 Suplantación de la identidad del usuario	[6]	[3]	[3]
	AD.3 Abuso de privilegios de acceso	[6]	[2]	[4]
	AD.5 Alteración de secuencia	[6]	[3]	[3]
	AD.6 Acceso no autorizado	[6]	[3]	[3]
	AD.15 Denegación de servicio	[6]	[2]	[4]
	AD.19 Alteración de la información	[6]	[4]	[2]
	AD.10 Introducción de falsa información	[6]	[4]	[2]
	AD.12 Destrucción de la información	[6]	[4]	[2]
	AD.13 Divulgación de información	[6]	[4]	[2]
	EFNI.12 Vulnerabilidades de los programas (software)	[6]	[4]	[2]
	EFNI.13 Errores de mantenimiento / actualización de programas (software)	[6]	[3]	[3]
EQUIPOS (Servidor de aplicaciones y Base de datos, Servidor de Correo, Switch Core, Switch Alcatel, Servidor de Backup, Radio enlace)	DN.1 Fuego	[10]	[4]	[6]
	DN.2 Daños por agua	[10]	[4]	[6]
	DN.3 Desastres naturales	[10]	[4]	[6]
	OI.3 Corte del suministro eléctrico	[10]	[3]	[30]
	OI.4 Condiciones inadecuadas de temperatura o humedad	[10]	[4]	[6]
	EFNI.1 Errores de los usuarios	[10]	[3]	[7]
	EFNI.2 Errores del administrador	[10]	[3]	[7]
	EFNI.3 Errores de monitorización	[10]		[10]
	EFNI.4 Errores de configuración	[10]	[3]	[7]
	EFNI.5 Difusión de software dañino	[10]	[3]	[7]
	EFNI.6 Errores de secuencia	[10]	[3]	[7]
	EFNI.12 Vulnerabilidades de los programas (software)	[10]	[4]	[6]
	EFNI.13 Errores de mantenimiento / actualización de programas (software)	[10]	[3]	[7]
	EFNI.14 Errores de mantenimiento / actualización de equipos (hardware)	[10]	[4]	[6]
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[10]	[3]	[7]
	AD.16 Robo de equipos	[10]	[4]	[6]
	AD.1 Manipulación de la configuración	[10]	[3]	[7]
	AD.2 Suplantación de la identidad del usuario	[10]	[4]	[6]
	AD.3 Abuso de privilegios de acceso	[10]	[3]	[7]
	AD.5 Alteración de secuencia	[10]	[3]	[7]
	AD.6 Acceso no autorizado	[10]	[4]	[6]
	AD.8 Interceptación de información (escucha)	[10]	[4]	[6]
	AD.14 Manipulación de programas	[10]	[4]	[6]
	AD.15 Denegación de servicio	[10]	[3]	[7]
	DN.1 Fuego	[10]	[4]	[6]
	DN.2 Daños por agua	[10]	[4]	[6]
	DN.3 Desastres naturales	[10]	[4]	[6]
	OI.3 Corte del suministro eléctrico	[10]	[3]	[7]

COMUNICACIÓN (Red inalámbrica, Red LAN)	OI.4 Condiciones inadecuadas de temperatura o humedad	[10]	[4]	[6]
	EFNI.17 Fallo de servicios de comunicaciones	[10]	[4]	[6]
	EFNI.2 Errores del administrador	[10]	[3]	[7]
	EFNI.4 Errores de configuración	[10]	[3]	[7]
	EFNI.6 Errores de secuencia	[10]	[3]	[7]
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[10]	[3]	[7]
	AD.1 Manipulación de la configuración	[10]	[3]	[7]
	AD.2 Suplantación de la identidad del usuario	[10]	[4]	[6]
	AD.3 Abuso de privilegios de acceso	[10]	[3]	[7]
	AD.5 Alteración de secuencia	[10]	[3]	[7]
	AD.6 Acceso no autorizado	[10]	[4]	[6]
	AD.7 Análisis de tráfico	[10]	[2]	[8]
	AD.8 Interceptación de información (escucha)	[10]	[4]	[6]
	AD.16 Robo de equipos	[10]	[4]	[6]
ELEMENTOS AUXILIARES (UPS, Cable UTP, Fibra óptica, Transformador de aislamiento)	DN.1 Fuego	[7]	[4]	[3]
	DN.2 Daños por agua	[7]	[4]	[3]
	DN.3 Desastres naturales	[7]	[4]	[3]
	OI.3 Corte del suministro eléctrico	[7]	[3]	[4]
	OI.4 Condiciones inadecuadas de temperatura o humedad	[7]	[4]	[3]
	AD.16 Robo de equipos	[7]	[4]	[3]

Tabla 52. Impacto repercutido: Integridad – Equipamiento (activo)

- **Personal**

Activo	Amenazas	Valor del Activo	Impacto	Impacto Repercutido
ADMINISTRADOR DE SISTEMAS Y BASE DE DATOS	AD.13 Divulgación de información	[7]	[4]	[3]
	EFNI.16 Indisponibilidad del personal	[7]	[3]	[4]
OPERADOR	AD.13 Divulgación de información	[7]	[4]	[3]
	EFNI.16 Indisponibilidad del personal	[7]	[3]	[4]

Tabla 53. Impacto repercutido: Integridad – Personal (activo)

- **Instalación**

Activo	Amenazas	Valor del Activo	Impacto	Impacto Repercutido
HOSPITAL III-IQUITOS	DN.1 Fuego	[10]	[4]	[6]
	DN.2 Daños por agua	[10]	[4]	[6]
	DN.3 Desastres naturales	[10]	[4]	[6]
	AD.6 Acceso no autorizado	[10]	[4]	[6]

Tabla 54. Impacto repercutido: Integridad – Instalación (activo)

c) [C] confidencialidad (dimensión)

- **Servicios internos**

Activo	Amenazas	Valor del Activo	Impacto	Impacto Repercutido
CORREO ELECTRONICO	EFNI.1 Errores de los usuarios	[4]	[2]	[2]
	EFNI.2 Errores del administrador	[4]	[2]	[2]
	EFNI.3 Errores de monitorización	[4]		[4]
	EFNI.4 Errores de configuración	[4]	[2]	[2]
	EFNI.6 Errores de secuencia	[4]	[2]	[2]
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[4]	[3]	[1]
	AD.1 Manipulación de la configuración	[4]	[3]	[1]
	AD.2 Suplantación de la identidad del usuario	[4]	[3]	[1]
	AD.3 Abuso de privilegios de acceso	[4]	[2]	[2]
	AD.5 Alteración de secuencia	[4]	[3]	[1]
	AD.6 Acceso no autorizado	[4]	[3]	[1]
	AD.15 Denegación de servicio	[4]	[2]	[2]
	EFNI.1 Errores de los usuarios	[5]	[3]	[2]

SISTEMA DE GESTION HOSPITALARIA	EFNI.2 Errores del administrador	[5]	[3]	[2]
	EFNI.3 Errores de monitorización	[5]	[3]	[2]
	EFNI.4 Errores de configuración	[5]		[5]
	EFNI.6 Errores de secuencia	[5]	[2]	[3]
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[5]	[3]	[2]
	AD.1 Manipulación de la configuración	[5]	[3]	[2]
	AD.2 Suplantación de la identidad del usuario	[5]	[3]	[2]
	AD.3 Abuso de privilegios de acceso	[5]	[3]	[2]
	AD.5 Alteración de secuencia	[5]	[2]	[3]
	AD.6 Acceso no autorizado	[5]	[3]	[2]
	AD.15 Denegación de servicio	[5]	[3]	[2]

Tabla 55. Impacto repercutido: Confidencialidad - Servicios internos (activo)

- **Equipamiento**

Activos	Amenazas	Valor del Activo	Impacto	Impacto Repercutido
APLICACIONES (Fox, Linux R.H 5.4,Cenos 5, Asterisk)	EFNI.1 Errores de los usuarios	[6]	[2]	[4]
	EFNI.2 Errores del administrador	[6]	[2]	[4]
	EFNI.3 Errores de monitorización	[6]		[6]
	EFNI.4 Errores de configuración	[6]	[2]	[4]
	EFNI.6 Errores de secuencia	[6]	[2]	[4]
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[6]	[3]	[3]
	AD.1 Manipulación de la configuración	[6]	[3]	[3]
	AD.2 Suplantación de la identidad del usuario	[6]	[3]	[3]
	AD.3 Abuso de privilegios de acceso	[6]	[2]	[4]
	AD.5 Alteración de secuencia	[6]	[3]	[3]
	AD.6 Acceso no autorizado	[6]	[3]	[3]
	AD.15 Denegación de servicio	[6]	[2]	[4]
	AD.19 Alteración de la información	[6]	[4]	[2]
	AD.10 Introducción de falsa información	[6]	[4]	[2]
	AD.12 Destrucción de la información	[6]	[4]	[2]
	AD.13 Divulgación de información	[6]	[4]	[2]
	EFNI.12 Vulnerabilidades de los programas (software)	[6]	[4]	[2]
	EFNI.13 Errores de mantenimiento / actualización de programas (software)	[6]	[3]	[3]
EQUIPOS (Servidor de aplicaciones y Base de datos, Servidor de Correo, Switch Core, Switch Alcatel, Servidor de Backup, Radio enlace)	DN.1 Fuego	[10]	[4]	[6]
	DN.2 Daños por agua	[10]	[4]	[6]
	DN.3 Desastres naturales	[10]	[4]	[6]
	OI.3 Corte del suministro eléctrico	[10]	[3]	[30]
	OI.4 Condiciones inadecuadas de temperatura o humedad	[10]	[4]	[6]
	EFNI.1 Errores de los usuarios	[10]	[3]	[7]
	EFNI.2 Errores del administrador	[10]	[3]	[7]
	EFNI.3 Errores de monitorización	[10]		[10]
	EFNI.4 Errores de configuración	[10]	[3]	[7]
	EFNI.5 Difusión de software dañino	[10]	[3]	[7]
	EFNI.6 Errores de secuencia	[10]	[3]	[7]
	EFNI.12 Vulnerabilidades de los programas (software)	[10]	[4]	[6]
	EFNI.13 Errores de mantenimiento / actualización de programas (software)	[10]	[3]	[7]
	EFNI.14 Errores de mantenimiento / actualización de equipos (hardware)	[10]	[4]	[6]
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[10]	[3]	[7]
	AD.16 Robo de equipos	[10]	[4]	[6]
	AD.1 Manipulación de la configuración	[10]	[3]	[7]
	AD.2 Suplantación de la identidad del usuario	[10]	[4]	[6]
	AD.3 Abuso de privilegios de acceso	[10]	[3]	[7]
	AD.5 Alteración de secuencia	[10]	[3]	[7]
	AD.6 Acceso no autorizado	[10]	[4]	[6]
	AD.8 Interceptación de información (escucha)	[10]	[4]	[6]
	AD.14 Manipulación de programas	[10]	[4]	[6]
	AD.15 Denegación de servicio	[10]	[3]	[7]
COMUNICACIÓN (Red inalámbrica, Red LAN)	DN.1 Fuego	[10]	[4]	[6]
	DN.2 Daños por agua	[10]	[4]	[6]
	DN.3 Desastres naturales	[10]	[4]	[6]
	OI.3 Corte del suministro eléctrico	[10]	[3]	[7]
	OI.4 Condiciones inadecuadas de temperatura o humedad	[10]	[4]	[6]

	EFNI.17 Fallo de servicios de comunicaciones	[10]	[4]	[6]
	EFNI.2 Errores del administrador	[10]	[3]	[7]
	EFNI.4 Errores de configuración	[10]	[3]	[7]
	EFNI.6 Errores de secuencia	[10]	[3]	[7]
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[10]	[3]	[7]
	AD.1 Manipulación de la configuración	[10]	[3]	[7]
	AD.2 Suplantación de la identidad del usuario	[10]	[4]	[6]
	AD.3 Abuso de privilegios de acceso	[10]	[3]	[7]
	AD.5 Alteración de secuencia	[10]	[3]	[7]
	AD.6 Acceso no autorizado	[10]	[4]	[6]
	AD.7 Análisis de tráfico	[10]	[2]	[8]
	AD.8 Interceptación de información (escucha)	[10]	[4]	[6]
	AD.16 Robo de equipos	[10]	[4]	[6]
ELEMENTOS AUXILIARES (UPS, Cable UTP, Fibra óptica, Transformador de aislamiento)	DN.1 Fuego	[7]	[4]	[3]
	DN.2 Daños por agua	[7]	[4]	[3]
	DN.3 Desastres naturales	[7]	[4]	[3]
	OI.3 Corte del suministro eléctrico	[7]	[3]	[4]
	OI.4 Condiciones inadecuadas de temperatura o humedad	[7]	[4]	[3]
	AD.16 Robo de equipos	[7]	[4]	[3]

Tabla 56. Impacto repercutido: Confidencialidad – Equipamiento (activo)

- **Personal**

Activo	Amenazas	Valor del Activo	Impacto	Impacto Repercutido
ADMINISTRADOR DE SISTEMAS Y BASE DE DATOS	AD.13 Divulgación de información	[7]	[4]	[3]
	EFNI.16 Indisponibilidad del personal	[7]	[3]	[4]
OPERADOR	AD.13 Divulgación de información	[7]	[4]	[3]
	EFNI.16 Indisponibilidad del personal	[7]	[3]	[4]

Tabla 57. Impacto repercutido: Confidencialidad – Personal (activo)

- **Instalación**

Activo	Amenazas	Valor del Activo	Impacto	Impacto Repercutido
HOSPITAL III-IQUITOS	DN.1 Fuego	[10]	[4]	[6]
	DN.2 Daños por agua	[10]	[4]	[6]
	DN.3 Desastres naturales	[10]	[4]	[6]
	AD.6 Acceso no autorizado	[10]	[4]	[6]

Tabla 58. Impacto repercutido: Confidencialidad – Instalación (activo)

d) [A] autenticidad de los usuarios y la información (dimensión)

- **Servicios internos**

Activo	Amenazas	Valor del Activo	Impacto	Impacto Repercutido
CORREO ELECTRONICO	EFNI.1 Errores de los usuarios	[4]	[2]	[2]
	EFNI.2 Errores del administrador	[4]	[2]	[2]
	EFNI.3 Errores de monitorización	[4]		[4]
	EFNI.4 Errores de configuración	[4]	[2]	[2]
	EFNI.6 Errores de secuencia	[4]	[2]	[2]
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[4]	[3]	[1]
	AD.1 Manipulación de la configuración	[4]	[3]	[1]
	AD.2 Suplantación de la identidad del usuario	[4]	[3]	[1]
	AD.3 Abuso de privilegios de acceso	[4]	[2]	[2]
	AD.5 Alteración de secuencia	[4]	[3]	[1]
	AD.6 Acceso no autorizado	[4]	[3]	[1]
	AD.15 Denegación de servicio	[4]	[2]	[2]
	EFNI.1 Errores de los usuarios	[5]	[3]	[2]

SISTEMA DE GESTION HOSPITALARIA	EFNI.2 Errores del administrador	[5]	[3]	[2]
	EFNI.3 Errores de monitorización	[5]	[3]	[2]
	EFNI.4 Errores de configuración	[5]		[5]
	EFNI.6 Errores de secuencia	[5]	[2]	[3]
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[5]	[3]	[2]
	AD.1 Manipulación de la configuración	[5]	[3]	[2]
	AD.2 Suplantación de la identidad del usuario	[5]	[3]	[2]
	AD.3 Abuso de privilegios de acceso	[5]	[3]	[2]
	AD.5 Alteración de secuencia	[5]	[2]	[3]
	AD.6 Acceso no autorizado	[5]	[3]	[2]
	AD.15 Denegación de servicio	[5]	[3]	[2]

Tabla 59. Impacto repercutido: Autenticidad de los usuarios y la información - Servicios internos (activo)

- **Equipamiento**

Activos	Amenazas	Valor del Activo	Impacto	Impacto Repercutido
APLICACIONES (Fox, Linux R.H 5.4,Cenos 5, Asterisk)	EFNI.1 Errores de los usuarios	[6]	[2]	[4]
	EFNI.2 Errores del administrador	[6]	[2]	[4]
	EFNI.3 Errores de monitorización	[6]		[6]
	EFNI.4 Errores de configuración	[6]	[2]	[4]
	EFNI.6 Errores de secuencia	[6]	[2]	[4]
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[6]	[3]	[3]
	AD.1 Manipulación de la configuración	[6]	[3]	[3]
	AD.2 Suplantación de la identidad del usuario	[6]	[3]	[3]
	AD.3 Abuso de privilegios de acceso	[6]	[2]	[4]
	AD.5 Alteración de secuencia	[6]	[3]	[3]
	AD.6 Acceso no autorizado	[6]	[3]	[3]
	AD.15 Denegación de servicio	[6]	[2]	[4]
	AD.19 Alteración de la información	[6]	[4]	[2]
	AD.10 Introducción de falsa información	[6]	[4]	[2]
	AD.12 Destrucción de la información	[6]	[4]	[2]
	AD.13 Divulgación de información	[6]	[4]	[2]
	EFNI.12 Vulnerabilidades de los programas (software)	[6]	[4]	[2]
	EFNI.13 Errores de mantenimiento / actualización de programas (software)	[6]	[3]	[3]
EQUIPOS (Servidor de aplicaciones y Base de datos, Servidor de Correo, Switch Core, Switch Alcatel, Servidor de Backup, Radio enlace)	DN.1 Fuego	[10]	[4]	[6]
	DN.2 Daños por agua	[10]	[4]	[6]
	DN.3 Desastres naturales	[10]	[4]	[6]
	OI.3 Corte del suministro eléctrico	[10]	[3]	[30]
	OI.4 Condiciones inadecuadas de temperatura o humedad	[10]	[4]	[6]
	EFNI.1 Errores de los usuarios	[10]	[3]	[7]
	EFNI.2 Errores del administrador	[10]	[3]	[7]
	EFNI.3 Errores de monitorización	[10]		[10]
	EFNI.4 Errores de configuración	[10]	[3]	[7]
	EFNI.5 Difusión de software dañino	[10]	[3]	[7]
	EFNI.6 Errores de secuencia	[10]	[3]	[7]
	EFNI.12 Vulnerabilidades de los programas (software)	[10]	[4]	[6]
	EFNI.13 Errores de mantenimiento / actualización de programas (software)	[10]	[3]	[7]
	EFNI.14 Errores de mantenimiento / actualización de equipos (hardware)	[10]	[4]	[6]
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[10]	[3]	[7]
	AD.16 Robo de equipos	[10]	[4]	[6]
	AD.1 Manipulación de la configuración	[10]	[3]	[7]
	AD.2 Suplantación de la identidad del usuario	[10]	[4]	[6]
	AD.3 Abuso de privilegios de acceso	[10]	[3]	[7]
	AD.5 Alteración de secuencia	[10]	[3]	[7]
	AD.6 Acceso no autorizado	[10]	[4]	[6]
	AD.8 Interceptación de información (escucha)	[10]	[4]	[6]
	AD.14 Manipulación de programas	[10]	[4]	[6]
	AD.15 Denegación de servicio	[10]	[3]	[7]
	DN.1 Fuego	[10]	[4]	[6]
	DN.2 Daños por agua	[10]	[4]	[6]
	DN.3 Desastres naturales	[10]	[4]	[6]
	OI.3 Corte del suministro eléctrico	[10]	[3]	[7]

COMUNICACIÓN (Red inalámbrica, Red LAN)	OI.4 Condiciones inadecuadas de temperatura o humedad	[10]	[4]	[6]
	EFNI.17 Fallo de servicios de comunicaciones	[10]	[4]	[6]
	EFNI.2 Errores del administrador	[10]	[3]	[7]
	EFNI.4 Errores de configuración	[10]	[3]	[7]
	EFNI.6 Errores de secuencia	[10]	[3]	[7]
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[10]	[3]	[7]
	AD.1 Manipulación de la configuración	[10]	[3]	[7]
	AD.2 Suplantación de la identidad del usuario	[10]	[4]	[6]
	AD.3 Abuso de privilegios de acceso	[10]	[3]	[7]
	AD.5 Alteración de secuencia	[10]	[3]	[7]
	AD.6 Acceso no autorizado	[10]	[4]	[6]
	AD.7 Análisis de tráfico	[10]	[2]	[8]
	AD.8 Interceptación de información (escucha)	[10]	[4]	[6]
	AD.16 Robo de equipos	[10]	[4]	[6]
ELEMENTOS AUXILIARES (UPS, Cable UTP, Fibra óptica, Transformador de aislamiento)	DN.1 Fuego	[7]	[4]	[3]
	DN.2 Daños por agua	[7]	[4]	[3]
	DN.3 Desastres naturales	[7]	[4]	[3]
	OI.3 Corte del suministro eléctrico	[7]	[3]	[4]
	OI.4 Condiciones inadecuadas de temperatura o humedad	[7]	[4]	[3]
	AD.16 Robo de equipos	[7]	[4]	[3]

Tabla 60. Impacto repercutido: Autenticidad de los usuarios y la información – Equipamiento (activo)

- **Personal**

Activo	Amenazas	Valor del Activo	Impacto	Impacto Repercutido
ADMINISTRADOR DE SISTEMAS Y BASE DE DATOS	AD.13 Divulgación de información	[7]	[4]	[3]
	EFNI.16 Indisponibilidad del personal	[7]	[3]	[4]
OPERADOR	AD.13 Divulgación de información	[7]	[4]	[3]
	EFNI.16 Indisponibilidad del personal	[7]	[3]	[4]

Tabla 61. Impacto repercutido: Autenticidad de los usuarios y la información – Personal (activo)

- **Instalación**

Activo	Amenazas	Valor del Activo	Impacto	Impacto Repercutido
HOSPITAL III-IQUITOS	DN.1 Fuego	[10]	[4]	[6]
	DN.2 Daños por agua	[10]	[4]	[6]
	DN.3 Desastres naturales	[10]	[4]	[6]
	AD.6 Acceso no autorizado	[10]	[4]	[6]

Tabla 62. Impacto repercutido: Autenticidad de los usuarios y la información – Instalación (activo)

e) [T] trazabilidad del servicio y de los datos (dimensión)

- **Servicios internos**

Activo	Amenazas	Valor del Activo	Impacto	Impacto Repercutido
CORREO ELECTRONICO	EFNI.1 Errores de los usuarios	[4]	[2]	[2]
	EFNI.2 Errores del administrador	[4]	[2]	[2]
	EFNI.3 Errores de monitorización	[4]		[4]
	EFNI.4 Errores de configuración	[4]	[2]	[2]
	EFNI.6 Errores de secuencia	[4]	[2]	[2]
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[4]	[3]	[1]
	AD.1 Manipulación de la configuración	[4]	[3]	[1]
	AD.2 Suplantación de la identidad del usuario	[4]	[3]	[1]
	AD.3 Abuso de privilegios de acceso	[4]	[2]	[2]
	AD.5 Alteración de secuencia	[4]	[3]	[1]
	AD.6 Acceso no autorizado	[4]	[3]	[1]
	AD.15 Denegación de servicio	[4]	[2]	[2]
SISTEMA DE GESTION	EFNI.1 Errores de los usuarios	[5]	[3]	[2]

HOSPITALARIA	EFNI.2 Errores del administrador	[5]	[3]	[2]
	EFNI.3 Errores de monitorización	[5]	[3]	[2]
	EFNI.4 Errores de configuración	[5]		[5]
	EFNI.6 Errores de secuencia	[5]	[2]	[3]
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[5]	[3]	[2]
	AD.1 Manipulación de la configuración	[5]	[3]	[2]
	AD.2 Suplantación de la identidad del usuario	[5]	[3]	[2]
	AD.3 Abuso de privilegios de acceso	[5]	[3]	[2]
	AD.5 Alteración de secuencia	[5]	[2]	[3]
	AD.6 Acceso no autorizado	[5]	[3]	[2]
	AD.15 Denegación de servicio	[5]	[3]	[2]

Tabla 63. Impacto repercutido: Trazabilidad del servicio y de los datos - Servicios internos (activo)

- **Equipamiento**

Activos	Amenazas	Valor del Activo	Impacto	Impacto Repercutido
APLICACIONES (Fox, Linux R.H 5.4,Cenos 5, Asterisk)	EFNI.1 Errores de los usuarios	[6]	[2]	[4]
	EFNI.2 Errores del administrador	[6]	[2]	[4]
	EFNI.3 Errores de monitorización	[6]		[6]
	EFNI.4 Errores de configuración	[6]	[2]	[4]
	EFNI.6 Errores de secuencia	[6]	[2]	[4]
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[6]	[3]	[3]
	AD.1 Manipulación de la configuración	[6]	[3]	[3]
	AD.2 Suplantación de la identidad del usuario	[6]	[3]	[3]
	AD.3 Abuso de privilegios de acceso	[6]	[2]	[4]
	AD.5 Alteración de secuencia	[6]	[3]	[3]
	AD.6 Acceso no autorizado	[6]	[3]	[3]
	AD.15 Denegación de servicio	[6]	[2]	[4]
	AD.19 Alteración de la información	[6]	[4]	[2]
	AD.10 Introducción de falsa información	[6]	[4]	[2]
	AD.12 Destrucción de la información	[6]	[4]	[2]
	AD.13 Divulgación de información	[6]	[4]	[2]
	EFNI.12 Vulnerabilidades de los programas (software)	[6]	[4]	[2]
	EFNI.13 Errores de mantenimiento / actualización de programas (software)	[6]	[3]	[3]
EQUIPOS (Servidor de aplicaciones y Base de datos, Servidor de Correo, Switch Core, Switch Alcatel, Servidor de Backup, Radio enlace)	DN.1 Fuego	[10]	[4]	[6]
	DN.2 Daños por agua	[10]	[4]	[6]
	DN.3 Desastres naturales	[10]	[4]	[6]
	OI.3 Corte del suministro eléctrico	[10]	[3]	[30]
	OI.4 Condiciones inadecuadas de temperatura o humedad	[10]	[4]	[6]
	EFNI.1 Errores de los usuarios	[10]	[3]	[7]
	EFNI.2 Errores del administrador	[10]	[3]	[7]
	EFNI.3 Errores de monitorización	[10]		[10]
	EFNI.4 Errores de configuración	[10]	[3]	[7]
	EFNI.5 Difusión de software dañino	[10]	[3]	[7]
	EFNI.6 Errores de secuencia	[10]	[3]	[7]
	EFNI.12 Vulnerabilidades de los programas (software)	[10]	[4]	[6]
	EFNI.13 Errores de mantenimiento / actualización de programas (software)	[10]	[3]	[7]
	EFNI.14 Errores de mantenimiento / actualización de equipos (hardware)	[10]	[4]	[6]
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[10]	[3]	[7]
	AD.16 Robo de equipos	[10]	[4]	[6]
	AD.1 Manipulación de la configuración	[10]	[3]	[7]
	AD.2 Suplantación de la identidad del usuario	[10]	[4]	[6]
	AD.3 Abuso de privilegios de acceso	[10]	[3]	[7]
	AD.5 Alteración de secuencia	[10]	[3]	[7]
	AD.6 Acceso no autorizado	[10]	[4]	[6]
	AD.8 Interceptación de información (escucha)	[10]	[4]	[6]
	AD.14 Manipulación de programas	[10]	[4]	[6]
	AD.15 Denegación de servicio	[10]	[3]	[7]
	DN.1 Fuego	[10]	[4]	[6]
	DN.2 Daños por agua	[10]	[4]	[6]
	DN.3 Desastres naturales	[10]	[4]	[6]
	OI.3 Corte del suministro eléctrico	[10]	[3]	[7]
	OI.4 Condiciones inadecuadas de temperatura o humedad	[10]	[4]	[6]
	EFNI.17 Fallo de servicios de comunicaciones	[10]	[4]	[6]
	EFNI.2 Errores del administrador	[10]	[3]	[7]

COMUNICACIÓN (Red inalámbrica, Red LAN)	EFNI.4 Errores de configuración	[10]	[3]	[7]
	EFNI.6 Errores de secuencia	[10]	[3]	[7]
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[10]	[3]	[7]
	AD.1 Manipulación de la configuración	[10]	[3]	[7]
	AD.2 Suplantación de la identidad del usuario	[10]	[4]	[6]
	AD.3 Abuso de privilegios de acceso	[10]	[3]	[7]
	AD.5 Alteración de secuencia	[10]	[3]	[7]
	AD.6 Acceso no autorizado	[10]	[4]	[6]
	AD.7 Análisis de tráfico	[10]	[2]	[8]
	AD.8 Interceptación de información (escucha)	[10]	[4]	[6]
	AD.16 Robo de equipos	[10]	[4]	[6]
ELEMENTOS AUXILIARES (UPS, Cable UTP, Fibra óptica, Transformador de aislamiento)	DN.1 Fuego	[7]	[4]	[3]
	DN.2 Daños por agua	[7]	[4]	[3]
	DN.3 Desastres naturales	[7]	[4]	[3]
	OI.3 Corte del suministro eléctrico	[7]	[3]	[4]
	OI.4 Condiciones inadecuadas de temperatura o humedad	[7]	[4]	[3]
	AD.16 Robo de equipos	[7]	[4]	[3]

Tabla 64. Impacto repercutido: Trazabilidad del servicio y de los datos – Equipamiento (activo)

- **Personal**

Activo	Amenazas	Valor del Activo	Impacto	Impacto Repercutido
ADMINISTRADOR DE SISTEMAS Y BASE DE DATOS	AD.13 Divulgación de información	[7]	[4]	[3]
	EFNI.16 Indisponibilidad del personal	[7]	[3]	[4]
OPERADOR	AD.13 Divulgación de información	[7]	[4]	[3]
	EFNI.16 Indisponibilidad del personal	[7]	[3]	[4]

Tabla 65. Impacto repercutido: Trazabilidad del servicio y de los datos – Personal (activo)

- **Instalación**

Activo	Amenazas	Valor del Activo	Impacto	Impacto Repercutido
HOSPITAL III-IQUITOS	DN.1 Fuego	[10]	[4]	[6]
	DN.2 Daños por agua	[10]	[4]	[6]
	DN.3 Desastres naturales	[10]	[4]	[6]
	AD.6 Acceso no autorizado	[10]	[4]	[6]

Tabla 66. Impacto repercutido: Trazabilidad del servicio y de los datos – Instalación (activo)

3.2.5. Caracterización del riesgo

- Riesgo acumulado

El riesgo acumulado es el calculado sobre un activo teniendo en cuenta:

- ✓ El impacto acumulado sobre un activo debido a una amenaza.
- ✓ La probabilidad de la amenaza.

El riesgo acumulado se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo el resultado final el valor del activo por la probabilidad de la amenaza *(Referencia bibliográfica pág.87 Magerit-III-Guía de Técnicas).*

Dimensiones:

[D] disponibilidad
[I] integridad de los datos
[C] confidencialidad de los datos
[A] autenticidad de los usuarios y de la información
[T] trazabilidad del servicio y de los datos.

