ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"IMPLEMENTACIÓN DE UN PLAN DE CONTINGENCIA A LA INTRANET DEL IESS HOSPITAL DE ANCÓN BASADO EN LA METODOLOGÍA ITIL"

EXAMEN DE GRADO (COMPLEXIVO)

Previo a la obtención del Título de:

MAGÍSTER EN SEGURIDAD INFORMÁTICA APLICADA

NELLY DEL ROCÍO BALÓN MAGALLAN

GUAYAQUIL – ECUADOR

AÑO: 2016

AGRADECIMIENTOS

Gracias a Dios porque cada día bendice mi vida con la hermosa oportunidad de estar y disfrutar al lado de las personas que me aman. A mi familia por ser los principales promotores de mis sueños, por confiar en mí y apoyarme en cada decisión y proyecto.

DEDICATORIA

El presente proyecto lo dedico a mi familia, mis padres, mi esposo y mis hijos. Este nuevo logro es en gran parte gracias a ustedes, al haber logrado concluir con éxito este proyecto. Quisiera dedicarles mi tesis, por ser siempre mi apoyo incondicional en todo momento.

TRIBUNAL DE SUSTENTACIÓN

Ing. Lenin Freire

DIRECTOR DE MSIA

Mgs. Robert Andrade

PROFESOR DELEGADO POR LA UNIDAD ACADÉMICA

Mgs. Néstor Arreaga

PROFESOR DELEGADO POR LA UNIDAD ACADÉMICA

RESUMEN

En el presente proyecto de titulación se desarrolla un Plan de Contingencias a la intranet del IESS Hospital de Ancón tomando como base la metodología ITIL. El primer capítulo muestra los antecedentes, la problemática del Hospital, se detalla la solución propuesta para mitigar los posibles riesgos encontrados, basándose en objetivos para cumplir el fin propuesto.

El segundo capítulo detalla la situación actual de la intranet del IESS Hospital de Ancón, la estructura de cómo está compuesta la infraestructura tecnológica. El tercer capítulo muestra un diseño de cómo se estructura el plan de contingencia iniciando con la identificación de equipos que conforman la intranet, identificación de riesgos, las amenazas, estableciendo planes de recuperación antes siniestros, planes de entrenamiento al personal involucrado en el proceso de las contingencias, en este capítulo se diseña las estrategias a seguir con la continuidad de los procesos de acuerdo a diferentes escenarios.

El cuarto capítulo finaliza con los procesos de implementación del plan de contingencia, los controles y tratamiento de riesgos. Adicional se establecen las pruebas a realizarse en el plan con la finalidad de establecer un esquema de seguridad en el Hospital.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍA

AP	Access Point (Punto de Acceso)
DNTI	Dirección Nacional de Tecnologías de Información
DOS	Denegación de Servicios
HW	Hardware
ISACA	Information Systems Audit and Control Association (Asociación de Auditoría y Control de Sistemas de Información)
LAN	Local Area Network (Red de Área Local)
PAC	Plan Anual de Contratación
SW	Software
WAN	Wide Area Network (Red de Área Amplia)

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

La seguridad de la información es considerada como un problema sólo tecnológico, no se toma en cuenta que la seguridad de la información es un problema organizativo y de gestión, las organizaciones no están preparadas para afrontar ataques derivados de cualquier lado.

Para realizar el plan de contingencia de la intranet del IESS Hospital de Ancón se tiene en cuenta la información como uno de los activos más importantes de la Institución, además que la infraestructura tecnológica está conformada por todos elementos necesarios para el manejo de la información que utiliza el hospital. Este plan implica efectuar un análisis de los riesgos de todos los equipos y sistemas que integran la intranet, pudiendo así emplear medidas de prevención para enfrentar contingencias.

El plan de contingencia permitirá salvaguardar la continuidad de los sistemas ante situaciones críticas del hospital disminuyendo impactos negativos que puedan afectar al nosocomio, a los empleados y afiliados; estos deben ser parte primordial de la institución y servir para evitar complicaciones, estar capacitados para fallas potenciales buscando en conjunto una solución.

Este plan ha sido elaborado tomando como base, la Metodología ITIL (Biblioteca de Infraestructura de Tecnologías de la Información), en el cual se mostrara el establecimiento de estándares que ayudaran en el control y administración de los recursos.

CAPÍTULO 1

1. GENERALIDADES

1.1 Antecedentes

Cualquier infraestructura de red está expuesta a diversos factores de riesgo humano y físicos pudiendo ser fuente de problemas.

Frente a cualquier evento, la velocidad en la determinación de la amenaza del problema depende de la capacidad y las estrategias a utilizar para señalar con precisión.

Pueden originarse pérdidas trágicas a partir de fallos de dispositivos críticos, bien por grandes o por fallas técnicas que producen daños

materiales irreparables. Ante los desastres solo queda el tiempo de recuperación, lo que significa adicionalmente la fuerte inversión en recurso humano y técnico para reconstruir la infraestructura de red y el sistema de información.

1.2 Descripción del problema

Las instituciones públicas día a día generan conocimientos, datos, material de diferente índole de suma importancia, lo cual representa toda la información que requieren para su funcionalidad. Esta información normalmente es almacenada en diferentes medios, siendo expuesta a personal que requiere hacer uso de la misma para reportes, toma de decisiones, entre otros.

La fuente de datos más valiosa con que cuenta una institución pública de salud, ya sea para conocer las características de la población afiliada, evaluar los resultados de la atención ofrecida, identificar los problemas de mayor prioridad es la información, para que este propósito se pueda lograr es necesario que existan medios que faciliten el ágil almacenamiento y utilización de los datos para que sean viables al ser utilizados por el personal de salud.

Tomando como caso de estudio el IESS Hospital de Ancón se puede determinar que los niveles de seguridad de la información en la intranet no son los adecuados los cuales pueden estar expuestos a vulnerabilidades, debido al crecimiento y expansión que tiene la unidad, la probabilidad de que la información sea interceptada y/o modificada por personas sin autorización de acceso aumenta exponencialmente lo cual resulta delicado. La información que se maneja es fundamental e importante para la realización de procesos la misma que puede ser vulnerada y amenazada ocasionando la interrupción de dichos procesos que conllevan de esta manera a una pérdida de información vital para el hospital.

Actualmente las instituciones tienen gran dependencia por la tecnología, esto hace necesario contar con una plataforma tecnológica confiable. Un incidente en la infraestructura tecnológica de unas pocas horas de duración en la intranet del IESS Hospital de Ancón puede tener un impacto catastrófico en las atenciones médicas ya que todos los registros médicos de la población afiliada se encuentran automatizados.

Por lo anteriormente expuesto se puede determinar que es de vital importancia contar con un plan de contingencia que permita obtener acciones que reduzcan la toma de decisiones durante las operaciones de recuperación de la infraestructura tecnológica, recupere eficazmente los

servicios críticos y permita un normal funcionamiento de los sistemas y procesos de inmediato, minimizando costos y niveles operativos.

1.3 Solución propuesta

Los grandes volúmenes de información que se manejan en la institución ya sea de parte contable, administrativa, operativa, información de registros médicos de afiliados constituyen un activo de gran importancia que actualmente no se protege con la prudencia necesario ni con las medidas formales que técnicamente se deben tener en cuenta en una institución.

La presencia de riesgos y amenazas tanto internas como externas hacen necesario generar la creación de medidas esenciales que logren proporcionar la seguridad de la información.

Este crecimiento de dicha información debido a su magnitud y responsabilidad con los afiliados del hospital necesita de mecanismos estandarizados.

Implementar un plan de contingencia en el IESS Hospital de Ancón permitirá:

- Realizar análisis de riesgos, identificando amenazas, vulnerabilidades e impactos en la entidad de salud.
- Establecer medidas de seguridad para gestionar los riesgos y ejecutar controles de tratamiento de riesgos.
- Mediante una estrategia de continuidad se puede establecer la viabilidad de la gestión.
- Garantizar la continuidad y disponibilidad del negocio.
- Definición de una estructura organizacional para el Plan de Contingencia en la intranet del IESS Hospital de Ancón.
- El incremento de los niveles de confianza de afiliados.
- Mayor compromiso y mejora de la seguridad.
- Identificar los puntos más críticos y vulnerables de los procesos en la intranet del IESS Hospital de Ancón.

Al establecer un plan de contingencia deben establecerse las expectativas sobre los riesgos del hospital en relación con la seguridad y especificar la autoridad responsable de aplicar los correctivos necesarios.

El propósito de implantar en el hospital un plan de contingencia es precisamente el de lograr garantizar que los riesgos de la seguridad de la información sean tomados con la responsabilidad del caso, documentados y estructurados.

1.4 Objetivo general

Analizar y diseñar un plan de contingencia basado en la metodología ITIL estableciendo los mecanismos adecuados para minimizar los riesgos asociados al uso de la información, de los sistemas y servicios informáticos aplicados en la intranet de la Institución pública de salud IESS Hospital de Ancón, otorgando un proceso de mejora continua y dotando a las mismas del concepto de calidad a la seguridad para la recuperación inmediata de la infraestructura tecnológica ante desastres Informáticos.

1.5 Objetivos específicos

- Garantizar la continuidad de las operaciones en la intranet del hospital evitando la suspensión de los servicios.
- Definir acciones y establecer procedimientos para ejecutarlos cuando se presentan fallas en elementos de la intranet.
- Garantizar la seguridad física, de todos los componentes involucrados en un sistema de información de datos.
- Establecer actividades que aprueben evaluar los resultados y retroalimentación del plan general.

1.6 Metodología

La Metodología ITIL (Biblioteca de Infraestructura de Tecnologías de la Información) son un conjunto de mejores prácticas y estándares en

procesos para hacer más eficaz el diseño y administración de las infraestructuras de datos dentro de la organización.

La metodología comprende: la identificación de riesgos, evaluación de la posibilidad de que ocurra un riesgo, evaluación del impacto en los procesos críticos y la creación de estrategias de contingencias.

ITIL especifica un método sistemático que garantiza la calidad de los servicios de TI. Ofrece una descripción detallada de los procesos más importantes en una organización de TI, incluyendo listas de verificación para tareas, procedimientos y responsabilidades que pueden servir como base para adaptarse a las necesidades concretas de cada organización [1].

Al aplicar esta metodología se podrá garantizar los requerimientos de la información en cuanto a seguridad, mantienen e incrementan sus niveles de fiabilidad, consistencia y calidad.

CAPÍTULO 2

2. ANÁLISIS SITUACIONAL DE LA INTRANET DEL IESS HOSPITAL DE ANCÓN

2.1 Antecedentes

El hospital tiene un área de 6.800 m², diariamente se atienden alrededor de 75 pacientes, de los cuales el 40% son mujeres, no solo de Ancón, sino de lugares cercanos tales como Santa Elena, La Libertad, Salinas, Anconcito, Ayangue, Valdivia, Palmar, Montañita, Atahualpa y otros sectores.

El mismo fue creado con el objetivo principal de desarrollar los mecanismos y las gestiones que permitan la implantación de un sistema de aseguramiento en salud, preferentemente para los afiliados y ciudadanos de la Provincia de Santa Elena, como una herramienta para

aumentar la cobertura, para brindar una atención de salud con calidad y calidez, contando con infraestructura y los soportes necesarios para su funcionamiento.

El IESS Hospital de Ancón es un hospital básico de nivel 1 que cuenta con la siguiente cartera de servicios. Ver Tabla 1, Tabla 2, Tabla 3.

Tabla 1. Cartera de Servicios

ORD	SERVICIO	N. DE PROFESIONALES POR ESPECIALIDAD	Nº CAMAS ACTUALES
1	Cirugía General	2	7
2	Ginecología y Obstetricia	3	9
3	Medicina Familiar y Preventiva	1	0
4	Urología	1	3
5	Cirugía Pediátrica	1	2
6	Anestesiología	2	0
7	Cardiología	1	0
8	Pediatría	2	7
9	Oftalmología	1	0
10	Medicina Interna	2	7
11	Odontología	2	0
12	Psicología	1	0
13	Nutrición	2	0
14	Dermatología	1	0
15	Medicina General	5	8
16	Emergencia	19	0
17	Laboratorio	5	0
18	Ecografía	1	0
19	Otorrinolaringología	2	0
20	Rayos X	3	0
21	Rehabilitación física	2	0
	TOTAL		48

Tabla 2. Emergencia

SERVICIO	CAMAS(ACTUALES)
Observación	3
Urgencias	1
Cuarto crítico	0
TOTAL	4

Tabla 3. Área Quirúrgica

TIPO	NÚMERO	OBSERVACIONES
Quirófanos	4	3 salas de quirófanos y 1 de partos
Sala de recuperación	1	
Esterilización	1	
TOTAL	5	

Para realizar el plan de contingencia en la intranet del IESS Hospital de Ancón se tiene en cuenta la información como uno de los activos más importantes de la unidad, además que la infraestructura informática está conformada por el hardware, software y elementos complementarios que soportan la información o datos críticos para la función de este nosocomio.

2.2 Infraestructura de red del Hospital

2.2.1 Ubicación física del Hospital

El IESS Hospital de Ancón se encuentra ubicado en la Provincia de Santa Elena, Cantón Santa Elena Parroquia Ancón, Barrio Otavalo, Calle Otavalo Número s/n, Intersección Calle Z, Detrás del Benemérito Cuerpo de Bomberos, con vigilancia las 24 horas del día.

El hospital posee dos pisos, distribuidos en área médica y área administrativa. En la planta alta se encuentran ubicados consultorios del área médica y en la planta baja las oficinas del área administrativa.

Con respecto a la disposición física de los equipos de redes del hospital, estos se encuentran ubicados en la planta alta en el área de Calificación de Derechos.

Los pisos ocupados por el hospital son de concreto, cuentan con cableado estructurado categoría 6 blindado, lo que facilita la administración de la red.

2.2.2 Estructura de red LAN del Hospital

La red LAN del IESS Hospital de Ancón se encuentra distribuida de la siguiente manera:

- 85 estaciones de trabajo (15 laptops y 70 computadores)

En el cuarto de servidores se tiene:

- Servidor HP PROLIANT DL380E GEN 8
- Switch HP 5500-48G-POE +- 4SFP HI
- Switch HP A5500-24G-EI-2SLOT
- Switch HP MSM710 MOBILITY CONTROLLER

- Switch HP 1910-24G-POE
- Switch HP A5120-24G POE
- Equipo optimizador de ancho de banda WAN

En exteriores:

- 6 access point HP MSM430 DUAL RADIO 802.11N AP (AM)
- SWITCH POE TPE-S80 8 PUERTOS 10/100 MBPS
- SWITCH DES-1016A DLINK 16 PUERTOS
- SWITCH TP-LINK TL-SF1016D 16 PUERTOS

La velocidad de transmisión por la red es de 100 Mbps por segundo.

2.2.2.1 Servidor

El servidor que posee el hospital tiene funcionalidades para dar habilitación de dominio e internet, cuyas características son las siguientes.

Tabla 4. Características del Servidor

HP PROLIANT DL380E GEN 8	
Procesador	Intel Xeon Six Core con tecnología VT
Disco Duro	1 TB
Memoria	20 GB DDR3 RDIMM
Configuración de arreglo	RAID 5 + Disco de Reserva
Sistema Operativo	Red Hat Enterprise Linux

2.2.2.2 Estaciones de trabajo

Las 85 estaciones de trabajo son empleadas para utilizar aplicaciones del área médica y administrativa tales como: Sistema Medico MIS AS-400, Sistema Contable Zebra, Sistema de Control y Ejecución Presupuestario, Sistema Nacional de Pagos a través de Red Pública (Sector Público y Cooperativas), Sistema Winsing, Sistema Evolution, Sistema de Control de Asistencia.

Además en la red LAN se encuentran conectadas 38 impresoras y 6 escáneres.

Actualmente en la red interna no se encuentra implementado ningún sistema de gestión que permita una administración de la red. Es decir no cuenta con ninguna herramienta de software, hardware que permita el monitoreo de la red y el análisis de vulnerabilidades.

2.2.3 Estructura de red WAN del Hospital

El IESS Hospital de Ancón cuenta con dos enlaces de datos, 1 principal contratado a la empresa Brigthcell y uno de backup de CNT

(Corporación Nacional de Telecomunicaciones), el acceso a Internet es facilitado por la DNTI (Dirección Nacional de Tecnologías de Información) perteneciente a la Matriz del IESS.

Cuenta con 2 módems que son propiedad de los proveedores del servicio de enlace de datos. Los que se encuentran conectados al Switch principal HP 5500-48G-POE +- 4SFP HI para proveer el servicio de datos a la red interna.

