UNIVERSIDAD PRIVADA ANTENOR ORREGO

FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA DE COMPUTACIÓN Y SISTEMAS

"PLAN DE MEJORA DE LA SEGURIDAD DE LA INFORMACIÓN DEL SEGURO SOCIAL DE SALUD – ESSALUD APLICANDO ESTÁNDAR ISO/IEC 27001"

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

LÍNEA DE INVESTIGACIÓN: SEGURIDAD DE LA INFORMACIÓN

AUTOR : Br. Luis Alejandro Poma Rosales

ASESOR: Dr. Jorge Lorenzo Huapaya Escobedo

FECHA DE SUSTENTACIÓN: 17/12/2019

TRUJILLO - PERÚ

2019

“PLAN DE MEJORA DE LA SEGURIDAD DE LA INFORMACIÓN DEL SEGURO SOCIAL DE SALUD – ESSALUD APLICANDO ESTÁNDAR ISO/IEC 27001”

Desarrollado por:

Br. Luis Alejandro Poma Rosales
Tesista

Aprobado por:

Ing. Jaime Eduardo Díaz Sánchez
Presidente
N.º CIP: 73304

Ing. Karla Vanessa Meléndez Revilla
Secretaria
N.º CIP: 120097

Ing. Albertis Florián Vigo
Vocal
N.º CIP: 114879

Dr. Jorge Lorenzo Huapaya Escobedo
Asesor
N.º CIP: 17215

PRESENTACIÓN

Señores Miembros del Jurado:

De conformidad a lo estipulado en el Reglamento de Grados y Títulos de la Universidad Privada Antenor Orrego y el Reglamento interno de la Escuela Profesional de Ingeniería de Computación y Sistemas, pongo a vuestra disposición la presente Tesis titulada: **"PLAN DE MEJORA DE LA SEGURIDAD DE LA INFORMACIÓN DEL SEGURO SOCIAL DE SALUD – ESSALUD APLICANDO ESTÁNDAR ISO/IEC 27001"** para obtener el Título Profesional de Ingeniero de Computación y Sistemas.

El contenido del presente trabajo ha sido desarrollado tomando como marco de referencia los lineamientos establecidos por la Escuela Profesional de Ingeniería de Computación y Sistemas y los conocimientos adquiridos durante nuestra formación profesional, consulta de fuentes bibliográficas e información obtenida en el Hospital Especializado Víctor Lazarte Echegaray, perteneciente a la Red Asistencial La Libertad.

Dedicatoria

A mis padres:

Por creer en mí y ayudarme a
mejorar como persona cada día.

Por motivarme en mi vida de estudiante
y alentarme a realizar este estudio.

Por ayudarme a llegar a ser quién soy ahora,
en tiempos buenos y difíciles.

Br. Luis Alejandro Poma Rosales

Agradecimientos

Este trabajo es muestra del esfuerzo invertido para poder demostrar parte del conocimiento obtenido durante los cinco años de vida universitaria.

Agradezco especialmente a mis padres por el apoyo incondicional brindado en todo momento y ser el motivo de superación cada día.

Al Asesor, el Dr. Jorge Lorenzo Huapaya Escobedo por depositar su confianza en mí y brindarme sus conocimientos para poder realizar y sustentar esta Tesis.

A mis compañeros de trabajo, de estudio y familiares por los consejos, buenos momentos y anécdotas.

Br. Luis Alejandro Poma Rosales

“PLAN DE MEJORA DE LA SEGURIDAD DE LA INFORMACIÓN DEL SEGURO SOCIAL DE SALUD – ESSALUD APLICANDO ESTÁNDAR ISO/IEC 27001”

Por:
Br. Luis Alejandro Poma Rosales

Resumen

El Seguro Social de Salud – EsSalud es una entidad peruana prestadora de servicios de salud y seguridad social la cual, con el transcurso de tiempo, está obteniendo demasiados problemas en seguridad de la información: recuperación y respaldo de información, comunicaciones y redes, contingencia y mitigación son las principales causas que impiden una correcta gestión de la seguridad de la información.

El objetivo principal de esta tesis es demostrar la importancia de una correcta administración de la seguridad de la información en entidades públicas peruanas. Para ello, se desarrollará un Plan de Seguridad de la Información en una entidad pública usando el estándar ISO 27001: Seguridad de la Información.

En este caso, se desarrollará un Plan de Seguridad de la Información en el Hospital Víctor Lazarte Echegaray de Trujillo, perteneciente a la Red Asistencial La Libertad. Para lograr el éxito de este estudio, se reunirá la información requerida y evidencias para el diseño del presente Plan.

“IMPROVEMENT PLAN OF INFORMATION SECURITY IN SEGURO SOCIAL DE SALUD – ESSALUD APLYING ISO / IEC 27001 STANDARD”

By:
Br. Luis Alejandro Poma Rosales

Abstract

Seguro Social de Salud – EsSalud is a Peruvian’s health public body, that over time is getting too many troubles in terms of information security: data recovering and backup. Communication and networking, contingency and mitigation are the main agents attempting infringe against information security in different ways.

The main purpose of this thesis is demonstrating why information security management in Peruvian’s public sector is important. Thus, it will develop an Information Security Plan in a health public entity using ISO 27001 standard: Information Security.

In this case, an Information Security Plan was developed in hospital Victor Lazarte Echegaray Hospital of Trujillo, located in La Libertad department. To assure the success of this thesis, we will gather required information and evidences to support our sources, design, implement and run of this Plan.

ÍNDICE

Lista de tablas

Lista de figuras

1 INTRODUCCIÓN

En la actualidad, el interés social en las organizaciones en general y en particular organizaciones e instituciones del estado peruano por la protección de los datos personales es consecuencia del aumento del riesgo de pérdida de confidencialidad, integridad o disponibilidad originado por su tratamiento automatizado (Alvarado, 2016), hoy denominada "transformación digital".

Tanto entidades públicas como privadas vienen enfrentando desafíos respecto al empleo racional de la tecnología de información (TICS), las cuales se han tornado más sofisticadas y pueden llegar a ser potencialmente devastadoras. Por ello, la estrategia debe incluir políticas que acompañen la gestión y la definición de sus procesos (Seclén Arana, 2016).

El Seguro Social de Salud – EsSalud es una entidad pública de Seguridad Social de Salud fundada el 12 de agosto de 1936 mediante Ley N.º 8433 como Caja Nacional del Seguro Social Obrero, luego como Instituto Peruano de Seguridad Social – IPSS mediante el 16 de julio de 1980 mediante Ley N.º 23161. Se creó sobre la base del Seguro Social de Salud – EsSalud bajo el Decreto de Ley N.º 27056 el 30 de enero de 1999. Actualmente cuenta con centros hospitalarios en todo el Perú. Su rubro son las prestaciones de salud, económicas y sociales.

El Hospital Víctor Lazarte Echegaray, perteneciente a la Red Asistencial La Libertad cuenta con 68 años de antigüedad y es el principal centro de atención en el departamento de La Libertad, junto con el Hospital de Alta Complejidad.

EsSalud, se encuentra en pleno proceso de modernización de sus servicios, ampliando la cobertura de atención para cubrir adecuadamente la demanda creciente de prestaciones (Seguro Social de Salud - EsSalud: Red Asistencial Moquegua, 2016). Sin embargo, la inadecuada gestión de las tecnologías de información impide a los diferentes niveles de decisión y en particular al nivel operativo solucionar los problemas rutinarios que se presentan a diario, tales como el mantenimiento preventivo y no programado de los equipos informáticos y la falta de comunicación entre los servicios. Está comprobado que la seguridad de las tecnologías de información es débil y está sujeta a vulnerabilidades que pueden traer perjuicio a la institución (Seguro Social de Salud - EsSalud: Red Asistencial Moquegua, 2016).

Debido a ello, en EsSalud , se ha establecido como estrategia global ejecutar planes de acción que le permitan lograr sus objetivos, especialmente, enfocados en la reingeniería de la estructura organizacional, la incorporación de nuevas aplicaciones informáticas para la gestión de la información bajo un enfoque integrador de la estrategia, las personas y la tecnología (Seguro Social de Salud - EsSalud: Sede Central, 2016).

Durante el inicio del estudio (segundo semestre del 2016) EsSalud detallaba el nivel de implementación del Sistema de Control Interno – SCI formulado según RC Nº 320-2006-CG (Controlaría General de la República, 2006) y aprobado según RC Nº 458-2006-CG (Contraloría General de La Repúplica, 2008), el cual se encontraba aún en desarrollo como se observa en la tabla 1.

A la fecha (diciembre del 2019), no se ha implementado el Sistema de Control Interno mas si planificado, documentado y evaluado.

Tabla 1: Nivel de implementación del Sistema de Control Interno

		PUNTAJE (1 a 5)	ESTADO
COMPONENTES	Ambiente de control	2.98	En proceso
	Evaluación de riesgos	1.17	Inicial
	Actividades de control gerencial	1.86	Inicial
	Información y comunicación	2.85	En proceso
	Supervisión	2.37	En proceso
Nivel de Implementación del SCI		2.95	En proceso

Fuente: (Seguro Social de Salud - EsSalud: Sede Central, 2016)

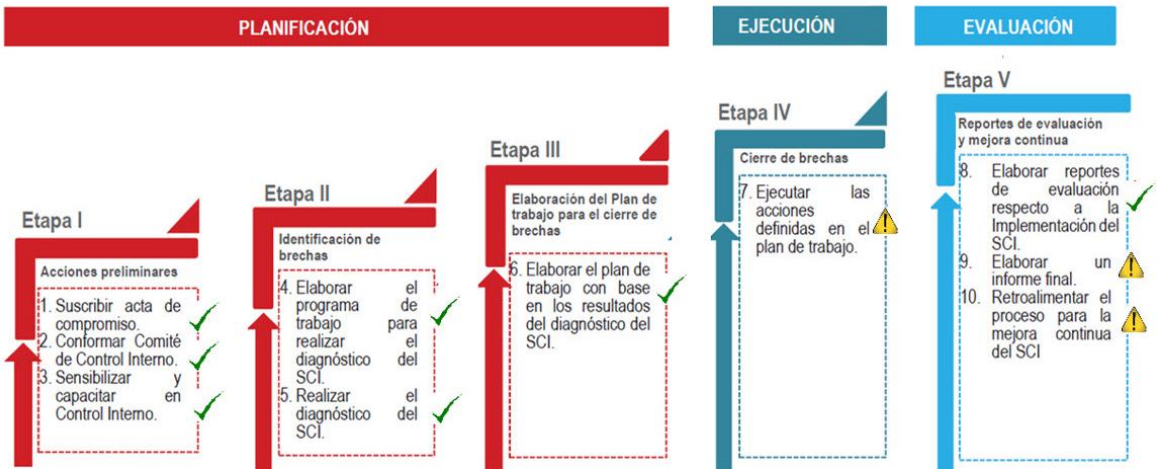


Ilustración 1: Estado de implemenetación del SCI (diciembre del 2019).

Fuente: (Seguro Social de Salud de Salud - EsSalud, 2019)

El estándar ISO/IEC 27001: Seguridad de la Información permite utilizar un criterio uniforme para seleccionar los objetivos de control y herramientas de auditoría que conducirá a la obtención de un informe fundamentado en estándares conocidos a nivel internacional (Paredes Cabrera, 2016). El diseño e implementación de controles, evaluación de seguridad de las comunicaciones, elaboración de la gestión de riesgos es viable y útil para el aseguramiento de las tecnologías de información (Gonzales Tintaya, 2017).

De acuerdo a lo descrito anteriormente, se formula el problema de investigación siguiente***:***

¿De qué manera se puede mejorar la gestión de la seguridad de la información del Hospital Víctor Especializado Lazarte Echegaray de la Red Asistencial La Libertad - EsSalud?

Y la hipótesis siguiente:

"El diseño de un Plan de Seguridad de la Información de acuerdo al estándar ISO/IEC 27001: "Seguridad de la Información" permitirá la mejora de la gestión de la seguridad de la información".

El objetivo principal de la investigación es

"Diseñar Plan de Seguridad de la Información de acuerdo al estándar ISO/IEC 27001: Seguridad de la Información" para la mejora de la gestión de la seguridad de la información en el Hospital Especializado Víctor Lazarte Echegaray, perteneciente a la Red Asistencial La Libertad.

Los objetivos específicos son:

- Verificar cumplimiento actual de objetivos y controles alineados al diseño del Plan de Seguridad de la Información.
- Evaluar nivel o grado de confidencialidad, disponibilidad e integridad con los responsables del centro hospitalario y grupos de interés (usuarios involucrados).
- Analizar resultados de la evaluación.

La investigación ha permitido documentar las respectivas observaciones, en concordancia los estándares establecidos en las Normas Técnicas Peruanas, ya que ello facilitará una adecuada gestión de calidad de las Tecnologías de la Información en el ámbito hospitalario de EsSalud.

El Informe contiene los capítulos siguientes: Introducción del estudio, Marco de referencia, Metodología, Resultados, Discusión de resultados.

Y finalmente el enunciado de las conclusiones y recomendaciones.

2 MARCO DE REFERENCIA

2.1. Antecedentes del estudio.

Landázuri Guevara (Landazuri Guevara, 2015) desarrolló un Plan de Auditoría "Auditoría a la Seguridad del Sistema de Información SIVIGILA de la Alcaldía de San Andrés de Tumaco basada en el Estándar ISO 27001" con el propósito de actualizar la forma de cómo se trata a la información en esta entidad, encontrándose lo siguiente:

- No hay políticas de seguridad de la información.
- Se tiene poco conocimiento la seguridad de la información.
- La información no se contempla como activo de la entidad.
- No hay mucho compromiso con la seguridad de la información.
- La palabra "auditoría" genera malestar laboral.
- Siempre hay temas más importantes que ser pioneros en la protección de los datos manejados en la organización.
- Poco orden en el desarrollo de los procesos.

Seclén Arana (Seclén Arana, 2016) recomienda en su estudio "Factores que afectan la Implementación del Sistema de Gestión de Seguridad de la Información en las Entidades Públicas Peruanas de acuerdo a la NTP-ISO/IEC 27001" apoyarse en las certificaciones como mecanismo para asegurar el correcto funcionamiento del Sistema de Gestión de la Seguridad de la Información, del Plan de Continuidad de Negocio y del Plan de Contingencia Tecnológica. Aplicar estrategias para la concientización del personal en seguridad de la información y añadir un presupuesto

central para una gestión adecuada de los recursos de seguridad de la información según lo dispuesto en la NTP-ISO/IEC 27001.

Ramírez Martínez afirma en su estudio "Análisis del Nivel de Cumplimiento de los Lineamientos Estratégicos de Gobierno y Gestión de Tecnologías de Información y Comunicaciones en las entidades Públicas de Manizales" que las entidades del estado colombiano son el principal objeto de estudio debido a que deben responder a la ciudadanía en sus modos de gobernar y gestionar las TI beneficiándolos y generando transparencia, agilidad, eficiencia y eficacia en sus procesos de gestión.

Se pudo determinar que los problemas que surgen en las organizaciones a nivel mundial tienen que ver mucho con el mal manejo de les dan a las TI. Las entidades deben estar siempre pendientes de la normatividad vigente que expide el gobierno nacional y cumplir con los decretos que promulga constantemente para la implementación del gobierno en línea (Ramírez Martínez, 2017).

2.2. Marco teórico.

2.2.1. Auditoría

La auditoría es el examen crítico y sistemático que realiza una persona o grupo de personas independientes del sistema auditado, que puede ser una persona, organización, sistema, proceso, proyecto o producto.

La auditoría es una serie de métodos de investigación y análisis con el objetivo de producir la revisión y evaluación profunda de la gestión efectuada (Amado Suárez, 2008).

2.2.2. ISO 27001: Seguridad de la información.

Este estándar internacional ha sido preparado con el fin de ofrecer un modelo para establecer, implementar, operar, monitorear, mantener y mejorar un efectivo

Sistema de Gestión de Seguridad de la Información. Este sistema de gestión preserva la confidencialidad, integridad y disponibilidad de la información aplicando un proceso de gestión de riesgos, y proporciona confianza a las partes interesadas en el sentido en que los riegos se manejan adecuadamente (Seclén Arana, 2016).

ISO 27001 proporciona instrucciones sobre cómo establecer un sistema de gestión que superponga una disciplina sobre cómo seleccionar controles y cómo establecer buenas prácticas para aplicar los controles de seguridad. Los procedimientos para implementar realmente los controles de seguridad dependen de la organización y variarán de acuerdo con el entorno físico y técnico (Árnason & Keith, 2008).

Es una especificación para un Sistema de Gestión de la Seguridad de la Información. Establece requisitos y utiliza palabras como un deber (Calder, 2009). Este estándar internacional provee a las organizaciones de cualquier tamaño y personas una visión general de todas las familias de estándares que contempla el SGSI; una introducción al SGSI y describir los fundamentos del SGSI, que forman el asunto de los SGSI y define los términos relacionados (Espinosa Betancur, 2016).

2.2.3. Auditoría de Seguridad de Sistemas de Información

Es el análisis y gestión de sistemas para identificar y posteriormente corregir las vulnerabilidades que pudieran presentarse en una revisión exhaustiva de las estaciones de trabajo, redes de comunicaciones o servidores (Costas Santos, 2014).

2.2.4. Auditoría de Sistemas y Tecnologías de Información.

La auditoría de SI es el proceso metodológico para valorar, identificar y evaluar la confianza que se puede depositar en las TI, identificando la adecuación de controles, nivel de cumplimiento y, fundamentalmente, identificar riesgos para el negocio.

2.2.5. Sistema de Control Interno.

(Seguro Social de Salud - EsSalud: Sede Central, 2016) Se denomina al conjunto de acciones, actividades, planes, políticas, normas, registros, organización, procedimientos y métodos, incluyendo la actitud de las autoridades y el personal, organizados e instituidos en cada entidad del Estado.

Según la Ley 28716, las entidades del Estado implantan obligatoriamente sistemas de control interno en sus procesos, actividades, recursos, operaciones y actos institucionales, orientando su ejecución al cumplimiento de los objetivos siguientes:

- Promover y optimizar la eficiencia, eficacia, transparencia y economía en las operaciones de la entidad, así como la calidad de los servicios públicos que presta.
- Cuidar y resguardar los recursos y bienes del Estado contra cualquier forma de pérdida, deterioro, uso indebido y actos ilegales, así como, en general, contra todo hecho irregular o situación perjudicial que pudiera afectarlos.
- Cumplir la normatividad aplicable a la entidad y sus operaciones.
- Garantizar la confiabilidad y oportunidad de la información.
- Fomentar e impulsar la práctica de valores institucionales.

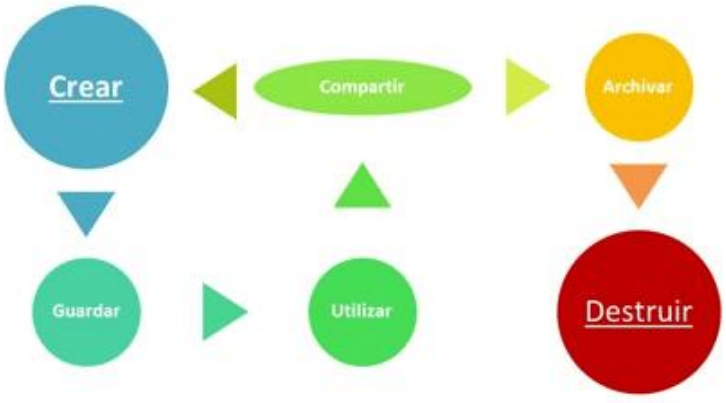
- Promover el cumplimiento de los funcionarios o servidores públicos de rendir cuenta por los fondos y bienes públicos a su cargo y/o por una misión u objetivo encargado y aceptado.

Para asegurar una correcta gestión de sus tecnologías de información y la continuidad de sus servicios EsSalud ha de implementar el Sistema de Control Interno con la finalidad de optimizar y mejorar procesos, actividades, recursos y operaciones cumpliendo normativas de estándares y normas técnicas.

2.2.6. Sistema de Gestión de la Seguridad de la Información - SGSI.

El SGSI se refiere a todo conjunto de datos organizados en poder de una entidad que poseen valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración (ISO 2700, 2012).

Ilustración 2: Proceso del SGSI



Fuente: (ISO 2700, 2012)

2.2.6.1.Confidencialidad.

La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

2.2.6.2.Integridad.

Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

2.2.6.3.Disponibilidad.

Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

2.2.7. Sistema de Gestión Hospitalaria.

(Seguro Social de Salud - EsSalud: Red Asistencial Moquegua, 2016)

El Sistema de Gestión Hospitalaria (SGH) es el principal Sistema de Información usado principalmente en los Hospitales nivel I, II y además en la mayoría de cada Red Asistencial a nivel nacional. Pese a su tiempo en funcionamiento, el sistema ha presentado mejora en diferentes funcionalidades.

Sin embargo, su principal problema es la naturaleza propia de su construcción, el cual no contempla un manejador de Base de Datos haciéndola desarticulada y difícil de explotar información. También, los mecanismos de seguridad son susceptibles de modificar, alterar o destruir información registrada. Otra debilidad importante es el mantenimiento y soporte de este sistema, que por su antigüedad y discontinuidad tecnológica la hace engorrosa y compleja.

2.3. Hipótesis.

El diseño de un Plan de Seguridad de la Información de acuerdo al estándar ISO/IEC 27001: “Seguridad de la Información" permitirá la mejora de la gestión de la seguridad de la información.

2.4. Operacionalización de variables.

Tabla 2: Operacionalización de variables.

Variables	Tipo de Variable	Definición Conceptual	Dimensiones	Indicadores	Instrumento
Gestión de la Seguridad de la Información	Dependiente	Evaluar cumplimiento de normativas Conocer la realidad situacional de las tecnologías de información. Revisar situación de equipamiento informático.	a) Confidencialidad b) Disponibilidad c) Integridad	$\text{CONF. (\%)} = \frac{\text{\# ACCESO NO AUTORIZ. (MES)}}{\text{\# ACCESO AUTORIZADO (MES)}} \text{X100}$ $\text{DISP. (\%)} = \frac{\text{\# HRS. PROM. DISP. (DÍA)}}{\text{24 HORAS (DÍA)}} \text{X100}$ $\text{INTE. (\%)} = \frac{\text{\# BACKUP A PRUEBA / CONFORMIDAD (MES)}}{\text{\# BACKUP (MES)}} \text{X100}$	Cuestionario Checklist
Norma Técnica Peruana NTP - ISO/IEC 27001	Independiente	Conjunto de estándares, políticas constituidos en objetivos y controles	Grado de cumplimiento	$\text{CUMP. (\%)} = \frac{\text{\# CUMPLIM. POLÍTICAS}}{\text{\# TOTAL DE POLÍTICAS}} \text{X100}$	Cuestionario Entrevista

3. METODOLOGÍA

3.1. Tipo y nivel de investigación.

a) Tipo de investigación.

Experimental: Se busca establecer en qué medida el diseño de un Plan de seguridad permita mejorar la gestión de cumplir las de políticas y normativas establecidas.

b) Nivel de investigación.

Descriptiva: Mediante este proyecto se propone encontrar y resolver problemas que puedan perjudicar una adecuada gestión de la seguridad de la información.

3.2. Población y muestra.

a) Población.

Total de eventos mensuales asociados al tratamiento de las tecnologías de la información y documentación.

Tabla 3: Registro de eventos de la población (año 2016).

EVENTO	**CANTIDAD**	**PORCENTAJE (%)**
Evento 1	Cantidad 1	Cantidad 1 / ∑ Cantidad
…	…	
Evento x	Cantidad x	Cantidad x / ∑ Cantidad
TOTAL	**∑ Cantidad**	

b) Muestra.

Porción probabilística de los eventos calculada mediante la fórmula siguiente:

$$n = \frac{Z_a^{\,2} \times p \times q}{d^2}$$

Ilustración 3: Cálculo de la muestra.

c) Unidad de análisis.

Eventos asociados a procesos de tratamiento de información haciendo uso de las tecnologías de información.

3.3. Técnicas e instrumentos de investigación.

Las técnicas e instrumentos para la recolección de datos fueron diseñados en concordancia al estándar a estudiar por el equipo investigador y entregadas al personal informático con la finalidad de obtener la información lo más exacta posible:

Tabla 4: Técnicas e instrumentos.

TÉCNICA	INSTRUMENTO	DEFINICIÓN
Entrevista	Guía	Se registrarán las respuestas, fundamentos y aportes del entrevistado y además las recomendaciones y observaciones encontradas por el equipo investigador.
Encuesta y observación directa	Cuestionario y Checklist	

3.4. Diseño de investigación.

3.4.1. Evaluación y control.

3.4.1.2. Evaluar ISO 27001: Seguridad de la Información

ISO 27001 es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan. Esto permite a los Sistemas Gestión de la Seguridad de la Información permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos. Se tomaron en cuenta los siguientes controles en la auditoría[1]:

6. Organización de la seguridad de la información
7. Seguridad de los recursos humanos
8. Gestión de activos
9. Control de accesos
10. Criptografía
11. Seguridad física y ambiental
12. Seguridad de las operaciones
13. Seguridad de las comunicaciones
15. Relación con los proveedores
16. Gestión de incidentes en la seguridad de la información
17. Aspectos de SI en gestión de la continuidad del negocio
18. Cumplimiento

[1] Se excluyeron los controles 5: Política de Seguridad y 14: Adquisición, desarrollo y mantenimiento del SI debido a que la Red Asistencial La Libertad no tiene jurisdicción siendo éstas únicamente establecidas por la Gerencia General.

3.4.1.2. Revisar documentación interna de EsSalud y realizar visita técnica.

Se revisará documentación sobre auditorías o estudios de seguridad de la información previos.

En este punto se comprueba el cumplimiento de controles y objetivos del estándar ISO 27001: Seguridad de la Información.

Además, se entrevistará previamente a los responsables del centro hospitalario, tanto como personal admistrativo y asistencial con la finalidad de establecer objetivos de auditoría.

3.4.1.3. Establecer objetivos del Plan

Con la información obtenida, se establecerá el alcance de la auditoría para así poder diseñar el Plan de Seguridad de la Información.

3.4.2. Análisis y elaboración del Plan.

3.4.2.1. Recopilar y evaluar resultados.

Con el registro de evidencias e información recopilada mediante técnicas (entrevista, encuesta y observación directa) e instrumentos (Guía, cuestionario y checklist), se establecerán los puntos débiles de la auditoría (confidencialidad, disponibilidad e integridad) de acuerdo a cada control.

3.4.2.2. Elaboración del Plan

Establecidas las causas y/o factores del incumplimiento de objetivos, se establecerá el Plan de Seguridad de la Información clasificados en los siguientes acápites:

1. Seguridad lógica
2. Seguridad en comunicaciones
3. Seguridad en aplicaciones

4. Seguridad física
5. Administración de la Oficina de Informática

Brindada esta información, se aportará a EsSalud a para una futura correcta elaboración de un Plan de Seguridad de Información que responda a posibles eventos no esperados.

Para la hipótesis alterna, el cumplimiento de los objetivos de la seguridad de la información debe ser mayor al cumplimiento anterior al estudio.

$$\mathbf{R_A} \rightarrow MGSI_A \rightarrow COSI_A$$

$$\mathbf{R_P} \rightarrow MGSI_B \rightarrow COSI_B$$

$$\mathbf{H_A} \rightarrow COSI_A < COSI_B$$

$$\mathbf{H_0} \rightarrow COSI_A \geq COSI_B$$

Donde:

$\mathbf{R_A}$	Realidad alterna	$\mathbf{MGSI_A}$	Modelo de Gestión de la SI "A"
$\mathbf{R_P}$	Realidad posterior	$\mathbf{MGSI_A}$	Modelo de Gestión de la SI "B"
$\mathbf{H_A}$	Hipótesis alterna	$\mathbf{COSI_A}$	Cumpl. de objetivos SI
$\mathbf{H_0}$	Hipótesis nula	$\mathbf{COSI_B}$	Cumpl. de objetivos SI

3.5. Procesamiento y análisis de datos.

Para la Verificación del Cumplimiento de Objetivos y Controles, se aplicó el cuestionario y Checklist descrito en **ANEXOS**. Dichos instrumentos se elaboraron considerando el estándar estudiado.

Las preguntas del cuestionario y Checklist fueron aplicadas a los operadores informáticos del centro hospitalario Víctor Lazarte Echegaray perteneciente a la Red Asistencial La Libertad del dicho centro hospitalario:

De acuerdo a la información proporcionada y las evidencias recopiladas, se establecen cuadros estadísticos que ayudarán a elaborar un Plan de acuerdo a las necesidades de la institución para poder salvaguardar su información y gestionar sus activos correctamente.

La escala de calificación se sustenta en la escala de Likert, habiéndose definido 5 niveles (3 aprobatorias a partir de una puntuación mayor a 53% y 2 desaprobatorias consideradas menores o iguales al 53%).

Se presenta los siguientes gráficos resumen de todo el estudio correspondiente a las técnicas e instrumentos de recolección de datos:

Tabla 5: Escala de calificación.

COLOR	DESCRIPCIÓN	CALIFICACIÓN
	Puntuación mayor a 85%	Satisfactoria
	Puntuación mayor a 65% y menor que 85%	Buena
	Puntuación mayor a 53% y menor que 65%	Aprobatoria
	Puntuación mayor a 25% y menor que 53%	Desaprobatoria
	Puntuación menor que 25%	Deficiente

4. PRESENTACIÓN DE RESULTADOS

4.1. En relación a verificar cumplimiento de controles y objetivos.

Para verificar el cumplimiento de objetivos y controles establecidos en la norma ISO 27001: Seguridad de la Información, utilizados en la gestión de la tecnología asociada a la seguridad de la información, se tomaron como referencia los siguientes objetivos del presente estándar:

6. Organización de la seguridad de la información
7. Seguridad de los recursos humanos
8. Gestión de activos
9. Control de accesos
10. Criptografía
11. Seguridad física y ambiental
12. Seguridad de las operaciones
13. Seguridad de las comunicaciones
15. Relación con los proveedores
16. Gestión de incidentes en la seguridad de la información
17. Aspectos de SI en gestión de la continuidad del negocio
18. Cumplimiento

Para evaluar el cumplimiento se aplicó la lista de verificación que se muestra en el **ANEXO N° 1,** de conformidad a los detalles especificados en dicho anexo.

Siendo en resumen los resultados los que se muestran en la **Tabla 6**:

Tabla 6: Resumen de índice de cumplimiento de objetivos.

OBJETIVO	**SI**	**NO**	**%**
ORGANIZACIÓN DE SI	6	6	**50**
SEGURIDAD DE LOS RECURSOS HUMANOS	12	6	**66.67**
GESTIÓN DE ACTIVOS	9	3	**75**
CONTROL DE ACCESOS	22	5	**81.48**
CRIPTOGRAFÍA	1	1	**50**
SEGURIDAD FÍSICA Y AMBIENTAL	69	58	**54.33**
SEGURIDAD DE LAS OPERACIONES	24	9	**72.73**
SEGURIDAD DE LAS COMUNICACIONES	6	1	**85.71**
RELACIÓN CON LOS PROVEEDORES	6	0	**100**
GESTIÓN DE INCIDENTES EN SI	9	11	**45**
ASPECTOS DE TI EN GESTIÓN DE CONTINUIDAD DEL NEGOCIO	1	13	**7.14**
CUMPLIMIENTO	3	7	**30**
TOTAL	**168**	**120**	**58.33**

Gráficamente, el resultado total se refleja en la **Ilustración 4**, siguiente:

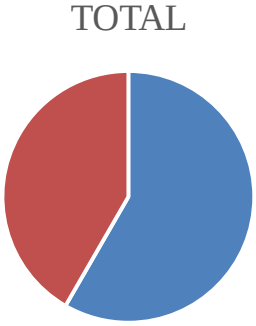


Ilustración 4: Índice global de cumplimento de objetivos.

Se cumple 168 de 288 enunciados haciendo un total de 58.33%, en función de la escala mostrada en la **Tabla 7**.

✓ **Organización de la seguridad de la información.**

Este objetivo está conformado por 12 controles y clasificado en 2:

Tabla 7: Organización de la seguridad de la información.

OBJETIVO			CUMPLIM.		
ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN			**SI**	**NO**	**TOTAL**
CONTROL	ORGANIZACIÓN INTERNA		4	6	10
	1	Roles y responsabilidades para la seguridad de la información	2	4	6
	2	Segregación de funciones	0	1	1
	3	Contacto con las autoridades	0	1	1
	4	Contacto con grupos especiales de interés	1	0	1
	5	Seguridad de la información en la gestión de proyectos	1	0	1
	DISPOSITIVOS MÓVILES Y TELETRABAJO		2	0	2
	1	Política de uso de dispositivos móviles	1	0	1
	2	Teletrabajo	1	0	1
		TOTAL	**6**	**6**	**12**

Se cumple con el 50% de los controles (6 de 12), obteniendo así una calificación **DESAPROBATORIA.**

Ilustración 5: Organización de la seguridad de la información.

- ✓ **Seguridad de los recursos humanos.**

Este objetivo está conformado por 18 controles y clasificado en 3:

Tabla 8: Seguridad de los recursos humanos.

OBJETIVO			CUMPLIM.		
SEGURIDAD DE LOS RECURSOS HUMANOS			SI	NO	TOTAL
CONTROL	ANTES DEL EMPLEO		5	4	9
	1	Selección	2	1	3
	2	Términos y condiciones de empleo	3	3	6
	DURANTE EL EMPLEO		3	1	4
	1	Responsabilidad de la gerencia	1	1	2
	2	Conciencia, educación y capacitación sobre la si	2	0	2
	TERMINACIÓN O CAMBIO DE EMPLEO		4	1	5
	1	Terminación o cambio de responsabilidades de empleo	4	1	5
		TOTAL	**12**	**6**	**18**

Se cumple con el 66.7% (12 de 18) de los controles, obteniendo así una calificación **BUENA**.

Ilustración 6: Seguridad de los recursos humanos.

- ✓ **Gestión de activos.**

Este objetivo está conformado por 12 controles y clasificado en 3:

Tabla 9: Gestión de activos.

	OBJETIVO		CUMPLIM.		
	GESTIÓN DE ACTIVOS		**SI**	**NO**	**TOTAL**
CONTROL	RESPONSABILIDAD POR LOS ACTIVOS		4	0	4
	1	Inventario de activos	1	0	1
	2	Propiedad de los activos	2	0	2
	3	Retorno de activos	1	0	1
	CLASIFICACIÓN DE LA INFORMACIÓN		3	0	3
	1	Directrices de la clasificación	1	0	1
	2	Etiquetado de la información	1	0	1
	3	Manejo de activos	1	0	1
	CLASIFICACIÓN DE LA INFORMACIÓN		2	3	5
	1	Gestión de medios extraíbles	2	0	2
	2	Disposición de medios	0	1	1
	3	Transferencia de medios físicos	0	2	2
		TOTAL	**9**	**3**	**12**

Se cumple con el 75% de los controles (9 de 12), obteniendo así una calificación **BUENA.**

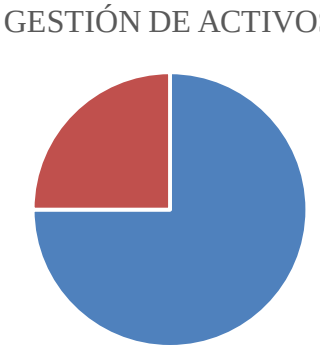


Ilustración 7: Gestión de activos.

- ✓ **Control de accesos.**

Este objetivo está conformado por 27 controles y clasificado en 4:

Tabla 10: Control de accesos.