VALORACIÓN:		
8-10	Alto	Daño grave al Hospital
5-7	Medio	Daño importante al Hospital
1-4	Bajo	Daño menor al Hospital
0	Despreciable	Irrelevantes a efectos prácticos

Referencia (Tabla 3-Valor a los activos)

Probabilidad de ocurrencia	Descripción
4%	Ocasional (Sucede alguna vez)
3%	Probable (Incidentes aislados)
2%	Frecuente (Incidentes repetidos)
1%	Remoto (Improbable que suceda)

Referencia (Tabla 06. Probabilidad de ocurrencia)

a) [D] disponibilidad (dimensión)

- **Servicios Internos**

Activo	Amenazas	Valor del Activo	Probabilidad	Riesgo Acumulado
CORREO ELECTRÓNICO INSTITUCIONAL	EFNI.1 Errores de los usuarios	[4]	2%	8%
	EFNI.2 Errores del administrador	[4]	2%	8%
	EFNI.3 Errores de monitorización	[4]	2%	8%
	EFNI.4 Errores de configuración	[4]	2%	8%
	EFNI.6 Errores de secuencia	[4]	2%	8%
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[4]	3%	12%
	AD.1 Manipulación de la configuración	[4]	3%	12%
	AD.2 Suplantación de la identidad del usuario	[4]	3%	12%
	AD.3 Abuso de privilegios de acceso	[4]	3%	12%
	AD.5 Alteración de secuencia	[4]	2%	8%
	AD.6 Acceso no autorizado	[4]	3%	12%
	AD.15 Denegación de servicio	[4]	3%	12%
SISTEMA DE GESTIÓN HOSPITALARIA.	EFNI.1 Errores de los usuarios	[5]	3%	15%
	EFNI.2 Errores del administrador	[5]	3%	15%
	EFNI.3 Errores de monitorización	[5]	2%	10%
	EFNI.4 Errores de configuración	[5]	3%	15%
	EFNI.6 Errores de secuencia	[5]	2%	10%
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[5]	3%	15%
	AD.1 Manipulación de la configuración	[5]	3%	15%
	AD.2 Suplantación de la identidad del usuario	[5]	3%	15%
	AD.3 Abuso de privilegios de acceso	[5]	3%	15%
	AD.5 Alteración de secuencia	[5]	2%	10%
	AD.6 Acceso no autorizado	[5]	3%	15%
	AD.15 Denegación de servicio	[5]	3%	15%

Tabla 67. Riesgo acumulado: Disponibilidad - Servicios internos (activo)

- **Equipamiento**

Activos	Amenazas	Valor del Activo	Probabilidad	Riesgo Acumulado
APLICACIONES (Fox, Linux R.H 5.4,Cenos 5, Asterisk)	EFNI.1 Errores de los usuarios	[6]	2%	12%
	EFNI.2 Errores del administrador	[6]	2%	12%
	EFNI.3 Errores de monitorización	[6]	2%	12%
	EFNI.4 Errores de configuración	[6]	2%	12%
	EFNI.6 Errores de secuencia	[6]	2%	12%
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[6]	3%	18%
	AD.1 Manipulación de la configuración	[6]	3%	18%
	AD.2 Suplantación de la identidad del usuario	[6]	3%	18%
	AD.3 Abuso de privilegios de acceso	[6]	3%	18%
	AD.5 Alteración de secuencia	[6]	2%	12%
	AD.6 Acceso no autorizado	[6]	3%	18%
	AD.15 Denegación de servicio	[6]	3%	18%
	AD.19 Alteración de la información	[6]	4%	24%
	AD.10 Introducción de falsa información	[6]	4%	24%
	AD.12 Destrucción de la información	[6]	4%	24%
	AD.13 Divulgación de información	[6]	4%	24%
	EFNI.12 Vulnerabilidades de los programas (software)	[6]	4%	24%
	EFNI.13 Errores de mantenimiento / actualización de programas (software)	[6]	4%	24%
EQUIPOS (Servidor de aplicaciones y Base de datos, Servidor de Correo, Switch Core, Switch Alcatel, Servidor de Backup, Radio enlace)	DN.1 Fuego	[10]	4%	40%
	DN.2 Daños por agua	[10]	4%	40%
	DN.3 Desastres naturales	[10]	4%	40%
	OI.3 Corte del suministro eléctrico	[10]	3%	30%
	OI.4 Condiciones inadecuadas de temperatura o humedad	[10]	3%	30%
	EFNI.1 Errores de los usuarios	[10]	2%	20%
	EFNI.2 Errores del administrador	[10]	2%	20%
	EFNI.3 Errores de monitorización	[10]	2%	20%
	EFNI.4 Errores de configuración	[10]	2%	20%
	EFNI.5 Difusión de software dañino	[10]	3%	30%
	EFNI.6 Errores de secuencia	[10]	2%	20%
	EFNI.12 Vulnerabilidades de los programas (software)	[10]	4%	40%
	EFNI.13 Errores de mantenimiento / actualización de programas (software)	[10]	4%	40%
	EFNI.14 Errores de mantenimiento / actualización de equipos (hardware)	[10]	4%	40%
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[10]	3%	30%
	AD.16 Robo de equipos	[10]	4%	40%
	AD.1 Manipulación de la configuración	[10]	3%	30%
	AD.2 Suplantación de la identidad del usuario	[10]	3%	30%
	AD.3 Abuso de privilegios de acceso	[10]	3%	30%
	AD.5 Alteración de secuencia	[10]	2%	20%
	AD.6 Acceso no autorizado	[10]	3%	30%
	AD.8 Interceptación de información (escucha)	[10]	3%	30%
	AD.14 Manipulación de programas	[10]	3%	30%
	AD.15 Denegación de servicio	[10]	3%	30%
COMUNICACIÓN (Red inalámbrica, Red LAN)	DN.1 Fuego	[10]	4%	40%
	DN.2 Daños por agua	[10]	4%	40%
	DN.3 Desastres naturales	[10]	4%	40%
	OI.3 Corte del suministro eléctrico	[10]	3%	30%
	OI.4 Condiciones inadecuadas de temperatura o humedad	[10]	3%	30%
	EFNI.17 Fallo de servicios de comunicaciones	[10]	3%	30%
	EFNI.2 Errores del administrador	[10]	2%	20%
	EFNI.4 Errores de configuración	[10]	2%	20%
	EFNI.6 Errores de secuencia	[10]	2%	20%
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[10]	3%	30%
	AD.1 Manipulación de la configuración	[10]	3%	30%
	AD.2 Suplantación de la identidad del usuario	[10]	3%	30%
	AD.3 Abuso de privilegios de acceso	[10]	3%	30%
	AD.5 Alteración de secuencia	[10]	2%	20%
	AD.6 Acceso no autorizado	[10]	3%	30%
	AD.7 Análisis de tráfico	[10]	3%	30%
	AD.8 Interceptación de información (escucha)	[10]	3%	30%
	AD.16 Robo de equipos	[10]	4%	40%

Activo	Amenazas	Valor del Activo	Probabilidad	Riesgo Acumulado
ELEMENTOS AUXILIARES (UPS, Cable UTP, Fibra óptica, Transformador de aislamiento)	DN.1 Fuego	[7]	4%	28%
	DN.2 Daños por agua	[7]	4%	28%
	DN.3 Desastres naturales	[7]	4%	28%
	OI.3 Corte del suministro eléctrico	[7]	3%	21%
	OI.4 Condiciones inadecuadas de temperatura o humedad	[7]	3%	21%
	AD.16 Robo de equipos	[7]	4%	28%

Tabla 68. Riesgo acumulado: Disponibilidad – Equipamiento (activo)

- **Personal**

Activo	Amenazas	Valor del Activo	Probabilidad	Riesgo Acumulado
ADMINISTRADOR DE SISTEMAS Y BASE DE DATOS	AD.13 Divulgación de información	[7]	3%	21%
	EFNI.16 Indisponibilidad del personal	[7]	1%	7%
OPERADOR	AD.13 Divulgación de información	[7]	3%	21%
	EFNI.16 Indisponibilidad del personal	[7]	1%	7%

Tabla 69. Riesgo acumulado: Disponibilidad – Personal (activo)

- **Instalación**

Activo	Amenazas	Valor del Activo	Probabilidad	Riesgo Acumulado
HOSPITAL III IQUITOS	DN.1 Fuego	[10]	4%	40%
	DN.2 Daños por agua	[10]	4%	40%
	DN.3 Desastres naturales	[10]	4%	40%
	AD.6 Acceso no autorizado	[10]	3%	30%

Tabla 70. Riesgo acumulado: Disponibilidad – Instalación (activo)

b) [I] integridad (dimensión)

- **Servicios Internos**

Activo	Amenazas	Valor del Activo	Probabilidad	Riesgo Acumulado
CORREO ELECTRÓNICO INSTITUCIONAL	EFNI.1 Errores de los usuarios	[4]	2%	8%
	EFNI.2 Errores del administrador	[4]	2%	8%
	EFNI.3 Errores de monitorización	[4]	2%	8%
	EFNI.4 Errores de configuración	[4]	2%	8%
	EFNI.6 Errores de secuencia	[4]	2%	8%
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[4]	3%	12%
	AD.1 Manipulación de la configuración	[4]	3%	12%
	AD.2 Suplantación de la identidad del usuario	[4]	3%	12%
	AD.3 Abuso de privilegios de acceso	[4]	3%	12%
	AD.5 Alteración de secuencia	[4]	2%	8%
	AD.6 Acceso no autorizado	[4]	3%	12%
	AD.15 Denegación de servicio	[4]	3%	12%
SISTEMA DE GESTIÓN HOSPITALARIA.	EFNI.1 Errores de los usuarios	[5]	3%	15%
	EFNI.2 Errores del administrador	[5]	3%	15%
	EFNI.3 Errores de monitorización	[5]	2%	10%
	EFNI.4 Errores de configuración	[5]	3%	15%
	EFNI.6 Errores de secuencia	[5]	2%	10%
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[5]	3%	15%
	AD.1 Manipulación de la configuración	[5]	3%	15%
	AD.2 Suplantación de la identidad del usuario	[5]	3%	15%
	AD.3 Abuso de privilegios de acceso	[5]	3%	15%
	AD.5 Alteración de secuencia	[5]	2%	10%
	AD.6 Acceso no autorizado	[5]	3%	15%
	AD.15 Denegación de servicio	[5]	3%	15%

Tabla 71. Riesgo acumulado: Integridad - Servicios internos (activo)

- **Equipamiento**

Activos	Amenazas	Valor del Activo	Probabilidad	Riesgo Acumulado
APLICACIONES (Fox, Linux R.H 5.4,Cenos 5, Asterisk)	EFNI.1 Errores de los usuarios	[6]	2%	12%
	EFNI.2 Errores del administrador	[6]	2%	12%
	EFNI.3 Errores de monitorización	[6]	2%	12%
	EFNI.4 Errores de configuración	[6]	2%	12%
	EFNI.6 Errores de secuencia	[6]	2%	12%
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[6]	3%	18%
	AD.1 Manipulación de la configuración	[6]	3%	18%
	AD.2 Suplantación de la identidad del usuario	[6]	3%	18%
	AD.3 Abuso de privilegios de acceso	[6]	3%	18%
	AD.5 Alteración de secuencia	[6]	2%	12%
	AD.6 Acceso no autorizado	[6]	3%	18%
	AD.15 Denegación de servicio	[6]	3%	18%
	AD.19 Alteración de la información	[6]	4%	24%
	AD.10 Introducción de falsa información	[6]	4%	24%
	AD.12 Destrucción de la información	[6]	4%	24%
	AD.13 Divulgación de información	[6]	4%	24%
	EFNI.12 Vulnerabilidades de los programas (software)	[6]	4%	24%
	EFNI.13 Errores de mantenimiento / actualización de programas (software)	[6]	4%	24%
EQUIPOS (Servidor de aplicaciones y Base de datos, Servidor de Correo, Switch Core, Switch Alcatel, Servidor de Backup, Radio enlace)	DN.1 Fuego	[10]	4%	40%
	DN.2 Daños por agua	[10]	4%	40%
	DN.3 Desastres naturales	[10]	4%	40%
	OI.3 Corte del suministro eléctrico	[10]	3%	30%
	OI.4 Condiciones inadecuadas de temperatura o humedad	[10]	3%	30%
	EFNI.1 Errores de los usuarios	[10]	2%	20%
	EFNI.2 Errores del administrador	[10]	2%	20%
	EFNI.3 Errores de monitorización	[10]	2%	20%
	EFNI.4 Errores de configuración	[10]	2%	20%
	EFNI.5 Difusión de software dañino	[10]	3%	30%
	EFNI.6 Errores de secuencia	[10]	2%	20%
	EFNI.12 Vulnerabilidades de los programas (software)	[10]	4%	40%
	EFNI.13 Errores de mantenimiento / actualización de programas (software)	[10]	4%	40%
	EFNI.14 Errores de mantenimiento / actualización de equipos (hardware)	[10]	4%	40%
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[10]	3%	30%
	AD.16 Robo de equipos	[10]	4%	40%
	AD.1 Manipulación de la configuración	[10]	3%	30%
	AD.2 Suplantación de la identidad del usuario	[10]	3%	30%
	AD.3 Abuso de privilegios de acceso	[10]	3%	30%
	AD.5 Alteración de secuencia	[10]	2%	20%
	AD.6 Acceso no autorizado	[10]	3%	30%
	AD.8 Interceptación de información (escucha)	[10]	3%	30%
	AD.14 Manipulación de programas	[10]	3%	30%
	AD.15 Denegación de servicio	[10]	3%	30%
COMUNICACIÓN (Red inalámbrica, Red LAN)	DN.1 Fuego	[10]	4%	40%
	DN.2 Daños por agua	[10]	4%	40%
	DN.3 Desastres naturales	[10]	4%	40%
	OI.3 Corte del suministro eléctrico	[10]	3%	30%
	OI.4 Condiciones inadecuadas de temperatura o humedad	[10]	3%	30%
	EFNI.17 Fallo de servicios de comunicaciones	[10]	3%	30%
	EFNI.2 Errores del administrador	[10]	2%	20%
	EFNI.4 Errores de configuración	[10]	2%	20%
	EFNI.6 Errores de secuencia	[10]	2%	20%
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[10]	3%	30%
	AD.1 Manipulación de la configuración	[10]	3%	30%
	AD.2 Suplantación de la identidad del usuario	[10]	3%	30%
	AD.3 Abuso de privilegios de acceso	[10]	3%	30%
	AD.5 Alteración de secuencia	[10]	2%	20%
	AD.6 Acceso no autorizado	[10]	3%	30%
	AD.7 Análisis de tráfico	[10]	3%	30%
	AD.8 Interceptación de información (escucha)	[10]	3%	30%
	AD.16 Robo de equipos	[10]	4%	40%

Activo	Amenazas	Valor del Activo	Probabilidad	Riesgo Acumulado
ELEMENTOS AUXILIARES (UPS, Cable UTP, Fibra óptica, Transformador de aislamiento)	DN.1 Fuego	[7]	4%	28%
	DN.2 Daños por agua	[7]	4%	28%
	DN.3 Desastres naturales	[7]	4%	28%
	OI.3 Corte del suministro eléctrico	[7]	3%	21%
	OI.4 Condiciones inadecuadas de temperatura o humedad	[7]	3%	21%
	AD.16 Robo de equipos	[7]	4%	28%

Tabla 72. Riesgo acumulado: Integridad – Equipamiento (activo)

- **Personal**

Activo	Amenazas	Valor del Activo	Probabilidad	Riesgo Acumulado
ADMINISTRADOR DE SISTEMAS Y BASE DE DATOS	AD.13 Divulgación de información	[7]	3%	21%
	EFNI.16 Indisponibilidad del personal	[7]	1%	7%
OPERADOR	AD.13 Divulgación de información	[7]	3%	21%
	EFNI.16 Indisponibilidad del personal	[7]	1%	7%

Tabla 73. Riesgo acumulado: Integridad – Personal (activo)

- **Instalación**

Activo	Amenazas	Valor del Activo	Probabilidad	Riesgo Acumulado
HOSPITAL III IQUITOS	DN.1 Fuego	[10]	4%	40%
	DN.2 Daños por agua	[10]	4%	40%
	DN.3 Desastres naturales	[10]	4%	40%
	AD.6 Acceso no autorizado	[10]	3%	30%

Tabla 74. Riesgo acumulado: Integridad – Instalación (activo)

c) [C] confidencialidad (dimensión)

- **Servicios Internos**

Activo	Amenazas	Valor del Activo	Probabilidad	Riesgo Acumulado
CORREO ELECTRÓNICO INSTITUCIONAL	EFNI.1 Errores de los usuarios	[4]	2%	8%
	EFNI.2 Errores del administrador	[4]	2%	8%
	EFNI.3 Errores de monitorización	[4]	2%	8%
	EFNI.4 Errores de configuración	[4]	2%	8%
	EFNI.6 Errores de secuencia	[4]	2%	8%
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[4]	3%	12%
	AD.1 Manipulación de la configuración	[4]	3%	12%
	AD.2 Suplantación de la identidad del usuario	[4]	3%	12%
	AD.3 Abuso de privilegios de acceso	[4]	3%	12%
	AD.5 Alteración de secuencia	[4]	2%	8%
	AD.6 Acceso no autorizado	[4]	3%	12%
	AD.15 Denegación de servicio	[4]	3%	12%
SISTEMA DE GESTIÓN HOSPITALARIA.	EFNI.1 Errores de los usuarios	[5]	3%	15%
	EFNI.2 Errores del administrador	[5]	3%	15%
	EFNI.3 Errores de monitorización	[5]	2%	10%
	EFNI.4 Errores de configuración	[5]	3%	15%
	EFNI.6 Errores de secuencia	[5]	2%	10%
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[5]	3%	15%
	AD.1 Manipulación de la configuración	[5]	3%	15%
	AD.2 Suplantación de la identidad del usuario	[5]	3%	15%
	AD.3 Abuso de privilegios de acceso	[5]	3%	15%
	AD.5 Alteración de secuencia	[5]	2%	10%
	AD.6 Acceso no autorizado	[5]	3%	15%
	AD.15 Denegación de servicio	[5]	3%	15%

Tabla 75. Riesgo acumulado: Confidencialidad - Servicios internos (activo)

- **Equipamiento**

Activos	Amenazas	Valor del Activo	Probabilidad	Riesgo Acumulado
APLICACIONES (Fox, Linux R.H 5.4,Cenos 5, Asterisk)	EFNI.1 Errores de los usuarios	[6]	2%	12%
	EFNI.2 Errores del administrador	[6]	2%	12%
	EFNI.3 Errores de monitorización	[6]	2%	12%
	EFNI.4 Errores de configuración	[6]	2%	12%
	EFNI.6 Errores de secuencia	[6]	2%	12%
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[6]	3%	18%
	AD.1 Manipulación de la configuración	[6]	3%	18%
	AD.2 Suplantación de la identidad del usuario	[6]	3%	18%
	AD.3 Abuso de privilegios de acceso	[6]	3%	18%
	AD.5 Alteración de secuencia	[6]	2%	12%
	AD.6 Acceso no autorizado	[6]	3%	18%
	AD.15 Denegación de servicio	[6]	3%	18%
	AD.19 Alteración de la información	[6]	4%	24%
	AD.10 Introducción de falsa información	[6]	4%	24%
	AD.12 Destrucción de la información	[6]	4%	24%
	AD.13 Divulgación de información	[6]	4%	24%
	EFNI.12 Vulnerabilidades de los programas (software)	[6]	4%	24%
	EFNI.13 Errores de mantenimiento / actualización de programas (software)	[6]	4%	24%
EQUIPOS (Servidor de aplicaciones y Base de datos, Servidor de Correo, Switch Core, Switch Alcatel, Servidor de Backup, Radio enlace)	DN.1 Fuego	[10]	4%	40%
	DN.2 Daños por agua	[10]	4%	40%
	DN.3 Desastres naturales	[10]	4%	40%
	OI.3 Corte del suministro eléctrico	[10]	3%	30%
	OI.4 Condiciones inadecuadas de temperatura o humedad	[10]	3%	30%
	EFNI.1 Errores de los usuarios	[10]	2%	20%
	EFNI.2 Errores del administrador	[10]	2%	20%
	EFNI.3 Errores de monitorización	[10]	2%	20%
	EFNI.4 Errores de configuración	[10]	2%	20%
	EFNI.5 Difusión de software dañino	[10]	3%	30%
	EFNI.6 Errores de secuencia	[10]	2%	20%
	EFNI.12 Vulnerabilidades de los programas (software)	[10]	4%	40%
	EFNI.13 Errores de mantenimiento / actualización de programas (software)	[10]	4%	40%
	EFNI.14 Errores de mantenimiento / actualización de equipos (hardware)	[10]	4%	40%
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[10]	3%	30%
	AD.16 Robo de equipos	[10]	4%	40%
	AD.1 Manipulación de la configuración	[10]	3%	30%
	AD.2 Suplantación de la identidad del usuario	[10]	3%	30%
	AD.3 Abuso de privilegios de acceso	[10]	3%	30%
	AD.5 Alteración de secuencia	[10]	2%	20%
	AD.6 Acceso no autorizado	[10]	3%	30%
	AD.8 Interceptación de información (escucha)	[10]	3%	30%
	AD.14 Manipulación de programas	[10]	3%	30%
	AD.15 Denegación de servicio	[10]	3%	30%
COMUNICACIÓN (Red inalámbrica, Red LAN)	DN.1 Fuego	[10]	4%	40%
	DN.2 Daños por agua	[10]	4%	40%
	DN.3 Desastres naturales	[10]	4%	40%
	OI.3 Corte del suministro eléctrico	[10]	3%	30%
	OI.4 Condiciones inadecuadas de temperatura o humedad	[10]	3%	30%
	EFNI.17 Fallo de servicios de comunicaciones	[10]	3%	30%
	EFNI.2 Errores del administrador	[10]	2%	20%
	EFNI.4 Errores de configuración	[10]	2%	20%
	EFNI.6 Errores de secuencia	[10]	2%	20%
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[10]	3%	30%
	AD.1 Manipulación de la configuración	[10]	3%	30%
	AD.2 Suplantación de la identidad del usuario	[10]	3%	30%
	AD.3 Abuso de privilegios de acceso	[10]	3%	30%
	AD.5 Alteración de secuencia	[10]	2%	20%
	AD.6 Acceso no autorizado	[10]	3%	30%
	AD.7 Análisis de tráfico	[10]	3%	30%
	AD.8 Interceptación de información (escucha)	[10]	3%	30%
	AD.16 Robo de equipos	[10]	4%	40%

Activo	Amenazas	Valor del Activo	Probabilidad	Riesgo Acumulado
ELEMENTOS AUXILIARES (UPS, Cable UTP, Fibra óptica, Transformador de aislamiento)	DN.1 Fuego	[7]	4%	28%
	DN.2 Daños por agua	[7]	4%	28%
	DN.3 Desastres naturales	[7]	4%	28%
	OI.3 Corte del suministro eléctrico	[7]	3%	21%
	OI.4 Condiciones inadecuadas de temperatura o humedad	[7]	3%	21%
	AD.16 Robo de equipos	[7]	4%	28%

Tabla 76. Riesgo acumulado: Confidencialidad – Equipamiento (activo)

- **Personal**

Activo	Amenazas	Valor del Activo	Probabilidad	Riesgo Acumulado
ADMINISTRADOR DE SISTEMAS Y BASE DE DATOS	AD.13 Divulgación de información	[7]	3%	21%
	EFNI.16 Indisponibilidad del personal	[7]	1%	7%
OPERADOR	AD.13 Divulgación de información	[7]	3%	21%
	EFNI.16 Indisponibilidad del personal	[7]	1%	7%

Tabla 77. Riesgo acumulado: Confidencialidad – Personal (activo)

- **Instalación**

Activo	Amenazas	Valor del Activo	Probabilidad	Riesgo Acumulado
HOSPITAL III IQUITOS	DN.1 Fuego	[10]	4%	40%
	DN.2 Daños por agua	[10]	4%	40%
	DN.3 Desastres naturales	[10]	4%	40%
	AD.6 Acceso no autorizado	[10]	3%	30%

Tabla 78. Riesgo acumulado: Confidencialidad – Instalación (activo)

d) [A] autenticidad de los usuarios y la información (dimensión)

- **Servicios Internos**

Activo	Amenazas	Valor del Activo	Probabilidad	Riesgo Acumulado
CORREO ELECTRÓNICO INSTITUCIONAL	EFNI.1 Errores de los usuarios	[4]	2%	8%
	EFNI.2 Errores del administrador	[4]	2%	8%
	EFNI.3 Errores de monitorización	[4]	2%	8%
	EFNI.4 Errores de configuración	[4]	2%	8%
	EFNI.6 Errores de secuencia	[4]	2%	8%
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[4]	3%	12%
	AD.1 Manipulación de la configuración	[4]	3%	12%
	AD.2 Suplantación de la identidad del usuario	[4]	3%	12%
	AD.3 Abuso de privilegios de acceso	[4]	3%	12%
	AD.5 Alteración de secuencia	[4]	2%	8%
	AD.6 Acceso no autorizado	[4]	3%	12%
	AD.15 Denegación de servicio	[4]	3%	12%
SISTEMA DE GESTIÓN HOSPITALARIA.	EFNI.1 Errores de los usuarios	[5]	3%	15%
	EFNI.2 Errores del administrador	[5]	3%	15%
	EFNI.3 Errores de monitorización	[5]	2%	10%
	EFNI.4 Errores de configuración	[5]	3%	15%
	EFNI.6 Errores de secuencia	[5]	2%	10%
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[5]	3%	15%
	AD.1 Manipulación de la configuración	[5]	3%	15%
	AD.2 Suplantación de la identidad del usuario	[5]	3%	15%
	AD.3 Abuso de privilegios de acceso	[5]	3%	15%
	AD.5 Alteración de secuencia	[5]	2%	10%
	AD.6 Acceso no autorizado	[5]	3%	15%
	AD.15 Denegación de servicio	[5]	3%	15%

Tabla 79. Riesgo acumulado: Autenticidad de los usuarios y la información - Servicios internos (activo)

- **Equipamiento**

Activos	Amenazas	Valor del Activo	Probabilidad	Riesgo Acumulado
APLICACIONES (Fox, Linux R.H 5.4,Cenos 5, Asterisk)	EFNI.1 Errores de los usuarios	[6]	2%	12%
	EFNI.2 Errores del administrador	[6]	2%	12%
	EFNI.3 Errores de monitorización	[6]	2%	12%
	EFNI.4 Errores de configuración	[6]	2%	12%
	EFNI.6 Errores de secuencia	[6]	2%	12%
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[6]	3%	18%
	AD.1 Manipulación de la configuración	[6]	3%	18%
	AD.2 Suplantación de la identidad del usuario	[6]	3%	18%
	AD.3 Abuso de privilegios de acceso	[6]	3%	18%
	AD.5 Alteración de secuencia	[6]	2%	12%
	AD.6 Acceso no autorizado	[6]	3%	18%
	AD.15 Denegación de servicio	[6]	3%	18%
	AD.19 Alteración de la información	[6]	4%	24%
	AD.10 Introducción de falsa información	[6]	4%	24%
	AD.12 Destrucción de la información	[6]	4%	24%
	AD.13 Divulgación de información	[6]	4%	24%
	EFNI.12 Vulnerabilidades de los programas (software)	[6]	4%	24%
	EFNI.13 Errores de mantenimiento / actualización de programas (software)	[6]	4%	24%
EQUIPOS (Servidor de aplicaciones y Base de datos, Servidor de Correo, Switch Core, Switch Alcatel, Servidor de Backup, Radio enlace)	DN.1 Fuego	[10]	4%	40%
	DN.2 Daños por agua	[10]	4%	40%
	DN.3 Desastres naturales	[10]	4%	40%
	OI.3 Corte del suministro eléctrico	[10]	3%	30%
	OI.4 Condiciones inadecuadas de temperatura o humedad	[10]	3%	30%
	EFNI.1 Errores de los usuarios	[10]	2%	20%
	EFNI.2 Errores del administrador	[10]	2%	20%
	EFNI.3 Errores de monitorización	[10]	2%	20%
	EFNI.4 Errores de configuración	[10]	2%	20%
	EFNI.5 Difusión de software dañino	[10]	3%	30%
	EFNI.6 Errores de secuencia	[10]	2%	20%
	EFNI.12 Vulnerabilidades de los programas (software)	[10]	4%	40%
	EFNI.13 Errores de mantenimiento / actualización de programas (software)	[10]	4%	40%
	EFNI.14 Errores de mantenimiento / actualización de equipos (hardware)	[10]	4%	40%
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[10]	3%	30%
	AD.16 Robo de equipos	[10]	4%	40%
	AD.1 Manipulación de la configuración	[10]	3%	30%
	AD.2 Suplantación de la identidad del usuario	[10]	3%	30%
	AD.3 Abuso de privilegios de acceso	[10]	3%	30%
	AD.5 Alteración de secuencia	[10]	2%	20%
	AD.6 Acceso no autorizado	[10]	3%	30%
	AD.8 Interceptación de información (escucha)	[10]	3%	30%
	AD.14 Manipulación de programas	[10]	3%	30%
	AD.15 Denegación de servicio	[10]	3%	30%
COMUNICACIÓN (Red inalámbrica, Red LAN)	DN.1 Fuego	[10]	4%	40%
	DN.2 Daños por agua	[10]	4%	40%
	DN.3 Desastres naturales	[10]	4%	40%
	OI.3 Corte del suministro eléctrico	[10]	3%	30%
	OI.4 Condiciones inadecuadas de temperatura o humedad	[10]	3%	30%
	EFNI.17 Fallo de servicios de comunicaciones	[10]	3%	30%
	EFNI.2 Errores del administrador	[10]	2%	20%
	EFNI.4 Errores de configuración	[10]	2%	20%
	EFNI.6 Errores de secuencia	[10]	2%	20%
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[10]	3%	30%
	AD.1 Manipulación de la configuración	[10]	3%	30%
	AD.2 Suplantación de la identidad del usuario	[10]	3%	30%
	AD.3 Abuso de privilegios de acceso	[10]	3%	30%
	AD.5 Alteración de secuencia	[10]	2%	20%
	AD.6 Acceso no autorizado	[10]	3%	30%
	AD.7 Análisis de tráfico	[10]	3%	30%
	AD.8 Interceptación de información (escucha)	[10]	3%	30%
	AD.16 Robo de equipos	[10]	4%	40%

Activo	Amenazas	Valor del Activo	Probabilidad	Riesgo Acumulado
ELEMENTOS AUXILIARES (UPS, Cable UTP, Fibra óptica, Transformador de aislamiento)	DN.1 Fuego	[7]	4%	28%
	DN.2 Daños por agua	[7]	4%	28%
	DN.3 Desastres naturales	[7]	4%	28%
	OI.3 Corte del suministro eléctrico	[7]	3%	21%
	OI.4 Condiciones inadecuadas de temperatura o humedad	[7]	3%	21%
	AD.16 Robo de equipos	[7]	4%	28%

Tabla 80. Riesgo acumulado: Autenticidad de los usuarios y la información – Equipamiento (activo)

- **Personal**

Activo	Amenazas	Valor del Activo	Probabilidad	Riesgo Acumulado
ADMINISTRADOR DE SISTEMAS Y BASE DE DATOS	AD.13 Divulgación de información	[7]	3%	21%
	EFNI.16 Indisponibilidad del personal	[7]	1%	7%
OPERADOR	AD.13 Divulgación de información	[7]	3%	21%
	EFNI.16 Indisponibilidad del personal	[7]	1%	7%

Tabla 81. Riesgo acumulado: Autenticidad de los usuarios y la información –Personal (activo)

- **Instalación**

Activo	Amenazas	Valor del Activo	Probabilidad	Riesgo Acumulado
HOSPITAL III IQUITOS	DN.1 Fuego	[10]	4%	40%
	DN.2 Daños por agua	[10]	4%	40%
	DN.3 Desastres naturales	[10]	4%	40%
	AD.6 Acceso no autorizado	[10]	3%	30%

Tabla 82. Riesgo acumulado: Autenticidad de los usuarios y la información – Instalación (activo)

e) [T] trazabilidad del servicio y de los datos

- **Servicios Internos**

Activo	Amenazas	Valor del Activo	Probabilidad	Riesgo Acumulado
CORREO ELECTRÓNICO INSTITUCIONAL	EFNI.1 Errores de los usuarios	[4]	2%	8%
	EFNI.2 Errores del administrador	[4]	2%	8%
	EFNI.3 Errores de monitorización	[4]	2%	8%
	EFNI.4 Errores de configuración	[4]	2%	8%
	EFNI.6 Errores de secuencia	[4]	2%	8%
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[4]	3%	12%
	AD.1 Manipulación de la configuración	[4]	3%	12%
	AD.2 Suplantación de la identidad del usuario	[4]	3%	12%
	AD.3 Abuso de privilegios de acceso	[4]	3%	12%
	AD.5 Alteración de secuencia	[4]	2%	8%
	AD.6 Acceso no autorizado	[4]	3%	12%
	AD.15 Denegación de servicio	[4]	3%	12%
SISTEMA DE GESTIÓN HOSPITALARIA.	EFNI.1 Errores de los usuarios	[5]	3%	15%
	EFNI.2 Errores del administrador	[5]	3%	15%
	EFNI.3 Errores de monitorización	[5]	2%	10%
	EFNI.4 Errores de configuración	[5]	3%	15%
	EFNI.6 Errores de secuencia	[5]	2%	10%
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[5]	3%	15%
	AD.1 Manipulación de la configuración	[5]	3%	15%
	AD.2 Suplantación de la identidad del usuario	[5]	3%	15%
	AD.3 Abuso de privilegios de acceso	[5]	3%	15%
	AD.5 Alteración de secuencia	[5]	2%	10%
	AD.6 Acceso no autorizado	[5]	3%	15%
	AD.15 Denegación de servicio	[5]	3%	15%

Tabla 83. Riesgo acumulado: Trazabilidad del servicio y de los datos - Servicios internos (activo)

- **Equipamiento**

Activos	Amenazas	Valor del Activo	Probabilidad	Riesgo Acumulado
APLICACIONES (Fox, Linux R.H 5.4,Cenos 5, Asterisk)	EFNI.1 Errores de los usuarios	[6]	2%	12%
	EFNI.2 Errores del administrador	[6]	2%	12%
	EFNI.3 Errores de monitorización	[6]	2%	12%
	EFNI.4 Errores de configuración	[6]	2%	12%
	EFNI.6 Errores de secuencia	[6]	2%	12%
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[6]	3%	18%
	AD.1 Manipulación de la configuración	[6]	3%	18%
	AD.2 Suplantación de la identidad del usuario	[6]	3%	18%
	AD.3 Abuso de privilegios de acceso	[6]	3%	18%
	AD.5 Alteración de secuencia	[6]	2%	12%
	AD.6 Acceso no autorizado	[6]	3%	18%
	AD.15 Denegación de servicio	[6]	3%	18%
	AD.19 Alteración de la información	[6]	4%	24%
	AD.10 Introducción de falsa información	[6]	4%	24%
	AD.12 Destrucción de la información	[6]	4%	24%
	AD.13 Divulgación de información	[6]	4%	24%
	EFNI.12 Vulnerabilidades de los programas (software)	[6]	4%	24%
	EFNI.13 Errores de mantenimiento / actualización de programas (software)	[6]	4%	24%
EQUIPOS (Servidor de aplicaciones y Base de datos, Servidor de Correo, Switch Core, Switch Alcatel, Servidor de Backup, Radio enlace)	DN.1 Fuego	[10]	4%	40%
	DN.2 Daños por agua	[10]	4%	40%
	DN.3 Desastres naturales	[10]	4%	40%
	OI.3 Corte del suministro eléctrico	[10]	3%	30%
	OI.4 Condiciones inadecuadas de temperatura o humedad	[10]	3%	30%
	EFNI.1 Errores de los usuarios	[10]	2%	20%
	EFNI.2 Errores del administrador	[10]	2%	20%
	EFNI.3 Errores de monitorización	[10]	2%	20%
	EFNI.4 Errores de configuración	[10]	2%	20%
	EFNI.5 Difusión de software dañino	[10]	3%	30%
	EFNI.6 Errores de secuencia	[10]	2%	20%
	EFNI.12 Vulnerabilidades de los programas (software)	[10]	4%	40%
	EFNI.13 Errores de mantenimiento / actualización de programas (software)	[10]	4%	40%
	EFNI.14 Errores de mantenimiento / actualización de equipos (hardware)	[10]	4%	40%
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[10]	3%	30%
	AD.16 Robo de equipos	[10]	4%	40%
	AD.1 Manipulación de la configuración	[10]	3%	30%
	AD.2 Suplantación de la identidad del usuario	[10]	3%	30%
	AD.3 Abuso de privilegios de acceso	[10]	3%	30%
	AD.5 Alteración de secuencia	[10]	2%	20%
	AD.6 Acceso no autorizado	[10]	3%	30%
	AD.8 Interceptación de información (escucha)	[10]	3%	30%
	AD.14 Manipulación de programas	[10]	3%	30%
	AD.15 Denegación de servicio	[10]	3%	30%
COMUNICACIÓN (Red inalámbrica, Red LAN)	DN.1 Fuego	[10]	4%	40%
	DN.2 Daños por agua	[10]	4%	40%
	DN.3 Desastres naturales	[10]	4%	40%
	OI.3 Corte del suministro eléctrico	[10]	3%	30%
	OI.4 Condiciones inadecuadas de temperatura o humedad	[10]	3%	30%
	EFNI.17 Fallo de servicios de comunicaciones	[10]	3%	30%
	EFNI.2 Errores del administrador	[10]	2%	20%
	EFNI.4 Errores de configuración	[10]	2%	20%
	EFNI.6 Errores de secuencia	[10]	2%	20%
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[10]	3%	30%
	AD.1 Manipulación de la configuración	[10]	3%	30%
	AD.2 Suplantación de la identidad del usuario	[10]	3%	30%
	AD.3 Abuso de privilegios de acceso	[10]	3%	30%
	AD.5 Alteración de secuencia	[10]	2%	20%
	AD.6 Acceso no autorizado	[10]	3%	30%
	AD.7 Análisis de tráfico	[10]	3%	30%
	AD.8 Interceptación de información (escucha)	[10]	3%	30%
	AD.16 Robo de equipos	[10]	4%	40%

Activo	Amenazas	Valor del Activo	Probabilidad	Riesgo Acumulado
ELEMENTOS AUXILIARES (UPS, Cable UTP, Fibra óptica, Transformador de aislamiento)	DN.1 Fuego	[7]	4%	28%
	DN.2 Daños por agua	[7]	4%	28%
	DN.3 Desastres naturales	[7]	4%	28%
	OI.3 Corte del suministro eléctrico	[7]	3%	21%
	OI.4 Condiciones inadecuadas de temperatura o humedad	[7]	3%	21%
	AD.16 Robo de equipos	[7]	4%	28%

Tabla 84. Riesgo acumulado: Trazabilidad del servicio y de los datos - Equipamiento (activo)

- **Personal**

Activo	Amenazas	Valor del Activo	Probabilidad	Riesgo Acumulado
ADMINISTRADOR DE SISTEMAS Y BASE DE DATOS	AD.13 Divulgación de información	[7]	3%	21%
	EFNI.16 Indisponibilidad del personal	[7]	1%	7%
OPERADOR	AD.13 Divulgación de información	[7]	3%	21%
	EFNI.16 Indisponibilidad del personal	[7]	1%	7%

Tabla 85. Riesgo acumulado: Trazabilidad del servicio y de los datos – Personal (activo)

- **Instalación**

Activo	Amenazas	Valor del Activo	Probabilidad	Riesgo Acumulado
HOSPITAL III IQUITOS	DN.1 Fuego	[10]	4%	40%
	DN.2 Daños por agua	[10]	4%	40%
	DN.3 Desastres naturales	[10]	4%	40%
	AD.6 Acceso no autorizado	[10]	3%	30%

Tabla 86. Riesgo acumulado: Trazabilidad del servicio y de los datos – Instalación (activo)

- Riesgo repercutido

El riesgo repercutido es el calculado sobre un activo teniendo en cuenta:

- ✓ El impacto repercutido sobre un activo debido a la amenaza.
- ✓ La probabilidad de la amenaza.

