UNIVERSIDAD PRIVADA DEL NORTE

ESCUELA DE POSGRADO

Gestión de la Historia Clínica y la Seguridad de la Información del Hospital II Cajamarca - ESSALUD bajo la NTP-ISO/IEC 27001:2014

Tesis para optar el grado **MAGÍSTER** en:

Ingeniería de Sistemas con Mención en Gerencia de Sistemas de Información.

Autores:

Bachiller Cueva Araujo, Paul Omar

Bachiller Ríos Mercado, Juan Antonio

Asesora:

Dra. Ena Cecilia Obando Peralta

Cajamarca – Perú

2017

Resumen

Existe una necesidad creada por obtener herramientas de verificación del cumplimiento de la aplicación de la "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición" que es de uso obligatorio para las empresas públicas integrantes del Sistema Nacional de Informática y que la Oficina Nacional de Gobierno Electrónico e Informática ONGEI exige para su aplicación. Las Instituciones que prestan servicios de Salud cuentan con su principal activo de información la Historia Clínica que al ser un documento médico-legal y que tiene que ver con los procesos de atención de los pacientes y el Seguro Social de Salud – EsSalud cuenta con una norma a nivel nacional para cumplimiento en todos sus centros asistencial sobre Gestión de la Historia Clínica en los Centros Asistenciales del Seguro Social de Salud – ESSALUD del año 2014. La hipótesis planteada para esta investigación es que la dimensión Administrativa de la Gestión de la Historia Clínica es la más relevante en la Seguridad de la Información, es por eso que el objetivo busca aplicar una evaluación normativa a la Gestión de las Historias Clínicas y la evaluación de las cláusulas y controles necesarios para la Seguridad de la Información para analizar las caracteristicas de estos dos aspectos. De los resultados encontrados se observa que en el Hospital II Cajamarca – EsSalud existen un cumplimiento del 60% de las buenas prácticas y recomendaciones sobre la Norma de Gestión de las Historias Clínicas de los pacientes del Centro Asistencial (ver *Tabla 44 Porcentaje de cumplimiento de la Gestión de la Historia Clínica en el Hospital II Cajamarca – EsSalud*), repercutiendo significativamente en los principios de la Seguridad de la Información como son la confidencialidad, disponibilidad e integridad. Se realiza unas recomendaciones para establecer los mecanismos necesarios para fortalecer la seguridad de la información y proteger los activos relacionados al proceso de la Gestión de las Historias Clínicas, que son el pilar de futuras investigaciones que complementen la Seguridad de la Información y que son el Análisis de Riesgos y la Continuidad del Negocio.

Palabras clave: Historia clínica, Gestión de la Historia Clínica, Seguridad de de la Información, Sistema de Gestión de Seguridad de la Información.

Abstract

There is a need created by obtaining tools to verify compliance with the application of the “NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición” that is of compulsory use for the public companies that are part of the National System of Informatics and that the Oficina Nacional de Gobierno Electrónico e Informática demands for its application. The Institutions that provide Health services have their main asset of information the Clinical History that being a medical-legal document and that has to do with the processes of patient care and Social Health Insurance - EsSalud has a standard At the national level for compliance in all its health care centers on Management of the Clinical History in the Social Health Insurance Assistance Centers - ESSALUD of the year 2014. The hypothesis proposed for this research is that the Administrative dimension of the Clinical History Management is the most relevant in Information Security, that is why the objective seeks to apply a normative evaluation to the Management of Clinical Histories and the evaluation of the clauses and controls necessary for Information Security to analyze the characteristics of these two aspects. From the results found it is observed that at Hospital II Cajamarca - EsSalud there is a 60% compliance with good practices and recommendations on the Management of Clinical Histories of the patients of the Assistance Center (see Tabla 44 Porcentaje de cumplimiento de la Gestión de la Historia Clínica en el Hospital II Cajamarca – EsSalud), with a significant impact on the principles of Safety Of information such as confidentiality, availability and integrity. Recommendations are made to establish the necessary mechanisms to strengthen information security and protect the assets related to the process of Management of Clinical Histories, which are the pillar of future research that complement Information Security and which are the Analysis Of Risks and Business Continuity.