OBJETIVO			CUMPLIM.		
CONTROL DE ACCESOS			SI	NO	TOT
CONTROL	REQUISITOS PARA EL CONTROL DE ACCESO		3	3	6
	1	Política de control de acceso	0	3	3
	2	Acceso de usuarios	3	0	3
	GESTIÓN DE USUARIOS		12	0	12
	1	Registro y baja de usuarios	2	0	2
	2	Aprovisionamiento de acceso a usuarios	6	0	6
	3	Gestión de derechos de acceso privilegiados	1	0	1
	4	Gestión de información de autenticación	1	0	1
	5	Revisión de derechos de acceso de usuarios	2	0	2
	RESPONSABILIDADES DE USUARIOS		1	0	1
	1	Uso de información de autenticación	1	0	1
	CONTROL DE ACCESO		6	2	8
	1	Restricción del acceso a la información	1	0	1
	2	Procedimientos de ingreso seguro	0	1	1
	3	Sistema de gestión de contraseñas	3	1	4
	4	Uso de programas utilitarios privilegiados	1	0	1
	5	Control de acceso: código fuente de programas	1	0	1
		TOTAL	**22**	**5**	**27**

Se cumple con el 81.48% (22 de 27) de los controles, obteniendo así una calificación **BUENA.**

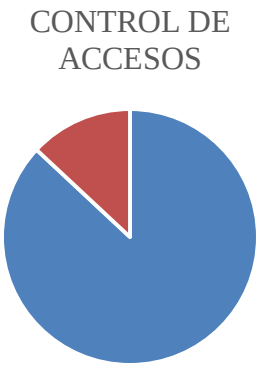


Ilustración 8: Control de accesos.

- ✓ **Criptografía**.

El objetivo está conformado por 2 controles y clasificado en 2:

Tabla 11: Criptografía

OBJETIVO			CUMPLIM.		
CRIPTOGRAFÍA			SI	NO	TOTAL
CONTROL	CONTROLES CRIPTOGRÁFICOS		1	1	2
	1	Política sobre el uso de controles criptográficos	1	0	1
	2	Gestión de claves	0	1	1
		TOTAL	**1**	**1**	**2**

Se cumple con el 50% de los controles, obteniendo así una calificación **DESAPROBATORIA.**

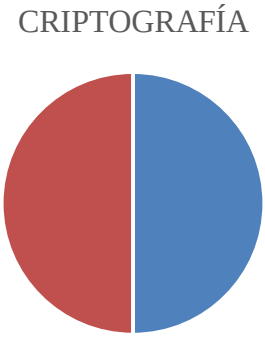


Ilustración 9: Criptografía.

- ✓ **Seguridad física y ambiental.**

El objetivo está conformado por 145 controles y clasificado en 2:

Tabla 12: Seguridad física y ambiental.

OBJETIVO			CUMPLIM.		
SEGURIDAD FÍSICA Y AMBIENTAL			SI	NO	TOTAL
CONTROL	ÁREAS SEGURAS		16	22	38
	1	Perímetro de seguridad física	0	3	3
	2	Controles de ingreso físico	1	4	5
	3	Asegurar oficinas, áreas e instalaciones	8	9	17
	4	Protección contra amenazas externas y ambientales	4	5	9
	5	Trabajo en Áreas Seguras	2	1	3
	6	Áreas de despacho y carga	1	0	1
	SEGURIDAD DE LOS EQUIPOS		62	45	107
	1	Emplazamiento y protección de equipos	19	20	39
	2	Suministro	43	25	68
		TOTAL	**78**	**67**	**145**

Se cumple con el 53.79% (78 de 145) de los controles, obteniendo así una calificación **APROBATORIA**.

Ilustración 10: Seguridad física y ambiental.

- ✓ **Seguridad de las operaciones.**

El objetivo está conformado por 33 controles y clasificado en 4:

Tabla 13: Seguridad de las operaciones.

	OBJETIVO		CUMPLIM.		
	SEGURIDAD DE LAS OPERACIONES		SI	NO	TOTAL
CONTROL	PROCEDIMIENTOS Y RESPONSABILIDADES OPERATIVAS		9	1	10
	1	Procedimientos operativos documentados	3	0	3
	2	Gestión del cambio	4	1	5
	3	Gestión de la capacidad	1	0	1
	4	Separación de los entornos de desarrollo, pruebas y operaciones	1	0	1
	PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS		4	3	7
	1	Controles contra códigos maliciosos	4	3	7
	RESPALDO		9	3	12
	1	Respaldo de la información	9	3	12
	REGISTROS Y MONITOREO		2	2	4
	1	Registro de eventos	0	1	1
	2	Protección de información de registros	1	0	1
	3	Registros de administrador y del operador	1	0	1
	4	Sincronización del reloj	0	1	1
		TOTAL	**24**	**9**	**33**

Se cumple con el 72.73% (24 de 33) de los controles, obteniendo así una calificación **BUENA.**

Ilustración 11: Seguridad de las operaciones.

- ✓ **Seguridad de las comunicaciones.**

El objetivo está conformado por 7 controles y clasificado en 2:

Tabla 14: Seguridad de las comunicaciones.

OBJETIVO			CUMPLIM.		
SEGURIDAD DE LAS COMUNICACIONES			SI	NO	TOTAL
CONTROL	GESTIÓN DE LA SEGURIDAD DE RED		3	0	3
	1	Controles de la red	1	0	1
	2	Seguridad de servicios de red	1	0	1
	3	Segregación en redes	1	0	1
	TRANSFERENCIA DE LA INFORMACIÓN		3	1	4
	1	Políticas y procedimientos de transferencia de la información	1	0	1
	2	Acuerdo sobre transferencia de información	1	0	1
	3	Mensajes electrónicos	0	1	1
	4	Acuerdos de confidencialidad o no divulgación	1	0	1
		TOTAL	**6**	**1**	**7**

Se cumple con el 85.71% (6 de 7) de los controles, obteniendo así una calificación de **SATISFACTORIA.**

Ilustración 12: Seguridad de las comunicaciones.

✓ **Relación con los proveedores.**

El objetivo está conformado por 6 controles y clasificado en 2:

Tabla 15: Relación con los proveedores.

OBJETIVO			CUMPLIM.		
RELACIÓN CON LOS PROVEEDORES			**SI**	**NO**	**TOTAL**
CONTROL	SI EN LAS ORGANIZACIONES CON LOS PROVEEDORES		4	0	4
	1	Política de SI para las relaciones con los proveedores	2	0	2
	2	Abordar la seguridad dentro de los acuerdos con los proveedores	1	0	1
	3	Cadena de suministro en TIC	1	0	1
	GESTIÓN DE ENTREGA DE SERVICIOS DEL PROVEEEDOR		2	0	2
	1	Monitoreo y revisión de servicios de los proveedores	1	0	1
	2	Gestión de cambios a los servicios de proveedores	1	0	1
		TOTAL	**6**	**0**	**6**

Se cumple con el 100% de los controles obteniendo así una calificación **SATISFACTORIA.**

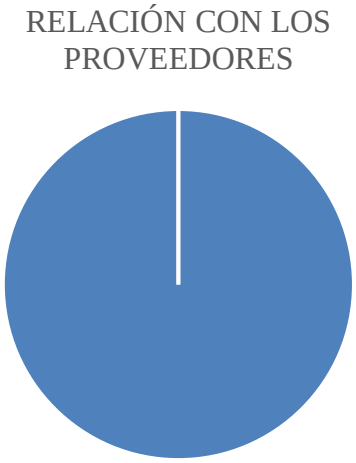


Ilustración 13: Relación con los proveedores.

- ✓ **Gestión de incidentes en la seguridad de la información.**

El objetivo está conformado por 20 controles:

Tabla 16: Gestión de incidentes en la seguridad de la información.

OBJETIVO			CUMPLIM.		
GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN			SI	NO	TOTAL
CONTROL	**GESTIÓN DE INCIDENTES DE SI Y MEJORAS**		9	11	20
	1	Responsabilidades y procedimientos	1	1	2
	2	Reporte de eventos de seguridad de la información	1	3	4
	3	Reporte de debilidades de seguridad de SI	1	1	2
	4	Evaluación y decisión sobre eventos de SI	1	1	2
	5	Respuesta a incidentes de seguridad SI	2	3	5
	6	Aprendizaje de los incidentes de SI	1	1	2
	7	Recolección (Recopilación de evidencias)	2	1	3
		TOTAL	**9**	**11**	**20**

Se cumple con el 45% (9 de 20) de los controles, obteniendo así una calificación DESAPROBATORIA.

Ilustración 14: Gestión de incidentes en la seguridad de la información.

- ✓ **Aspectos de SI en gestión de la continuidad del negocio.**

El objetivo está conformado por 14 controles y clasificado en 2:

Tabla 17:Aspectos de SI en gestión de la continuidad del negocio.

OBJETIVO			CUMPLIM.		
ASPECTOS DE SI EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO			SI	NO	TOTAL
CONTROL	CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN		1	12	13
	1	Planificación de la continuidad de SI	1	8	9
	2	Implementación de la continuidad de SI	0	2	2
	3	Verificación, revisión y evaluación de la continuidad de SI	0	2	2
	REDUNDANCIAS		0	1	1
	1	Controles contra códigos maliciosos	0	1	1
		TOTAL	**1**	**13**	**14**

Su calificación es **DEFICIENTE**: siendo 14 los controles estudiados, se cumple únicamente 1.

Ilustración 15: Aspectos de SI en gestión de la continuidad del negocio.

- ✓ **Cumplimiento**

El objetivo está conformado por 10 controles y clasificado en 2:

Tabla 18: Cumplimiento.

OBJETIVO			CUMPLIM.		
CUMPLIMIENTO			SI	NO	TOTAL
CONTROL	REQUISITOS LEGALES Y CONTRACTUALES		1	5	6
	1	Identificación de requisitos contractuales y la legislación aplicable	0	1	1
	2	Derechos de propiedad intelectual	1	1	2
	3	Protección de los registros	0	1	1
	4	Privacidad y protección de datos personales	0	1	1
	5	Regulación de controles criptográficos	0	1	1
	REVISIONES DE SI		1	3	4
	1	Revisión independiente de la SI	1	0	1
	2	Cumplimiento de políticas y normas de seguridad	0	1	1
	3	Revisión (y comprobación) de cumplimiento técnico	0	2	2
		TOTAL	**2**	**8**	**10**

Se comprobó que se cumple con el 30%, obteniendo así una calificación **DESAPROBATORIA**.

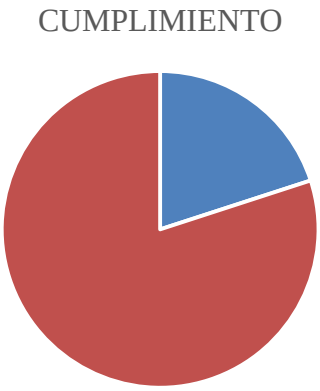


Ilustración 16: Cumplimiento.

4.1.1. Descripción del proceso de verificación de controles.

En el presente anexo se detalla lo observado de acuerdo a la estructura del Plan de Seguridad de la Información.

1. Seguridad lógica.

En este objetivo se verificó el nivel de seguridad de acceso a los sistemas de información: cómo se gestiona la integridad y confidencialidad de la información y cuentas de usuario.

1.1. Identificación de usuarios.

Se pudo comprobar que no existe un formulario establecido para el alta o baja de usuarios. Esto se justifica para estandarizar dicho proceso.

1.1.1. Alta de usuarios.

Para poder crear un usuario, el coordinador del Servicio debe enviar un correo electrónico a Informática con los datos del trabajador y el sustento para su creación: responsabilidades del trabajador y acceso a módulos.

Para registrar un usuario se ingresa la siguiente información (no se admiten caracteres especiales):

- **Código:** primera letra del nombre seguido de su apellido. Cabe recordar que el límite de caracteres para poder crear un usuario es de 8 y no se admiten caracteres especiales. En consecuencia, si el apellido excede de 7 se debe abreviar.

  Para casos de homonimia, se reservan caracteres para su diferencia a criterio del operador.
- **Contraseña:** se crea una contraseña simple, siendo esta un carácter. Luego, el trabajador debe modificarla y no exceder la cantidad de 8 para su primer uso. Cabe recalcar que el primer carácter no puede ser un número.
- **Nombre del usuario:** apellidos y nombres del trabajador. Si se supera los 22 caracteres, se debe abreviar considerando un nombre o apellido.
- **Tipo:** en este campo de carácter opcional se ingresa la colegiatura del trabajador (en caso se requiera: tales como médicos, químicos, biólogos, administradores o contadores).
- **Status:** consiste de un carácter lógico (0 o 1) el cual indica si el usuario está activo o retirado.

1.1.2. Baja de usuarios.

El operador informático está autorizado a deshabilitar la cuenta siempre y cuando el coordinador del Servicio indique su baja.

Cabe recalcar que este proceso no está automatizado, Recursos Humanos e Informática son los responsables de este proceso.

Si la persona ya no está trabajando para la institución o ha salido trasladado a otro centro asistencial, Informática debe ser informada para darlo de baja en el establecimiento.

1.1.3. Mantenimiento.

No existe una programación para el mantenimiento y control de las cuentas de usuario.

Sin embargo, el operador informático a menudo revisa la tabla para revisar usuarios inactivos, bloqueados, permisos y mantenimiento (reindexación).

1.1.4. Permisos.

En el correo electrónico, el solicitante debe especificar a los privilegios y a qué módulos el usuario puede acceder. Por cada servicio y ubicación, existe estandarización de accesos de acuerdo la responsabilidad de cada trabajador.

Incluso sea una cuenta existente, la solicitud de elevación de permisos por correo electrónico es obligatorio. Es conocido que, un usuario con privilegios menores puede acceder a ciertas secciones de módulos. Sin embargo, no puede registrar o modificar de acuerdo a restricciones.

1.1.5. Inactividad.

Aunque no exista un programa de mantenimiento y control de actividad de usuario, el operador informático revisa regularmente la tabla.

En ciertos casos, el operador debe consultar al responsable del Servicio para que la cuenta pueda ser deshabilitada.

Si la última fecha de acceso comprende mucho tiempo y la cantidad de ingresos supera el mínimo establecido el usuario es considerado como inactivo.

1.1.6. Cuentas de usuario.

Con el motivo de ahorrar recursos, cada Servicio posee una cantidad limitada de cuentas para poder acceder a los sistemas de información (no confundir con la cuenta personal).

Sin embargo, no se verifica cuántas ventanas puede tener abiertas un usuario. Esto se debe por la necesidad de los usuarios de registrar, modificar y consultar datos en simultáneo dado que la interfaz no ayuda en este aspecto.

Por cada cambio en la información, tales como registro o modificación de información, se identifica el usuario que realizó dicha actividad. Por ello, se ha concientizado a cada usuario a no divulgar su cuenta por motivos de seguridad.

1.2. Autenticación.

En la pantalla de autenticación se muestra en la parte superior el nombre, la dirección del servidor que almacena el sistema de información y la fecha. En la parte central se muestra una descripción de autenticación y una tecla de atajo para cambiar la clave (F10) y en la parte inferior salir (ESC).

Los campos de acceso son usuario y la clave: el usuario tiene tres intentos para poder acceder, si se supera dicho número la contraseña procede a ser

deshabilitada. En consecuencia, debe informarse al personal informático para su activación.

1.3. Contraseñas.

Como se ha mencionado anteriormente, no existe un proceso o estandarización para la creación de contraseñas.

1.3.1. Generación.

Para su primer uso, el operador informático debe crear una contraseña el cual puede consistir de una letra o el nombre de usuario. Luego se le notifica al usuario que debe cambiar su contraseña para poder acceder a los sistemas de información.

1.3.2. Cambios.

Cuando el usuario ingresa al formulario de autenticación, se le indica la modificación de la contraseña (F10).

Las facultades para crear este campo son muy limitadas. Esto suele generar confusión en los trabajadores debido a que desconocen dichas restricciones:

- No puede empezar con un valor numérico.
- No se aceptan caracteres especiales y de puntuación.
- La longitud no puede superar los 8 caracteres.

1.4. Segregación de funciones.

No se supervisa si existe responsabilidad total de un usuario en módulos y secciones por lo que existe un alto grado de ocurrencia de fraude y manipulación inadecuada de información.

2. Seguridad en comunicaciones.

2.1. Topología.

2.1.1. Componentes.

a) Computadoras

Se posee computadoras de diversas marcas y modelos. Equipos con sistema operativo Windows cuentan con licencia:

DELL

- 755 (LINUX – RedHat 5.1 – 5.8 y CentOS 32 y 64 bits)
- OptiPlex 9020 (Windows 8.1 Professional 64 bits)

HP

- 7600 – Torre (Windows XP Professional)
- Compaq DC7800 Ultra Slim (RedHat y CentOS 32 bits)
- Compaq DC7900 Ultra Slim (RedHat y CentOS 32 bits)
- 7900 (RedHat y CentOS 32 y 64 bits)
- 8000 (RedHat y Windows XP Professional 32 bits)

LENOVO

- ThinkCentre 9481(Windows XP Professional 32 bits)
- ThinkCentre 3Q6 (Windows 7 Professional 64 bits)

Toda computadora posee antivirus Sophos. Se cuenta con software de ofimática licenciado (Microsoft Office 2003 y 2016) y gratuito (OpenOffice).

b) Impresoras

La empresa utiliza impresoras de marca HP modelo LaserJet 2015dn, 2055 y Kyocera FS-1100, matriciales y tiqueteras que son utilizadas en todas las áreas del Hospital.

Actualmente se han instalado Lectores Biométricos Futronic FS10 en diversas áreas para verificar la identidad de asegurados, siendo instaladas en computadoras con sistema operativo Linux con distribución CentOs y Windows 7.

c) Servidores

Cable recalcar que únicamente el servidor principal y telefonía son adecuados para su uso.

- Principal: PowerEdge r710
- Administrativo: HP 8000
- Telefonía: IBM x3650
- Back-Up: HP 7600
- Correo: Dell OptiPlex 755

2.1.2. Descripción de la red.

Para acceder a la red, toda computadora necesita ser conectada directa o indirectamente: por puntos (Hub o Switch) o mediante un teléfono IP; todos estos distribuidos sin ubicación específica. Todos los terminales son conectados a un determinado switch y centralizado al administrativo para ser conectado al principal (Sala de Servidores).

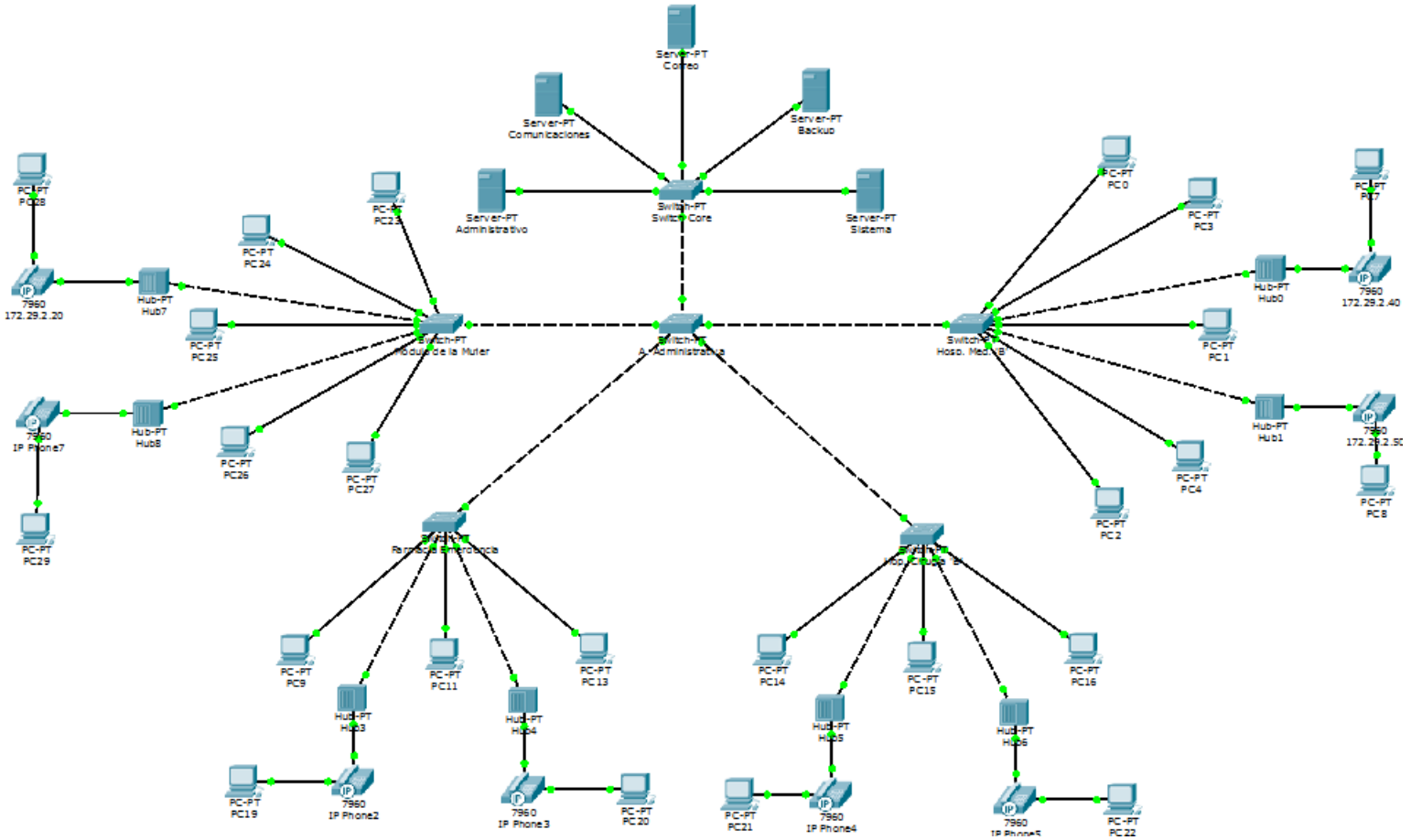


Ilustración 17: Topología de red.

2.2. Conexión a internet.

En toda la dependencia, para conectarse tanto a Intranet como Internet es necesario conectarse al Servidor Proxy (administrado por la Oficina Central de Informática), tres direcciones DNS y una Puerta de Enlace (Gateway).

El acceso a internet es de carácter exclusivo, la dirección IP se habilita de acuerdo a solicitud. Su uso es monitoreado por la Oficina Central de Informática y se habilita determinadas páginas web.

En caso se requiera, el responsable directo del Servicio debe solicitar acceso a Informática sustentando su uso.

El operador informático debe registrar la dirección IP del ordenador para luego solicitar la Oficina Central de Informática, anexando la solicitud del usuario.

La Oficina Central de Informática debe aprobar y habilitar su uso para poder tener acceso a Internet. El operador puede ahora ingresar las direcciones proxy, DNS y la Gateway.

Además de tener una dirección IP las cuales algunas tienen ingreso exclusivo a Internet, autorizada por la sede principal ubicada en Lima siguiendo los respectivos procedimientos y protocolos establecidos.

2.3. Correo electrónico.

a) Alta y baja de usuarios.

El uso de correo electrónico de carácter institucional: es usado para la comunicación entre trabajadores con la responsabilidad de informar y solicitar información.

Como se mencionó anteriormente, existe un proceso de solicitud para la creación de una cuenta de correo: el responsable del Servicio debe solicitar a Informática la creación de una cuenta justificando la necesidad de la misma.

b) Configuración.

Los servidores de correo, tanto entrante como saliente corresponden al servicio POP e IMAP ("@essalud.gob.pe").

Para el sistema operativo Windows, se usa su propio cliente de correo Outlook y Hotmail.

Mientras que, en Linux, los clientes de correo son Mozilla Thunderbird y Evolution.

Se comprobó que no existe un procedimiento de copia de seguridad establecido por la GCTC. En consecuencia, el operador hace el respaldo cuando se requiera.

Cabe recalcar que, terminada la configuración, como no se cuenta con Active Directory, el operador informático debe asegurarse que la ventana de Vista Previa del correo electrónico debe ser desactivada.

c) Redacción.

El usuario tiene todas las facultades de categorías que un cliente le puede proporcionar (Bandeja de entrada, salida, correo basura y papelera de reciclaje).

La redacción de correo incluyendo contenido multimedia no debe de superar los 4 MB de tamaño, generando en muchas ocasiones problemas al momento de remitir información.

Las firmas digitales suelen ser solicitadas por el usuario para su personalización.

2.4. Antivirus.

Toda computadora debe contar con sistema operativo Windows cuenta con software antivirus Sophos licenciado.

La GCTIC habilita el uso de internet del programa para poder conectarse al servidor para descargar e instalar actualizaciones de seguridad, siendo así una de las escasas excepciones.

Este software de seguridad tiene programado comprobar actualizaciones al iniciar el sistema operativo y horas determinadas por el desarrollador.

Se encontró que los ordenadores con las distribuciones de Linux no cuentan con software licenciado.

Se ha detectado vulnerabilidades en el software antivirus: no detecta ni elimina la mayoría de programas malintencionados autoejecutables vía unidades extraíbles y de “acceso directo”.

2.5. Firewall

a) Configuración

La GCTIC establece a través de su política qué servicios son accesibles y cuáles no.

Los puertos 22 (SSH), 23 (Telnet) y 25 (SMTP) 80 (HTTP) son permitidos para el uso interno:

- El puerto 22 (SSH) es usado para el acceso a los sistemas de información y acceso a los servidores.
- El puerto 23 (Telnet) para la comunicación remota.
- El puerto 25 (SMTP) para el uso de correo electrónico.
- El puerto 80 (HTTP) es usado para la conexión a la intranet e internet.

Se observa que se emplea el puerto 25 (SMTP), un protocolo desactualizado y no seguro para el uso de correo electrónico que no cuenta con cifrado SSL (seguridad de la capa de transporte) y requiere la autenticación del usuario para la recepción y envío de información.

2.6. Ataques.

Se comprobó que no se cuenta con medidas, técnicas ni herramientas de detección de ataques.

Las medidas de protección de datos son mínimas, la adquisición de un software antivirus y la configuración básica del firewall no es suficiente ni garantiza una total protección de la información.

3. Seguridad en aplicaciones.

3.1. Software.

La institución optó 8por adquirir 5 servidores con sistema operativo Linux por diversos motivos:

- Ahorro de costos: debido al costo por adquisición de licencia de uso se optó por usar este sistema operativo.
- Seguridad y compatibilidad: se conoce que servidores con sistema operativo Linux son menos vulnerables que los de sistema operativo Windows.
- Compatibilidad y accesibilidad: se puede ingresar desde otro sistema operativo mediante clientes (WinSCP) con la finalidad de acceder a los recursos de los servidores y realizar mantenimiento.

3.2. Seguridad de bases de datos.

Para acceder a la base de datos se usa el gestor de FoxPro, el cual comprende de tablas indexadas en formato ".dbf".

Únicamente los operadores informáticos tienen conocimiento de las credenciales de acceso a la base de datos: se puede ingresar a la base de datos mediante el mismo servidor y por el cliente WinSCP: para poder acceder se debe ingresar con la dirección IP del servidor y estar autenticado con la cuenta de administrador.

Se ha comprobado que existen registros de acceso. Sin embargo, no existe seguridad adicional para el control de carpetas y ficheros.

3.3. Control de datos.

Las políticas de la GCTI indican a informática que la instalación, modificación y ejecución de programas sea únicamente con credenciales de administrador.

El uso de recursos y programas que son autorizados únicamente con el sustento adecuado del respectivo Servicio u Hospital:

- Habilitación de unidades extraíbles
- Configuración de correo electrónico
- Acceso a internet

Se cuenta con imágenes de respaldo para cada modelo de ordenador, en caso se detecte algún problema con el sistema operativo.

El programa antivirus tiene la facultad de registrar los programas que se encuentran instalados en cada ordenador. En caso de intromisión e incumplimiento de las normativas establecidas, la GCTIC notifica al responsable informático de la Red y de la dependencia en caso de penetrar la seguridad y logra instalar programas de forma ilegal y no autorizados durante el trabajo, por ejemplo.

3.4. Ciclo de vida.

La metodología de desarrollo que se utiliza para el desarrollo de los sistemas es prototipada. Diariamente se reportan problemas y excepciones en los sistemas de información por lo que es necesario analizar nuevamente los requerimientos y realizar reingeniería de procesos.

Para la actualización del sistema, el equipo desarrollador genera un script el cual es enviado a cada operador informático y debe ser

ejecutado para su aplicación. Para ello, se necesita detener toda actividad en los servidores, esta operación comprende normalmente a 08:00 y 13:00 horas.

4. Seguridad física.

4.1. Equipamiento.

a) Servidores

Cable recalcar que únicamente el servidor principal y telefonía son adecuados para su uso. Se cuenta con un UPS para todos

- Principal: PowerEdge r710
- Administrativo: HP 8000
- Telefonía: IBM x3650
- Back-Up: HP 7600
- Correo: Dell OptiPlex 755

b) Computadoras:

DELL

- 755 (LINUX – RedHat 5.1 – 5.8 y CentOS 32 y 64 bits)
- OptiPlex 9020 (Windows 8.1 Professional 64 bits)

HP

- 7600 – Torre (Windows XP Professional)
- Compaq DC7800 Ultra Slim (RedHat y CentOS 32 bits)
- Compaq DC7900 Ultra Slim (RedHat y CentOS 32 bits)
- 7900 (RedHat y CentOS 32 y 64 bits)
- 8000 (RedHat y Windows XP Professional 32 bits)

Toda computadora con sistema operativo Windows posee antivirus Sophos. Se cuenta con software de ofimática licenciado (Microsoft Office 2003 y 2016) y gratuito (OpenOffice).

c) Impresoras

La empresa utiliza impresoras de marca HP modelo LaserJet 2015dn, 2055 y Kyocera modelo FS-1100, matriciales y tiqueteras que son utilizadas en todas las áreas del Hospital.

Actualmente se han instalado Lectores Biométricos marca Futronic FS10 en diversas áreas para la verificación de identidad de asegurados instalados en sistemas Linux con distribución CentOs y Windows 7.

4.2. Control de acceso físico a la Sala de Servidores.

En la revisión de objetivos alineados a la normativa utilizada, se ha comprobado que no existen medios para el registro de entrada y salida de personas a la Sala de Servidores y menos aún dispositivos de videovigilancia y/o personal de seguridad a los alrededores.

Se resume también que en los alrededores circula tanto personal de la institución como personas ajenas probando así una alta probabilidad de acceso de personas no autorizadas. Esto se debe a que existen servicios cercanos a esta, tales como oficinas y consultorios.

4.3. Control de acceso a equipos.

a) Unidades extraíbles.

La GCTIC establece que los mencionados puertos deben ser habilitados únicamente a determinados usuarios para su uso debidamente sustentado.

Una de las frecuentes justificaciones son las que, debido a que la información que se necesita enviar vía correo electrónico supera el tamaño máximo permitido (4 MB).

b) Gabinetes.

Se ha comprobado que no todos los gabinetes están debidamente asegurados y conservados: cables sobrexpuestos, canaletas sueltas y en mal estado de conservación.

c) Mantenimiento.

No existe un programa de mantenimiento preventivo para equipos informáticos. El mantenimiento que se realiza es de carácter correctivo y predictivo por parte del personal informático.

Con respecto a los servidores, no se posee un Plan de Contingencia en caso que el servidor principal se encuentre inoperativo, como principal observación destaca que no existe un equipo de respaldo en caso de inoperatividad.

d) Dispositivos de soporte.

- Aire acondicionado: se cuenta con un equipo que mantiene la temperatura del ambiente entre 18 a 21 grados centígrados. Este equipo tiene asignado un programa de mantenimiento preventivo por el servicio de electromecánicos.
- UPS: La Sala cuenta únicamente con un UPS para todos los servidores siendo recomendable uno para cada servidor.

No se cuenta con la mayoría de dispositivos necesarios para este ambiente: extintores, descarga a tierra, generador de energía, humificador, estabilizadores de tensión, luz de emergencia, piso aislante, sistema anti incendios y alarmas.

e) Estructura del edificio.

Se han realizado diversos estudios y revisiones de seguridad de la infraestructura resaltando las mismas observaciones.

- La Sala de Servidores se ubica en un sitio improvisado. Esto se debe a que no se había considerado en la construcción inicial del hospital (infraestructura con casi 70 años de antigüedad).
- La construcción no es de material noble: los exteriores han sido elaborados por vidrio y madera. La pared donde está ubicada el equipo de aire acondicionado es la única que se encuentra enrejada.
- El tipo de vidrio utilizado no es el adecuado debido a que se puede visualizar los interiores.

5. Administración de la Oficina de Informática.

5.1. Administración de la Oficina de Informática.

a) Responsabilidades.

El centro hospitalario cuenta con dos operadores informáticos con la finalidad de brindar soporte informático y dar mantenimiento a los sistemas de información.

No existen responsabilidades asignadas por servicio: esto quiere decir que no hay servicios asignados para cada operador por lo que puede haber colaboración mutua.

El cargo de coordinador se le asigna a un operador. Sin embargo, ambos operadores pueden realizar diversos trámites. El cargo de coordinador es considerado únicamente funcional debido a que ambos trabajadores pueden realizar diversos trámites bajo propia responsabilidad.

b) Planes.

Debido a la no elaboración de un programa de mantenimiento preventivo de equipos informáticos, el carácter es correctivo y predictivo.

Además, los sistemas de información son desarrollados y corregidos únicamente por el equipo de programadores asignados por la GCTIC.

Los operadores informáticos tienen únicamente la facultad de modificar campos de la base de datos y actualizar los sistemas de información mediante scripts, los cuales son generados por el equipo desarrollador.

c) Permisos.

Ambos encargados cuentan con los mismos privilegios para acceder a herramientas e información.

d) Mantenimiento.

- Las solicitudes de carácter predictivo y correctivo son notificadas directamente al operador informático.
- Las solicitudes para la creación de cuentas de correo, acceso a internet y sistemas de información son de carácter formal y debe ser remitido vía correo electrónico con copia a las jefaturas pertinentes.
- Para la solicitud de implementación de nuevas tecnologías de información en ambientes debe ser elaborada vía correo electrónico y por carta. De acuerdo a la prioridad y envergadura se suele incluir Hoja de Ruta para la notificación y solicitud respectiva a diversas dependencias de la Red Asistencial.
- Se gestiona un inventario de equipos informáticos el cual se registra por marca, modelo, serie, tipo de equipamiento, prioridad, ubicación y servicio.
- Para el alta de equipos, se constituye un comité de recepción de bienes el cual suele ser conformado por el coordinador del Servicio, personal administrativo, informático y de la Unidad de Control Patrimonial.
- Para poder dar de baja a un equipo, debe ser solicitado por el coordinador del Servicio y notificado a Informática.

Confirmada la solicitud, la Unidad de Control Patrimonial debe recoger el equipo y retirarlo de la dependencia. Si se solicita reposición, debe adjuntarse el requerimiento y la solicitud de la misma.

e) Interacción.

La GCTIC remite información vía correo electrónico a trabajadores de todas las redes del país información sobre el uso adecuado de los sistemas y tecnologías de información: consejos de seguridad, configuración básica y manuales de uso.

f) Instaladores.

El operador informático gestiona programas e información de dos formas:

- Compartiendo carpetas de su ordenador que contienen registros, instaladores de programas y utilitarios con la configuración de solo lectura. Estos son accesibles desde cualquier computador que esté conectado a la red.
- También se posee dispositivos físicos de almacenamiento, tales como CD y disco duro externo. Se usan estos medios en caso de formateo y/o recuperación de información en caso que el ordenador no pueda conectarse a la red.