El riesgo repercutido se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo el resultado final la degradación del valor del activo con la probabilidad de la amenaza (*Referencia bibliográfica pág.87 Magerit-III-Guía de Técnicas).*

Dimensiones:

[D] disponibilidad
[I] integridad de los datos
[C] confidencialidad de los datos
[A] autenticidad de los usuarios y de la información
[T] trazabilidad del servicio y de los datos

VALORACIÓN:		
8-10	Alto	Daño grave al Hospital
5-7	Medio	Daño importante al Hospital
1-4	Bajo	Daño menor al Hospital
0	Despreciable	Irrelevantes a efectos prácticos

Referencia (Tabla 3-Valor a los activos)

Probabilidad de ocurrencia	Descripción
4%	Ocasional (Sucede alguna vez)
3%	Probable (Incidentes aislados)
2%	Frecuente (Incidentes repetidos)
1%	Remoto (Improbable que suceda)

Referencia (Tabla 06. Probabilidad de ocurrencia)

a) [D] disponibilidad (dimensión)

- **Servicios Internos**

Activo	Amenazas	Valor del Activo	Probabilidad	Riesgo Repercutido
CORREO ELECTRÓNICO INSTITUCIONAL	EFNI.1 Errores de los usuarios	[4]	2%	2%
	EFNI.2 Errores del administrador	[4]	2%	2%
	EFNI.3 Errores de monitorización	[4]	2%	2%
	EFNI.4 Errores de configuración	[4]	2%	2%
	EFNI.6 Errores de secuencia	[4]	2%	2%
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[4]	3%	1%
	AD.1 Manipulación de la configuración	[4]	3%	1%
	AD.2 Suplantación de la identidad del usuario	[4]	3%	1%
	AD.3 Abuso de privilegios de acceso	[4]	3%	1%
	AD.5 Alteración de secuencia	[4]	2%	2%
	AD.6 Acceso no autorizado	[4]	3%	1%
	AD.15 Denegación de servicio	[4]	3%	1%
SISTEMA DE GESTIÓN HOSPITALARIA.	EFNI.1 Errores de los usuarios	[5]	3%	2%
	EFNI.2 Errores del administrador	[5]	3%	2%
	EFNI.3 Errores de monitorización	[5]	2%	3%
	EFNI.4 Errores de configuración	[5]	3%	2%
	EFNI.6 Errores de secuencia	[5]	2%	3%
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[5]	3%	2%
	AD.1 Manipulación de la configuración	[5]	3%	2%
	AD.2 Suplantación de la identidad del usuario	[5]	3%	2%
	AD.3 Abuso de privilegios de acceso	[5]	3%	2%
	AD.5 Alteración de secuencia	[5]	2%	3%
	AD.6 Acceso no autorizado	[5]	3%	2%
	AD.15 Denegación de servicio	[5]	3%	2%

Tabla 87 Riesgo repercutido: Disponibilidad - Servicios internos (activo)

- **Equipamiento**

Activos	Amenazas	Valor del Activo	Probabilidad	Riesgo Repercutido
APLICACIONES (Fox, Linux R.H 5.4,Cenos 5, Asterisk)	EFNI.1 Errores de los usuarios	[6]	2%	4%
	EFNI.2 Errores del administrador	[6]	2%	4%
	EFNI.3 Errores de monitorización	[6]	2%	4%
	EFNI.4 Errores de configuración	[6]	2%	4%
	EFNI.6 Errores de secuencia	[6]	2%	4%
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[6]	3%	3%
	AD.1 Manipulación de la configuración	[6]	3%	3%
	AD.2 Suplantación de la identidad del usuario	[6]	3%	3%
	AD.3 Abuso de privilegios de acceso	[6]	3%	3%
	AD.5 Alteración de secuencia	[6]	2%	4%
	AD.6 Acceso no autorizado	[6]	3%	3%
	AD.15 Denegación de servicio	[6]	3%	3%
	AD.19 Alteración de la información	[6]	4%	2%
	AD.10 Introducción de falsa información	[6]	4%	2%
	AD.12 Destrucción de la información	[6]	4%	2%
	AD.13 Divulgación de información	[6]	4%	2%
	EFNI.12 Vulnerabilidades de los programas (software)	[6]	4%	2%
	EFNI.13 Errores de mantenimiento / actualización de programas (software)	[6]	4%	2%
EQUIPOS (Servidor de aplicaciones y Base de datos, Servidor de Correo, Switch Core, Switch Alcatel, Servidor de Backup, Radio enlace)	DN.1 Fuego	[10]	4%	6%
	DN.2 Daños por agua	[10]	4%	6%
	DN.3 Desastres naturales	[10]	4%	6%
	OI.3 Corte del suministro eléctrico	[10]	3%	7%
	OI.4 Condiciones inadecuadas de temperatura o humedad	[10]	3%	7%
	EFNI.1 Errores de los usuarios	[10]	2%	8%
	EFNI.2 Errores del administrador	[10]	2%	8%
	EFNI.3 Errores de monitorización	[10]	2%	8%
	EFNI.4 Errores de configuración	[10]	2%	8%
	EFNI.5 Difusión de software dañino	[10]	3%	7%
	EFNI.6 Errores de secuencia	[10]	2%	8%
	EFNI.12 Vulnerabilidades de los programas (software)	[10]	4%	6%
	EFNI.13 Errores de mantenimiento / actualización de programas (software)	[10]	4%	6%
	EFNI.14 Errores de mantenimiento / actualización de equipos (hardware)	[10]	4%	6%
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[10]	3%	7%
	AD.16 Robo de equipos	[10]	4%	6%
	AD.1 Manipulación de la configuración	[10]	3%	7%
	AD.2 Suplantación de la identidad del usuario	[10]	3%	7%
	AD.3 Abuso de privilegios de acceso	[10]	3%	7%
	AD.5 Alteración de secuencia	[10]	2%	8%
	AD.6 Acceso no autorizado	[10]	3%	7%
	AD.8 Interceptación de información (escucha)	[10]	3%	7%
	AD.14 Manipulación de programas	[10]	3%	7%
	AD.15 Denegación de servicio	[10]	3%	7%
COMUNICACIÓN (Red inalámbrica, Red LAN)	DN.1 Fuego	[10]	4%	6%
	DN.2 Daños por agua	[10]	4%	6%
	DN.3 Desastres naturales	[10]	4%	6%
	OI.3 Corte del suministro eléctrico	[10]	3%	7%
	OI.4 Condiciones inadecuadas de temperatura o humedad	[10]	3%	7%
	EFNI.17 Fallo de servicios de comunicaciones	[10]	3%	7%
	EFNI.2 Errores del administrador	[10]	2%	8%
	EFNI.4 Errores de configuración	[10]	2%	8%
	EFNI.6 Errores de secuencia	[10]	2%	8%
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[10]	3%	7%
	AD.1 Manipulación de la configuración	[10]	3%	7%
	AD.2 Suplantación de la identidad del usuario	[10]	3%	7%
	AD.3 Abuso de privilegios de acceso	[10]	3%	7%
	AD.5 Alteración de secuencia	[10]	2%	8%
	AD.6 Acceso no autorizado	[10]	3%	7%
	AD.7 Análisis de tráfico	[10]	3%	7%
	AD.8 Interceptación de información (escucha)	[10]	3%	7%
	AD.16 Robo de equipos	[10]	4%	6%

Activo	Amenazas	Valor del Activo	Probabilidad	Riesgo Repercutido
ELEMENTOS AUXILIARES (UPS, Cable UTP, Fibra óptica, Transformador de aislamiento)	DN.1 Fuego	[7]	4%	3%
	DN.2 Daños por agua	[7]	4%	3%
	DN.3 Desastres naturales	[7]	4%	3%
	OI.3 Corte del suministro eléctrico	[7]	3%	4%
	OI.4 Condiciones inadecuadas de temperatura o humedad	[7]	3%	4%
	AD.16 Robo de equipos	[7]	4%	3%

Tabla 88. Riesgo repercutido: Disponibilidad – Equipamiento (activo)

- **Personal**

Activo	Amenazas	Valor del Activo	Probabilidad	Riesgo Repercutido
ADMINISTRADOR DE SISTEMAS Y BASE DE DATOS	AD.13 Divulgación de información	[7]	3%	4%
	EFNI.16 Indisponibilidad del personal	[7]	1%	6%
OPERADOR	AD.13 Divulgación de información	[7]	3%	4%
	EFNI.16 Indisponibilidad del personal	[7]	1%	6%

Tabla 89. Riesgo repercutido: Disponibilidad – Personal (activo)

- **Instalación**

Activo	Amenazas	Valor del Activo	Probabilidad	Riesgo Repercutido
HOSPITAL III IQUITOS	DN.1 Fuego	[10]	4%	6%
	DN.2 Daños por agua	[10]	4%	6%
	DN.3 Desastres naturales	[10]	4%	6%
	AD.6 Acceso no autorizado	[10]	3%	7%

Tabla 90. Riesgo repercutido: Disponibilidad – Instalación (activo)

b) [I] integridad (dimensión)

- **Servicios Internos**

Activo	Amenazas	Valor del Activo	Probabilidad	Riesgo Repercutido
CORREO ELECTRÓNICO INSTITUCIONAL	EFNI.1 Errores de los usuarios	[4]	2%	2%
	EFNI.2 Errores del administrador	[4]	2%	2%
	EFNI.3 Errores de monitorización	[4]	2%	2%
	EFNI.4 Errores de configuración	[4]	2%	2%
	EFNI.6 Errores de secuencia	[4]	2%	2%
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[4]	3%	1%
	AD.1 Manipulación de la configuración	[4]	3%	1%
	AD.2 Suplantación de la identidad del usuario	[4]	3%	1%
	AD.3 Abuso de privilegios de acceso	[4]	3%	1%
	AD.5 Alteración de secuencia	[4]	2%	2%
	AD.6 Acceso no autorizado	[4]	3%	1%
	AD.15 Denegación de servicio	[4]	3%	1%
SISTEMA DE GESTIÓN HOSPITALARIA.	EFNI.1 Errores de los usuarios	[5]	3%	2%
	EFNI.2 Errores del administrador	[5]	3%	2%
	EFNI.3 Errores de monitorización	[5]	2%	3%
	EFNI.4 Errores de configuración	[5]	3%	2%
	EFNI.6 Errores de secuencia	[5]	2%	3%
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[5]	3%	2%
	AD.1 Manipulación de la configuración	[5]	3%	2%
	AD.2 Suplantación de la identidad del usuario	[5]	3%	2%
	AD.3 Abuso de privilegios de acceso	[5]	3%	2%
	AD.5 Alteración de secuencia	[5]	2%	3%
	AD.6 Acceso no autorizado	[5]	3%	2%
	AD.15 Denegación de servicio	[5]	3%	2%

Tabla 91. Riesgo repercutido: Integridad - Servicios internos (activo)

- **Equipamiento**

Activos	Amenazas	Valor del Activo	Probabilidad	Riesgo Repercutido
APLICACIONES (Fox, Linux R.H 5.4,Cenos 5, Asterisk)	EFNI.1 Errores de los usuarios	[6]	2%	4%
	EFNI.2 Errores del administrador	[6]	2%	4%
	EFNI.3 Errores de monitorización	[6]	2%	4%
	EFNI.4 Errores de configuración	[6]	2%	4%
	EFNI.6 Errores de secuencia	[6]	2%	4%
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[6]	3%	3%
	AD.1 Manipulación de la configuración	[6]	3%	3%
	AD.2 Suplantación de la identidad del usuario	[6]	3%	3%
	AD.3 Abuso de privilegios de acceso	[6]	3%	3%
	AD.5 Alteración de secuencia	[6]	2%	4%
	AD.6 Acceso no autorizado	[6]	3%	3%
	AD.15 Denegación de servicio	[6]	3%	3%
	AD.19 Alteración de la información	[6]	4%	2%
	AD.10 Introducción de falsa información	[6]	4%	2%
	AD.12 Destrucción de la información	[6]	4%	2%
	AD.13 Divulgación de información	[6]	4%	2%
	EFNI.12 Vulnerabilidades de los programas (software)	[6]	4%	2%
	EFNI.13 Errores de mantenimiento / actualización de programas (software)	[6]	4%	2%
EQUIPOS (Servidor de aplicaciones y Base de datos, Servidor de Correo, Switch Core, Switch Alcatel, Servidor de Backup, Radio enlace)	DN.1 Fuego	[10]	4%	6%
	DN.2 Daños por agua	[10]	4%	6%
	DN.3 Desastres naturales	[10]	4%	6%
	OI.3 Corte del suministro eléctrico	[10]	3%	7%
	OI.4 Condiciones inadecuadas de temperatura o humedad	[10]	3%	7%
	EFNI.1 Errores de los usuarios	[10]	2%	8%
	EFNI.2 Errores del administrador	[10]	2%	8%
	EFNI.3 Errores de monitorización	[10]	2%	8%
	EFNI.4 Errores de configuración	[10]	2%	8%
	EFNI.5 Difusión de software dañino	[10]	3%	7%
	EFNI.6 Errores de secuencia	[10]	2%	8%
	EFNI.12 Vulnerabilidades de los programas (software)	[10]	4%	6%
	EFNI.13 Errores de mantenimiento / actualización de programas (software)	[10]	4%	6%
	EFNI.14 Errores de mantenimiento / actualización de equipos (hardware)	[10]	4%	6%
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[10]	3%	7%
	AD.16 Robo de equipos	[10]	4%	6%
	AD.1 Manipulación de la configuración	[10]	3%	7%
	AD.2 Suplantación de la identidad del usuario	[10]	3%	7%
	AD.3 Abuso de privilegios de acceso	[10]	3%	7%
	AD.5 Alteración de secuencia	[10]	2%	8%
	AD.6 Acceso no autorizado	[10]	3%	7%
	AD.8 Interceptación de información (escucha)	[10]	3%	7%
	AD.14 Manipulación de programas	[10]	3%	7%
	AD.15 Denegación de servicio	[10]	3%	7%
COMUNICACIÓN (Red inalámbrica, Red LAN)	DN.1 Fuego	[10]	4%	6%
	DN.2 Daños por agua	[10]	4%	6%
	DN.3 Desastres naturales	[10]	4%	6%
	OI.3 Corte del suministro eléctrico	[10]	3%	7%
	OI.4 Condiciones inadecuadas de temperatura o humedad	[10]	3%	7%
	EFNI.17 Fallo de servicios de comunicaciones	[10]	3%	7%
	EFNI.2 Errores del administrador	[10]	2%	8%
	EFNI.4 Errores de configuración	[10]	2%	8%
	EFNI.6 Errores de secuencia	[10]	2%	8%
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[10]	3%	7%
	AD.1 Manipulación de la configuración	[10]	3%	7%
	AD.2 Suplantación de la identidad del usuario	[10]	3%	7%
	AD.3 Abuso de privilegios de acceso	[10]	3%	7%
	AD.5 Alteración de secuencia	[10]	2%	8%
	AD.6 Acceso no autorizado	[10]	3%	7%
	AD.7 Análisis de tráfico	[10]	3%	7%
	AD.8 Interceptación de información (escucha)	[10]	3%	7%
	AD.16 Robo de equipos	[10]	4%	6%

Activo	Amenazas	Valor del Activo	Probabilidad	Riesgo Repercutido
ELEMENTOS AUXILIARES (UPS, Cable UTP, Fibra óptica, Transformador de aislamiento)	DN.1 Fuego	[7]	4%	3%
	DN.2 Daños por agua	[7]	4%	3%
	DN.3 Desastres naturales	[7]	4%	3%
	OI.3 Corte del suministro eléctrico	[7]	3%	4%
	OI.4 Condiciones inadecuadas de temperatura o humedad	[7]	3%	4%
	AD.16 Robo de equipos	[7]	4%	3%

Tabla 92. Riesgo repercutido: Integridad – Equipamiento (activo)

- **Personal**

Activo	Amenazas	Valor del Activo	Probabilidad	Riesgo Repercutido
ADMINISTRADOR DE SISTEMAS Y BASE DE DATOS	AD.13 Divulgación de información	[7]	3%	4%
	EFNI.16 Indisponibilidad del personal	[7]	1%	6%
OPERADOR	AD.13 Divulgación de información	[7]	3%	4%
	EFNI.16 Indisponibilidad del personal	[7]	1%	6%

Tabla 93. Riesgo repercutido: Integridad – Personal (activo)

- **Instalación**

Activo	Amenazas	Valor del Activo	Probabilidad	Riesgo Repercutido
HOSPITAL III IQUITOS	DN.1 Fuego	[10]	4%	6%
	DN.2 Daños por agua	[10]	4%	6%
	DN.3 Desastres naturales	[10]	4%	6%
	AD.6 Acceso no autorizado	[10]	3%	7%

Tabla 94. Riesgo repercutido: Integridad – Instalación (activo)

c) [C] confidencialidad (dimensión)

- **Servicios Internos**

Activo	Amenazas	Valor del Activo	Probabilidad	Riesgo Repercutido
CORREO ELECTRÓNICO INSTITUCIONAL	EFNI.1 Errores de los usuarios	[4]	2%	2%
	EFNI.2 Errores del administrador	[4]	2%	2%
	EFNI.3 Errores de monitorización	[4]	2%	2%
	EFNI.4 Errores de configuración	[4]	2%	2%
	EFNI.6 Errores de secuencia	[4]	2%	2%
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[4]	3%	1%
	AD.1 Manipulación de la configuración	[4]	3%	1%
	AD.2 Suplantación de la identidad del usuario	[4]	3%	1%
	AD.3 Abuso de privilegios de acceso	[4]	3%	1%
	AD.5 Alteración de secuencia	[4]	2%	2%
	AD.6 Acceso no autorizado	[4]	3%	1%
	AD.15 Denegación de servicio	[4]	3%	1%
SISTEMA DE GESTIÓN HOSPITALARIA.	EFNI.1 Errores de los usuarios	[5]	3%	2%
	EFNI.2 Errores del administrador	[5]	3%	2%
	EFNI.3 Errores de monitorización	[5]	2%	3%
	EFNI.4 Errores de configuración	[5]	3%	2%
	EFNI.6 Errores de secuencia	[5]	2%	3%
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[5]	3%	2%
	AD.1 Manipulación de la configuración	[5]	3%	2%
	AD.2 Suplantación de la identidad del usuario	[5]	3%	2%
	AD.3 Abuso de privilegios de acceso	[5]	3%	2%
	AD.5 Alteración de secuencia	[5]	2%	3%
	AD.6 Acceso no autorizado	[5]	3%	2%
	AD.15 Denegación de servicio	[5]	3%	2%

Tabla 95. Riesgo repercutido: Confidencialidad - Servicios internos (activo)

- **Equipamiento**

Activos	Amenazas	Valor del Activo	Probabilidad	Riesgo Repercutido
APLICACIONES (Fox, Linux R.H 5.4,Cenos 5, Asterisk)	EFNI.1 Errores de los usuarios	[6]	2%	4%
	EFNI.2 Errores del administrador	[6]	2%	4%
	EFNI.3 Errores de monitorización	[6]	2%	4%
	EFNI.4 Errores de configuración	[6]	2%	4%
	EFNI.6 Errores de secuencia	[6]	2%	4%
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[6]	3%	3%
	AD.1 Manipulación de la configuración	[6]	3%	3%
	AD.2 Suplantación de la identidad del usuario	[6]	3%	3%
	AD.3 Abuso de privilegios de acceso	[6]	3%	3%
	AD.5 Alteración de secuencia	[6]	2%	4%
	AD.6 Acceso no autorizado	[6]	3%	3%
	AD.15 Denegación de servicio	[6]	3%	3%
	AD.19 Alteración de la información	[6]	4%	2%
	AD.10 Introducción de falsa información	[6]	4%	2%
	AD.12 Destrucción de la información	[6]	4%	2%
	AD.13 Divulgación de información	[6]	4%	2%
	EFNI.12 Vulnerabilidades de los programas (software)	[6]	4%	2%
	EFNI.13 Errores de mantenimiento / actualización de programas (software)	[6]	4%	2%
EQUIPOS (Servidor de aplicaciones y Base de datos, Servidor de Correo, Switch Core, Switch Alcatel, Servidor de Backup, Radio enlace)	DN.1 Fuego	[10]	4%	6%
	DN.2 Daños por agua	[10]	4%	6%
	DN.3 Desastres naturales	[10]	4%	6%
	OI.3 Corte del suministro eléctrico	[10]	3%	7%
	OI.4 Condiciones inadecuadas de temperatura o humedad	[10]	3%	7%
	EFNI.1 Errores de los usuarios	[10]	2%	8%
	EFNI.2 Errores del administrador	[10]	2%	8%
	EFNI.3 Errores de monitorización	[10]	2%	8%
	EFNI.4 Errores de configuración	[10]	2%	8%
	EFNI.5 Difusión de software dañino	[10]	3%	7%
	EFNI.6 Errores de secuencia	[10]	2%	8%
	EFNI.12 Vulnerabilidades de los programas (software)	[10]	4%	6%
	EFNI.13 Errores de mantenimiento / actualización de programas (software)	[10]	4%	6%
	EFNI.14 Errores de mantenimiento / actualización de equipos (hardware)	[10]	4%	6%
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[10]	3%	7%
	AD.16 Robo de equipos	[10]	4%	6%
	AD.1 Manipulación de la configuración	[10]	3%	7%
	AD.2 Suplantación de la identidad del usuario	[10]	3%	7%
	AD.3 Abuso de privilegios de acceso	[10]	3%	7%
	AD.5 Alteración de secuencia	[10]	2%	8%
	AD.6 Acceso no autorizado	[10]	3%	7%
	AD.8 Interceptación de información (escucha)	[10]	3%	7%
	AD.14 Manipulación de programas	[10]	3%	7%
	AD.15 Denegación de servicio	[10]	3%	7%
COMUNICACIÓN (Red inalámbrica, Red LAN)	DN.1 Fuego	[10]	4%	6%
	DN.2 Daños por agua	[10]	4%	6%
	DN.3 Desastres naturales	[10]	4%	6%
	OI.3 Corte del suministro eléctrico	[10]	3%	7%
	OI.4 Condiciones inadecuadas de temperatura o humedad	[10]	3%	7%
	EFNI.17 Fallo de servicios de comunicaciones	[10]	3%	7%
	EFNI.2 Errores del administrador	[10]	2%	8%
	EFNI.4 Errores de configuración	[10]	2%	8%
	EFNI.6 Errores de secuencia	[10]	2%	8%
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[10]	3%	7%
	AD.1 Manipulación de la configuración	[10]	3%	7%
	AD.2 Suplantación de la identidad del usuario	[10]	3%	7%
	AD.3 Abuso de privilegios de acceso	[10]	3%	7%
	AD.5 Alteración de secuencia	[10]	2%	8%
	AD.6 Acceso no autorizado	[10]	3%	7%
	AD.7 Análisis de tráfico	[10]	3%	7%
	AD.8 Interceptación de información (escucha)	[10]	3%	7%
	AD.16 Robo de equipos	[10]	4%	6%

Activo	Amenazas	Valor del Activo	Probabilidad	Riesgo Repercutido
ELEMENTOS AUXILIARES (UPS, Cable UTP, Fibra óptica, Transformador de aislamiento)	DN.1 Fuego	[7]	4%	3%
	DN.2 Daños por agua	[7]	4%	3%
	DN.3 Desastres naturales	[7]	4%	3%
	OI.3 Corte del suministro eléctrico	[7]	3%	4%
	OI.4 Condiciones inadecuadas de temperatura o humedad	[7]	3%	4%
	AD.16 Robo de equipos	[7]	4%	3%

Tabla 96. Riesgo repercutido: Confidencialidad – Equipamiento (activo)

- **Personal**

Activo	Amenazas	Valor del Activo	Probabilidad	Riesgo Repercutido
ADMINISTRADOR DE SISTEMAS Y BASE DE DATOS	AD.13 Divulgación de información	[7]	3%	4%
	EFNI.16 Indisponibilidad del personal	[7]	1%	6%
OPERADOR	AD.13 Divulgación de información	[7]	3%	4%
	EFNI.16 Indisponibilidad del personal	[7]	1%	6%

Tabla 97. Riesgo repercutido: Confidencialidad – Personal (activo)

- **Instalación**

Activo	Amenazas	Valor del Activo	Probabilidad	Riesgo Repercutido
HOSPITAL III IQUITOS	DN.1 Fuego	[10]	4%	6%
	DN.2 Daños por agua	[10]	4%	6%
	DN.3 Desastres naturales	[10]	4%	6%
	AD.6 Acceso no autorizado	[10]	3%	7%

Tabla 98. Riesgo repercutido: Confidencialidad – Instalación (activo)

d) [A] autenticidad de los usuarios y la información (dimensión)

- **Servicios Internos**

Activo	Amenazas	Valor del Activo	Probabilidad	Riesgo Repercutido
CORREO ELECTRÓNICO INSTITUCIONAL	EFNI.1 Errores de los usuarios	[4]	2%	2%
	EFNI.2 Errores del administrador	[4]	2%	2%
	EFNI.3 Errores de monitorización	[4]	2%	2%
	EFNI.4 Errores de configuración	[4]	2%	2%
	EFNI.6 Errores de secuencia	[4]	2%	2%
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[4]	3%	1%
	AD.1 Manipulación de la configuración	[4]	3%	1%
	AD.2 Suplantación de la identidad del usuario	[4]	3%	1%
	AD.3 Abuso de privilegios de acceso	[4]	3%	1%
	AD.5 Alteración de secuencia	[4]	2%	2%
	AD.6 Acceso no autorizado	[4]	3%	1%
	AD.15 Denegación de servicio	[4]	3%	1%
SISTEMA DE GESTIÓN HOSPITALARIA.	EFNI.1 Errores de los usuarios	[5]	3%	2%
	EFNI.2 Errores del administrador	[5]	3%	2%
	EFNI.3 Errores de monitorización	[5]	2%	3%
	EFNI.4 Errores de configuración	[5]	3%	2%
	EFNI.6 Errores de secuencia	[5]	2%	3%
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[5]	3%	2%
	AD.1 Manipulación de la configuración	[5]	3%	2%
	AD.2 Suplantación de la identidad del usuario	[5]	3%	2%
	AD.3 Abuso de privilegios de acceso	[5]	3%	2%
	AD.5 Alteración de secuencia	[5]	2%	3%
	AD.6 Acceso no autorizado	[5]	3%	2%
	AD.15 Denegación de servicio	[5]	3%	2%

Tabla 99. Riesgo repercutido: Autenticidad de los usuarios y la información - Servicios internos (activo)

- **Equipamiento**

Activos	Amenazas	Valor del Activo	Probabilidad	Riesgo Repercutido
APLICACIONES (Fox, Linux R.H 5.4,Cenos 5, Asterisk)	EFNI.1 Errores de los usuarios	[6]	2%	4%
	EFNI.2 Errores del administrador	[6]	2%	4%
	EFNI.3 Errores de monitorización	[6]	2%	4%
	EFNI.4 Errores de configuración	[6]	2%	4%
	EFNI.6 Errores de secuencia	[6]	2%	4%
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[6]	3%	3%
	AD.1 Manipulación de la configuración	[6]	3%	3%
	AD.2 Suplantación de la identidad del usuario	[6]	3%	3%
	AD.3 Abuso de privilegios de acceso	[6]	3%	3%
	AD.5 Alteración de secuencia	[6]	2%	4%
	AD.6 Acceso no autorizado	[6]	3%	3%
	AD.15 Denegación de servicio	[6]	3%	3%
	AD.19 Alteración de la información	[6]	4%	2%
	AD.10 Introducción de falsa información	[6]	4%	2%
	AD.12 Destrucción de la información	[6]	4%	2%
	AD.13 Divulgación de información	[6]	4%	2%
	EFNI.12 Vulnerabilidades de los programas (software)	[6]	4%	2%
	EFNI.13 Errores de mantenimiento / actualización de programas (software)	[6]	4%	2%
EQUIPOS (Servidor de aplicaciones y Base de datos, Servidor de Correo, Switch Core, Switch Alcatel, Servidor de Backup, Radio enlace)	DN.1 Fuego	[10]	4%	6%
	DN.2 Daños por agua	[10]	4%	6%
	DN.3 Desastres naturales	[10]	4%	6%
	OI.3 Corte del suministro eléctrico	[10]	3%	7%
	OI.4 Condiciones inadecuadas de temperatura o humedad	[10]	3%	7%
	EFNI.1 Errores de los usuarios	[10]	2%	8%
	EFNI.2 Errores del administrador	[10]	2%	8%
	EFNI.3 Errores de monitorización	[10]	2%	8%
	EFNI.4 Errores de configuración	[10]	2%	8%
	EFNI.5 Difusión de software dañino	[10]	3%	7%
	EFNI.6 Errores de secuencia	[10]	2%	8%
	EFNI.12 Vulnerabilidades de los programas (software)	[10]	4%	6%
	EFNI.13 Errores de mantenimiento / actualización de programas (software)	[10]	4%	6%
	EFNI.14 Errores de mantenimiento / actualización de equipos (hardware)	[10]	4%	6%
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[10]	3%	7%
	AD.16 Robo de equipos	[10]	4%	6%
	AD.1 Manipulación de la configuración	[10]	3%	7%
	AD.2 Suplantación de la identidad del usuario	[10]	3%	7%
	AD.3 Abuso de privilegios de acceso	[10]	3%	7%
	AD.5 Alteración de secuencia	[10]	2%	8%
	AD.6 Acceso no autorizado	[10]	3%	7%
	AD.8 Interceptación de información (escucha)	[10]	3%	7%
	AD.14 Manipulación de programas	[10]	3%	7%
	AD.15 Denegación de servicio	[10]	3%	7%
COMUNICACIÓN (Red inalámbrica, Red LAN)	DN.1 Fuego	[10]	4%	6%
	DN.2 Daños por agua	[10]	4%	6%
	DN.3 Desastres naturales	[10]	4%	6%
	OI.3 Corte del suministro eléctrico	[10]	3%	7%
	OI.4 Condiciones inadecuadas de temperatura o humedad	[10]	3%	7%
	EFNI.17 Fallo de servicios de comunicaciones	[10]	3%	7%
	EFNI.2 Errores del administrador	[10]	2%	8%
	EFNI.4 Errores de configuración	[10]	2%	8%
	EFNI.6 Errores de secuencia	[10]	2%	8%
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[10]	3%	7%
	AD.1 Manipulación de la configuración	[10]	3%	7%
	AD.2 Suplantación de la identidad del usuario	[10]	3%	7%
	AD.3 Abuso de privilegios de acceso	[10]	3%	7%
	AD.5 Alteración de secuencia	[10]	2%	8%
	AD.6 Acceso no autorizado	[10]	3%	7%
	AD.7 Análisis de tráfico	[10]	3%	7%
	AD.8 Interceptación de información (escucha)	[10]	3%	7%
	AD.16 Robo de equipos	[10]	4%	6%

Activo	Amenazas	Valor del Activo	Probabilidad	Riesgo Repercutido
ELEMENTOS AUXILIARES (UPS, Cable UTP, Fibra óptica, Transformador de aislamiento)	DN.1 Fuego	[7]	4%	3%
	DN.2 Daños por agua	[7]	4%	3%
	DN.3 Desastres naturales	[7]	4%	3%
	OI.3 Corte del suministro eléctrico	[7]	3%	4%
	OI.4 Condiciones inadecuadas de temperatura o humedad	[7]	3%	4%
	AD.16 Robo de equipos	[7]	4%	3%

Tabla 100. Riesgo repercutido: Autenticidad de los usuarios y la información – Equipamiento (activo)

- **Personal**

Activo	Amenazas	Valor del Activo	Probabilidad	Riesgo Repercutido
ADMINISTRADOR DE SISTEMAS Y BASE DE DATOS	AD.13 Divulgación de información	[7]	3%	4%
	EFNI.16 Indisponibilidad del personal	[7]	1%	6%
OPERADOR	AD.13 Divulgación de información	[7]	3%	4%
	EFNI.16 Indisponibilidad del personal	[7]	1%	6%

Tabla 101. Riesgo repercutido: Autenticidad de los usuarios y la información –Personal (activo)

- **Instalación**

Activo	Amenazas	Valor del Activo	Probabilidad	Riesgo Repercutido
HOSPITAL III IQUITOS	DN.1 Fuego	[10]	4%	6%
	DN.2 Daños por agua	[10]	4%	6%
	DN.3 Desastres naturales	[10]	4%	6%
	AD.6 Acceso no autorizado	[10]	3%	7%

Tabla 102. Riesgo repercutido: Autenticidad de los usuarios y la información – Instalación (activo)

e) [T] trazabilidad del servicio y de los datos

- **Servicios Internos**

Activo	Amenazas	Valor del Activo	Probabilidad	Riesgo Repercutido
CORREO ELECTRÓNICO INSTITUCIONAL	EFNI.1 Errores de los usuarios	[4]	2%	2%
	EFNI.2 Errores del administrador	[4]	2%	2%
	EFNI.3 Errores de monitorización	[4]	2%	2%
	EFNI.4 Errores de configuración	[4]	2%	2%
	EFNI.6 Errores de secuencia	[4]	2%	2%
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[4]	3%	1%
	AD.1 Manipulación de la configuración	[4]	3%	1%
	AD.2 Suplantación de la identidad del usuario	[4]	3%	1%
	AD.3 Abuso de privilegios de acceso	[4]	3%	1%
	AD.5 Alteración de secuencia	[4]	2%	2%
	AD.6 Acceso no autorizado	[4]	3%	1%
	AD.15 Denegación de servicio	[4]	3%	1%
SISTEMA DE GESTIÓN HOSPITALARIA.	EFNI.1 Errores de los usuarios	[5]	3%	2%
	EFNI.2 Errores del administrador	[5]	3%	2%
	EFNI.3 Errores de monitorización	[5]	2%	3%
	EFNI.4 Errores de configuración	[5]	3%	2%
	EFNI.6 Errores de secuencia	[5]	2%	3%
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[5]	3%	2%
	AD.1 Manipulación de la configuración	[5]	3%	2%
	AD.2 Suplantación de la identidad del usuario	[5]	3%	2%
	AD.3 Abuso de privilegios de acceso	[5]	3%	2%
	AD.5 Alteración de secuencia	[5]	2%	3%
	AD.6 Acceso no autorizado	[5]	3%	2%
	AD.15 Denegación de servicio	[5]	3%	2%

Tabla 103. Riesgo repercutido: Trazabilidad del servicio y de los datos - Servicios internos (activo)