2.2.3.1 Enlace de comunicaciones

El IESS Hospital de Ancón cuenta para su funcionamiento con dos enlaces de datos, a continuación se da una descripción de cada uno de los enlaces:

Tabla 5. Características del enlace con Brigthcell

Proveedor	Brigthcell
Teléfono	(02) 2232329
Contacto	sclientes@brigthcell.com
Ancho de Banda	1 Mbps

Tabla 6. Características del enlace con CNT

Proveedor	Corporación Nacional de Telecomunicaciones
Teléfono	(04) 3731700
Contacto	cntcorp@cnt.gob.ec
Ancho de Banda	1 Mbps

2.3 Identificación de mecanismos de seguridad informáticos implementados actualmente en el Hospital

2.3.1 Políticas de uso de Hardware y Software

Con fecha 20 de enero del 2014 el área de TIC envía a la Dirección Administrativa mediante Memorando Nro. IESS-HANC-TIC-2014-0008-M en donde se detallan las políticas de uso de Hardware y de Software, documento en el cual se detalla las responsabilidades que cada usuario debe tener.

2.3.2 Seguridad de comunicaciones

ANTIVIRUS

El IESS Hospital de Ancón cuenta desde inicios del 2011 con 70 licencias corporativas del antivirus McAfee, con lo cual se tienen protegidas al Servidor de Dominio (licencia para servidor) y al número de PC`s indicadas (licencias Cliente).

Desde Internet se actualizan las listas de virus de McAfee, el mismo que se actualiza en el Servidor. Los usuarios son los responsables de actualizar sus propios antivirus y para esto tienen en su escritorio un icono apuntando a la última actualización bajada de Internet. No se hacen chequeos ocasionales para ver si se han actualizado los antivirus.

No se hacen escaneos periódicos buscando virus en los servidores ni en las PC´s. No hay ninguna frecuencia para realizar este procedimiento, ni se denominó a ningún responsable.

ATAQUES DE RED

En el hospital no disponen de herramientas para prevenir los ataques de red, hasta el momento no se han presentado este tipo de problemas. No hay herramientas para detección de intrusos.

No existen herramientas que detecten la Denegación de servicios para generar avisos y limitar el tráfico de red de acuerdo a los valores medidos.

CONTRASEÑAS

Las contraseñas de uso de los diferentes sistemas que utiliza el hospital están definidas por el administrador de cada sistema de manera inicial de forma que al momento de hacer uso por primera vez de los mismos debe proceder a cambiarlas.

Cada vez que se configura un usuario se indica al usuario la responsabilidad que conlleva el uso del mismo.

Una contraseña debe cumplir las condiciones siguientes [2]:

- No debe contener todo o parte del nombre del usuario.
- Debe tener una longitud mínima de 6 caracteres.
- Debe contener al menos 3 de las 4 categorías siguientes:
- Letras en mayúsculas (a a Z)
- Letras en minúscula de (a a z)
- Cifras (0a9)
- Símbolos (como por ejemplo;,!%-)

Mediante memorandos emitidos por la Dirección central del IESS se recalca la importancia y confidencialidad del manejo de usuarios.

SEGURIDAD DE INFORMACION

Los cuatro arquetipos de patrones relacionados con el ejercicio de la función de seguridad de la información (operaciones, gobierno, operaciones y gobierno, operaciones, gobierno y aspectos legales), que nos puede dar orientación sobre donde se encuentra ubicada la práctica actual [3].

Énfasis	Operaciones	Gobierno	Operaciones y gobierno	Operaciones, gobierno y aspectos legales
Responsabilidades	• Seguridad informática • Monitoreo y análisis de eventos • Respuesta a incidentes y análisis forense • Gestión de vulnerabilidades y amenazas	• Establecer el nivel de apetito al riesgo • Gestión de riesgos de seguridad de la información • Cumplimiento de TI • Riesgos de TI • Protección de la información • Clasificación de la información	Adicional a los que se tiene en operaciones y gobierno: • Gestión de riesgos de seguridad con terceras partes • Gestión de identidades y accesos • Diseño de arquitecturas de seguridad	• Notificación de brechas de privacidad • Protección de la información • Descubrimiento electrónico (Soporte electrónico de litigios) • Monitoreo y análisis de eventos • Respuesta a incidentes y análisis forense • Clasificación de información • Gestión de vulnerabilidades y amenazas

Tomado y traducido de: Corporate Executive Board Chief Information Office Leadership Council, Common Archetypes of Security Functions: Implementation Tool, *www.irec.executiveboard.com*

Figura 2.1: Arquetipos de la función de seguridad de la información

2.3.3 Seguridad de aplicaciones

SEGURIDAD DE BASE DE DATOS

El IESS Hospital de Ancón hace uso del Sistema Medico MIS-AS400 para la atención médica a la población afiliada, el servidor con la base de datos que utiliza el sistema reposa en el área de Tecnologías del Hospital Carlos Andrade Marín en la ciudad de Quito.

En aplicaciones tales como Sistema Contable Zebra, Sistema de Control y Ejecución Presupuestario, Sistema Evolution, Sistema de Control de Asistencia, Sistema Winsing, el nivel de acceso se lo realiza a través del propio aplicativo, en los módulos de

administración, donde se registran y se dan los accesos respectivos a cada uno de los usuarios de los sistemas.

El Sistema Nacional de Pagos a través de Red Pública (Sector Público y Cooperativas) se lo realiza a través de la página del Banco Central del Ecuador, cuyos usuarios de acceso los asignan en el BCE.

La única persona que puede tener acceso a los archivos de la base de datos de los aplicativos son los administradores de los sistemas.

2.3.4 Seguridad física

CONTROL DE ACCESO FÍSICO AL CUARTO DE TELECOMUNICACIONES

En el año 2006 se implementó la infraestructura de red, no se efectuó un análisis de costo-beneficio para determinar que controles de acceso físico sería necesario implementar.

El área donde se encuentra ubicado los equipos de redes forman parte del área de Calificación de Derechos. La sala no dispone de un sistema de detección y extinción de incendios.

El IESS Hospital de Ancón cuenta con los servicios de un prestador externo para poseer la asistencia de guardias de seguridad; en horarios laborales se ubican en el exterior e interior de la misma las 24 horas al día.

En horas de oficina hay un control de entrada que identifica a los empleados y registra su hora de entrada, almuerzo y de salida a través del Biométrico cuyo administrador es el área de Recursos Humanos. Los controles de acceso son propios de la unidad. Los guardias también llevan un registro manual de las personas que ingresan y salen del hospital.

El hospital no cuenta con cámaras de seguridad.

CAPÍTULO 3

3. DISEÑO DE UN PLAN DE CONTINGENCIA PARA LA INTRANET DEL IESS HOSPITAL DE ANCÓN BASADO EN LA METODOLOGÍA ITIL

3.1 Metodología ITIL

Al realizar un plan de contingencia para la intranet del IESS Hospital de Ancón basado en la metodología ITIL se desea acercar una visión de los procesos ITIL que han surgido a raíz de la gran expansión de servicios que se ha producido durante los últimos años.

Se pretende poner en conocimiento las “mejores prácticas” para mejorar el uso de los recursos con que se dispone actualmente. La implantación de procesos ITIL, debe permitir alcanzar los objetivos del hospital, eliminando los puntos débiles de la red y conseguir de este modo que el hospital sea

considerado como una entidad de alta calidad en cuanto a rendimiento de sus redes y en cuanto a los servicios ofertados.

La implementación de esta metodología para los procesos a través de ITIL, debe considerar las funciones y áreas comunes dentro del hospital, permitiendo una aceptación estructurada; para ello es necesario comenzar agrupando los procesos ITIL de una forma en la cual se facilite aparte de la implementación en sí, la aceptación y pronto alcance de sus beneficios.

Bajo este enfoque el hospital podrá seleccionar a la gente con alguna área de responsabilidad común para realizar la transición hacia este nuevo modelo de operación.

La implementación de estas mejores prácticas es dirigida y optimizada por soluciones tecnológicas diseñadas para tal fin, por lo tanto su uso está encaminado a la integración y automatización de los procesos de ITIL. Las soluciones tecnológicas deberán ser fáciles de adaptarse a las necesidades únicas del hospital.

3.2 Identificación y análisis de riesgos

El análisis de riesgos es el proceso cuantitativo o cualitativo que permite evaluar los riesgos, el cual comprende la estimación de las pérdidas que implicaría la interrupción parcial o total de las operaciones. En esta etapa se

desarrolla la posibilidad de ocurrencia, posibles mitigaciones, el Impacto y probabilidades de los riesgos, las alternativas de corrección de los mismos.

3.2.1 Identificación de servicios y equipos de tecnología de información y comunicación

Identificación de equipos de redes LAN de la infraestructura tecnológica del hospital

En la Figura 3.1 se muestra la forma como está distribuida la red LAN del IESS Hospital de Ancón.

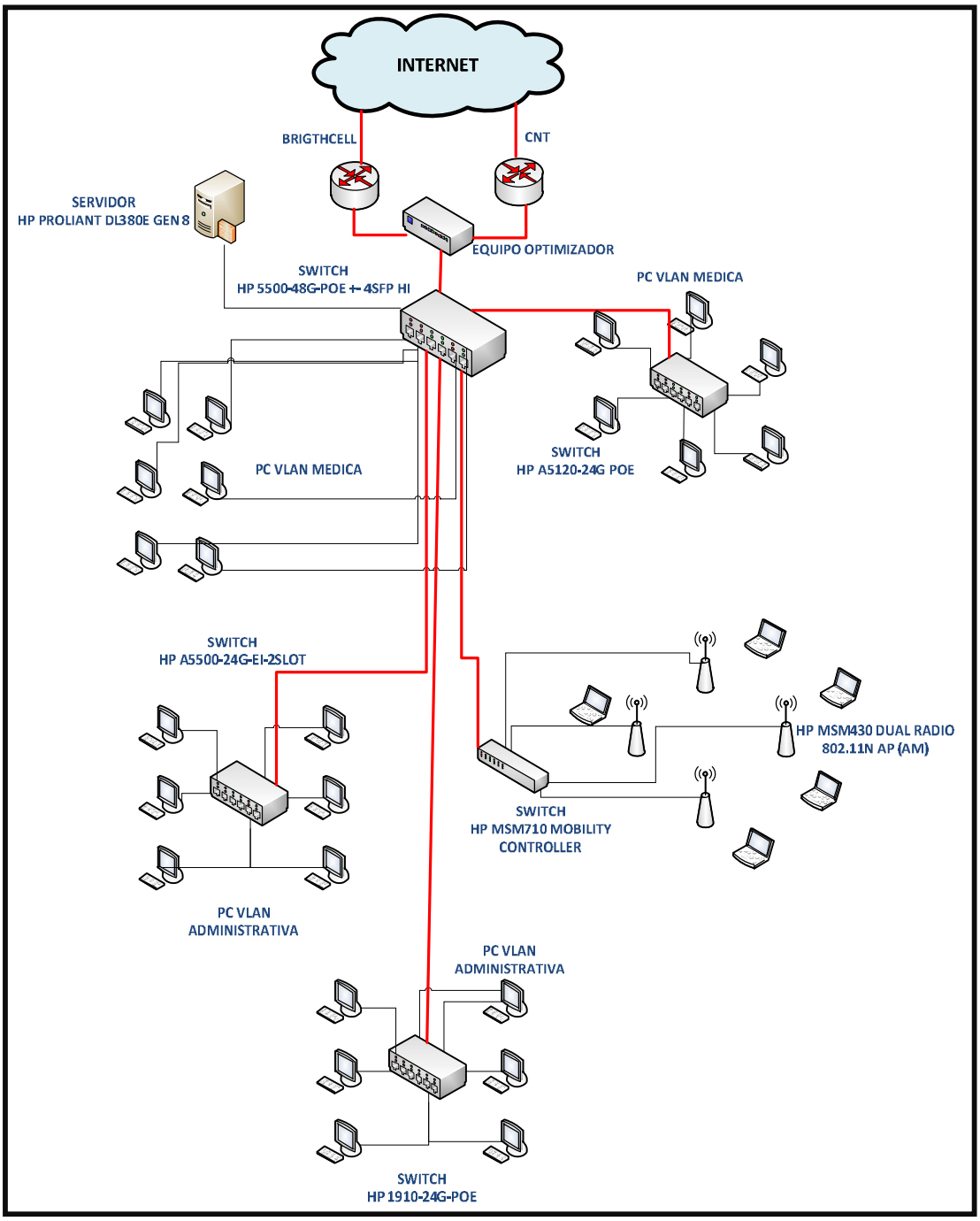

Figura 3.1: Equipos de redes LAN

Identificación de enlaces WAN de la infraestructura tecnológica del hospital

En la Figura 3.2 se muestra la forma como está distribuida la red WAN del IESS Hospital de Ancón.

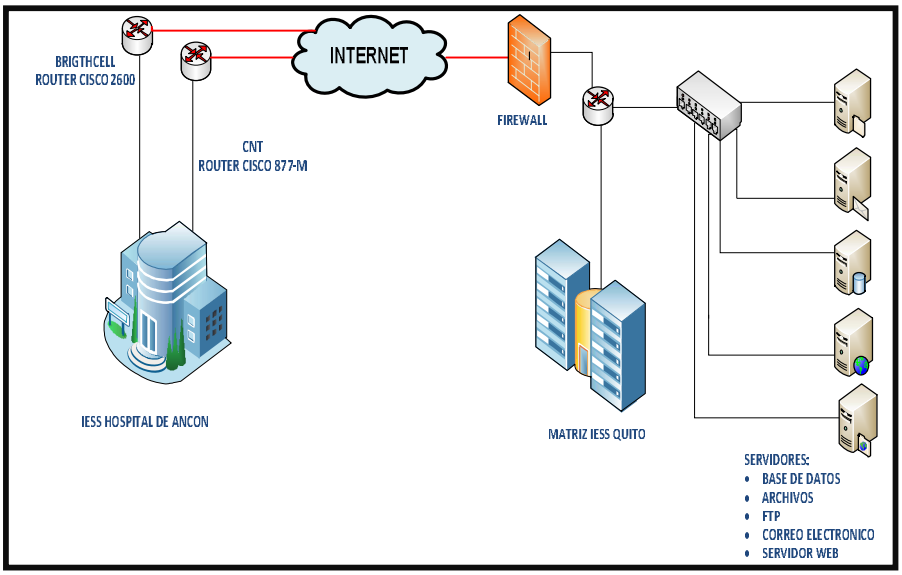

Figura 3.2: Enlaces WAN

Identificación de activos (resumen de equipos de cómputo del hospital)

Tabla 7. Equipos del Área Administrativa

DEPENDENCIA	DISPOSITIVO	MARCA	MODELO	SERIE
SECRETARIA	CPU/MONITOR	HP	ELITE ONE 800 G1	MXL4521F1D
	TECLADO	HP		BDMHE0C5Y7K49S
	MOUSE	HP		FCMHH0AHD7E3WN
BODEGA	CPU	HP	COMPAQ 6000 PRO	MXJ9480328
	MONITOR	FLATRON	W19435S	007TPQ1Y348
	TECLADO	GENIUS	K639	WE1291003660
	MOUSE	GENIUS	GM050009P	139051801892
SECRETARIA DE QUIROFANO	CPU	HP	COMPAQ 8100 ELITE	MXL10821XC
	MONITOR	HP	S1933	CNC103RYGQ
	TECLADO	HP	KB0316	BAUDOKVB2QAXA

	MOUSE	HP	SBF96	417441002
SERVICIOS GENERALES	CPU/MONITOR	HP	ELITE ONE 800 G1	MXL4521F1G
	TECLADO	HP		BDMHE0C5Y7K49D
	MOUSE	HP		FCMHH0AHD7E3W3
	CPU	HP	DC 5100	MXJ5500ADL
	MONITOR	LG	F W1742S	007TPPB1X696
	TECLADO	HP	SK2880	B93CB0ACPSABZA
	MOUSE	GENIUS	NET SCROLL 12	X71629907828
SERVICIO AL ASEGURADO - CALIFICACION DE DERECHO	CPU/MONITOR	HP	ELITE ONE 800 G1	MXL4521F18
	TECLADO	HP		BDMHE0CCP7LAED
	MOUSE	HP		FCMHH0AHD7E3WX
	CPU/MONITOR	HP	ELITE ONE 800 G1	MXL4521F19
	TECLADO	HP		BDMHE0CHH7L31M
	MOUSE	HP		FCMHH0AHD7E3XJ
	CPU	HP	COMPAQ PRO 6300	MXL2501XVB
	MONITOR	HP	LV2011	CNC224PF6T
	TECLADO	HP	KB0316	BDAEV0QVB3KBBH
	MOUSE	HP	MOFXKO	FCGLH0DHD3HFII
	CPU	HP	DC5100	MXJ55004GH
	MONITOR	HP	L1710	CNC932Q655
	TECLADO	GENIUS	K639	WE1291003304
	MOUSE	HP	M-SBF96	FATSQ0CN3Y4AEF
ESTADISTICA	CPU	HP	COMPAQ PRO 6300	MXL2501XV2
	MONITOR	LG	W1742S	007PSL1Y518
	TECLADO	GENIUS	K339	ZM8802048017
	MOUSE	HP	M-SBF96	FB7330AN3X01384
TESORERIA	CPU	HP	COMPAQ DC5100	MXJ55004F6
	MONITOR	LG	F W1742S	007TPHG1X697
	TECLADO	GENIUS	K639	ZM8802048016
	MOUSE	HP	417441-002	X72144900549
FINANCIERO	CPU	HP	COMPAQ 8100 ELITE	MXL1091SM
	MONITOR	HP	51933	CNC103RZ1T
	TECLADO	HP	KB0316	BAUDU0JVBZ75RS
	MOUSE	HP	SBF96	FATSQ0CFZZSPU8
	CPU	HP	COMPAQ 8100 ELITE	MXL1090C60
	MONITOR	HP	S1933	CNC103RYHS
	TECLADO	HP	KB0316	BAVDUOKVB2X10A
	MOUSE	HP	417441002	FATSQ0C8KZXU46
	CPU	HP	ELITE ONE 800 G1	MXL4521F1B
	TECLADO	HP		BDMHE0C5Y7K49Q
	MOUSE	HP		FCMHH0AHD7E3X5