5.2. Capacitación.

Existen sistemas de información especializados para cada servicio. En caso se implemente y configure uno nuevo, se capacita a los trabajadores y se realizan pruebas de uso para poder despejar dudas.

5.3. Copias de seguridad.

Cada servidor genera copias de seguridad a las 00:00 horas diariamente. Sin embargo, se gestionan localmente en una carpeta predeterminada por lo que se tiene que transferir a un medio externo u otro ordenador para su adecuada custodia. Para poder acceder a las copias de seguridad generadas se accede vía cliente WinSCP el cual tiene la facultad de ingresar a directorios de sistema operativo Linux.

6. Plan de contingencia.

a) Administración de incidentes.

En el transcurso del tiempo se elaboraron planes de contingencia. Sin embargo, no están enfocados en la seguridad de la información.

Dichos planes de contingencia fueron elaborados por EsSalud (anteriormente como Instituto Peruano de Seguridad Social - IPSS) en conjunto y supervisión de Defensa Civil teniendo como objetivo preservar la integridad del mobiliario y edificaciones. El responsable directo es Informática mientras que la Dirección y Administración son los encargados de responder por todo el centro hospitalario.

b) Equipamiento de respaldo.

Se ha comprobado que no existe equipamiento de respaldo en caso uno deje de funcionar por lo que existe un alto riesgo de inoperatividad de los servicios. No se emplean técnicas recomendadas por la normativa, tales como la técnica espejo (Mirroring) y la generación de copias de seguridad en unidades externas.

Cada servidor posee un disco duro los cuales están particionados en dos unidades.

c) Estrategias de recuperación de incidentes.

- Pérdida de información: por Servicio, el responsable directo es el usuario y por la Sala de Servidores y comunicaciones es el encargado de Informática.
- Pérdida de equipos: Administración debe responder inmediatamente por cada incidente encontrado y notificado a Dirección para realizar la denuncia pertinente.
- Servicios críticos: En caso de incidentes encontrados, el operador debe acudir de acuerdo a la siguiente prioridad:
    - Unidad de Cuidados Intensivos (considerado únicamente para equipos biomédicos y electromecánicos)
    - Emergencia
    - Consulta Externa
    - Cirugía
    - Hospitalización
    - Oficinas administrativas
- Dado a que no existen medidas establecidas, el operador informático debe realizar un mantenimiento predictivo para descartar problemas y/o causas. En caso requiera reparación y/o cambio de componentes, se debe verificar que el equipo se encuentre en garantía.

4.2. En relación a determinar causas de bajo rendimiento

Según los resultados obtenidos, se elaborará el plan de acuerdo a los objetivos con menor calificación.

- ✓ **Integridad.**

  Siete son los objetivos involucrados, siendo de calificación mínima "Seguridad Física y Ambiental" y desaprobatoria "Gestión de Incidentes en la Seguridad de la Información".

Tabla 19: Integridad.

OBJETIVO	SI	NO	%
GESTIÓN DE ACTIVOS	9	3	**75**
CONTROL DE ACCESOS	22	5	**81.48**
SEGURIDAD FÍSICA Y AMBIENTAL	69	58	**54.33**
SEGURIDAD DE LAS OPERACIONES	24	9	**72.73**
SEGURIDAD DE LAS COMUNICACIONES	6	1	**85.71**
RELACIÓN CON LOS PROVEEDORES	6	0	**100**
GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN	9	11	**45**
TOTAL	**145**	**87**	**62,5**

- ✓ **Disponibilidad.**

  Cuatro son los objetivos involucrados, siendo de calificación desaprobatoria "Gestión de incidentes en SI" y deficiente "Aspectos de TI en Gestión de la Continuidad del Negocio".

Tabla 20: Disponibilidad.

OBJETIVO	SI	NO	%
GESTIÓN DE ACTIVOS	9	3	**75**
SEGURIDAD DE LAS COMUNICACIONES	6	1	**85.71**
RELACIÓN CON LOS PROVEEDORES	6	0	**100**
ASPECTOS DE TI EN GEST. DE CONT. DEL NEGOCIO	1	13	**7.14**
GESTIÓN DE INCIDENTES EN SEG. INF.	9	11	**45**
TOTAL	**31**	**28**	**52.54**

- ✓ **Confidencialidad**.

Siete son los objetivos involucrados, siendo de calificación desaprobatoria "Organización de la Seguridad de la Información", "Criptografía" y "Cumplimiento".

Tabla 21: Confidencialidad.

OBJETIVO	SI	NO	%
ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	6	6	**50**
SEGURIDAD DE LOS RECURSOS HUMANOS	12	6	**66.67**
CONTROL DE ACCESOS	22	5	**81.48**
CRIPTOGRAFÍA	1	1	**50**
SEGURIDAD DE LAS OPERACIONES	24	9	**72.73**
RELACIÓN CON LOS PROVEEDORES	6	0	**100**
CUMPLIMIENTO	3	7	**30**
TOTAL	**74**	**34**	**68.52**

4.3. En relación a analizar resultados.

Los resultados de este objetivo se obtienen comparando el resultado anterior a su diseño:

Integridad

Se cumplió con 179 de 232 controles de 7 controles involucrados. Se obtuvo un porcentaje de 77,16 % obteniendo una calificación BUENA. De acuerdo a la calificación anterior al diseño del Plan (62.5%), existe una mejora de 14,66 % de cumplimiento de objetivos y controles.

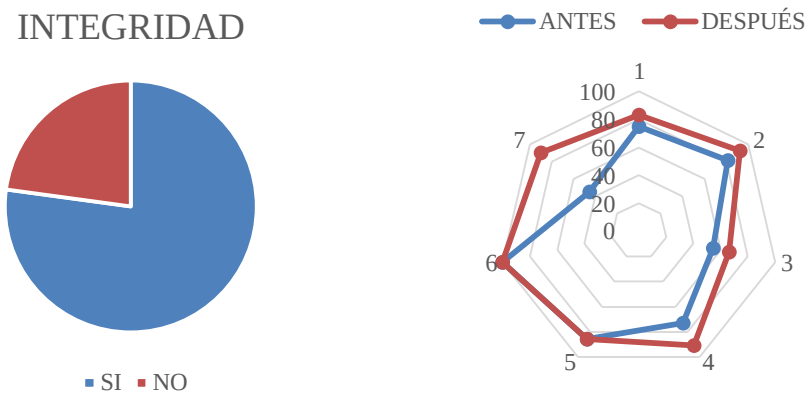


Ilustración 18: Integridad.

La integridad de la información se comprueba según el proceso de recuperación y respaldo de información mensual. Los backups son creados por el usuario o automáticamente, pero necesitan ser transferidas a una unidad de almacenamiento independiente a los gestores de información (**Ver ANEXO 3**).

Tabla 22: Integridad - mes.

MES	BACKUP		RESPALDO	INTE. (%)
	GENERADO	AUTOMÁTICO		
AGOSTO	2	31	1	96,97
SEPTIEMBRE	2	30	2	93,75
OCTUBRE	1	31	1	96,88
NOVIEMBRE	2	30	1	96,88
SUMA	7	122	5	96,12

Durante el estudio, se encontró que el punto más débil es la ubicación y conservación (integridad) de sus activos además de la poca respuesta hacia los eventos de riesgo que puedan ocurrir.

Disponibilidad

La disponibilidad del servidor de producción es afectada mensualmente una hora y treinta y cuatro minutos frecuentemente por las mañanas. Esto se debe a la alta demanda de los servicios y la consulta masiva de información (reportes), actualización de los sistemas de información y alguna actividad imprevista.

Se cumplió con 49 de 59 controles de 5 objetivos involucrados.

Se obtuvo un porcentaje de 83,05% obteniendo una calificación BUENA

De acuerdo a la calificación anterior al diseño del Plan (52.54%), existe una mejora de 30,51 % de cumplimiento de objetivos y controles.

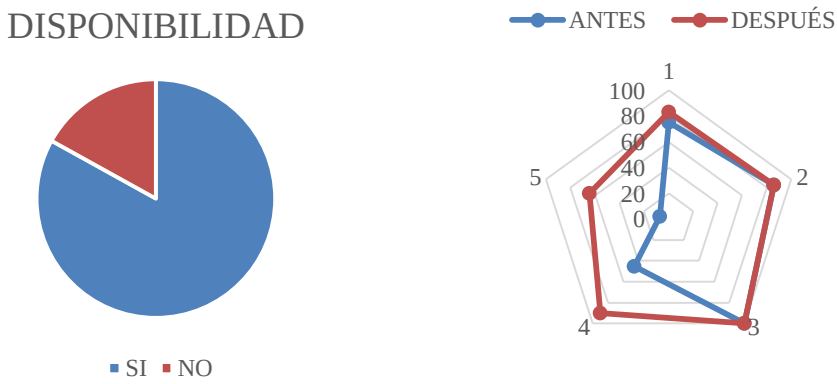


Ilustración 19: Disponibilidad.

Durante los cuatro meses de estudio, la operatividad de los servicios fue afectada mayormente en horas de la mañana durante aproximadamente 4 horas cada mes, promediando así, una disponibilidad de 99.50% considerando el reinicio de servicios (más común), actualización de sistema y mantenimiento correctivo como actividades frecuentes **(Ver ANEXO 2).**

El reinicio de servicios se debe a la distribución inadecuada y al alto consumo de recursos por parte de un terminal ya sea una solicitud de un reporte complejo o por alguna excepción en el sistema por lo que debe identificar el usuario comprometido, terminar su sesión y reiniciar los servicios para poder liberar espacio.

Tabla 23: Disponibilidad – mes.

MES	HRS. INACTIVO	HORA PROM.	DISP. (%)
AGOSTO	2:18	10:34	99,69 %
SEPTIEMBRE	5:05	12:11	99,33 %
OCTUBRE	2:30	11:00	99,66 %
NOVIEMBRE	5:54	12:23	99,21 %
PROMEDIO	**3:56**	**11:32**	**99,47 %**

Confidencialidad

Siendo 7 los objetivos involucrados, se cumplió con 93 de 108 controles. Se obtuvo un porcentaje de 86,11 % obteniendo una calificación SATISFACTORIA.

De acuerdo a la calificación anterior a la diseño del Plan (68.52%), existe una mejora de 17,59 % de cumplimiento de objetivos y controles.

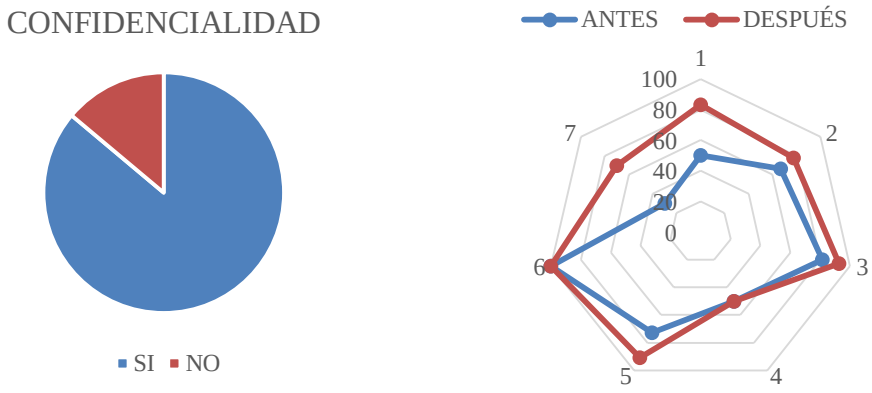


Ilustración 20: Confidencialidad.

La confidencialidad se midió calculando los ingresos autorizados y no autorizados por servicio **(ver ANEXO 2).**

El ingreso no autorizado se puede dar por ingreso incorrecto de credenciales y por exceso de límite de usuarios conectados asignados por servicio (sesión).

Tabla 24: Confidencialidad - mes.

SERVICIO	NO AUTORIZ.	AUTORIZ.	TOTAL	%
CONSULTA EXTERNA	409	4580	4989	91.03
EMERGENCIA - UCI	290	3407	3697	91.42
HOSPITALIZACIÓN	105	1502	1607	93.01
LABORATORIO	155	3977	4132	96.04
CENTRO OBSTÉTRICO	151	2599	2750	94.19
ADMISIÓN	201	8247	8448	97.53
CENTRO QUIRÚRGICO	142	2242	2384	93.50
FARMACIA	168	4151	4319	95.96
IMAGENOLOGÍA	193	2783	2976	93.02
MATERNO INFANTIL	146	2046	2192	92.84
TOTAL	**1960**	**35534**	**37494**	**93.85**

4.4. Conclusiones de la auditoría.

De acuerdo a la auditoría aplicada en la organización, se valida lo siguiente de acuerdo a los tres pilares del estándar estudiado:

a) Integridad

La institución debe fortalecer medidas de seguridad respecto a la Sala de Servidores. Esto se debe a que su ubicación y conservación es inadecuada y expuesta altamente a riesgos.

No existe un programa de mantenimiento preventivo y actividades predictivas de las tecnologías de información, debido a que es únicamente de carácter correctivo, especialmente para las comunicaciones y equipos de cómputo.

b) Disponibilidad

Siendo un centro hospitalario de alta demanda, no se posee equipamiento de respaldo (servidores y computadoras), siendo este un indicador de alto riesgo de pérdida de información en caso de inactividad de alguno de ellos.

c) Confidencialidad

El acceso y uso exclusivo de información y recursos no está comprobado ni regulado bajo procedimiento y/o registro alguno. Sin embargo, se encuentran bajo responsabilidad única del personal informático.

Además, el proceso de respaldo de información no está automatizado y no existen directivas ni políticas que verifiquen el cumplimiento de una correcta gestión de cuentas de usuario (Directorio Activo).

4.5. Plan de Mejora.

Teniendo en cuenta los resultados y hallazgos encontrados, se ha establecido el Plan de Mejora de la Seguridad de la Información para auditorías futuras:

1. Seguridad lógica
    - Diseño de un formato para solicitud de alta/baja, acceso a internet y permisos para el uso de correo y acceso a sistemas de información. Este será de carácter válido tanto en digital, como impreso (**Ver ANEXO 9**).
    - Para usuarios nuevos, se le debe remitir (adjuntar en caso de tener correo institucional) el manual de uso de los sistemas de información.
2. Seguridad en comunicaciones
    - Adquirir equipamiento nuevo (computadoras e impresoras), debido a que la mayoría de estos han superado su tiempo de vida útil y su reparación es onerosa.
    - Adquirir un servidor espejo de carácter urgente para el servidor principal.
3. Seguridad en aplicaciones
    - Bloquear puertos USB en computadoras de uso común.
    - Teniendo en cuenta que el Sistema de Gestión Hospitalaria cambiará de plataforma (web), capacitar al usuario periódicamente antes de su lanzamiento y previas actualizaciones.
    - Implementar directorio activo.
4. Seguridad física
    - Desplazamiento a un ambiente protegido y aislado de todos los servicios carácter urgente. Este debe ser construido bajo estándares de seguridad actuales y protegido. Cada ingreso debe ser registrado y monitoreado.

- Adquirir equipamiento de prevención de desastres (aire acondicionado, extintores, detector de humo y fuego) aprobado por Defensa Civil.
- Adquirir un gabinete para los servidores.
- Instalar dispositivos de seguridad en computadoras y actualizar inventario periódicamente (mensual o trimestral).
- Mejorar calidad del cableado y reemplazar si es necesario, principalmente en zonas de alto tránsito.

5. Administración de la Oficina de Informática
    - Segregación de funciones: distribuir responsabilidades prioritarias a cada operador informática de acuerdo al servicio asignado.
    - Implementar un registro de incidentes y de mantenimiento para futuros eventos imprevistos.
    - Elaborar un registro de personal responsable de servicio por equipamiento.
    - Elaborar un programa de mantenimiento de acuerdo a servicio y ubicación (preventivo, predictivo y de rutina) (**Ver ANEXO 9**).

4.5.1. Cronograma de desarrollo.

Tabla 25: Cronograma de desarrollo

ACTIVIDAD / PERIODO	2016																				2019							
	AGO				SEP				OCT				NOV				DIC				ENE				FEB			
	S 1	S 2	S 3	S 4	S 1	S 2	S 3	S 4	S 1	S 2	S 3	S 4	S 1	S 2	S 3	S 4	S 1	S 2	S 3	S 4	S 1	S 2	S 3	S 4	S 1	S 2	S 3	S 4
ACTIVIDADES INTRODUCTORIAS																												
Revisar antecedentes y terminologías																												
Entrevista con representantes																												
Establecer herramientas e instrumentos de recolección de datos																												
Establecer objetivos de auditoría																												
EVALUACIÓN Y CONTROL																												
Evaluar ISO 27001: Seguridad de la Información																												
Revisar documentación (auditorías y estudios previos)																												
Aplicar herramientas e instrumentos de recolección de datos																												
Registrar evidencias																												
Verificar cumplimiento de controles y objetivos																												
Evaluar nivel de confidencialidad, disponibilidad e integridad																												
Establecer objetivos del Plan de SI																												
ANÁLISIS Y ELABORACIÓN DEL PLAN																												
Elaboración																												
Presentación																												
Ejecución																												
Evaluar resulados																												
Elaborar Tesis																												

4.5.2. Presupuesto referencial.

El presupuesto para la ejecución del Plan consiste en adquirir nuevo equipamiento dado a su antigüedad y prioridad: servidores y comunicaciones (gabinetes, switches y cableado).

De acuerdo al monto y políticas de reglamento de adquisición de bienes[2], no se puede especificar la marca y modelo para su compra directa o por concurso público. Además del precio exacto, por lo que se considera como precio referencial.

Tabla 26: Presupuesto referencial

DESCRIPCIÓN DEL BIEN O MATERIAL	CANT. (UND, MT)	PRECIO REF.	TOTAL
SERVIDOR PRINCIPAL - ALTO RENDIMIENTO	01	S/50.000,00	S/50.000,00
SERVIDOR RAID 01 PRINCIPAL - ALTO RENDIMIENTO	01	S/50.000,00	S/50.000,00
SERVIDOR (CORREO, TELEFONÍA E HISTÓRICO)	03	S/10.000,00	S/30.000,00
CABLE UTP CAT 3	200	S/1,00	S/200,00
CABLE THW14WG (TOMACORRIENTE)	30	S/1,50	S/45,00
TERMINAL RJ-45	100	S/0,15	S/15,00
SWITCH 24 PUERTOS RACKEABLE	05	S/800,00	S/4.000,00
GABINETE SERVIDORES - TIPO PISO	01	S/2.500,00	S/2.500,00
GABINETE METÁLICO - TIPO PARED	05	S/350,00	S/1.750,00
		T O T A L	**S/138.510,00**

[2] Las adjudicaciones están contrastadas por la Ley de Contrataciones del Estado N° 30225. Este especifica que las adjudicaciones de carácter directo son efectuadas hasta las 8 Unidades Tributarias – UIT (4200 soles). De lo contrario, es obligatorio contratar bajo modalidades de contratación como licitación pública, concurso público, acuerdo marco, entre otros..

5. DISCUSIÓN

5.1. Análisis de la Hipótesis

La hipótesis de este estudio es "El diseño de un Plan de Seguridad de la Información de acuerdo al estándar ISO/IEC 27001: Seguridad de la Información permitirá la mejora de la gestión de la seguridad de la información".

La variable independiente es el Plan de Seguridad conforme al estándar ISO/IEC 27001 y la variable dependiente es la gestión de la seguridad de la información.

Tabla 27: Plan de Seguridad conforme al estándar ISO 27001.

DIMENSIONES	INDICADORES
Cumplimiento de políticas y normativas	$\text{CUMP. (\%)} = \frac{\text{\# CUMPLIM. POLÍTICAS}}{\text{\# TOTAL DE POLÍTICAS}} \text{X100}$

Tabla 28: Gestión de la seguridad de la información.

DIMENSIONES	INDICADORES
Confidencialidad	$\text{CONF. (\%)} = \frac{\text{\# ACCESO NO AUTORIZ. (MES)}}{\text{\# ACCESO AUTORIZADO (MES)}} \text{X100}$
Disponibilidad	$\text{DISP. (\%)} = \frac{\text{\# HRS. PROM. DISP. (DÍA)}}{\text{24 HORAS (DÍA)}} \text{X100}$
Integridad	$\text{INTE. (\%)} = \frac{\text{\# BACKUP A PRUEBA / CONFORMIDAD (MES)}}{\text{\# BACKUP (MES)}} \text{X100}$

De acuerdo al objetivo principal “Diseñar un Plan de Seguridad de la Información de acuerdo al estándar ISO/IEC 27001: Seguridad de la Información" se comprobó una mejora en la gestión de la seguridad de la información proporciona información para una correcta gestión de la seguridad de la información.

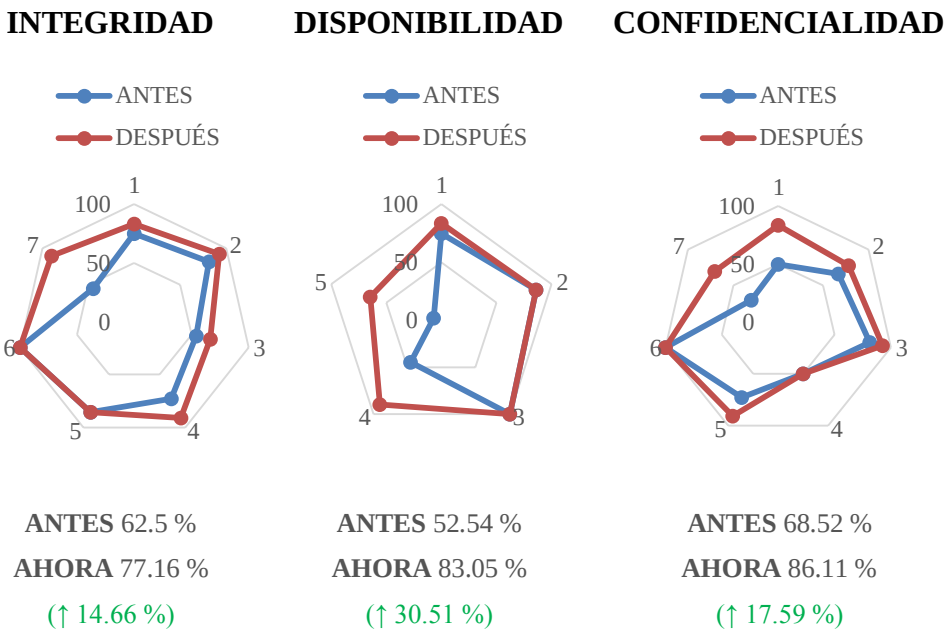


Ilustración 21: Resultados – después del diseño.

De acuerdo a los resultados obtenidos, se confirma los enunciados de Iriarte Ahón (2013), Landázuri Guevara (2015), Seclén Arana (2016) y Ramírez Martínez (2017) indicando el incumplimiento de las normativas de la seguridad de la información en entidades del estado se debe a la poca supervisión y seguimiento del cumplimiento de objetivos y controles establecidos por normativas estandarizadas.

En consecuencia, el incumplimiento de las normativas expone a un alto riesgo a sus activos informáticos afectando la integridad, disponibilidad y confidencialidad de su información.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. Respondiendo a la formulación del problema ***"¿De qué manera se puede mejorar la gestión de la seguridad de la información del Hospital Víctor Lazarte Echegaray de la Red Asistencial La Libertad - EsSalud?"***; este estudio desmostró que, aplicando del estándar ISO/IEC 27001: Seguridad de la Información se puede elaborar un Plan de Seguridad acorde a los resultados obtenidos y evidencias registradas.

2. Con la elaboración del Plan de Seguridad aportó a la mejora de la seguridad de la información proporcionando una mejora (Confidencialidad ↑17.59%, Disponibilidad ↑30.51% e Integridad ↑14.66%).

3. El presente Plan aportará a la institución perteneciente a la Red Asistencial La Libertad emitir sugerencias a la Sede Central para tomar en cuenta las actividades realizadas y considerarlas en la etapa de evaluación y evlauación del presente Sistema de Control Interno y para la planificación de futuras actualizaciones.

RECOMENDACIONES

a) Sobre la Sala de Servidores.

- Traslado de carácter urgente a otro ambiente seguro y que cumpla con los requerimientos establecidos por Defensa Civil.
- Delimitación de Sala de Servidores y alrededores. La ubicación del nuevo ambiente debe cumplir y estar alineada a certificaciones y cumplir con las evaluaciones periódicas que se requieran. Debe ser implementada con equipamiento auxiliar certificado necesario, tales como aire acondicionado, extintor, unidades UPS por cada equipo, humificador, piso aislante y línea puesta a tierra.

b) Sobre las tecnologías de información.

- Automatizar el proceso de transferencia de archivos de copias de seguridad. Como se sabe, las copias de seguridad son almacenadas en el ordenador ubicado en la Sala de Servidores.
- Adquirir unidades de almacenamiento adicional para gestionar las copias de seguridad generadas por los servidores.
- Adquirir el equipamiento indicado para los servidores de telefonía, histórico, producción y correo. Se recomienda ser configurado en arquitectura 64 bits.
- Implementar Active Directory y configurar las respectivas políticas.
- Adquirir un gabinete para una adecuada distribución y conservación de los servidores.
- Gestionar adecuadamente la distribución de recursos para cada cliente: se demostró que en ciertas ocasiones el servidor administrativo presenta sobrecarga y alto consumo de recursos debido a una excepción del programa.

c) Sobre las comunicaciones.

- Diseñar un mapa de conexiones de comunicaciones y delimitarlo por ambiente y switch para una mejor organización.
- Para las nuevas conexiones, implementar con material adecuado (cableado y canaletas).
- Canalizar puntos de conexiones y cables en los ambientes observados.
- Realizar mantenimiento preventivo y predictivo de los switches ya sea de carácter bimestral, trimestral o semestral.

d) Sobre los usuarios.

- Concientizar al usuario a no divulgar credenciales de acceso a los sistemas de información.
- Elaborar formularios para solicitudes de acceso a internet, creación de usuarios y elevación de permisos.

e) Sobre el Plan de Contingencia.

- Fortalecer medidas de comunicación entre la Gerencia Central de las Tecnologías de Información y Comunicaciones y la Oficina de Soporte Informático de la Red Asistencial La Libertad.
- De acuerdo al Plan de Mejora propuesto por este estudio, elaborar un Plan de Contingencia que cumpla con las exigencias y necesidades del centro hospitalario.
- Elaborar un Programa de Mantenimiento Preventivo a todo equipamiento informático de carácter trimestral.
- Realizar informes de la seguridad de la información con un periodo no menor a un semestre, registrando todo tipo de acontecimientos sin considerar el grado de impacto y riesgo.

REFERENCIAS BIBLIOGRÁFICAS

Alvarado, F. J. (2016). *La Gestión de la Seguridad de la Información en el Régimen Peruano de Protección de Datos Personales.* Lima. Recuperado el 14 de diciembre de 2018, de www.gobiernodigital.gob.pe/docs/Política_Nacional_de_Ciberseguridad.pdf

Amado Suárez, A. (2008). *Auditoría de Comunicación.* Buenos Aires: La Crujía.

Árnason, S., & Keith, W. (2008). *Cómo lograr la Certificación 27001: Un ejemplo de Gestión de Cumplimiento Aplicado.* Auerbach Publications. Recuperado el 2 de noviembre de 2019

Calder, A. (2009). *Impelementando Seguridad de la Información basado en ISO 27001/27001 A Management Guide.* Van Haren Publishing. Recuperado el 23 de setiembre de 2019

Contraloría General de La Repúplica. (2008). *Guía para la Implementación del Sistema del Control Interno de las Entidades del Estado.* Lima. Recuperado el 02 de noviembre de 2019

Controlaría General de la República. (2006). *Normas de Control Interno.* Lima. Recuperado el 02 de noviembre de 2019

Costas Santos, J. (2014). *Seguridad y Alta Disponibilidad.* Madrid: RA-MA.

Espinosa Betancur, J. G. (2016). *Sistema de Gestión de Seguridad de la Información para los Tres Procesos Misionales de la Corporación Autónoma Regional de Risaralda (CARDER).* Colombia. Recuperado el 20 de julio de 2019, de http://hdl.handle.net/20.500.12423/539

Gonzales Tintaya, I. A. (2017). *Diseño e Implementación de Controles de Seguridad para las Comunicaciones de Red en Un Centro de Datos de Una Entidad del Estado Basado en la NTP-ISO/IEC 27001:2014.* Lima. Recuperado el 27 de noviembre de 2018, de http://repositorio.utp.edu.pe/bitstream/UTP/914/1/Ivan%20Gonzales_Tesis_Titulo%20Profesional_2017.pdf

ISO 2700. (2012). *Sistema de Gestión de Sistemas de Información.* Recuperado el 21 de Marzo de 2018, de http://www.iso27000.es/sgsi.html

Landazuri Guevara, Y. A. (2015). *Auditoría a la Seguridad del Sistema de Información SIVIGILA de la Alcaldía de San Andrés de Tumaco Basada en el Estándar ISO 27001.* San Juan de Pasto. Recuperado el 14 de septiembre de 2018, de http://biblioteca.udenar.edu.co:8085/atenea/biblioteca/91290.pdf

Paredes Cabrera, C. A. (2016). *Mejoramiento de Calidad de Auditoría a las Tecnologías de Información y Comunicaciones.* Lima, Perú. Recuperado el 17 de septiembre de 2018, de http://cybertesis.unmsm.edu.pe/bitstream/handle/cybertesis/6045/Paredes_cc.pdf?sequence=1&isAllowed=y

Plattini Velthius, M. (2008). *Auditoría de Tecnologías y Sistemas de Información.* Madrid, España: RA-MA. Recuperado el marzo de 14 de 2019

Ramírez Martínez, O. J. (2017). *Análisis del Nivel de Cumplimiento de los Lineamientos Estratégicos de Gobierno y Gestión de Tecnologías de Información y Comunicaciones en las entidades Públicas de Manizales.* Manizales, Colombia. Recuperado el 20 de septiembre de 2018, de http://bdigital.unal.edu.co/58664/1/13871614.2017.pdf

Seclén Arana, J. A. (2016). *Factores que afectan la implementación del sistema de gestión de seguridad de la información en las entidades públicas peruanas de acuerdo a la NTP-ISO/IEC 27001.* Lima. Recuperado el 19 de octubre de 2018, de http://cybertesis.unmsm.edu.pe/bitstream/handle/cybertesis/4884/Seclen_aj.pdf?sequence=1&isAllowed=y

Seguro Social de Salud - EsSalud: Red Asistencial La Libertad. (2017). *Oficina de Seguros y Prestaciones Económicas: Acreditaciones 2012-2017.* Trujillo, La Libertad. Recuperado el 23 de diciembre de 2017

Seguro Social de Salud - EsSalud: Red Asistencial Moquegua. (2016). *Auditoría Informática EsSalud Red Asistencial Moquegua.* Moquegua, Perú. Recuperado el 18 de septiembre de 2018

Seguro Social de Salud - EsSalud: Sede Central. (2016). *Informe de Evaluación de Control Interno.* Lima. Recuperado el 16 de diciembre de 2018, de http://www.essalud.gob.pe/downloads/sist_cont_interno/inform_eval_sistem_control_int_sedecentral.pdf

Seguro Social de Salud de Salud - EsSalud. (2019). Lima. Recuperado el 15 de marzo de 2019, de www.essalud.gob.pe

ANEXOS

ANEXO 01

6.1. CUMPLIMIENTO DE OBJETIVOS Y CONTROLES

Aplicando la técnica de encuesta a los trabajadores que actúan como operadores informáticos, así como la información recopilada y proporcionada por los ingenieros supervisores (infraestructura y electromecánicos) que trabajan en la sede en la sede del Hospital Víctor Lazarte Echegaray, tal como se evidencia en los documentos adjuntos que conforman el presente anexo:

OBJETIVOS Y CONTROLES	**CUMPLE**		**OBSERVACIONES / RECOMENDACIONES**	**RESPONSABLE**
	SI	**NO**		
6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN				
6.1. Organización Interna				
Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación de seguridad de la información.				
6.1.1. Roles y responsabilidades para la seguridad de la información.				
a) El Ejecutivo de mayor nivel de la instalación tiene conocimiento y la responsabilidad máxima respecto a Seguridad de Información.		X	El director del Hospital IV Víctor Lazarte Echegaray, perteneciente a la Red Asistencial La Libertad, tiene un bajo conocimiento sobre la seguridad de las tecnologías de información. **Recomendación:**	• Gerente General de la Red Asistencial La Libertad - RALL • Director del Hospital IV Víctor Lazarte Echegaray • Administrador general • Jefe de informática

			Se le presentará un informe comprendiendo los resultados, conclusiones y recomendaciones aplicando el estándar ISO /IEC 27001 para hacer llegar el alto grado de responsabilidad que estos tienen sobre la protección y un uso adecuado de las TI.	
b) ¿Se ha conformado el Comité Técnico de Seguridad de la Información integrado por el Ejecutivo de mayor nivel quien lo preside, así como los ejecutivos de las diferentes áreas de su estructura orgánica y el Encargado de la Oficina de Soporte Informático?		X	No está conformado dicho Comité ni se tiene conocimiento sobre la misma. Sin embargo, las áreas involucradas comunican eventualmente a la Sede Central sobre la problemática mas no se realizan acciones concretas para solventarlos. **Recomendación:** Conformar el Comité Técnico de Seguridad a la brevedad posible y programar reuniones periódicas entre las áreas responsables para realizar un	• Gerente General de la Red Asistencial La Libertad – RALL • Director del Hospital IV Víctor Lazarte Echegaray • Administrador • Jefe de Informática