- **Equipamiento**

Activos	Amenazas	Valor del Activo	Probabilidad	Riesgo Repercutido
APLICACIONES (Fox, Linux R.H 5.4,Cenos 5, Asterisk)	EFNI.1 Errores de los usuarios	[6]	2%	4%
	EFNI.2 Errores del administrador	[6]	2%	4%
	EFNI.3 Errores de monitorización	[6]	2%	4%
	EFNI.4 Errores de configuración	[6]	2%	4%
	EFNI.6 Errores de secuencia	[6]	2%	4%
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[6]	3%	3%
	AD.1 Manipulación de la configuración	[6]	3%	3%
	AD.2 Suplantación de la identidad del usuario	[6]	3%	3%
	AD.3 Abuso de privilegios de acceso	[6]	3%	3%
	AD.5 Alteración de secuencia	[6]	2%	4%
	AD.6 Acceso no autorizado	[6]	3%	3%
	AD.15 Denegación de servicio	[6]	3%	3%
	AD.19 Alteración de la información	[6]	4%	2%
	AD.10 Introducción de falsa información	[6]	4%	2%
	AD.12 Destrucción de la información	[6]	4%	2%
	AD.13 Divulgación de información	[6]	4%	2%
	EFNI.12 Vulnerabilidades de los programas (software)	[6]	4%	2%
	EFNI.13 Errores de mantenimiento / actualización de programas (software)	[6]	4%	2%
EQUIPOS (Servidor de aplicaciones y Base de datos, Servidor de Correo, Switch Core, Switch Alcatel, Servidor de Backup, Radio enlace)	DN.1 Fuego	[10]	4%	6%
	DN.2 Daños por agua	[10]	4%	6%
	DN.3 Desastres naturales	[10]	4%	6%
	OI.3 Corte del suministro eléctrico	[10]	3%	7%
	OI.4 Condiciones inadecuadas de temperatura o humedad	[10]	3%	7%
	EFNI.1 Errores de los usuarios	[10]	2%	8%
	EFNI.2 Errores del administrador	[10]	2%	8%
	EFNI.3 Errores de monitorización	[10]	2%	8%
	EFNI.4 Errores de configuración	[10]	2%	8%
	EFNI.5 Difusión de software dañino	[10]	3%	7%
	EFNI.6 Errores de secuencia	[10]	2%	8%
	EFNI.12 Vulnerabilidades de los programas (software)	[10]	4%	6%
	EFNI.13 Errores de mantenimiento / actualización de programas (software)	[10]	4%	6%
	EFNI.14 Errores de mantenimiento / actualización de equipos (hardware)	[10]	4%	6%
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[10]	3%	7%
	AD.16 Robo de equipos	[10]	4%	6%
	AD.1 Manipulación de la configuración	[10]	3%	7%
	AD.2 Suplantación de la identidad del usuario	[10]	3%	7%
	AD.3 Abuso de privilegios de acceso	[10]	3%	7%
	AD.5 Alteración de secuencia	[10]	2%	8%
	AD.6 Acceso no autorizado	[10]	3%	7%
	AD.8 Interceptación de información (escucha)	[10]	3%	7%
	AD.14 Manipulación de programas	[10]	3%	7%
	AD.15 Denegación de servicio	[10]	3%	7%
COMUNICACIÓN (Red inalámbrica, Red LAN)	DN.1 Fuego	[10]	4%	6%
	DN.2 Daños por agua	[10]	4%	6%
	DN.3 Desastres naturales	[10]	4%	6%
	OI.3 Corte del suministro eléctrico	[10]	3%	7%
	OI.4 Condiciones inadecuadas de temperatura o humedad	[10]	3%	7%
	EFNI.17 Fallo de servicios de comunicaciones	[10]	3%	7%
	EFNI.2 Errores del administrador	[10]	2%	8%
	EFNI.4 Errores de configuración	[10]	2%	8%
	EFNI.6 Errores de secuencia	[10]	2%	8%
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[10]	3%	7%
	AD.1 Manipulación de la configuración	[10]	3%	7%
	AD.2 Suplantación de la identidad del usuario	[10]	3%	7%
	AD.3 Abuso de privilegios de acceso	[10]	3%	7%
	AD.5 Alteración de secuencia	[10]	2%	8%
	AD.6 Acceso no autorizado	[10]	3%	7%
	AD.7 Análisis de tráfico	[10]	3%	7%
	AD.8 Interceptación de información (escucha)	[10]	3%	7%
	AD.16 Robo de equipos	[10]	4%	6%

Activo	Amenazas	Valor del Activo	Probabilidad	Riesgo Repercutido
ELEMENTOS AUXILIARES (UPS, Cable UTP, Fibra óptica, Transformador de aislamiento)	DN.1 Fuego	[7]	4%	3%
	DN.2 Daños por agua	[7]	4%	3%
	DN.3 Desastres naturales	[7]	4%	3%
	OI.3 Corte del suministro eléctrico	[7]	3%	4%
	OI.4 Condiciones inadecuadas de temperatura o humedad	[7]	3%	4%
	AD.16 Robo de equipos	[7]	4%	3%

Tabla 104. Riesgo repercutido: Trazabilidad del servicio y de los datos - Equipamiento (activo)

- **Personal**

Activo	Amenazas	Valor del Activo	Probabilidad	Riesgo Repercutido
ADMINISTRADOR DE SISTEMAS Y BASE DE DATOS	AD.13 Divulgación de información	[7]	3%	4%
	EFNI.16 Indisponibilidad del personal	[7]	1%	6%
OPERADOR	AD.13 Divulgación de información	[7]	3%	4%
	EFNI.16 Indisponibilidad del personal	[7]	1%	6%

Tabla 105. Riesgo repercutido: Trazabilidad del servicio y de los datos – Personal (activo)

- **Instalación**

Activo	Amenazas	Valor del Activo	Probabilidad	Riesgo Repercutido
HOSPITAL III IQUITOS	DN.1 Fuego	[10]	4%	6%
	DN.2 Daños por agua	[10]	4%	6%
	DN.3 Desastres naturales	[10]	4%	6%
	AD.6 Acceso no autorizado	[10]	3%	7%

Tabla 106. Riesgo repercutido: Trazabilidad del servicio y de los datos – Instalación (activo)

3.3. Gestión de riesgos

Para el desarrollo de un adecuado Plan de Contingencia se categorizarán e identificarán los eventos que a continuación presentaremos:

Item	Eventos Controlables
1	Fuego
2	Daños por agua
3	Corte del suministro eléctrico
4	Condiciones inadecuadas de temperatura y/o humedad
5	Fallo de servicios de comunicaciones
6	Errores de los usuarios
7	Errores del administrador
8	Errores de monitorización
9	Errores de configuración
10	Difusión de software dañino
11	Errores de secuencia
12	Alteración accidental de la información
13	Vulnerabilidades de los programas (software)
14	Errores de mantenimiento/actualización de programas (software)
15	Errores de mantenimiento/actualización de equipos (hardware)
16	Caída del sistema por agotamiento de recursos UPS
17	Indisponibilidad del personal
18	Manipulación de la configuración
19	Abuso de privilegios de acceso
20	Alteración de la secuencia
21	Acceso no autorizado
22	Análisis de tráfico
23	Modificación de información
24	Manipulación de programas
25	Denegación de servicio
26	Robo de equipos
27	Alteración de la información

Tabla 107. Eventos Controlables

Item	Eventos No Controlables
1	Desastres naturales (terremotos, inundaciones, etc.)
2	Introducción de falsa información
3	Degradación de la información
4	Destrucción de la información
5	Divulgación de la información
6	Suplantación de la identidad del usuario
7	Intercepción de información (escucha)
8	Corrupción de la información

Tabla 108. Eventos No Controlables

A continuación se evaluará las amenazas que entrarán al Plan de Contingencia. Amenazas en alerta roja entran al Plan de Contingencia.

- **Servicios Internos**

Activo	Amenazas	Impacto	Probabilidad	Riesgo Acumulado	Alerta	Evento
CORREO ELECTRÓNICO INSTITUCIONAL	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[4]	3%	12%	ROJA	C
	AD.1 Manipulación de la configuración	[4]	3%	12%	ROJA	C
	AD.2 Suplantación de la identidad del usuario	[4]	3%	12%	ROJA	NC
	AD.6 Acceso no autorizado	[4]	3%	12%	ROJA	C
SISTEMA DE GESTIÓN HOSPITALARIA	EFNI.1 Errores de los usuarios	[4]	3%	12%	ROJA	C
	EFNI.2 Errores del administrador	[4]	3%	12%	ROJA	C
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[4]	3%	12%	ROJA	C
	AD.1 Manipulación de la configuración	[4]	3%	12%	ROJA	C
	AD.2 Suplantación de la identidad del usuario	[4]	3%	12%	ROJA	NC
	AD.6 Acceso no autorizado	[4]	3%	12%	ROJA	C

Tabla 109 Amenazas seleccionadas – Servicios Internos

- **Equipamiento**

Activo	Amenazas	Impacto	Probabilidad	Riesgo Acumulado	Alerta	Evento
APLICACIONES	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[4]	3%	12%	ROJA	C
	AD.1 Manipulación de la configuración	[4]	3%	12%	ROJA	C
	AD.2 Suplantación de la identidad del usuario	[4]	3%	12%	ROJA	NC
	AD.6 Acceso no autorizado	[4]	3%	12%	ROJA	C
	AD.15 Denegación de servicio	[4]	3%	12%	ROJA	C
	AD.19 Alteración de la información	[4]	4%	16%	ROJA	C
	AD.10 Introducción de falsa información	[4]	4%	16%	ROJA	NC
	AD.12 Destrucción de la información	[4]	4%	16%	ROJA	NC
	AD.13 Divulgación de información	[4]	4%	16%	ROJA	NC
	EFNI.12 Vulnerabilidades de los programas (software)	[3]	4%	12%	ROJA	C
	EFNI.13 Errores de mantenimiento / actualización de programas (software)	[3]	4%	12%	ROJA	C
EQUIPOS	DN.1 Fuego	[4]	4%	16%	ROJA	C
	DN.2 Daños por agua	[4]	4%	16%	ROJA	C
	DN.3 Desastres naturales	[4]	4%	16%	ROJA	NC
	OI.3 Corte del suministro eléctrico	[4]	3%	12%	ROJA	C
	OI.4 Condiciones inadecuadas de temperatura o humedad	[4]	3%	12%	ROJA	C
	EFNI.5 Difusión de software dañino	[4]	3%	12%	ROJA	C
	EFNI.12 Vulnerabilidades de los programas (software)	[4]	4%	16%	ROJA	C
	EFNI.13 Errores de mantenimiento / actualización de programas (software)	[4]	4%	16%	ROJA	C
	EFNI.14 Errores de mantenimiento / actualización de equipos (hardware)	[4]	4%	16%	ROJA	C
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[4]	3%	12%	ROJA	C
	AD.16 Robo de equipos	[4]	4%	16%	ROJA	C
	AD.2 Suplantación de la identidad del usuario	[4]	3%	12%	ROJA	NC
	AD.6 Acceso no autorizado	[4]	3%	12%	ROJA	C
	AD.8 Interceptación de información (escucha)	[4]	3%	12%	ROJA	NC

Activo	Amenazas	Impacto	Probabilidad	Riesgo Acumulado	Alerta	Evento
COMUNICACIONES	DN.1 Fuego	[4]	4%	16%	ROJA	C
	DN.2 Daños por agua	[4]	4%	16%	ROJA	C
	DN.3 Desastres naturales	[4]	4%	16%	ROJA	NC
	OI.3 Corte del suministro eléctrico	[4]	3%	12%	ROJA	C
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	[4]	3%	12%	ROJA	C
	AD.2 Suplantación de la identidad del usuario	[4]	3%	12%	ROJA	NC
	AD.6 Acceso no autorizado	[4]	3%	12%	ROJA	C
	AD.8 Interceptación de información (escucha)	[4]	4%	16%	ROJA	NC
	AD.16 Robo de equipos	[4]	4%	16%	ROJA	C
ELEMENTOS AUXILIARES	DN.1 Fuego	[4]	4%	16%	ROJA	C
	DN.2 Daños por agua	[4]	4%	16%	ROJA	C
	DN.3 Desastres naturales	[4]	4%	16%	ROJA	NC
	OI.3 Corte del suministro eléctrico	[4]	3%	12%	ROJA	C
	AD.16 Robo de equipos	[4]	4%	16%	ROJA	C

Tabla 110 Amenazas seleccionadas – Equipamiento

- **Personal**

Activo	Amenazas	Impacto	Probabilidad	Riesgo Acumulado	Alerta	Evento
ADMINISTRADOR DE SISTEMAS Y BASE DE DATOS	AD.13 Divulgación de información	[4]	3%	12%	ROJA	NC
	EFNI.16 Indisponibilidad del personal	[3]	4%	12%	ROJA	C
OPERADOR	AD.13 Divulgación de información	[4]	3%	12%	ROJA	NC
	EFNI.16 Indisponibilidad del personal	[3]	4%	12%	ROJA	C

Tabla 111 Amenazas seleccionadas – Personal

- **Instalación**

Activo	Amenazas	Impacto	Probabilidad	Riesgo Acumulado	Alerta	Evento
HOSPITAL III IQUITOS	DN.1 Fuego	[4]	4%	16%	ROJA	C
	DN.2 Daños por agua	[4]	4%	16%	ROJA	C
	DN.3 Desastres naturales	[4]	4%	16%	ROJA	NC

Tabla 112 Amenazas seleccionadas – Instalación

3.3.1. Plan de contingencia

Es el proceso de determinar qué hacer si una catástrofe sucede en una empresa. La Institución debe estar lista a la reanudación de las actividades ante una calamidad, misma que podría ser una de las situaciones más difíciles con las que una organización deba enfrentarse. Luego de un desastre, existe la posibilidad de que las edificaciones queden totalmente destruidas, o que no se disponga de ninguno de los recursos, es posible que no se pueda contar con todo el personal, es por esto que tanto el Hospital III-Iquitos, como el personal que labora en la Institución deben estar preparados para salir de dicho problema, por más pequeño que este sea.

- **Servicios Internos**

Activo	Amenazas	Condiciones de Prevención de la Amenaza	Acciones Después de activarse la Contingencia
CORREO ELECRONICO	EFNI.15 Caída del sistema por agotamiento de recursos UPS	- Realizar inspecciones de seguridad periódicamente del equipo UPS. - Asegurar la disponibilidad de un UPS de al menos 2Kva. - Hacer cambio de baterías del equipo UPS al menos una vez al año. - **Obtener una copia de seguridad de la base de datos de usuarios y mensaje antes del agotamiento de la batería UPS del servidor.** - **Asegurar el apagado del servidor de correo de manera correcta, para evitar errores del SO.**	- **Comunicar al jefe de informática.** - **Comunicar a todo el personal del hospital sobre el agotamiento y falla del equipo UPS, mediante el aplicativo que usualmente utilizan(UTALK)** - **Identificar el backup más actual de la base de datos de usuarios y mensajes obtenidos previamente.** - De no tener respuesta de fluido eléctrico para la recarga del UPS por más de una hora se deberá poner en marcha el equipo servidor backup de correo en otra sede de la Red Loreto.
	AD.1 Manipulación de la configuración	- **Asegurar que la clave del administrador del servidor de correo solo sea guardado por el jefe de informática.** - La clave deberá ser mixta, es decir debe comprender entre letras y números. - **El jefe de informática deberá tomar nota sobre todo acceso y/o modificación solicitada por personal de la sede central vía remota.** - **Antes de realizar cualquier modificación deberá obtener una copia de la configuración actual.** - **Borrar periódicamente los temporales del sistema operativo.**	- **Comunicar al jefe de informática.** - **Comunicar a todo el personal del hospital sobre el error de configuración que sufrió el servidor de correo.** - **Identificar el backup más actual de la configuración del servidor de correo.** - **Identificar el backup más actual de la base de datos de usuarios y mensajes obtenidos previamente.** - **De no tener respuesta del servidor por más de una hora por errores de configuración, poner en marcha el equipo backup de correo.**
	AD.2 Suplantación de la identidad del usuario	- Asegurar que la clave del administrador del servidor de correo solo sea guardado por el jefe de informática. - La clave deberá mixta, es decir debe comprender entre letras y números. - Protección del servidor de correo en un lugar de acceso restringido. - Registrar en una bitácora de eventos todas las acciones realizadas por cualquier usuario registrado y con permiso admitido.	- **El jefe de informática deberá realizar las averiguaciones del caso.** - El jefe de informática deberá realizar una entrevista a todo el personal que tiene acceso al servidor. - Verificar el registro de videos, obtenidos de la seguridad del data center.
	AD.6 Acceso no autorizado	- **Solicitar mediante formato correspondiente el acceso al servidor de correo.** - Registrar la hora y el día al personal que solicite acceso al servidor de correo para realizar alguna acción. - **Dar a conocer a la jefatura inmediata sobre el acceso admitido.**	- **Dar a conocer a la jefatura de informática, sobre la magnitud de riesgo.** - **El jefe de informática deberá proponer alguna sanción para el personal no autorizado.** - **El jefe de informática deberá verificar el normal funcionamiento del servidor de correo luego de detectar el acceso no autorizado.**

Activo	Amenazas	Condiciones de Prevención de la Amenaza	Acciones Después de activarse la Contingencia
SISTEMA DE GESTION HOSPITALARIA	EFNI.1 Errores de los usuarios	- **Solicitar mediante formato correspondiente el acceso al SGH el cual deberá estar firmado por su jefe inmediata.** - **Capacitar a los usuarios que tengan acceso al sistema SGH.** - **El jefe de informática deberá dar conocer a la jefatura inmediata del usuario admitido sobre el acceso admitido.**	- **El jefe de informática y/o el operador del SGH deberá verificar mediante la base de datos al usuario que realizó algún error.** - **Se deberá informar al usuario sobre la magnitud de error que realizó y que o quienes puede afectar.** - **El jefe de informática deberá proponer alguna sanción para el usuario.** - **El jefe de informática deberá verificar el normal funcionamiento del servidor de correo luego de detectar el error del usuario.**
	EFNI.2 Errores del administrador del SGH	- **El operador central – administrador del SGH deberá obtener una copia de toda la configuración antes de aplicar los pases – actualizaciones ordenadas por la sede central.** - **El operador central – administrador del SGH deberá verificar diariamente la operatividad de todos los módulos (admisión, consulta externa, farmacia, hospitalización, emergencia.) a través de consultas por correo electrónico a los usuarios responsables**.	- **El operador – administrador del SGH deberá comunicar al jefe de informática sobre los errores que afectaron la operatividad.** - **Comunicar a la sede central - Lima para el apoyo correspondiente.** - **Verificar los registros de errores del sistema y verificar si los errores han sido voluntarios por el administrador.** - **De detectar errores voluntarios, el jefe deberá proponer sanción administrativa a la gerencia de Red.** - **De no tener respuesta del SGH por más de una hora por errores de administrador, se deberá poner en marcha el equipo backup del SGH.**
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	- Realizar inspecciones de seguridad periódicamente del equipo UPS. - Asegurar la disponibilidad de un UPS de al menos 2Kva. - Hacer cambio de baterías del equipo UPS al menos una vez al año. - **Obtener una copia de seguridad de la base de datos de usuarios y mensaje antes del agotamiento de la batería UPS del servidor.** - **Asegurar el apagado del servidor de correo de manera correcta, para evitar errores del SO.**	- **Comunicar al jefe de informática.** - **Comunicar a todo el personal del hospital sobre el agotamiento y falla del equipo UPS.** - **Identificar el backup más actual de la base de datos obtenidos previamente.** - De no tener respuesta de fluido eléctrico para la recarga del UPS por más de una hora se deberá poner en marcha el equipo servidor backup de SGH en otra sede de la Red Loreto.
	AD.1 Manipulación de la configuración	- Asegurar que la clave del administrador del servidor del SGH solo sea guardado por el jefe de informática y/o el operador central. - La clave deberá ser mixta, es decir debe comprender entre letras y números. - **El jefe de informática deberá tomar nota sobre todo acceso y/o modificación solicitada por personal de la sede central vía remota.** - **Antes de realizar cualquier modificación se deberá obtener una copia de la configuración actual.** - **Borrar periódicamente los temporales del sistema operativo.**	- **Comunicar al jefe de informática.** - **Comunicar a todo el personal del hospital sobre el error de configuración que sufrió el servidor del SGH.** - **Identificar el backup más actual de la configuración del servidor del SGH.** - **Identificar el backup más actual de la base de datos de usuarios obtenidos previamente en el servidor backup del SGH.** - **De no tener respuesta del servidor por más de una hora por errores de configuración, poner en marcha el equipo backup.**
	AD.2 Suplantación de la identidad del usuario	- Asegurar que la clave del administrador del servidor del SGH solo sea guardado por el jefe de informática y/o el operador central. - La clave deberá mixta, es decir debe comprender entre letras y números. - Protección del servidor del SGH en un lugar de acceso restringido. - Registrar en una bitácora de eventos todas las acciones realizadas por el operador central.	- **El jefe de informática deberá realizar las averiguaciones del caso.** - El jefe de informática deberá realizar una entrevista a todo el personal que tiene acceso al servidor. - Verificar el registro de videos, obtenidos de la seguridad del data center.
	AD.6 Acceso no autorizado	- **Solicitar mediante formato correspondiente el acceso al servidor del SGH.** - Registrar la hora y el día al personal que solicite acceso al servidor de correo para realizar alguna acción. - **Dar a conocer a la jefatura inmediata sobre el acceso admitido.**	- **Dar a conocer a la jefatura de informática, sobre la magnitud de riesgo.** - **El jefe de informática deberá proponer alguna sanción para el personal no autorizado.** - **El jefe de informática deberá verificar el normal funcionamiento del servidor de correo luego de detectar el acceso no autorizado.**

Tabla 113 Plan de Contingencia – Servicios Internos

- **Equipamiento**

Activo	Amenazas	Condiciones de Prevención de la Amenaza	Acciones Después de activarse la Contingencia
APLICACIONES	EFNI.15 Caída del sistema por agotamiento de recursos UPS	- Realizar inspecciones de seguridad periódicamente del equipo UPS. - Asegurar la disponibilidad de un UPS de al menos 2Kva. - Hacer cambio de baterías del equipo UPS al menos una vez al año. - **Obtener una copia de seguridad de la base de datos de usuarios y mensaje antes del agotamiento de la batería UPS del servidor.** - **Asegurar el apagado del servidor de correo de manera correcta, para evitar errores del SO.**	- **Comunicar al jefe de informática.** - **Comunicar a todo el personal del hospital sobre el agotamiento y falla del equipo UPS.** - **Identificar el backup más actual de la base de datos de usuarios y mensajes obtenidos previamente.** - De no tener respuesta de fluido eléctrico para la recarga del UPS por más de una hora se deberá poner en marcha el equipo servidor backup de correo en otra sede de la Red Loreto.
	AD.1 Manipulación de la configuración	- Asegurar que la clave del administrador del servidor del SGH solo sea guardado por el jefe de informática y/o el operador central. - La clave deberá ser mixta, es decir debe comprender entre letras y números. - **El jefe de informática deberá tomar nota sobre todo acceso y/o modificación solicitada por personal de la sede central vía remota.** - **Antes de realizar cualquier modificación de deberá obtener una copia de la configuración actual.** - **Borrar periódicamente los temporales del sistema operativo.**	- **Comunicar al jefe de informática.** - **Comunicar a todo el personal del hospital sobre el error de configuración que sufrió el servidor del SGH.** - **Identificar el backup más actual de la configuración del servidor del SGH.** - **Identificar el backup más actual de la base de datos de usuarios obtenidos previamente en el servidor backup del SGH.** - **De no tener respuesta del servidor por más de una hora por errores de configuración, poner en marcha el equipo backup.**
	AD.2 Suplantación de la identidad del usuario	- Asegurar que la clave del administrador del servidor de correo solo sea guardado por el jefe de informática. - La clave deberá mixta, es decir debe comprender entre letras y números. - Protección del servidor de correo en un lugar de acceso restringido. - Registrar en una bitácora de eventos todas las acciones realizadas por cualquier usuario registrado y con permiso admitido.	- **El jefe de informática deberá realizar las averiguaciones del caso.** - El jefe de informática deberá realizar una entrevista a todo el personal que tiene acceso al servidor. - Verificar el registro de videos, obtenidos de la seguridad del data center.
	AD.6 Acceso no autorizado	- **Solicitar mediante formato correspondiente el acceso al servidor de correo.** - Registrar la hora y el día al personal que solicite acceso al servidor de correo para realizar alguna acción. - **Dar a conocer a la jefatura inmediata sobre el acceso admitido.**	- **Dar a conocer a la jefatura de informática, sobre la magnitud de riesgo.** - **El jefe de informática deberá proponer alguna sanción para el personal no autorizado.** - **El jefe de informática deberá verificar el normal funcionamiento del servidor de correo luego de detectar el acceso no autorizado.**
	AD.15 Denegación de servicio	- **Verificar de manera periódica que todas las aplicaciones que se encuentran en el hospital estén operativas, es decir consultar a los usuarios mediante correo sobre los errores que mantienen a la actualidad de manera que se otorgue el soporte en el momento.** - **Establecer el inventario actualizado de todos los aplicativos que se encuentren en el hospital**	- **Los usuarios encargados deberán informar mediante correo electrónico al jefe de informática para el soporte necesario.** - **Solicitar el apoyo a la sede central sobre los problemas que suceden a los aplicativos cuyas base de datos y ejecutables se encuentre alojados en dicha sede.** - Manejar las bitácoras de eventos para verificar alguna manera de solucionar los problemas frecuentes y que al pasar el tiempo no se recuerda la manera de solucionar.
	AD.19 Alteración de la información	- **Solicitar mediante formato correspondiente y firmado por el jefe inmediato el tipo de acceso y a los módulos a la cual deberá tener el usuario.** - **Los usuarios deberán ser capacitados por el área de soporte informático para evitar ingresos erróneos a los sistemas y que alteren la información de los asegurados.** - Se deberá realizar reporte o bitácoras de los ingresos realizados durante la semana o durante el mes a los sistemas para ser visados por el jefe inmediato de cada usuario.	- **Informar al jefe de informática sobre las alteraciones detectadas.** - **Se deberá indicar al jefe inmediato de los usuarios sobre las alteraciones realizadas en los sistemas de información.** - **Corregir las alteraciones detectadas con la finalidad de informar a la sede central.**
	AD.10 Introducción de falsa información	- Cada jefe inmediato de los usuarios con acceso a los sistemas, deberán verificar y contrastar los reportes y/o informes en relación a la información física que se maneja en el hospital.	- **El jefe inmediato deberá proponer sanción administrativa a la gerencia de Red, teniendo en cuenta la magnitud de la información falsa ingresada a las aplicaciones y el problema que genera la misma.**

Activo	Amenazas	Condiciones de Prevención de la Amenaza	Acciones Después de activarse la Contingencia
APLICACIONES	AD.12 Destrucción de la información	- **Guardar los backup de información en servidores ubicados en distintos lugares de donde se ubica el servidor principal.** - Verificar periódicamente los distintos sistemas de información en cada área de la periferia del hospital tales como tesorería y mantenimiento.	- **Obtener el backup más reciente para su aplicación en el sistema de información afectado.**
	AD.13 Divulgación de información	- Indicar a la vigilancia del hospital para revisar todo artefacto tecnológico de los trabajadores. - **En los servidores no se deberá permitir el uso de USB's.** - Configurar un servidor de archivos para los trabajadores del hospital a la cual solo tendrán acceso de administración los responsables de soporte informático. - Comunicar y/o advertir a todo el personal del hospital sobre las sanciones existentes por divulgación de información confidencial en digital.	- **Decomisar la información a los usuarios responsables del manejo de información confidencial.** - **Verificar que la información divulgada no fue eliminada y deberá haber una copia del mismo.** - **El jefe de informática deberá proponer frente al jefe inmediato del usuario divulgador una sanción justa y responsable.**
	EFNI.12 Vulnerabilidades de los programas (software)	- Especificar si es un aplicativo desarrollado por la Red o por la Sede Central (Lima) para recomendar la creación del módulo de seguridad mediante perfiles y responsabilidades. - **Cada usuario deberá recibir mediante memorándum su usuario y clave el cual debe ser único e intransferible.** - **Verificar que los manejadores de bases de datos sean verdaderos gestores, es decir que permitan la creación de usuarios y tipos de accesos para manipular las bases de datos.**	- **Investigar las vulnerabilidades sufridas en los aplicativos para detectar los posibles responsables.** - **Verificar la operatividad de los aplicativos luego de haber sido vulnerada.** - **De obtener información errónea del aplicativo a causa de la vulnerabilidad, se deberá informar a los responsables del sistema de las fallas encontradas.** - **Asimismo, el jefe de informática deberá proponer la sanción administrativa correspondiente.**
	EFNI.13 Errores de mantenimiento / actualización de programas (software)	- El jefe de informática deberá verificar si el sistema fue desarrollado por la Red o la Sede Central (Lima) para solicitar el mantenimiento o modificación del mismo. - **Antes se deberá obtener una copia de toda la configuración.** - El jefe de informática y/o el operador central deberá verificar diariamente la operatividad de todos los módulos de cada aplicativo que haya recibido mantenimiento o haya sido actualizado a través de consultas por correo electrónico a los usuarios responsables.	- **El responsable y/o el operador del aplicativo deberá comunicar al jefe de informática sobre los errores que afectaron la operatividad debido al mantenimiento.** - **En caso sea un aplicativo desarrollado por la sede central se deberá comunicar para el apoyo correspondiente.** - **Verificar los registros de errores del sistema y verificar si fueron voluntarios o casualidad del técnico que realizó dicha actualización.** - **De detectar errores voluntarios, el jefe deberá proponer sanción administrativa a la gerencia de Red o el no pago por el mantenimiento realizado.** - **De no tener respuesta del aplicativo por más de una hora por errores de mantenimiento, se deberá poner en marcha el equipo backup y su base de datos.**

Activo	Amenazas	Condiciones de Prevención de la Amenaza	Acciones Después de activarse la Contingencia
EQUIPOS	DN.1 Fuego	- Realizar inspecciones de seguridad periódicamente. - Mantener las conexiones eléctricas seguras en el rango de su vida útil. - Charlas sobre el uso y manejo de extintores de cada uno de los tipos. - Acatar las indicaciones del INDECI, en torno al evento - Contar con una relación de teléfonos de emergencia que incluya a los bomberos, ambulancias, y personal del hospital responsable de las acciones de prevención y ejecución de la contingencia. - Implementar detectores de humo en el data center. - **Mantener actualizado los extintores**.	- Desconectar el fluido eléctrico y cerrar las llaves de gas u otros líquidos inflamables si corresponde. - Tratar de apagar el incendio con extintores. - Comunicar al personal responsable del hospital. - Evacuar el área. - En todo momento se coordinará con el Comité de Contingencia y Seguridad, para las acciones que deban ser efectuadas por ellos. Luego de extinguido el incendio, se deberán realizar las siguientes actividades: - Evaluación de los daños ocasionados al personal, bienes e instalaciones. - En caso de daños del personal prestar asistencia médica inmediata. - Inventario general de la documentación, personal, equipos, etc. y/o recursos afectados, indicando el estado de operatividad de los mismos. - En caso se haya detectado bienes afectados por el evento, se evaluará el caso para determinar la reposición o restauración.
	DN.2 Daños por agua	- Mantener constantemente comunicación con SENAMHI sobre eventos como: lluvias torrenciales y/o tormentas eléctricas. - Mantener firmes los muros de contención cercanas a la sede del hospital. - **Contar con un pozo de agua en la parte posterior del hospital, donde se acumule el agua para su posterior bombeo, este sistema debe ser revisada periódicamente.** - Contar con equipos de bombeo en buenas condiciones.	- Desconectar el fluido eléctrico y cerrar las llaves de gas u otros líquidos inflamables si corresponde. - En caso de inundación se debe evacuar de acuerdo a las disposiciones de la administración a zonas altas donde no llegue el agua (lugares asignadas por las autoridades de INDECI). - Evacuar el agua a través del sistema de bombeo. - Evaluación de los daños ocasionados por el agua sobre la instalación, estanterías, documentos, etc. - Inventario general de documentación, personal, equipos, etc. y/o recursos afectados, indicando el estado de operatividad de los mismos. - Limpieza de las áreas afectadas por la inundación. En caso sea necesario, se utilizarán equipos especializados (motobombas) para realizar el trabajo. - Fumigación del lugar para prevenir aparición del dengue. - En todo momento se coordinará con personal de mantenimiento del hospital, para las acciones que deban ser efectuadas por ellos.
	DN.3 Desastres naturales	- **Contar con un plan de evacuación de las instalaciones del hospital, el mismo que debe ser de conocimiento de todo el personal que labora.** - **Realizar simulacros de evacuación con la participación de todo el personal de la sede del hospital.** - **Mantener las salidas libres de obstáculos.** - **Señalizar todas las salidas.** - **Señalizar las zonas seguras.** - **Definir los puntos de reunión en caso de evacuación.**	- Desconectar el fluido eléctrico y cerrar las llaves de gas u otros líquidos inflamables si corresponde. - Evacuar las oficinas de acuerdo a las disposiciones de la administración utilizando las rutas establecidas durante los simulacros. - Verificar que todo el personal del hospital que labora en el área se encuentren bien. - Brindar los primeros auxilios al personal afectado si fuese necesario. - Alejarse de las lunas (ventanas) para evitar sufrir cortes por roturas y/o desprendimiento de trozos de vidrio. - Evaluación de los daños ocasionados por el sismo sobre las instalaciones físicas, ambientes de trabajo, estanterías, instalaciones eléctricas, documentos, etc. - En caso requerirse personal especializado (ejemplo INDECI), coordinar su presencia a través de la Coordinación Ejecutora del Plan de Contingencias. - Inventario general de documentación, personal, equipos, etc. y/o recursos afectados, indicando el estado de operatividad de los mismos. - Limpieza de las áreas afectadas por el sismo. - En todo momento se coordinará con personal de mantenimiento del hospital, para las acciones que deban ser efectuadas por ellos.