DIRECCION MEDICA	CPU	HP	COMPAQ 6000 PRO	MXJ9490534
	MONITOR	HP	L1710	CNC92Q6Q1
	TECLADO	HP	KB0316	BAUDU0HGAXY0P1
	MOUSE	HP	SFB96	FATSQ0CN3Y4AED
RESPONSABILIDAD PATRONAL	CPU	HP	COMPAQ 6000 PRO	MXL0390H7V
	MONITOR	HP	L1710	CNC932Q6QM
	TECLADO	HP	KB0316	BAUDUOHBY4BH6
	MOUSE	HP	SBF96	FATSQ0CN3Y4ADS
	CPU	HP	COMPAQ 6000 PRO	MXJ9490538
	MONITOR	HP	L1710	CNC912RL03
	TECLADO	HP	SK2880	B93CBOACPSAA6F
	MOUSE	HP	SBF96	FB7330ASBXT0LI9L
	CPU	HP	COMPAQ 6000 PRO	MXJ949052D
	MONITOR	HP	L1710	CNC821Q3KH
	TECLADO	HP	KB0316	BAUDUOHVBY4BHA
	MOUSE	HP	SBF96	FATSQ0CN3Y4AE4
RECURSOS HUMANOS	CPU	HP	COMPAQ 6000 PRO	MXL0390H7X
	MONITOR	HP	S1933	CNC104SXSB
	TECLADO	HP	KB0316	BAUDU0JVBZ1MJG
	MOUSE	HP	MOAFKOA	FATSQ0B9WZVPVT
	CPU	HP	COMPAQ PRO 6300	MXL2501XW2
	MONITOR	HP	LV2011	CNC224PF6R
	TECLADO	HP	KB0316	BDAEV0QVB3KBPC
	MOUSE	HP	S0005-O	FCGLH0DHD3HFIA
TIC	CPU	TERRAX		MXJ55004H5
	MONITOR	HP	L 1710	3CQ8444MZS
	TECLADO	HP	KB 0316	BC3370GVBWYF8V
	MOUSE	HP	MOAFKOA	537748001
	CPU/MONITOR	HP	ELITE ONE 800 G1	MXL4521F16
	TECLADO			BDMHE0C5Y7K49X
	MOUSE			FCMHH0AHD7E3WJ
COMPRAS PUBLICAS	CPU/MONITOR	HP	ELITE ONE 800 G1	MXL4521F15
	TECLADO	HP		BDMHE0C5Y7K49K
	MOUSE	HP		FCMHH0AHD7E3Y8

Tabla 8. Equipos del Área Medica

DEPENDENCIA	DISPOSITIVO	MARCA	MODELO	SERIE
MEDICINA GENERAL	CPU	HP	COMPAQ 8100 ELITE	MXL1091SIT
	MONITOR	HP	S1933	CNC103RYGW
	TECLADO	HP	KB-0316	BC3370GVBWU5RH
	MOUSE	HP	CP15K	FATSQ0B9WZUMNF
MEDICINA INTERNA	CPU	HP	COMPAQ 8100 ELITE	MXL1091S1X

	MONITOR	HP	S1933	CNC103RY3J
	TECLADO	HP	KB-0316	BAUDU0KVBZQAXA
	MOUSE	HP	MOAFKOA	FAT5Q0B9WZUMNX
UROLOGIA	CPU	HP	COMPAQ PRO 6300 MT	MXL3411M47
	MONITOR	HP	LV2011	CNC313NTVQ
	TECLADO	HP	KB-0316	BDAEV0Q5Y5F0RN
	MOUSE	HP	S0005-O	FCGLH0DCW4Y5CU
PEDIATRIA	CPU	HP	COMPAQ PRO 6300	MXL2501XTJ
	MONITOR	HP	LV2011	CNC224PF6D
	TECLADO	HP	KB0316	BDAEV0QVB3KBNR
	MOUSE	HP	MOFXKO	FCGLH0DHD3HFI7
ODONTOLOGIA	CPU	HP	COMPAQ 8100 ELITE	MXL1091S27
	MONITOR	LG	W1943SS	103TPBF28845
	TECLADO	XTRATECH		C2275LK1400
	MOUSE	HP	SBF96	FB7330AN3W11K6F
MEDICINA INTERNA	CPU/MONITOR	HP	ELITE ONE 800 G1	MXL4521F1H
	TECLADO	HP		BDMHE0C5Y7K49I
	MOUSE	HP		FCMHH0AHD7EX8
CARDIOLOGIA	CPU	HP	COMPAQ 8100 ELITE	MXL1091S1T
	MONITOR	LG	E2240S	002TPCA28019
	TECLADO	HP	KB-0316	BAUDU0KVBZS00S
	MOUSE	GENIUS		
OBSTETRICIA	CPU	HP	COMPAQ PRO 6300 MT	MXL3411M4K
	MONITOR	HP	LV2011	CNC313NVMR
	TECLADO	HP	KB-0316	BAUDU0KVBZS09T
	MOUSE	HP	S0005-O	FCGLH0DCW4Y4TE
GINECOLOGIA	CPU	HP	COMPAQ PRO 6300	MXL2501XTM
	MONITOR	HP	LV2011	CNC224PF6R
	TECLADO	HP	SK2880	B93CB0ACPSABV9
	MOUSE	HP	600553-002	FCGLH0DHD3HFIA
	CPU	HP	COMPAQ 8100 ELITE	MXL1091S1D
	MONITOR	HP	S1933	CNC103RY27
	TECLADO	GENIUS		WE1B92012015
	MOUSE	HP	M-SBF96	FATSQ0CFZZ5PS1
MEDICINA GENERAL	CPU	HP	COMPAQ 8100 ELITE	MXL1091S1Z
	TECLADO	HP		BDAEV0Q5Y5F0RZ
	MOUSE	HP		FATSQOCN3Y4AEN
MEDICINA PREVENTIVA	CPU	HP	COMPAQ 6000 PRO	MXJ948033R
	MONITOR	HP	S1933	CNC103RY4K
	TECLADO	GENIUS		WE1291002185
	MOUSE	GENIUS		X72144900577
CURACIONES E	CPU/MONITOR	HP	ELITE ONE	MXL4521F16

INYECCIONES			800 G1	
	TECLADO	HP		BDMHE0C5Y7K49E
	MOUSE	HP		FCMHH0AHD7ETK
RAYOS X	CPU	HP	COMPAQ 8100 ELITE	MXL109151L
	MONITOR	HP	7540	CNC5411FDD
	TECLADO	HP	SK2880	B93CB0ACPSABS3
	MOUSE	HP	SBF96	FATSQ0CFZZ5PUA
FARMACIA	CPU	HP	COMPAQ PRO 6300	MXL2501XV6
	MONITOR	HP	LV2011	CNC224PFQ4
	TECLADO	HP		40401903
	MOUSE	HP	M-S0005-0	FCGLH0DN33B8XE
	CPU	HP	DC5800	MXJ91108T0
	MONITOR	LG	W1943SS-PF	102UXYG0N658
	TECLADO	HP	KB-0316	BC3370GVBWYCFC
	MOUSE		SPM001	50300821
	CPU	HP	COMPAQ PRO 6300	MXL2501XTL
	MONITOR	HP	LV2011	CNC224PFPZ
	TECLADO	HP	KB0-316	BDAEV0QVB3KBP8
	MOUSE	HP	M-S0005-O	FCGLH0DN33B8X7
	CPU	HP	COMPAQ PRO 6300	MXL2501XW9
	MONITOR	HP	LV2011	CNC224PF6P
	TECLADO	HP	KB0316	BDAEV0QVB3KBNT
	MOUSE	HP	S00056	FCGLH0DN33BBBV
IMAGENOLOGIA	CPU/MONITOR	HP	ELITE ONE 800 G1	MXL4521F18
	TECLADO	HP		BDMHE0C5Y7K49I
	MOUSE	HP		FCMHH0AHD7ETL
EMERGENCIA	CPU	HP	ELITE ONE 800 G1	MXL4521F17
	TECLADO	HP		BDMHE0C5Y7K49J
	MOUSE	HP		FCMHH0AHD7E3WA
	CPU	HP	COMPAQ DX2400	MXL8280YX0
	MONITOR	HP	L1710	CNC821QLGL
	TECLADO	HP	KB0316	BC3370FVBW15U4
	MOUSE	HP	MOAFKOA	FB7330A9WW3M255
	CPU	HP	COMPAQ 6000 PRO	MXJ949052V
	MONITOR	FLATRON	W1742S	007TPDT1X706
	TECLADO	HP	KB0316	BAUDU0KVBZS3B0
	MOUSE	GENIUS	NETSCROLL 120	X72144900569
	CPU/MONITOR	HP	ELITE ONE 800 G1	MXL4521F1K
	TECLADO	HP		BDMHE0C5Y7K49F
	MOUSE	HP		FCMHH0AHD7E3W7
	CPU	CASE S/N		
	MONITOR	HP	L1710	CNC821QLJG

	TECLADO	HP		BDAEV0QVB3KBR9
	MOUSE	GENIUS		X72144900553
	CPU	HP	COMPAQ 6300	MXL3411M4Q
	MONITOR	HP	LV2011	CNC313NTP0
	TECLADO	HP		BDAEV005Y5F0RU
	MOUSE			
	CPU	HP	COMPAQ PRO 6300	MXL2501XV4
TRAUMATOLOGIA	MONITOR	HP	LV2011	CNC224PFQD
	TECLADO	HP	SK2880	B913BOACPSABWX
	MOUSE	HP		FCGLH0DN33B8XJ
	CPU/MONITOR	HP	ELITE ONE 800 G1	MXL4521F1F
CIRUGIA GENERAL	TECLADO	HP		BDMHE0C5Y7K49L
	MOUSE	HP		FCMHH0AHD7E3XS
	CPU	HP	COMPAQ DC5100 MT	MXJ55004CV
	MONITOR	HP	LV2011	CNC224PFPQ
	TECLADO	HP	KB0316	BDAEV0QVB3KBNV
	MOUSE	HP		FCGLH0DN33B8XK
	CPU	HP	COMPAQ DX2400	MXL8280YSH
	MONITOR	HP	LV2011	CNC224PFQX
	TECLADO	HP	KB0316	BDAEV0QVB3KBVF
	MOUSE	HP	GENIUS	X72144900578
	CPU	HP	COMPAQ DC5100 MT	MXJ55004CQ
	MONITOR	HP	LV2011	CNC821Q3KM
	TECLADO	HP		BDAEV0QVB3KBQS
	MOUSE	HP		FCGLHODN33BBB4
	CPU	HP	ELITE ONE 800 G1	MXL4521F1L
	TECLADO	HP		BDMHE0C5Y7K499
	MOUSE	HP		FCMHH0AHD7E3UO
	CPU	HP	COMPAQ 6000 PRO	MXL0390H8M
QUIROFANO	MONITOR	HP	HPLE1711	CNL030N228B
	TECLADO	HP	KB0316	BAUDUOJVBZ75RQ
	MOUSE	HP	CP15K	F6AB70AUSRS8LW
	CPU	XTRATECH	INC100140	LC1309
OFTALMOLOGIA	MONITOR	AOC	9315WL	716A3BA004284
	TECLADO	HP		BAUDU0KVBZS0KG
	MOUSE	XTRATECH	LM8835	LM1309
	CPU	HP	COMPAQ 6300	MXL3411M4D
DERMATOLOGIA	MONITOR	FLATON	W1943SS	102UXYG0N682
	TECLADO	GENIUS		WE1291003301
	MOUSE	GENIUS	X71629907822	6110150
	CPU	HP	COMPAQ 6300	MXL2501XTR
FISIATRIA	MONITOR	HP	51933	CNC104SXSS

	TECLADO	HP	SK2880	B93CB0ACPS80J1
	MOUSE	GENIUS		X72144900562
REHABILITACION	CPU	HP	COMPAQ DC 5100 MT	MXJ55004GK
	MONITOR	LG	W1943SS	103TPLC28472
	TECLADO	GENIUS	KL0210	7CE7A0901251
	MOUSE	HP	UAE96	F93A90A5BTJ1A95
NUTRICION	CPU	HP	COMPAQ DC 5100 MT	MXJ55004FL
	MONITOR	SAMSUNG	7X0NW	MA17H9NQ827442H
	TECLADO	HP	SK2880	BC3370ADPU456L
	MOUSE	HP	IBF26	417441001
	CPU	HP	COMPAQ 6300	MXL3412DMG
	MONITOR	HP	LV2011	CNC313NTNX
	TECLADO	HP	SK2880	BDAEV0Q5Y5A5P2
	MOUSE	HP	IBF26	FCGLH0D5D4YRFH
PSICOLOGIA	CPU	HP	COMPAQ PRO 6300 MT	MXL34129RC
	MONITOR	HP	LV2011	CNC313NT5D
	TECLADO	HP	KB-0316	BDAEV0Q5Y5A30P
	MOUSE	HP	600553-002	FCGLH0D5D5C54A
MEDICINA GENERAL	CPU	HP	COMPAQ PRO 6300 MT	MXL3411M4N
	MONITOR	HP	LV2011	CNC313NT3
	TECLADO	HP	KYBD WIN8	BDAEV0Q5Y5F0RO
	MOUSE	HP	S0005-O	FCGLH0D5D4YREQ
LABORATORIO	CPU	HP	COMPAQ 8100	MXL1091S1S
	MONITOR	HP	S1933	CNC104SXXT
	TECLADO	HP	KB-0316	BAUDU0KVBZS0A2
	MOUSE	HP	UAE96	F93A90A5BTK2H40
	CPU	HP	COMPAQ 8100 ELITE	MXL1091S22
	MONITOR	HP	SI933	CNC103RYHD
	TECLADO	HP	BK0316	BAUDU0KVBZS1IP
	MOUSE	HP	MOAFKOA	FATSQ0B9WZUQN8
	CPU	HP	COMPAQ DX2400	MXL8280YPL
	MONITOR	LG	FLATRON W1742S	007TPTM1Y401
	TECLADO	HP	KB-0316	BC3370FVBW3DCH
	MOUSE	HP	SBF96	FATSQ0CN3Y4ADZ
	CPU	HP	COMPAQ PRO 6300	MXL2501XT7
	MONITOR	HP	LV2011	CNC224PFQL
	TECLADO	HP	KB0316	BDAEV0QVB3KBV5
	MOUSE	HP	MOFXKO	FCGLH0DHD3HFJ5
	CPU	HP	COMPAQ 6000 PRO	MXJ949052R
	MONITOR	FLATRON	W1943SS	103TPNY28863
	TECLADO	HP	KB0316	BAUDU0HVBY0JPQ
	MOUSE	HP	CP15K	F6AB70AUSRS8LH

	CPU	HP	ELITE ONE 800 G1	MXL4521F1J
	TECLADO	HP		BDMHE0C5Y7K49N
	MOUSE	HP		FCMHH0AHD7E3WD
	CPU	HP	COMPAQ DC 5800	MXJ91108VR

Tabla 9. Portátiles del Área Administrativa y Medica

DEPENDENCIA	DISPOSITIVO	MARCA	MODELO	SERIE
DIRECCION	LAPTOP	HP	PROBOOK 4540S	2CE24020QW
SERVICIOS GENERALES	LAPTOP	HP	PROBOOK 4540S	2CE2450PPX
FINANCIERO	LAPTOP	HP	PROBOOK 4540S	2CE24020QY
FINANCIERO	LAPTOP	HP	PROBOOK 450 G2	CND447G3ZV
QUIROFANO	LAPTOP	HP	PROBOOK 4540S	2CE24020VD
QUIROFANO	LAPTOP	HP	PROBOOK 4540S	2CE24020TW
QUIROFANO	LAPTOP	HP	PROBOOK 4540S	2CE2450PP2
FINANCIERO	LAPTOP	HP	PROBOOK 4540S	2CE24020SN
GINECOLOGIA	LAPTOP	HP	PROBOOK 4420s	CNF1031X08
DIRECCION MEDICA	LAPTOP	HP	PROBOOK 4420s	CNF1031X0F
SISTEMAS	LAPTOP	HP	Pavilon G6-1D73CA	196216480887
HOSPITALIZACION	LAPTOP	HP	PROBOOK 4420s	CNF1031WV8
HOSPITALIZACION	LAPTOP	HP	PROBOOK 4420s	CFN1031WZ2
ODONTOLOGIA	LAPTOP	HP	NX6120	CNU5480XB0
MEDICINA GENERAL	LAPTOP	HP	PAVILION DV4	CND9091B7W

Tabla 10. Equipos de Comunicaciones

TIPO	EQUIPOS DE COMUNICACIÓN	EQUIVALENTE	SERIE
SWITCH	HP A5500-24G-EI-2SLOT	HP 5500-24G-EI	CN1AB9V0FK
	HP 5500-48G-POE +- 4SFP HI	HP 5500-48G-POE	
	HP MSM710 MOBILITY CONTROLLER	HP-PROCURVE MSM710	TW206LBTL
	HP 1910-24G-POE	HP V1910-24G	CN16BX30M1
	HP A5120-24G POE	H3C-5510-24P	CN11BYWOGD
ACCESS POINT	HP MSM430 DUAL RADIO 802.11N AP (AM)	HP MSM430	CN29DWY1ZK
	HP MSM430 DUAL RADIO 802.11N AP (AM)	HP MSM430	CN23DWY1D2
	HP MSM430 DUAL RADIO 802.11N AP (AM)	HP MSM430	CN23DWY1DN
	HP MSM430 DUAL RADIO 802.11N AP (AM)	HP MSM430	CN29DWY1ZQ
	HP MSM430 DUAL RADIO 802.11N AP (AM)	HP MSM430	CN23DWY14M
	HP MSM430 DUAL RADIO 802.11N AP (AM)	HP MSM430	CN23DWY168
SERVIDOR	HP PROLIANT DL380E GEN 8	HP PROLIANT DL380E	MXQ229088R

3.2.2 Descripción de análisis de riesgos

Los riesgos viables que pueden afectar la continuidad y operatividad normal de los sistemas de información con que cuenta el hospital, son los riesgos con incidencia externa e interna.