Keywords: Clinic history, Management of the Clinical History, Information security,

Information Security Management System.

Dedicatoria

A mis Padres, hermanos y hermanas por todas sus enseñanzas y apoyo a lo largo de mi vida, de manera especial a mi Madre por su entrega y amor que me han permitido perseverar y dar lo mejor de mí.

A mi Esposa Maritza, mi fiel compañera, amiga y el amor de mi vida, quien siempre me ha apoyado en mis decisiones personales y profesionales, eres una gran bendición para mí.

A Ana Paula, mi adorada hija, una inmensa bendición de Dios para mi vida.

A mis grandes amigos y hermanos en la fe, con quienes he compartido muchas cosas importantes y de quienes siempre he recibido su apoyo y compañía.

Paul Omar Cueva Araujo

Dedico con todo mi amor y cariño a mi querida hija Annie Gianella, Alejandro André y Karen Janet por su paciencia y apoyo en este momento importante de mi vida, quienes son la motivación e inspiración para cada ser mejor persona y profesional.

A mi amada madre por estar siempre conmigo, con su cariño y apoyo incondicional, a mis hermanos que con su compañía complementan mi felicidad y que los quiero mucho, a mi padre que no está presente, pero que me dejó muchas enseñanzas y valores que me han abierto muchas puertas en la vida.

A mis amigos y compañeros del trabajo que compartieron sus ideas y conocimientos sin esperar algo a cambio.

Juan Antonio Ríos Mercado

Agradecimientos

A Dios que me conforta y apoya con sus bendiciones en todo momento.

A la Dr. Ena Obando por su apoyo en el desarrollo de la presente investigación.

A mi estimado colega Luis Gómez Vargas por sus orientaciones siempre acertadas para poder encaminar esta investigación.

A mi compañero y amigo Juan Antonio Ríos por su apoyo personal y compartir esta aventura en bien de la seguridad de la información de EsSalud.

Paul Omar Cueva Araujo

A mi asesora la Dra. Ena Obando por su apoyo en la elaboración de esta investigación. Asimismo al Prof. Luis Gómez Vargas, por su invalorable paciencia, y a mis compañeros de trabajo que con su ayuda desinteresada me otorgaron parte de su tiempo para desarrollar ésta investigación.

Juan Antonio Ríos Mercado

Tabla de contenidos

Índice de Ilustraciones

Índice de tablas

I. INTRODUCCIÓN

I.1 Realidad problemática

El Hospital II Cajamarca, es una Institución Prestadora de Servicios de Salud (IPRESS), perteneciente al Seguro Social de Salud - EsSalud, registrado en la Superintendencia Nacional de Salud, SUSALUD con código RENAES 00010272, de categoría II-2.

El Hospital II Cajamarca, es una IPRESS del II Nivel de Atención, con población asignada que brinda atención de las necesidades de salud más frecuentes de baja y mediana complejidad. Desarrolla actividades de atención integral ambulatoria, hospitalaria y de emergencia en cuatro especialidades básicas y otras especialidades según demanda; atención de partos y cirugía de mediana complejidad. Realiza actividades de promoción de la salud, prevención de los riesgos y daños, recuperación y rehabilitación (Gerencia Central de Infraestructura EsSalud, 2014)

Actualmente uno de los principales problemas que tiene el Hospital II Cajamarca es, haber crecido en el número de asegurados debido al boom minero que experimento la ciudad por lo cual el número de la población se ha duplicado desde el año 2007, ocasionando el colapso en la infraestructura del Hospital con servicios desbordados en la atención, además de que al ser un solo hospital está dividido físicamente en dos locales, uno para hospitalización y emergencia y otro a tres kilómetros para la consulta externa, ocasionando gastos de tiempo para los usuarios internos y externos, duplicar costos, recursos y dificultar la operatividad del hospital.