			Informe Técnico y remitirlo a la Sede Central.	
c) El encargado de Soporte Informático tiene como función de supervisar el cumplimiento de la presente norma y de asesorar en materia de seguridad de la información a las diferentes dependencias de la instalación que así lo requiera.	X		Los operadores de la Oficina de Soporte Informático tienen como destacadas funciones: • Copias de seguridad (usualmente una o dos veces al día: 8:00, 13:00 y 17:00 horas). • Re-indexación de data (una vez al día: 8:00 o 13:00 a 14:00 horas). • Actualización del sistema (usualmente a 8:00, 13:00 y 17:00 horas). • Soporte Informático • Informar a Alta Dirección sobre requerimientos y estado situacional de equipos tecnológicos. **Recomendación:** • Gestionar las copias de seguridad en los medios apropiados. • Verificar y hacer pruebas de respaldo por motivos de prevención.	• Jefe de Informática

d) Dentro de la organización interna de Seguridad de la Información se han identificado los roles: Custodio, Usuario o Propietario de la Información, cada trabajador con estos roles debe identificar, analizar, evaluar, tratar y monitorear el cumplimiento de la normatividad institucional en materia de seguridad de la información. **Usuarios:** Son las personas que utilizan, procesan o producen y generan información como parte de su trabajo diario. **Propietarios (Dueños):** Son los jefes de áreas que producen información y/o tienen a su cargo la actualización y explotación de la misma. **Custodios:** Los custodios de la información son aquellos que tienen la posesión física o lógica de los aplicativos y la información y se encargan de custodiarla.	X		Cada usuario tiene conocimiento del rol que deben de desempeñar en los sistemas de información. **Recomendación:** Elaborar una relación completa de usuarios que utilizan los sistemas de información por servicio incluyendo privilegios.	• Gerencia General de la Red Asistencial La Libertad – RALL • Director • Administrador • Jefe de Informática
e) El custodio vela por mantener la triple restricción de la seguridad de información como son disponibilidad, confidencialidad e integridad; el Usuario o Propietario es el responsable de autorizar los accesos a los sistemas de		X	Cada usuario tiene acceso a los sistemas de información de acuerdo al nivel de privilegio que se le solicita y otorga.	• Gerente General de la Red Asistencial La Libertad – RALL • Director • Administrador • Jefe Informática

información y sostener una trazabilidad con el uso y difusión que se le otorgue a esta información.			**Recomendación:**
			• Concientizar y sensibilizar al usuario sobre la importancia de prevalecer la confidencialidad, privacidad y protección de su cuenta para evitar algún uso malintencionado de un usuario ajeno al servicio.
			• Modificar política de inhabilitación o suspensión de usuarios
			  o Inactividad
			  o Cada servicio debe informar a Informática sobre qué usuario deja de operar para poder ser dado de baja, ya sea por término de vínculo laboral o traslado.
				• Responsable de servicio correspondiente

f) El Comité Técnico de Seguridad de la Información organizará eventos de capacitación, concientización y sensibilización a todos los trabajadores en lo referente a las disposiciones en materia de Seguridad de la Información.		X	Aunque que no exista un Comité Técnico de Seguridad de la Información, el área de Informática se encarga de orientar al nuevo usuario a usar los sistemas de información, capacitándolos periódicamente mediante material físico y digital. Además, cuando se implementa un	• Gerente General de la Red Asistencial La Libertad – RALL • Director • Administrador • Jefe de Informática

			nuevo sistema informático, se capacita a los usuarios por servicio de forma personalizada como sea solicitado. **Recomendación:** Establecer el Comité Técnico de Seguridad de la Información y programar fechas para capacitación de usuarios.	
6.1.2. Segregación de funciones.				
La responsabilidad de la información está segregada por trabajador y por área para evitar conflictos en cuanto a responsabilidades. Lo anterior permite reducir oportunidades de modificación (intencional o no) no autorizada o mal uso de los activos de la organización.		X		• Gerente General de la Red Asistencial La Libertad – RALL • Director • Jefe de Informática • Responsable de Servicio
6.1.3. Contacto con las autoridades.				
Se mantienen los contactos apropiados con las autoridades pertinentes, en caso de encontrar violación a las disposiciones de Seguridad de la Información.		X	**Recomendación:** Fortalecer comunicación entre la institución y autoridades pertinentes.	• Gerente General de la Red Asistencial La Libertad – RALL • Director • Jefe de Informática • Responsable de Servicio

6.1.4. Contacto con grupos especiales de interés.				
Se mantienen los contactos apropiados con los grupos de interés especializados y asociaciones profesionales para que puedan ser contactados de manera oportuna en el caso de que se presente un incidente de Seguridad de la Información.	X			• Gerente General de la Red Asistencial La Libertad – RALL • Adquisiciones • Logística • Jefe de Informática
6.1.5. Seguridad de la Información en la Gestión de Proyectos.				
a) En los proyectos de ampliación, remodelación, asignación de funciones, reordenamiento de personal, entre otros se tienen en cuenta los aspectos relacionados a la Seguridad de la Información.	X			• Gerente General de la Red Asistencial La Libertad – RALL • Director • Jefe de Recursos Humanos • Administrador • Jefe de Informática • Responsable de Servicio
6.2. Dispositivos móviles y teletrabajo.				
Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.				
6.2.1. Política de uso de dispositivos móviles.				
El uso de los dispositivos móviles en la institución es permitido a usuarios y están protegidos mediante el uso de políticas de seguridad y los siguientes controles	X		• Se le es otorgado al responsable de cada Servicio un dispositivo móvil con SO Android para la comunicación con diversos	• Gerente General de la Red Asistencial La Libertad – RALL • Director

tecnológicos: Antivirus, Cifrado de datos, Restricción en la ejecución de aplicaciones, Restricción de conexión de dispositivos USB.			servicios y centros hospitalarios de la Red. • Controles Tecnológicos: Se posee un software antivirus. La ejecución, escritura y modificación de programas es únicamente con privilegios de administrador, lo cual debe ser solicitado a Informática. Se restringe la conexión de dispositivos USB. Para su desbloqueo, es necesario que el responsable de Servicio solicite a Informática mediante correo electrónico las necesidades de la misma del usuario para su uso.	• Jefe de Recursos Humanos • Administrador • Jefe de Informática • Responsable de Servicio
6.2.2. Teletrabajo.				
Todo trabajador autorizado que requiera tener acceso a la información de la Institución desde redes externas, podrá acceder remotamente mediante un proceso de autenticación y uso de conexiones seguras. Deberá verificar el cumplimiento de requisitos de seguridad de los equipos desde los que se accede.	X			• Gerencial General de la Red Asistencial La Libertad – RALL • Dirección • Administración • Informática

OBJETIVOS Y CONTROLES	CUMPLE		OBSERVACIONES / RECOMENDACIONES	RESPONSABLE
	SI	NO		
7. SEGURIDAD DE LOS RECURSOS HUMANOS				
7.1. Antes del empleo				
Objetivo: Asegurar que los trabajadores y terceros conozcan sus responsabilidades y que estas son adecuadas para las funciones que realizan. Son las acciones seguidas para la contratación.				
7.1.1. Selección				
En la selección de personal son verificados los antecedentes en concordancia con las leyes, regulaciones y ética relevantes, y proporcional a los requisitos de EsSalud. Se considera la clasificación de la información a la que se tendrá acceso y los riesgos percibidos.	X		Para la inscripción de un proceso de convocatoria, los postulantes deben inscribirse adjuntando los siguientes formatos: 1. Declaración Jurada de Cumplimiento de Requisitos 2. Declaración Jurada sobre Impedimento y Nepotismo 3. Declaración Jurada de Confidencialidad e Incompatibilidad 4. Declaración Jurada para médicos que no cuentan con Título de Especialista o constancia emitida por la Universidad de haber concluido el Residentado Médico	• Gerente General de la Red Asistencial La Libertad – RALL • Jefe de Recursos Humanos • Comisión Evaluadora

			5. Declaración Jurada de no registrar antecedentes penales	
Es verificada la confiabilidad (significa verificar si el candidato ha incurrido, entre otros; en fraude, actos de corrupción, dolo o uso indebido de fondos para beneficio personal).		X	**Observación:** Durante el proceso de selección de personal, la información no es debidamente analizada. En algunos casos se llega a revelar que el antes postulante, ahora trabajador, ha mentido en alguna documentación. Por consiguiente, se debe aplicar los términos de contrato en caso de falsificación de información en la hoja de vida o uso indebido de fondos y por consiguiente separados de la institución. **Recomendación:**	• Gerente General de la Red Asistencial La Libertad – RALL • Jefe de Recursos Humanos • Comisión Evaluadora

			La Comisión Evaluadora debe analizar minuciosamente la hoja de vida de cada postulante.	
Son verificados los antecedentes penales y judiciales (para determinar si el candidato presenta antecedentes de condena penal).	X		El Formato 5: "Declaración Jurada de no registrar antecedentes penales" asegura que el postulante deba presentar esta documentación.	• Gerente General de la Red Asistencial La Libertad – RALL • Jefe de Recursos Humanos • Comisión Evaluadora
7.1.2. Términos y condiciones del empleo				
a) Se establecen las funciones y responsabilidades que competen a cada trabajador en lo referente a la Seguridad de la Información, sistemas y demás bienes de la institución.	X		En la suscripción del contrato se indica las actividades que el trabajador debe cumplir.	• Gerente General de la Red Asistencial La Libertad – RALL • Jefe de Recursos Humanos
b) Se deja en claro que dichas responsabilidades continuarán teniendo aplicación aún una vez finalizado el período de contratación tanto dentro como fuera de las instalaciones.	X		Si el empleado deja de trabajar en la institución, no debe incumplir con las restricciones que atenten la información.	• Gerente General de la Red Asistencial La Libertad – RALL • Jefe de Recursos Humanos
c) Se suscribe el Acuerdo de Confidencialidad.		X	Este Acuerdo es únicamente suscrito cuando la información y el acceso es	• Gerente General de la Red Asistencial La Libertad – RALL • Jefe de Recursos Humanos

			restringido y la información es sumamente confidencial.	• Director • Responsable de Servicio
d) Se establecen las sanciones en caso de incurrir en faltas referidas a la Seguridad de la Información.		X	Los usuarios ya sean administrativos o asistenciales que infringen las políticas de seguridad es amonestado verbalmente por su coordinador de servicio más cercano. En el mayor de los casos, por pérdida de información de gran volumen o de un determinado periodo, el personal informático involucrado es sancionado administrativamente o separado de su cargo de acuerdo a la gravedad de la pérdida.	• Gerente General de la Red Asistencial La Libertad – RALL • Director • Jefe de Recursos Humanos • Administrador • Jefe de Informática • Coordinador de Servicio
e) Se entrega el reglamento interno del trabajo al personal contratado.		X	El reglamento interno del trabajo varía de acuerdo al servicio y especialidad del trabajador. Sin embargo, no todos los servicios poseen uno. Cabe mencionar que algunos servicios poseen reglamento interno, pero	• Gerente General de la Red Asistencial La Libertad – RALL • Director • Administrador • Coordinador de Servicio

			únicamente se muestran en su respectiva jefatura.	
f) Se hace conocer al trabajador sus deberes y derechos de acuerdo a ley.	X		Al momento de suscribir el contrato de vínculo con la institución, se entrega documentación a todo empleado que se integre a la institución, detallando tanto sus deberes y derechos como las restricciones.	• Gerente General de la Red Asistencial La Libertad – RALL • Jefe de Recursos Humanos
7.2. Durante el empleo				
Objetivo: Asegurar que los trabajadores y terceros conozcan sus responsabilidades en lo referente a la Seguridad de la Información.				
7.2.1. Responsabilidad de la Gerencia				
a) La Administración pedirá a todos los trabajadores y terceros, aplicar la Seguridad de Información de acuerdo con las políticas y procedimientos establecidos todos los trabajadores y terceros tendrán acceso permanente a las políticas y disposiciones de Seguridad de la Información y se obligan a cumplirla.	X			• Gerente General de la Red Asistencial La Libertad – RALL • Director • Administrador • Jefe Informática
b) Debe verificarse mensualmente que cada trabajador o tercero está cumpliendo con las disposiciones referentes a		X	**Observación:**	• Gerente General de la Red Asistencial La Libertad – RALL • Director

disciplina en general y de seguridad de la información en particular.			Se verifica el cumplimiento. Sin embargo, no es controlado mensualmente.	• Administrador • Jefe de Informática
7.2.2. Conciencia, educación y capacitación sobre la Seguridad de la Información				
a) Ante la ocurrencia de una falta disciplinaria que atente contra la Seguridad de la Información, se deberán aplicar las sanciones que correspondan de acuerdo a los establecido en el Reglamento Interno de Trabajo de EsSalud.	X		Si el infractor es personal de la institución, este puede ser amonestado verbalmente, formalmente, sancionado o separado de acuerdo a la gravedad y recurrencia de la(s) falta(s). Si el infractor es personal externo, este puede ser amonestado formalmente, penalizado o dar por resuelto su contrato (según cláusulas) de acuerdo a la gravedad y recurrencia de la(s) falta(s).	• Gerente General de la Red Asistencial La Libertad – RALL • Jefe de Recursos Humanos
b) En casos de sustracción o sabotaje de equipamiento y documentación se procederá a la denuncia penal que corresponda de acuerdo a la legislación vigente de esta materia.	X			• Gerente General de la Red Asistencial La Libertad – RALL • Director • Administrador

7.3. Terminación o cambio de empleo.				
Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación del empleo.				
7.3.1. Terminación o cambio de responsabilidades de empleo				
a) Cualquiera sea el motivo del cese del trabajador no podrá retener, divulgar ni retirar ninguna información confidencial de la institución.	X		En el contrato firmado se adjunta el Formato 3: "Declaración Jurada de Confidencialidad e Incompatibilidad"	• Gerente General de la Red Asistencial La Libertad – RALL • Jefe de Recursos Humanos
b) El trabajador deberá devolver todos los equipos y activos que tuviera en su poder y anular toda autorización de acceso lógico y físico.	X		Cuando el trabajador termina su vínculo con la institución debe entregar todo bien con el que este se desempeñaba. Luego de su cese, Informática es responsable de dar de baja a la cuenta la cual se tenía acceso.	• Gerente General de la Red Asistencial La Libertad – RALL • Jefe de Recursos Humanos • Jefe de Informática
c) Todas las contraseñas que usaba el trabajador deben ser anuladas y su cuenta de correo electrónico deshabilitada.	X		El coordinador de servicio es el encargado de informar mediante correo electrónico a Informática el alto o baja de un usuario justificando el motivo. Todo esto bajo supervisión de la Dirección y Administración.	• Gerente General de la Red Asistencial La Libertad – RALL • Director • Administrador • Jefe de Informática • Coordinador de Servicio

d) En el caso el trabajador tenga que recuperar documentos y efectos personales, dicha tarea será realizada por otro trabajador designado por el Jefe de Área.	X		**Observación:** En ciertas ocasiones muy especiales y formalmente justificadas, el ex trabajador puede recoger dicho material, bajo supervisión de un trabajador designado por el Servicio.	• Gerente General de la Red Asistencial La Libertad – RALL • Director • Administrador • Jefe de Informática • Coordinador de Servicio
e) Todo derecho de acceso a las instalaciones de la institución queda revocada inmediatamente y las credenciales de identificación son devueltas al Personal de Administración o quien corresponda.		X	**Observación:** El antes trabajador puede tener acceso a ciertos ambientes (ya sea por confianza o desconocimiento de su cese por parte del personal). **Recomendación:** Fortalecer medidas de seguridad.	• Gerente General de la Red Asistencial La Libertad – RALL • Director • Administrador • Jefe de Recursos Humanos

OBJETIVOS Y CONTROLES	CUMPLE		OBSERVACIONES / RECOMENDACIONES	RESPONSABLE
	SI	NO		
8. GESTIÓN DE ACTIVOS				
8.1. Responsabilidad por los activos.				
Objetivo: Identificar los activos de la organización y definir las responsabilidades de protección adecuados. Todos los activos de información en EsSalud serán clasificados según el contenido, y los controles adecuados serán implementados de acuerdo a su importancia en la organización.				
8.1.1. Inventario de activos.				
Los activos relacionados con la información y las instalaciones de procesamiento de información están identificados dentro del inventario de activos de EsSalud.	X			• Gerente General de la Red Asistencial La Libertad – RALL • Director • Administrador • Oficina de Control Patrimonial
8.1.2. Propiedad de los activos.				
Los activos mantenidos en el inventario son propiedad de EsSalud.	X			• Gerente General de la Red Asistencial La Libertad – RALL • Director • Administrador • Oficina de Control Patrimonial • Coordinador de Servicio
Las normas para el uso aceptable de la información y de los activos asociados a la información y las instalaciones de procesamiento de información están identificados y se cumplen en forma obligatoria por sus responsables.	X			

8.1.4. Retorno de activos.				
Todos los trabajadores y contratistas devuelven todos los activos de la organización en su poder a la terminación de su empleo, contrato o acuerdo.	X		Se registra la entrada y salida de todos los activos pertenecientes a la institución, indicando la dependencia y centro hospitalario solicitante, el motivo de su desplazamiento y toda la información del activo.	• Gerente General de la Red Asistencial La Libertad – RALL • Director • Administrador • Oficina de Control Patrimonial • Coordinador de Servicio
8.2. Clasificación de la Información.				
Objetivo: Asegurar que la información reciba el nivel adecuado de protección en concordancia con su importancia para la organización				
8.2.1. Directrices de la clasificación.				
La información se clasifica en función de los requisitos legales, el valor, criticidad y sensibilidad a la divulgación o modificación no autorizada (información interna, pública y confidencial)	X			• Gerente General de la Red Asistencial La Libertad – RALL • Administrador • Oficina de Control Patrimonial
8.2.2. Etiquetado de la información.				
Los procedimientos para el etiquetado de la información son aplicados de acuerdo con el esquema de clasificación de la información aprobada por EsSalud, lo anterior teniendo en	X			• Gerente General de la Red Asistencial La Libertad – RALL • Administrador

cuenta las Tablas de Retención Documental aprobadas para las diferentes áreas.				• Oficina de Control Patrimonial
8.2.3. Manejo de activos.				
Se aplican procedimientos para el manejo de los activos de conformidad con el esquema de clasificación de la información aprobada por EsSalud.	X			• Gerente General de la Red Asistencial La Libertad – RALL • Administrador • Oficina de Control Patrimonial
8.3. Manejo de los medios.				
Objetivo: Prevenir la divulgación, modificación, remoción o destrucción no autorizada de información almacenada en medios. Evitar la divulgación no autorizada, modificación, eliminación o destrucción de la información almacenada en los medios de comunicación Manejo de los medios de almacenamiento.				
8.3.1. Gestión de los medios removibles.				
a) La gestión de medios extraíbles se realiza de acuerdo con el esquema de clasificación institucional.	X			
b) Los equipos de cómputo que tienen autorizado el manejo de USB y unidades reproductoras de CD/DVD, deben cumplir los siguientes requisitos: Tener habilitado el escaneo automático de virus, tener configurada en la herramienta de antivirus institucional, el bloqueo de la reproducción automática de archivos ejecutables.	X			• Gerente General de la Red Asistencial La Libertad – RALL • Jefe de Informática

8.3.2. Disposición de medios.				
La información es eliminada de los medios de comunicación de forma segura cuando ya no sea necesaria, utilizando procedimientos formales.		X	**Observación:** En ciertos casos, como por ejemplo en el cambio de computadoras, no se llega a eliminar la información que es almacenada. **Recomendación:** En caso que el bien sea dado de baja o reemplazo para ser puesto en licitación, debe formatearse o removerse la unidad de almacenamiento.	• Gerente General de la Red Asistencial La Libertad – RALL • Jefe de Informática • Oficina de Control Patrimonial
8.3.3. Transferencia de medios físicos.				
a) Los medios que contienen información están protegidos contra el acceso no autorizado, mal uso o corrupción durante el transporte.		X	**Observación:** Únicamente está protegido por autenticación. No existe otro medio de seguridad. **Recomendación:** Fortalecer medidas y técnicas de seguridad, tales como encriptación o	• Gerente General de la Red Asistencial La Libertad – RALL • Jefe de Informática • Oficina de Control Patrimonial
b) Se ha implementado la utilización de protocolos de seguridad para la encriptación de las claves más sofisticadas (Encriptación Simétrica, Asimétrica, WLAN, etc.).		X		

			bloquear su uso durante el tiempo de traslado.	
OBJETIVOS Y CONTROLES	CUMPLE		OBSERVACIONES / RECOMENDACIONES	RESPONSABLE
	SI	NO		
9 CONTROL DE ACCESOS				
9.1. Requisitos de la empresa para el Control de Acceso.				
Objetivo: Limitar el acceso a la información y las instalaciones de procesamiento de la información.				
9.1.1. Política de Control de Acceso.				
a) EsSalud garantiza entornos con controles de acceso idóneos, los cuales aseguran el perímetro, tanto en oficinas, recintos, áreas de carga y descarga, así como en entornos abiertos para evitar el acceso no autorizado a ellos Del mismo modo, controla las amenazas físicas externas y vela por proveer las condiciones medioambientales requeridas para el funcionamiento de la plataforma tecnológica y para la preservación de sus activos de información documentales.		X	**Observación:** Se exige a los proveedores en cumplir dichas exigencias. Sin embargo, no se les proporciona un ambiente adecuado. El ambiente no es el adecuado: está potencialmente al alcance de cualquier riesgo (ver anexos). El acceso a la Sala de Servidores no es únicamente del personal de Informática: en ciertos casos, personal de la empresa de servicios de vigilancia	• Gerente General de la Red Asistencial La Libertad – RALL • Director • Administrador • Jefe de Informática
b) Asimismo, exige a los proveedores de servicios de tecnología, el cumplimiento de la implantación y efectividad de mecanismos de seguridad física, controles de acceso				

físico y condiciones medioambientales con que éste debe contar.			accede para solicitar algún registro del sistema de video vigilancia y en otras ocasiones personal externo que ejecute mantenimiento de los servidores de imágenes que provee. **Recomendación:** Cambio de ambiente que cumpla con las especificaciones de seguridad adecuadas, fortalecer medidas de seguridad asignando personal de vigilancia que supervise la entrada y salida y mejorar la señalización de la misma.	
c) Los servidores responsables de las áreas seguras tienen la obligación de vigilar y garantizar que se cumplan las siguientes medidas de seguridad: Las áreas de producción se catalogan como seguras y deben permanecer cerradas y custodiadas. El acceso a áreas seguras donde se procesa o almacena información confidencial y restringida, es limitado únicamente a personas autorizadas. El acceso a áreas seguras requiere esquemas de control de acceso, como tarjetas, llaves o candados. El responsable de un área segura debe asegurar que no ingresen cámaras fotográficas, videos, teléfonos móviles con cámaras, salvo se tenga una autorización expresa del funcionario responsable del área segura. Se utilizan formatos para registrar la entrada y salida del personal. Se restringe el acceso físico a dispositivos como puntos de acceso inalámbricos, puertas de enlace a redes y terminales de red que estén ubicadas en las áreas seguras.				

9.1.2. Acceso de usuarios.				
d) Los usuarios que dispongan de acceso y servicios de la red son los que han sido específicamente autorizados para su uso.	X		El coordinador de servicio es el encargado de informar mediante correo electrónico a Informática el alto o baja, acceso a módulos y privilegios de un usuario justificando el motivo. Todo esto bajo supervisión de la Dirección y Administración.	• Gerente General de la Red Asistencial La Libertad – RALL • Director • Administrador • Jefe de Informática • Responsable de Servicio
e) Cada usuario es responsable por sus acciones mientras usa cualquier recurso de información de EsSalud. Por lo tanto, la identidad de cada usuario de los recursos de información está establecida de una manera única. Esta identidad de ninguna manera o por ninguna circunstancia podrá ser compartida. El sobrepaso a este medio será tratado como una Infracción a la Seguridad de la Información.				
f) Los niveles de acceso deben reflejar permanentemente una necesidad clara y demostrar de negocio y no deben comprometer la segregación de funciones y responsabilidades.				

9.2.1. Registro y baja de usuarios.				
a) Se lleva a cabo un proceso formal de registro y anulación de usuario para permitir la asignación de derechos de acceso.	X		El coordinador de servicio es el encargado de informar mediante correo electrónico a Informática el alto o baja, acceso a módulos y privilegios de un usuario justificando el motivo. Todo esto bajo supervisión de la Dirección y Administración.	• Gerente General de la Red Asistencial La Libertad – RALL • Director • Administrador • Jefe de Informática • Responsable de Servicio
b) La eliminación de las credenciales de usuario se realiza inmediatamente después de finalizada la relación contractual del Usuario con EsSalud.	X			
9.2.2. Aprovisionamiento de acceso a usuarios.				
a) El acceso a la información de EsSalud, es otorgado únicamente a usuarios autorizados, basados en lo que es requerido para realizar las tareas relacionadas con su responsabilidad o tipo de servicio. El acceso a los recursos de información de EsSalud, es restringido en todos los casos sin excepción, y se da específicamente a quienes lo requieran en razón de sus funciona, con los privilegios apropiados y por un tiempo limitado.	X		El acceso a la información se da únicamente a personal autorizado de acuerdo al servicio asignado según privilegios de acceso. EsSalud monitorea el uso de recursos y actividad de cada usuario que accede a los sistemas de información.	• Gerente General de la Red Asistencial La Libertad – RALL • Jefe de Informática

b) Se identifica y autentica a cualquier usuario que, de manera local o remota, requiera utilizar los Recursos de Tecnología y Operación de EsSalud, para lo que se requiere contar con sistemas de seguridad que cumplan con las siguientes características: Debe estar activo para accederá la plataforma tecnológica y de operación de EsSalud, lo que significa que cada usuario tiene que identificarse y autenticarse antes de acceder a un recurso de tecnología por medio de un usuario y una contraseña. Una vez se han identificado y autenticado, los usuarios únicamente podrán acceder a los recursos sobre los cuales están autorizados. Los eventos de ingreso y autenticación de usuarios serán registrados y monitoreados por los responsables de la información.	X		Si se observa un desnivel en el rendimiento debido a una consulta masiva o alguna excepción en el terminal del operador que implique un alto consumo, el operador informático debe cerciorarse que no se pierda el progreso de trabajo del usuario y luego terminar la conexión del terminal.	
c) Los usuarios cumplen prácticas para la selección y uso de las contraseñas.	X		**Recomendación:** Aumentar complejidad de contraseñas.	• Gerente General de la Red Asistencial La Libertad – RALL • Jefe de Informática
d) El acceso a los Activos de Información de EsSalud, debe ser controlado mediante un proceso formal de creación, modificación y eliminación del identificador de usuario.	X			• Gerente General de la Red Asistencial La Libertad – RALL • Jefe de Informática

e) Únicamente el responsable de la información (el jefe del área usuaria), puede autorizar la creación de un usuario. Ésta credencial (usuario y clave), de usuario debe ser asociado sólo a un individuo y la solicitud debe obedecer a una razón legítima de negocio.	X		Como ya se indicó anteriormente, el responsable de cada servicio es el encargado de solicitar a Informática la creación de usuarios para el uso de correo institucional y de cualquier sistema de información. Todo esto bajo la supervisión de la Administración y registrado en Dirección.	• Gerente General de la Red Asistencial La Libertad – RALL • Director • Administrador • Jefe de Informática • Responsable de Servicio
f) El uso remoto de los activos de información y la computación móvil será realizado bajo una autorización previa de los responsables de la información, junto con su respectivo manejo de riesgo aprobado por EsSalud.	X		**Recomendación:** Formalizar solicitud de acceso ya sea por correo electrónico o documentario en caso de pérdida de información o algún otro escenario no favorable.	
9.2.3. Gestión de derechos de acceso privilegiados.				
La asignación y utilización de los derechos de acceso preferente es restringida y controlada. El uso de las claves de usuarios administradoras, tales como: "root", "adm" y "system", entre otros, son controladas de acuerdo a los	X			• Gerente General de la Red Asistencial La Libertad – RALL • Jefe de Informática

establecido en los alineamientos que forman parte de esta política.				
9.2.4. Gestión de información de autenticación secreta de usuarios.				
La asignación de la información secreta de autenticación se controla a través de un proceso de gestión formal y de acuerdo a la clasificación dada a los activos (información) por parte de los responsables.	X			• Gerente General de la Red Asistencial La Libertad – RALL • Jefe de Informática
9.2.5. Revisión de derechos de acceso de usuarios.				
a) Los propietarios de activos revisan los derechos de acceso de los usuarios a intervalos regulares. Cualquier desviación será tratada como un Incidente en Seguridad de la Información.	X		**Recomendación:** Revisar con más frecuencia debido a que su revisión es semestral, anual o en casos eventuales que comprendan la pérdida de información.	• Gerente General de la Red Asistencial La Libertad – RALL • Director • Administrador • Jefe de Informática • Responsable de Servicio

b) Los responsables de acceso de todos los trabajadores y/o contratistas de la información e instalaciones de informática serán retirados en el momento de retiro de su empleo y/o terminación de contrato.	X			• Gerente General de la Red Asistencial La Libertad – RALL • Director • Administrador • Jefe de Informática
9.3. Responsabilidades de los usuarios.				
Objetivo. Hacer que los usuarios respondan por la salvaguarda de su información de autenticación.				
9.3.1. Uso de información de autentificación confidencial.				
Se exige a los usuarios que sigan prácticas de la organización en el uso de información confidencial de autenticación.	X		**Recomendación:** Concientizar al usuario sobre la confidencialidad de su cuenta.	• Gerente General de la Red Asistencial La Libertad – RALL • Director • Administrador • Jefe de Informática
9.4. Control de acceso a sistema y aplicación.				
Objetivo: Prevenir el acceso no autorizado a los sistemas y aplicaciones.				
9.4.1. Restricción del acceso a la información.				
El acceso a la información está restringido de conformidad con la Política de Control de Acceso.	X			• Gerente General de la Red Asistencial La Libertad – RALL • Director • Administrador • Jefe de Informática

9.4.2. Procedimientos de ingreso seguro.				
El acceso a los servicios de información sólo es posible a través de un proceso de conexión seguro.		X		• Gerente General de la Red Asistencial La Libertad – RALL • Jefe de Informática
9.4.3. Sistema de gestión de contraseñas.				
a) Junto con el nombre de usuario el funcionario recibe una contraseña o clave para acceder a los recursos informáticos EsSalud, la cual es de cambio obligatorio en el primer uso garantizando así su responsabilidad y único conocimiento sobre la misma. Dicha contraseña debe tener una longitud mínima de 8(ocho) caracteres alfanuméricos, diferentes a nombres propios o cualquier otra palabra de fácil identificación		X	**Observación:** El coordinador y/o responsable del servicio solicitante le informa a Informática vía correo institucional sobre la creación del usuario justificando el motivo. Luego se le informa del cambio de carácter obligatorio de su contraseña después de su primer uso. Sin embargo, no cumple con los estándares establecidos por este acápite debido a que no se analiza la complejidad de esta.	• Gerente General de la Red Asistencial La Libertad – RALL • Director • Administrador • Jefe de Informática • Responsable de Servicio • Usuario

b) Por seguridad se cambian dichas claves con una periodicidad máxima de 90 (noventa) días.	X		Si el usuario se encuentra inactivo por un determinado tiempo, la cuenta procede a ser bloqueada.	• Gerente General de la Red Asistencial La Libertad – RALL • Jefe de Informática
c) Después de 3(tres) intentos no exitosos de digitar la contraseña el usuario es bloqueado de manera inmediata y deberá solicitar el desbloqueo a la Oficina de Soporte Informático.	X		La cuenta es bloqueada luego de 3 intentos fallidos. Después de ello, el usuario debe informar al Servicio e Informático indicando el motivo. El usuario debe presentarse a Informática para activación de su cuenta y la asignación de una nueva.	• Gerente General de la Red Asistencial La Libertad – RALL • Jefe de Informática • Responsable de Servicio • Usuario
d) Está prohibido el uso de contraseñas compartidas. La contraseña es personal e intransferible. Las contraseñas nunca serán modificadas telefónicamente.	X		**Recomendación:** Concientizar al usuario indicando que el proceso es únicamente personal y directo.	• Gerente General de la Red Asistencial La Libertad – RALL • Director • Administrador • Jefe de Informática • Responsable de Servicio • Usuario

9.4.4. Uso de programas utilitarios privilegiados.				
El uso de programas de utilidad que podrían ser capaces de anular el sistema y de aplicaciones con controles principales está restringido y estrechamente controlado.	X			• Gerente General de la Red Asistencial La Libertad – RALL • Director • Administrador • Jefe de Informática
9.4.5. Control de acceso al código fuente de los programas.				
El acceso al código fuente del programa es limitado. Solamente los ingenieros del equipo de soporte podrán contar con acceso a esta información y harán uso de la misma. Se monitorean los registros de Log In.	X			• Gerente General de la Red Asistencial La Libertad – RALL • Director • Administrador • Jefe de Informática

OBJETIVOS Y CONTROLES	CUMPLE		OBSERVACIONES / RECOMENDACIONES	RESPONSABLE
	SI	NO		
10. CRIPTOGRAFÍA				
10.1. Controles criptográficos.				
Objetivo: Asegurar el uso adecuado y efectivo de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información.				
10.1.1. Política sobre el uso de controles criptográficos				
Se utilizan controles criptográficos en los siguientes casos: Para la protección de claves de acceso a sistemas, datos y servicios. Para la transmisión de información clasificada, fuera del ámbito de la instalación, cuando así surja de la evaluación de riesgos realizada por el Propietario de la Información y el Responsable de Seguridad Informática.	X		**Recomendación:** Fortalecer complejidad de protección de contraseñas	• Gerente General de la Red Asistencial La Libertad – RALL • Jefe de Informática
10.1.1. Gestión de claves				
La política sobre uso, protección y duración de las claves criptográficas se realiza a través del directorio activo durante todo su ciclo de vida.		X	**Observación:** La Red Asistencial no posee Active Director.	• Gerente General de la Red Asistencial La Libertad – RALL • Jefe de Informática

OBJETIVOS Y CONTROLES	CUMPLE		OBSERVACIONES / RECOMENDACIONES	RESPONSABLE
	SI	NO		
11. SEGURIDAD FÍSICA Y AMBIENTAL				
11.1. Áreas Seguras				
Objetivo: Impedir el acceso físico no autorizado, daños e interferencia a la información y a las instalaciones de procesamiento de información de la Institución.				
11.1.1. Perímetro de seguridad física.				
a) El Área Segura es un ambiente completamente cerrado y restringido su acceso sólo al personal autorizado Está ubicado en un ambiente independiente, no accesible ni visible por personal ajeno a EsSalud. Indicar el lugar de ubicación.		X	**Observación:** Aunque únicamente ingresa personal informático (también personal interno y externo previa autorización y/o solicitud), no existe una supervisión o registro de entrada y salida a la Sala de Servidores.	• Gerente General de la Red Asistencial La Libertad – RALL • Ingeniería Hospitalaria • Director • Administrador • Jefe de Informática
b) Los vidrios del perímetro de las Áreas Seguras serán de vidrio templado, o de vidrio primario con la aplicación de lámina de seguridad de 4 micras de espesor como mínimo.		X		

c) Toda Área Segura cuenta con Rótulo de identificación, así como un Rótulo de Limitación de Ingreso.		X	Ambiente no cumple con la ubicación ni protección de instalaciones de procesamiento de información. **Recomendación:** Solicitar traslado de ambiente haciendo un estudio de riesgos (adjuntando especificaciones técnicas, plano de ubicación, etc.)	
11.1.2. Controles de ingreso físico.				
a) Las Áreas Seguras se protegen mediante controles de entrada adecuados para garantizar que se le permita el acceso únicamente al personal autorizado. Sólo podrán ingresar a las Áreas Seguras los trabajadores que laboran en dichas áreas, haciendo uso visible de su documento de identificación institucional (Fotocheck) y con la autorización respectiva.		X	**Recomendación:** Registrar entrada y salida de personas a la Sala de Servidores tanto como personal interno y externo. Solicitar Fotocheck al momento de la entrada y justificar su ingreso (en caso fuera externo, estar acompañado con personal interno).	• Gerente General de la Red Asistencial La Libertad – RALL • Ingeniería Hospitalaria • Director • Administrador • Jefe de Informática

b) El personal de EsSalud y personal de servicios de terceros que ingrese a áreas seguras hace un uso de un Formato de Ingreso / Salida contando con la autorización del responsable del Área Segura.		X	**Observación:** No se solicita documento alguno para entrar a cualquier Zona Segura. Esto se da únicamente cuando la empresa prestadora de servicios solicita a un personal ser trasladado a otro Centro Hospitalario con motivos de apoyo, suplencia o recojo/entrega de material. En caso sea trabajador de la institución, se requiere presentarse con Fotocheck en caso el personal de seguridad lo solicite.	• Gerente General de la Red Asistencial La Libertad – RALL • Ingeniería Hospitalaria • Director • Administrador
c) El Personal de Seguridad exige la identificación de todo visitante mediante un documento oficial (DNI) y la autorización respectiva antes de ingresar al Área Segura.		X		• Gerente General de la Red Asistencial La Libertad – RALL • Ingeniería Hospitalaria • Director • Administrador

d) Es revisado todo maletín y bolsa de mano de las personas que se retiran de la edificación.	X		**Observación:** Se solicita maletín y bolsa de mano a personal interno y externo únicamente cuando sale e ingresa al Centro Hospitalario. **Recomendación:** Con el transcurso del tiempo. Se ha descubierto robos en componentes de equipos tanto biomédicos como de cómputo (tarjetas, procesadores, unidades de almacenamiento, etc.) Se recomienda a la empresa de seguridad (bajo supervisión de la Unidad de Ingeniería) usar detectores electrónicos.	• Gerente General de la Red Asistencial La Libertad – RALL • Ingeniería Hospitalaria • Director • Administrador
e) Se tiene un registro de las personas que han ingresado al Área Segura.		X	**Recomendación:** El personal de seguridad (bajo supervisión de la Unidad de Ingeniería) debe registrar el ingreso y salida de todo tipo de personal.	• Gerente General de la Red Asistencial La Libertad – RALL • Ingeniería Hospitalaria • Director • Administrador