RIESGOS CON INCIDENCIA EXTERNA

Gubernamentales

Modificaciones a la constitución política ya sea por asamblea nacional, referendo, consulta popular, o mediante leyes orgánicas, reestructuración o supresión de entidades.

RIESGOS CON INCIDENCIA INTERNA

Incumplimiento de los contratistas

Este riesgo puede ocurrir a causa del posible atraso en la ejecución o infracción del contratista, en la actualización, modificación, mantenimiento de los contratos.

Retrasos en Procesos Administrativos

La ejecución de los procesos tecnológicos relacionados con la realización de los contratos, implica el desarrollo de diligencias administrativos los cuales deben cumplir los requisitos, extendiendo el tiempo de cumplimiento de las actividades.

Pérdida de información

Es un riesgo con posibilidades de que ocurra ya que el plan de contingencias posee un proceso de respaldo.

Falla de hardware fuera de inventario

Este riesgo se presenta por la falta de prevención, con la no inclusión de soluciones al quitar equipos de los inventarios, por desconocimiento o por no haber sido reportados a tiempo al área de TIC.

3.2.3 Identificación de amenazas

Se ha determinado que existen amenazas que podrían afectar la operación normal del IESS Hospital de Ancón causando serios problemas. Se han definido como posibles amenazas las siguientes:

Acceso no autorizado

El control de acceso es un término genérico que se utiliza para designar el proceso por el que un sistema controla la interacción entre los usuarios y los recursos del sistema, de tal forma que los primeros accedan a los recursos deseados. [5]

- Vulneración de sistemas de seguridad instalados.
- Manipulación de claves de acceso, tanto del servidor como de los sistemas, correo electrónico, equipos de cómputo, equipos de telecomunicaciones, etc.
- Instalación e infección de virus en la red, ya sea por medios externos mediante e-mail con archivos infectados o por dispositivos extraíbles.
- Sabotaje.
- Robo.
- Espionaje.

Desastres naturales

Accidente físico de origen natural: riada, fenómeno sísmico o volcánico, meteoro, rayo, corrimiento de tierras, avalancha, derrumbe [4].

Se indica el derrumbamiento como una amenaza ya que el territorio donde está ubicado el hospital es de arcilla expansiva, al revisar las

instalaciones se encontraran con áreas donde las paredes están cuarteadas, pisos hundidos, todo esto por la calidad del suelo.

Proximidad de peligros

Se estima como peligro la zona donde está ubicado el hospital con riesgo medio propenso a ataques de delincuentes.

Fallas en equipos de soporte

Problemas de energía eléctrica, existe el peligro latente de perder el suministro público ya sea por carencia en la zona o por sistemas eléctricos muy antiguos (instalaciones y dispositivos eléctricos).

- Equipos de aires acondicionados.
- Telecomunicaciones, podrían presentarse problemas en cualquiera de los siguientes medios de comunicación.
- Red interna de comunicación por cableado estructurado (fibra óptica y/o cable UTP, sistemas inalámbricos), que interconectan a 85 PCs de usuarios del hospital.
- Fallas en los equipos que forman parte la red interna de comunicación (switch, routers, etc).

Indisponibilidad de personal

Se han considerado claves en la operación normal de los sistemas:

- Médicos
- Responsable de Presupuesto
- Responsable de Facturación
- Contador
- Personal de Talento Humano
- Responsable de TIC

Sobre el personal indicado existen las siguientes amenazas:

- Enfermedad
- Accidentes
- Renuncia
- Abandono de puesto de trabajo
- En menor grado rapto o prisión

Fallas de hardware

Los equipos están sujetos como cualquier otro a fallas de hardware, aun cuando siempre se han seguido recomendaciones y escogiendo los mejores equipos y proveedores del medio, entre las amenazas tenemos:

- Fallas de disco duro y otros componentes del servidor HP PROLIANT DL380E GEN 8

- Fallas de componentes en Switch core HP 5500-48G-POE +-4SFP HI
- Fallas de componentes en Switch HP A5500-24G-EI-2SLOT
- Fallas de componentes en Switch HP MSM710 MOBILITY CONTROLLER
- Fallas de componentes en Switch HP 1910-24G-POE
- Fallas de componentes en Switch HP A5120-24G POE
- Fallas de componentes en access point HP MSM430 DUAL RADIO 802.11N AP (AM)
- Fallas en router de proveedor de enlace de datos.

Perspectiva anual de daños

Combinando la estimación de daños potenciales y el análisis de amenazas se ha producido una base para estimar lo que costaría en reposición de bienes perdidos y en las medidas de seguridad para cada uno de ellos, se ha multiplicado el daño potencial por la frecuencia de ocurrencia para obtener una estimación anual de los daños.

Tabla 11. Estimación anual de daños

AMENAZA	ACTIVO AFECTADO	FRECUENCIA	IMPACTO	COSTO MENSUAL	COSTO REPOSICION ANUAL	PERDIDA
INGRESO NO AUTORIZADO	Hardware Software Información	2	1	$2.800	$33.600	$67.200
INDISPONIBILIDAD DEL PERSONAL DE TIC	Información	1	1	$1.400	$16.800	$16.800
SABOTAJE	Hardware Software Información	1	3	$2.800	$33.600	$33.600
ROBO	Hardware Información	1	2	$2.800	$33.600	$33.600
FALLA DE SISTEMA ELECTRICO	Hardware Información	2	1	$182.000	$2´184.000	$4´368.000
FALLA DE ENLACE DE DATOS	Hardware Información	2	1	$600	$7.200	$14.400
FALLA EN SERVIDOR	Hardware Software Información LAN	2	1	$4.000	$48.000	$52.000
FALLA EN SWITCH	Hardware LAN	1	1	$11.000	$132.000	$132.000
FALLA EN EL SISTEMA MIS-AS400	Información	1	1	$450.000	$5´400.000	$5´400.000
FALLA EN HW	Hardware	2	1	$61.053	$732.636	$1´465.272

Escala de Frecuencia

1 Improbable
2 Ocasional
3 Frecuente

Impacto

1 Alto
2 Medio
3 Bajo

Problemas de conectividad de red

Este tipo de problemas puede darse porque las tarjetas de red de cada una de los computadores de la Institución no funcionan correctamente, ya que el dispositivo no está correctamente instalado físicamente o el driver o controlador del dispositivo no está correctamente instalado.

Si un computador no se conecta correctamente a la red, se puede deber a lo siguiente:

- El conector RJ-45 no está correctamente conectado a la tarjeta de red.
- El patch cord tiene defectos, puede estar deteriorado.
- El patch cord debe estar bien conectado tanto en el punto de red, como en la tarjeta de red del computador.
- El cable de red debe tener conexión desde el punto de red hasta donde se encuentra el switch.
- El funcionamiento de los switch deben ser los correctos.

Inestabilidad de energía

El fluido eléctrico es de gran importancia para el funcionamiento del hospital, puesto que los dispositivos en los que se trabaja dependen de la corriente eléctrica para su desempeño.

El equipo de aire acondicionado y ambiente adecuado en el Área de Rack, favorece su correcto funcionamiento.

Para que las computadoras de escritorio funcionen adecuadamente, necesitan de una fuente de alimentación eléctrica fiable, si se interrumpe inesperadamente la alimentación eléctrica o varia en forma, las consecuencias pueden ser muy serias, podrían provocar daños en el hardware y la información podría perderse.

Por lo expuesto anteriormente se debe tener en cuenta lo siguiente:

Tomas a Tierra

La toma a tierra permite la protección a las personas de los aparatos conectados a la corriente eléctrica, esta lleva a tierra derivaciones indebidas de la corriente eléctrica a los dispositivos que puedan estar en contacto con los usuarios, evitando así el paso de corriente.

Estas conexiones se las realizan por medio de placas, varillas o tubos de cobre enterrados a profundidad en tierra, según especificaciones técnicas indicadas para las instalaciones eléctricas.

Extensiones eléctricas

Pocas oficinas y consultorios no poseen suficientes placas de pared para conexiones eléctricas por lo que muchas veces es necesario conectar más equipos siendo necesarias las extensiones eléctricas. Se debe tomar precauciones en su uso para evitar daños físicos al momento de poder tropezarse con las mismas logrando ocasionar apagado de equipos.

3.2.4 Evaluación de vulnerabilidades

Las vulnerabilidades son debilidades que pueden ser utilizadas para convertir una amenaza en un riesgo real que puede causar daños graves en el hospital. Por cada amenaza se detallan los posibles escenarios a presentarse y el nivel de protección de los mismos; a continuación se detallan las siguientes vulnerabilidades:

Tabla 12. Exposición de Vulnerabilidades

AMENAZA	CAUSA CONTROLABLE	PROBABILIDAD DE OCURRENCIA	INTENSIDAD DEL DAÑO (1-10)
DESASTRES NATURALES			
Incendios	Si	Baja	10
Inundaciones	Si	Baja	10
Deslizamientos	No	Baja	10
Terremotos	No	Baja	10
CASOS FORTUITOS			
Fallas en suministro eléctrico	No	Media	10

Fallas de UPS	No	Media	8
Fallas de Hardware	No	Media	10
Fallas de Enlace	No	Media	10
Fallas de equipos de redes	No	Media	10
Fallas de Sistemas	No	Media	10
ROBOS			
Fraude	Si	Media	5
Robo de equipos	Si	Media	5
Robo de información	Si	Alta	5
ACCESO NO AUTORIZADO			
Acceso físico no autorizado	Si	Alta	5
Acceso lógico no autorizado	Si	Alta	5
VANDALISMO INFORMATICO			
Borrado de Información	Si	Alta	8
ERRORES HUMANOS			
Perdida de claves de acceso	Si	Media	5

3.2.5 Evaluación de impacto

Por cada incidente que ocurra en la infraestructura tecnológica del IESS Hospital de Ancón se produce un impacto; a continuación se detallan los principales impactos:

Tabla 13. Procesos

DESCRIPCION	SUBPROCESO	FRECUENCIA	RESPONSABLE
PROCESO 1: INGRESAR HISTORIAS CLINICAS			
Realizar la creación de historias clínicas para poder acceder a la atención médica, mediante verificación si posee o no derecho de atención de acuerdo al número de aportaciones.	Registrar datos personales del afiliado	Diariamente	Personal de Calificación de Derechos
PROCESO 2: VERIFICACION DE APORTACIONES			
Verificar aportaciones, para acceder a la atención necesita 3 aportaciones consecutivas.	Verificación de Información en Página del IESS	Diariamente	Personal de Calificación de Derechos
PROCESO 3: INGRESO DE CITAS MEDICAS			

Ingreso de citas médicas por apertura o disponibilidad de agendas.	Verificación de información en Sistema MIS AS/400	Diariamente	Personal de Calificación de Derechos
PROCESO 4: ATENCIONES MEDICAS			
Ingreso de registro médico, exámenes, procedimientos, medicamentos, etc.	Registrar datos en sistema MIS AS/400	Diariamente	Médicos
PROCESO 5: INTERNACIONES MEDICAS			
Ingreso de pacientes de Consulta Externa o Emergencia a Hospitalización	Registrar datos en sistema MIS AS/400	Diariamente	Médicos
PROCESO 6: CIRUGIAS PROGRAMADAS/DE EMERGENCIA/AMBULATORIAS			
Transferencia de pacientes de Consulta Externa, Emergencia u Hospitalización a Quirófano por Cirugías Programadas, de Emergencia o Ambulatorias	Registrar datos en sistema MIS AS/400	Diariamente	Médicos Cirujanos/Médicos Internistas/Médicos Residentes/Médicos de Hospitalización
PROCESO 7: REGISTRO DE MEDICAMENTOS			
Registro de medicamentos, stock, lotes, etc.	Registrar datos en sistema MIS AS/400	Diariamente	Responsable de Bodega de Fármacos
PROCESO 8: REGISTRO DE INSUMOS			
Registro de insumos médicos stock, lotes, etc.	Registrar datos en sistema MIS AS/400	Diariamente	Responsable de Bodega de Insumos
PROCESO 9: REGISTRO DE EXAMENES			
Registro de resultados de exámenes	Registrar datos en sistema MIS AS/400	Diariamente	Licenciadas de Laboratorio
PROCESO 10: REGISTROS DE EMERGENCIA			
Registros médicos para pacientes de emergencia	Registrar datos en sistema MIS AS/400	Diariamente	Médicos Residentes

Tabla 14. Sistema que soporta cada proceso

SUBPROCESO	NOMBRE DEL SISTEMA/MODULO	CRITIC.	TIPO DE SISTEMA (PC/SERVIDOR)	Nº DE EQUIPOS CON LA APLICAC.	RESPONSABLE
PROCESO 1: INGRESAR HISTORIAS CLINICAS					
Registrar datos personales del afiliado	MIS AS/400-MODULO DE ADMISION	1	PC/SERVIDOR	3	CINDY CHONILLO-ROSY ORTIZ-GLENNYS SUAREZ-VIVIANA GONZALEZ-STEFANNY VASQUEZ
PROCESO 2: VERIFICACION DE APORTACIONES					

Verificación de Información en Página del IESS	PAGINA DEL IESS	1	PC/SERVIDOR	3	CINDY CHONILLO-ROSY ORTIZ-GLENNYS SUAREZ-VIVIANA GONZALEZ-STEFANNY VASQUEZ
PROCESO 3: INGRESO DE CITAS MEDICAS					
Verificación de información en Sistema MIS AS/400	MIS AS/400-MODULO DE ADMISION	1	PC/SERVIDOR	3	CINDY CHONILLO-ROSY ORTIZ-GLENNYS SUAREZ-VIVIANA GONZALEZ-STEFANNY VASQUEZ
PROCESO 4: ATENCIONES MEDICAS					
Registrar datos en sistema MIS AS/400	MIS AS/400-MODULO DE CONSULTA EXTERNA	1	PC	19	TODOS LOS 25 MEDICOS DE CONSULTA EXTERNA
PROCESO 5: INTERNACIONES MEDICAS					
Registrar datos en sistema MIS AS/400	MIS AS/400-MODULO DE CONSULTA EXTERNA-MODULO DE EMERGENCIA-MODULO DE HOSPITALIZACION-MODULO DE ADMISION HOSPITALARIA	1	PC/SERVIDOR	25	25 MEDICOS DE CONSULTA EXTERNA-16 MEDICOS RESIDENTES
PROCESO 6: CIRUGIAS PROGRAMADAS/DE EMERGENCIA/AMBULATORIAS					
Registrar datos en sistema MIS AS/400	MIS AS/400-MODULO DE CONSULTA EXTERNA-MODULO DE EMERGENCIA-MODULO DE HOSPITALIZACION-MODULO DE QUIROFANO	1	PC	15	10 MEDICOS CIRUJANOS-16 MEDICOS RESIDENTES
PROCESO 7: REGISTRO DE MEDICAMENTOS					
Registrar datos en sistema MIS AS/400	MIS AS/400-MODULO DE BODEGA DE FARMACOS	1	PC	2	FRANCISCO AVELINO-ALEXANDRA HUERTA
PROCESO 8: REGISTRO DE INSUMOS					
Registrar datos en sistema MIS AS/400	MIS AS/400-MODULO DE BODEGA DE INSUMOS	1	PC	1	REYNALDO MITE
PROCESO 9: REGISTRO DE EXAMENES					