Activos	Amenazas	Condiciones de Prevención de la Amenaza	Acciones Después de activarse la Contingencia
EQUIPOS	OI.3 Corte del suministro eléctrico	- **Durante las operaciones diarias del servicio u operaciones del hospital se contará con los UPS necesarios para asegurar el suministro eléctrico en las estaciones de trabajo consideradas como críticas.** - Asegurar que los equipos UPS cuenten con el mantenimiento debido y con suficiente energía para soportar una operación continua de 30 minutos como máximo. El tiempo variará de acuerdo a la función que cumplan los equipos UPS. - Realizar pruebas periódicas de los equipos UPS para asegurar su correcto funcionamiento. - Contar con UPS para proteger los servidores de correo y desarrollo, previniendo la pérdida de datos durante las labores. La autonomía del equipo UPS no deberá ser menor a 30 minutos. - Contar con UPS para proteger los equipos de vigilancia (cámaras, sistemas de grabación) y de control de acceso a las instalaciones del hospital (puertas, contactos magnéticos, etc.). - **Contar con equipos de luces de emergencia con tolerancia de 15 minutos, accionados automáticamente al producirse el corte de fluido eléctrico, los cuales deben estar instalados en los ambientes críticos.** - Contar con procedimientos operativos alternos para los casos de falta de sistemas, de tal forma que no se afecten considerablemente las operaciones en curso.	- **Informar a la Administración y/o Jefe de Informática del problema presentado.** - **Dar aviso del corte de energía eléctrica en forma oportuna a todas las áreas del hospital y coordinar las acciones necesarias.** - **Las actividades afectadas por la falta de uso de aplicaciones, deberán iniciar sus procesos de contingencia a fin de no afectar las operaciones en curso.** - **En el caso de los equipos que entren en funcionamiento automático con UPS´s, se deberá monitorear el tiempo de autonomía del equipo y no exceder el indicado anteriormente. En caso la interrupción de energía sea mayor a quince minutos, se deberán apagar los servidores de producción, desarrollo y correo hasta que regrese el fluido eléctrico.**
	OI.4 Condiciones inadecuadas de temperatura o humedad	- **Acondicionar adecuadamente y en un nivel de temperatura moderada el área donde se encuentra los activos informáticos, para evitar el recalentamiento de dichos equipos.** - **Verificar que dicha área este libre de filtración de agua ya que causará la humedad dentro de ello provocando daños a los activos.** - Revisar y evaluar los equipos de acondicionamiento periódicamente para así evitar cualquier descongelamiento del hielo formado dentro de ellos.	- **Hacer un inventario de los equipos afectados.** - **Informar al Jefe inmediato sobre el problema causado por la humedad.** - **Solicitar los requerimientos necesarios para dar solución al problema suscitado.** - **Dar mantenimiento a los equipos de acondicionamiento averiados.**
	EFNI.5 Difusión de software dañino	- **Establecimiento de políticas de seguridad para prevenir el uso de aplicaciones no autorizadas en las estaciones de trabajo.** - **Restringir el acceso a Internet a las estaciones de trabajo que por su uso no lo requieran.** - Deshabilitar los puertos de usb, y eliminar los quemadores de CD, etc. en estaciones de trabajo que no lo requieran, para prevenir la conexión de unidades de almacenamiento externo. - Aplicar filtros para restricción de correo entrante, y revisión de archivos adjuntos en los correos y así prevenir la infección de los terminales de trabajo por virus. - **Contar con antivirus instalados en cada estación de trabajo, el mismo que debe estar actualizado permanentemente.** - **Contar con equipos de respaldo ante posibles fallas de las estaciones, para su reemplazo provisional hasta su desinfección y habilitación.**	- **Desconectar la estación infectada de la red del hospital.** - **Verificar si el equipo se encuentra infectado, utilizando un detector de virus actualizado.** - **Rastrear de ser necesario el origen de la infección (archivo infectado, correo electrónico, etc.)** - **Eliminar el agente causante de la infección.** - **Remover el virus del sistema.** - **Probar el sistema.** **En caso no solucionarse el problema :** - **Formatear el equipo.** - **Personalizar la estación para el usuario.** - **Conectar la estación a la red del hospital.** - **Efectuar las pruebas necesarias con el usuario.** - **Solicitar conformidad del servicio de soporte informático**.
	EFNI.12 Vulnerabilidades de los programas (software)	- Especificar si es un aplicativo desarrollado por la Red o por la Sede Central (Lima) para recomendar la creación del modulo de seguridad mediante perfiles y responsabilidades. - **Cada usuario deberá recibir mediante memorándum su usuario y clave el cual debe ser único e intransferible.** - **Verificar que los manejadores de bases de datos sean verdaderos gestores, es decir que permitan la creación de usuarios y tipos de accesos para manipular las bases de datos.**	- **Investigar las vulnerabilidades sufridas en los aplicativos para detectar los posibles responsables.** - **Verificar la operatividad de los aplicativos luego de haber sido vulnerada.** - **De obtener información errónea del aplicativo a causa de la vulnerabilidad, se deberá informar a los responsables del sistema de las fallas encontradas.** - **Asimismo, el jefe de informática deberá proponer la sanción administrativa correspondiente.**

Activos	Amenazas	Condiciones de Prevención de la Amenaza	Acciones Después de activarse la Contingencia
EQUIPOS	AD.2 Suplantación de la identidad del usuario	- **Asegurar que la clave del administrador del servidor de correo solo sea guardado por el jefe de informática.** - La clave deberá mixta, es decir debe comprender entre letras y números. - Protección del servidor de correo en un lugar de acceso restringido. - Registrar en una bitácora de eventos todas las acciones realizadas por cualquier usuario registrado y con permiso admitido.	- **El jefe de informática deberá realizar las averiguaciones del caso.** - El jefe de informática deberá realizar una entrevista a todo el personal que tiene acceso al servidor. - Verificar el registro de videos, obtenidos de la seguridad del data center.
	AD.3 Abuso de privilegios de acceso	- **Hacerle llegar las funciones que le corresponde a cada personal con su área.** - **Habilitar sólo los privilegios relacionados a las funciones que cumple el personal con dicha área; tales como en aplicaciones, programas, web site, entre otros.**	- **De no cumplir solo con sus funciones establecidas, informar a su jefe inmediato para su llamada de atención y si es a mayor el daño proceder a una sanción inmediata.** - **Habilitar los servidores del Domain Name, servidores del Web y servidores del correo en sistemas separados y restringir el acceso a la red a través de un firewall.** - **Es también beneficioso deshabilitar los servicios innecesarios para que el atacante no pueda tener acceso a ningún sistema.**
	AD.5 Alteración de secuencia	- **Aplicación de directivas y/o reglamente de trabajo, para buen uso de los equipos de cómputo, internet y correo institucional.** - **Inventario de cada equipo con su respectivo IP, nombre de la PC y los datos de cada responsable de dicho activo, cabe mencionar: apellidos y nombres completos, número del documento nacional de identidad (DNI), el área al que pertenece, jefe inmediato, entre otros**.	- **Informar al jefe inmediato para su llamada de atención y si es a mayor el daño proceder a una sanción inmediata.** - **Analizar los archivos log** - **Bloquear el equipo en donde se ha realizado una transacción no autorizada.** - **Bloquear la cuenta del usuario utilizada en el ataque.** - **El personal responsable verificará nuevamente cada uno de los puntos de red.** - **Realizar un informe de los eventos sucedidos, de los correctivos y las acciones realizadas y lograr un seguimiento de estos incidentes para observar su evolución y determinar de manera más fácil si vuelve a ocurrir.** - **Si hubiere el caso de que vuelva a ocurrir dicha acción, el responsable de sistemas podrá determinar con exactitud quien es el responsable o el causante y tomar las medidas pertinentes al caso.**
	AD.6 Acceso no autorizado	- **Solicitar mediante formato correspondiente el acceso al servidor de correo.** - Registrar la hora y el día al personal que solicite acceso al servidor de correo para realizar alguna acción. - **Dar a conocer a la jefatura inmediata sobre el acceso admitido.**	- **Dar a conocer a la jefatura de informática, sobre la magnitud de riesgo.** - **El jefe de informática deberá proponer alguna sanción para el personal no autorizado.** - **El jefe de informática deberá verificar el normal funcionamiento del servidor de correo luego de detectar el acceso no autorizado.**
	AD.8 Interceptación de información (escucha)	- **Inventario de cada equipo de comunicación, datos de cada responsable de dicho activo, cabe mencionar: apellidos y nombres completos, número del documento nacional de identidad (DNI), el área al que pertenece, feje inmediato, entre otros; y si es un equipo de comunicación con IP registrarlo adecuadamente.**	- **Informar al jefe inmediato para su llamada de atención y si es a mayor el daño proceder a una sanción inmediata.**
	AD.14 Manipulación de programas	- **Hacerle llegar las funciones que le corresponde a cada personal con su área.** - **Habilitar sólo los privilegios relacionados a las funciones que cumple el personal con dicha área; cabe menciones aplicaciones, programas, web site, entre otros.**	- **De no cumplir solo con sus funciones establecidas, informar a su jefe inmediato para su llamada de atención y si es a mayor el daño proceder a una sanción inmediata.** - **Habilitar los servidores del Domain Name, servidores del Web y servidores del correo en sistemas separados y restringir el acceso a la red a través de un firewall.** - **Es también beneficioso deshabilitar los servicios innecesarios para que el atacante no pueda tener acceso a ningún sistema.**
	AD.15 Denegación de servicio	- **Verificar de manera periódica que todas las aplicaciones que se encuentran en el hospital estén operativas, es decir consultar a los usuarios mediante correo sobre los errores que mantienen a la actualidad de manera que se otorgue el soporte en el momento.** - **Establecer el inventario actualizado de todos los aplicativos que se encuentren en el hospital**	- **Los usuarios encargados deberán informar mediante correo electrónico al jefe de informática para el soporte necesario.** - **Solicitar el apoyo a la sede central sobre los problemas que suceden a los aplicativos cuyas base de datos y ejecutables se encuentre alojados en dicha sede.** - Manejar las bitácoras de eventos para verificar alguna manera de solucionar los problemas frecuentes y que al pasar el tiempo no se recuerda la manera de solucionar.

Activo	Amenazas	Condiciones de Prevención de la Amenaza	Acciones Después de activarse la Contingencia
COMUNICACION	DN.1 Fuego	- Realizar inspecciones de seguridad periódicamente. - Mantener las conexiones eléctricas seguras en el rango de su vida útil. - Charlas sobre el uso y manejo de extintores de cada uno de los tipos. - Acatar las indicaciones del INDECI, en torno al evento - Contar con una relación de teléfonos de emergencia que incluya a los bomberos, ambulancias, y personal del hospital responsable de las acciones de prevención y ejecución de la contingencia. - Implementar detectores de humo en el data center. - **Mantener actualizado los extintores.**	- Desconectar el fluido eléctrico y cerrar las llaves de gas u otros líquidos inflamables si corresponde. - Tratar de apagar el incendio con extintores. - Comunicar al personal responsable del hospital. - Evacuar el área. - En todo momento se coordinará con el Comité de Contingencia y Seguridad, para las acciones que deban ser efectuadas por ellos. Luego de extinguido el incendio, se deberán realizar las siguientes actividades: - Evaluación de los daños ocasionados al personal, bienes e instalaciones. - En caso de daños del personal prestar asistencia médica inmediata. - Inventario general de la documentación, personal, equipos, etc. y/o recursos afectados, indicando el estado de operatividad de los mismos. En caso se haya detectado bienes afectados por el evento, se evaluará el caso para determinar la reposición o restauración.
	DN.2 Daños por agua	- Mantener constantemente comunicación con SENAMHI sobre eventos como: lluvias torrenciales y/o tormentas eléctricas. - Mantener firmes los muros de contención cercanas a la sede del hospital. - **Contar con un pozo de agua en la parte posterior del hospital, donde se acumule el agua para su posterior bombeo, este sistema debe ser revisada periódicamente.** - Contar con equipos de bombeo en buenas condiciones.	- Desconectar el fluido eléctrico y cerrar las llaves de gas u otros líquidos inflamables si corresponde. - En caso de inundación se debe evacuar de acuerdo a las disposiciones de la administración a zonas altas donde no llegue el agua (lugares asignadas por las autoridades de INDECI). - Evacuar el agua a través del sistema de bombeo. - Evaluación de los daños ocasionados por el agua sobre la instalación, estanterías, documentos, etc. - Inventario general de documentación, personal, equipos, etc. y/o recursos afectados, indicando el estado de operatividad de los mismos. - Limpieza de las áreas afectadas por la inundación. En caso sea necesario, se utilizarán equipos especializados (motobombas) para realizar el trabajo. - Fumigación del lugar para prevenir aparición del dengue. - En todo momento se coordinará con personal de mantenimiento del hospital, para las acciones que deban ser efectuadas por ellos.
	DN.3 Desastres naturales	- **Contar con un plan de evacuación de las instalaciones del hospital, el mismo que debe ser de conocimiento de todo el personal que labora.** - **Realizar simulacros de evacuación con la participación de todo el personal de la sede del hospital.** - **Mantener las salidas libres de obstáculos.** - **Señalizar todas las salidas.** - **Señalizar las zonas seguras.** - **Definir los puntos de reunión en caso de evacuación**.	- Desconectar el fluido eléctrico y cerrar las llaves de gas u otros líquidos inflamables si corresponde. - Evacuar las oficinas de acuerdo a las disposiciones de la administración utilizando las rutas establecidas durante los simulacros. - Verificar que todo el personal del hospital que labora en el área se encuentren bien. - Brindar los primeros auxilios al personal afectado si fuese necesario. - Alejarse de las lunas (ventanas) para evitar sufrir cortes por roturas y/o desprendimiento de trozos de vidrio. - Evaluación de los daños ocasionados por el sismo sobre las instalaciones físicas, ambientes de trabajo, estanterías, instalaciones eléctricas, documentos, etc. - En caso requerirse personal especializado (ejemplo INDECI), coordinar su presencia a través de la Coordinación Ejecutora del Plan de Contingencias. - Inventario general de documentación, personal, equipos, etc. y/o recursos afectados, indicando el estado de operatividad de los mismos. - Limpieza de las áreas afectadas por el sismo. - En todo momento se coordinará con personal de mantenimiento del hospital, para las acciones que deban ser efectuadas por ellos.

Activo	Amenazas	Condiciones de Prevención de la Amenaza	Acciones Después de activarse la Contingencia
ELEMENTOS AUXILIARES	DN.1 Fuego	- Realizar inspecciones de seguridad periódicamente. - Mantener las conexiones eléctricas seguras en el rango de su vida útil. - Charlas sobre el uso y manejo de extintores de cada uno de los tipos. - Acatar las indicaciones del INDECI, en torno al evento - Contar con una relación de teléfonos de emergencia que incluya a los bomberos, ambulancias, y personal del hospital responsable de las acciones de prevención y ejecución de la contingencia. - Implementar detectores de humo en el data center. - **Mantener actualizado los extintores.**	- Desconectar el fluido eléctrico y cerrar las llaves de gas u otros líquidos inflamables si corresponde. - Tratar de apagar el incendio con extintores. - Comunicar al personal responsable del hospital. - Evacuar el área. - En todo momento se coordinará con el Comité de Contingencia y Seguridad, para las acciones que deban ser efectuadas por ellos. Luego de extinguido el incendio, se deberán realizar las siguientes actividades: - Evaluación de los daños ocasionados al personal, bienes e instalaciones. - En caso de daños del personal prestar asistencia médica inmediata. - Inventario general de la documentación, personal, equipos, etc. y/o recursos afectados, indicando el estado de operatividad de los mismos. En caso se haya detectado bienes afectados por el evento, se evaluará el caso para determinar la reposición o restauración.
	DN.2 Daños por agua	- Mantener constantemente comunicación con SENAMHI sobre eventos como: lluvias torrenciales y/o tormentas eléctricas. - Mantener firmes los muros de contención cercanas a la sede del hospital. - **Contar con un pozo de agua en la parte posterior del hospital, donde se acumule el agua para su posterior bombeo, este sistema debe ser revisada periódicamente.** - Contar con equipos de bombeo en buenas condiciones.	- Desconectar el fluido eléctrico y cerrar las llaves de gas u otros líquidos inflamables si corresponde. - En caso de inundación se debe evacuar de acuerdo a las disposiciones de la administración a zonas altas donde no llegue el agua (lugares asignadas por las autoridades de INDECI). - Evacuar el agua a través del sistema de bombeo. - Evaluación de los daños ocasionados por el agua sobre la instalación, estanterías, documentos, etc. - Inventario general de documentación, personal, equipos, etc. y/o recursos afectados, indicando el estado de operatividad de los mismos. - Limpieza de las áreas afectadas por la inundación. En caso sea necesario, se utilizarán equipos especializados (motobombas) para realizar el trabajo. - Fumigación del lugar para prevenir aparición del dengue. - En todo momento se coordinará con personal de mantenimiento del hospital, para las acciones que deban ser efectuadas por ellos.

Activo	Amenazas	Condiciones de Prevención de la Amenaza	Acciones Después de activarse la Contingencia
ELEMENTOS AUXILIARES	DN.3 Desastres naturales	- **Contar con un plan de evacuación de las instalaciones del hospital, el mismo que debe ser de conocimiento de todo el personal que labora.** - **Realizar simulacros de evacuación con la participación de todo el personal de la sede del hospital.** - **Mantener las salidas libres de obstáculos.** - **Señalizar todas las salidas.** - **Señalizar las zonas seguras.** - **Definir los puntos de reunión en caso de evacuación**.	- Desconectar el fluido eléctrico y cerrar las llaves de gas u otros líquidos inflamables si corresponde. - Evacuar las oficinas de acuerdo a las disposiciones de la administración utilizando las rutas establecidas durante los simulacros. - Verificar que todo el personal del hospital que labora en el área se encuentren bien. - Brindar los primeros auxilios al personal afectado si fuese necesario. - Alejarse de las lunas (ventanas) para evitar sufrir cortes por roturas y/o desprendimiento de trozos de vidrio. - Evaluación de los daños ocasionados por el sismo sobre las instalaciones físicas, ambientes de trabajo, estanterías, instalaciones eléctricas, documentos, etc. - En caso requerirse personal especializado (ejemplo INDECI), coordinar su presencia a través de la Coordinación Ejecutora del Plan de Contingencias. - Inventario general de documentación, personal, equipos, etc. y/o recursos afectados, indicando el estado de operatividad de los mismos. - Limpieza de las áreas afectadas por el sismo. - En todo momento se coordinará con personal de mantenimiento del hospital, para las acciones que deban ser efectuadas por ellos.
	OI.3 Corte del suministro eléctrico	- **Durante las operaciones diarias del servicio u operaciones del hospital se contará con los UPS necesarios para asegurar el suministro eléctrico en las estaciones de trabajo consideradas como críticas.** - Asegurar que los equipos UPS cuenten con el mantenimiento debido y con suficiente energía para soportar una operación continua de 30 minutos como máximo. El tiempo variará de acuerdo a la función que cumplan los equipos UPS. - Realizar pruebas periódicas de los equipos UPS para asegurar su correcto funcionamiento. - Contar con UPS para proteger los servidores de correo y desarrollo, previniendo la pérdida de datos durante las labores. La autonomía del equipo UPS no deberá ser menor a 30 minutos. - Contar con UPS para proteger los equipos de vigilancia (cámaras, sistemas de grabación) y de control de acceso a las instalaciones del hospital (puertas, contactos magnéticos, etc.). - **Contar con equipos de luces de emergencia con tolerancia de 15 minutos, accionados automáticamente al producirse el corte de fluido eléctrico, los cuales deben estar instalados en los ambientes críticos.**	- **Informar a la Administración y/o Jefe de Informática del problema presentado.** - **Dar aviso del corte de energía eléctrica en forma oportuna a todas las áreas del hospital y coordinar las acciones necesarias.** - **Las actividades afectadas por la falta de uso de aplicaciones, deberán iniciar sus procesos de contingencia a fin de no afectar las operaciones en curso.** - **En el caso de los equipos que entren en funcionamiento automático con UPS´s, se deberá monitorear el tiempo de autonomía del equipo y no exceder el indicado anteriormente. En caso la interrupción de energía sea mayor a quince minutos, se deberán apagar los servidores de producción, desarrollo y correo hasta que regrese el fluido eléctrico.**
	AD.16 Robo de equipos	- **El personal de vigilancia debe estar atento a todo movimiento o desplazamiento ya sea interno como externo de cualquier activo, mediante papeletas de desplazamiento autorizados y firmados por el personal que envía el activo como el que recibe de acuerdo ala conformidad.** - El personal de seguridad debe contar con el control estricto de las personas autorizadas del ingreso alas diferentes áreas. - **El personal que tenga acceso a determinados lugares debe tener su respectiva identificación.** - Se debe contar con una cámara de vigilancia tanto dentro como fuera de cada área donde se encuentra los activos las 24 horas del día. - **Todos los equipos deben contar con sus códigos patrimoniales, y en caso de no contar con ello, asignarles uno.**	- **Un nuevo inventario de todos los activos.** - **El personal encargado del área realizará e informe detallado de lo sustraído y lo presentará a su jefe inmediato.** - **El personal de vigilancia tendrá que revisar las papeletas de desplazamiento de los activos y a la vez el control de ingreso y salida de todo el personal a dicha área donde se produjo la sustracción.** - Revisar minuciosamente las cámaras de vigilancia.

Tabla 114 Plan de Contingencia – Equipamiento

- **Personal**

Activo	Amenazas	Condiciones de Prevención de la Amenaza	Acciones Después de activarse la Contingencia
ADMINISTRADOR DE SISTEMAS Y BASE DE DATOS	AD.13 Divulgación de información	- **Concientizar aún más sobre temas de confidencialidad de información e integridad de datos al personal asignado para dicha función.** - **El jefe de la Unidad de Soporte Informático debe tan sólo de dar privilegios de algunas informaciones que harán posible el desarrollo de su función asignado.** - **Si requiere de alguna u otra información debe ser evaluado y aprobado por el Jefe del área.**	- Informar al jefe inmediato para su sanción inmediata. - Detectar la información divulgada. - Eliminar la información divulgada para evitar sea redistribuida a personas no autorizadas
	EFNI.16 Indisponibilidad del personal	- **Dar conocimiento al Jefe de Informática por parte del reporte de inasistencia del Control de Asistencia.** - **Dar conocimiento al Jefe de Informática por comunicación telefónica por parte del personal o algún familiar.**	- Confirmado la inasistencia del personal, el Jefe de Informática asignará la responsabilidad al Asistente del área capacitado para reemplazar en las funciones que el personal titular de soporte técnico poseía. - El Jefe de Informática solicitará al Jefe inmediato, el reemplazo del personal.
OPERADOR	AD.13 Divulgación de información	- **Concientizar aún más sobre temas de confidencialidad de información e integridad de datos al personal asignado para dicha función.** - **El jefe de la Unidad de Soporte Informático debe tan sólo de dar privilegios de algunas informaciones que harán posible el desarrollo de su función asignado.** - **Si requiere de alguna u otra información debe ser evaluado y aprobado por el Jefe del área.**	- Informar al jefe inmediato para su sanción inmediata. - Detectar la información divulgada. - Eliminar la información divulgada para evitar sea redistribuida a personas no autorizadas
	EFNI.16 Indisponibilidad del personal	- **Dar conocimiento al Jefe de Informática por parte del reporte de inasistencia del Control de Asistencia.** - **Dar conocimiento al Jefe de Informática por comunicación telefónica por parte del personal o algún familiar.**	- Confirmado la inasistencia del personal, el Jefe de Informática asignará la responsabilidad al Asistente del área capacitado para reemplazar en las funciones que el personal titular de soporte técnico poseía. - El Jefe de Informática solicitará al Jefe inmediato, el reemplazo del personal.

Tabla 115 Plan de Contingencia – Personal

- **Instalación**

Activo	Amenazas	Condiciones de Prevención de la Amenaza	Acciones Después de activarse la Contingencia
HOSPITAL III IQUITOS	DN.1 Fuego	- Realizar inspecciones de seguridad periódicamente. - Mantener las conexiones eléctricas seguras en el rango de su vida útil. - Charlas sobre el uso y manejo de extintores de cada uno de los tipos. - Acatar las indicaciones del INDECI, en torno al evento - Contar con una relación de teléfonos de emergencia que incluya a los bomberos, ambulancias, y personal del hospital responsable de las acciones de prevención y ejecución de la contingencia. - Implementar detectores de humo en el data center. - **Mantener actualizado los extintores.**	- Desconectar el fluido eléctrico y cerrar las llaves de gas u otros líquidos inflamables si corresponde. - Tratar de apagar el incendio con extintores. - Comunicar al personal responsable del hospital. - Evacuar el área. - En todo momento se coordinará con el Comité de Contingencia y Seguridad, para las acciones que deban ser efectuadas por ellos. Luego de extinguido el incendio, se deberán realizar las siguientes actividades: - Evaluación de los daños ocasionados al personal, bienes e instalaciones. - En caso de daños del personal prestar asistencia médica inmediata. - Inventario general de la documentación, personal, equipos, etc. y/o recursos afectados, indicando el estado de operatividad de los mismos. En caso se haya detectado bienes afectados por el evento, se evaluará el caso para determinar la reposición o restauración.
	DN.2 Daños por agua	- Mantener constantemente comunicación con SENAMHI sobre eventos como: lluvias torrenciales y/o tormentas eléctricas. - Mantener firmes los muros de contención cercanas a la sede del hospital. - **Contar con un pozo de agua en la parte posterior del hospital, donde se acumule el agua para su posterior bombeo, este sistema debe ser revisada periódicamente.** - Contar con equipos de bombeo en buenas condiciones.	- Desconectar el fluido eléctrico y cerrar las llaves de gas u otros líquidos inflamables si corresponde. - En caso de inundación se debe evacuar de acuerdo a las disposiciones de la administración a zonas altas donde no llegue el agua (lugares asignadas por las autoridades de INDECI). - Evacuar el agua a través del sistema de bombeo. - Evaluación de los daños ocasionados por el agua sobre la instalación, estanterías, documentos, etc. - Inventario general de documentación, personal, equipos, etc. y/o recursos afectados, indicando el estado de operatividad de los mismos. - Limpieza de las áreas afectadas por la inundación. En caso sea necesario, se utilizarán equipos especializados (motobombas) para realizar el trabajo. - Fumigación del lugar para prevenir aparición del dengue. - En todo momento se coordinará con personal de mantenimiento del hospital, para las acciones que deban ser efectuadas por ellos.
	DN.3 Desastres naturales	- **Contar con un plan de evacuación de las instalaciones del hospital, el mismo que debe ser de conocimiento de todo el personal que labora.** - **Realizar simulacros de evacuación con la participación de todo el personal de la sede del hospital.** - **Mantener las salidas libres de obstáculos.** - **Señalizar todas las salidas.** - **Señalizar las zonas seguras.** - **Definir los puntos de reunión en caso de evacuación.**	- Desconectar el fluido eléctrico y cerrar las llaves de gas u otros líquidos inflamables si corresponde. - Evacuar las oficinas de acuerdo a las disposiciones de la administración utilizando las rutas establecidas durante los simulacros. - Verificar que todo el personal del hospital que labora en el área se encuentren bien. - Brindar los primeros auxilios al personal afectado si fuese necesario. - Alejarse de las lunas (ventanas) para evitar sufrir cortes por roturas y/o desprendimiento de trozos de vidrio. - Evaluación de los daños ocasionados por el sismo sobre las instalaciones físicas, ambientes de trabajo, estanterías, instalaciones eléctricas, documentos, etc. - En caso requerirse personal especializado (ejemplo INDECI), coordinar su presencia a través de la Coordinación Ejecutora del Plan de Contingencias. - Inventario general de documentación, personal, equipos, etc. y/o recursos afectados, indicando el estado de operatividad de los mismos. - Limpieza de las áreas afectadas por el sismo. - En todo momento se coordinará con personal de mantenimiento del hospital, para las acciones que deban ser efectuadas por ellos.

Tabla 116 Plan de Contingencia – Instalación

CAPÍTULO IV: RESULTADO Y DISCUSIÓN

PRIMER INDICADOR A EVALUAR

Cantidad de Prevención de la Amenaza de Servicios Internos

Activo	Sin Plan de Contingencia	Con Plan de Contingencia
CORREO ELECRONICO	7	17
SISTEMA DE GESTION HOSPITALARIA	12	22
TOTAL	**19**	**39**

Se establece que para las amenazas de los Servicios Internos hemos identificados 39 posibles prevenciones con Plan de Contingencia en relación a los **19** existente sin Plan de Contingencia por la experiencia del actual jefe de informática (***referencia Tabla 113 Plan de Contingencia – Servicios Internos)***

Cantidad de Prevención de la Amenaza de Equipamiento

Activo	Sin Plan de Contingencia	Con Plan de Contingencia
APLICACIONES	16	35
EQUIPOS	30	52
COMUNICACION	19	48
ELEMENTOS AUXILIARES	14	59
TOTAL	**79**	**194**

Se establece que para las amenazas de los Equipamiento internos hemos identificados 194 posibles prevenciones con Plan de Contingencia en relación a los **79** existente sin Plan de Contingencia por la experiencia del actual jefe de informática (***referencia Tabla 114 Plan de Contingencia – Equipamiento)***

Cantidad de Prevención de la Amenaza del Personal

Activo	Sin Plan de Contingencia	Con Plan de Contingencia
ADMINISTRADOR DE SISTEMAS Y BASE DE DATOS	4	5
OPERADOR	**4**	**5**
TOTAL	**8**	**10**

Se establece que para las amenazas del Personal hemos identificados 10 posibles prevenciones con Plan de Contingencia en relación a los **8** existente sin Plan de Contingencia por la experiencia del actual del actual jefe de informática (***referencia Tabla 115 Plan de Contingencia – Personal)***

Cantidad de Prevención de la Amenaza De la Instalación

Activo	Sin Plan de Contingencia	Con Plan de Contingencia
HOSPITAL III IQUITOS	8	17
TOTAL	**8**	**17**

Se establece que para las amenazas de la Instalación hemos identificados 17 posibles prevenciones con Plan de Contingencia en relación a los **8** existente sin Plan de Contingencia por la experiencia del actual jefe de informática (***referencia Tabla 116 Plan de Contingencia – Instalación)***

SEGUNDO INDICADOR A EVALUAR

Cantidad de Acciones después de activarse la contingencia en los Servicios Internos

Activo	Sin Plan de Contingencia	Con Plan de Contingencia
CORREO ELECRONICO	12	15
SISTEMA DE GESTION HOSPITALARIA	21	24
TOTAL	**33**	**39**

Se establece que para las Contingencias ocurridas de los Servicios Internos hemos identificados 39 posibles acciones con Plan de Contingencia en relación a los 33 existente sin Plan de Contingencia por la experiencia del actual jefe de informática (***referencia Tabla 113 Acciones después de activarse la contingencia – Servicios Internos)***.

Cantidad de Acciones después de activarse la contingencia de Equipamiento

Activo	Sin Plan de Contingencia	Con Plan de Contingencia
APLICACIONES	31	35
EQUIPOS	43	72
COMUNICACION	**19**	**47**
ELEMENTOS AUXILIARES	**7**	**33**
TOTAL	**100**	**187**

Se establece que para las amenazas de Equipamiento hemos identificados 187 posibles acciones con Plan de Contingencia en relación a los **100** existentes sin Plan de Contingencia por la experiencia del actual jefe de informática (***referencia Tabla 114 Acciones después de activarse la contingencia – Equipamiento)***

Cantidad de Prevención de la Amenaza del Personal

Activo	Sin Plan de Contingencia	Con Plan de Contingencia
ADMINISTRADOR DE SISTEMAS Y BASE DE DATOS	0	5
OPERADORES	**0**	**5**
TOTAL		**10**

Se establece que para las amenazas del Personal hemos identificados 10 posibles acciones con Plan de Contingencia y ninguna sin Plan de Contingencia ya que aún no se dio la situación (***referencia Tabla 115 Plan de Contingencia – Personal)***

Cantidad de Prevención de la Amenaza de la Instalación

Activo	Sin Plan de Contingencia	Con Plan de Contingencia
HOSPITAL III IQUITOS	0	25
TOTAL	**0**	**25**

Se establece que para las amenazas de la Instalación hemos identificados 25 posibles acciones con Plan de Contingencia y ninguna sin Plan de Contingencia ya que aún no se dio la situación (***referencia Tabla 116 Plan de Contingencia – Personal)***

TERCER INDICADOR A EVALUAR

Tiempo de respuesta frente a las amenazas

Se tomará un tiempo menos de lo establecido al utilizar el Plan de Contingencia al momento de dar solución a los problemas suscitados por la amenazas, identificados que ponen en riesgo a los activos del Hospital III-ESSALUD

Activo	Problema / riesgo/Contingencia	Sin Plan de Contingencia	Nivel Sin Plan de Contingencia	Con Plan de Contingencia	Nivel Con Plan de Contingencia
CORREO ELECRONICO	Manipulación de la configuración	**1 hora**	DEFICIENTE	**30 min**	REGULAR
SISTEMA DE GESTION HOSPITALARIA	Errores del administrador del SGH	**45 min**	DEFICIENTE	**10 min**	EFICIENTE
	Manipulación de la configuración	**1 hora**	DEFICIENTE	**20 min**	REGULAR
APLICACIONES	Manipulación de la configuración	**45 min**	DEFICIENTE	**20 min**	REGULAR
	Vulnerabilidades de los programas (software)	**45 min**	DEFICIENTE	**30 min**	REGULAR
	Errores de mantenimiento / actualización de programas (software)	**1 hora 1/2**	DEFICIENTE	**30 min**	REGULAR

Activo	Problema / riesgo/Contingencia	Sin Plan de Contingencia	Nivel Sin Plan de Contingencia	Con Plan de Contingencia	Nivel Con Plan de Contingencia
EQUIPOS	Difusión de software dañino	**1 hora**	DEFICIENTE	**30 min**	REGULAR
	Abuso de privilegios de acceso	**30 min**	REGULAR	**10 min**	EFICIENTE
	Manipulación de programas	**45 min**	DEFICIENTE	**20 min**	**REGULAR**
COMUNICACIONES	Análisis de tráfico	**20 min**	REGULAR	**10 min**	EFICIENTE
ADMINISTRADOR DE SISTEMAS Y BASE DE DATOS	Indisponibilidad del personal	**1 hora**	DEFICIENTE	**30 min**	REGULAR
OPERADOR	Indisponibilidad del personal	**1 hora**	DEFICIENTE	**30 min**	REGULAR

PRIMER INDICADOR A EVALUAR

Entonces teniendo en cuenta el índice de evaluación **el hospital se encuentra en la actualidad en un nivel REGULAR** de **Prevención de Amenaza de Servicios Internos** sin un plan de contingencia, lo que mediante la aplicación del mismo se **encontraría en un nivel BUENO**.

Entonces teniendo en cuenta el índice de evaluación **el hospital se encuentra en la actualidad en un nivel BUENO** de **Prevención de la Amenaza de Equipamiento** sin un plan de contingencia.

Entonces teniendo en cuenta el índice de evaluación **el hospital se encuentra en la actualidad en un nivel BUENO** de **Prevención de la Amenaza del Personal** sin un plan de contingencia.

Entonces teniendo en cuenta el índice de evaluación **el hospital se encuentra en la actualidad en un nivel REGULAR** de **Prevención de la Amenaza de la Instalación** sin un plan de contingencia, lo que mediante la aplicación del mismo se **encontraría en un nivel BUENO**.

SEGUNDO INDICADOR A EVALUAR

Entonces teniendo en cuenta el índice de evaluación **el hospital se encuentra en la actualidad en un nivel BUENO** de **Acciones después de activarse la contingencia en los Servicios Internos** sin un plan de contingencia, lo que mediante la aplicación del mismo se encontraría en un nivel BUENO.

Entonces teniendo en cuenta el índice de evaluación **el hospital se encuentra en la actualidad en un nivel BUENO** de **Acciones después de activarse la contingencia De Equipamiento** sin un plan de contingencia.

En la actualidad y hasta la fecha no se dieron situaciones de **Amenaza del Personal** como también ni de **Amenaza de la Instalación.**

TERCER INDICADOR A EVALUAR

Así mismo, se **mejoró el tiempo de respuesta** a los problemas ocurridos.

CAPÍTULO V: CONCLUSIONES

- Se identificó lo activos con las que cuenta el Hospital III-Iquitos, lo cual nos permitió establecer las medidas de seguridad para su protección adecuada.

- Así como se llegó a identificar los activos de dicha sede, también identificamos las amenazas con las que cuentan; con la cual se llegó a la conclusión de que todo tipo de activo ya sea informático o no, siempre serán vulnerables a cualquier tipo de amenazas, y si no se cuenta con las medidas necesarias o la aplicabilidad de una metodología para su protección, podría ocasionar muchos daños a cualquier institución, tanto económico, como también la pérdida de información y afectar de manera directa la operatividad de éste.