11.1.3. Asegurar oficinas, áreas e instalaciones.				
11.1.3.1. Prevención y control de incendios.				
a) Cuenta con extintores adecuados (mayormente CO2 Y H2O Desmineralizada), a una distancia no menor de 22 metros entre ellos, y con un extintor por cada 50m2 de área. No son recomendables los extintores PQS por afectar a los equipos informáticos y de laboratorio.		X	**Observación:** Existe una demarcación para extintores. Sin embargo, la Sala de Servidores no cuenta con alguno.	• Gerente General de la Red Asistencial La Libertad – RALL • Ingeniería Hospitalaria • Director • Administrador • Jefe de Informática
b) Están llenadas las Tarjetas de Control de Extintores y se verifica su recarga anual.	X		Se cuenta con Tarjetas de Control con las respectivas fechas de mantenimiento registradas.	• Gerente General de la Red Asistencial La Libertad – RALL • Ingeniería Hospitalaria • Director • Administrador • Jefe de Informática
c) Los extintores deben contar con el Certificado de Operatividad y Prueba Hidrostática otorgado por el proveedor del servicio, cuya vigencia es de un año.		X	**Recomendación:** Se debe contar con Certificado de Operatividad el cual debe ser adquirido por la empresa proveedora.	• Gerente General de la Red Asistencial La Libertad – RALL • Ingeniería Hospitalaria • Director • Administrador • Jefe de Informática

d) El personal está capacitado para la operación de extintores.		X	**Recomendación:** Capacitar periódicamente al personal para su correcto uso	• Gerente General de la Red Asistencial La Libertad – RALL • Ingeniería Hospitalaria • Director • Administrador
11.1.3.2. Control de aniegos.				
a) Se mantienen en buenas condiciones las griferías y tuberías.	X			• Gerente General de la Red Asistencial La Libertad – RALL • Ingeniería Hospitalaria • Administrador
b) Los equipos están instalados a una altura no menor de 20 centímetros sobre el nivel del piso. De ser necesario se les colocará sobre plataformas.		X	**Observación:** Se aprecian UPS en el piso puestos en forma de torre. **Recomendación:** Colocar todo equipo en sobre plataformas.	• Gerente General de la Red Asistencial La Libertad – RALL • Ingeniería Hospitalaria • Director • Administrador • Jefe de Informática
c) Ante la ocurrencia de un aniego es cortado el fluido eléctrico.	X			• Gerente General de la Red Asistencial La Libertad – RALL • Ingeniería Hospitalaria

11.1.3.3. Respuesta ante apagones.				
a) La edificación donde se ubican las Áreas Seguras cuentan con luces de emergencia.		X		• Gerente General de la Red Asistencial La Libertad – RALL • Ingeniería Hospitalaria
b) Las Áreas Seguras cuentan con equipos UPS y la edificación con Grupo Electrógeno.		X	Se cuenta con un Grupo Electrónico para todo el Hospital, mas no para uso exclusivo para la Sala de Servidores	• Gerente General de la Red Asistencial La Libertad – RALL • Ingeniería Hospitalaria
c) El Personal de Seguridad ocupa sus puestos de vigilancia, alertándose sobre la situación reinante, a fin de extremar las medidas de seguridad.	X		**Recomendación:** Reforzar medidas de seguridad, registrando la entrada y salida del perímetro, ya sea personal interno, externo o pacientes.	• Gerente General de la Red Asistencial La Libertad – RALL • Ingeniería Hospitalaria
11.1.3.4. De la ubicación y ambientes de las Áreas Seguras.				
a) Las Áreas Seguras se ubican en el interior de las instalaciones, en lugares que minimizan la posibilidad de que sean afectadas por disturbios, explosiones y todo tipo de agresión contra el local institucional. No se ubican en un lugar expuesto a peligros por sismos, contaminación, incendio,		X	**Observación:** El centro hospitalario tiene cerca de 68 años de antigüedad. Debido a ello se ha ido expandiendo según las necesidades y exigencias sin tener en cuenta las áreas y zonas seguras	• Gerente General de la Red Asistencial La Libertad – RALL • Ingeniería Hospitalaria

inundación, disturbios sociales y todos los que lo pongan en riesgo.			El Hospital se encuentra expuesto a posibles desastres.	
b) Las Áreas Seguras no se ubican en lugares expuestos a presencia de polvo. Tampoco deben ubicarse cerca de instalaciones de agua y desagüe.	X			
c) Las Áreas Seguras se ubican fuera de zonas del tránsito regular del personal en general.		X	**Recomendación:** Se debe trasladar el ambiente a una zona segura y que cumpla con las especificaciones de seguridad.	
d) En las edificaciones en donde se ubican las Áreas Seguras, las zonas que no estén encementadas, deben ser cubiertas con jardines a fin de reducir la producción de polvo.	X			
e) El ambiente de toda Área Segura no es compartido con ninguna área ajena a sus labores.		X		• Gerente General de la Red Asistencial La Libertad – RALL • Ingeniería Hospitalaria • Director • Administrador
f) No existe hacinamiento en las Áreas Seguras.	X			

g) Las tomas de aire de los equipos están ubicadas de forma que no sean susceptibles de ser obstruidas.	X			
11.1.4. Protección contra amenazas externas y ambientales.				
a) La edificación donde se ubican las Áreas Seguras cuenta con la Certificación de Seguridad en Defensa Civil otorgada por la autoridad competente, de acuerdo a legislación vigente al respecto.		X	**Observación:** No se cuenta con la certificación, se desconoce si se tuvo anteriormente. **Recomendación:** Solicitar y obtener las respectivas certificaciones.	• Gerente General de la Red Asistencial La Libertad – RALL • Ingeniería Hospitalaria • Director
b) Cuentan con brigadas de evacuación, lucha contra incendio y primeros auxilios recomendadas por las normas de Defensa Civil, y han sido capacitadas.	X		**Observación:** Existe documentación que describe la estructura de las brigadas.	
c) Cuentan con el Plan de Seguridad incluyendo el Análisis de Riesgos respectivo, así como el Plan de Evacuación, Funciones de las Brigadas, Procedimientos de respuesta en caso de accidente, sismo, incendio, apagones y aniegos, de acuerdo con la estructura y distribución de las áreas del inmueble.		X	**Recomendación:** Elaborar Plan de Seguridad	
d) Cuentan con la señalética necesaria (Zonas Seguras, Riesgo Eléctrico, Señales Direccionales de Evacuación, Ubicación de Extintores y Salida de Emergencia).		X	**Observación:**	

			Se puede apreciar señalizaciones en ciertas partes del hospital mas no en su totalidad.	
e) Cuentan con Salida de Emergencia señalizada.	X			
f) Tienen Plan de Evacuación comprobado mediante simulacros.		X		• Gerente General de la Red Asistencial La Libertad – RALL • Ingeniería Hospitalaria • Director
g) Las puertas y ventanas permanecen cerradas cuando no se ejecutan operaciones.	X			
h) Todas las condiciones de riesgo han sido identificadas y se han implementado las medidas de control o mitigación.		X	**Observación:** No se cuenta con un Plan de Prevención.	
i) Cuentan con iluminación adecuada.	X		**Recomendación:** Supervisar con más frecuencia las iluminaciones.	
11.1.5. Trabajo en Áreas Seguras (La Jefatura encargada del Área Segura verifica que:)				
a) No se permita el uso de equipos de fotografía, video, audio y otras formas de registro a realizarse por terceros (salvo autorización superior expresa).	X		**Observación:**	• Gerente General de la Red Asistencial La Libertad – RALL • Ingeniería Hospitalaria

b) Los recursos de tratamiento de información de la información de la institución se encuentran separados de los recursos de terceros.		X	Cualquier uso de dispositivos tecnológicos es supervisado por un personal de EsSalud.	• Director • Administrador • Jefe de Informática
c) Las labores realizadas por terceros son supervisadas por personal de EsSalud.	X		En la Sala de Servidores se encuentra el servidor que administra el sistema de video de la empresa de vigilancia. También, por mencionar, el servidor de diagnóstico por imágenes administrado (por motivos de soporte) y proveído de la misma forma por una empresa tercera se encuentra en esta Zona. **Recomendación:** Trasladar a una zona independiente la Sala de Servidores los equipos informáticos pertenecientes únicamente a la Institución.	

11.1.6. Áreas de despacho y carga.				
Los puntos de acceso, tales como la entrega y las zonas de carga y otros puntos en los que las personas no autorizadas puedan entrar, se deberán controlar y, si es posible, deberán estar aisladas del procesamiento de la información en las instalaciones.	X			• Gerente General de la Red Asistencial La Libertad – RALL • Ingeniería Hospitalaria • Director • Administrador • Jefe de Informática
11.2. EQUIPOS (SEGURIDAD DE LOS EQUIPOS)				
Objetivo Prevenir la pérdida, daño, robo o compromiso de activos e interrupción de las operaciones de la organización.				
11.2.1. Emplazamiento y protección de equipos.				
11.2.1.1. Del Emplazamiento (Instalación)				
a) No están expuestos a polvo.		X	**Observación:** La limpieza del área está programada de lunes a viernes a las 14:00 horas (supervisada por la Unidad de Ingeniería). No se programa los días sábados y domingos (a excepciones) debido a que debe haber personal presente a la hora de la limpieza.	• Gerente General de la Red Asistencial La Libertad – RALL • Ingeniería Hospitalaria • Administrador • Jefe de Informático

			Sin embargo, por motivos de falta de energía o aire acondicionado se debe abrir una ventana o puerta (siempre con presencial de personal informático) ya que en época de verano el ambiente puede llegar a 25 a 30º C.	
b) Están lejos de instalaciones de agua y desagüe.		X	**Observación:** Se encuentran servicios higiénicos a menos de 10 metros de distancia.	
c) Están afuera del alcance del público en general.		X	**Observación:** Los consultorios externos (20 metros), Archivo y las oficinas de Programación, Referencias y Contrarreferencias (5 a 10 metros) se encuentran a una distancia muy corta de la Sala de Servidores. Las oficinas antes mencionadas son concurridas frecuentemente por el público por diversos problemas	• Gerente General de la Red Asistencial La Libertad – RALL • Ingeniería Hospitalaria • Director • Administrador • Jefe de Informática

			(aseguramiento, programación, referencias y contra referencia de citas, solicitud de adicionales y algún reclamo). **Recomendación:** Solicitar cambio de ambiente.
d) Están ubicados en mobiliarios que los protejan de golpes o acciones indebidas.		X	**Observación:** Los equipos informáticos no se encuentran correctamente ubicados en mobiliarios que protejan su integridad física. Además, se verificó que existe cableado que no se encuentran debidamente instalados y cubiertos.
e) No existen instalaciones provisionales o con sobrecarga de conexiones eléctricas.	X		
f) Cuentan con un Plan de Evacuación del Hardware que permita reubicarlo en otro edificio o área en un mínimo de tiempo.		X	

g) Los equipos informáticos deben estar situados y protegidos para reducir los riesgos de las amenazas ambientales y los riesgos y las oportunidades de acceso no autorizado.		X		
11.2.1.2. De la protección de equipos (Todo trabajador:)				
a) Apaga su equipo de inmediato al presentarse una situación de emergencia.	X		**Observación:** Todo personal que trabaja en Informática es consciente de los riesgos y conoce las medidas de seguridad. El operador informático en ocasiones deja el computador encendido por motivos de realización de respaldo de información o alguna operación que tome un tiempo considerable fuera de horas de trabajo. Para estos casos, el apagado del equipo es programado.	
b) Apaga su equipo al término de sus labores.	X			
c) Verifica que cerca de los equipos informáticos, no se consumen alimentos, no se fume ni se realicen actos que pongan en riesgo el funcionamiento del equipo o deterioren la información almacenada.	X			
d) Todo trabajador que opera equipos informáticos debe mantener resguardado en lugares seguros (tales como: armarios, mobiliarios cerrados, escritorios, entre otros), y fuera del alcance de terceros los medios informáticos (tales como: documentos, disquetes, CD's, impresos, USB, memorias físicas, entre otras), que contengan información clasificada como secreta o confidencial para la organización.	X			• Gerente General de la Red Asistencial La Libertad – RALL • Ingeniería Hospitalaria • Director • Administrador • Jefe de Informática • Responsable del Servicio

e) Cuando el trabajador se tenga que ausentar temporalmente de su puesto de trabajo y requiere tener el equipo informático encendido, deberá activar el protector de pantalla con contraseña o cualquier otra medida que no permita acceder a un tercero a la información contenida en el equipo a su cargo.	X		Sin embargo, existe personal asistencial y administrativo que incumple con ciertas condiciones: Por ejemplo, dejar medios extraíbles, documentos en el mobiliario, dejar el equipo encendido estando ausente o dejar alimentos (especialmente bebidas) que pueda perjudicar la integridad del equipo. **Recomendación:** Concientizar al personal asistencial y administrativo a respetar las políticas de seguridad de la Institución.	
f) Se debe retirar inmediatamente de las impresoras toda información calificada como completa o confidencial.	X			
g) Se deben mantener los escritorios limpios y ordenados una vez finalizada la jornada laboral.	X			
11.2.1.3. La Gerencia o Jefatura a cargo del Área Segura verifica que los equipos:				
a) Estén ubicados como mínimo a 20 centímetros sobre el nivel del piso para hacer frente a inundaciones.	X		**Recomendación:** Reemplazar por un mobiliario adecuado.	

b) Sus condiciones físicas y de entorno no sean contrarias a las recomendaciones del fabricante de los equipos, medios de comunicación y dispositivos de soporte.		X	**Recomendación:** Trasladar de ambiente.	
c) Se encuentren ubicados en racks cerrados, en armarios con llave o en ambientes bajo control de acceso.		X	**Observación:** Los gestores de información se encuentran únicamente protegidos con el seguro incorporado. Se ha notificado que se ha adquirido un gabinete para su instalación (ver anexo).	• Gerente General de la Red Asistencial La Libertad – RALL • **Ingeniería Hospitalaria** • Administrador • Jefe de Informática
d) Cuenten con mecanismos de seguridad física reglamentaria tales como dobles fuentes de alimentación, dispositivos tolerantes a fallas, entre otros.	X			
e) Tengan cajas que estén herméticamente cerradas a fin de impedir su apertura por manipuleo.		X		
f) Cuenten con kits de herramientas para reparaciones mejores.		X	**Recomendación:** Adquirir kit de herramientas certificado.	

g) El Área Segura cuenta con termómetro si lo requiere el tipo de operaciones que se realicen.		X		
11.2.1.4. Mecanismos de seguridad.				
a) El Área Segura cuenta con detectores de humedad y de humo para prever la posibilidad de ser afectados por una inundación o incendio respectivamente.		X	**Recomendación:** Adquirir detectores de humedad y humo certificado.	• Gerente General de la Red Asistencial La Libertad – RALL • **Ingeniería Hospitalaria** • Director • Administrador
b) Cuenta con equipos de aire acondicionado, salvo que las condiciones naturales del ambiente no lo hagan necesario.	X		**Recomendación:** Adquirir un nuevo equipo de aire acondicionado certificado, debido a que el que se posee es muy propenso a fallas.	
c) Cuenta con línea puesta a tierra y pozo de tierra.		X		• Gerente General de la Red Asistencial La Libertad – RALL • **Ingeniería Hospitalaria** • Director • Administrador
d) Cuenta con sistema contra incendio el cual es probado una vez por año y cuenta con el certificado de operatividad respectivo.		X	**Recomendación:** Certificación sanitaria avalado por un ingeniero colegiado y especializado en el tema.	
e) El personal está capacitado para la utilización de extintores y manguera contra incendio.		X	**Observación:** El personal ha sido orientado de carácter únicamente teórico.	
11.2. Suministro.				

11.2.1. Servicio de suministro				
a) Los tableros de distribución tienen la capacidad requerida por el Área Segura.	X			• Gerente General de la Red Asistencial La Libertad – RALL • **Ingeniería Hospitalaria** • Director • Administrador
b) Cuenta con circuitos eléctricos y tableros de distribución independiente a cualquier otra conexión.	X			
c) Cuenta con línea de puesta a tierra y pozo de tierra.		X		
d) No hay sobrecarga del cableado eléctrico.	X			
e) No existen fuentes de líquidos, gas u otros elementos de riesgo cercano a las instalaciones eléctricas.		X		
f) No existen tomacorrientes destinados para otros equipos ajenos a la función del Área Segura.		X		
g) Existe continuidad regular en cuanto al voltaje y amperaje del fluido eléctrico.	X			
h) Cuenta con equipos UPS (Suministro de Energía Ininterrumpida), conectados a los equipos informáticos.	X		**Recomendación:** Adquirir UPS certificados de preferencia para cada equipo ya que se cuenta con uno y la energía es distribuida con todos .	

i) Se cuenta con grupo electrógeno conectado a los equipos, verificando periódicamente su operatividad. Debe contar con Certificado de Operatividad otorgado por un Ingeniero Electricista colegiado y habilitado. Dicho Certificado debe ser renovado anualmente El grupo electrógeno debe contar con reserva de combustible para 3 días (72 horas) de operación autónoma continua.		X	**Observación:** El hospital cuenta con un grupo electrógeno, pero no está designado únicamente para la Sala de Servidores.	
j) Tiene en lugar visible el procedimiento para el encendido de equipos de emergencia.		X	**Observación:** No existe la señalización adecuada y los tableros deben ser protegidos adecuadamente.	• Gerente General de la Red Asistencial La Libertad – RALL • **Ingeniería Hospitalaria** • Director • Administrador
k) La edificación cuenta con planos del sistema eléctrico, custodiados por la Jefatura encargada de los servicios eléctricos		X		
l) Los gabinetes de los tableros eléctricos son de material aprobado y adecuado para el ambiente donde se encuentra.		X		
m) Los tableros cuentan con señal de riesgo eléctrico en la tapa o junto a ella, directorio de circuitos impreso, mandil y tapas de reserva.		X	**Recomendación:** Cambiar señalización.	
n) Los interruptores termomagnéticos corresponden a la capacidad de corriente de los conductores que protegen.	X			

o) Los tableros eléctricos cuentan con barra de tierra, la cual debe estar conectada a tierra.	X			
p) Existe suficiente espacio alrededor del tablero con el objeto de permitir una rápida y segura manipulación y mantenimiento.	X			
q) Los interruptores termomagnéticos no incorporados en tableros eléctricos cuentan con caja de protección de material aprobado y adecuado para el ambiente donde se encuentra. Si la caja de protección es metálica, debe tener conexión a tierra.	X			• Gerente General de la Red Asistencial La Libertad – RALL • **Ingeniería Hospitalaria** • Director • Administrador
r) Todos los tableros eléctricos deben contar con interruptores diferenciales los cuales pueden instalarse en tableros adyacentes (según lo establece el CNE U 020.132).	X			
11.2.2. Seguridad del cableado				
11.2.2.1. Cableado.				
a) El tipo de conductores eléctricos utilizados debe ser el adecuado y encontrarse protegido mecánicamente (empotrado, entubado o en canaletas). Debe cumplir con los estándares CNE.		X		• Gerente General de la Red Asistencial La Libertad – RALL • **Ingeniería Hospitalaria**

b) El cableado de datos y telefonía se encuentra empotrado, entubado o en canaletas. El cableado cumplirá con los estándares EIA/TIA y CNE.		X		• Director • Administrador
c) Los cables de la red eléctrica y de comunicaciones están separados para evitar interferencias.	X			
d) La capacidad de corriente de los conductores debe corresponder a la corriente del circuito y cumple con las secciones mínimas.	X			• Gerente General de la Red Asistencial La Libertad – RALL • **Ingeniería Hospitalaria** • Dirección • Administración
e) Las secciones mínimas de los conductores no alimentadores de cobre son de una sección nominal no menor de 1.5 mm2.	X			
f) No deben instalarse en el alambrado fijo, cables mellizos. No se deben tener instalaciones con cables mellizos.	X			
11.2.3.2. Tomacorrientes.				
a) Todos los tomacorrientes deben estar conectados al sistema de puesta a tierra.	X		**Recomendación:** Proteger y no dejar expuestos los tomacorrientes. Verificar operatividad de tomacorrientes periódicamente. En caso que presente desperfectos proceder a su cambio inmediato.	• Gerente General de la Red Asistencial La Libertad – RALL • **Ingeniería Hospitalaria** • Director • Administrador
b) La carga corresponde a la capacidad de corriente del circuito.		X		
c) Las tapas de los tomacorrientes están fijas con sus respectivos tornillos de fijación, no presentan rajaduras o roturas.		X		

d) Los enchufes no presentan partes activas expuestas.		X		
e) Todos los equipos se encuentran conectados a la línea de tierra.	X			• Gerente General de la Red Asistencial La Libertad – RALL • **Ingeniería Hospitalaria** • Director • Administrador
f) Los tomacorrientes se encuentran a una altura apropiada (40 cm). La distancia del tomacorriente a cualquier equipo no será mayor a 1.5 m.	X			
g) Los tomacorrientes deben ser usados exclusivamente para los equipos del Área Segura al cual sirven.	X			
11.2.3.3. Alumbrado e iluminación.				
a) Los equipos de alumbrado están firmemente instalados.	X			• Gerente General de la Red Asistencial La Libertad – RALL • **Ingeniería Hospitalaria** • Director • Administrador
b) Los equipos de alumbrado no presentan partes activas expuestas.		X	**Recomendación:** Reemplazar a la brevedad.	
c) Los fluorescentes cuentan con luminarias protectoras de seguridad o cintillos de sujeción.	X			
d) Las partes conductivas expuestas de los equipos de alumbrado están conectadas a la línea de tierra.	X			• Gerente General de la Red Asistencial La Libertad – RALL • **Ingeniería Hospitalaria** • Director • Administrador
e) Los conductores para alumbrado tienen una sección mínima de 0.75 mm2.	X			
f) Existe adecuada iluminación en las Áreas Seguras.	X			

g) Las tapas de los interruptores están fijas con sus respectivos tornillos de fijación, no presentan rajaduras ni roturas.		X	**Observación:** Se presenta ligero y notorio desprendimiento en coberturas de algunos interruptores.	
h) Los interruptores se encuentran a una altura apropiada (1.40 m).		X	**Observación:** Existen interruptores que no cumplen con la medida adecuada.	
11.2.3.3. Sistema de Puesta a Tierra.				
a) La instalación debe contar con una línea de puesta a tierra conectada a uno o más pozos de tierra.		X		• Gerente General de la Red Asistencial La Libertad – RALL • **Ingeniería Hospitalaria** • Director • Administrador
b) Debe contar con Certificado de Resistividad de los pozos de tierra firmados por un ingeniero Electricista o Mecánico colegiado. Dicho Certificado debe renovarse cada año a fin de garantizar la idoneidad de la operación de la línea de tierra.	X			
c) La sección del conductor de puesta a tierra es la adecuada de acuerdo a la demanda del sistema.	X			
d) Los pozos de tierra deben recibir mantenimiento por lo menos una vez al año.	X			
11.2.3.5 Equipos de aire acondicionado.				

a) La capacidad de corriente de los alimentadores corresponde a la carga.	X			• Gerente General de la Red Asistencial La Libertad – RALL • **Ingeniería Hospitalaria** • Director • Administrador
b) Las partes activas están resguardadas contra contacto accidental por medio de gabinetes apropiados y otras formas aprobadas.		X	**Recomendación:** Equipar y ubicar en un lugar adecuado.	
c) Deben contar con conexión a tierra.	X			
d) En el caso específico de los Data Center, estos deben operar a 21ºC.	X			• Gerente General de la Red Asistencial La Libertad – RALL • **Ingeniería Hospitalaria** • Director • Administrador
11.2.3.6. Otras consideraciones de seguridad en instalaciones eléctricas.				
a) Debe verificarse la no existencia de recipientes que almacenen gases o líquidos combustibles en las cercanías de las Áreas Seguras.	X			• Gerente General de la Red Asistencial La Libertad – RALL • **Ingeniería Hospitalaria** • Director • Administrador
b) Debe contar con un Plan de Mantenimiento Preventivo Anual de las instalaciones eléctricas.	X			
c) En el caso específico de los Data Center, no deben guardarse elementos combustibles (tales como cajas, PC's, impresoras, archivos, etc.).		X		

d) Los Data Center deben contar con un Plan Anual de revisión de los parámetros eléctricos (tensión y corriente en un verdadero valor y los índices de armónicos).		X	**Observación:** Sin documentación disponible. Sin embargo, tiene tarjeta de control periódico.	
e) Toda edificación debe contar con un Plan Anual de revisión de los parámetros eléctricos (tensión y corriente en verdadero valor y los índices de armónicos).	X			
11.2.4. Mantenimiento de equipos.				
a) Toda instalación debe contar con un Programa de Mantenimiento Preventivo para los equipos informáticos y dispositivos de soporte informático, así como del equipamiento de las Áreas Seguras en general, a fin de asegurar su operatividad. Dicho Programa debe estar diseñado en base a las recomendaciones de los proveedores de los equipos.		X	**Observación:** Como ya es mencionado, se posee únicamente con programa de mantenimiento preventivo a equipos biomédicos, electromecánicos y para servicios generales. **Recomendación:** Elaborar un Plan enfocado a equipos informáticos.	• Gerente General de la Red Asistencial La Libertad – RALL • **Ingeniería Hospitalaria** • Director • Administrador
b) Se debe supervisar que las recomendaciones del fabricante para la protección del equipamiento sean observadas permanentemente.	X			

c) Mantener un Registro sobre las fallas y los servicios de mantenimiento (preventivos y correctivos) realizados sobre los equipos informáticos y/o los dispositivos de soporte informáticos, así como del equipamiento de las Áreas Seguras en general.		X	**Observación:** Únicamente se registran todo mantenimiento que requiera reemplazo de algún componente o deba ser dado de baja.	• Gerente General de la Red Asistencial La Libertad – RALL • Director • Administrador • **Jefe de Informática**
11.2.5. Remoción de activos (Salida de activos fuera de las instalaciones de la empresa).				
Se verifica que los equipos informáticos que se encuentren malogrados y que contengan información sensible o software licenciado, y que para su reparación deban ser trasladados fuera de las instalaciones de EsSalud (o por cualquier otro motivo debidamente autorizado), antes de su traslado, ha sido copiada dicha información en un medio de respaldo y ha sido eliminada la referida información de dichos equipos.		X	**Recomendación:** Fortalecer medidas de seguridad, entregando únicamente los componentes necesarios tales como la fuente de energía o la placa madre (en caso se diagnostique problemas en ella), conservar el disco duro con el fin de preservar la información.	• Gerente General de la Red Asistencial La Libertad – RALL • Director • Administrador • **Jefe de Informática**
11.2.6. Seguridad de equipos y activos fuera de las instalaciones.				
a) La movilización de equipos informáticos fuera de los Data Center, así como de los equipos de las Áreas Seguras en general, por motivos de mantenimiento, préstamo o cualquier otro, sólo podrá ser utilizado por el funcionario a cargo del	X			

Área Segura, con el visto bueno del ejecutivo a cargo de la instalación donde se ubican las Áreas Seguras.				• Gerente General de la Red Asistencial La Libertad – RALL • **Ingeniería Hospitalaria** • Director • Administrador • Jefe de Infomática
b) Se verifica que el ambiente ubicado fuera de los locales de la institución y designado para la instalación de equipos informáticos, así como de los equipos de las Áreas Seguras en general de EsSalud, cuenten con las condiciones técnicas y de entorno establecido por las especificaciones técnicas de dichos equipos.	X		**Observación:** La Institución es consciente que no se encuentra en un lugar adecuado por motivos de disponibilidad de ambientes.	
c) Supervisar y cautelar que el traslado de los equipos de las Áreas Seguras fuera de sus instalaciones, se efectúe brindando la protección adecuada a los equipos.	X		**Recomendación:** Registrar eventos.	
d) Debe ser el caso de tener que trasladar equipos informáticos a otra instalación de EsSalud, se debe, informar al nuevo custodio sobre la información contenida (datos, aplicativos, software licenciados, entre otros) en dicho activo, para que este último adopte las medidas de protección adecuadas que aseguren la preservación y confidencialidad.	X			• Gerente General de la Red Asistencial La Libertad – RALL • **Jefe de Informática**

e) Supervisar que la instalación de los equipos informáticos de un Data Center, así como de los equipos de las Áreas Seguras en general de EsSalud en ambientes externos, no afecte la aplicación de los programas de mantenimiento previamente establecidos.	X			
f) De acuerdo a las circunstancias y la decisión que adopte el funcionario a cargo del Data Center, toda la información o software bajo licencia y residente en los equipos que serán trasladados, deben ser borrados, anulados o imposibilitados de todo uso, copiando previamente la información en un medio de respaldo.	X			
g) En los casos que los determine el funcionario a cargo de un Data Center, se inhabilitarán temporalmente los dispositivos y conexiones que permiten la grabación de información en medios externos (como: disqueteras, CD, conexiones USB, entre otros.), de aquellos activos informáticos que almacenan información de las siguientes características: Datos calificados como secretos o confidenciales, aplicativos, software licenciados, entre otros.	X		**Recomendación:** Fortalecer medidas de seguridad, entregando únicamente los componentes necesarios tales como la fuente de energía o la placa madre (en caso se diagnostique problemas en ella), conservar el disco duro con el fin de preservar la información.	• Gerente General de la Red Asistencial La Libertad – RALL • **Jefe de Informática**
11.2.7. Disposición o reutilización segura de equipos (Reutilización o retirada segura de dispositivos de almacenamiento).				

Se verifica que toda información o software bajo licencia y residente en los dispositivos de almacenamiento de los equipos que serán dados de baja o reusados, debe copiarse en un medio de respaldo y luego borrar toda la información de dichos dispositivos.	X			• Gerente General de la Red Asistencial La Libertad – RALL • **Jefe de Informática**
11.2.8. Equipos de usuarios desatendidos.				
Los usuarios se aseguran que los equipos informáticos que no cuentan con vigilancia tengan la protección adecuada (por ejemplo: activación del protector de pantalla y solicitud de clave al ingreso).	X		**Recomendación:** Formalizar proceso de solicitud en caso de pérdida o robo de información.	• Gerente General de la Red Asistencial La Libertad – RALL • **Jefe de Informática** • Usuario directo
11.2.9. Política de escritorio limpio y pantalla limpia (pantalla bloqueada).				
a) Se cumple la política de la pantalla y escritorio limpio. Los puestos de trabajo deben estar limpios de papeles, soportes de almacenamiento extraíbles y cuando un computador esté desatendido deberá bloquease la pantalla.		X		• Gerente General de la Red Asistencial La Libertad – RALL • Director • Administrador • **Jefe de Informática** • Responsable del Servicio • Usuario directo
b) Los papeles y medios de información deben estar asegurados en armarios especiales, especialmente en horas fuera de las normales de trabajo.		X		
c) Las fotocopiadoras deben estar protegidas de uso no autorizado.	X			

OBJETIVOS Y CONTROLES	CUMPLE		OBSERVACIONES / RECOMENDACIONES	RESPONSABLE
	SI	NO		
12. SEGURIDAD DE LAS OPERACIONES				
12.1. Procedimientos y responsabilidades operativas.				
Objetivo: Asegurar que las operaciones de instalaciones de procesamiento de la información sean correctas y seguras.				
12.1.1. Procedimientos operativos documentados.				
a) Los procedimientos de operación son documentados y puestos a disposición de los usuarios que los necesitan.	X		**Observación:** Se reporta un informe de trabajo final resumido adjuntando el diagnóstico y su solución. **Recomendación:** Formalizar toda operación realizada al detalle, así como reportar todo incidente que se puede presentar.	• **Gerente Central de las Tecnologías de Información y Comunicaciones** • Gerente General de la Red Asistencial La Libertad – RALL • **Jefe de Informática**
b) Las GCTIC provee a sus funcionarios de manuales de configuración y operación de los Sistemas Operativos, funciones de red, Bases de Datos y Sistemas de Información (comunicaciones y servicios como correo, Intranet WEB) así como todos los componentes de la plataforma tecnológica de la información.	X			
c) Se garantiza la documentación y actualización de los procedimientos relacionados con la operación y administración de la plataforma tecnológica que apoya los procesos de negocio de EsSalud.	X			

12.1.2. Gestión del cambio.				
a) EsSalud a través del área responsable establece, coordina y controla los cambios realizados en los activos de información tecnológicos y los recursos informáticos, asegurando los cambios efectuados sobre la plataforma tecnológica, tanto el software operativo como los Sistemas de Información	X		**Recomendación:** Aumentar la frecuencia de supervisión, ya sea trimestral, semestral o anual.	• **Gerente Central de las Tecnologías de Información y Comunicaciones** • Gerente General de la Red Asistencial La Libertad – RALL • **Jefe de Informática**
b) La GCTIC garantiza que todo cambio realizado a un componente de la plataforma tecnológica, el cual conlleve modificación de accesos, modificación o mantenimiento de software, actualización de versiones o modificación de parámetros, certifica y mantiene los niveles de seguridad existentes.	X		**Recomendación**: Cumplir con las fechas de plazo estimadas. Fortalecer comunicación entre la Gerencia Central de las TIC e Informática.	
c) Se garantiza que todo cambio realizado sobre la plataforma tecnológica de EsSalud, quedará formalmente documentado desde su solicitud hasta su implantación cumpliendo con el procedimiento correspondiente.	X			• **Gerente Central de las Tecnologías de Información y Comunicaciones** • Gerente General de la Red Asistencial La Libertad – RALL • Unidad de Adquisiciones • **Jefe de Informática**
d) Los dueños o responsables de los activos de información tecnológicos y recursos informáticos solicitan formalmente los requerimientos de nuevas funcionalidades, servicios o modificaciones sobre sus sistemas de información.	X			

e) Los administradores de los activos de información tecnológicos y recursos informáticos garantizan que las modificaciones o adiciones en las funcionalidades de los sistemas de información están soportadas por las solicitudes realizadas por los usuarios, siguiendo el procedimiento vigente para dicha acción.		X	**Observación:** Los sistemas de información del área de Producción se encuentran obsoletos. **Recomendación:** Se requiere adquirir nueva tecnología.	
12.1.3. Gestión de la capacidad.				
El uso de los recursos es monitoreado, afinado y se debe hacer proyecciones de los futuros requisitos de capacidad para asegurar el desempeño requerido del sistema.	X			• Gerente General de la Red Asistencial La Libertad – RALL • **Jefe de Informática**
12.1.4. Separación de los entornos de desarrollo, pruebas y operaciones (producción).				
El desarrollo, las pruebas y producción están separados para reducir los riesgos de acceso no autorizado o cambios en el entorno operativo Se deben garantizar los recursos necesarios que permitan la separación de ambientes de desarrollo, pruebas y producción, así como de la independencia de los funcionarios que ejecutan dichas labores.	X			• Gerente General de la Red Asistencial La Libertad – RALL • **Jefe de Informática**