Registrar datos en sistema MIS AS/400	MIS AS/400-MODULO DE SERVICIO DE LABORATORIO	1	PC	5	LCDAS DE LABORATORIO
PROCESO 10: REGISTROS DE EMERGENCIA					
Registrar datos en sistema MIS AS/400	MIS AS/400-MODULO DE EMERGENCIA-MODULO DE ADMISION HOSPITALARIA	1	PC	4	16 MEDICOS RESIDENTES

Rangos de Criticidad:

1 Proceso no puede ejecutarse sin el sistema

2 Proceso puede ejecutarse parcialmente sin el sistema

3 Proceso puede ejecutarse sin el sistema

Tabla 15. Tiempo de interrupción de cada proceso

PROCESO	SUBPROCESO	NECESIDADES DE RECUPERACION	CRITICIDAD
INGRESAR HISTORIAS CLINICAS	Registrar datos personales del afiliado	A	1
VERIFICACION DE APORTACIONES	Verificación de Información en Página del Iess	A	1
INGRESO DE CITAS MEDICAS	Verificación de información en Sistema MIS AS/400	A	1
ATENCIONES MEDICAS	Registrar datos en sistema MIS AS/400	A	1
INTERNACIONES MEDICAS	Registrar datos en sistema MIS AS/400	A	1
CIRUGIAS PROGRAMADAS/DE EMERGENCIA/AMBULATORIAS	Registrar datos en sistema MIS AS/400	A	1
REGISTRO DE MEDICAMENTOS	Registrar datos en sistema MIS AS/400	A	1
REGISTRO DE INSUMOS	Registrar datos en sistema MIS AS/400	A	1

REGISTRO DE EXAMENES	Registrar datos en sistema MIS AS/400	A	1
REGISTROS DE EMERGENCIA	Registrar datos en sistema MIS AS/400	A	1

3.2.6 Evaluación de riesgo

Se va a determinar la evaluación de riesgos de acuerdo a la matriz de probabilidad/impacto.

		IMPACTO		
		Bajo	Medio	Alto
PROBABILIDAD	Baja	Muy bajo	Bajo	Medio
	Media	Bajo	Medio	Alto
	Alta	Medio	Alto	Muy alto

Figura 3.3: Matriz de probabilidad/impacto

A continuación se detallan los posibles riesgos que se pueden presentar en el IESS Hospital de Ancón.

Tabla 16. Evaluación de Riesgos

DESCRIPCION	PROBABILIDAD	IMPACTO	RIESGO
Incendios	B	A	RM
Inundaciones	B	A	RM
Deslizamientos	B	A	RM
Terremotos	B	A	RM
Fallas en suministro eléctrico	M	A	RA
Fallas de UPS	M	A	RA
Fallas de Hardware	M	A	RA

Fallas de Enlace	M	A	RA
Fallas de equipos de redes	M	A	RA
Fallas de Sistemas	M	A	RA
Fraude	M	M	RM
Robo de equipos	M	M	RM
Robo de información	A	A	RMA
Acceso físico no autorizado	A	A	RMA
Acceso lógico no autorizado	A	A	RMA
Borrado de Información	A	A	RMA
Perdida de claves de acceso	M	M	RM

3.2.7 Evaluación de contramedidas

En base a la matriz de riesgos se realiza la evaluación de contramedidas a los respectivos riesgos.

Tabla 17. Evaluación de Contramedidas

DESCRIPCION	RIESGO	CONTROLES PREVENTIVOS	CONTROLES DETECTIVOS	ACCIONES A TOMAR
Incendios	RM	Instalar un sistema de detección de incendios	Sensor de humo	Recuperación de información perdida
		Establecer normas de seguridad contra incendios		
Inundaciones	RM	Establecer un plan de acción contra inundaciones	Monitorear eventos	Recuperación de información perdida
Deslizamientos	RM	Establecer un plan de acción contra derrumbes o deslizamientos	Monitorear eventos	Recuperación de información perdida
Terremotos	RM	Disponer de un área alterna	Monitorear eventos	Habilitar el área alterna

Fallas en suministro eléctrico	RA	Mantenimiento al sistema eléctrico de manera eventual	Monitorear eventos	Reemplazar conexiones eléctricas averiadas
		Establecer un plan de acción de suministro eléctrico		
Fallas de UPS	RA	Dar mantenimiento eventuales al UPS		Puesta en marcha de equipos
		Documentación del UPS		
Fallas de Hardware	RA	Mantenimiento preventivos de los equipos	Monitorear eventos	Recuperación de datos
		Establecer procedimientos de manejo de HW		
Fallas de Enlace	RA	Definir ancho de banda	Monitorear eventos	Recuperación de datos
		Mantener activo el enlace de backup		
Fallas de equipos de redes	RA	Mantenimiento preventivos de los equipos de red	Monitorear eventos	Levantamiento de enlace
		Monitorear equipos de red		
Fallas de Sistemas	RA	Establecer políticas de seguridad	Monitorear procesos	Recuperación de datos
Robo de equipos	RM	Supervisión de inventario de red	Monitorear procesos	Recuperación de datos
		Establecer políticas de seguridad		
Robo de información	RMA	Establecer políticas de seguridad de	Monitorear procesos	Recuperación de datos

		información		
Acceso físico no autorizado	RMA	Establecer procedimientos de seguridad	Monitorear procesos	Recuperación de datos
Acceso lógico no autorizado	RMA	Establecer métodos de autenticación	Monitorear procesos	Recuperación de datos
Borrado de Información	RMA	Establecer procesos de respaldo de información	Monitorear procesos	Recuperación de datos
Perdida de claves de acceso	RM	Establecer procesos de control	Monitorear procesos	Recuperación de datos

3.2.8 Enfoque de riesgos para identificar actividades, compromisos y preferencias en la administración de los riesgos de la seguridad de la intranet.

Las responsabilidades de los funcionarios implicados en la seguridad de la información para la gestión de los riesgos de acuerdo a la estructuración con que cuenta actualmente el hospital se describen a continuación:

Director

La Dirección, es responsable de la calidad y eficiencia de las acciones de prevención, curación y rehabilitación que se realizan en el Hospital.

Las responsabilidades a desempeñar se muestran a continuación:

1. Planea, organiza, dirige, controla y evalúa los procesos y productos de la prestación médica en régimen ambulatorio o de hospitalización.
2. Supervisa y evalúa la ejecución de los programas de atención ambulatoria y hospitalización.
3. Difunde y supervisa la aplicación de las guías de práctica clínica elaboradas por la aseguradora.
4. Consolida, revisa y avala los requerimientos de insumos, materiales, fármacos y equipos de las áreas a su cargo, previo a su traslado a la Dirección.
5. Aplica, coordina y evalúa el sistema de referencia y contra-referencia de pacientes, de acuerdo con el nivel de complejidad de las demás unidades médicas.
6. Supervisa, evalúa y aprueba observa el correcto registro de la información estadística y contable de las áreas a su cargo para evitar inconsistencia.
7. Evalúa el desempeño del personal a su cargo y establece necesidades educativas.
8. Cumple y Supervisa la aplicación de las normas de seguridad y salud en el trabajo en el ámbito de su gestión.
9. Asesora y recomienda a la Dirección acciones para mejorar la calidad y eficiencia de las prestaciones médicas e incrementar la satisfacción de los usuarios.

10. Cuida y promueve el buen uso y mantenimiento de las instalaciones, equipos y materiales en el ámbito de su gestión.
11. Prepara los pliegos y especificaciones técnicas de los bienes o servicios requeridos para el debido funcionamiento de su área de gestión, y los traslada al ordenador de gasto para su aprobación.
12. Elaborar informe de gestión mensual/POA.
13. Demás que le asigne su jefe inmediato.

Responsable de Recursos Humanos

Responsable del óptimo aprovechamiento y el continuo mejoramiento de las competencias y talentos de los servidores del Hospital, así como del cumplimiento oportuno y a satisfacción de las obligaciones institucionales hacia su personal.

Las responsabilidades a desempeñar se muestran a continuación:

1. Atender y resolver necesidades del área de usuarios internos y externos
2. Planear, organizar y ejecutar actividades relacionadas con la administración del personal.

3. Revisar la documentación de los aspirantes a un puesto por contrato y verificar su conformidad con la normativa vigente.
4. Elaborar documentos contractuales para revisión del Director de la Unidad, su envío a la Dirección del Seguro de Salud Individual y Familiar para su análisis y trámite ante la Dirección General del IESS.
5. Coordinar con los responsables de áreas para consolidar la información relativa a las necesidades educativas de los servidores de la Unidad.
6. Coordinar con responsables de áreas, la información de funciones y perfil de cada uno de los puestos existentes en la Unidad para elaborar y actualizar el Manual de Funciones con sus respectivos Perfiles de Puestos en cada una de las áreas de gestión.
7. Elaborar y mantener actualizada una base de datos con información completa de los servidores de la Unidad.
8. Preparar informes sobre aspectos técnicos, económicos y legales relativos a la contratación de personal y al óptimo aprovechamiento de los recursos de planta del Hospital.
9. Tramitar y registrar la aplicación de incentivos o acciones disciplinarias determinadas por el Jefe Inmediato superior previo confirmación del caso y Visto Bueno de la Dirección del Hospital verificando el cumplimiento del debido proceso.

10. Organizar y controlar los sistemas de registro de identidad, asistencia, vacaciones, permisos, licencias y demás acciones de personal.
11. Coordinar, registrar e informar sobre la aplicación de los procesos de evaluación del desempeño al personal de la Unidad.
12. Facilitar la entrega oportuna a cada servidor el desglose de la remuneración mensual recibida (rol de pagos).
13. Elaborar los informes de liquidación de haberes a los servidores que terminan su relación laboral con la institución.
14. Cumplir con normas de seguridad y salud en el trabajo, en el ámbito de su gestión.
15. Asesorar y recomendar a la Dirección acciones para mantener un clima laboral favorable al óptimo desempeño de todos los servidores.
16. Cuidar y promover el cuidado, buen uso y mantenimiento de las instalaciones, equipos y materiales en el ámbito de su gestión.
17. Preparar los pliegos y especificaciones técnicas de los bienes o servicios requeridos para el debido funcionamiento de su área de gestión, y los traslados al ordenador de gasto para su aprobación.
18. Presentar informes de gestión a la Dirección.

Responsable de TIC

Implementar y administrar la plataforma tecnológica informática, hardware, software, sistemas, bases de datos, servicios, redes, comunicaciones para optimizar los procesos y generar información confiable y oportuna

Las responsabilidades a desempeñar se muestran a continuación:

1. Implementar sistemas, soluciones y servicios informáticos
2. Sacar respaldo de información del usuario de cada equipo en caso de requerir reparación.
3. Administrar y garantizar la productividad de la plataforma tecnológica informática: hardware, software, sistemas, bases de datos, servicios, redes, comunicaciones.
4. Gestionar y garantizar la integridad y seguridad de los sistemas y bases de datos de la Unidad.
5. Aplicar políticas y normas, estándares y procedimientos tecnológicos.
6. Aplicar el Plan de Contingencias y Recuperación de la plataforma tecnológica.
7. Desarrollar aplicativos como respuestas a particularidades
8. Capacitar y brindar soporte a usuarios de los otros procesos Institucionales.
9. Configurar equipos, redes e instalar software.

10. Participar en la planificación del proceso
11. Realizar Plan y mantenimiento de los equipos de la Unidad de manera semestral.
12. Presentar informes de gestión mensual al Administrador
13. Demás actividades que le fueren encomendadas por su Jefe Inmediato.

Responsable de Servicios Generales

La Unidad de Servicios Generales tiene por naturaleza la planificación, control y logística de los servicios de apoyo que el Hospital requiere, brindando una atención ágil y oportuna a las diferentes áreas solicitantes, priorizando urgencias para que la atención sea continua y funcional. Garantiza además el confort del usuario durante su permanencia.

Las responsabilidades a desempeñar se muestran a continuación:

1. Atender requerimientos de usuarios internos de la Unidad.
2. Supervisar, evaluar y gestionar el mejoramiento de la calidad del Servicio de Alimentación.
3. Supervisar, evaluar y gestionar el mejoramiento de la calidad del servicio de guardianía.
4. Supervisar, evaluar y gestionar el mejoramiento de la calidad del servicio de limpieza y mantenimiento de áreas verdes.

5. Supervisar, evaluar y gestionar el mejoramiento de la calidad del servicio de transporte de pacientes.
6. Supervisar, evaluar y gestionar el mejoramiento de la calidad del servicio de lavandería
7. Gestionar la adquisición oportuna de insumos para la prestación de servicios de apoyo en la Unidad.
8. Gestionar el mantenimiento preventivo y correctivo de equipos relacionados con la prestación de servicios generales.
9. Entregar oportunamente la información contable sobre las actividades producidas, a la subgerencia financiera de la Unidad.
10. Evaluar el desempeño del personal a su cargo y establece necesidades educativas.
11. Cumplir y supervisar el cumplimiento de normas de salud y seguridad en el trabajo, en el ámbito de su gestión.
12. Cumplir y supervisar el cuidado, buen uso y funcionamiento de las instalaciones, equipos y materiales a su cargo.
13. Procesar requerimientos de compras por áreas en el Sistema PORTAL o directamente.
14. Presentar informes de gestión mensual a la Dirección General y Técnica.
15. Revisar, aprobar u observar los informes elaborados por el personal subordinado.

16. Demás funciones que le asigne su jefe inmediato.

3.3 Plan de Respaldo

3.3.1 Respaldo de datos valiosos

Identificar las áreas para realizar respaldos de:

- Sistemas en Red.
- Sistemas no conectados a Red.
- Correos electrónicos institucionales.
- Información de Pcs

3.3.2 Análisis de criticidad

Este tipo de análisis debe ser realizado periódicamente, con el objetivo de revisar la criticidad, cada vez que se agregue un servicio a la infraestructura de red o se implemente un sistema nuevo estos deben ser incluidos en el plan de respaldos.

Este análisis deberá estar enmarcado en los siguientes niveles de criticidad:

Alta: cuando la información es altamente crítica.

Media: cuando la información es medianamente crítica.

Baja: cuando la información no es crítica.

3.3.3 Designación de responsables

3.3.3.1 Comité Directivo

Se designara a funcionarios de nivel directivo:

- Director Administrativo
- Director Medico
- Jefatura Financiera
- Responsable de Servicios Generales

Los funcionarios deberán llevar los lineamientos para el control del plan de contingencia, evaluar la implementación del plan.

3.3.3.2 Coordinador del plan de contingencia

Es el intermediario entre el comité directivo y quienes desarrollan el plan, se encargara de asegurar que el plan se cumpla a cabalidad.

En el hospital el Coordinador del plan es la Responsable de TIC.

3.3.3.3 Grupo de desarrollo del plan

Este grupo lo conformaran personas de las áreas involucradas dentro del plan, estará conformado por personal de la área administrativa y médica.

Funciones

- Ejecutar, en tiempo y forma, todas las actividades planeadas.
- Documentar de manera correcta el plan de contingencias.
- Diseñar planes de entrenamiento para el personal del hospital, involucrándose así en las tareas del plan.
- Diseñar cronogramas.
- Mantener debidamente actualizado el plan de contingencias.

3.3.4 Estudio de impacto a los procesos

El objetivo principal del estudio del Impacto a los procesos, es determinar cuan critica pueden llegar a ser los procesos e infraestructura de soporte para la contingencia operativa del hospital.

Para efectuar un análisis se debe tomar en cuenta lo siguiente:

- Proveer estrategias para la contingencia operativa en caso de un desastre.
- Identificar cuanto tiempo se tomara en restablecer los procesos críticos del hospital de manera normal.

- La Dirección decidirá qué tema es prioritario en el caso de que exista inconvenientes en el funcionamiento de los sistemas producidas por alguna contingencia.