- Con la ayuda de MAGERIT, se identificó las salvaguardas con la cual contaremos para poder minimizar los riesgos a las que están expuestos los activos identificados; y así tener una idea clara de cómo actuar frente a ellos ante cualquier incidencia.

- Se formuló el Plan de Contingencia para cada activo, frente a las amenazas más sobresalientes, describiendo las prevenciones y acciones a tomar para minimizar el impacto de los riesgos en un tiempo considerable y mejorado.

CAPÍTULO VI: RECOMENDACIONES

- Hacer de conocimiento al personal informático el contenido del presente Plan de Contingencia, con la finalidad de instruirlos adecuadamente.
- El personal que asumirá los roles establecidos en el plan de contingencia debe ser capacitado anualmente en sus funciones.
- Se debe tener una adecuada política de seguridad orientada a proteger todos los recursos informáticos.
- El Plan de Contingencia debe ser actualizado anualmente, así mismo revisado/evaluado cuando se materialice u ocurra una amenaza.
- Hacer llegar las distintas necesidades de requerimientos a la Gerencia de la Red Asistencial Loreto, para la protección de los distintos activos con las que cuenta el Hospital III Iquitos, como también el de un personal capacitado en el tema de Seguridad.
- Y a la vez también informar a la oficina de la Unidad de Soporte Informático sede central Lima, sobre la situación real en la que se encuentra la USI de la Red Asistencial Loreto.

BIBLIOGRAFÍA

- **[Magerit-I-Metodo:2006]**

  Ministerio de Administración Públicas, Madrid 20 Junio del 2006, "MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgo de los Sistemas de Información, I – Método", Versión 1.1, MAP, http://publicaciones.administracion.es.

- **[Magerit-II- Catálogo de Elementos:2006]**

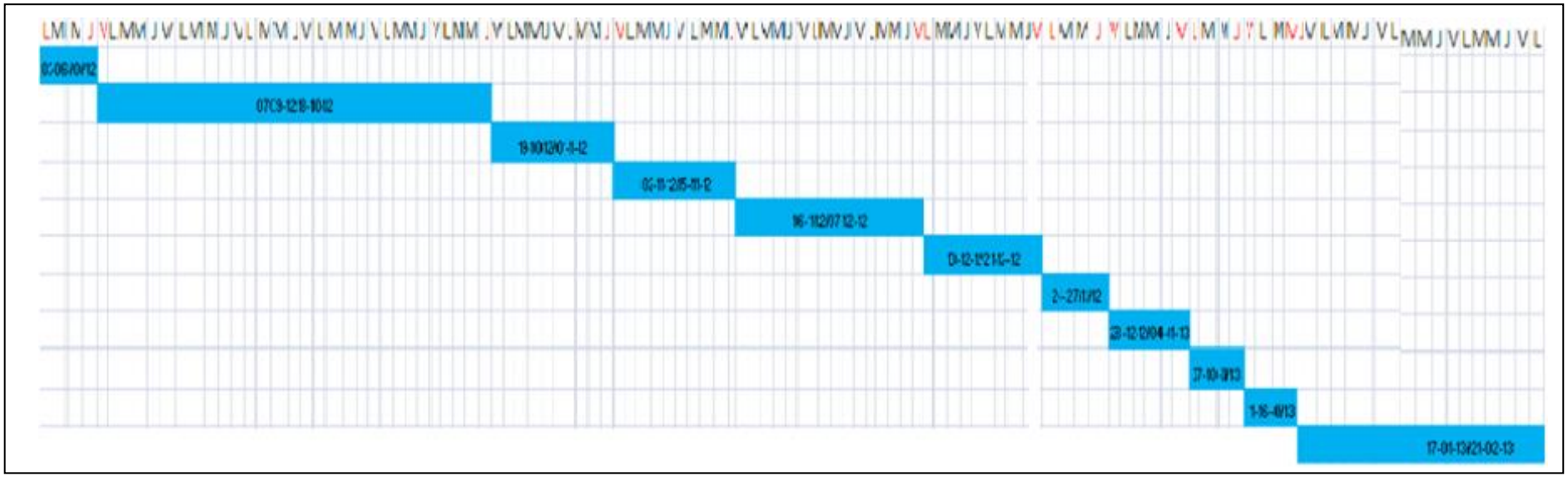
  Ministerio de Administración Públicas, Madrid 20 Junio del 2006, "MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgo de los Sistemas de Información, II – Catálogo de Elementos", Versión 1.1, MAP, http://publicaciones.administracion.es.

- **[Magerit-III- Guía de Técnicas :2006]**

  Ministerio de Administración Públicas, Madrid 20 Junio del 2006, "MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgo de los Sistemas de Información, III – Guía de Técnicas", Versión 1.1, MAP, http://publicaciones.administracion.es.

ANEXO

TAREA	DURACION	COMIENZO	FIN
DETERMINACION DE LIMITES DE TRABAJO	4 DIAS	03/09/2012	06/09/2012
INDENTIFICACION DE ACTIVOS	30 DIAS	07/09/2012	18/10/2012
DEPENDENCIA DE ACTIVOS	10 DIAS	19/10/2012	01/11/2012
VALORACION DE ACTIVOS	10 DIAS	02/11/2012	15/11/2012
IDENTIFICACION DE AMENAZAS	16 DIAS	16/11/2012	07/12/2012
VALORACION DE AMENAZAS	10 DIAS	10/12/2012	21/12/2012
IDENTIFICACION DE SALVAGUARDAS	4 DIAS	24/12/2012	27/12/2012
VALORACION DE SALVAGUARDAS	6 DIAS	28/12/2012	04/01/2013
ESTIMACION DEL IMPACTO	4 DIAS	07/01/2013	10/01/2013
ESTIMACION DEL RIESGO	4 DIAS	11/01/2013	16/01/2013
PLAN DE CONTINGENCIA	26 DIAS	17/01/2013	21/01/2013



ANEXO Nº01 DURACIÓN ESTIMADA DE EJECUCIÓN DEL PROYECTO

ANEXO Nº 02- ENTREVISTA

Se le formuló las siguientes preguntas a las personas entrevistadas Sr. Roner Ruiz Utia y al Sr. Giancarlo Pinedo Picciotti.

1. ¿Se han adoptado medidas de seguridad en el área de la Unidad de Soporte Informático?

   Rpta. No, ya que no cuentan con alguna metodología, norma, o plan de contingencia puesta en práctica.

2. ¿Existen una persona responsable de la seguridad?

   Rpta. No, porque sólo existe el personal a cargo (operador), en la sede central del Hospital III-Iquitos-EsSalud.

3. ¿Se ha dividido la responsabilidad para tener un mejor control de la seguridad?

   Rpta. No, por falta de personal.

4. ¿Existe personal de vigilancia en la institución?

   Rpta. Si, personal contratado ajeno a la institución ESVISAC

5. ¿Existe una clara definición de funciones entre los puestos clave?

   Rpta. Si, por difusión de la institución para cada personal.

6. ¿Se controla el trabajo fuera de horario?

   Rpta. No, ya que el personal de vigilancia solo controla la hora de entrada y salida del personal de la institución.

7. ¿Se registran las acciones de los operadores para evitar que realicen algunas pruebas que puedan dañar los sistemas?

   Rpta. No, el operador es el encargado del área en la sede central del Hospital III-Iquitos, y nadie lleva el control de sus actividades o acciones.

8. ¿Existe vigilancia a la entrada del departamento de cómputo las 24 horas?

   Rpta. No, vigilancia solo en la puerta principal a la entrada del Hospital III-Iquitos.

9. ¿Se permite el acceso a los archivos y programas a los programadores, analistas y operadores?

   Rpta. Si, manejan archivos compartidos y sin privilegios.

10. ¿Se ha instruido a estas personas sobre qué medidas tomar en caso de que alguien pretenda entrar sin autorización?

    Rpta. Si, informar al jefe de la USI (Unidad de Soporte Informático) sobre lo suscitado.

11. ¿El área donde se encuentra la computadora a que amenazas está expuesta?

    Rpta. Está expuesta a las inundaciones e incendios, a la mano del hombre; como robos, sabotajes, entre otros.

12. ¿El centro de cómputo tiene salida al exterior?

    Rpta. Si

13. ¿Se registra el acceso al área de cómputo de personas ajenas a la unidad de informática?

    Rpta. No, ya que no existe ningún personal dedicado a ello.

14. ¿Se vigilan la moral y comportamiento del personal de la unidad de informática con el fin de mantener una buena imagen y evitar un posible fraude?

    Rpta. Si, el Operador es el encargado a la vez de evaluar la personalidad de todo aquel que esta de apoyo en el área de la USI.

15. ¿Existe algún tipo de alarma para cualquier desastre natural?

    Rpta. No

16. ¿Existen extintores de fuego?

    Rpta. Si

17. ¿Se ha capacitado al personal en el manejo de los extintores?

    Rpta. Si, por el personal de bomberos o defensa civil cada cierto tiempo.

18. ¿Los interruptores de energía están debidamente protegidos, etiquetados y sin obstáculos para alcanzarlos?

    Rpta. Si, evaluados por el personal de mantenimiento.

19. ¿Sabe que hacer el operador del departamento de cómputo, en caso de que ocurra una emergencia ocasionado por fuego?

    Rpta. Si, ya que fue capacitado para aquello.

20. ¿El personal ajeno a operación sabe qué hacer en el caso de una emergencia (incendio)?

    Rpta. Si, ya que la capacitación fue para todos.

21. ¿Existe salida de emergencia?

    Rpta. Si

22. ¿Esta puerta es posible abrirla?

    Rpta. Si, tanto dentro como por fuera.

23. ¿Se revisa frecuentemente que no esté abierta o descompuesta la cerradura de esta puerta y de las ventanas, si es que existen?

    Rpta. Si, por el personal de mantenimiento.

24. ¿Se ha capacitado a todo el personal en la forma en que se deben desalojar las instalaciones en caso de emergencia?

    Rpta. Si, por defensa civil.

25. Se ha tomado medidas para minimizar la posibilidad de fuego:

    Rpta. Si, evitando artículos inflamables en el departamento de cómputo, prohibiendo fumar a los operadores en el interior, vigilando y manteniendo el sistema eléctrico, etc.

26. ¿Se ha prohibido a los operadores el consumo de alimentos y bebidas en el interior del departamento de cómputo para evitar daños al equipo?

    Rpta. Si, por orden de gerencia.

27. ¿Se cuenta con copias de los archivos en lugar distinto al de la computadora?

    Rpta. Si, en una computadora de respaldo.

28. ¿Se tienen establecidos procedimientos de actualización a estas copias?

    Rpta. Si, emitidos por sede central de Lima.

29. ¿Existe departamento de auditoría interna en la sede central del Hospital III-Iquitos?

    Rpta. Si

30. ¿Este departamento de auditoría interna conoce todos los aspectos de los sistemas?

    Rpta. No, solo aspectos administrativos.

31. ¿Se auditan los sistemas en operación?

    Rpta. No, por falta de conocimiento.

32. ¿Cuándo se efectúan modificaciones a los programas, a iniciativa de quién es?

    Rpta. Tanto del jefe de informática como del operador.

33. ¿La solicitud de modificaciones a los programas se hace en forma?

    Rpta. En forma oral y escrita.

34. Una vez efectuadas las modificaciones, ¿se presentan las pruebas a los interesados?

    Rpta. Si.

35. ¿Existe control estricto en las modificaciones?

    Rpta. Si.

36. ¿Se revisa que tengan la fecha de las modificaciones cuando se hayan efectuado?

    Rpta. Si

37. Si se tienen terminales conectadas, ¿se ha establecido procedimientos de operación?

    Rpta. Si, emitidos por sede central de Lima.

38. Se verifica identificación:

    Rpta. De la terminal y el usuario

39. ¿Se ha establecido a que información se puede tener acceso y por qué persona?

    Rpta. Si, mediante privilegios de usuarios.

ANEXO Nº 03 PROPUESTA PRESUPUESTAL

DESCRIPCIÓN	CANTIDAD	COSTO UNITARIO S/.	COSTO TOTAL S/.
UPS 500 KW	1	250.00	27,750.00
SERVIDOR	2	10,000.00	20,000.00
SWITCH DE DISTRIBUCION ADMINISTRABLE	1	12,000.00	12,000.00
SWITCH CORE PUERTOS FIBRA OPTICA	1	18,000.00	18,000.00
MANTENIMIENTO PREVENTIVO DE EQUIPOS DE COMPUTO	CADA 6 MESES	50.00	
MANTENIMIENTO PREVENTIVO SERVIDORES	ANUAL	150.00	
PRESUPUESTO TOTAL			S/. 77,750.00

Cabe mencionar que el mantenimiento preventivo de equipos de cómputo se realizará cada 6 meses, esto quiere decir que estaríamos hablando de 111 equipos por 50 soles, teniendo un costo de 5,550 soles en gastos por mantenimiento.

Como también del mantenimiento preventivo de equipos de servidores, que se realizaría anualmente, esto quiere decir que estaríamos hablando de 1 servidor con la que contamos, más dos que solicitamos teniendo 3 servidores por 150 soles, teniendo un costo de 450 soles anuales en gastos por mantenimiento.

.

ANEXO Nº04

ACTA DE CONFORMIDAD DE LOS INDICADORES, DE LAS PREVENCIONES Y ACCIONES UTILIZADAS POR LA UNIDAD DE SOPORTE INFORMÀTICO DE LA RED ASISTENCIAL LORETO PARA SALVAGUARDAR LOS ACTIVOS EXISTENTES EN EL HOSPITAL III – IQUITOS-RALO

INDICADORES	ÍNDICES	HERRAMIENTA
CANTIDAD DE CONDICIONES DE PREVENCIÓN DE LAS AMENAZAS.	➢ > 10 - BUENO ➢ 5 - 10 - REGULAR ➢ < 5 - DEFICIENTE	➢ ENTREVISTA CON EL JEFE DE INFORMATICA ➢ OBSERVACION DIRECTA IN SITU AL HOSPITAL ➢ INVENTARIO DE ACIVOS
CANTIDAD DE SALVAGUARDAS O ACCIONES DESPUÉS DE ACTIVARSE LA CONTINGENCIA.	➢ > 10 – BUENO ➢ 5 - 10 - REGULAR ➢ < 5 - DEFICIENTE	➢ ENTREVISTA CON EL JEFE DE MANTENIMIENTO Y DE SOPORTE INFORMÁTICO
TIEMPO DE RESPUESTA FRENTE A ALAS AMENAZAS.	➢ <= 10 MIN - EFICIENTE ➢ 10 - 30 MIN – REGULAR ➢ > 30 – DEFICIENTE	➢ APLICACIÓN DEL PLAN DE CONTINGENCIA

- **Servicios Internos**

Activo	Amenazas	Prevención de la Amenaza	Acciones que toman
CORREO ELECRONICO	EFNI.15 Caída del sistema por agotamiento de recursos UPS	- **Obtener una copia de seguridad de la base de datos de usuarios y mensaje antes del agotamiento de la batería UPS del servidor.** - **Asegurar el apagado del servidor de correo de manera correcta, para evitar errores del SO.**	- **Comunicar al jefe de informática.** - **Comunicar a todo el personal del hospital sobre el agotamiento y falla del equipo UPS, mediante el aplicativo que usualmente utilizan(UTALK)** - **Identificar el backup más actual de la base de datos de usuarios y mensajes obtenidos previamente.** -
	AD.1 Manipulación de la configuración	- **Asegurar que la clave del administrador del servidor de correo solo sea guardado por el jefe de informática.** - **El jefe de informática deberá tomar nota sobre todo acceso y/o modificación solicitada por personal de la sede central vía remota.** - **Antes de realizar cualquier modificación deberá obtener una copia de la configuración actual.** - **Borrar periódicamente los temporales del sistema operativo.**	- **Comunicar al jefe de informática.** - **Comunicar a todo el personal del hospital sobre el error de configuración que sufrió el servidor de correo.** - **Identificar el backup más actual de la configuración del servidor de correo.** - **Identificar el backup más actual de la base de datos de usuarios y mensajes obtenidos previamente.** - **De no tener respuesta del servidor por más de una hora por errores de configuración, poner en marcha el equipo backup de correo.**
	AD.2 Suplantación de la identidad del usuario		- **El jefe de informática deberá realizar las averiguaciones del caso.**
	AD.6 Acceso no autorizado	- **Solicitar mediante formato correspondiente el acceso al servidor de correo.** - **Dar a conocer a la jefatura inmediata sobre el acceso admitido.**	- **Dar a conocer a la jefatura de informática, sobre la magnitud de riesgo.** - **El jefe de informática deberá proponer alguna sanción para el personal no autorizado.** - **El jefe de informática deberá verificar el normal funcionamiento del servidor de correo luego de detectar el acceso no autorizado.**

Activo	Amenazas	Prevención de la Amenaza	Acciones que toman
SISTEMA DE GESTION HOSPITALARIA	EFNI.1 Errores de los usuarios	- **Solicitar mediante formato correspondiente el acceso al SGH el cual deberá estar firmado por su jefe inmediata.** - **Capacitar a los usuarios que tengan acceso al sistema SGH.** - **El jefe de informática deberá dar conocer a la jefatura inmediata del usuario admitido sobre el acceso admitido.**	- **El jefe de informática y/o el operador del SGH deberá verificar mediante la base de datos al usuario que realizó algún error.** - **Se deberá informar al usuario sobre la magnitud de error que realizó y que o quienes puede afectar.** - **El jefe de informática deberá proponer alguna sanción para el usuario.** - **El jefe de informática deberá verificar el normal funcionamiento del servidor de correo luego de detectar el error del usuario.**
	EFNI.2 Errores del administrador del SGH	- **El operador central – administrador del SGH deberá obtener una copia de toda la configuración antes de aplicar los pases – actualizaciones ordenadas por la sede central.** - **El operador central – administrador del SGH deberá verificar diariamente la operatividad de todos los módulos (admisión, consulta externa, farmacia, hospitalización, emergencia.) a través de consultas por correo electrónico a los usuarios responsables**.	- **El operador – administrador del SGH deberá comunicar al jefe de informática sobre los errores que afectaron la operatividad.** - **Comunicar a la sede central - Lima para el apoyo correspondiente.** - **Verificar los registros de errores del sistema y verificar si los errores han sido voluntarios por el administrador.** - **De detectar errores voluntarios, el jefe deberá proponer sanción administrativa a la gerencia de Red.** - **De no tener respuesta del SGH por más de una hora por errores de administrador, se deberá poner en marcha el equipo backup del SGH.**
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	- **Obtener una copia de seguridad de la base de datos de usuarios y mensaje antes del agotamiento de la batería UPS del servidor.** - **Asegurar el apagado del servidor de correo de manera correcta, para evitar errores del SO.**	- **Comunicar al jefe de informática.** - **Comunicar a todo el personal del hospital sobre el agotamiento y falla del equipo UPS.** - **Identificar el backup más actual de la base de datos obtenidos previamente.**
	AD.1 Manipulación de la configuración	- **El jefe de informática deberá tomar nota sobre todo acceso y/o modificación solicitada por personal de la sede central vía remota.** - **Antes de realizar cualquier modificación se deberá obtener una copia de la configuración actual.** - **Borrar periódicamente los temporales del sistema operativo.**	- **Comunicar al jefe de informática.** - **Comunicar a todo el personal del hospital sobre el error de configuración que sufrió el servidor del SGH.** - **Identificar el backup más actual de la configuración del servidor del SGH.** - **Identificar el backup más actual de la base de datos de usuarios obtenidos previamente en el servidor backup del SGH.** - **De no tener respuesta del servidor por más de una hora por errores de configuración, poner en marcha el equipo backup.**
	AD.2 Suplantación de la identidad del usuario		- **El jefe de informática deberá realizar las averiguaciones del caso.**
	AD.6 Acceso no autorizado	- **Solicitar mediante formato correspondiente el acceso al servidor del SGH.** - **Dar a conocer a la jefatura inmediata sobre el acceso admitido.**	- **Dar a conocer a la jefatura de informática, sobre la magnitud de riesgo.** - **El jefe de informática deberá proponer alguna sanción para el personal no autorizado.** - **El jefe de informática deberá verificar el normal funcionamiento del servidor de correo luego de detectar el acceso no autorizado.**

- **Equipamiento**

Activo	Amenazas	Prevención de la Amenaza	Acciones que toman
APLICACIONES	EFNI.15 Caída del sistema por agotamiento de recursos UPS	- **Obtener una copia de seguridad de la base de datos de usuarios y mensaje antes del agotamiento de la batería UPS del servidor.** - **Asegurar el apagado del servidor de correo de manera correcta, para evitar errores del SO.**	- **Comunicar al jefe de informática.** - **Comunicar a todo el personal del hospital sobre el agotamiento y falla del equipo UPS.** - **Identificar el backup más actual de la base de datos de usuarios y mensajes obtenidos previamente.**
	AD.1 Manipulación de la configuración	- **El jefe de informática deberá tomar nota sobre todo acceso y/o modificación solicitada por personal de la sede central vía remota.** - **Antes de realizar cualquier modificación de deberá obtener una copia de la configuración actual.** - **Borrar periódicamente los temporales del sistema operativo.**	- **Comunicar al jefe de informática.** - **Comunicar a todo el personal del hospital sobre el error de configuración que sufrió el servidor del SGH.** - **Identificar el backup más actual de la configuración del servidor del SGH.** - **Identificar el backup más actual de la base de datos de usuarios obtenidos previamente en el servidor backup del SGH.** - **De no tener respuesta del servidor por más de una hora por errores de configuración, poner en marcha el equipo backup.**
	AD.2 Suplantación de la identidad del usuario	.	- **El jefe de informática deberá realizar las averiguaciones del caso.**
	AD.6 Acceso no autorizado	- **Solicitar mediante formato correspondiente el acceso al servidor de correo.** - **Dar a conocer a la jefatura inmediata sobre el acceso admitido.**	- **Dar a conocer a la jefatura de informática, sobre la magnitud de riesgo.** - **El jefe de informática deberá proponer alguna sanción para el personal no autorizado.** - **El jefe de informática deberá verificar el normal funcionamiento del servidor de correo luego de detectar el acceso no autorizado.**
	AD.15 Denegación de servicio	- **Verificar de manera periódica que todas las aplicaciones que se encuentran en el hospital estén operativas, es decir consultar a los usuarios mediante correo sobre los errores que mantienen a la actualidad de manera que se otorgue el soporte en el momento.** - **Establecer el inventario actualizado de todos los aplicativos que se encuentren en el hospital**	- **Los usuarios encargados deberán informar mediante correo electrónico al jefe de informática para el soporte necesario.** - **Solicitar el apoyo a la sede central sobre los problemas que suceden a los aplicativos cuyas base de datos y ejecutables se encuentre alojados en dicha sede.**
	AD.19 Alteración de la información	- **Solicitar mediante formato correspondiente y firmado por el jefe inmediato el tipo de acceso y a los módulos a la cual deberá tener el usuario.** - **Los usuarios deberán ser capacitados por el área de soporte informático para evitar ingresos erróneos a los sistemas y que alteren la información de los asegurados.**	- **Informar al jefe de informática sobre las alteraciones detectadas.** - **Se deberá indicar al jefe inmediato de los usuarios sobre las alteraciones realizadas en los sistemas de información.** - **Corregir las alteraciones detectadas con la finalidad de informar a la sede central.**
	AD.10 Introducción de falsa información		- **El jefe inmediato deberá proponer sanción administrativa a la gerencia de Red, teniendo en cuenta la magnitud de la información falsa ingresada a las aplicaciones y el problema que genera la misma.**

Activo	Amenazas	Prevención de la Amenaza	Acciones que toman
APLICACIONES	AD.12 Destrucción de la información	- **Guardar los backup de información en servidores ubicados en distintos lugares de donde se ubica el servidor principal.**	- **Obtener el backup más reciente para su aplicación en el sistema de información afectado.**
	AD.13 Divulgación de información	- **En los servidores no se deberá permitir el uso de USB's.**	- **Decomisar la información a los usuarios responsables del manejo de información confidencial.** - **Verificar que la información divulgada no fue eliminada y deberá haber una copia del mismo.** - **El jefe de informática deberá proponer frente al jefe inmediato del usuario divulgador una sanción justa y responsable.**
	EFNI.12 Vulnerabilidades de los programas (software)	- **Cada usuario deberá recibir mediante memorándum su usuario y clave el cual debe ser único e intransferible.** - **Verificar que los manejadores de bases de datos sean verdaderos gestores, es decir que permitan la creación de usuarios y tipos de accesos para manipular las bases de datos.**	- **Investigar las vulnerabilidades sufridas en los aplicativos para detectar los posibles responsables.** - **Verificar la operatividad de los aplicativos luego de haber sido vulnerada.** - **De obtener información errónea del aplicativo a causa de la vulnerabilidad, se deberá informar a los responsables del sistema de las fallas encontradas.** - **Asimismo, el jefe de informática deberá proponer la sanción administrativa correspondiente.**
	EFNI.13 Errores de mantenimiento / actualización de programas (software)	- **Antes se deberá obtener una copia de toda la configuración.**	- **El responsable y/o el operador del aplicativo deberá comunicar al jefe de informática sobre los errores que afectaron la operatividad debido al mantenimiento.** - **En caso sea un aplicativo desarrollado por la sede central se deberá comunicar para el apoyo correspondiente.** - **Verificar los registros de errores del sistema y verificar si fueron voluntarios o casualidad del técnico que realizó dicha actualización.** - **De detectar errores voluntarios, el jefe deberá proponer sanción administrativa a la gerencia de Red o el no pago por el mantenimiento realizado.** - **De no tener respuesta del aplicativo por más de una hora por errores de mantenimiento, se deberá poner en marcha el equipo backup y su base de datos.**
EQUIPOS	DN.1 Fuego	- **Mantener actualizado los extintores**.	
	DN.1 Daños por agua	- **Contar con un pozo de agua en la parte posterior del hospital, donde se acumule el agua para su posterior bombeo, este sistema debe ser revisada periódicamente.**	
	DN.3 Desastres naturales	- **Contar con un plan de evacuación de las instalaciones del hospital, el mismo que debe ser de conocimiento de todo el personal que labora.** - **Realizar simulacros de evacuación con la participación de todo el personal de la sede del hospital.** - **Mantener las salidas libres de obstáculos.** - **Señalizar todas las salidas.** - **Señalizar las zonas seguras.** - **Definir los puntos de reunión en caso de evacuación.**	

Activos	Amenazas	Prevención de la Amenaza	Acciones que toman
EQUIPOS	OI.3 Corte del suministro eléctrico	- **Durante las operaciones diarias del servicio u operaciones del hospital se contará con los UPS necesarios para asegurar el suministro eléctrico en las estaciones de trabajo consideradas como críticas.** - **Contar con equipos de luces de emergencia con tolerancia de 15 minutos, accionados automáticamente al producirse el corte de fluido eléctrico, los cuales deben estar instalados en los ambientes críticos.**	- **Informar a la Administración y/o Jefe de Informática del problema presentado.** - **Dar aviso del corte de energía eléctrica en forma oportuna a todas las áreas del hospital y coordinar las acciones necesarias.** - **Las actividades afectadas por la falta de uso de aplicaciones, deberán iniciar sus procesos de contingencia a fin de no afectar las operaciones en curso.** - **En el caso de los equipos que entren en funcionamiento automático con UPS´s, se deberá monitorear el tiempo de autonomía del equipo y no exceder el indicado anteriormente. En caso la interrupción de energía sea mayor a quince minutos, se deberán apagar los servidores de producción, desarrollo y correo hasta que regrese el fluido eléctrico.**
	OI.4 Condiciones inadecuadas de temperatura o humedad	- **Acondicionar adecuadamente y en un nivel de temperatura moderada el área donde se encuentra los activos informáticos, para evitar el recalentamiento de dichos equipos.** - **Verificar que dicha área este libre de filtración de agua ya que causará la humedad dentro de ello provocando daños a los activos.** -	- **Hacer un inventario de los equipos afectados.** - **Informar al Jefe inmediato sobre el problema causado por la humedad.** - **Solicitar los requerimientos necesarios para dar solución al problema suscitado.** - **Dar mantenimiento a los equipos de acondicionamiento averiados.**
	EFNI.5 Difusión de software dañino	- **Establecimiento de políticas de seguridad para prevenir el uso de aplicaciones no autorizadas en las estaciones de trabajo.** - **Restringir el acceso a Internet a las estaciones de trabajo que por su uso no lo requieran.** - **Contar con antivirus instalados en cada estación de trabajo, el mismo que debe estar actualizado permanentemente.** - **Contar con equipos de respaldo ante posibles fallas de las estaciones, para su reemplazo provisional hasta su desinfección y habilitación.**	- **Desconectar la estación infectada de la red del hospital.** - **Verificar si el equipo se encuentra infectado, utilizando un detector de virus actualizado.** - **Rastrear de ser necesario el origen de la infección (archivo infectado, correo electrónico, etc.)** - **Eliminar el agente causante de la infección.** - **Remover el virus del sistema.** - **Probar el sistema.** **En caso no solucionarse el problema :** - **Formatear el equipo.** - **Personalizar la estación para el usuario.** - **Conectar la estación a la red del hospital.** - **Efectuar las pruebas necesarias con el usuario.** - **Solicitar conformidad del servicio de soporte informático**.
	EFNI.12 Vulnerabilidades de los programas (software)	- **Cada usuario deberá recibir mediante memorándum su usuario y clave el cual debe ser único e intransferible.** - **Verificar que los manejadores de bases de datos sean verdaderos gestores, es decir que permitan la creación de usuarios y tipos de accesos para manipular las bases de datos.**	- **Investigar las vulnerabilidades sufridas en los aplicativos para detectar los posibles responsables.** - **Verificar la operatividad de los aplicativos luego de haber sido vulnerada.** - **De obtener información errónea del aplicativo a causa de la vulnerabilidad, se deberá informar a los responsables del sistema de las fallas encontradas.** - **Asimismo, el jefe de informática deberá proponer la sanción administrativa correspondiente.**

Activos	Amenazas	Prevención de la Amenaza	Acciones que toman
EQUIPOS	AD.2 Suplantación de la identidad del usuario	- **Asegurar que la clave del administrador del servidor de correo solo sea guardado por el jefe de informática.**	- **El jefe de informática deberá realizar las averiguaciones del caso.**
	AD.3 Abuso de privilegios de acceso	- **Hacerle llegar las funciones que le corresponde a cada personal con su área.** - **Habilitar sólo los privilegios relacionados a las funciones que cumple el personal con dicha área; tales como en aplicaciones, programas, web site, entre otros.**	- **De no cumplir solo con sus funciones establecidas, informar a su jefe inmediato para su llamada de atención y si es a mayor el daño proceder a una sanción inmediata.** - **Habilitar los servidores del Domain Name, servidores del Web y servidores del correo en sistemas separados y restringir el acceso a la red a través de un firewall.** - **Es también beneficioso deshabilitar los servicios innecesarios para que el atacante no pueda tener acceso a ningún sistema.**
	AD.5 Alteración de secuencia	- **Aplicación de directivas y/o reglamente de trabajo, para buen uso de los equipos de cómputo, internet y correo institucional.** - **Inventario de cada equipo con su respectivo IP, nombre de la PC y los datos de cada responsable de dicho activo, cabe mencionar: apellidos y nombres completos, número del documento nacional de identidad (DNI), el área al que pertenece, jefe inmediato, entre otros**.	- **Informar al jefe inmediato para su llamada de atención y si es a mayor el daño proceder a una sanción inmediata.** - **Analizar los archivos log** - **Bloquear el equipo en donde se ha realizado una transacción no autorizada.** - **Bloquear la cuenta del usuario utilizada en el ataque.** - **El personal responsable verificará nuevamente cada uno de los puntos de red.** - **Realizar un informe de los eventos sucedidos, de los correctivos y las acciones realizadas y lograr un seguimiento de estos incidentes para observar su evolución y determinar de manera más fácil si vuelve a ocurrir.** - **Si hubiere el caso de que vuelva a ocurrir dicha acción, el responsable de sistemas podrá determinar con exactitud quien es el responsable o el causante y tomar las medidas pertinentes al caso.**
	AD.6 Acceso no autorizado	- **Solicitar mediante formato correspondiente el acceso al servidor de correo.** - **Dar a conocer a la jefatura inmediata sobre el acceso admitido.**	- **Dar a conocer a la jefatura de informática, sobre la magnitud de riesgo.** - **El jefe de informática deberá proponer alguna sanción para el personal no autorizado.** - **El jefe de informática deberá verificar el normal funcionamiento del servidor de correo luego de detectar el acceso no autorizado.**
	AD.8 Interceptación de información (escucha)	- **Inventario de cada equipo de comunicación, datos de cada responsable de dicho activo, cabe mencionar: apellidos y nombres completos, número del documento nacional de identidad (DNI), el área al que pertenece, feje inmediato, entre otros; y si es un equipo de comunicación con IP registrarlo adecuadamente.**	- **Informar al jefe inmediato para su llamada de atención y si es a mayor el daño proceder a una sanción inmediata.**
	AD.14 Manipulación de programas	- **Hacerle llegar las funciones que le corresponde a cada personal con su área.** - **Habilitar sólo los privilegios relacionados a las funciones que cumple el personal con dicha área; cabe menciones aplicaciones, programas, web site, entre otros.**	- **De no cumplir solo con sus funciones establecidas, informar a su jefe inmediato para su llamada de atención y si es a mayor el daño proceder a una sanción inmediata.** - **Habilitar los servidores del Domain Name, servidores del Web y servidores del correo en sistemas separados y restringir el acceso a la red a través de un firewall.** - **Es también beneficioso deshabilitar los servicios innecesarios para que el atacante no pueda tener acceso a ningún sistema.**
	AD.15 Denegación de servicio	- **Verificar de manera periódica que todas las aplicaciones que se encuentran en el hospital estén operativas, es decir consultar a los usuarios mediante correo sobre los errores que mantienen a la actualidad de manera que se otorgue el soporte en el momento.** - **Establecer el inventario actualizado de todos los aplicativos que se encuentren en el hospital**	- **Los usuarios encargados deberán informar mediante correo electrónico al jefe de informática para el soporte necesario.** - **Solicitar el apoyo a la sede central sobre los problemas que suceden a los aplicativos cuyas base de datos y ejecutables se encuentre alojados en dicha sede.**