12.2. Protección contra códigos maliciosos.				
Objetivo: Asegurar que la información y las instalaciones de procesamiento de la información estén protegidas contra códigos maliciosos.				
12.2.1. Controles contra códigos maliciosos.				
a) Se aplican controles de detección, prevención y recuperación para protegerse contra el código malicioso, en combinación con el conocimiento del usuario correspondiente.		X		• **Gerente Central de las Tecnologías de Información y Comunicaciones** • **Informática**
b) EsSalud provee los recursos necesarios que garanticen la protección de la información y los recursos de procesamiento de la misma manera adoptando controles necesarios para evitar la divulgación, modificación o daño permanente ocasionados por la contaminación u/o el contagio de software malicioso.	X		**Observación:** Todo equipo debe contar con software antivirus licenciado. Sin embargo, existen programas maliciosos que logran vulnerar la protección. **Recomendación:** Adquirir un software antivirus más sofisticado y moderno.	• **Gerente Central de las Tecnologías de Información y Comunicaciones** • Unidad de Adquisiciones • **Jefe Informática**
c) La GCTIC garantiza que los activos de información, así como, los recursos tecnológicos son actualizados periódicamente, evitando que códigos maliciosos y virus ejecuten vulnerabilidades del sistema de los mismos. Al respecto: El software usado para la mitigación de virus informáticos cuenta con las licencias de uso aprobadas, garantizando su autenticidad y su periódica actualización. La información almacenada en los activos de información		X		

tecnológicos que es transportada por la red de datos, es escaneada con una periodicidad establecida para garantizar así la seguridad de la misma. Los usuarios de los activos de información tecnológicos no pueden modificar la configuración establecida para el software antivirus.				
d) Los usuarios de activos de información tecnológicos y recursos informáticos hacen uso exclusivo de hardware y software autorizado por los funcionarios de la instalación.	X			• **Gerente Central de las Tecnologías de Información y Comunicaciones** • **Jefe de Informática** • Usuario Directo
e) Los usuarios de activos de información tecnológicos y recursos informáticos garantizan que las descargas de archivos adjuntos de los correos electrónicos o descargados de internet realizadas, provienen de fuentes conocidas, seguras y exclusivas de acuerdo con las funciones encomendadas.	X			
f) Los usuarios de activos de información tecnológicos y recursos informáticos corren el software antivirus sobre archivos y/o documentos que son abiertos y/o ejecutados por primera vez.	X			• **Gerente Central de las Tecnologías de Información y Comunicaciones** • **Jefe Informática** • Usuario Directo

g) Los usuarios de activos de información tecnológicos se comunican con la GCTIC al encontrar un virus, del cual no se sabe cómo eliminarlo, o cómo actuar frente al mismo o de considerarlo necesario.		X	**Recomendación:** Fortalecer comunicación y reportar todo tipo de incidentes.	
12.3. Respaldo.				
Objetivo: Proteger contra la pérdida de datos				
12.3.1. Respaldo de la información				
a) Las copias de seguridad de la información y software se toman y prueban regularmente de acuerdo con una política de copia de seguridad acordada.		X	**Recomendación:** Programar fechas para la prueba de copias de seguridad de manera frecuente.	• **Gerente Central de las Tecnologías de Información y Comunicaciones** • **Jefe de Informática**
b) Los funcionarios responsables de la gestión del almacenamiento y respaldo de la información deberán proveer los recursos necesarios para garantizar el correcto tratamiento de la misma.	X		**Recomendación:** La GCTIC debe atender con más prioridad las solicitudes, tales como las unidades de almacenamiento.	
c) Los dueños o responsables de los activos de información tecnológicos y recursos informáticos definen con la Oficina de Soporte Informático de la Red las estrategias para la correcta y adecuada generación, retención y rotación de las copias de respaldo de la información.	X			

d) Los dueños o responsables de información tecnológicos y recursos informáticos velan por el cumplimiento de los procedimientos de respaldo de la información.	X			
e) La Oficina de Soporte Informático de la Red establece lineamientos para la generación y almacenamiento de las copias de respaldo.	X			
f) La Política de Seguridad Informática EsSalud ha establecido procedimientos para la correcta y segura generación, así como el adecuado tratamiento de las copias de respaldo.	X		**Recomendación:** Evaluar copias de seguridad con más frecuencia	
g) La información que es salvaguardada por la Oficina de Soporte Informático de la Red, está almacenada y respaldada y/o externamente a la instalación, de acuerdo con las normas establecidas de tal forma que se garantice su disponibilidad en cualquier momento. Debe existir una definición formal de la estrategia de generación, retención y rotación de las copias de respaldo que se realizan.	X			• **Gerente Central de las Tecnologías de Información y Comunicaciones** • **Jefe de Informática**
h) La Oficina de Soporte Informático de la Red cuenta con procedimientos y recursos informáticos para realizar pruebas a las copias de respaldo para garantizar su integridad y usabilidad en caso de ser requerido.	X		**Observación:** Se tienen procedimientos sin embargo no se realizan las pruebas correspondientes.	

i) Los administradores de los activos de información tecnológicos y recursos informáticos ejecutan los procedimientos provistos por la GCTIC con los medios autorizados para realizar pruebas a las copias de respaldo.		X		
j) Los administradores de los activos de información tecnológicos y recursos informáticos realizan pruebas periódicas de recuperación de la información respaldada y documentan sus resultados.		X		
k) Se realizan todas las copias de respaldo de las bases de datos que contienen los sistemas de información institucionales y demás servicios, todos los días, esta tarea se realiza en forma automática y además cada sistema de información debe guardar los datos en tiempo real de digitación de los mismos por el usuario.	X			• **Gerente Central de las Tecnologías de Información y Comunicaciones** • **Jefe de Informática**

l) Los funcionarios y/o contratistas de EsSalud, son responsables de realizar los Backup's de la información institucional que cada uno maneja en sus equipos de escritorio, ya que dicha información una vez finalice el vínculo laboral con la Institución debe ser entregada como proceso para finalizar dicha vinculación.	X		El personal de EsSalud es el encargado de realizar todo procedimiento de seguridad de información.	
12.4. Registros y monitoreo (Registro de actividad y supervisión)				
Objetivo: Registrar eventos y generar evidencia.				
12.4.1. Registro de eventos				
Se efectúan revisiones regulares y cuidados a los registros de eventos que se graban de las actividades del usuario, excepciones, fallas y eventos de seguridad de la información, deben ser producidos, mantenidos y regularmente revisados.		X		• **Gerente Central de las Tecnologías de Información y Comunicaciones** • **Jefe de Informática**
12.4.2. Protección de información de registros (Protección de registros de información)				
Las instalaciones para registros (logs) y la información de los registros(logs) deben ser protegidas contra la adulteración y el acceso no autorizado. Los registros de información se protegen contra la manipulación y el acceso no autorizado.	X			• **Gerente Central de las Tecnologías de Información y Comunicaciones** • **Jefe de Informática**

12.4.3. Registros de administrador y del operador (Registros de actividad del administrador y operador del sistema)				
Las actividades del administrador del sistema y del operador del sistema deben ser registradas y los registros (logs) deben ser protegidos y revisados regularmente	X			• **Gerente Central de las Tecnologías de Información y Comunicaciones** • **Jefe de Informática**
12.4.4. Sincronización del reloj.				
Los relojes de todos los sistemas de informática relevantes están sincronizados a una fuente de tiempo de referencia única.		X	**Observación:** Se puede constatar que, la hora no está sincronizada correctamente. Esto a veces suele generar problemas a la hora de registrar o consultar información.	• **Gerente Central de las Tecnologías de Información y Comunicaciones** • **Jefe de Informática**

OBJETIVOS Y CONTROLES	CUMPLE		OBSERVACIONES / RECOMENDACIONES	RESPONSABLE
	SI	NO		
13. SEGURIDAD DE LAS COMUNICACIONES				
13.1. Gestión de la seguridad de la red				
Objetivo: Asegurar la protección de la información en las redes y sus instalaciones de procesamiento de información de apoyo.				
13.1.1. Controles de la red				
a) Las redes deben ser gestionadas y controladas para proteger la información en los sistemas y las aplicaciones.	X			• Gerente General de la Red Asistencial La Libertad – RALL • **Ingeniería Hospitalaria** • **Jefe de Informática**
13.1.2. Seguridad de servicios de red				
a) Mecanismos de seguridad, niveles de servicio y requisitos de gestión de todos los servicios de red deben ser identificados e incluidos en acuerdos de servicios de red, ya sea que estos servicios se provean internamente o sean tercerizados.	X			• Gerente General de la Red Asistencial La Libertad – RALL • **Unidad de Adquisiciones** • **Jefe de Informática**
13.1.3. Segregación en redes				
a) Grupos de servicios de información, usuarios y sistemas de información deben ser segregados en redes.	X			• Gerente General de la Red Asistencial La Libertad – RALL • **Jefe de Informática**

13.2. Transferencia de información				
Objetivo: Transferencia de información (Intercambio de información con partes externas)				
13.2.1. Políticas y procedimientos de transferencia de la información				
Políticas, procedimientos y controles de transferencia formales deben aplicarse para proteger la transferencia de información a través del uso de todo tipo de instalaciones de comunicación.	X			• Gerente General de la Red Asistencial La Libertad – RALL • **Jefe de Informática**
13.2.2. Acuerdo sobre transferencia de información				
Los acuerdos deben dirigir la transferencia segura de información del negocio entre la organización y partes externas.	X			• Gerente General de la Red Asistencial La Libertad – RALL • **Unidad de Adquisiciones** • **Jefe de Informática**
13.2.3. Mensajes electrónicos				
La información involucrada en mensajería electrónica debe ser protegida apropiadamente.		X	**Observación:** No existen medidas de seguridad en protección de correos electrónicos. La información puede ser transferida o alterada. **Recomendación:** Fortalecer medidas de seguridad.	• Gerente General de la Red Asistencial La Libertad – RALL • **Jefe de Informática**
13.2.4. Acuerdos de confidencialidad o no divulgación				

Requisitos para los acuerdos de confidencialidad o no divulgación que reflejan las necesidades de la organización para la protección de la información deben ser identificados, revisados y documentados regularmente.	X			• Gerente General de la Red Asistencial La Libertad – RALL • **Unidad de Adquisiciones**

OBJETIVOS Y CONTROLES	CUMPLE		OBSERVACIONES / RECOMENDACIONES	RESPONSABLE
	SI	NO		
15. RELACIÓN CON LOS PROVEEDORES				
15.1. Seguridad de la Información en las organizaciones con los proveedores				
Objetivo: Asegurar protección a los activos de la organización que son accesibles con los proveedores.				
15.1.1. Política de Seguridad de la Información para las relaciones con los proveedores				
a) Se formulan acuerdos documentados de los requisitos de la Seguridad de la Información requeridos por los activos de la organización con el objetivo de mitigar los riesgos asociados al acceso por parte de proveedores y terceras personas.	X			• Gerente General de la Red Asistencial La Libertad – RALL • Ingeniería Hospitalaria • **Unidad de Adquisiciones**
b) Los acuerdos deben ser plasmados en los contratos suscritos con los proveedores.	X			
15.1.2. Abordar la seguridad dentro de los acuerdos con los proveedores (Tratamiento del riesgo dentro de acuerdos de proveedores)				

a) Se han establecido y acordado todos los requisitos de Seguridad de la Información pertinentes a cada proveedor que puede acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura de TI que dan soporte a la información de la Organización.	X			• Gerente General de la Red Asistencial La Libertad – RALL • Ingeniería Hospitalaria • **Unidad de Adquisiciones**
15.1.3. Cadena de suministro en Tecnologías de la Información y Comunicaciones				
a) Los acuerdos con los proveedores incluyen los requisitos para abordar los riesgos de seguridad de la información asociados con la cadena de suministro de los servicios y productos de Tecnología de Información y Comunicación.	X			• Gerente General de la Red Asistencial La Libertad – RALL • Ingeniería Hospitalaria • **Unidad de Adquisiciones**
15.2. Gestión de entrega de servicios del proveedor				
Objetivo: Mantener un nivel de seguridad de la información y entrega de servicios acordado en línea con los acuerdos con los proveedores.				
15.2.1. Monitoreo y revisión de servicios de los proveedores				
a) Se monitorean, revisan y auditan regularmente la prestación de servicios por parte de los proveedores.	X		**Observación:** La prestación de servicios en equipos informáticos consiste en dar soporte para mantenimiento correctivo siempre y cuando se cumplan ciertas	• Gerente General de la Red Asistencial La Libertad – RALL • **Ingeniería Hospitalaria** • **Unidad de Adquisiciones**

			condiciones establecidas en el contrato. Sin embargo, no pasa lo mismo con equipos biomédicos y electromecánicos, que tienen mantenimiento preventivo programado, ya sea trimestral o semestral (de acuerdo a contrato). **Recomendación:** Elaborar un Programa para todos los equipos informáticos.	
15.2.2. Gestión de cambios a los servicios de proveedores				
a) Los cambios en la prestación de servicios por parte de los proveedores, incluyendo el mantenimiento y la mejora de las actuales políticas de seguridad de información, procedimientos y controles, se gestionarán, teniendo en cuenta la criticidad de la información, sistemas y procesos que intervienen y una reevaluación de los riesgos.	X		**Recomendación:** Elaborar un presupuesto (ya sea trimestral, semestral o anual) de acuerdo a necesidades.	• Gerente General de la Red Asistencial La Libertad – RALL • Ingeniería Hospitalaria • **Unidad de Adquisiciones**

OBJETIVOS Y CONTROLES	CUMPLE		OBSERVACIONES / RECOMENDACIONES	RESPONSABLE
	SI	NO		
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN				
Incidentes de Seguridad de la Información -Definición: Evento producto de la materialización de un peligro que tiene la capacidad de interrumpir el normal desarrollo de las operaciones y amenazar la seguridad de la información. Entre los principales tenemos: Uso indebido de información crítica. Ingeniería social, fraude o Phishing, Uso prohibido de un recurso informático o de red de la Institución, Modificación no autorizada de un sitio o página web de la Institución, Divulgación no autorizada de información personal, Eliminación insegura de información, Intrusión física, Modificación o eliminación no autorizada de datos, Destrucción no autorizada de información, Anomalía o vulnerabilidad técnica de software, Robo, pérdida o adulteración de información, Robo o afectación a los equipos de procesamiento de información, Amenaza o acoso por medio electrónico, Interrupción prolongada en u sistema o servicio de red, Ataque o infección por código malicioso (virus, gusanos, troyanos, etc.), Modificación, instalación o eliminación no autorizada de software, Robo o pérdida de un recurso informático de la institución, Acceso o intento de acceso no autorizado a un sistema informático o ambiente donde se guarda información, entre otros.				
16.1. Gestión de incidentes de seguridad de la información y mejoras.				
Objetivo: Asegurar un enfoque consistente y efectivo a la gestión de incidentes de seguridad de la información, incluyendo la comunicación sobre eventos de seguridad y debilidades.				

16.1.1. Responsabilidades y procedimientos				
a) La responsabilidad y el procedimiento de manejo para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información recae sobre el Administrador del Centro Asistencial o quien haga sus veces.	X			• Gerente General de la Red Asistencial La Libertad – RALL • **Ingeniería Hospitalaria** • Director • **Administrador** • **Jefe de Informática**
b) Se tienen diseñados procedimientos de respuesta para cada tipo de incidente tipificado, tales como acceso no autorizado, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a la Política de Seguridad de la Información de la Institución, entre otros.		X	**Observaciones:** Se comprueba que, en unos casos, el personal divulga su cuenta con motivos de apoyo. Sin embargo, de esta manera se expone a riesgos. **Recomendaciones:** Concientizar al usuario directo a no divulgar su cuenta.	• Gerente General de la Red Asistencial La Libertad – RALL • **Ingeniería Hospitalaria** • **Jefe de Informática** • Responsable del Servicio • Usuario Directo

<table>
<tr><td colspan="5">16.1.2. Reporte (notificación) de los Eventos de Seguridad de la Información</td></tr>
<tr><td>a) Se tiene un escalamiento o procedimiento para notificar los eventos de seguridad de información. El reporte (notificación) de los incidentes permite responder a los mismos en forma sistemática, minimizar su ocurrencia, facilitar una recuperación rápida y eficiente de las actividades minimizando la pérdida de información y la interrupción de los servicios, y manejar correctamente los aspectos legales que correspondan.</td><td></td><td>X</td><td rowspan="3">Observación:
Existe comunicación entre Informática y trabajadores. Sin embargo, todo es notificado verbalmente y no se registran los eventos (únicamente son registrados las excepciones producidas por cualquier sistema de información).

Recomendación:
Formalizar todo proceso de notificación o solicitud, ya sea vía correo y/o documentario.</td><td rowspan="3">• Gerente General de la Red Asistencial La Libertad – RALL
• Ingeniería Hospitalaria
• Jefe de Informática
• Responsable del Servicio
• Usuario Directo</td></tr>
<tr><td>b) Se tienen diseñados procedimientos de respuesta para cada tipo de incidente tipificado, tales como acceso no autorizado, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a la Política de Seguridad de la Información de la Institución, entre otros.</td><td></td><td>X</td></tr>
<tr><td>c) Se tiene una coordinación estrecha con la Oficina de Seguridad Informática y/o la Oficina de Soporte Informático y la Dirección de la instalación a fin de informar rápidamente acerca de la ocurrencia de un incidente.</td><td>X</td><td></td></tr>
</table>

d) Se tiene un registro de incidentes de Seguridad de la Información.		X		
16.1.3. Reporte de Debilidades de Seguridad de la Información				
a) Personal asistencial y administrativo reporta las debilidades de seguridad de la información al correo mesadeayuda@essalud.gob.pe y al correo osi@essalud.gob.pe y al anexo 1111.		X	**Observación:** Personal desconoce dicha información de contacto. Reportes suelen ser notificados localmente al personal informático.	• Gerente General de la Red Asistencial La Libertad – RALL • Director • Administrador • **Jefe de Informática** • **Responsable del Servicio**
b) Se ha informado y motivado adecuadamente a todo el personal, contratistas o personal externo la obligación de reportar debilidades en la seguridad de los sistemas y servicios.	X		**Observación:** Al personal interno, externo y contratistas se les notifica y/o les hace llegar la respectiva información al momento de firmar contrato. En el caso de personal externo y contratista (supervisado por Ingeniería), se les hace llegar mediante contrato con el representante legal de la empresa.	• Gerente General de la Red Asistencial La Libertad – RALL • **Ingeniería Hospitalaria** • Director • Administrador • **Jefe de Informática** • Responsable del Servicio

16.1.4. Evaluación y decisión sobre eventos de Seguridad de la Información				
a) El Administrador de CAS o quien haga sus veces, es el encargado de valorar los eventos de Seguridad de Información y decidir si han de ser clasificados como Incidentes de Seguridad de la Información.	X		**Observación:** El Administrador es el encargado de reportar los eventos previo diagnóstico e informe del personal informático. Sin embargo, todo asunto que tenga que ver con las tecnologías de información son tomados en segundo plano, a excepción de solicitudes de acceso a internet y desbloqueo de uso de unidades extraíbles. **Recomendación:** Concientizar al área administrativa en reportar todo tipo de eventos que involucren a las tecnologías de información, para dar un mejor diagnóstico y solucionarlo en un tiempo razonable.	• Gerente General de la Red Asistencial La Libertad – RALL • Director • **Administrador** • **Jefe de Informática**

b) Se tiene un registro de los incidentes de Seguridad de Información indicando la valoración de los daños ocasionados.		X		• Gerente General de la Red Asistencial La Libertad – RALL • Ingeniería Hospitalaria • Director • Administrador • **Ingeniería Hospitalaria**
16.1.5. Respuesta a incidentes de Seguridad de la Información				
a) Se tienen identificados los riesgos que amenazan la información.	X		**Observación:** Los riesgos son identificados y se sabe cómo confrontarlos. Sin embargo, no se realizan medidas preventivas.	• Gerente General de la Red Asistencial La Libertad – RALL • Ingeniería Hospitalaria • Director • Administrador • **Jefe de Informática**
b) Para cada riesgo identificado se han desarrollado procedimientos de respuesta.	X			
c) Se ha constituido el Comité Técnico de Seguridad de la Información conformado por funcionarios y personal administrativo (en el que se incluye personal de TI), y asistenciales.		X		
d) Los procedimientos de respuesta han sido probados efectuando simulacros o simulaciones según sea el caso.		X		
e) Se comunica a la Oficina de Seguridad Interna y Asesoría Jurídica de su jurisdicción o quienes hagan sus veces para que ejecuten las acciones que correspondan.		X		

16.1.6. Aprendizaje de los incidentes de Seguridad de la Información				
a) Los conocimientos adquiridos a partir del análisis y la resolución de incidentes de Seguridad de Información se utilizan para reducir la probabilidad o el impacto de los incidentes en el futuro.	X			• Gerente General de la Red Asistencial La Libertad – RALL • Ingeniería Hospitalaria • Director • Administrador • **Jefe de Informática**
b) Se han adoptado las medidas de prevención necesarias para eliminar o minimizar las causas que dieron origen al incidente de seguridad de la información a fin de que no ocurren eventos similares al futuro.		X	**Observación:** El diagnóstico se da predictivamente y el mantenimiento es únicamente de carácter correctivo.	
16.1.7. Recolección (Recopilación de evidencias)				
a) Se identifican, recopilan y conservan las evidencias probatorias de la ocurrencia de un incidente.		X	**Observación:** No se notifica formalmente salvo un inconveniente de mayor envergadura. **Recomendación:** Formalizar procedimientos ya sea documentario o vía correo electrónico.	• Gerente General de la Red Asistencial La Libertad – RALL • Ingeniería Hospitalaria • Director • Administrador • **Jefe de Informática**
b) Se realiza una incautación de los equipos afectados cuando se haya cometido un delito.	X			
c) Se tiene un procedimiento a seguir en caso de presunción u ocurrencia de un delito.	X			

OBJETIVOS Y CONTROLES	CUMPLE		OBSERVACIONES / RECOMENDACIONES	RESPONSABLE
	SI	NO		
17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO				
17.1. Continuidad de Seguridad de la Información.				
Objetivo: La continuidad de seguridad de la información debe estar embebida en los sistemas de gestión de continuidad del negocio de la organización -Contrarrestar las interrupciones en las actividades del negocio y proteger sus procesos críticos contra los efectos de fallas importantes en los Sistemas de Información o contra desastres y asegurar su recuperación oportuna.				
17.1.1. Planificación de la continuidad de la Seguridad de la Información				
a) Se han elaborado el Plan de Seguridad ante Contingencias en la Oficina de Soporte Informático de acuerdo a la Directiva Nº 001-OCTIC-ESSALUD-2011 "Guía para la Elaboración del Plan Seguridad ante Contingencias de las Oficinas de Soporte Informático.		X	**Observación:** Se conoce sobre la obligación de elaborar un Plan de Seguridad mas no se le da una adecuada prioridad ni un estudio minucioso por parte de la Gerencia General. **Recomendaciones**: Concientizar a la Alta Dirección que emplee las medidas correctas y necesarias a la brevedad junto a la Oficina de Soporte Informático de la Red para elaborar el Plan de	• Gerente General de la Red Asistencial La Libertad – RALL • **Jefe de Informática**

			Seguridad, siendo el traslado de los servidores a un lugar seguro frente a riesgos y amenazas.	
b) Se ha elaborado el Plan de Seguridad de la Información el cual comprende los siguientes aspectos enunciados en los literales c) a i). Para ello es necesario: Identificar los procesos críticos del negocio. Identificar los eventos que pueden provocar interrupciones en los procesos de negocio de la organización (ejemplo: Fallas de equipos, errores humanos, robos, incendios, desastres naturales y actos terroristas.) Evaluar los riesgos para determinar la probabilidad y los efectos de dichas interrupciones en cuanto a tiempo, escala de daños y período de recuperación. Identificar los riesgos asociados a la pérdida de la confiabilidad de la información en el ámbito del Sistema de Gestión de la Seguridad de Información, y establece acciones de control y responsables de contribuir en la mitigación de los riesgos. **La Confiabilidad de la Información** significa la validez de la información y que sólo existirá si la información cumple con las condiciones de: Confidencialidad, Integridad. Disponibilidad:		X	**Observación:** No existe un plan establecido que haya sido estudiado adecuadamente y que sea ejecutado por la Oficina de Soporte Informático y supervisado por la Alta Dirección periódicamente. Sin embargo, existen técnicas y herramientas que aseguran de alguna manera la información. Únicamente se identifican eventos cuando ocurren fallas en los equipos informáticos (mantenimiento correctivo). **Recomendación:**	• Gerente General de la Red Asistencial La Libertad – RALL • **Jefe de Informática**

Confidencialidad (la información solo puede ser conocida por individuos autorizados); Integridad (la información no ha sido alterada, borrada, reordenada, copiada, etc.); Disponibilidad (la información puede ser recuperada en el momento que se necesite).			Promover a la Oficina de Soporte informático de la Red y a la Alta Dirección en elaborar el Plan de Seguridad.	
c) Se tienen procedimientos de respuesta los cuales describen las acciones a ejecutar cuando ocurre un incidente que interrumpe las operaciones del negocio, proporcionando mecanismos alternos y temporales para continuar con el procesamiento de información.		X	**Observación**: Como es mencionado anteriormente, existen técnicas y herramientas que protegen la información. En algunos casos, existe pérdida de información que comprende desde la última copia de seguridad hasta el momento del siniestro.	
d) Se tienen procedimientos de recuperación los cuales describen las acciones a seguir para trasladar las actividades del negocio a un centro alterno de recuperación.		X	**Observación:** No se emplea la técnica espejo (Mirroring).	

e) Se tienen procedimientos de retorno los cuales describen las acciones a seguir para regresar las operaciones normales a las instalaciones originales.		X	**Observación:** Únicamente se restaura la copia de seguridad anterior al cambio.	
f) Se tienen programación de pruebas, las cuales describen la periodicidad en que el Plan de Continuidad debe ser probado.		X	**Observación:** Existe un consolidado de copias de seguridad, pero no se realizan pruebas de respaldo. El respaldo de información se da únicamente cuando se necesita. **Recomendación:** Revisar copias de seguridad.	• Gerente General de la Red Asistencial La Libertad – RALL • **Jefe de Informática**
g) Actualización periódica: El Plan debe actualizarse anualmente o cuando los cambios realizados en el ambiente operativo impacten su funcionalidad.		X	**Observación:** No existe un Plan alineado a los requerimientos del hospital.	
h) Cuando se realicen pruebas, simulacros o se tengan incidentes (contingencias) reales, los resultados y sugerencias deben ser entregadas a los responsables de la información quienes deben actualizar sus planes y mantenerlos al día conforme los riesgos de disponibilidad lo dictamen.	X		**Recomendación:** La información proporcionada debe ser tenida en cuenta en una posible siguiente actualización del Plan.	

i) El proceso de copia y respaldo de la Información debe cumplir con los requerimientos del negocio, los de seguridad de la información y los legales. Este proceso junto con sus procedimientos es la entrada para la ejecución de los planes de continuidad de las operaciones, en caso de presentarse un evento que amerite la activación del Plan.		X		• Gerente General de la Red Asistencial La Libertad – RALL • **Jefe de Informática**
17.1.2. Implementación de la continuidad de la Seguridad de la Información				
a) Se ha elaborado el Plan de Seguridad ante Contingencias de la Oficina de Soporte Informático y el Plan de Seguridad de la Información.		X	**Observación:** No está alineado a los requerimientos del hospital.	• Gerente General de la Red Asistencial La Libertad – RALL • **Jefe de Informática**
b) Se han establecido, documentado, implementado y mantenido procesos, procedimientos y controles para garantizar el nivel necesario de continuidad para la Seguridad de la Información durante una situación adversa.		X		
17.1.3. Verificación, revisión y evaluación de la continuidad de la Seguridad de la Información				
a) Se han efectuado pruebas del Plan de Seguridad de Información.		X		• Gerente General de la Red Asistencial La Libertad – RALL • **Jefe de Informática**
b) Se han efectuado mejoras al Plan de acuerdo a la experiencia lograda en la Prueba del Plan.		X		

17.2. Redundancias				
Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de la información				
a) Se cuenta con Redundancia de: fluido eléctrico (UPS, grupo electrógeno); aire acondicionado (dos equipos de aire acondicionado como mínimo); de discos (arreglo de discos-espejo, etc.); de fuente (doble fuente de alimentación).		X	Existe únicamente un grupo electrónico para todo el hospital. Sin embargo, no le es asignado a equipos informáticos. La ubicación de los servidores es potencialmente vulnerable a riesgos. Posee únicamente un equipo de aire acondicionado el cual su estado es regular. Copias de seguridad son generadas en una hora determinada programada. Sin embargo, no emplea la técnica por espejo (Mirroring). La energía es únicamente suministrada por una UPS.	• Gerente General de la Red Asistencial La Libertad – RALL • **Jefe de Informática**

OBJETIVOS Y CONTROLES	CUMPLE		OBSERVACIONES / RECOMENDACIONES	RESPONSABLE
	SI	NO		
18. CUMPLIMIENTO				
18.1. Cumplimiento con requisitos legales y contractuales.				
Objetivo: Evitar infracciones de las obligaciones legales, estatutarias, regulatorias (reglamentarias) o contractuales relacionadas a la Seguridad de la Información y a cualquier requisito de seguridad.				
18.1.1. Identificación de requisitos contractuales y la legislación aplicable.				
a) Todos los requisitos pertinentes, legislativos estatutarios, reglamentarios y contractuales, y el planeamiento de la entidad para cumplir con estos requisitos están explícitamente identificados, documentados y protegidos al día para cada Sistema de Información y la Organización.		X	**Observación:** El personal informático conoce del tema. Sin embargo, no posee dicha información ya sea en formato digital o en físico.	• Gerente General de la Red Asistencial La Libertad – RALL • **Jefe de Informática**
18.1.2. Derechos de propiedad intelectual				
a) Se aplica procedimientos apropiados para garantizar el cumplimiento de requisitos legales, reglamentarios y contractuales, relacionados con los derechos de propiedad intelectual y uso de productos de software propietario.		X	**Observación:** El uso de software adquirido por EsSalud es únicamente administrado por el personal informático. Sin embargo, este es administrado únicamente vía local (instalación, modificación y	• Gerente General de la Red Asistencial La Libertad – RALL • **Jefe de Informática**

			ejecución de programas es permitido únicamente mediante Administrador). **Recomendación:** Se debe aplicar políticas en Active Directory (no posee) para una correcta gestión. Concientizar al usuario directo en usar únicamente software licenciado por la institución.	
b) Se establecen en los contratos de trabajo del personal y en los contratos de desarrollo realizados por proveedores y contratistas, cláusulas respecto a la propiedad intelectual de EsSalud, al material y productos generados en el desarrollo del negocio.	X		**Observación:** Existe documentación que avale este acápite. Sin embargo, debe haber una supervisión más profunda al momento de entregar equipamiento informático en garantía a proveedores, ya que información confidencial puede ser expuesta. **Recomendación:**	• Gerente General de la Red Asistencial La Libertad – RALL • **Jefe de Informática**

			Ejemplo: El personal informático debe dar un diagnóstico previo a ser entregado al proveedor para su revisión. Si el equipo presenta fallas en componentes de la placa madre, la información en el disco duro debe ser salvaguardada o en casos especiales retenido por el personal.	
18.1.3. Protección de los registros				
a) Los registros están protegidos contra pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada, de conformidad con los requisitos de legalidad, reglamentarias, contractuales y comerciales.		X	**Observación:** La sala de servidores no se encuentra en un lugar adecuado (ver anexos), debe ser reubicada.	• Gerente General de la Red Asistencial La Libertad – RALL • **Jefe de Informática**
18.1.4. Privacidad y protección de datos personales				
a) Se garantiza la privacidad y la protección de la información de identificación personal a lo dispuesto en la legislación y la reglamentación pertinente en su caso.		X	**Recomendación:** Concientizar al usuario directo a no divulgar o facilitar el acceso a su cuenta que pueda involucrar a la integridad de su información.	• Gerente General de la Red Asistencial La Libertad – RALL • Director • Administrador

				• **Jefe de Informática** • Responsable del Servicio • Usuario directo
18.1.5. Regulación de controles criptográficos				
a) Los controles criptográficos son utilizados en cumplimiento a todos los acuerdos pertinentes, la legislación y los reglamentos.		X	**Recomendación**: Aplicar técnicas en la información, ya que únicamente se presentan en cuentas de usuario en simplicidad.	• Gerente General de la Red Asistencial La Libertad – RALL • **Jefe de Informática**
18.2. Revisiones de Seguridad de Información				
Objetivo: Asegurar que la Seguridad de la Información está implementada y es operada de acuerdo con las políticas y procedimientos organizativos.				
18.2.1. Revisión Independiente de la Seguridad de la Información				
a) El enfoque de la Organización para la Gestión de Seguridad de la Información y su aplicación (es decir, los objetivos de control, controles, políticas, procesos y procedimientos para la Seguridad de la Información) son revisados de forma independiente a intervalos planificados o cuando se produzcan cambios significativos.	X		**Recomendación:** Se debe revisar la información periódicamente en cambios menores y cuando se requiera.	• Gerente General de la Red Asistencial La Libertad – RALL • **Jefe de Informática**

18.2.2. Cumplimiento de Políticas y Normas de Seguridad				
a) La Gerencia Central de Tecnologías de la Información y la Comunicación verifica periódicamente el cumplimiento a las políticas de seguridad, las normas y otros requisitos de seguridad.		X	**Observación:** Se hacen visitas inopinadas (ver anexos - siendo la última vez del 26 al 30 de septiembre del año 2016). **Recomendación:** Comunicación y supervisión periódica más frecuente.	• Gerente General de la Red Asistencial La Libertad – RALL • **Jefe de Informática**
18.2.3. Revisión (Comprobación) del Cumplimiento Técnico				
a) Los sistemas de información son revisados regularmente para cerciorarse que se da cumplimiento a las Políticas y Normas de Seguridad de la Información de la Institución.		X	**Observación:** Los sistemas de información son supervisados por el personal informático mas no se alinean a las Políticas de Seguridad de la Información institucionales.	• Gerente General de la Red Asistencial La Libertad – RALL • **Jefe de Informática**

b) Las situaciones o acciones que violen la Seguridad de la Información son detectadas, registradas, analizadas, resueltas e informadas al Comité de Seguridad de la Información y a las áreas responsables para su tratamiento de manera inmediata.		X	**Observación:** Se registra el uso inadecuado de las cuentas de usuario y de la información mas no se detecta, resuelve ni informa al Comité de Seguridad de la Información. El personal informático es informado por el usuario directo y luego resuelve el problema. **Recomendación:** Automatizar procedimientos.	• Gerente General de la Red Asistencial La Libertad – RALL • **Jefe de Informática**

ANEXO 02

6.2. REGISTRO DE EVIDENCIAS

En este anexo se detallan todas las actividades encontradas de acuerdo a la confidencialidad y disponibilidad en los diversos servicios.