Figura 1. Distribución de Locales de la Red Asistencial Cajamarca y Hospital II Cajamarca

El Hospital II Cajamarca cuenta con el Sistema de Gestión Hospitalaria el cual el servidor se encuentra ubicado físicamente en el local de la Administración de la Red Asistencial y empezó a funcionar en 1998, actualmente está en su versión 5.0 y ha sido elaborado con el lenguaje de programación Fox Pro 2.6 para DOS, este sistema almacena la información en tablas individuales, el menú principal muestra las siguientes opciones:

Tabla 1

Módulos Sistema de Gestión - Hospital II ESSALUD Cajamarca

Opciones del sistema	Opciones del sistema
1. Admisión	2. Historias Clínicas
3. Consulta Externa	4. Farmacia
5. Patología Clínica	6. Imagenología
7. Anatomía Patológica	8. Hospitalización
9. Emergencia	10. Centro Quirúrgico

11. Central de Depósitos	12. Estadística
13. Facturación	14. Rehabilitación
15. Banco de Sangre	16. Enfermería (Procedimientos)
17. Servicio Social	18. Almacén SAP
19. Programación de Trabajo Asistencial	20. Seguridad
21. Utilitarios	22. Interfaces

Nota. Opciones del SGHC

El tipo de personal con el que cuenta el Hospital II Cajamarca es:

Tabla 2

Tipo de Profesionales Asistenciales del Hospital II ESSALUD Cajamarca

PERSONAL MÉDICO	PROFESIONALES DE LA SALUD	PERSONAL TÉCNICO Y ADMINISTRATIVO
Médicos Internistas	Psicólogos	Técnico en Laboratorio
Médicos Generales	Enfermeras	Técnico en Rayos X
Pediatras	Obstetrices	Técnico o Auxiliar de Enfermería
Gíneco-obstetras	Nutricionistas	Técnico Asistencial
Cirujanos Generales	Químicos Farmacéuticos	Administrador
Cardiólogos	Tecnólogo Médico en Imagenología	Técnico Administrativo
Gastroenterólogos	Tecnólogo Médico en Laboratorio	Profesional en Estadística
Geriatra	Tecnólogo Médico en Terapia Física	Técnicos Informáticos
Médicos Anestesiólogos		Personal de Servicios Generales
Neurólogo		
Oftalmólogos		
Patólogo Clínico		

Médicos Rehabilitadores
Otorrinolaringólogos
Urólogos
Dermatólogos
Médicos Radiólogos
Médico Traumatólogos
Odontólogos

Nota. Limitado al Hospital II EsSalud Cajamarca. Fuente: Gerencia Central de Prestaciones de Salud, (2013)

El 22 de enero del 1999 con Resolución de Gerencia General N° 094-GG-IPSS-99, se eleva a Categoría de Nivel II, donde toma hasta la fecha el nombre de Hospital II Cajamarca. (Gerencia Central de Infraestructura EsSalud, 2014)

Las principales deficiencias que se encuentran son:

- Cumplimiento parcial de la Directiva N° 001-GG-ESSALUD-2014 “Gestión de la Historia Clínica en los Centros Asistenciales del Seguro Social de Salud - EsSalud”, aprobado con Resolución N° 107-GG-ESSALUD-2014.
- Sistema de Gestión Hospitalaria, la base de datos no cumple con conceptos actuales de Sistema de Gestión de Base de Datos Relacional (SGBDR) e Integridad Referencial (IR).
- Comité de Historias Clínicas que funciona parcialmente.
- Historias Clínicas en el sistema duplicadas para un mismo paciente.
- Diagnósticos de Historias Clínicas de un Paciente en otro Paciente en el Sistema y en archivo físico.
- Pérdida de Historias Clínicas o documentos que conforman la Historia Clínica.
- Desorden en el almacenamiento de documentos auxiliares a la Historia Clínica.
- Hospital funcionalmente dividido en dos locales.

I.2 Pregunta de investigación

¿Cuáles son las características más relevantes, de la Gestión de la Historia Clínica y la Seguridad de la Información en el Hospital II Cajamarca – EsSalud bajo la NTP-ISO/IEC 27001:2014?