Activo	Amenazas	Prevención de la Amenaza	Acciones que toman
COMUNICACION	DN.1 Fuego	- **Mantener actualizado los extintores.**	
	DN.2 Daños por agua	- **Contar con un pozo de agua en la parte posterior del hospital, donde se acumule el agua para su posterior bombeo, este sistema debe ser revisada periódicamente.**	
	DN.3 Desastres naturales	- **Contar con un plan de evacuación de las instalaciones del hospital, el mismo que debe ser de conocimiento de todo el personal que labora.** - **Realizar simulacros de evacuación con la participación de todo el personal de la sede del hospital.** - **Mantener las salidas libres de obstáculos.** - **Señalizar todas las salidas.** - **Señalizar las zonas seguras.** - **Definir los puntos de reunión en caso de evacuación**.	
	OI.3 Corte del suministro eléctrico	- **Durante las operaciones diarias del servicio u operaciones del hospital se contará con los UPS necesarios para asegurar el suministro eléctrico en las estaciones de trabajo consideradas como críticas.** - **Contar con equipos de luces de emergencia con tolerancia de 15 minutos, accionados automáticamente al producirse el corte de fluido eléctrico, los cuales deben estar instalados en los ambientes críticos.**	- **Informar a la Administración y/o Jefe de Informática del problema presentado.** - **Dar aviso del corte de energía eléctrica en forma oportuna a todas las áreas del hospital y coordinar las acciones necesarias.** - **Las actividades afectadas por la falta de uso de aplicaciones, deberán iniciar sus procesos de contingencia a fin de no afectar las operaciones en curso.** - **En el caso de los equipos que entren en funcionamiento automático con UPS´s, se deberá monitorear el tiempo de autonomía del equipo y no exceder el indicado anteriormente. En caso la interrupción de energía sea mayor a quince minutos, se deberán apagar los servidores de producción, desarrollo y correo hasta que regrese el fluido eléctrico.**
	EFNI.15 Caída del sistema por agotamiento de recursos UPS	- **Obtener una copia de seguridad de la base de datos de usuarios y mensaje antes del agotamiento de la batería UPS del servidor.** - **Asegurar el apagado del servidor de correo de manera correcta, para evitar errores del SO.**	- **Comunicar al jefe de informática.** - **Comunicar a todo el personal del hospital sobre el agotamiento y falla del equipo UPS.** - **Identificar el backup más actual de la base de datos de usuarios y mensajes obtenidos previamente.**
	AD.2 Suplantación de la identidad del usuario	- **Asegurar que la clave del administrador del servidor del SGH solo sea guardado por el jefe de informática y/o el operador central.**	- **El jefe de informática deberá realizar las averiguaciones del caso.**
	AD.6 Acceso no autorizado	- **Solicitar mediante formato correspondiente el acceso al servidor de correo.** - **Dar a conocer a la jefatura inmediata sobre el acceso admitido.**	- **Dar a conocer a la jefatura de informática, sobre la magnitud de riesgo.** - **El jefe de informática deberá proponer alguna sanción para el personal no autorizado.** - **El jefe de informática deberá verificar el normal funcionamiento del servidor de correo luego de detectar el acceso no autorizado.**
	AD.7 Análisis de tráfico		- **Desconectar la estación que causa el tráfico por alguna infección de virus u otro caso.** - **Eliminar los correos que se encuentran en bandeja de salida y que están causando cuello de botella en el servidor.**

Activo	Amenazas	Prevención de la Amenaza	Acciones que toman
	AD.8 Interceptación de información (escucha)		- **Informar al jefe inmediato para su llamada de atención y si es a mayor el daño proceder a una sanción inmediata.**
COMUNICACION	AD.16 Robo de equipos	- **El personal de vigilancia debe estar atento a todo movimiento o desplazamiento ya sea interno como externo de cualquier activo, mediante papeletas de desplazamiento autorizados y firmados por el personal que envía el activo como el que recibe de acuerdo ala conformidad.** - **El personal que tenga acceso a determinados lugares debe tener su respectiva identificación.** - **Todos los equipos deben contar con sus códigos patrimoniales, y en caso de no contar con ello, asignarles uno**. - **Inventario de todos los activos a proteger.**	- **Un nuevo inventario de todos los activos.** - **El personal encargado del área realizará e informe detallado de lo sustraído y lo presentará a su jefe inmediato.** - **El personal de vigilancia tendrá que revisar las papeletas de desplazamiento de los activos y a la vez el control de ingreso y salida de todo el personal a dicha área donde se produjo la sustracción.**
ELEMENTOS AUXILIARES	DN.1 Fuego	- **Mantener actualizado los extintores.**	
	DN.2 Daños por agua	- **Contar con un pozo de agua en la parte posterior del hospital, donde se acumule el agua para su posterior bombeo, este sistema debe ser revisada periódicamente.**	
	DN.3 Desastres naturales	- **Contar con un plan de evacuación de las instalaciones del hospital, el mismo que debe ser de conocimiento de todo el personal que labora.** - **Realizar simulacros de evacuación con la participación de todo el personal de la sede del hospital.** - **Mantener las salidas libres de obstáculos.** - **Señalizar todas las salidas.** - **Señalizar las zonas seguras.** - **Definir los puntos de reunión en caso de evacuación**.	
	OI.3 Corte del suministro eléctrico	- **Durante las operaciones diarias del servicio u operaciones del hospital se contará con los UPS necesarios para asegurar el suministro eléctrico en las estaciones de trabajo consideradas como críticas.** - **Contar con equipos de luces de emergencia con tolerancia de 15 minutos, accionados automáticamente al producirse el corte de fluido eléctrico, los cuales deben estar instalados en los ambientes críticos.**	- **Informar a la Administración y/o Jefe de Informática del problema presentado.** - **Dar aviso del corte de energía eléctrica en forma oportuna a todas las áreas del hospital y coordinar las acciones necesarias.** - **Las actividades afectadas por la falta de uso de aplicaciones, deberán iniciar sus procesos de contingencia a fin de no afectar las operaciones en curso.** - **En el caso de los equipos que entren en funcionamiento automático con UPS´s, se deberá monitorear el tiempo de autonomía del equipo y no exceder el indicado anteriormente. En caso la interrupción de energía sea mayor a quince minutos, se deberán apagar los servidores de producción, desarrollo y correo hasta que regrese el fluido eléctrico.**
	AD.16 Robo de equipos	- **El personal de vigilancia debe estar atento a todo movimiento o desplazamiento ya sea interno como externo de cualquier activo, mediante papeletas de desplazamiento autorizados y firmados por el personal que envía el activo como el que recibe de acuerdo ala conformidad.** - **El personal que tenga acceso a determinados lugares debe tener su respectiva identificación.** - **Todos los equipos deben contar con sus códigos patrimoniales, y en caso de no contar con ello, asignarles uno.**	- **Un nuevo inventario de todos los activos.** - **El personal encargado del área realizará e informe detallado de lo sustraído y lo presentará a su jefe inmediato.** - **El personal de vigilancia tendrá que revisar las papeletas de desplazamiento de los activos y a la vez el control de ingreso y salida de todo el personal a dicha área donde se produjo la sustracción.**

- **Personal**

Activo	Amenazas	Prevención de la Amenaza	Acciones que toman
ADMINISTRADOR DE SISTEMAS Y BASE DE DATOS	AD.13 Divulgación de información	- **Concientizar aún más sobre temas de confidencialidad de información e integridad de datos al personal asignado para dicha función.** - **El jefe de la Unidad de Soporte Informático debe tan sólo de dar privilegios de algunas informaciones que harán posible el desarrollo de su función asignado.** - **Si requiere de alguna u otra información debe ser evaluado y aprobado por el Jefe del área.**	
	EFNI.16 Indisponibilidad del personal	- **Dar conocimiento al Jefe de Informática por parte del reporte de inasistencia del Control de Asistencia.** - **Dar conocimiento al Jefe de Informática por comunicación telefónica por parte del personal o algún familiar.**	
OPERADOR	AD.13 Divulgación de información	- **Concientizar aún más sobre temas de confidencialidad de información e integridad de datos al personal asignado para dicha función.** - **El jefe de la Unidad de Soporte Informático debe tan sólo de dar privilegios de algunas informaciones que harán posible el desarrollo de su función asignado.** - **Si requiere de alguna u otra información debe ser evaluado y aprobado por el Jefe del área.**	
	EFNI.16 Indisponibilidad del personal	- **Dar conocimiento al Jefe de Informática por parte del reporte de inasistencia del Control de Asistencia.** - **Dar conocimiento al Jefe de Informática por comunicación telefónica por parte del personal o algún familiar.**	

- **Instalación**

Activo	Amenazas	Prevención de la Amenaza	Acciones que toman
HOSPITAL III IQUITOS	DN.1 Fuego	- **Mantener actualizado los extintores.**	
	DN.2 Daños por agua	- **Contar con un pozo de agua en la parte posterior del hospital, donde se acumule el agua para su posterior bombeo, este sistema debe ser revisada periódicamente.**	
	DN.3 Desastres naturales	- **Contar con un plan de evacuación de las instalaciones del hospital, el mismo que debe ser de conocimiento de todo el personal que labora.** - **Realizar simulacros de evacuación con la participación de todo el personal de la sede del hospital.** - **Mantener las salidas libres de obstáculos.** - **Señalizar todas las salidas.** - **Señalizar las zonas seguras.** - **Definir los puntos de reunión en caso de evacuación.**	

Jefe de Unidad de Soporte
Informático-USI
RED LORETO
ESSALUD

ANEXO Nº 05

Red Asistencial Loreto				
Unidad de Soporte Informático.				
Bitácora de Incidencias del Sistema de Gestión Hospitalaria				
Centro Asistencial / Sede Admin.				
Nombre del Responsable (Operador)				
Nombre del Servidor				
Dirección IP.				
Nombre del Jefe de la U.S.I.				
FECHA	**HORA**	**INCIDENCIAS**	**OBSERVACIONES**	**FIRMA DEL RESPONSABLE**
			Sello y Firma	
			Jefe Unidad de Soporte Informático	
			Red Asistencial Loreto	

ANEXO Nº 06

Solicitud de Nuevo Usuario al Sistema de Información							
Unidad Orgánica (Sede Central Red Asistencial)			**RED ASISTENCIAL LORETO**				
Jefe de la Unidad / Area Solicitante							
Correo Electrónico del Jefe de la Unidad / Area							
Datos del Empleado							
N°	**Apellidos y Nombres**	**Correo Electrónico**	**Código de Planilla**	**Area / Función que Realiza**	**Sustento para el Acceso al Sistema (Indicar los módulos a las que va acceder, de acuerdo a la función, cargo que tiene el usuario)**		
1							
2							
REDES ASISTENCIALES: Gerente o Jefe Administrativo y Jefe de la Unidad de Sooporte Informático							
		_____				_____	
		Gerente / Jefe Administrativo				Jefe de Informática	

ANEXO Nº 07

Eliminación y/o Inhabilitación de Usuario al Sistema de Gestión Hospitalaria									
Unidad Orgánica (Sede Central Red Asistencial)			**RED ASISTENCIAL LORETO**						
Jefe de la Unidad / Area Solicitante									
Correo Electrónico del Jefe de la Unidad /Area			-						
Datos del Empleado									
N°	**Apellidos y Nombres**	**Correo Electrónico**	**Código de Planilla**	**Area**	**Función que Realiza (o)**	**Sustento para la inhabilitación al SGH (Vacaciones / Licencia)**		**Sustento para la eliminación al SGH (Cese de funciones / Cese de la Institución)**	
1					-				
2									
NOTA: Deberá contar con la firma y sello de los siguientes funcionarios:									
REDES ASISTENCIALES: Gerente o Jefe Administrativo y Jefe de la Unidad de Soporte Informático									
		Gerente / Jefe Administrativo				Jefe de Informática			

ANEXO Nº 08

Red Asistencial Loreto

Unidad de Soporte Informático.

FORMATO DE CONTROL DE BACKUP Y RESGUARDO DE LA INFORMACIÓN.

FECHA	HORA	EQUIPO				BACKUP		PROCESO		ERROR (ES)		DESCRIPCION DEL ERROR	OBSERVACIONES	RESPONSABLE	FIRMA
		PC	SERV	NOMBRE	IP.	DATA	APLIC	AUTO.	MANU.	SI	NO				

Sello y Firma
Jefa Unidad de Soporte Informático
Red Asistencial Loreto

ANEXO Nº 09

FORMATO DE ENTRADA Y SALIDA DE PERSONAS AL AREA RESTRINGIDA
CENTRO DE COMPUTO

Unidad Orgánica (Sede Central Red Asistencial)	RED ASISTENCIAL LORETO
Centro Asistencial / Oficina Administrativa	
Responsable del Centro de Computo / Area Restringida	

DATOS DE LA PERSONA						
APELLIDOS Y NOMBRES	AREA DE ORIGEN	FECHA	ENTRADA HORA	SALIDA HORA	FIRMA	MOTIVO DEL INGRESO

Sello y Firma
Jefe Unidad de Soporte Informático

ANEXO Nº 10 - Dominio y Límites

Infraestructura Física de la Sede Hospital III IQUITOS – Loreto

Detalles de construcción de los edificios (ver el Plano de Distribución de Puntos de la Sede Hospital III IQUITOS):

Edificio "A", cuenta con tres niveles, construido con material noble y en el techo se cuenta con la antena principal de los Radios Enlaces con los demás Locales. En este edificio se encuentran las oficinas según se detalla por niveles:

Primer Nivel: Consultorios Externos (01 - 25), Consultorio Reumatología, Programas, Archivos Historias Clínicas, EsSalud en Línea, Centro de Computo, Módulos de Atención al Asegurado, Laboratorio, Farmacia, Control de personal, Voluntariado, Tramite documentario, ORI, OAAS.

Segundo Nivel: Servicios de emergencias, Centro Quirúrgico, Hospitalización Medicina, Hospitalización Cirugía, Hospitalización Pediatría, Modulo Neonatología, Modulo Ginecología, Hospitalización Gineco-Obstetricia, Medicina Física y Rehabilitación, Tomografías.

Tercer Nivel: Cuerpo médico, Mantenimiento, Ingeniería hospitalaria, Oficinas de Planificación y calidad, estadística, red científica, facturación.

Edificio "B", cuenta con un solo nivel; está construido con material noble. En este edificio se encuentran las oficinas según se detalla:

- Administración de Almacén.
- Recepción.
- Despacho.
- Área Almacenera.

Veredas: Todos los edificios están rodeados de veredas de cemento enlucido, cuentan alcantarillado tapado que empalma con La pista de La calle

Cableado de Datos

1. Requerimientos Generales del Cableado: El cableado de datos deberá cumplir con los siguientes requerimientos y/o especificaciones:

    - Categoría-6.
    - Comprende solo el cableado para la red de datos.
    - El sistema de cableado deberá estar proyectado para soportar un factor de crecimiento del 40%.
    - El material del cableado deberá ser del mismo fabricante (canal completo).
    - Los puntos de red (outlets) deberán ser instalados en la pared, a una altura mínima de 45 cm.
    - Se deberá prever el anclaje adecuado de las canaletas sobre: material noble, adobe y tabiquerías.
    - El canalizado en interiores deberá hacerse utilizando canaletas plásticas y deberán instarse a una altura mínima de 45 cm.
    - Toda curva (en interiores / exteriores) deberá respetar el estándar ANSI/EIA/TIA 569A, para lo cual es imprescindible que sean normalizadas y se incluyan los accesorios adecuados. No se aceptarán codos o ángulos en 90º.
    - Se requiere de etiquetas auto laminable en ambos extremos del cable UTP, cable de fibra óptica, cables multipar y patch cords. Para los patch panel y face plates se requiere que las etiquetas autoadhesivas estén cubiertas por una mica transparente para garantizar su longevidad.

- Utilizar face plates dobles que soporten iconos de identificación al lado de cada puerto y tapa ciega.
- Todo el sistema de sujeción de los cables UTP dentro de los gabinetes se realizará utilizando cintas del tipo velcro, no se deberá utilizar cintillos.
- La instalación, ordenación e identificación de los patch cords que van desde el patch panel hasta los equipos activos de red deberá ser realizada por el contratista.
- Se deberán dejar las instalaciones (paredes, tabiquería, piso, etc.) en iguales o mejores condiciones a las entregadas antes de la ejecución de las obras, cuidando mucho la apariencia estética de las instalaciones.

2. El trabajo de cableado de datos deberá cumplir con las siguientes normas:

ANSI/TIA/EIA 568-B:
Estándar de Cableado para Edificios Comerciales y Telecomunicaciones.
ANSI/TIA/EIA 568-B.1:
Requerimientos Generales.
ANSI/TIA/EIA 568-B.2:
Componentes de Cableado Par Trenzado Balanceado.
ANSI/TIA/EIA-568-B.2-1:
Especificaciones de Desempeño de Transmisión para Cableado Categoría 6.
ANSI/TIA/EIA 569B:
Rutas y Espacios. ANSI/TIA/EIA 606A: Administración.

3. Ubicación de los puntos de red:

En la siguiente tabla se detalla el nombre de la oficina, cantidad de puntos por oficina, ubicación y gabinete al cual estarán conectados los puntos de red (ver Plano de Distribución de Puntos de la Sede Hospital III Iquitos – Loreto).

				# Puntos X
Oficina	# de puntos	Ubicación	Gabinete	Gabinete
Essalud en Línea	9	Edificio “A” Primer Nivel	A	**58**
Consultorios Externos 01	1	Edificio “A” Primer Nivel	A	
Consultorios Externos 02	1	Edificio “A” Primer Nivel	A	
Consultorios Externos 03	1	Edificio “A” Primer Nivel	A	
Consultorios Externos 04	1	Edificio “A” Primer Nivel	A	
Consultorios Externos 05	1	Edificio “A” Primer Nivel	A	
Consultorios Externos 06	1	Edificio “A” Primer Nivel	A	
Consultorios Externos 07	1	Edificio “A” Primer Nivel	A	
Consultorios Externos 08	1	Edificio “A” Primer Nivel	A	
Consultorios Externos 09	1	Edificio “A” Primer Nivel	A	
Consultorios Externos 10	1	Edificio “A” Primer Nivel	A	
Consultorios Externos 11	1	Edificio “A” Primer Nivel	A	
Consultorios Externos 12	1	Edificio “A” Primer Nivel	A	
Consultorios Externos 13	1	Edificio “A” Primer Nivel	A	
Consultorios Externos 14	1	Edificio “A” Primer Nivel	A	
Consultorios Externos 15	1	Edificio “A” Primer Nivel	A	

Consultorios Externos 16	1	Edificio “A” Primer Nivel	A	
Consultorios Externos 17	1	Edificio “A” Primer Nivel	A	
Consultorios Externos 18	1	Edificio “A” Primer Nivel	A	
Consultorios Externos 19	1	Edificio “A” Primer Nivel	A	
Archivos Historias Clínicas	12	Edificio “A” Primer Nivel	A	
Centro de Computo	6	Edificio “A” Primer Nivel	A	
Módulos de Atención al Asegurado 01	1	Edificio “A” Primer Nivel	A	
Módulos de Atención al Asegurado 02	1	Edificio “A” Primer Nivel	A	
Módulos de Atención al Asegurado 03	1	Edificio “A” Primer Nivel	A	
Módulos de Atención al Asegurado 04	1	Edificio “A” Primer Nivel	A	
Control de personal	2	Edificio “A” Primer Nivel	A	
Voluntariado	1	Edificio “A” Primer Nivel	A	
Tramite documentario	2	Edificio “A” Primer Nivel	A	
ORI	2	Edificio “A” Primer Nivel	A	
OAAS	1	Edificio “A” Primer Nivel	A	
Laboratorio	20	Edificio “A” Primer Nivel	B	**25**
Farmacia	5	Edificio “A” Primer Nivel	B	
Consultorios Externos 20	1	Edificio “A” Primer Nivel	C	
Consultorios Externos 21	1	Edificio “A” Primer Nivel	C	
Consultorios Externos 22	1	Edificio “A” Primer Nivel	C	
Consultorios Externos 23	1	Edificio “A” Primer Nivel	C	**8**
Consultorios Externos 24	1	Edificio “A” Primer Nivel	C	
Consultorios Externos 25	1	Edificio “A” Primer Nivel	C	
Consultorios Reumatología	1	Edificio “A” Primer Nivel	C	
Programas	1	Edificio “A” Primer Nivel	C	
Servicios de emergencias	6	Edificio “A” Segundo Nivel	D	
Centro Quirúrgico	1	Edificio “A” Segundo Nivel	D	
Hospitalización Medicina	1	Edificio “A” Segundo Nivel	D	
Hospitalización Cirugía	1	Edificio “A” Segundo Nivel	D	
Hospitalización Pediatría	2	Edificio “A” Segundo Nivel	D	**16**
Módulo Neonatología	1	Edificio “A” Segundo Nivel	D	
Módulo Ginecología	1	Edificio “A” Segundo Nivel	D	
Hospitalización Gineco-Obtetricia	1	Edificio “A” Segundo Nivel	D	
Medicina Física y Rehabilitación	1	Edificio “A” Segundo Nivel	D	
Tomografías	1	Edificio “A” Segundo Nivel	D	
Cuerpo médico	1	Edificio “A” Tercer Nivel	E	**24**

Mantenimiento	6	Edificio “A” Tercer Nivel	E	
Ingeniería hospitalaria	4	Edificio “A” Tercer Nivel	E	
Oficinas de Planificación y calidad	4	Edificio “A” Tercer Nivel	E	
Estadística	4	Edificio “A” Tercer Nivel	E	
Red Científica	2	Edificio “A” Tercer Nivel	E	
Facturación	3	Edificio “A” Tercer Nivel	E	
Administración	3	Edificio “B” Primer Nivel	E	**5**
Recepción	1	Edificio “B” Primer Nivel	E	
Despacho	1	Edificio “B” Primer Nivel	E	
TOTAL	**136**			

NOTA: La ubicación física de los puntos de red y gabinete es mostrada en el plano adjunto, pudiendo haber variaciones mínimas las cuales serán coordinadas con la empresa que ejecute el proyecto bajo el consentimiento del Ingeniero Supervisor.

4. Ubicación y especificaciones de los Closet de Telecomunicaciones (TC):

Gabinete “A” y "F":

Estos gabinete deberá estar ubicado en el Edificio “A” - Primer Nivel en la Of. De Soporte y Comunicaciones (ver Plano de Distribución de la Sede Hospital III IQUITOS – LORETO).

Debe tener las siguientes características generales:

- Gabinete de pie con puerta frontal de marco metálico y plancha de acrílico. Puertas posteriores y laterales con llave.
- Techo, base para cables .04 perfiles ajustables de profundidad, agujeros con tuercas enjauladas.
- Dimensiones 2145x670x800mm (45 unidades de rack).
- Tratamiento anticorrosivo de fosfatizado y pintado electrostáticamente con pintura en polvo Epoxi- poliester.
- 01 Bandeja metálica de 19” retráctil para teclado y mouse.
- 01 Bandeja metálica de 19” x 12” de profundidad (para monitor).
- 01 Bandeja metálica de 19” x 12” de profundidad (para equipos colocar equipos no rackeables).
- 01 Bandeja metálica de 19” 490mm profundidad para 60 Kgs, soportados en 4 posiciones (para instalar el servidor).
- 01 Bandeja metálica de 19” 490mm profundidad para 60 Kgs, soportados en 4 posiciones (para instalar el UPS).
- Barra(s) de energía rackeable, con un mínimo de 16 tomas independientes u 08 tomas dobles, de tres espigas + ITM 2x20A.
- Barra de cobre de 3x10 mm.
- Kit de ventiladores axiales (mínimo 4 ventiladores) de 220V.
- Los ordenadores horizontales de cable deberá ser de 2 RU (mínimo) y de tipo canaletas, según se requiera para la cantidad de puntos.

Gabinete "B":

Este gabinete deberá estar ubicado en el Edificio "A" - Primer Nivel en el servicio de farmacia (ver Plano de Distribución de Puntos de la Sede Hospital III Iquitos – LORETO), pudiendo ser modificada su ubicación por la empresa que ejecute el proyecto bajo el consentimiento del Ingeniero Supervisor.

El gabinete deberá tener las siguientes características:

- Gabinete de pared con puerta frontal de marco metálico y plancha de acrílico.
- Base adosable a pared y cuerpo batiente en acero laminado.
- Puertas laterales desmontables.
- Techo, base para cables STD 19" x 12 RU.
- 02 perfiles ajustables de profundidad.
- Agujeros con tuercas enjauladas.
- Dimensiones 518x500x355mm.
- Tratamiento anticorrosivo de fosfatizado y pintado electrostáticamente con pintura en polvo Epoxi- poliester.
- Los ordenadores horizontales de cable deberá ser de 2 RU (mínimo) y de tipo canaletas, según se requiera para la cantidad de puntos.
- Barra(s) de energía rackeable, con un mínimo de 08 tomas independientes u 04 tomas dobles, de tres espigas + ITM 2x20A.
- Barra de cobre de 3x10 mm.

Gabinete "C":

Este gabinete deberá estar ubicado en el Edificio "A" - Primer Nivel en el servicio de farmacia (ver Plano de Distribución de Puntos de la Sede Hospital III Iquitos – LORETO), pudiendo ser modificada su ubicación por la empresa que ejecute el proyecto bajo el consentimiento del Ingeniero Supervisor.

Este gabinete deberá tener las mismas características que las mencionadas para el gabinete "B".

Gabinete "D":

Este gabinete deberá estar ubicado en el Edificio "A" - Segundo Nivel en el servicio de farmacia (ver Plano de Distribución de Puntos de la Sede Hospital III Iquitos – LORETO), pudiendo ser modificada su ubicación por la empresa que ejecute el proyecto bajo el consentimiento del Ingeniero Supervisor.

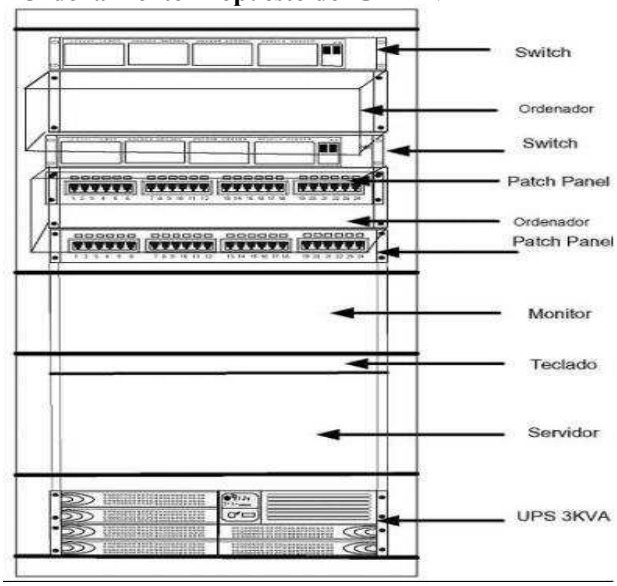
Este gabinete deberá tener las mismas características que las mencionadas para el gabinete "B".

Gabinete "E":

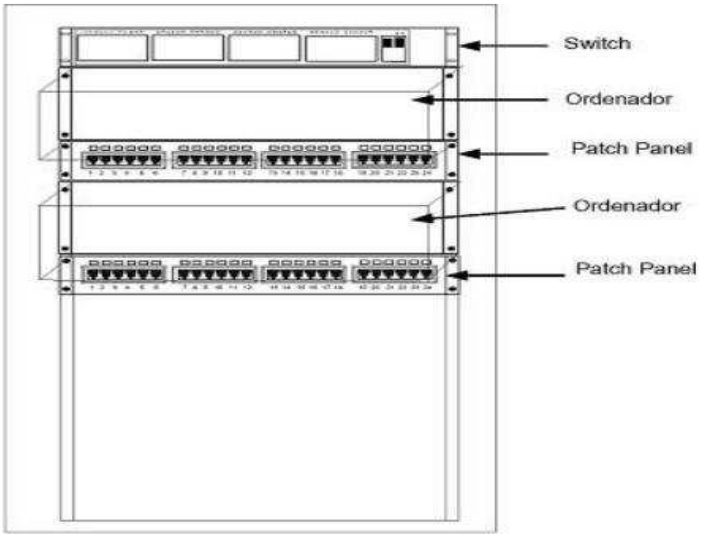
Este gabinete deberá estar ubicado en el Edificio "A" - Tercer Nivel en el servicio de farmacia (ver Plano de Distribución de Puntos de la Sede Hospital III Iquitos – LORETO), pudiendo ser modificada su ubicación por la empresa que ejecute el proyecto bajo el consentimiento del Ingeniero Supervisor.

Este gabinete deberá tener las mismas características que las mencionadas para el gabinete "B".

Ordenamiento Propuesto del GABINETE "A"



Ordenamiento Propuesto del GABINETE "B", "C", "D", "E"



5. Puertos libres:

Se deberá dejar como reserva la siguiente cantidad de puertos libres (en el switch y patch panel) para cada gabinete, según como se especifica a continuación:

GABINETE "A": 20 puertos libres.
GABINETE "B": 10 puertos libres.
GABINETE "C": 10 puertos libres.
GABINETE "D": 10 puertos libres.
GABINETE "D": 10 puertos libres.

6. Cable UTP:

- El cable UTP es el usado para el tendido del cableado horizontal, no debe exceder de 90 metros desde el Outlet al Patch Panel por cada enlace.
- Cable de cobre sólido Unshield Twisted Pair de 4 pares trenzados, 23-24 AWG, 100 Ohm, en presentación de cajas selladas.
- Debe cumplir o superar las especificaciones de la norma TIA/EIA 568-B.2-1 Transmission
- Performance Specifications for 4 Par 100 Ω Category 6 Cabling y los requisitos de cable categoría 6 (clase E) de la norma ISO/IEC 11801. Debe estar certificado por Laboratorios independientes: UL o ETL.
- El cable debe tener aislante de polietileno de alta densidad y la chaqueta del cable UTP debe ser del tipo CMR, tipo No Plenum.
- El cable debe tener un se parador de pares del tipo cruz y debe ser retardante a la flama.
- Se deberá utilizar cable UTP para exteriores en los tramos que corresponden a los ambientes fuera de oficinas y canalizaciones subterráneas.

7. Line Cords:

- El Line Cord es el cable utilizado para conectar el equipo periférico (PC, Servidor, Impresora, o similar) con la toma para datos conformada por el Jack y el Face Plate.
- El Line Cord debe estar conformado solamente por cable de cobre multifilar Unshield Twisted Pair de 4 pares trenzados 24 AWG, y con un plug RJ45 Categoría-6 de 8 posiciones en cada extremo. Debe estar confeccionado integralmente por el fabricante en configuración pin a pin según el esquema EIA/TIA 568A.
- Debe cumplir con las pruebas de performance de la EIA/TIA 568B.2-1 Categoría-6, certificados por Laboratorios independientes: UL o ETL.
- Los Line Cords deberán ser ensamblados y certificados de fábrica.
- Deberá contar con aislamiento dieléctrico en los plugs RJ45 en cada uno de los pares a fin de mejorar el parámetro de acoplamiento NEXT.
- Debe tener una variedad de 8 colores para poder identificar el servicio según la TIA/EIA 606A.
- Los Plug RJ45 de cada Line Cord deben tener un sistema anti enredo o capuchas como parte del Plug RJ45 para evitar atascos durante movimientos o reordenamiento y no deberán tener algún accesorio que amplíe sus dimensiones laterales.
- La longitud del Line Cord debe ser no mayor a 3 metros.

8. Patch Cords:

- El Patch Cord es el cable utilizado para conectar el Patch Panel con el equipo activo de red (switch, hub o similar) en configuración directa o en configuración cross-connect.
- El Patch Cord Categoría-6 debe estar conformado solamente por cable de cobre multifilar Unshield
- Twisted Pair de 4 pares trenzados 24 AWG y con un plug RJ45 Categoría-6 de 8 posiciones en cada extremo. Debe estar confeccionado integralmente por el fabricante en configuración pin a pin según el esquema 68B.2-1 Categoría-6.
- Los Patch Cords deberán ser ensamblados y certificados de fábrica.
- Debe tener una variedad de 8 colores para poder identificar el servicio según la TIA/EIA 606A.
- Deberá contar con aislamiento dieléctrico en los plugs RJ45 en cada uno de los pares a fin de mejorar el parámetro de acoplamiento NEXT.
- Los Plug RJ45 de cada Parch Cord deben tener un sistema anti enredo o capuchas como parte del Plug RJ45 para evitar atascos durante movimientos o reordenamiento y no deberán tener algún accesorio que amplié sus dimensiones laterales.

- Debe cumplir con las pruebas de performance de la EIA/TIA 568B.2-1 Categoría-6, certificado por
- Laboratorios independientes: UL o ETL.
- La chaqueta del cable UTP debe ser de PVC, tipo No Plenum.
- La longitud del Patch Cord debe ser de 1.5 metros para los gabinetes. Garantizando un correcto ordenamiento de cables con los ordenadores solicitados para el patch panel y gabinete.
- Se deberán suministrar adicionalmente 10 patch cords Categoría-6 de 3m de longitud, para realizar las conexiones entre el servidor, router y enlaces dentro del gabinete "A". Estos patch Cords deberán ser de diferente color a los utilizados dentro del gabinete para que puedan ser diferenciados.

9. Patch Panel:

- El patch panel debe ser de 19 pulgadas para ser montado sobre los bastidores de los gabinetes. La base del patch panel debe ser de material metálico.
- Cada jack del patch panel debe cumplir con las pruebas de performance de la EIA/TIA 568B.2-1 Categoría-6, certificado por laboratorios independientes: UL o ETL.
- Cada puerto del patch panel debe contar con sistema de identificación por etiquetas frontal.
- Cada puerto deberá estar etiquetados en la parte posterior para trabajar con el sistema de cableado tipo T568A.
- Cada puerto frontal RJ45 debe soportar como mínimo 500 inserciones de Plug RJ45 de 8 posiciones.
- El patch panel debe permitir una fuerza de retensión suficiente para evitar la desconexión, tanto del plug RJ45 como del cable sólido instalado en él.
- Deben contar con una protección plástica transparente, para grupos de 4 puertos, que impida el contacto directo de las manos u otros objetos con las etiquetas garantizando con ello su longevidad de acuerdo a la ANSI/TIA/EIA 606A.

10. Outlets:

- Deberán instalarse face plates dobles por área de trabajo, la salida no utilizada deberá ir con tapa ciega.
- Deberá tener un icono de identificación al lado de cada salida RJ45 para identificar si el servicio es de telefonía o datos.
- Las salidas del faceplate deberán tener un ángulo de inclinación de 45º para asegurar el radio de giro de los patch cords.
- El FacePlate debe instalarse en una caja plástica adosable del tipo 4" x 2" o en la canaleta adecuada para este módulo, debiendo encajar correctamente en esta. No se aceptarán rosetas.
- Debe incluir sus tornillos de sujeción y etiquetas de identificación para cada puerto del Face Plate, con cobertor de policarbonato transparente.

11. Canaletas:

- Las canaletas plásticas que se utilicen deberán tener en una de sus caras tapas removibles, ángulos internos y externos, para poder realizar el mantenimiento y crecimiento de puntos.
- Deberán cumplir con las normas internacionales: EIA/TIA569-A para el radio de curvatura, certificación UL (nivel de flamabilidad), herméticas, no conductivas, resistente a los impactos, auto- extinguibles y resistente a los rayos UV.
- Se deberán utilizar dos tipos de canaletas:
  Canaleta Principal : Será utilizada para el recorrido principal, como pasadizos. Las canaletas deberán ir empernadas. Los tamaños de estas canaletas estarán en función de los cables a pasar, dejando un margen del 40% adicional según recomienda la norma, para un

posible crecimiento.
Deberán instalarse todos los accesorios necesarios como ángulos internos y externos, así como las uniones y tapas finales.
Canaleta Secundaria: Estas canaletas serán las derivaciones de las canaletas principales, éstas ingresarán a las oficinas de cada sede hacia los puntos de usuario. Deberán instalarse todos los accesorios necesarios como ángulos internos y externos, así como las uniones y tapas finales.

- Las canaletas (principal y secundaria) deberán asegurar el radio de giro para Categoría-6.
- En caso de ser necesario instalar cajas de pase para cableado de datos, estas deben ser de la misma marca que la proporcionada para las canaletas.