Registro de eventos (agosto – noviembre del 2016)

CONFIDENCIALIDAD

Consulta Externa

MES	NO AUTORIZADO	AUTORIZADO	TOTAL	%
AGOSTO	108	1263	1371	91,44893
SEPTIEMBRE	91	1092	1183	91,66667
OCTUBRE	125	1079	1204	88,4152
NOVIEMBRE	85	1146	1231	92,5829
PROMEDIO	**102,25**	**1145**	**1247,25**	**91,0284**
SUMA	**409**	**4580**	**4989**	

Emergencia – UCI

MES	NO AUTORIZADO	AUTORIZADO	TOTAL	%
AGOSTO	52	793	845	93,44262
SEPTIEMBRE	68	925	993	92,64865
OCTUBRE	90	767	857	88,26597
NOVIEMBRE	80	922	1002	91,32321
PROMEDIO	**72,5**	**851,75**	**924,25**	**91,4201**
SUMA	**290**	**3407**	**3697**	

Hospitalización

MES	NO AUTORIZADO	AUTORIZADO	TOTAL	%
AGOSTO	30	411	441	92,70073
SEPTIEMBRE	21	371	392	94,33962
OCTUBRE	29	380	409	92,36842
NOVIEMBRE	25	340	365	92,64706
PROMEDIO	**26,25**	**375,5**	**401,75**	**93,014**
SUMA	**105**	**1502**	**1607**	

Centro Obstétrico

MES	NO AUTORIZADO	AUTORIZADO	TOTAL	%
AGOSTO	42	678	720	93,80531
SEPTIEMBRE	44	654	698	93,27217
OCTUBRE	37	613	650	93,96411
NOVIEMBRE	28	654	682	95,71865
PROMEDIO	**37,75**	**649,75**	**687,5**	**94,1901**
SUMA	**151**	**2599**	**2750**	

Admisión

MES	NO AUTORIZADO	AUTORIZADO	TOTAL	%
AGOSTO	55	2036	2091	97,29862
SEPTIEMBRE	40	2330	2370	98,28326
OCTUBRE	48	1935	1983	97,51938
NOVIEMBRE	58	1946	2004	97,01953
PROMEDIO	**50,25**	**2061,75**	**2112**	**97,5302**
SUMA	**201**	**8247**	**8448**	

Centro Quirúrgico

MES	NO AUTORIZADO	AUTORIZADO	TOTAL	%
AGOSTO	40	564	604	92,90780142
SEPTIEMBRE	33	651	684	94,93087558
OCTUBRE	27	563	590	95,20426288
NOVIEMBRE	42	464	506	90,94827586
PROMEDIO	**35,5**	**560,5**	**596**	**93,49780393**
SUMA	**142**	**2242**	**2384**	

Farmacia

MES	NO AUTORIZADO	AUTORIZADO	TOTAL	%
AGOSTO	28	1006	1034	97,2167
SEPTIEMBRE	34	1116	1150	96,95341
OCTUBRE	65	1073	1138	93,94222
NOVIEMBRE	41	956	997	95,7113
PROMEDIO	**42**	**1037,75**	**1079,75**	**95,9559**
SUMA	**168**	**4151**	**4319**	

Imagenología

MES	NO AUTORIZADO	AUTORIZADO	TOTAL	%
AGOSTO	45	755	800	94,03974
SEPTIEMBRE	58	637	695	90,89482
OCTUBRE	60	713	773	91,58485
NOVIEMBRE	30	678	708	95,57522
PROMEDIO	**48,25**	**695,75**	**744**	**93,0237**
SUMA	**193**	**2783**	**2976**	

Materno Infantil

MES	NO AUTORIZADO	AUTORIZADO	TOTAL	%
AGOSTO	36	473	509	92,38901
SEPTIEMBRE	46	524	570	91,22137
OCTUBRE	39	514	553	92,41245
NOVIEMBRE	25	535	560	95,3271
PROMEDIO	**36,5**	**511,5**	**548**	**92,8375**
SUMA	**146**	**2046**	**2192**	

DISPONIBILIDAD

Agosto

DIA	HORA	TIEMPO DE PARA (HRS.)	MOTIVO	SERVICIO RESPONSABLE	%
1		0:00			100
2		0:00			100
3	8:35	0:17	REINICIO DE SERVICIOS	ANATOMÍA PATOLÓGICA	98,82
4	11:26	0:11	REINICIO DE SERVICIOS	FARMACIA	99,24
5		0:00			100
6		0:00			100
7		0:00			100
8	13:14	0:41	ACTUALIZACIÓN DEL SISTEMA	INFORMÁTICA	97,15
9		0:00			100
10		0:00			100
11		0:00			100
12		0:00			100
13	10:40	0:14	REINICIO DE SERVICIOS	CENTRO QUIRÚRGICO	99,03
14		0:00			100
15		0:00			100
16		0:00			100
17	8:50	0:23	MANTENIMIENTO CORRECTIVO	INFORMÁTICA	98,40
18		0:00			100
19		0:00			100
20	9:12	0:13	REINICIO DE SERVICIOS	IMAGENOLOGÍA	99,10
21		0:00			100
22		0:00			100
23		0:00			100
24	10:19	0:19	REINICIO DE SERVICIOS	FARMACIA	98,68
25		0:00			100
26		0:00			100
27		0:00			100
28		0:00			100
29		0:00			100
30		0:00			100
31		0:00			100

Septiembre

DIA	HORA	TIEMPO DE PARA (HRS.)	MOTIVO	SERVICIO RESPONSABLE	%
1		00:00			100
2		00:00			100
3	09:53	00:17	REINICIO DE SERVICIOS	FARMACIA	98.82
4		00:00			100
5	10:33	00:23	CORTE ELÉCTRICO	-	98.40
6		00:00			100
7		00:00			100
8		00:00			100
9	09:27	00:15	REINICIO DE SERVICIOS	ANATOMÍA PATOLÓGICA	98.96
10	11:53	00:19	REINICIO DE SERVICIOS	FARMACIA	98.68
11		00:00			100
12		00:00			100
13		00:00			100
14		00:00			100
15		00:00			100
16	15:25	00:11	REINICIO DE SERVICIOS	ANATOMÍA PATOLÓGICA	99.24
17		00:00			100
18		00:00			100
19		00:00			100
20		00:00			100
21		00:00			100
22		00:00			100
23	10:51	02:47	MANTENIMIENTO CORRECTIVO	INFORMÁTICA	88.40
24	13:02	00:37	ACTUALIZACIÓN DEL SISTEMA	INFORMÁTICA	97.85
25		00:00			100
26		00:00			100
27		00:00			100
28	15:10	00:16	REINICIO DE SERVICIOS	IMAGENOLOGÍA	98.89
29		00:00			100
30		00:00			100
31		00:00			100

Octubre

DIA	HORA	TIEMPO DE PARA (HRS.)	MOTIVO	SERVICIO RESPONSABLE	%
1		00:00			100
2		00:00			100
3		00:00			100
4	11:43	00:18	REINICIO DE SERVICIOS	ANATOMÍA PATOLÓGICA	98.75
5		00:00			100
6		00:00			100
7	10:49	00:16	REINICIO DE SERVICIOS	FARMACIA	98.89
8		00:00			100
9		00:00			100
10		00:00			100
11		00:00			100
12		00:00			100
13	15:40	00:34	MANTENIMIENTO CORRECTIVO	INFORMÁTICA	97.64
14	09:47	00:14	REINICIO DE SERVICIOS	CENTRO QUIRÚRGICO	99.03
15		00:00			100
16		00:00			100
17	08:46	00:19	REINICIO DE SERVICIOS	IMAGENOLOGÍA	98.68
18	13:20	00:34	ACTUALIZACIÓN DEL SISTEMA	INFORMÁTICA	97.64
19		00:00			100
20		00:00			100
21		00:00			100
22		00:00			100
23		00:00			100
24		00:00			100
25		00:00			100
26	11:36	00:15	REINICIO DE SERVICIOS	ANATOMÍA PATOLÓGICA	98.96
27		00:00			100
28		00:00			100
29		00:00			100
30		00:00			100
31		00:00			100

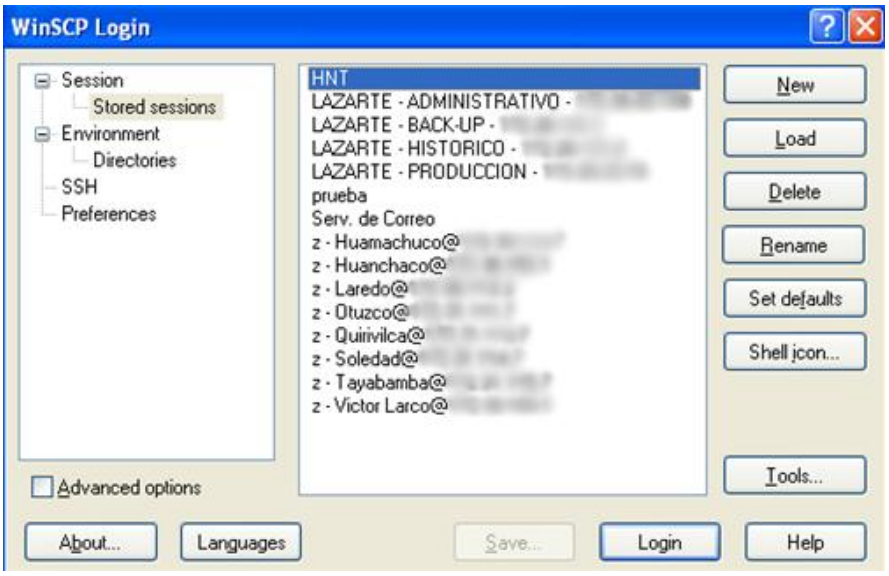
Noviembre

DIA	HORA	TIEMPO DE PARA (HRS.)	MOTIVO	SERVICIO RESPONSABLE	%
1		00:00			100
2		00:00			100
3	09:25	00:14	REINICIO DE SERVICIOS	ANATOMÍA PATOLÓGICA	99.03
4	10:55	00:21	REESTRUCTURACIÓN DE CABLEADO	INFORMÁTICA	98.54
5		00:00			100
6		00:00			100
7		00:00			100
8		00:00			100
9	11:39	00:15	REINICIO DE SERVICIOS	FARMACIA	98.96
10		00:00			100
11		00:00			100
12		00:00			100
13	14:12	00:13	REINICIO DE SERVICIOS	FARMACIA	99.10
14		00:00			100
15		00:00			100
16		00:00			100
17	11:07	00:12	REINICIO DE SERVICIOS	ANATOMÍA PATOLÓGICA	99.17
18		00:00			100
19		00:00			100
20	11:54	03:24	MANTENIMIENTO CORRECTIVO	INFORMÁTICA	87.22
21	13:17	00:38	ACTUALIZACIÓN DEL SISTEMA	INFORMÁTICA	97.36
22	12:15	00:18	REINICIO DE SERVICIOS	IMAGENOLOGÍA	98.75
23		00:00			100
24		00:00			100
25		00:00			100
26		00:00			100
27		00:00			100
28	16:20	00:19	REINICIO DE SERVICIOS	ANATOMÍA PATOLÓGICA	98.68
29		00:00			100
30		00:00			100
31		00:00			100

ANEXO 03

6.3. PROCESO DE RESPALDO Y RECUPERACIÓN

Acceso a Servidores y Almacenamiento de Copias de Seguridad



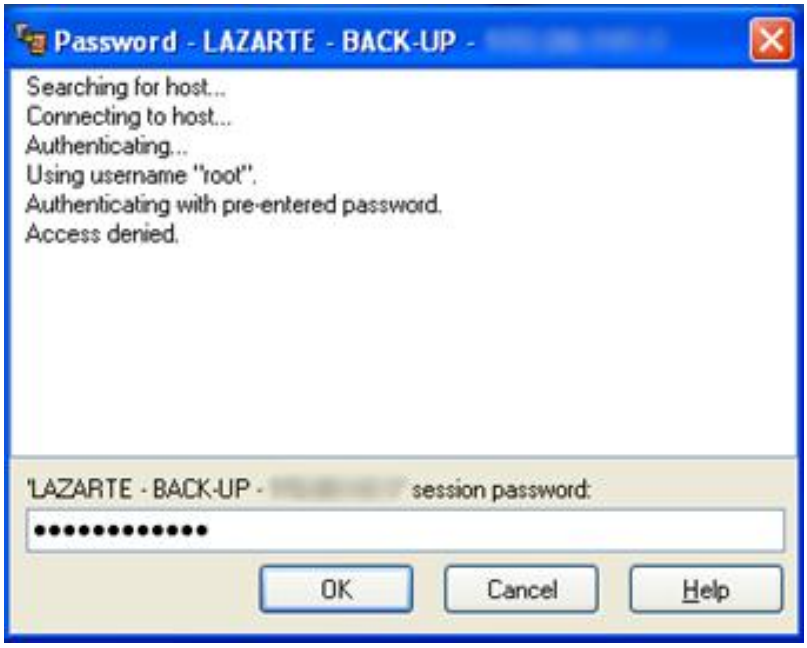
Servidores locales.

- LAZARTE – ADMINISTRATIVO
- LAZARTE – BACK-UP
- LAZARTE – HISTÓRICO
- LAZARTE – PRODUCCIÓN
- SERV. DE CORREO

Servidores externos.

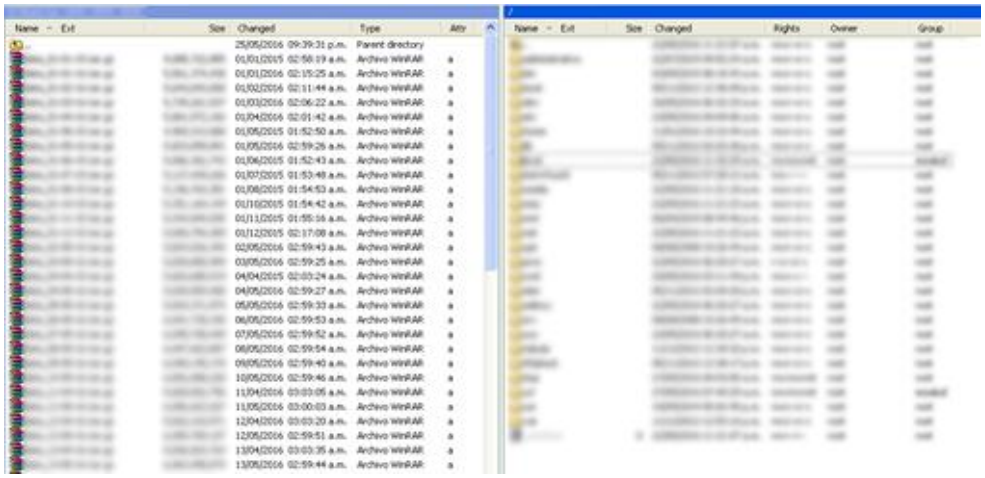
- Z-HUAMACHUCO
- Z-HUANCHACO
- Z-LAREDO
- Z-OTUZCO
- Z-QUIRUVILCA
- Z-SOLEDAD
- Z-TAYABAMBA
- Z-VICTOR LARCO

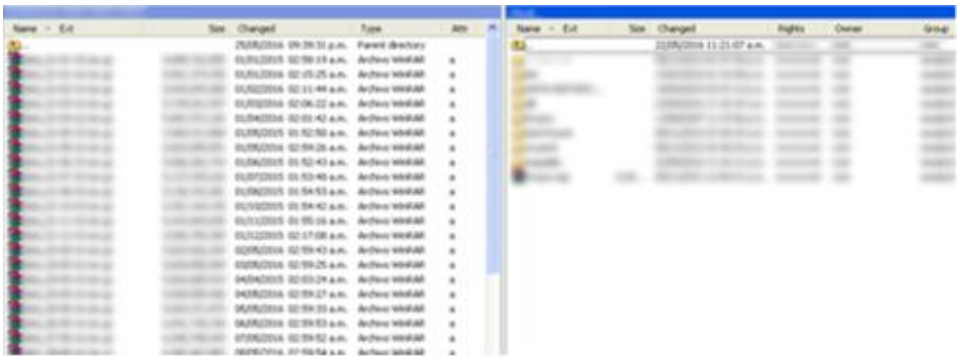
Acceso al directorio de copias de seguridad.



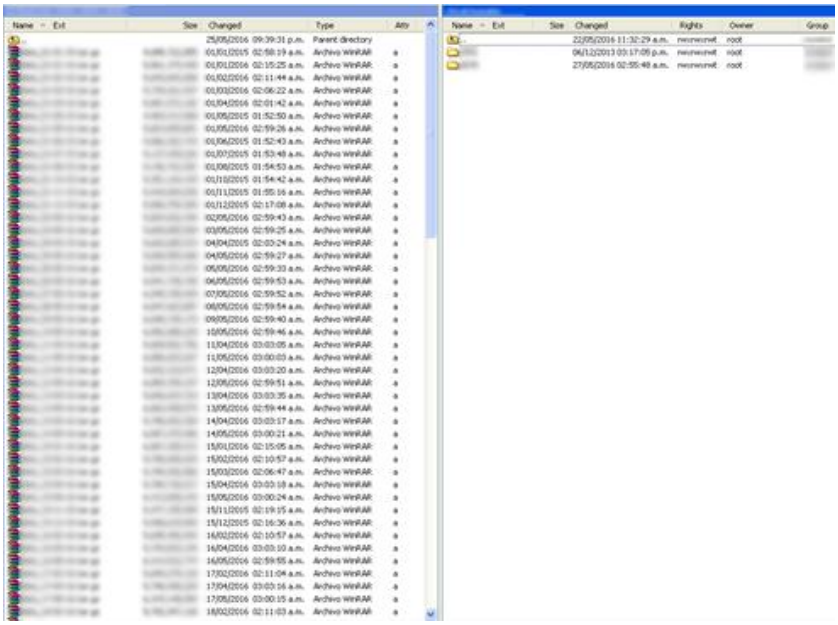
Interfaz y repositorio de copias de seguridad

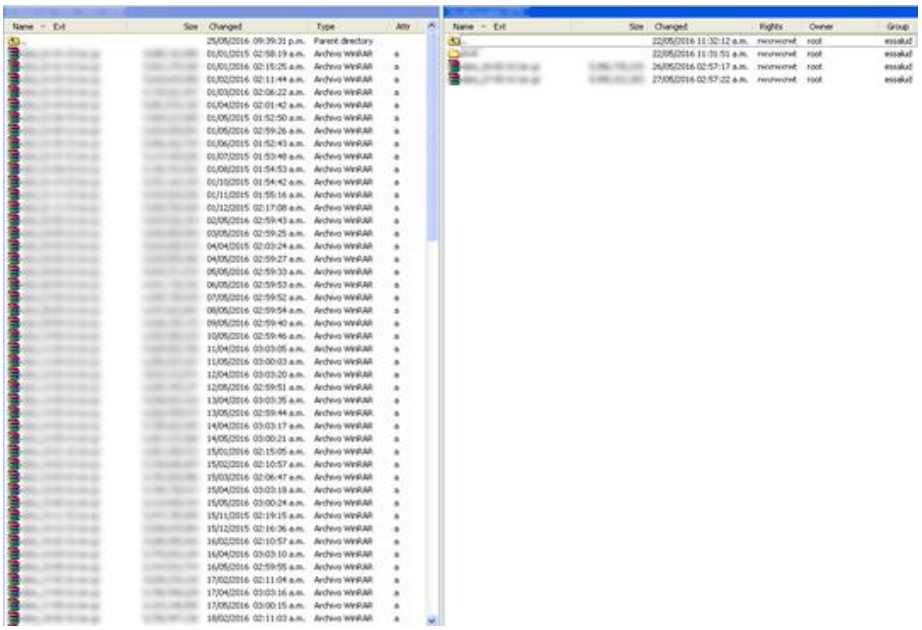
(A la izquierda: directorio local y a la derecha: servidor)



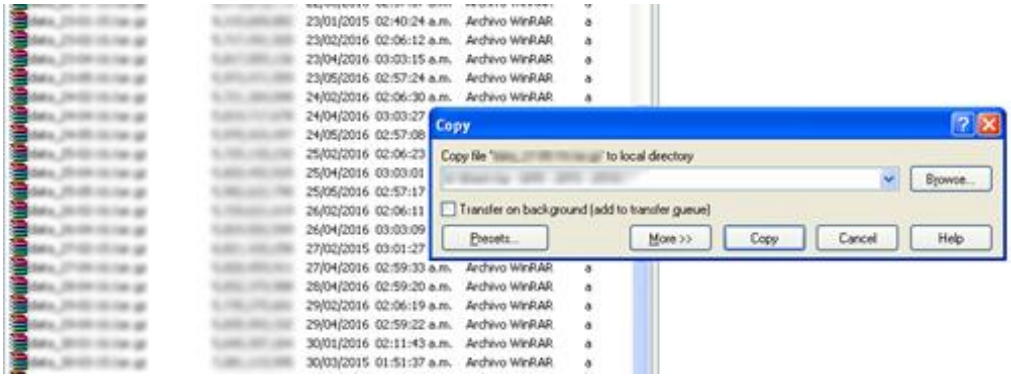


A la derecha: ubicación de copias de seguridad generadas.

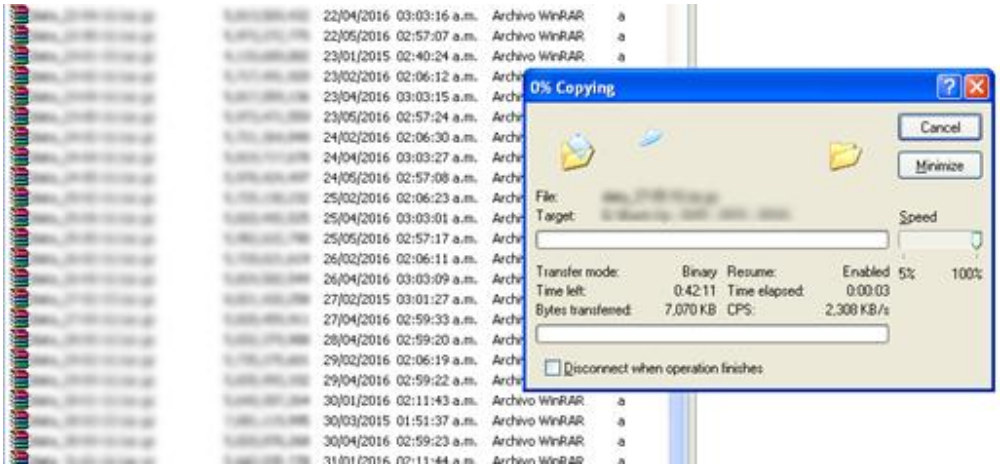




Copia y almacenamiento de copias de seguridad.



Almacenamiento de copia de seguridad

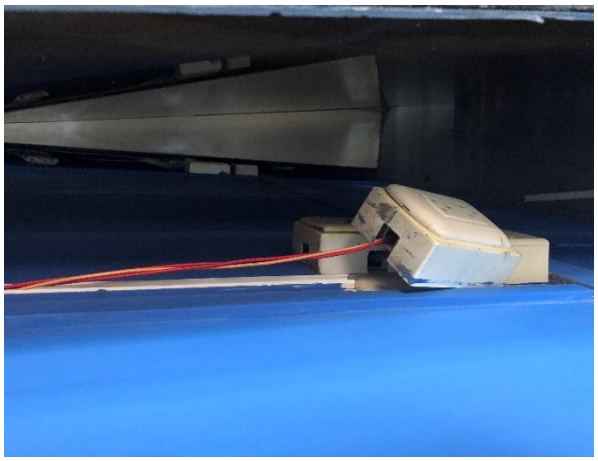


ANEXO 04

6.4. COMUNICACIONES

Switches en varios ambientes se encuentran expuestos y en pésimas condiciones: en muchas ocasiones se pueden observar sin gabinete alguno que los proteja y cierto cableado se encuentra cortado.

Debido a ello, informática informó que es complicado ejecutar mantenimiento de carácter preventivo ya que no hay identificación y clasificación de cableado por lo que las observaciones se van levantando de carácter correctivo.

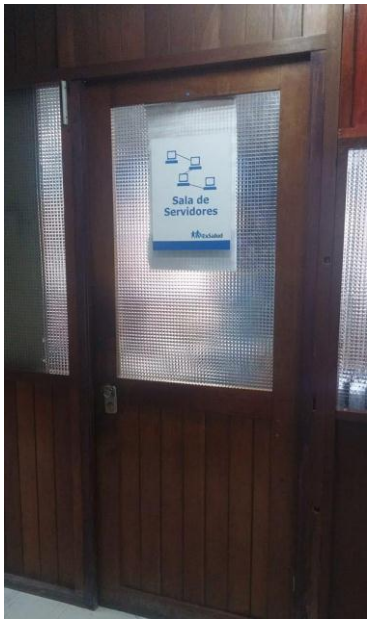


Se pudo comprobar en los siguientes ambientes repetidas veces lo siguiente:

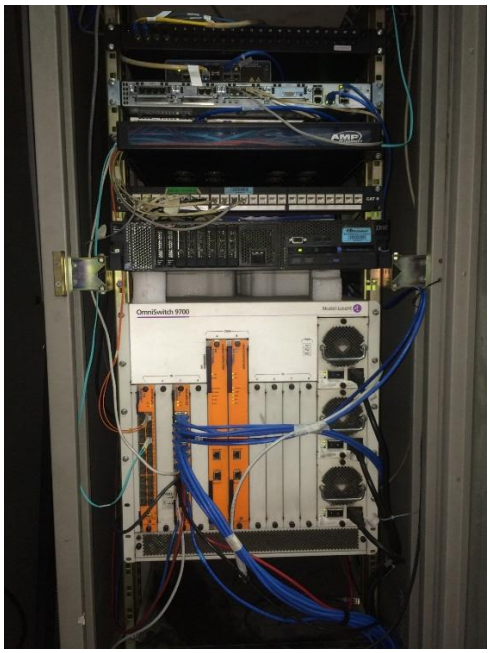
- Extintores: Algunos no tenían tarjeta de mantenimiento, otras se encontraban correctamente aseguradas y en otros casos no había equipo alguno.
- Tablero eléctrico: se pudo comprobar que tableros eléctricos están expuestos sin seguridad y al alcance de cualquier persona.
- Conexiones eléctricas: En muchas ocasiones se pudo apreciar el mal estado de inturruptores eléctricos y su cableado en pésimo estado de conservación.

ANEXO 05

6.5. SALA DE SERVIDORES: ANTES DEL DISEÑO



Ambiente donde se ubica la Sala de Servidores no cumple con los requerimientos mínimos establecidos: delimitación y seguridad.



Comunicaciones en Sala de Servidores inadecuada: cables expuestos y mal distribuidos tanto cableado UTP como de fibra óptica además del mal aseguramiento del gabinete, puesto que no está protegido.

Servidores se encuentran sin protección y ubicados únicamente sobre una mesa produciendo una alta probabilidad de riesgo y eventos no deseados.

Como se puede observar, el monitor multientrada para los servidores se encuentra encima del servidor principal.

Servidores secundarios (respaldo, telefonía y mensajería) y el teclado principal se ubican uno encima de otro.

ANEXO 06

6.6. SALA DE SERVIDORES: DESPUÉS DEL DISEÑO

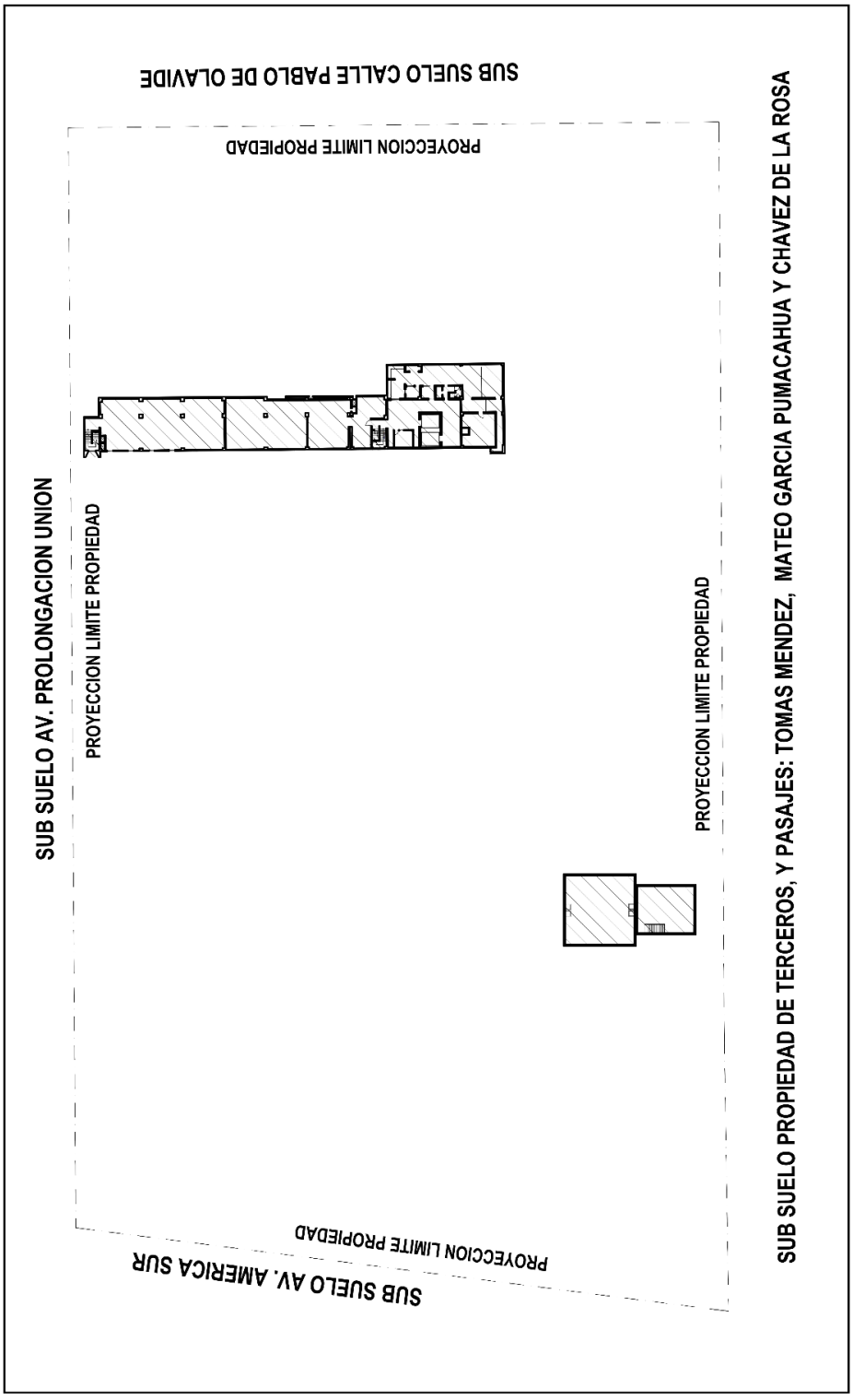
Se distribuyó e identificó el cableado, organizándolo de acuerdo a su ubicación mas no se corrigió la sobreexposición de estas debido a la limitación de interrupción de servicios.

Se adquirió un gabinete para uso exclusivo de los servidores, tanto principal como secundarios.

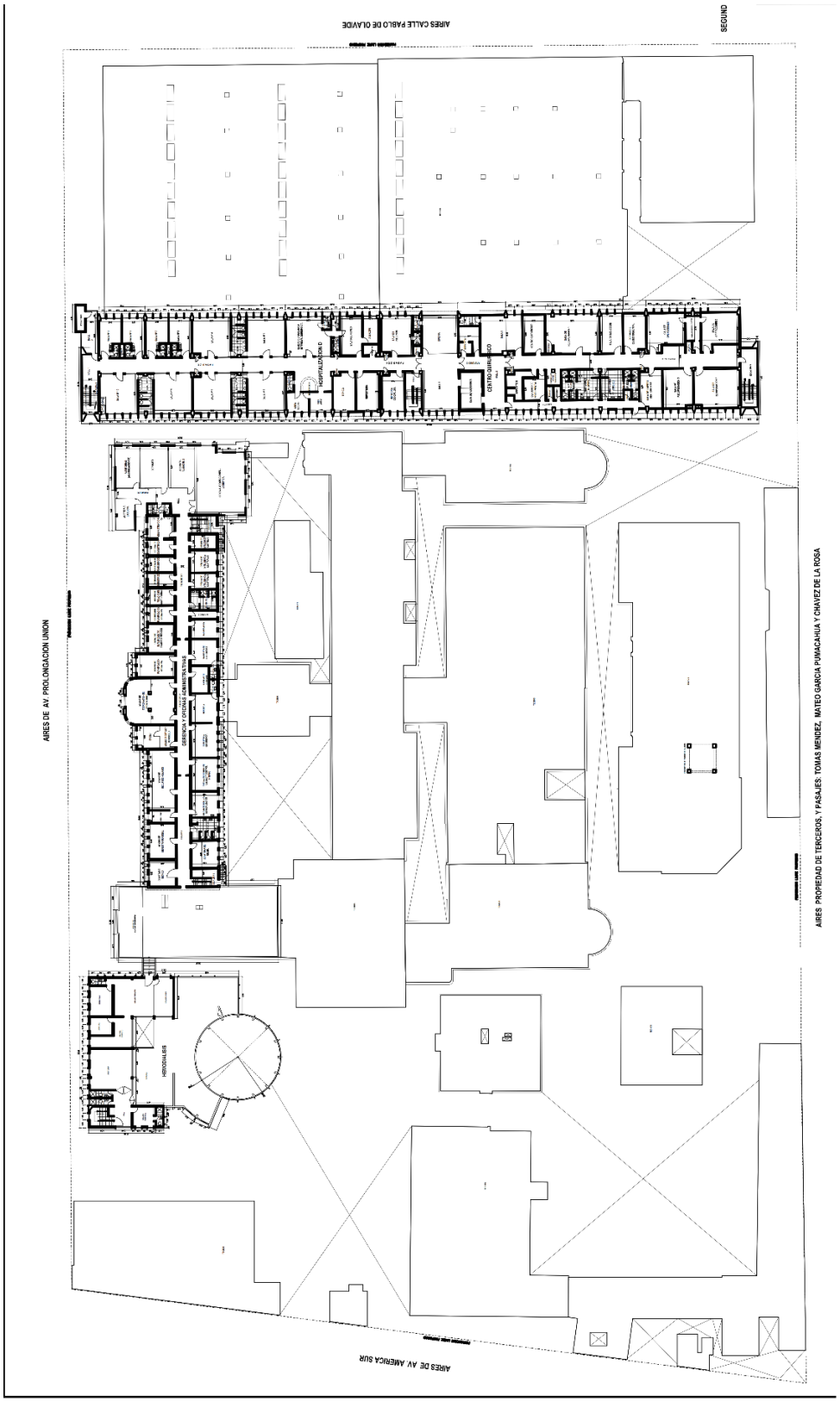
Se implementó seguridad tanto para el gabinete como para los servidores (seguridad independiente).