I.3 Objetivos de la investigación

I.3.1 Objetivo General

Determinar las características más relevantes de la Gestión de la Historia Clínica y la Seguridad de la Información en el Hospital II Cajamarca – EsSalud bajo la NTP-ISO/IEC 27001:2014.

I.3.2 Objetivos Específicos

- Analizar la Gestión de las Historias Clínicas y su implementación en el Hospital II Cajamarca – EsSalud y proponer mejoras.
- Analizar la Seguridad de la Información en el Hospital II Cajamarca - EsSalud tomando como base los controles definidos en la NTP ISO/IEC 27001:2014.

I.4 Justificación de la investigación

La presente investigación aplica los controles definidos en el estándar **ISO/IEC 27001:2013** referidos al Sistema de Gestión de Seguridad de la Información tomando en cuenta el **uso obligatorio** de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición" (Presidencia del Consejo de Ministros, 2016), según resolución Nº 004-2016-PCM en todas las entidades integrantes del Sistema Nacional de Informática dentro de las cuales se encuentra el Hospital II Cajamarca - EsSalud.

La presente investigación encuentra su justificación práctica en que ayudará a analizar la seguridad de la Información según los controles definidos en la NTP ISO/IEC 27001:2014 y proponer mejoras a la Seguridad de la Información de las Historias Clínicas en el Hospital II Cajamarca - EsSalud.

I.5 Alcance de la investigación

El alcance de la presente investigación es analizar las brechas de cumplimiento del Hospital II Cajamarca – EsSalud, respecto a los controles que están definidos en la normatividad vigente para el Perú (NTP ISO/IEC 27001:2014) enfocándose en el análisis del principal activo de información el cuál es la Historia Clínica de cada uno de sus pacientes.

Se analiza para esto la Gestión de las Historias Clínicas en base a la normatividad que rige este proceso dentro de EsSalud, la cual se denomina Gestión de la Historia Clínica en los Centros Asistenciales del Seguro Social de Salud – ESSALUD (Gerencia General de EsSalud, 2014)

Se realiza asimismo un análisis de riesgos complementario y relacionado a las Historias Clínicas que sirva como modelo a ser aplicado por EsSalud para mejorar la seguridad de la información y garantizar la continuidad de negocio en la medida en que sea implementado.

II. MARCO TEÓRICO

III.1 Antecedentes

Entre los principales antecedentes Internacionales se cuentan con:

En la tesis titulada “Historia Clínica informática única una herramienta en la mejora de procesos en salud pública” (Atienza, 2013) de la Universidad Nacional de Córdova –Argentina, el autor realizó el trabajo para el Servicio de atención ambulatoria del Hospital Nacional de Clínicas de la provincia de Córdoba, República Argentina, donde presenta un nuevo modelo de gestión de información que reordena los procesos en la administración de la información y conduce a un mejor ordenamiento y de la gestión de la información en los servicios de salud, esto conlleva a un mejor desarrollo profesional, cuenta con criterios fundamentales como la integridad y la accesibilidad de la información, buscando ventajas competitivas en todos los ámbitos del desarrollo de actividades de las instituciones de salud principalmente en el conocimiento de los pacientes, con una correcta orientación en el proceso de la información que aborde conceptos de enseñanza aprendizaje, analice y produzca una devolución de los datos ingresados aportando nuevos conocimientos y la casuística en la formación profesional, las conclusiones que presenta luego de un año de uso del sistema indica conocimiento de estadística general con motivo de consulta prevalente, enfermedades asociadas a patologías reumáticas, frecuencia de edad por sexo, síntoma más frecuente, el usar un sistema de historia clínica electrónica permite automatizar el registro médico además de todo el proceso asistencial. (Gerencia General de EsSalud, 2014)

El uso de sistemas informáticos como herramienta de gestión de un hospital ayuda en la mejora de los procesos al agilizar el día a día reduciendo la tasa de errores humanos, optimizando los costos hospitalarios, facilitando el acceso a la información y contar con historias clínicas informatizadas mejorando la toma de decisiones en cualquier nivel de usuario, se aprecia la importancia de sistematizar los procesos y resguardar información importante para los pacientes, profesionales y no profesionales involucrados.