3.3.5 Sistemas de Información del Hospital

En el IESS Hospital de Ancón se utilizan los siguientes sistemas informáticos:

- Sistema Medico MIS AS-400
- Sistema Contable Zebra
- Sistema de Control y Ejecución Presupuestario
- Sistema Nacional de Pagos a través de Red Pública (Sector Público y Cooperativas)
- Sistema Winsing
- Sistema Evolution
- Sistema de Control de Asistencia

Sistema Medico MIS AS-400

Los módulos del sistema utilizados tanto por el área administrativa como medica se detallan a continuación:

- Administración
- Bodegas (Fármacos e insumos)
- Admisión Consulta Externa
- Admisión Hospitalización
- Calificación de Derechos
- Facturación

- Servicios:
  - Laboratorio
  - Enfermería CE
  - Enfermería EM
  - Rayos X
  - Ecografías
  - Electrocardiogramas
  - Colposcopias
- Farmacia
- Emergencia
- Hospitalización
- Módulo de Enfermería
- Modulo Medico
- Consulta Externa
  - Medicina General
  - Cardiología
  - Dermatología
  - Pediatría
  - Cirugía General
  - Cirugía Pediátrica
  - Nutrición y Dietética
  - Medicina Interna
  - Urología
  - Oftalmología

  - Medicina Preventiva
  - Odontología
  - Medicina Domiciliaria
  - Medicina Familiar
  - Ginecología
  - Obstetricia
- Quirófano
- Cirugías del Día
- Cirugías programadas
- Modulo Enfermería de Quirófano
- Modulo Enfermería de Recuperación

Modulo Admisión

Registro y seguimiento de las citas médicas y laboratorios en la consulta externa, desde la solicitud de la atención médica hasta la entrega de las recetas producto de la prescripción médica. Incluye exámenes de laboratorio, registro del historial clínico de los afiliados, así como los controles necesarios durante el desarrollo de este proceso.

El registro de las citas puede realizarse, según el perfil de usuario, únicamente a los pacientes que concurren al dispensario o a cualquier dispensario cuando la cita se lo realiza telefónicamente o un médico concede una cita subsiguiente o una interconsulta.

Calificación de Derechos

Verificar automáticamente la condición de aportes de los afiliados previos a la consulta médica.

Modulo Bodegas

Registro y seguimiento de los movimientos relacionados con el control y administración de los productos existentes en las bodegas. Incluye ingresos, egresos y ajustes, así como los controles necesarios durante el desarrollo de este proceso.

Modulo Administración

Administrar, parametrizar, registro y control de los diferentes módulos que componen el sistema médico del Instituto Ecuatoriano de Seguridad Social.

Modulo Servicios

Registro y seguimiento de los laboratorios y demás servicios médicos de la consulta externa, desde la solicitud en la atención médica hasta la entrega de los resultados correspondientes. Incluye exámenes de laboratorio, así como los controles necesarios durante el desarrollo de este proceso.

Como servicio médico se define a los exámenes y demás ayudas para el diagnóstico y tratamiento de enfermedades, tales como:

- Laboratorios Clínicos
- Rayos X general (Imagen Directa)
- Electrocardiogramas
- Rehabilitaciones
- Curaciones
- Servicios de ultrasonido
- Entre otros.

Consulta Externa

Registro médico de la atención a pacientes en la consulta externa. Una vez que el paciente fue registrado en el sistema y asignado una cita para la atención médica, el médico referido podrá visualizar, en su agenda, los pacientes a los que debe atender.

El módulo permite visualizar todo el historial clínico del paciente, registrar los síntomas, exámenes, revisiones, diagnósticos presuntivos y definitivos, así como también las recomendaciones exámenes, recetas, órdenes de laboratorio y demás elementos necesarios en las consultas médicas.

Farmacia

Registro y seguimiento de los despachos para dispensarios anexos y subrogados de la consulta externa, desde la solicitud en la atención médica hasta la entrega de los resultados correspondientes.

Facturación

El módulo FT (AS400) permite visualizar las atenciones con cédula (es decir por afiliado) con sus respectivos valores, los reportes para su impresión son generados de forma global dentro de ciertos parámetros como son tipo de afiliado, dependencia, fecha, etc.

Sistema Contable Zebra

Sistema contable diseñado con tecnología de orientación de objetos para ambientes cliente/servidor. La flexibilidad de sus opciones permite segregar funciones de control sobre el manejo presupuestario, financiero y contable de la Unidad.

Tiene como propósito principal agilitar el proceso financiero y administrativo, eliminando los trámites innecesarios y facilitando mecanismos modernos de comunicación interdepartamental.

Sistema de Control y Ejecución Presupuestario

Sistema que facilita la consolidación de información concerniente a la elaboración de requisitos de cada área y la elaboración de la pro forma presupuestaria de la Unidad Médica.

Sistema Nacional de Pagos a través de Red Pública (Sector Público y Cooperativas)

Programa que permite generar a las Instituciones del Sector Público el archivo que contiene la información con el detalle de las órdenes de pago, que por concepto de pago de obligaciones sobre base devengada, deben realizar las Instituciones Públicas.

Sistema Winsing

WinSIG es una herramienta analítica para la toma de decisiones, enmarcada en los procesos de gerencia productiva de los sistemas de salud.

Su principal aporte consiste no en generar nueva información, sino en relacionar selectivamente la información existente.

Las funciones principales del WinSIG son:

- Evaluar globalmente el desempeño de instituciones, programas y redes de servicios de salud.

- Identificar los factores o problemas más relevantes del perfil de productividad institucional correspondiente.
- Facilitar el análisis de dichos factores o problemas a fin de determinar opciones de cambio, en el marco de los procesos de reforma sectorial y modernización de la gestión sanitaria.
- Monitorear los procesos de cambio y la evaluación del impacto de las medidas de ajuste institucional adoptadas para abordar la problemática que el propio WinSIG permite identificar.
- Establecer los costos de los servicios como resultantes de la eficiencia en las funciones de producción.

Jefes de áreas informan datos de producción e insumos utilizados en forma mensual, datos que se ingresan al sistema.

Sistema Evolution

Es una herramienta de Recursos Humanos y Nomina que simplifica y automatiza procesos y actividades de administración de personal. Permite además la mejora de los servicios a los colaboradores y la adopción a tecnologías de forma amigable e intuitiva con los modelos de autoservicio.

Administración de Personal, permite mantener de forma organizada la información relacionada con las personas vinculadas a la Unidad,

donde se detalla el curriculum, vacaciones y demás datos relevantes del mismo.

Administración Del Tiempo

Cálculo de horas laboradas, sobre tiempo y ausentismo.

- Recolección de datos
- Generación y transferencia de datos a la nómina
- Manejo de hojas de tiempo
- Planificación y control de horarios, turnos o planes de rotación
- Manejo de Excepciones
- Supervisión y aprobación de las horas
- Reportes que le permitirán administrar de mejor manera a los empleados.

Liquidación De Personal

Permite ejecutar las liquidaciones, cuando un colaborador sale de la Unidad, por cualquier motivo, calculando los rubros de ley, generando las actas de finiquito de manera automática.

Sistema de Control de Asistencia

Sistema que permite llevar el control de asistencia del personal que labora en la Unidad así como sus horas trabajadas, permisos, control y administración de marcaciones.

Sistema de Gestión Documental Quipux

Servicio web que la Subsecretaría de Tecnologías de Información de la Secretaría Nacional de la Administración Pública, pone a disposición de entidades o instituciones públicas, la misma que permite el registro, control, circulación y organización de los documentos digitales y/o físicos que se envían y reciben en la Unidad.

Disponibilidad de Camas MSP

Herramienta que permite el registro y movimiento de pacientes en los hospitales con el fin de generar un reporte de disponibilidad de camas en todo el país evitando el peregrinaje de los pacientes en busca de hospitales con disponibilidad de camas.

3.3.6 Principales servicios que deberán ser restablecidos y/o recuperados

- Enlaces de datos
- Sistema MIS AS-400
- Sistemas Operativos de las PCs

- Correo Electrónico
- Internet
- Antivirus
- Paquetes de programas informáticos
- Respaldos de Información
- Respaldos de los sistemas

3.4 Plan de Recuperación

3.4.1 Objetivos del plan de recuperación

- Luego de haber ocurrido un desastre se deberá planificar la restauración de todos los servicios dentro de las 5 horas como máximo, principalmente equipos de red y accesos a los sistemas.
- Mantenimiento y supervisión de las aplicaciones de manera permanente.

3.4.2 Lista de verificación para un plan de recuperación de desastres

Cuando mencionamos la gestión de la continuidad del negocio hablamos de disminuir la posibilidad de ocurrencia de incidentes disruptivos y, en caso de realizarse, el hospital está preparado para responder en forma adecuada y oportuna, de esa manera se reduce de manera significativa un daño potencial que pueda ser ocasionado por ese incidente.

A continuación se muestran las actividades que deben realizarse cuando se requiere establecer una recuperación de desastres:

- Detectar las fallas y desastres.
- Conocer los motivos que generan daños producido por la contingencia.
- Analizar el tiempo de riesgo y el impacto en el IESS Hospital de Ancón,
- Notificar a los responsables que deben tomar las acciones correspondientes.
- Definir la funcionalidad mínima que requiere el negocio en caso de contingencia.
- Establecer los períodos mínimos de recuperación requeridos en los que no se vea afectado el hospital.
- Identificar las aplicaciones consideradas críticas para las operaciones del hospital.

3.4.3 Alcance del plan de recuperación

En el plan se considera al área de TIC como el proveedor del servicio de procesamiento de datos quien tiene como principal función la recuperación del servicio en el menor tiempo posible.

El plan durara de acuerdo a las necesidades que se presenten y la capacidad de los equipos de trabajo para procesar la reconstrucción y recuperación de los sistemas.

3.4.4 Activación del Plan

La decisión es tomada por la Dirección Administrativa, determinando la activación del Plan de Desastres, y además indicar el lugar alterno de ejecución del respaldo, basándose en las recomendaciones indicadas por éste.

3.4.5 Duración estimada

Los responsables de cada área determinarán el tiempo que se tomara estar fuera de los servicios de acuerdo a cada grado de responsabilidad.

3.4.6 Responsabilidades

Tabla 18. Responsabilidades

DESCRIPCION	RESPONSABLES
Orden de Ejecución del Plan	Dirección Administrativa
Supervisión General de Plan	Propia y/o empresa en convenio para Recuperación
Supervisión del Plan de Recuperación	Responsables de Área(s)
Abastecimiento (HW, SW)	Personal de TIC
Tareas de Recuperación	Personal de tareas afines

3.4.7 Aplicación del plan

El plan de contingencia se lo aplicara siempre que ocurra una pérdida de servicio por un período mayor de 24 horas, cuando sea fin de mes, se lo aplicara en un período mayor a 12 horas. En áreas críticas se lo aplicara en un periodo menor a 4 horas.

3.4.8 Priorizar la recuperación de recursos

A continuación se detalla el tipo de prioridad que se asocia a la recuperación de recursos:

Tabla 19. Priorizar la recuperación de recursos

RECURSOS	NIVEL DE PRIORIDAD
Pc	Alto
Laptop	Medio
Sistema Medico MIS AS-400	Alto
Sistema Contable Zebra	Alto
Sistema de Control y Ejecución Presupuestario	Alto
Sistema Winsing	Alto
Sistema Evolution	Alto
Sistema de Control de Asistencia	Alto
Servidor de Dominio	Alto
Enlace de Datos	Alto
Internet	Alto
Intranet del IESS	Alto
Herramientas de Office	Medio

Debido a que las unidades médicas del IESS están regidas al PAC se debe incluir presupuesto para los gastos en el planeamiento de contingencias referente a:

- Hardware.
- Transporte.
- Pruebas.

- Entrenamiento.
- Materiales.
- Tiempo a incurrir.
- Servicios, etc.

3.4.9 Detalle de posibles causas de la falla del servidor

Entre las posibles causas para que falle un servidor pueden ser:

- Error físico de disco duro
- Error de memoria RAM
- Error lógico de datos
- Fallas de alimentación eléctrica
- Por climatización
- Daños de fábrica
- Falta de mantenimiento

3.4.10 Consecuencias de la interrupción del fluido eléctrico

A continuación se presentan consecuencias de interrupción de fluido eléctrico:

Tabla 20. Interrupción de Fluido Eléctrico

CONSECUENCIA/IMPACTO	ÁREAS AFECTADAS
Cierre Inapropiado de las aplicaciones	Todas
Falla de un componente de equipo Servidor	Todas
Pérdida total o parcial de la operatividad de los sistemas	Todas

3.4.11 Contingencia para el suministro de energía eléctrica

Inicialmente el Hospital ha contado con un UPS Modelo TLS MST MS de 30KV 24 KW el cual abastece a los equipos de computación y a ciertos equipos médicos de la Unidad.

Debido a acontecimientos suscitados anteriormente en el hospital se pone en marcha un UPS Central para las áreas críticas del hospital.

El sistema de UPS posee las siguientes características:

- Dos módulos de transformación para entrada y salida.
- Un UPS marca TLE modelo TLE Series S1 de 160 KVA.
- Un banco de baterías de 40 baterías.
- Un sistema de bypass de 1000 amperios.
- Un TVSS de protección.
- Cableado eléctrico.

La alimentación del sistema de bypass fue tomada directo al tablero de transferencia, para tomar toda la potencia disponible del generador y del transformador principal, propiedad del hospital; este sistema de bypass alimenta a los transformadores de entrada y salida.

Los transformadores adecuan el voltaje de entrada hacia el UPS y toman el voltaje regulado de este último, para proveer de aislamiento

galvánico a la carga (equipos conectados). Las baterías van conectadas al UPS y son las que van a proporcionar de Respaldo a los equipos durante cortes de energía.

Los trabajos eléctricos para la interconexión de estos sistemas fueron los siguientes:

- Instalación de electro-canales tipo escalera, desde tablero de transferencia hasta el tablero de bypass.
- Instalación de electro-canales, desde tablero de bypass hasta módulos de transformadores y sistema de entrada-salida de UPS.
- Tendido de acometida eléctrica tablero de transferencia hasta tablero de bypass.
- Tendido eléctrico desde bypass hasta transformadores y a UPS.
- Conexión de TVSS conectado al sistema de bypass.

Una vez listas las instalaciones se comprueban los parámetros eléctricos entre ellos:

- Voltaje de alimentación
- Consumo de carga (equipos), que va ir conectada en UPS.
- Verificación del sistema de tierra.
- Verificación de conexiones ambientales

- Verificación física

Se energiza el nuevo sistema comprobando los siguientes parámetros:

- Voltaje y frecuencia en tablero de bypass
- Secuencia de fases en la alimentación
- Voltaje e el primario y secundario de los transformadores
- Voltaje y frecuencia de alimentación al UPS
- Temperatura de trabajo en el cuarto de UPS

Pruebas de UPS

Una vez verificado que los parámetros se encuentran en el rango normal se procede a realizar la calibración y pruebas en el UPS. Se comprueba:

- Sincronización entre UPS y alimentación de entrada
- Calibración de rangos de voltaje y de frecuencia
- Calibración de niveles máximos y mínimos
- Pruebas por etapas, entrada, rectificador, bypass electrónico, inversor
- Pruebas de funcionamiento entre etapas
- Pruebas de funcionamiento con baterías.
- Sincronización con generador
- Recarga de baterías

Siendo las pruebas satisfactorias se procede a energizar al tablero de carga que contiene a los Quirófanos, área de TIC, Farmacia. El UPS queda online y funcionando correctamente.

3.4.12 Recursos de contingencias generales

Entre los recursos de contingencia se debe tomar en cuenta lo siguiente:

- Router (Prevenido por el proveedor de Internet y WAN).
- Componentes de red (tarjetas, conectores, etc)
- Servidor y Equipos de Comunicación (Switchs, Fibra, etc.).
- Rack.
- UPS de rack.
- Respaldo diario de la información de los Sistemas.
- Instaladores de Sistema MIS AS-400, Sistema Operativo, etc.
- Componente de Remplazo (Memoria, Disco Duro, UPS, etc.).

3.4.13 Impacto de la caída y tiempos aceptables de caída

A continuación se muestra el detalle de los tiempos aceptables que se pueden determinar para solventar una contingencia.

Tabla 21. Impacto de la caída y tiempos aceptables de caída

RECURSO	IMPACTO	TIEMPO ACEPTABLE DE CAÍDA (HORAS)
Pc	Alto	1
Laptop	Medio	1
Sistema Medico MIS AS-400	Alto	0.30
Sistema Contable Zebra	Alto	0.30
Sistema de Control y Ejecución Presupuestario	Alto	0.30
Sistema Winsing	Alto	0.30
Sistema Evolution	Alto	0.30
Sistema de Control de Asistencia	Alto	0.30
Servidor de Dominio	Alto	0.30
Enlace de Datos	Alto	0.30
Internet	Alto	0.30
Intranet del Iess	Alto	0.30
Herramientas de Office	Medio	2

3.4.14 Plan de contingencia para la coordinación administrativa de tecnologías de información

- Números de teléfono, mapas y direcciones.
- Responsabilidades y procedimientos.
- Información sobre adquisiciones y compras.
- Diagramas de las instalaciones de red
- Sistemas, configuraciones y copias de seguridad
- Medios de comunicación como radios, celulares ante cualquier incidencia.