12. Cableado de Backbone y Cruces:

Toda canalización en exteriores deberá hacerse de forma subterránea, no deberá existir ninguna canalización o cruce aéreo, salvo casos extremos justificados y aprobados por el Ingeniero Supervisor de EsSalud.

En el plano de Distribución de Puntos de la Sede Hospital III Iquitos – LORETO se sugieren las rutas que deben seguir. Éstos finalmente quedan a criterio del proveedor, previa coordinación con el Ingeniero Supervisor de EsSalud.

Se deben tener en cuenta los siguientes requerimientos generales para las canalizaciones:

- Utilizar tubos PVC SAP, de 2" como mínimo.
- Utilizar curvas normalizadas, no codos de 90º. Cumplir con la norma ANSI/EIA/TIA 569A.
- Las cajas de paso exteriores deberán ser empotradas en la pared, galvanizadas y pintadas de acuerdo al color original de la pared.
- Todas las instalaciones deberán ser impermeables y resistentes a lluvias.
- Las zanjas deberán cumplir con los siguientes requerimientos:
- Las dimensiones deberán ser de 45 cm de ancho x 60 cm de profundidad.
- Deberá agregarse 20 cm de arena fina debajo de los tubos PVC.
- La distancia mínima de separación entre el ducto PVC para datos y la parte eléctrica deberá ser de 15 cm.
- Se deberá agregar desmonte retirado previamente cernido (aproximadamente 20 cm) y compactar.
- Se deberá agregar una capa de 10 cm de afirmado y compactar.
- Se deberá agregar una capa de 10 cm de concreto y/o asfalto, donde sea necesario.
- En caso de romper piso de tipo cerámico u otro deberán reponerse los paños completos.
- Se debe dejar las instalaciones en iguales o mejores condiciones a las entregadas a la ejecución de las obras, cuidando mucho la apariencia estética de las instalaciones.

13. Documentación:

El contratista deberá entregar como documentación final:

- Reporte de pruebas del total del cableado (certificación de puntos).
- Diagramas de topología, distribución, esquemas de los gabinetes de telecomunicaciones (en forma impresa y digital).
- Planos detallados con la ubicación de los puntos instalados, la numeración por punto, cajas de paso, acometidas eléctricas, pozo a tierra y las rutas de la canalización de interiores y exteriores.
- Los planos de distribución de las oficinas serán entregados en formato digital (Autocad) a la empresa contratista para su edición.

14. Certificación de puntos:

El contratista deberá certificar todos los puntos de red (canal completo) en Categoría-6 utilizando los probadores de campo adecuados.

El proceso de certificación de puntos deberá ser realizado en presencia del Ingeniero Supervisor de EsSalud, o técnico designado por él mismo.

El reporte del instrumento de medición es imprescindible para que el Ingeniero Supervisor de EsSalud de conformidad al trabajo.

15. Garantía y tiempos de respuesta:

Tres (03) años para materiales y mano de obra, con 24 horas de tiempo de respuesta después de haberse reportado la falla. La cobertura de la garantía y tiempo de respuesta solicitado deberá abarcar la ubicación de la Sede Hospital III IQUITOS – LORETO.

Acometidas Eléctricas y Tableros Eléctricos

1. Acometidas Eléctricas:

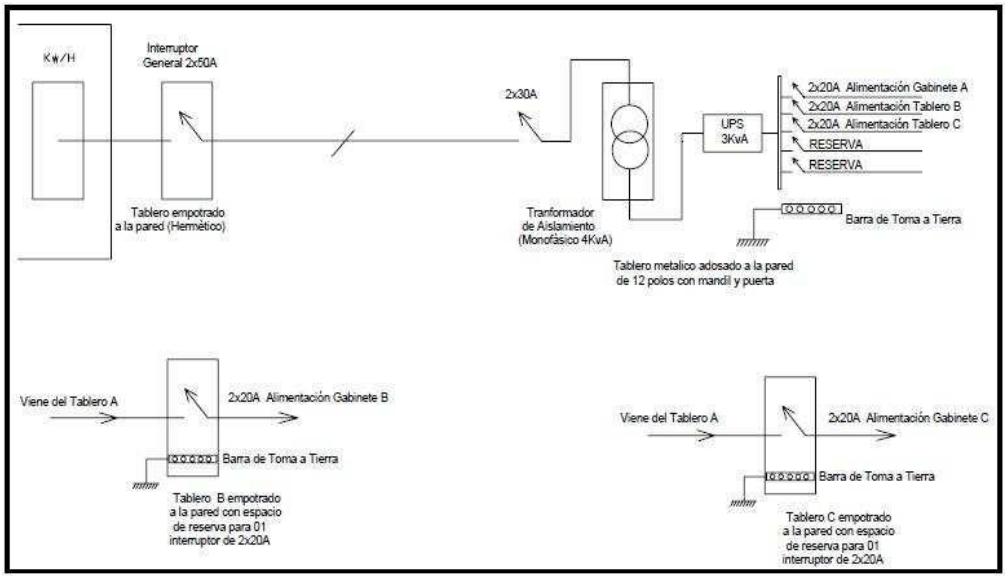
- Se deberán instalar las acometidas eléctricas desde el medidor de Corriente Principal hasta el tablero eléctrico del GABINETES "A", donde estará ubicado el UPS.
- La acometida eléctrica que parte desde el medidor de corriente principal hasta el tablero eléctrico del GABINETE "A" deberá tener un mínimo de 10 mm2 y deberá utilizar cables de tipo NYY,
- vulcanizado o similar, que aseguren una protección adecuada frente a las condiciones ambientales de la Región.
- Instalación de un circuito eléctrico desde la ubicación del tablero de UPS hasta el tablero eléctrico del GABINETE "B".
- Instalación de un circuito eléctrico desde la ubicación del tablero de UPS hasta el tablero eléctrico del GABINETE "C".
- Instalación de un circuito eléctrico desde la ubicación del tablero de UPS hasta el tablero eléctrico del GABINETE "D".
- Instalación de un circuito eléctrico desde la ubicación del tablero de UPS hasta el tablero eléctrico del GABINETE "E".
- Los cables de acometida para los gabinetes secundarios "B", "C", "D" y "E", deberán ser de tipo NYY, vulcanizado o similar.
- No se permitirá utilizar empalmes en ducterías.
- La ubicación del Medidor de Corriente Principal se indica en el plano adjunto.
- Se deben cumplir los mismos requerimientos para la construcción de la zanjas, tal como es especificado en la sección "Cableado de Backbone y Cruces".
- Seguir los lineamientos indicados en el diagrama (Punto 5.3).

2. Tableros Eléctricos:

- Se deberán instalar los tableros eléctricos para los GABINETES "A", "B", "C" y "D", los cuales deberán ser ubicados al costado de cada gabinete a una altura de 1.20m a partir de la base del tablero.
- Los tableros se instalarán adosados a la pared.
- Deberán llevar una calcomanía autoadhesiva en la tapa que indique peligro, riesgo de electrocutarse.

- Incluir interruptores termomagnéticos, según el dimensionamiento mostrado en el diagrama (Punto 5.3).
- Seguir los lineamientos indicados en el diagrama (Punto 5.3).

3. Diagramas:



Nota: Considerar el Tablero Eléctrico "C", en caso de ser aplicable.

Sistema Puesta a Tierra

1. Requerimientos Generales:

- Se requiere la instalación de un sistema de puesta a tierra menor a 4.50 ohm, con capacidad para soportar como mínimo 40 amperios, para la protección eléctrica de los equipos que serán instalados en los GABINETES "A", "B", "C" y "D" y garantizar su crecimiento futuro.
- Se deberá utilizar tierra de chacra para el relleno del foso, cable de calibre 6 AWG (mínimo), ductería de 16mm, barra de tierra de interconexión y caja de registro de alto impacto.
- Las dimensiones del foso no deberán exceder 5m x 1m x 2m, debido a las restricciones de espacio disponible.
- Se deberá suministrar todos los materiales y/o mano de obra requeridos a todo costo para la instalación del sistema de puesta a tierra.
- El proveedor deberá minimizar el espacio requerido para la instalación del sistema de puesta a tierra, cumpliendo las especificaciones indicadas.
- El proveedor deberá realizar la medición con telurómetro digital y entregar un informe técnico de los resultados obtenidos de la instalación. La medición del sistema de puesta a tierra deberá ser realizada en presencia del Ingeniero supervisor de EsSalud.
- Deberá garantizarse su correcto funcionamiento perdurable por 5 años libres de mantenimiento.
- De ser el caso se podrá aprovechar la zanja abierta para la canalización de datos (utilizando una ductería independiente) que viene del GABINETE "B" y "C" hacia el GABINETE "A".
- Los componentes químicos del sistema de puesta a tierra, no deberán contener productos nocivos y/o contaminantes para el medio ambiente.

6.2. Ubicación:

Se recomienda ubicarlo en un área próxima al Edificio "A", como se muestra en el plano de Distribución de la Sede Hospital III IQUITOS – LORETO. La empresa que ejecute el proyecto podrá sugerir otra ubicación del sistema de puesta a tierra, justificando debidamente las razones técnicas y siendo aprobado por el Ingeniero Supervisor de EsSalud.

6.3. Documentación:

El proveedor deberá entregar la documentación general del sistema eléctrico instalado, incluyendo diagramas y reportes de pruebas.

- Carta de garantía de libre mantenimiento durante 5 años, del fabricante o representante para el Perú del producto ofertado.
- Carta del fabricante o de la empresa que ejecute el proyecto, garantizando que los componentes químicos del sistema de puesta a tierra no contaminan el medio ambiente.

Capacitación

El proveedor deberá proporcionar capacitación in situ con un total de 08 horas (mínimas) sobre:

- Mantenimiento general y operación del sistema eléctrico, UPS y puesta a tierra.
- Recomendaciones generales para el mantenimiento del cableado estructurado y gabinetes.

Switches de Red

Los switches de red deberán cumplir como mínimo con los siguientes requisitos técnicos y condiciones:

	Firma :			
	Pais de Origen :			
	Fabricante:			
	Características a tomar en cuenta	**CUMPLE**		
1	**ESPECIFICACIONES TECNICAS SWITCH**	**SI**	**NO**	**OBSERVACIONES**
1.1	Factor de Forma: Montable en rack, 1RU, incluye manijas de montaje para rack.			
1.2	Número de puertos: Mayor o igual a 24 puertos.			
1.3	Puertos Gigabit: 02 puertos (adicionales) Gigabit Ethernet 1000base-T vía RJ45.			
1.4	Características de los puertos: 10/100TX (conectores RJ45). Autonegociables. Auto MDI/MDI-X			
1.5	Capas: Operación en Capas 2 y 3 (Layer 2, 3)			
1.6	Modo de operación: Store adn Forward.			
1.7	LEDs indicadores: LINK/ACT, velocidad y estado duplex para cada puerto			

1.8	Soporte de protocolos / características: VLANS basadas en puerto, port trunking, port mirroring, port based and IEEE 802.1p-based QoS			
1.9	Control de acceso: Basado en contraseña			
1.1	Performance mínimo: 8.8 Gbps (mínimo), Memoria de 8000 direcciones MAC (mínimo).			
1.11	Apilamiento: Mínimo de 2 Gbps a través de puertos gigabit ethernet (10/100/1000 RJ45 o SFP).			
1.12	Características de Red: Soporte de Listas de Control de Acceso en capas 2 / 3 / 4, Clase de Servicio y Priorización de Tráfico. Soporte de Filtrado Multicast y protocolo RIP.			
1.13	Alimentación de poder: Voltaje 100-240V AC.			
1.14	Cumplimiento de estándares: IEEE 802.3x, IEEE 802.1Q			
1.15	Administración: Software de administración basado en Web			
2	**Garantía**			
2.1	Tres años para partes			
2.2	Tres años para mano de obra On site			
2.3	Certificado de Garantía: Certificado de garantía otorgado por el fabricante o subsidiaria local, indicando el período de garantía de los equipos ofertados, detallando las condiciones y características de la garantía; como son reposición de partes y equipos de respaldo.			
2.4	Tiempo de respuesta: 24 horas después de haberse [illegible]			
3	**Otros**			
3.1	Accesorios: El equipo deberá contar con sus accesorios, cables de conexión, y documentación.			

Servidor

El servidor deberá cumplir como mínimo con los siguientes requisitos técnicos y condiciones:

	Firma:			
	Pais de Origen:			
	Fabricante:			
	Características a tomar en cuenta	**CUMPLE**		
1	**ESPECIFICACIONES TECNICAS - SERVIDOR**	**SI**	**NO**	**OBSERVACIONES**
1.1	Factor de forma: Torre, con opción de convertir a rack mediante un kit (no se requiere incluir el kit de conversión a rack)			
1.2	Procesador: Doble Núcleo			
1.3	Velocidad del Procesador: 1.86 GHz por cada núcleo o superior			
1.4	Memoria cache: Nivel 2 de 4MB (1 x 4MB)			

1.5	Expansión SMP: Opción de adicionar un segundo procesador			
1.6	Memoria RAM: 01 GB con ECC			
1.7	Puertos: 2 USB (USB 2.0), 1 serial, 1 PS/2			
1.8	Controladora SCSI: Con soporte para RAID 0 y 1			
1.9	Disco Duro: 01 SCSI de 72 GB, 10K RPM, Hot Swap			
1.1	Lectora de CD-Rom: 48X o superior			
1.11	Tarjetas de Red: 02 tarjetas de 10/100/1000 con conector RJ45			
1.12	Tarjeta de Video: 16 Mb. de memoria (o superior)			
1.13	Teclado: En inglés (US)			
1.14	Mouse: PS/2 o USB, 2 botones, con scroll			
1.15	Monitor: 17 pulgadas			
2	**Garantía**			
2.1	Tres años para partes.			
2.2	Tres años para mano de obra On site.			
2.3	Certificado de Garantía: Certificado de garantía otorgado por el fabricante o subsidiaria local, indicando el período de garantía de los equipos ofertados, detallando las condiciones y características de la garantía; como son reposición de partes y equipos de respaldo.			
2.4	2.4 Tiempo de respuesta: 24 horas después de haberse reportado la falla.			
3	**Certificaciones**			
3.1	Certificación del Fabricante: Carta del fabricante del producto o subsidiaria local en donde acredite de forma expresa la propuesta del servidor y sus componentes que está presentando el postor a EsSalud.			
3.2	Certificación del producto: El producto ofertado deberá estar certificado bajo las normas ISO9000, CE, FCC Clase A, UL. Adjuntar carta del fabricante acreditando dicha certificación.			
4	**Otros**			
4.1	4.1 Accesorios: Los equipos deberán contar con sus accesorios, cables de conexión, documentación y software necesario para su correcto funcionamiento.			
4.2	Compatibilidad: Indispensable compatibilidad con el sistema operativo RedHatLinux Enterprise Linux 5 (o versión vigente).			

Sistema de Alimentación Ininterrumpida (UPS)

El UPS deberá cumplir como mínimo con los siguientes requisitos técnicos y condiciones:

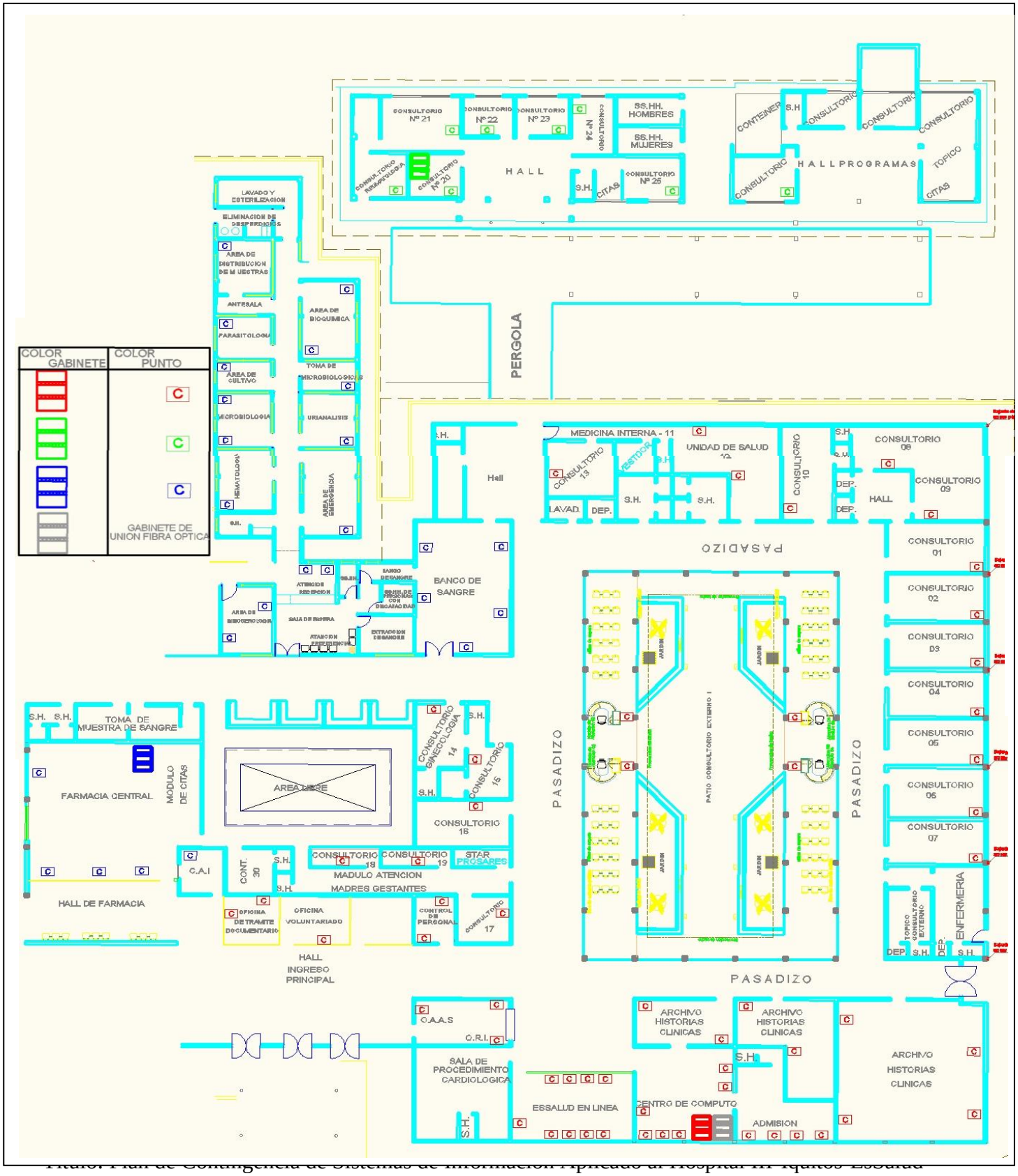
	Firma:			
	Pais de Origen:			
	Fabricante:			
	Características a tomar en cuenta	**CUMPLE**		
1	**ESPECIFICACIONES TECNICAS - UPS**	**SI**	**NO**	**OBSERVACIONES**
1.1	Tecnología: On Line de doble conversión			
1.2	**Especificaciones de entrada (INPUT)**			
1.2.1	Voltaje (Vac): 160 a 280			
1.2.2	Probabilidad (Hz): 50 / 60 +/- 5% (Auto Sensing)			
1.2.3	Fase: Monofásico			
1.2.4	Factor de entrada de poder: > 0.98 (a plena carga)			
1.3	**Especificaciones de Salida (OUTPUT)**			
1.3.1	Voltaje (Vac): 220/230/240			
1.3.2	Capacidad (VA/W): 3000VA / 2100W			
1.3.3	Factor de Potencia: 0.7			
1.3.4	Forma de onda: Senoidal, THD < 3% (no load to full load)			
1.3.5	Regulación de voltaje: +/- 2%			
1.3.6	Respuesta transitoria (ms): +/- 4% a plena carga, cambio y corrección en 60 ms.			
1.3.7	Estabilidad de probabilidad: +/- 0.5Hz (free running)			
1.3.8	Sincronización: Slew Rate: 1Hz/Sec. Max. Ventana de Sincronización: +/- 5%			
1.3.9	Tiempo de transferencia: 0 ms por ser Doble Conversión Continua			
1.3.10	Factor de cresta: 3:1			
1.3.11	Eficiencia: (AC-AC): > 88%			
1.3.12	Autonomía (Plena carga): 8 min			
1.3.13	Arranque en frío (con baterías sin AC): Si			
1.4	**Batería**			
1.4.1	Tipo: Selladas de plomo ácido y del tipo libres de mantenimiento			
1.4.2	Cantidad : 8			
1.4.3	Voltaje (Vdc): 96			
1.4.4	Tiempo de recarga: 8 Horas al 90%			
1.5	**Protección**			

1.5.1	Corto circuito: Apagado y reposición manual			
1.5.2	Sobre temperatura: Transferencia a Bypass			
1.5.3	Sobre voltaje (High voltage trip): Transferencia a baterías			
1.5.4	Batería baja: Alarma de alertar y apagado del equipo			
1.6	**1.6 Protección de sobrecarga en modo AC**			
1.6.1	< 105% continuamente			
1.6.2	105% - 120% por 50 segundos antes de la transferencia a bypass			
1.6.3	120% - 150% por 10 segundos antes de la transferencia a bypass			
1.6.4	> 150% transferencia inmediata a bypass			
1.7	**Aspectos físicos**			
1.7.1	Con capacidad para ser montable en rack			
1.7.2	Salidas (IEC/Local) 220/230 Vac: Terminal/2pcs			
	Interconexión con PC: RS232, software de administración			
1.8	**compatible con Windows 98/2000/XP.**			
1.9	**Alarmas: Falla de línea, batería baja, transferencia a bypass, condiciones de falla del sistema.**			
1.10	**Panel de Información (Display)**			
1.10.1	LEDs: Entrada AC, Batería, Inversor, Bypass, Autotest, Sobrecarga, Nivel de Carga y baterías, Condiciones de Falla.			
2	**Garantía**			
2.1	Tres años para partes			
2.2	Tres años para mano de obra On Site			
2.3	Certificado de Garantía: Certificado de garantía otorgado por el fabricante o subsidiaria local, indicando el período de garantía de los equipos ofertados, detallando las condiciones y características de la garantía; como son reposición de partes y equipos de respaldo.			
2.4	Tiempo de respuesta: 24 horas después de haberse reportado la falla.			
3	**Otros**			
3.1	Accesorios: El equipo deberá contar con sus accesorios, cables de conexión, y documentación.			
3.2	Instalación: El UPS deberá ser instalado y puesto en operatividad por el proveedor, dentro del Gabinete "A" de cada Oficina de EsSalud según indicación.			
3.3	Certificación ISO 9001			

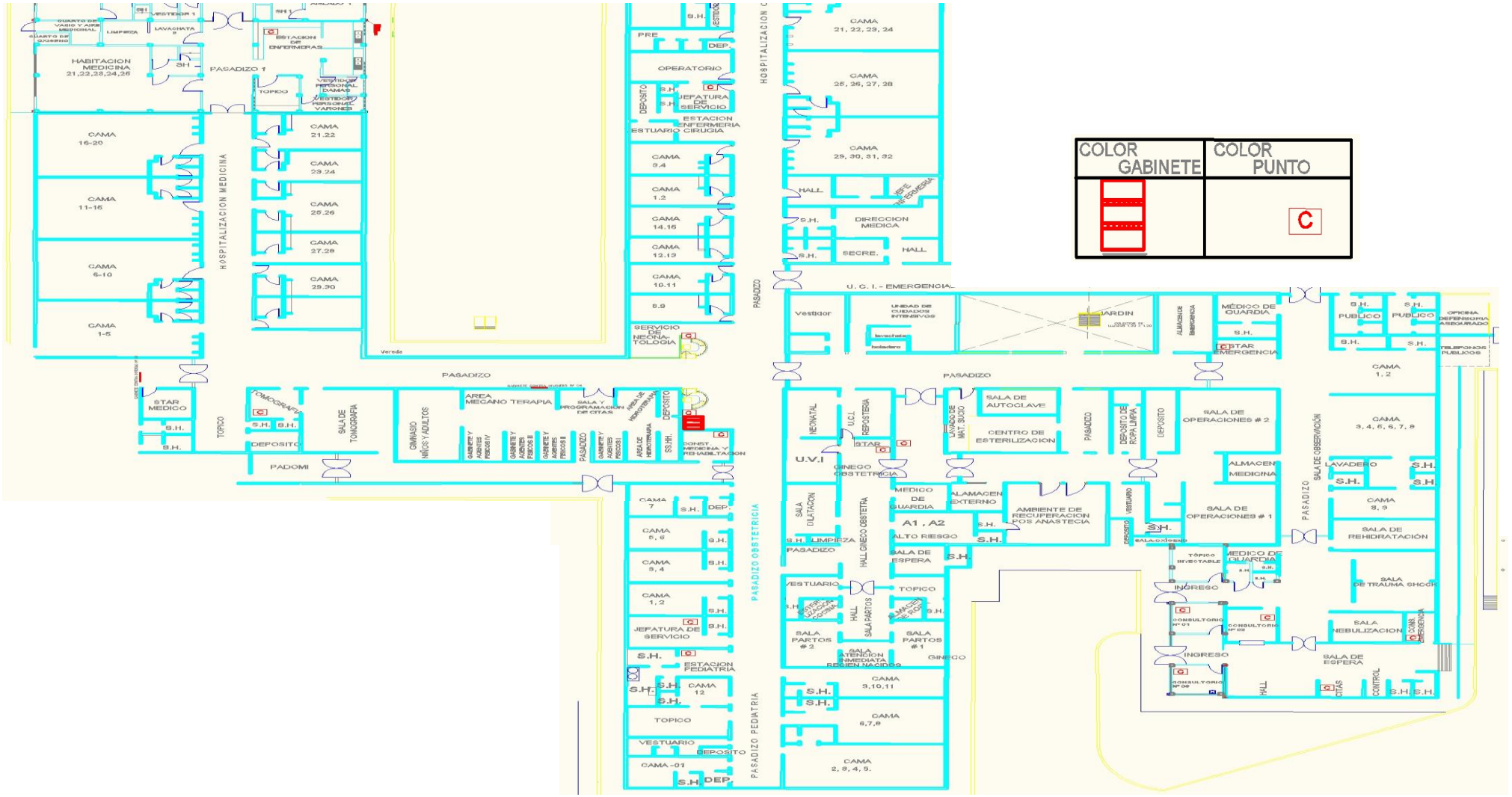
Modelo de Estructura de Costos

Ítem	Descripción	Costo
1	Cableado Estructurado: Instalación de 60 puntos Categoría-6 certificados.	
2	Gabinetes: 01 de 45 RU (de piso) + accesorios y 02 de 12 RU (de pared) + accesorios.	
3	Backbone y Cruces: Canalización exterior, cajas de paso, enlaces de red.	
4	Acometidas Eléctricas: 03 acometidas desde el medidor de corriente principal hacia los Gabinetes A, B y C.	
5	Tableros Eléctricos: 03 tableros adosados a la pared con sus interruptores termomagnéticos.	
6	Sistema de Puesta a Tierra: Menor a 5 ohmnios, de cemento conductivo.	
7	Switches de red: 02 de 48 puertos, 01 de 24 puertos.	
8	Servidor: Xeon Dual Core 1.8 GHz, 1 GB RAM, HD SCSI 72 GB HS, Monitor 17".	
9	UPS: En línea de doble conversión, 3000VA.	
10	Transformador de Aislamiento	
11	Viáticos y Fletes	
	TOTAL	

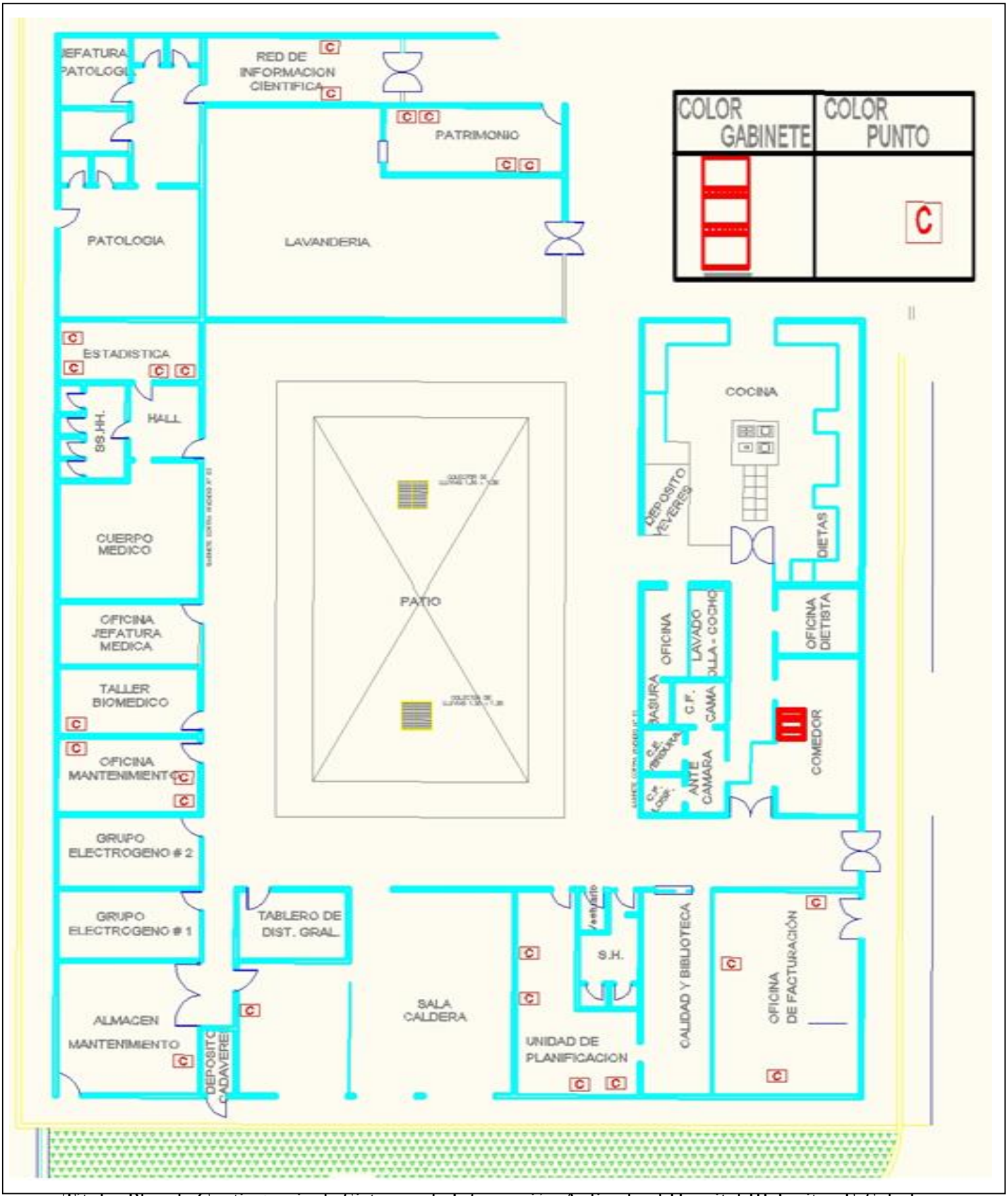
PLANO DEL EDIFICIO (LOCAL SEDE CENTRAL LORETO)
EDIFICIO "A" PRIMER NIVEL (Existen 03 Gabinetes)



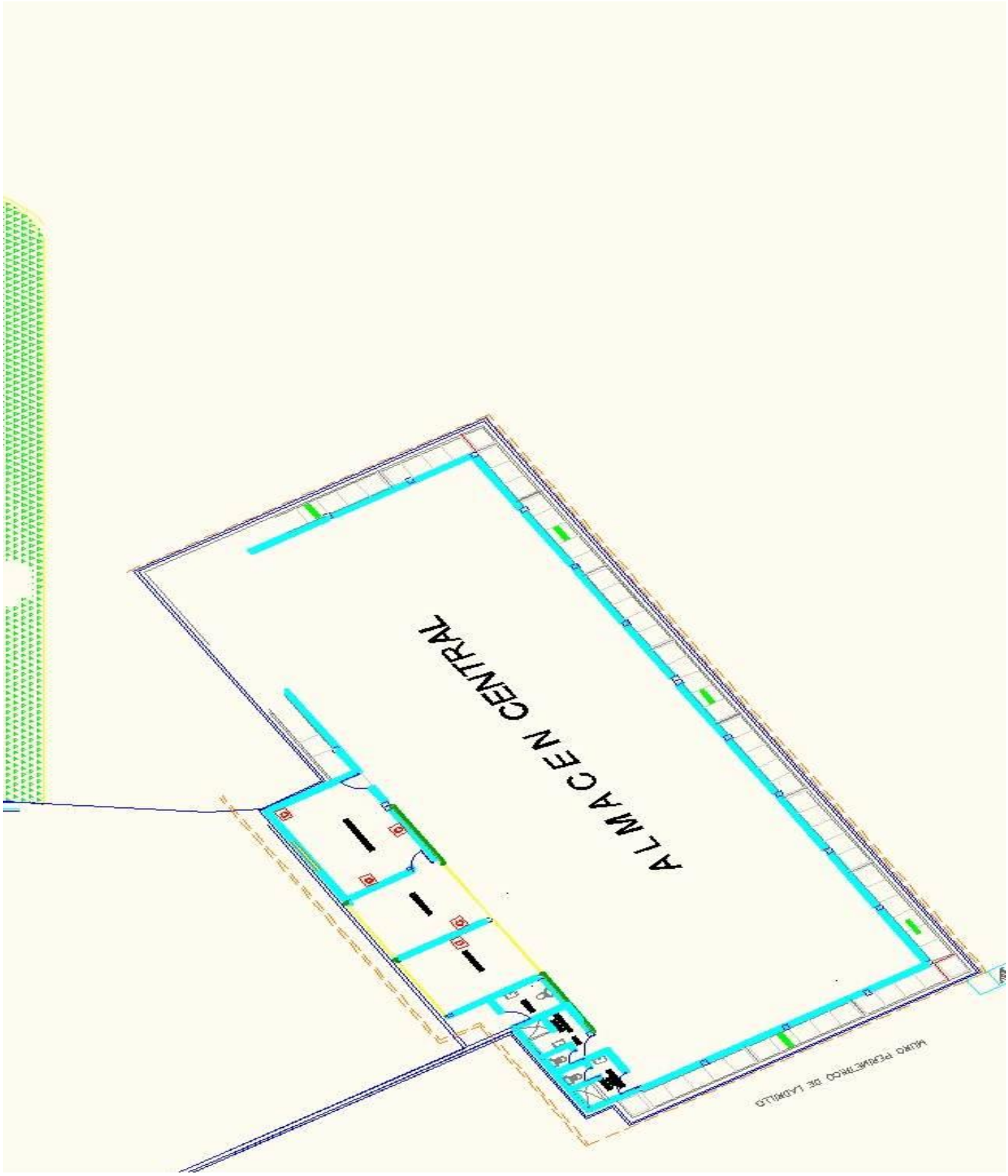
PLANO DEL EDIFICIO (LOCAL SEDE CENTRAL LORETO)
EDIFICIO "A" SEGUNDO NIVEL (Existe 01 Gabinete)



EDIFICIO "A" TERCER NIVEL (Existe 01 Gabinete)



EDIFICIO "B" PRIMER NIVEL
(Esta interconectado con el Gabinete del Edificio "A" Tercer Nivel)



Vista Completa de la unión de los Edificios por medio de un Gabinete