ANEXO 07

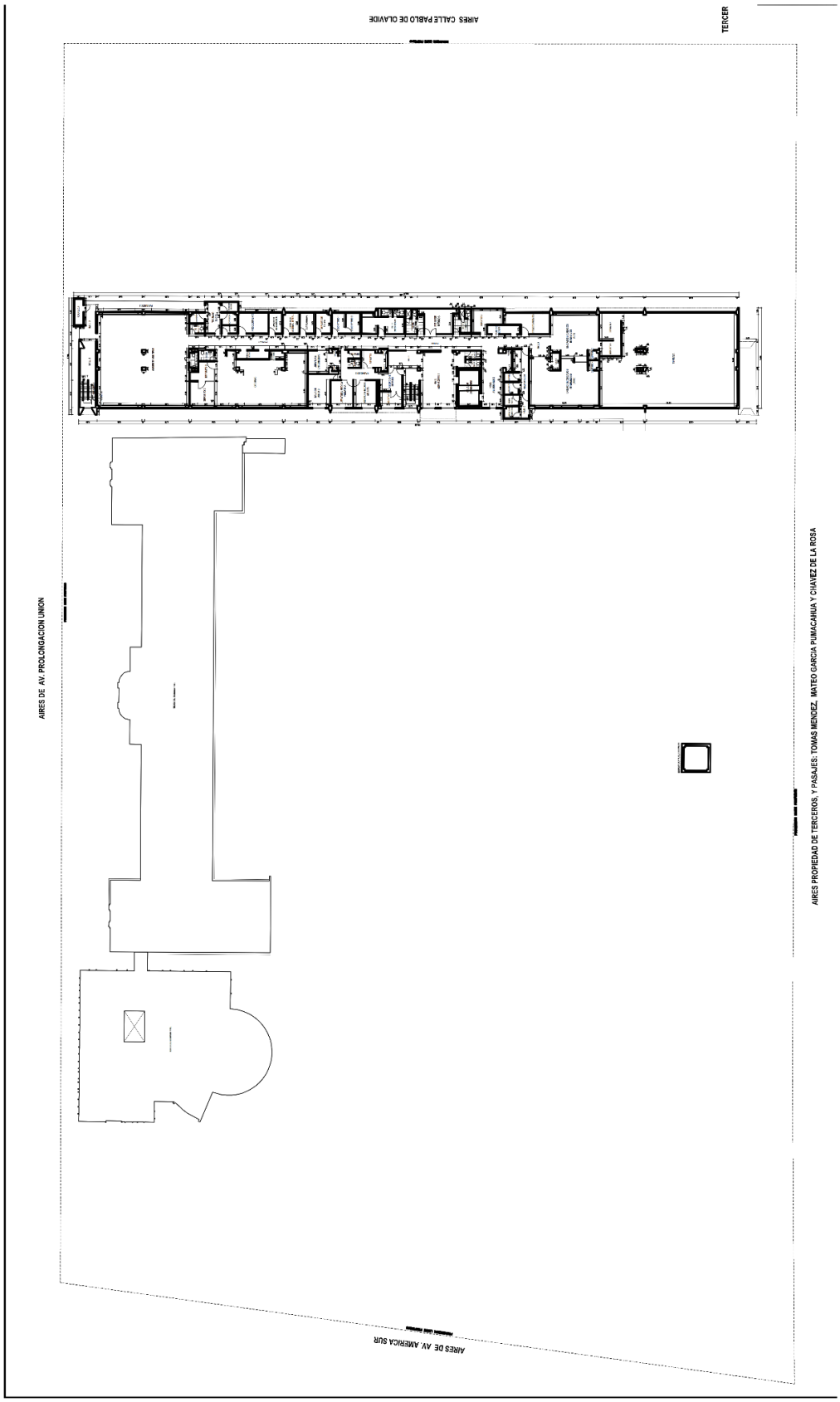
6.7. DELIMITACIÓN Y UBICACIÓN DE SERVICIOS



Sub suelo: Debajo de la Sala de Servidores se encuentran ambientes pertenecientes a Farmacia y Central de Esterilización (Av. Prolongación Unión y Calle Pablo de Olavide).



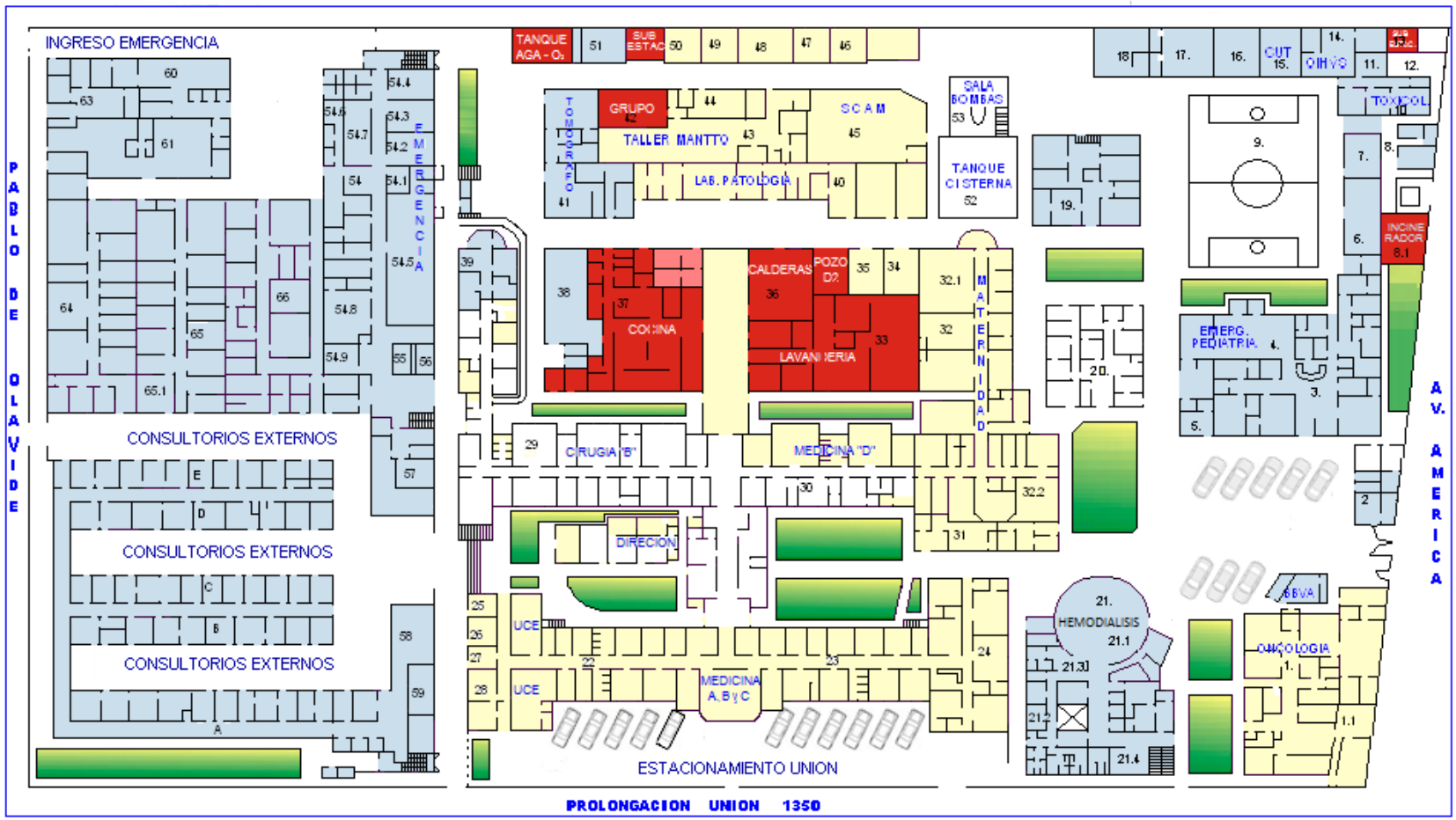
Primer piso: La entrada a Sala de Servidores es por la puerta de la Av. Prolongación Unión. Está limitado con el servicio de Admisión y Consulta Externa.



Segundo piso: Sala de Servidores limita con Hospitalización.

HOSPITAL IV "VICTOR LAZARTE ECHEGARAY"

DISTRIBUCION DE AMBIENTES - PRIMER PISO



ANEXO 08

6.8. ACREDITACIÓN DE ESTUDIO

EsSalud

"AÑO DE LA LUCHA CONTRA LA CORRUPCIÓN Y LA IMPUNIDAD"

Viernes, 19 de julio del 2019

CARTA N° 891 - D-HE-VLE-G-ESSALUD-2019

Dr. Luis Vladimir Urrelo Huiman
Director de la Escuela Profesional de Ingeniería de Computación y Sistemas
Universidad Privada Antenor Orrego

PRESENTE. -

ASUNTO: ACREDITACIÓN DE ESTUDIO

Mediante la presente, se acredita el estudio realizado por el Bachiller en Ingeniería de Sistemas, **Luis Alejandro Poma Rosales** en el **Hospital Especializado Víctor Lazarte Echegaray**, perteneciente a la Red Asistencial La Libertad durante los meses de agosto-diciembre del 2016 y enero-febrero del 2019.

Se le brindó el acceso a diversos servicios del Hospital y además la información requerida por Informática e Ingeniería Hospitalaria con el propósito de recopilar evidencias y sustentar con pruebas los eventos relacionados a la seguridad de la información.

El motivo del estudio es la elaboración de la tesis titulada "**Plan de Mejora de la Seguridad de la Información del Seguro Social de Salud – EsSalud aplicando el estándar ISO/IEC 27001: Seguridad de la Información"**.

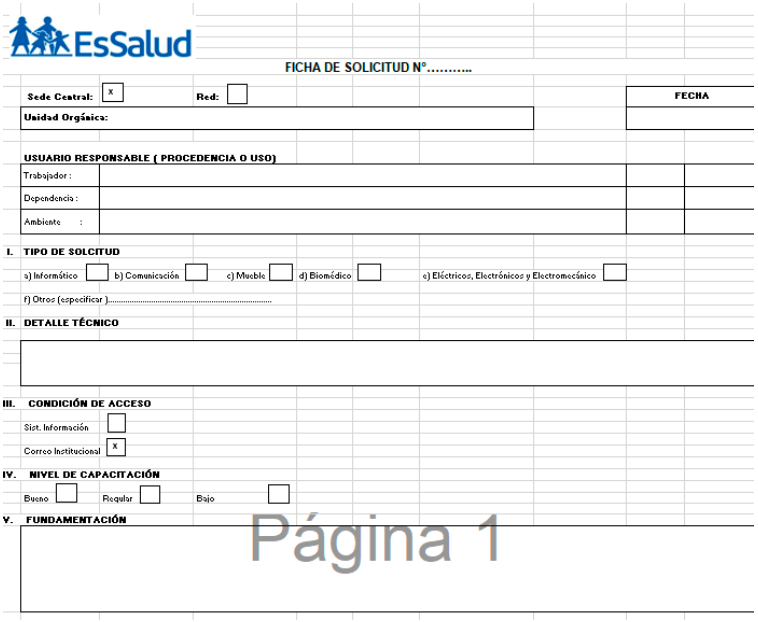
Sin otro particular, quedo de Ud.
Atentamente

DRA. TANIA R. RODAS MALCA
DIRECTOR
CMP. 26981
Hospital Especializado "Víctor Lazarte Echegaray"
EsSalud

AREA AÑO CORRELATIVO
NIT 1457 2019 4847

ANEXO 09

6.9. PLAN DE MEJORA: DOCUMENTACIÓN



EsSalud

FICHA DE SOLICITUD N°.....

Sede Central: X Red: FECHA

Unidad Orgánica:

USUARIO RESPONSABLE (PROCEDENCIA O USO)

Trabajador :

Dependencia :

Ambiente :

I. TIPO DE SOLCITUD

a) Informático b) Comunicación c) Mueble d) Biomédico e) Eléctricos, Electrónicos y Electromecánico

f) Otros (especificar).....

II. DETALLE TÉCNICO

III. CONDICIÓN DE ACCESO

Sist. Información

Correo Institucional X

IV. NIVEL DE CAPACITACIÓN

Bueno Regular Bajo

V. FUNDAMENTACIÓN

La ficha de solicitud diseñada debe comprender lo siguiente:

- Datos de la persona solicitante (hospital, servicio, ubicación).
- Tipo de acceso y su alcance.
- Datos del usuario beneficiado.
- Nivel de capacitación del usuario.
- Fundamentación para permiso / acceso.

SERVICIO	UBICACIÓN	COD. PAT.	DESCRIPCIÓN	MODELO	MARCA	SERIE	ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC
CONSULTA EXTERNA	CE ODONTOESTOMATOLOGÍA 1						X			X			X			X		
CONSULTA EXTERNA	CE ODONTOESTOMATOLOGÍA 2						X			X			X			X		
CONSULTA EXTERNA	CE GASTROENTEROLOGÍA 1						X			X			X			X		
CONSULTA EXTERNA	CE GASTROENTEROLOGÍA 2						X			X			X			X		
CONSULTA EXTERNA	CE MEDICINA GENERAL						X			X			X			X		
CONSULTA EXTERNA	CE CARDIOLOGÍA 1						X			X			X			X		
CONSULTA EXTERNA	CE CARDIOLOGÍA 2						X			X			X			X		
CONSULTA EXTERNA	CE NEUROLOGÍA						X			X			X			X		
CONSULTA EXTERNA	CE NEUMOLOGÍA						X			X			X			X		
CONSULTA EXTERNA	CE NEFROLOGÍA							X			X			X			X	
CONSULTA EXTERNA	CE MEDICINA FÍSICA Y REHABILITACIÓN 1							X			X			X			X	
CONSULTA EXTERNA	CE MEDICINA FÍSICA Y REHABILITACIÓN 2							X			X			X			X	
CONSULTA EXTERNA	FISIOTERAPIA 1							X			X			X			X	
CONSULTA EXTERNA	FISIOTERAPIA 2							X			X			X			X	
CONSULTA EXTERNA	CE OFTALMOLOGÍA 1							X			X			X			X	
CONSULTA EXTERNA	CE OFTALMOLOGÍA 2							X			X			X			X	
CONSULTA EXTERNA	CE OFTALMOLOGÍA 3							X			X			X			X	
CONSULTA EXTERNA	CE OFTALMOLOGÍA 4							X			X			X			X	
CONSULTA EXTERNA	CE OTORRINOLARINGOLOGÍA 1								X			X			X			X
CONSULTA EXTERNA	CE OTORRINOLARINGOLOGÍA 2								X			X			X			X
CONSULTA EXTERNA	CE OTORRINOLARINGOLOGÍA 3								X			X			X			X
EMERGENCIA	EMERGENCIA - ADMISIÓN								X			X			X			X
EMERGENCIA	EMERGENCIA - TRAUMA SHOCK								X			X			X			X
EMERGENCIA	EMERGENCIA - OBSERVACIÓN								X			X			X			X
EMERGENCIA	EMERGENCIA - TÓPICO								X			X			X			X
EMERGENCIA	EMERGENCIA - TRIAJE								X			X			X			X
ADMISIÓN	ADMISIÓN - PROGRAMACIÓN								X			X			X			X

El programa de mantenimiento preventivo de equipos informáticos debe estar organizado por servicio, luego por ubicación y tipo de bien. El periodo de mantenimiento debe ser de carácter trimestral para asegurar la continuidad del equipo en el servicio.

6.10. TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS

CHECKLIST

Objetivo	**Evaluar la Tecnología de Información implementada y/o implantada para identificar los riesgos tecnológicos existentes**		
Actividad	Revisar los procedimientos relativos a altas, bajas, transferencias y cambios en el hardware de TI		
Cuestionario			
Pregunta	**SI**	**NO**	**N/A**
¿Se cuenta con un inventario de todos los equipos que integran el centro de cómputo?			
¿Con cuanta frecuencia se revisa el inventario?			
¿Se posee de bitácoras de fallas detectadas en los equipos?			
Características de la bitácora (señale las opciones).			
¿La bitácora es llenada por personal especializado? ¿Señala fecha de detección de la falla? ¿Señala fecha de corrección de la falla y revisión de que el equipo funcione correctamente? ¿Se poseen registros individuales de los equipos? ¿La bitácora hace referencia a hojas de servicio, en donde se detalla la falla, y las causas que la originaron, así como las refacciones utilizadas?			
¿Se lleva un control de los equipos en garantía, para que a la finalización de ésta, se integren a algún programa de mantenimiento?			
¿Se cuenta con servicio de mantenimiento para todos los equipos?			
¿Con cuanta frecuencia se realiza mantenimiento a los equipos?			
¿Se cuenta con procedimientos definidos para la adquisición de nuevos equipos?			
¿Se tienen criterios de evaluación para determinar el rendimiento de los equipos a adquirir y así elegir el mejor?			
¿Se lleva un control de los equipos en garantía, para que a la finalización de ésta, se integren a algún programa de mantenimiento?			
¿Se cuenta con servicio de mantenimiento para todos los equipos?			
¿Con cuanta frecuencia se realiza mantenimiento a los equipos?			
¿Se cuenta con procedimientos definidos para la adquisición de nuevos equipos?			
¿Se tienen criterios de evaluación para determinar el rendimiento de los equipos a adquirir y así elegir el mejor?			
Documentos probatorios presentados:			

Objetivo	**Analizar y evaluar la seguridad de acceso al centro de cómputo principal de la organización.**			
Actividades	Revisar el acceso por la puerta principal al local donde se encuentra el centro de cómputo principal.			
Cuestionario				
Pregunta		**SI**	**NO**	**N/A**
¿Se cuenta con sistemas de seguridad para impedir el paso al local?				
¿Se toma nota de los datos del visitante?				
Documentos probatorios presentados:				

Objetivo	**Analizar y evaluar la seguridad de acceso al centro de cómputo principal de la organización.**			
Actividades	Revisar el procedimiento en recepción para otorgar tickets de visitante y permitir el acceso a las instalaciones del local.			
Cuestionario				
Pregunta		**SI**	**NO**	**N/A**
¿Se otorga algún tipo de identificación a los visitantes?				
¿Existen lugares de acceso restringido?				
¿Se cuenta con sistemas de seguridad para impedir el paso a lugares de acceso restringido?				
Documentos probatorios presentados:				

Objetivo	**Analizar y evaluar la seguridad de acceso al centro de cómputo principal de la organización.**			
Actividades	Revisar el acceso por la entrada al centro de cómputo principal.			
Cuestionario				
Pregunta		**SI**	**NO**	**N/A**
¿Se cuenta con sistemas de seguridad para impedir el paso al DataCenter?				
¿A este mecanismo de seguridad se le han detectado debilidades?				
¿Tiene medidas implementadas ante la falla del sistema de seguridad?				
¿Con cuanta frecuencia se actualizan las claves o credenciales de acceso?				
¿Se tiene un registro de las personas que ingresan al DataCenter?				
¿Se tienen sistemas de seguridad para evitar que se sustraiga equipo de las instalaciones?				
¿Existen prohibiciones para fumar, consumir alimentos y bebidas?				
¿Con cuanta frecuencia se limpian las instalaciones?				
¿Con cuanta frecuencia se limpian los ductos de aire y la cámara de aire que existe debajo del piso falso (si existe)?				
Documentos probatorios presentados				

	CONTROLES DE OPERACIONES Y MANTENIMIENTO DE EQUIPOS	SI	NO	N/A	OBSERVACIONES
1.-	Se elabora periódicamente un plan de renovación de equipos				
2.-	Se lleva un control de inventario de hardware de la entidad				
3.-	El control de inventario contempla información detallada de las características y componentes del equipo inventariado				
4.-	El mantenimiento de los equipos de cómputo se da por funcionarios internos				
5.-	Se le da mantenimiento de tipo preventivo a los equipos de cómputo				
6.-	El mantenimiento correctivo del equipo de cómputo se tiene contratado externamente				
7.-	Se lleva un control de las garantías del equipo de cómputo para saber cuál de estos cuentan con esta cobertura.				
8.-	Se cuenta con las licencias del software que se utiliza en la entidad				
9.-	Se lleva un inventario del software que se encuentra instalado en todas las computadoras de la entidad				
10.-	¿Se evalúa el rendimiento del personal directivo y operativo?				
11.-	Se efectúa en forma anual una evaluación de mantenimiento y de proveedores?				
12.-	¿Cuál es la cobertura de los seguros contratados?				
13.-	¿Existe una bitácora sobre el uso de los computadores y su posterior evaluación del tipo de utilización?				
14.-	¿Se cumple con la bitácora de los procedimientos que cumple el operador, durante el día y está es revisada				
	por el supervisor inmediato o el Gerente de sistemas?				
15.-	¿Existe la bitácora sobre el mantenimiento que se le da a los equipos, con la novedades correspondientes?				
16.-	¿Existen procedimientos escritos sobre la actualización de archivos?				
17.-	¿Existen procedemientos por escrito sobre la utilización de las librerías?				
18.-	¿Existen programas de control y revisión sobre los archivos manejados por el usuario?				
19.-	¿Está prohibido la operación del equipo de analistas y programadores?				
20.-	¿Los operadores del equipo conocen de la lógica de los programas a tal punto que puedan hacer cambios o actualizaciones?				
21.-	¿Se ha creado archivos que proporcionen pistas para la intervención posterior de Auditoría?				

	CONTROLES PARA EL ANÁLISIS, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN	SI	NO	N/A	OBSERVACIONES
1.-	¿Se ha determinado alguna metodología de los estándares para diseño de sistemas?				
2.-	¿Existen estudios de factibilidad?				
3.-	¿Se han elaborado planes de diseño, desarrollo de la implantación de sistemas?				
4.-	¿Se han diseñado, sistemas integrados de información?				
5.-	¿Qué procedimiento se utiliza para los estudios de Costo - Beneficio.?				
6.-	¿Cuál es la política de costo utilizada?				
7.-	¿Se cumplen los planes de procesamiento de datos comparando lo ejecutado con lo planeado.?				
8.-	¿Participan los auditores internos en los procesos de planificación para expresar sus necesidades.?				
9.-	¿Existe una metodología escrita para el análisis desarrollo de implantación de sistemas?				
10.-	¿Existen planes para adquisiciones futuras de equipos.?				
11.-	¿Se aplican los procedimientos para planificar software?				
12.-	¿Participa auditoría en el desarrollo de sistemas?				
13.-	¿Se han diseñado procedimientos estándares para todas las áreas usuarias?				
14.-	¿Es el usuario el responsable del ingreso de los datos?				
15.-	¿Se ha efectuado una racionalización de los formularios que facilite el ingreso de datos?				
16.-	¿Se han incluido en los sistemas cifras de control que facilite detectar inconsistencias durante el proceso?				
17.-	¿Los planes de procesamiento de datos están adecuadamente coordinados con los planes generales de la institución.?				
18.-	¿Se cumplen los planes de desarrollo de sistemas?				
19.-	¿Las modificaciones de los programas se realizan de acuerdo a los estándares existentes?				
20.-	¿Los usuarios revisan y prueban los resultados de los cambios antes de su implantación?				
21.-	¿Qué criterio de selección se utilizó para el uso del lenguaje de programación?				
22.-	¿Existe documentación de los programas, cuales son los documentos que la forman?				
23.-	¿Existe un procedimiento de actualización?				
24.-	¿En caso de cambios o actualizaciones de programas existe la documentación necesaria que respalde dichos cambios?				
25.-	¿Existen controles adecuados establecidos para solicitar y aprobar los cambios a los programas?				
26.-	¿Existen normas estándares para la codificación de los programas?				

	ASPECTOS GENERALES DEL SISTEMA	SI	NO	N/A	OBSERVACIONES
1.-	El sistema fue desarrollado internamente				
2.-	El mantenimiento del Sistema lo dan funcionarios de la Entidad				
3.-	El Sistema es una aplicación desarrollada a la medida				
4.-	El Sistema está desarrollado con base en un lenguaje de programación que es estándar de la Entidad				
5.-	El Sistema está desarrollado con base en una plataforma de base de datos que es estándar para la entidad				
6.-	El Sistema tiene menos de cinco años de funcionamiento				
7.-	El Sistema es integrado con otras aplicaciones automatizadas de la municipalidad				
8.-	El Sistema ha sido auditado ya sea por la Auditoría Interna o por una firma externa				
11.-	¿Los cambios, modificaciones, o nuevos programas son autorizados antes de proceder a su realización?.				
12.-	¿Existen cronogramas de trabajo para el personal , tanto de operaciones como programación y análisis?.				
13.-	¿Si la respuesta anterior es afirmativa, quienes son los responsables de la evaluación de su cumplimiento?.				
14.-	¿La elaboración y desarrollo de los programas es efectuado en una librería de pruebas, independiente de				
	la librería de programas en línea?.				
15.-	¿Se documenta adecuadamente cualquier cambio o modificación al un sistema ?.				
16.-	¿Existe un inventario actualizado de los manuales y documentación del sistema?.				
21.-	¿Se da mantenimiento al sistema en forma regular?.				
22.-	¿Está integrado el sistema en un todo?.				
23.-	¿Existen procedimientos escritos y detallados con instrucciones concretas acerca del uso del sistema?.				
24.-	¿Está cada usuario o grupo de usuarios provistos de una palabra clave o código secreto de seguridad?.				
25.-	¿Se cambia las claves de seguridad cada que tiempo y quienes son los responsables de hacerlo?.				
26.-	¿El acceso a las palabras claves o secretas es restringido?.				
27.-	Cuando se da el retiro de alguna persona del Centro de Cómputo, o de cualquier otro departamento, ¿Cuál es el				
	Procedimiento que se aplica sobre las claves de seguridad asignadas?				
28.-	¿Las fallas de funcionamiento el sistema son documentadas y revisadas adecuadamente?				
30.-	¿Existen procedimientos escritos para descargar o restaurar información al computador?				
31.-	¿Emite el sistema un listado de control donde se especifique la hora, la fecha, los módulos utilizados y los usuarios				
	respectivos ?				
36.-	¿Hay procedimientos y controles para detectar un intento de ingresar al computador por parte de personas no autorizadas ?.				

	SEGURIDADES FISICAS	SI	NO	N/A	OBSERVACIONES
1.-	Cuenta el sistema con un regulador de voltaje?				
2.-	Si la respuesta a la pregunta anterior es sí, ¿está funcionando adecuadamente?				
3.-	¿Cuenta el sistema con una fuente de poder capaz de dar energía al computador cuando se suprime la corriente eléctrica?				
4.-	Si la respuesta a la pregunta anterior es sí, ¿Está funcionando adecuadamente?, indique en observaciones				
	cuantos minutos de energía le da al computador.				
5.-	¿La instalación eléctrica del CPD, tiene conexión a tierra?				
6.-	¿Existe en el centro de cómputo extintor de incendio?				
7.-	Si la respuesta a la pregunta anterior es sí, ¿Está dentro del período de carga y con la presión adecuada?				
8.-	Cuenta el sistema con un equipo de aire acondicionado adecuado?				
9.-	¿Se mide con frecuencia la temperatura y la humedad?				
10.-	¿Las instalaciones de CPD se encuentran en un lugar funcional?				
11.-	¿Las líneas eléctricas de CPD son independientes del resto de la instalación eléctrica?				
12.-	¿Tienen protección para sobre cargas?				
13.-	¿Existe un sistema adecuado de detección de incendios?				
14.-	Existen reglas y letreros que indiquen: "Prohibición de fumar", " Prohibición de ingreso a personal no autorizado"				
15.-	¿Está restringido el acceso al CPD?				
16.-	¿Tiene el departamento de CPD alguna puerta de escape y ésta puede ser utilizada como entrada?				
17.-	¿Existe algún plan de seguridad de emergencia escrito y aprobado?				
18.-	¿Existen pólizas de seguros contratadas y éstas qué tipo de riesgo cubren?				
19.-	¿Existe un mantenimiento adecuado y periódico a los equipos de computación?				
20.-	¿Existe algún manual o reglamento que trate acerca de la seguridad física del CPD?				
21.-	¿Existe alguna librería con llave para guardar los manuales y documentos de los programas y aplicaciones?				
22.-	¿Copia de estos manuales se entregan para que sean guardados en otro lugar fuera de la empresa,				
	en caso de algún siniestro?				
23.-	En caso que la respuesta anterior sea sí, ¿las llaves y copias por quién se encuentran custodiadas?				
24.-	¿Existe algún tipo de control de acceso al Dpto. de CPD? Si existe alguno descríbalo brevemente en observaciones?				
25.-	Se tiene algún control de entrada/salida del personal No Autorizado?				
26.-	¿Se cuenta con alguna área definida de Cintoteca o Discoteca?				
27.-	Esta área es de acceso restringido?				
28.-	Se tiene un procedimiento para el control de Entrada/Salida de información de esta área?				

CUESTIONARIO

1. ¿El lugar donde se ubica el centro de cómputo está seguro de inundaciones, robo o cualquier otra situación que pueda poner en peligro los equipos? Si _____ No _____

2. ¿El centro de cómputo da hacia el exterior? Si _____ No _____

3. ¿El material con que está construido el centro de cómputo es confiable? Si _____ No _____

4. ¿Dentro del centro de cómputo existen materiales que puedan ser inflamables o causar algún daño a los equipos?
Si _____
¿Cuál?_____ No_____

5. ¿Existe lugar suficiente para los equipos? Si _____ No _____

6 .¿Aparte del centro de cómputo se cuenta con algún lugar para almacenar otros equipos de cómputo, muebles, suministros, etc.? Si _____
¿Dónde? _____ No ____

7. ¿Se cuenta con una salida de emergencia? Si _____ No _____

8. Existen señalamientos que las hagan visibles? Si _____
¿Dónde? _____ No _____

9. ¿Es adecuada la iluminación del centro de cómputo? Si _____ No _____
¿Por qué? _____

10. ¿El color de las paredes es adecuado para el centro de cómputo? Si _____ No _____
¿Por qué?_____

11. ¿Existen lámparas dentro del centro de cómputo? Si _____
¿Cuántas?_____ No _____

12. ¿Qué tipo de lámparas utilizan?

	CONTROLES A LAS BASES DE DATOS	**SI**	**NO**	**N/A**	**OBSERVACIONES**
1.-	¿Se tiene definido un área o persona para la administración de la base de Datos en la entidad?				
2.-	¿Se tienen definidos perfiles de acceso para los funcionarios en la base de datos aparte de los del sistema?				
3.-	¿Se realizan afinamientos "Tunning" periódicos de las Bases de Datos?				
4.-	¿Las bases de datos tienen definidas un password para lograr accederlas?				
5.-	¿Se tiene un procedimiento formal el cual se debe aplicar en el caso de que se deba realizar alguna modificación a los datos de una base de datos en producción?				
6.-	Se utilizan las fortalezas de validación de información que ofrece la base de datos (¿Triggers, integridad referencial y validaciones personalizadas por el programador?				

13. ¿Cómo se encuentran distribuidas las lámparas dentro del centro de cómputo?

14. ¿Es suficiente la iluminación del centro de cómputo? Si _____ No _____
¿Por qué?_____

15 ¿La temperatura a la que trabajan los equipos es la adecuada de acuerdo a las normas bajo las cuales se rige? Si _____ No _____

16. ¿Están limpios los ductos del aire acondicionado? Si _____ No _____

17. ¿La ubicación de los aires acondicionado es adecuada? Si _____ No _____

18. ¿Existe algún otro medio de ventilación aparte del aire acondicionado? ____ Si _____
¿Cuál? _____ No _____

19. ¿El aire acondicionado emite algún tipo de ruido? Si _____ No _____

20. ¿Se cuenta con tierra física? Si _____ No _____

21. ¿La tierra física cumple con los requisitos establecidos en las normas bajo las cuales se rige? Si _____ No _____

22. ¿El cableado se encuentra correctamente instalado? Si _____ No _____

23. ¿Podemos identificar cuáles son cables positivos, negativos o de tierra física? Si _____ No _____

24. ¿Los contactos de los equipos de cómputo están debidamente identificadas? Si _____ No _____

25 ¿Se cuenta con los planos de instalación eléctrica? Si _____ No _____

26. ¿La instalación eléctrica del equipo de cómputo es independiente de otras instalaciones? Si _____ No _____

27. ¿Los equipos cuentan con un regulador? Si _____ No _____

28 ¿Se verifica la regulación de las cargas máximas y mínimas? Si _____ No _____

29. Se cuenta con equipo interrumpible? Si _____ No _____

30. ¿Se tiene switch de apagado en caso de emergencia en algún lugar visible? Si _____ No _____

31. ¿Los cables están dentro de paneles y canales eléctricos? Si _____ No _____

32. ¿Los interruptores de energía están debidamente protegidos y sin obstáculos para alcanzarlos? Si _____ No _____

33. ¿Con que periodo se les da mantenimiento a las instalaciones y suministros de energía?

34. ¿Se cuenta con alarma contra incendios? Si _____ No _____

35. ¿Dónde se encuentran ubicadas?

36. ¿Se cuenta con alarmas contra inundaciones? Si _____ No _____

37. ¿Dónde se encuentran ubicadas?

38. ¿Es perfectamente audible? Si _____ No _____

39. ¿Existen extintores? Si _____
¿Cuántos? _____ No _____ Tipo de extintores: Manual ____ Automático ____ No existen ___

40. ¿Cuentan con algún tipo de control de entradas y salidas de usuario? Si_____ No_____ 41.

¿El usuario respeta ese control?

Si_____ No_____

42. ¿Con que tipo de programas cuentan en los equipos de computo? _____ _____ ____ _____ _____ _____ _____ _____ _____ _____ _____ _____

43. ¿Cuentan con manuales para cada programa que se maneja? Si___ No___

44. ¿El personal sabe del contenido de estos manuales? Si___ No___

45. ¿Se cuenta con reglamento para el usuario, maestro y personal? Si___ No___

46. ¿Usuarios y maestros respetan los reglamentos y políticas estipuladas dentro del centro de cómputo? Si___ No___

47. ¿El reglamento está a la vista del usuario? Si___ No___

48. ¿Qué tipo de mantenimiento realizan?
a. Preventivo
b. Correctivo

49. ¿Por qué razón?

50. ¿Qué materiales utilizan para realizar el mantenimiento del hardware?

51. ¿Tienen un lugar específico para guardar el material de mantenimiento de hardware?
Si___ No___

52. ¿Qué materiales utilizan para realizar el mantenimiento de software?

53. ¿Tienen un lugar específico para guardar el material de mantenimiento de software?
Si___ No___

54. ¿Los usuarios tienen la suficiente confianza como para presentar su queja sobre fallas en los equipos? Si___ No___

55. ¿Cuál es la disponibilidad de refacciones necesarias para dar el mantenimiento a las máquinas? a. Excelente
b. Muy buena
c. Buena
d. Regular
e. Mala
f. Muy mala
¿Por qué?_____

56. ¿Se registra el acceso al departamento de cómputo de personas ajenas a la dirección de informática?
Si___ No___

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

58. ¿Se tienen establecidos procedimientos de actualización a estas copias? Si___ No___

59. ¿Se ha establecido que información puede ser acezada y por qué persona? Si___ No___

60. ¿Se han instalado equipos que protejan la información y los dispositivos en caso de variación de voltaje como: reguladores de voltaje, supresores pico, U PS, generadores de energía? Si___ No___

61. ¿Se mantiene programas y procedimientos de detección e inmunización de virus en copias no autorizadas o datos procesados en otros equipos? Si___ No___

COORDINADOR:

1. ¿Sabe que hacer el personal en caso de una emergencia? Si _____ No _____

2. ¿Se ha adiestrado al personal sobre el uso de extintores? Si _____ No _____

3. ¿Existe una persona responsable de la seguridad de autorización de acceso? Si _____ No _____

4. ¿Se supervisa que esta persona realice sus actividades? Si _____
¿Quién? _____ No _____

5. ¿El personal que trabaja actualmente es adecuado para cumplir con las funciones encomendadas? Si___ No___
¿Por qué?_____

6. ¿Se da algún tipo de inducción al personal para que este informado de las funciones que realizará? Si____ No____

7. ¿Cuál es la forma de darles a conocer sus funciones? _____
_____ _____
_____
_____

8. ¿Cuál es la causa de que no estén por escrito? _____
_____ _____
_____
___

9. ¿Se establece algún tipo de objetivo para el área de cómputo? Si___ No___

10. ¿Estos objetivos están por escrito? Si___ No____

11. ¿En caso de ser si, en que tipo de documentos se encuentra? _____
_____ _____
_____

12. ¿En caso de ser no, por que no están definidos por escrito? _____
_____ _____
_____

13. ¿Cumple el personal o encargado del centro de cómputo con dichos objetivos ?Si___ No____
¿Por qué?_____

14. ¿Los niveles jerárquicos establecidos son necesarios para el desarrollo de las actividades del área? Si____ No___

15. ¿Permiten los niveles actuales que se tenga una ágil toma de decisiones y comunicación ascendente y descendente?