3.4.15 Métodos para realizar pruebas de planes de contingencia

Prueba Específica

Consiste en preparar al personal en una función determinada, basándose en los procedimientos definidos en el Plan de Contingencia. De esta manera los funcionarios de la unidad médica

tendrán un trabajo bien definido y desarrollará la habilidad para cumplirla.

Prueba de Escritorio

Se desarrolla un plan de pruebas a través de un conjunto de preguntas.

Características:

- Se desarrolla en un formato preestablecido.
- Está orientado a las personas que conforman el grupo de recuperación de contingencias.
- Permite probar las habilidades de nivel gerencial del personal para la toma correcta de decisiones.

Simulación en Tiempo Real

Las pruebas de simulación real, se realizara en un tiempo definido.

- Las pruebas se hacen en tiempo real.
- Es usado para probar partes específicas del plan.
- Se debe trabajar en equipo para afrontar las contingencias.

3.4.16 Preparaciones PRE prueba

- Revisar minuciosamente el plan de contingencia.
- Verificar si se han asignado las respectivas responsabilidades.

- Verificar que el plan este aprobado por la dirección administrativa del hospital.
- Preparar a todo el personal, indicando los objetivos del plan, roles, responsabilidades y la apreciación global del proceso.
- Establecer la fecha y hora en que se puede ejecutar la prueba.
- Crear un documento y distribuirlo antes de realizar su ejecución en el cual incluya objetivos, alcances y metas.
- Analizar los resultados obtenidos, tomando en cuenta las vulnerabilidades encontradas en la prueba.
- Orientar los procesos críticos que dependen de sistemas específicos donde se asume que hay inconvenientes.
- Definir el lugar para realizar las reuniones del equipo de recuperación de contingencias.

3.4.17 Comprobación de Plan de contingencias

La funcionalidad del plan de contingencia se determina en que tan cerca se encuentren los resultados de la prueba con las metas planteadas.

Las estrategias básicas para disponer de equipo de reemplazo son:

Acuerdos con proveedores: Se establecen acuerdos de nivel de servicios con los proveedores, se debe determinar el tiempo de respuesta requerido.

Inventario de equipos: Los equipos requeridos se compran por adelantado y se almacenan en un sitio alterno al hospital.

Infraestructura del Ambiente Alterno: se requiere adecuar un ambiente alterno que pueda ser utilizado como área de rack en el momento de la contingencia con las dimensiones apropiadas para facilitar la ubicación de los equipos.

Los recursos básicos con que debe contar el sitio alterno están:

- 1 servidor debidamente configurado por el área de redes de la DNTI.
- 1 escritorio
- 1 mesa
- 1 silla
- 1 switch de 48 puertos
- 1 Router para la conexión a internet
- 1 UPS

3.5 Plan de Mantenimiento

El plan de contingencia debe adecuarse a cambios que puedan efectuarse en el hospital, por lo tanto siempre debe estar actualizado.

3.5.1 Control de cambios al plan

Se recomienda implantar controles del cambio para cubrir cualquier modificación que se tenga al Plan de Contingencia.

Se debe realizar una solicitud de cambios, la misma que debe ser aprobada por la Dirección Administrativa del Hospital.

3.5.2 Responsabilidad en el mantenimiento de cada parte del plan

Cada parte del plan será asignada a un integrante del equipo del Plan de Contingencia, que será responsable de mantener actualizado el plan.

La persona designada del equipo de Plan de Contingencia, mantendrá el control completo del plan.

3.5.3 Pruebas a todos los cambios del plan

El equipo del Plan de Contingencia, nombrará una o más personas que serán responsables de disponer todos los procesos de prueba y asegurar que todo cambio que se realice al plan se efectuara las pruebas respectivas para asegurar la calidad de los mismos.

Deberá existir una comunicación entre el coordinador del Plan de Contingencia y los coordinadores de cada área afectada ya que mostrara información acerca de los cambios que se requieren probar o examinar.

3.6 Plan de Entrenamiento

Toda el Área de TIC, debe entrenarse en el proceso de Recuperación del Plan de Contingencia. Se deben realizar sesiones de seguimiento para informar resultados conseguidos cuando se hayan realizado las respectivas pruebas.

Se debe realizar una campaña de sensibilización con los responsables de área cuyo objetivo será entrenar a los componentes de los equipos de recuperación.

3.6.1 Objetivo del entrenamiento

Planificar como tener actualizado el plan y al mismo tiempo conseguir que el personal esté preparado para poder utilizarlo correctamente.

3.6.2 Alcance del entrenamiento

- La capacitación se realiza a todo el personal en forma integral con el fin de que todo el personal conozca el proceso completo del plan.
- El hospital se encargara de difundir de acuerdo a un programa institucional todos los procedimientos que conllevara el plan

3.6.3 Revisión y actualización

El seguimiento periódico del plan permite conocer el avance, el cumplimiento de metas propuestas y los ajustes requeridos del mismo.

Esta evaluación se la puede realizar a través de:

Simulacros,- permiten entrenar al personal ante eventos posibles.

Evaluación del desempeño por evento.- valorar el programa de capacitación para asegurar su calidad y eficacia.

3.7 Diseño de estrategia de continuidad de los procesos y servicios que brinda el IESS Hospital de Ancón

3.7.1 Fallas en la comunicación entre cliente – servidor

El esquema Cliente/Servidor proporciona a los diferentes departamentos del hospital, soluciones locales, permitiendo la integración de la información relevante a nivel global.

Se procede a realizar la verificación a través de los siguientes pasos básicos:

1. El usuario reporta que no cuenta con acceso a la red.
2. El técnico del área de TIC procederá a identificar el problema en el sitio, verificando punto de red, si el punto esta averiado se procede a realizar el cambio respectivo.

3. Verificar el cable UTP, si existe daño, realizar el cambio del cable.
4. Si el problema no es en el punto de red se procede a verificar en el patch panel.
5. Se realiza el mantenimiento del punto de red del usuario y del gabinete de comunicaciones
6. Si no se resuelve el problema proceder a constatar si existe problema en la tarjeta de red del equipo, si el daño es en el mismo se realiza el cambio de tarjeta.
7. Se procede a recuperar el enlace de red para el usuario.

3.7.2 Falla del servidor

Si el servidor del hospital empieza a presentar fallas en su funcionamiento se deben tomar las siguientes precauciones:

Daños en disco duro

1. Determinar cuál es el disco dañado
2. Colocar todas las pcs con ip estáticas
3. Se comunica a los usuarios que procederán a quedarse sin internet e intranet.
4. Se procede a apagar el servidor.
5. Se retira el disco dañado y se coloca otro con la misma configuración e imagen del original, se configura de acuerdo a los parámetros establecidos por la DNTI.

6. Se restaura el último backup en el disco.
7. Se levantan los servicios en el servidor.
8. Se comprueba que todo funcione correctamente.
9. Se comunica a los usuarios que encuentra habilitado el internet e intranet.

3.7.3 Ausencia parcial o permanente del personal de TIC.

El IESS Hospital de Ancón cuenta con solo una funcionaria que es la responsable del área de TIC, el ausentarse del hospital implica que cause varios impactos tales como:

- Falta de soporte técnico
- En caso de presentarse algún inconveniente con los equipos informáticos no existiría la contingencia necesaria.
- No existiría monitoreo en los enlaces de datos.

3.7.4 Interrupción del fluido eléctrico.

Caso I: Interrupción del suministro eléctrico en lapsos cortos consecutivos

- Comunicarse con el área de servicios generales para la supervisión del generador principal del hospital.
- Monitorear el UPS central cada 20 min. para programar acciones mayores.

- Tomar la decisión de apagar los equipos activos y dar de baja los servicios para evitar daños y/o pérdida de información y de equipos.

Caso II: Interrupción del suministro eléctrico no mayor a una hora

- Comunicarse con área de servicios generales para la supervisión del generador principal del hospital.
- Monitorear el UPS central cada 10 min. para programar acciones mayores.
- Apagar los equipos no prioritarios como impresoras, monitores o PC que no demanden su uso.
- Contar con los procedimientos para apagar los equipos activos.

Caso III: Interrupción del suministro eléctrico mayor a una hora

- Dar aviso de la contingencia a los usuarios prioritarios: Dirección Administrativa, Dirección Médica, Financiero, Recursos Humanos, Médicos, TIC.
- Proceder al apagado de los equipos activos.
- Comunicarse con área de servicios generales para la supervisión inmediata del generador principal del hospital.
- Monitorear el UPS central cada 5 min. para programar acciones mayores.

3.7.5 Corte del servicio del enlace de datos.

El hospital cuenta con dos servicios de enlace de datos proporcionados por la empresa Brightcell y CNT.

El enlace principal es Brightcell, en caso de interrupciones de enlace por problemas en las troncales se activa automáticamente el enlace de backup de CNT así evitando la interrupción en el acceso a los servicios de internet, intranet y a los sistemas que utiliza el hospital.

CAPÍTULO 4

4. IMPLEMENTACIÓN Y ANÁLISIS DE RESULTADOS

4.1 Procedimientos para la implementación del plan de contingencias.

ETAPA DE ALERTA

Elaborar procedimiento de notificación de desastres.- Cualquier funcionario que identifique un incidente grave que pueda afectar al hospital, debe comunicarlo a alguno de los integrantes del comité del plan, proporcionando el mayor detalle posible en la descripción de los hechos, para que se proceda a evaluar la situación.

Elaborar procedimiento de ejecución del plan.- con toda la información de detalle sobre el incidente, se decidirá si se activa o no el plan de

contingencia. En caso afirmativo, se iniciará el procedimiento de ejecución del Plan.

Entre las acciones a realizarse para ejecutar el Plan están:

- Analizar la situación actual del hospital con respecto a los controles y acciones preventivas definidas para mitigar los riesgos.
- Seleccionar las opciones alternativas que se van a utilizar una vez sucedido un incidente que haya provocado una interrupción en los servicios.
- El método seleccionado garantizará la restauración de los procesos afectados.
- Se analizará la situación actual con respecto a los tiempos de respuesta requeridos por los sistemas.
- Se definirá un plan de trabajo y presupuesto requeridos, para implementar las acciones e infraestructura.
- Evaluar el análisis de impacto de la situación actual.
- Ejecutar las pruebas.

ETAPA DE TRANSICION

Elaborar procedimiento de traslado de equipos.- el área de servicios generales en conjunto con el área de TIC son los encargados de llevar los equipos de respaldo a un lugar alterno para ponerlos en funcionamiento.

ETAPA DE RECUPERACION

Elaborar procedimiento de restauración.- Los sistemas con criticidad de (1) son los que deben recuperarse lo antes posible, en las 48 horas siguientes.

Tabla 22. Procedimiento de Restauración

PROCESO	SUBPROCESO	NOMBRE DEL SISTEMA/MODULOS	CRITICIDAD	NECESIDADES DE RECUPERACION
INGRESAR HISTORIAS CLINICAS	Registrar datos personales del afiliado	MIS AS/400-MODULO DE ADMISION	1	LUNES A DOMINGO
VERIFICACION DE APORTACIONES	Verificación de Información en Página del IESS	PAGINA DEL IESS	1	LUNES A DOMINGO
INGRESO DE CITAS MEDICAS	Verificación de información en Sistema MIS AS/400	MIS AS/400-MODULO DE ADMISION	1	LUNES A DOMINGO
ATENCIONES MEDICAS	Registrar datos en sistema MIS AS/400	MIS AS/400-MODULO DE CONSULTA EXTERNA	1	LUNES A DOMINGO
INTERNACIONES MEDICAS	Registrar datos en sistema MIS AS/400	MIS AS/400-MODULO DE CONSULTA EXTERNA-MODULO DE EMERGENCIA-MODULO DE HOSPITALIZACION-MODULO DE ADMISION HOSPITALARIA	1	LUNES A DOMINGO
CIRUGIAS PROGRAMADAS/DE EMERGENCIA/ AMBULATORIAS	Registrar datos en sistema MIS AS/400	MIS AS/400-MODULO DE CONSULTA EXTERNA-MODULO DE EMERGENCIA-MODULO DE HOSPITALIZACION-MODULO DE QUIROFANO	1	LUNES A DOMINGO
REGISTRO DE MEDICAMENTOS	Registrar datos en sistema MIS AS/400	MIS AS/400-MODULO DE BODEGA DE FARMACOS	1	LUNES A DOMINGO
REGISTRO DE INSUMOS	Registrar datos en sistema MIS AS/400	MIS AS/400-MODULO DE BODEGA DE INSUMOS	1	LUNES A DOMINGO
REGISTRO DE EXAMENES	Registrar datos en sistema MIS AS/400	MIS AS/400-MODULO DE SERVICIO DE LABORATORIO	1	LUNES A DOMINGO
REGISTROS DE EMERGENCIA	Registrar datos en sistema MIS AS/400	MIS AS/400-MODULO DE EMERGENCIA-MODULO DE ADMISION HOSPITALARIA	1	LUNES A DOMINGO

Elaborar procedimiento de soporte.- Se informa a las áreas para que realicen las comprobaciones necesarias de los sistemas con el fin de certificar que funcionen de manera correcta y pueda continuar dando el servicio, dando las garantías de seguridad necesarias (confidencialidad, integridad, disponibilidad).

Tiempos máximos de atención de requerimientos

Tabla 23. Tiempos de atención a requerimientos

RESPONSABILIDADES	ACTIVIDAD	TIEMPO MAXIMO DE ATENCION (min)
CREACION DE USUARIOS	CREACION DE NUEVOS USUARIOS EN EL SISTEMA MIS AS400	30
	CREACION DE NUEVOS USUARIOS EN EL SISTEMA DE GESTION DOCUMENTAL QUIPUX	20
	CREACION DE NUEVOS USUARIOS DE CORREO ELECTRONICO	15
	CONFIGURACION DE ACCESOS	15
	REALIZAR LAS PRUEBAS RESPECTIVAS DE LA CONFIGURACION	10
ADMINISTRACION DE MODULOS DE SISTEMA AS400	CAMBIO DE AGENDAS DE MÉDICOS	60
	MOVIMIENTO DE CITAS MÉDICAS	30
	CAMBIO DE HORARIOS DE MÉDICOS	30
	REPORTES AL CALL CENTER POR MOVIMIENTO DE AGENDAS	15
	IMPLEMENTACIÓN DE NUEVOS MÓDULOS DEL SISTEMA MIS AS400	30
	ADMINISTRACIÓN GENERAL DEL SISTEMA MIS AS400 EN LOS MÓDULOS: BODEGA, ADMISIÓN CE, ADMISIÓN HO, FACTURACIÓN, SERVICIOS (LABORATORIO, ENFERMERÍA CE, ENFERMERÍA EM, RAYOS X, ECOGRAFÍAS, ELECTROCARDIOGRAMAS, COLPOSCOPIAS), FARMACIA, EMERGENCIA, HOSPITALIZACIÓN, MODULO DE ENFERMERÍA, MODULO MEDICO, CONSULTA EXTERNA, QUIRÓFANO, CIRUGÍAS DEL DÍA, CIRUGÍAS PROGRAMADAS,	60

	MODULO ENFERMERÍA DE QUIRÓFANO, MODULO ENFERMERÍA DE RECUPERACIÓN	
	CREACIÓN DE CODIFICACIÓN EN EL SISTEMA AS400	30
ADMINISTRACION DE SISTEMAS	ADMINISTRACIÓN DE HERRAMIENTA WEBMIN	30
	ADMINISTRACIÓN DE HERRAMIENTA WEB PHP LDAP ADMIN PARA USUARIOS DEL DOMINIO	30
	ADMINISTRACIÓN DEL SISTEMA DE GESTIÓN DOCUMENTAL QUIPUX	30
	ADMINISTRACION DE HERRAMIENTA DE DISPONIBILIDAD DE CAMAS MSP	30
ADMINISTRACION DE EQUIPOS DE RED	ADMINISTRACIÓN DE EQUIPOS LAN DEL HOSPITAL PARA LA COMUNICACIÓN DE DATOS INTERNA. (SWITCH, ROUTERS, ETC)	45
	ADMINISTRACIÓN DE SERVIDOR	45
	ADMINISTRACIÓN DE AP	45
	ADMINISTRACIÓN DE CABLEADO ESTRUCTURADO	45
	GESTIÓN DE DIRECCIONAMIENTO IP	45
	ADMINISTRACIÓN DE PLATAFORMA TECNOLÓGICA	45
IMPLEMENTAR Y ADMINISTRAR SEGURIDADES	GESTIONAR Y GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS INFORMÁTICOS DEL HOSPITAL	45
	APLICACIÓN DE PLANES DE CONTINGENCIA EN CASO DE DETECCIÓN DE AVERÍAS EN LA INFRAESTRUCTURA TECNOLÓGICA	60
	SUPERVISIÓN DE EQUIPOS WAN POR PARTE DEL PROVEEDOR DE SERVICIOS DE INTERNET (TRANSCIVERS, MODEMS, ETC)	45
PROPORCIONAR SEGURIDAD ESPECIFICANDO EL CUMPLIMIENTO DE LOS OBJETIVOS	APLICACIÓN DE POLÍTICAS Y NORMAS DE LOS PROCEDIMIENTOS TECNOLÓGICOS	30
	ACOGER, AJUSTAR E IMPLEMENTAR ESTÁNDARES EN LOS PROCESOS DE GESTIÓN DE LA TECNOLOGÍA DE INFORMACIÓN Y LA COMUNICACIÓN	30
	GENERAR LINEAMIENTOS Y POLITICAS PARA LA GESTIÓN DE INFRAESTRUCTURA DE LA TECNOLOGÍA DE INFORMACIÓN	30
	COORDINAR Y PARTICIPAR EN LOS PROCESOS DE CONTRATACIÓN, PRUEBAS Y RECEPCIÓN DE EQUIPOS	60
	ASEGURAR LA DISPONIBILIDAD PERMANENTE, ACTUALIZADA Y CONFIABLE DE RECURSOS DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIÓN	60
ATENCION DE REQUERIMIENTOS DE AFILIADOS	VERIFICACION DE INFORMACION DEL AFILIADO EN EL SISTEMA MEDICO AS400	30

MANTENER EL BUEN FUNCIONAMIENTO DE LOS EQUIPOS DE COMPUTO Y DAR SEGUIMIENTO A LAS GARANTIAS DE LOS MISMOS	REALIZAR PROGRAMACION DE REVISION DE EQUIPOS	30
	APLICAR A TODOS LOS EQUIPOS ASIGNADOS A LAS DIFERENTES AREAS DE LA UNIDAD	120
	SE RECIBE EL EQUIPO AVERIADO	30
	DIAGNOSTICAR SI EL/LOS EQUIPOS PRESENTAN FALLAS EN SU FUNCIONAMIENTO YA SEA POR EL TIEMPO Y FRECUENCIA DE USO O INAPROPIADA MANIPULACION	60
	REALIZAR REPARACION O REEMPLAZO DEL COMPONENTE	90
PROPORCIONAR SOPORTE TECNICO A TODOS LOS USUARIOS DE EQUIPOS DE COMPUTO EN CUESTION DE SOFTWARE Y HARDWARE	SOPORTE AL SISTEMA DE GESTIÓN DOCUMENTAL QUIPUX	45
	SOPORTE TÉCNICO A USUARIOS MÉDICOS Y ADMINISTRATIVOS DEL HOSPITAL	60
	BRINDAR SERVICIO DE ATENCIÓN PRIMARIA A USUARIOS EN ASPECTOS OPERATIVOS DEL SISTEMA MEDICO	30
	CAMBIOS DE CLAVES DE USUARIOS	15
	APOYO EN LA SOLUCIÓN DE PROBLEMAS RELACIONADOS CON EL USO DE LOS EQUIPOS Y LA RED	30
CONFIGURACION DE EQUIPOS SEGÚN LAS POLITICAS DE USO	INTEGRAR A LA RED DE LA UNIDAD EL EQUIPO DE COMPUTO DE NUEVA ADQUISICION	45
	ACTUALIZACION, SUSTITUCION O INSTALACION DE DIFERENTES COMPONENTES DE SOFTWARE O HARDWARE	45
SALVAGUARDAR TODA LA INFORMACION RELEVANTE DE LOS EQUIPOS	ALMACENAMIENTO DE RESPALDOS DE INFORMACION	90
REGISTRAR INFORMACION	ADMINISTRAR EL INVENTARIO DE RECURSOS DE TECNOLOGÍA DE INFORMACIÓN DE LA UNIDAD	60
	REALIZAR INFORMES DE GESTIÓN	30
	ELABORAR INFORMES TECNICOS	30
	MANTENER ACTUALIZADA LA DOCUMENTACIÓN TÉCNICA Y DE USUARIOS	60
	ELABORACIÓN DE MANUALES Y DOCUMENTACIÓN	90

4.2 Implementación del plan de tratamiento de riesgos.

En esta sección se tomara la acción más apropiada de tratamiento para cada uno de los riesgos identificados.

Mitigar el riesgo.- reducir mediante la implantación de controles que reduzcan el riesgo a un nivel aceptable.

Asumir el riesgo.- la Dirección Administrativa asume el riesgo ya que está por debajo de un valor de riesgo aceptable, simplemente requiere que quede documentado que la dirección conoce y acepta estos riesgos.

Transferir el riesgo a un tercero.- asegurar el activo que tiene el riesgo, subcontratando el servicio.

Eliminar el riesgo.- eliminar el activo, eliminar el proceso.

Tabla 24. Plan de tratamiento de riesgos

ACTIVO	AMENAZAS	VULNERABILIDADES	Plan de Tratamiento de Riesgos
PC´S	Fuego	Falta de protección contra fuego	Mitigar
	Daños por agua	Falta de protección física adecuada	Mitigar
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres	Aceptar
	Acceso no autorizado al equipo	Falta de Protección por desatención de equipos	Mitigar
	Corte de suministro eléctrico	Inconvenientes en el funcionamiento del UPS	Mitigar
	Instalación no autorizada o cambios de Software	Falta de control de acceso	Mitigar
	Incumplimiento con la legislación	Falta de conocimiento de protección de derechos de SW por parte de los empleados	Mitigar

	Uso no previsto	Falta de las políticas	Mitigar
	Incumplimiento con controles de seguridad	Falta de conocimiento de seguridad por parte del personal	Mitigar
	Deterioro del HW	Falta de mantenimiento adecuado	Mitigar
	Robo	Falta de protección física	Mitigar

SERVIDOR	Fuego	Falta de protección contra fuego	Mitigar
	Daños por agua	Falta de protección física adecuada	Aceptar
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres	Aceptar
	Acceso no autorizado al equipo	Falta de Protección por desatención de equipos	Mitigar
	Corte de suministro eléctrico o Falla en el aire acondicionado	Funcionamiento no confiable del UPS o funcionamiento no adecuado del aire acondicionado	Mitigar
	Instalación no autorizada o cambios de Software	Falta de control de acceso	Mitigar
	Uso no previsto	Falta de las políticas	Mitigar
	Incumplimiento con controles de seguridad	Falta de conocimiento de seguridad por parte del personal	Mitigar
	Deterioro del HW	Falta de mantenimiento adecuado	Mitigar
	Manipulación de la Configuración	Falta en control de acceso	Mitigar
	Análisis de tráfico	Falta de establecimiento de una conexión segura (VPN)	Mitigar
	Brechas de seguridad no detectadas	Falta de monitoreo de los servidores	Mitigar

SOPORTE ELECTRONICO	Fuego	Falta de protección contra fuego	Mitigar
	Daños por agua	Falta de protección física adecuada	Aceptar
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres	Aceptar
	Condiciones inadecuadas de	Susceptibilidad al calor	Aceptar

	temperatura		
	Robo	Falta de protección física	Mitigar
	Escape de información	Manipulación inadecuada de información	Mitigar

REGISTROS Y DOCUMENTACION	Fuego	Falta de protección contra fuego	Mitigar
	Daños por agua	Falta de protección física adecuada	Mitigar
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres	Aceptar
	Acceso no autorizado al equipo	Falta de Protección por desatención de equipos	Mitigar
	Perdida de Información	Errores de usuarios-Almacenamiento no protegido	Mitigar
	Incorrecta o incompleta información del sistema	Falta documentación actualizada del sistema	Mitigar
	Modificación no autorizada de la información	Desconocimiento de políticas de los empleados	Mitigar

HOSPITAL	Fuego	Falta de protección contra fuego	Mitigar
	Daños por agua	Falta de protección física adecuada	Mitigar
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres	Aceptar
	Acceso no autorizado	Desconocimiento de políticas, falta de protección física	Mitigar

CORREO ELECTRONICO	Errores de los usuarios	Desconocimiento del servicio	Mitigar
	Suplantación de usuario	Falta de control de acceso	Mitigar
	Uso indebido	Desconocimiento de políticas	Mitigar
	Fallas de enlace	Falta de acuerdos definidos por proveedores	Mitigar

SISTEMA OPERATIVO	Negación de Servicio	Capacidad insuficiente de los recursos	Mitigar
	Errores de Configuración	Falta de capacitación del administrador	Mitigar
	Virus, Fuerza Bruta y ataques de diccionario	Falta de Protección	Mitigar
	Falta de capacidad de restauración	Falta de copias de backup continuas	Mitigar
	Pérdida de Servicio	Actualizaciones incorrectas	Mitigar
	Controles de Seguridad no cumplidos	Falta de Políticas de Seguridad	Mitigar
	Alteración no autorizada de la configuración	Falta de control de acceso	Mitigar

4.3 Implementación de controles.

Topología de red

Deberá existir documentación detallada sobre los diagramas topológicos de la red.

Deberán existir medios alternos de transmisión en caso de que alguna contingencia afecte al medio de comunicación.

Con respecto a la utilización de la intranet deben almacenarse datos sobre:

- Ancho de banda utilizado.
- Recursos de los servidores que utilizan las aplicaciones.
- El estado de cada aplicación.
- Intentos de intrusión

Antivirus

En todos los equipos del hospital se debe instalar y correr el antivirus actualizado, el mismo que debería cumplir con lo siguiente:

- El antivirus debe ejecutarse en tiempo real.
- Revisar y detectar software malicioso en las estaciones de trabajo.
- Actualizar las definiciones del software antivirus.
- Debe ser un producto con licencia.

Deberá existir un procedimiento formal a seguir en caso que se detecte un virus en algún equipo del sistema.

Ataques de red

Deberá utilizarse una herramienta que monitoree la red, con el fin de evitar el ataque de denegación de servicio (DoS).

Para disminuir el riesgo de sniffing, la red del hospital deberá segmentarse física y/o lógicamente.

Con el fin de disminuir la posibilidad de spoofing el firewall deberá denegar el acceso a cualquier tráfico de red externo que posea una dirección fuente que debería estar en el interior de la red interna.

Seguridad física

Los computadores del hospital deben permanecer seguros, cuando se han implantado las medidas de control apropiadas para proteger el software, el hardware y los datos. No se permite fumar, comer o beber mientras se está usando un PC.

Deben protegerse los equipos de riesgos del medioambiente (por ejemplo, polvo, incendio y agua).

Cualquier falla en los computadores o en la red debe reportarse inmediatamente ya que podría causar problemas serios como pérdida de la información o indisponibilidad de los servicios.

No pueden moverse los equipos o reubicarlos sin permiso. Para llevar un equipo fuera del hospital se requiere una autorización firmada por el Director Administrativo.

La pérdida o robo de cualquier componente de hardware debe ser reportada inmediatamente.

Control de acceso físico al hospital

Se deberá asegurar que todos las personas que entren a áreas restringidas se identifiquen y sean autenticados y autorizados para entrar.

Deberán existir guardias de seguridad en permanente monitorización, durante el horario laboral. Se deberán ubicar en el exterior y el interior del hospital.

Los servidores de red y los equipos de comunicación deben estar ubicados en lugares apropiados, protegidos contra daños y robo.

Debe restringirse severamente el área de rack a personas no autorizadas mediante el uso de cerraduras y otros sistemas de acceso.

Cableado estructurado

Se deberá documentar en planos los canales de tendidos de cables y la red existentes.

Deberán tomarse las acciones correctivas necesarias con respecto a la medición del ancho de banda.

Ante un corte del suministro de energía eléctrica deberán apagarse los equipos del área de rack de forma segura, como medida de prevención.

Respaldos

Se deberá asegurar la existencia de un procedimiento aprobado para la generación de copias de respaldo sobre toda la información necesaria para las operaciones del hospital, donde se especifique la periodicidad y el lugar físico donde se deben mantener las copias generadas.

Deben generar copias de respaldo de las configuraciones de los servidores, documentando las modificaciones realizadas para identificar las distintas versiones.

4.4 Mantenimiento de Plan de contingencias y revisiones.

Se debe dar un seguimiento continuo al plan de contingencia ya que las limitaciones encontradas en las pruebas deben analizarse planteando alternativas y soluciones.

Capacitaciones

Se deben efectuar reuniones semestrales con el personal de TIC y el comité de plan de contingencia con el fin de realizar simulacros que permitan evidenciar debilidades que se puedan encontrar en el plan.

Estas reuniones servirán como entrenamiento para evaluar los resultados obtenidos y determinar el tiempo de recuperación de los servicios.

Reuniones de mantenimiento y actualización del plan

Estas reuniones se las realizan con los departamentos que conforman la comisión para el mantenimiento del Plan de Contingencia; tienen como objetivo revisar y dar soluciones.

Se deberá poner a consideración a los responsables de área todas las soluciones que se establecieron en las reuniones de capacitación y entrenamiento.

4.5 Entorno de las Pruebas del Plan de contingencias.

Durante la aplicación de la propuesta del Plan de contingencia a la intranet del IESS Hospital de Ancón, se realizaron las siguientes actividades:

- Configuración de un servidor de respaldo en un equipo que será utilizado como contingente, el servidor cuenta con todos los servicios instalados por parte de la DNTI para que sea utilizado como proxy.
- Se procedió a la adquisición de otro gabinete para independizar al servidor y al switch de respaldo.
- Se habilito una conexión eléctrica independiente para los gabinetes del área de rack que están enlazadas con el UPS principal de la Unidad.
- Se sugirió en base a estadísticas la contratación de un técnico informático debido a que solo existe una sola persona en el área de TIC y se hace prescindible la presencia de otro funcionario con conocimientos de redes para poder solventar inconvenientes que se presenten en el hospital.
- Se entregó el plano de la construcción y activación del área de rack alterno debido al tiempo se habilitara en el próximo periodo.
- Se coordinó con el área de Tecnologías en la ciudad de Quito para la contratación en el próximo periodo los servicios de un prestador externo para los mantenimientos de los equipos de red.

A continuación se presenta el cronograma de pruebas del Plan de Contingencia:

Tabla 25. Cronograma del Plan de Contingencias

TAREA	DURACIÓN (DIAS)
Desarrollo de entorno de prueba	2
Capacitación del Personal del área médica y administrativa	5
Preparación de equipos de contingencia	1
Ejecución de actividades de contingencia en entorno de prueba	1
Ejecución de Actividades	1
Evaluación de Resultados	1
Presentación de cambios sobre actividades de contingencia	1
Verificación funcional de cambios en entorno de prueba	1
Retroalimentación del Plan de Contingencia	1

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

1. Con la implementación de un plan de contingencia a la intranet del IESS Hospital de Ancón se lograra mejorar la disponibilidad de infraestructura tecnológica alcanzando la productividad de atención a la comunidad afiliada con menos caídas y mejores tiempos de respuesta a la resolución de problemas.

2. Aplicar la metodología ITIL promueve la calidad para alcanzar la efectividad y eficiencia en los servicios de TI que utiliza el hospital.

3. Un adecuado monitoreo de los recursos que forman parte de la intranet del hospital permitirán determinar posibles cuellos de botella que ocasionarían fallas en los sistemas y de seguridad

4. Este plan de contingencia permitirá al hospital estar preparado ante procesos críticos, mediante la elaboración, prueba y mantenimiento sin exponer la integridad del personal.

5. Tomando en cuenta este trabajo el hospital puede establecer los perfiles de las responsabilidades que debe cumplir el comité destinado para el plan de contingencia.

Recomendaciones

1. Programar las actividades indicadas en el plan de contingencia para lograr obtener un respaldo de todos los procesos que conlleva el hospital adquiriendo así continuidad en sus operaciones.

2. Realizar periódicamente análisis de los riesgos y monitorear continuamente la situación, pues la seguridad que se requiere proporcionar debe ser un proceso continuo.

3. Capacitar al personal de TIC en temas de seguridad informática.

4. Difundir este plan de contingencia al área administrativa y médica, con la finalidad de instruir al personal del hospital.

5. Tener una adecuada seguridad a los recursos informáticos desde el dato más simple hasta el más valioso que es el recurso humano.

BIBLIOGRAFÍA

[1] Jean-Marc Royer, Seguridad en la informática de empresa: Riesgos, Amenazas, prevención y soluciones, Ediciones ENI, 2004.

[2] Jan Van Bon, Fundamentos de ITIL V3. Zaltbommel: Van Haren Pub., 2008.

[3] ISACA, La función de seguridad de la información. Presiones actuales y emergentes desde la inseguridad de la información [En línea]. Disponible: http://www.isaca.org/Journal/archives/2014/Volume-6/Documents/The-Information-Security-Function_joa_Spa_1114.pdf, 2016

[4] Martínez Juan Gaspar, El Plan de Continuidad del Negocio: Una guía práctica para su elaboración. Ediciones Díaz de Santos, 2008

[5] Javier Areitio, Seguridad de la Información: redes, informática y sistemas de información, Ediciones Paraninfo, 2008