En la Tesis de grado denominada “Desarrollo de un Sistema de Gestión de Seguridad de la Información (SGSI) para la Empresa Comware S.A. en la

Ciudad de Quito, Aplicando la Norma ISO/IEC 27001" (Calderón Merchán & Sanchez Meza, 2012), publicada por la Universidad Politécnica Salesiana de Quito, Ecuador los autores desarrollan como objetivo el diseño de un Sistema de Gestión de Seguridad de la Información para la empresa Comware S.A en la ciudad de Quito y se basan en la Norma ISO 27001:2005, con el fin de lograr un esquema que sirva como guía para la posterior implementación y certificación en la Norma ISO 27001:2005 producto de la investigación se logra evidenciar las amenazas y riesgos que se encuentran presentes y pueden llegar a afectar el correcto funcionamiento de los sistemas informáticos proponiéndose procedimientos para el tratamiento de los mismos y se culmina con una explicación de cuáles son los pasos a seguir para que la empresa pueda certificarse en la Norma ISO 27001:2005, el análisis de esta tesis sirve en nuestra investigación para evidenciar la necesidad de partir de un análisis de riesgos de los activos de información el cual permita establecer los controles necesarios para minimizar o controlar las amenazas a las que estaría expuesta la información y de esta manera poder asegurar de cierta forma la información empresarial.

Entre los principales antecedentes nacionales se cuenta con:

En la tesis de grado titulada "Diseño de Procedimientos de auditoría de cumplimiento de la norma NTP-ISO/IEC 17799:2007 como parte del proceso de implantación de la norma técnica NTP-ISO/IEC 27001:2008 en Instituciones del Estado Peruano" (Huamán Monzón, 2014), publicada por la Pontificia Universidad Católica del Perú, presentó como objetivo general el establecer un procedimiento de auditoría de cumplimiento para la Norma Técnica Peruana NTP-ISO/IEC 17799:2007 en las instituciones del Estado Peruano basado en el marco COBIT 5.0, como parte del proceso de implantación de la Norma Técnica Peruana NTP-ISO/IEC 27001:2008 con la finalidad de mejorar la gestión de la seguridad de la información; donde busca elaborar procedimientos utilizando COBIT 5.0 y establecer que controles de la NTP-ISO/IEC 17799 serán establecidos e implementados por las instituciones del estado peruano sobre los activos de información que cuentan de acuerdo a los dominios de COBIT hacia los controles de la NTP, el autor concluye que son efectivas las pruebas realizadas y así cubrir vacíos que se presentan en el escenario informático nacional y que busca reconocer que estos procedimientos si bien se enfocan en empresas del sector público,

recomienda trasladarlo a empresas privadas y serán mejor beneficiados los ciudadanos, las empresas y/o organizaciones.

La necesidad de dar una herramienta de auditoría a las instituciones públicas del Perú, siguiendo las normas dadas por el estado peruano, donde se buscar proteger los activos de información aplicando la NTP-ISO/IEC 17799:2007 y COBIT 5, esto refuerza la necesidad de ir contando con documentos que permitan a las instituciones públicas o privadas realizar auditorías de sistemas de información.

En la tesis de grado denominada “Diseño de un Sistema de Gestión de Seguridad de la Información para una Entidad Estatal de Salud de Acuerdo a la ISO/IEC 27001:2013” (Talavera Álvarez , 2015) publicada por la Pontificia Universidad Católica del Perú, cuyo objetivo es el de diseñar un sistema de gestión de seguridad de la información para una institución estatal de salud, de acuerdo a la norma ISO/IEC 27001:2013. se analizan los riesgos a los que puede estar expuesta la información a nivel del personal propio o externo de una entidad de Salud implicando ello una fuga o exposición de información sensible ante lo cual las instituciones públicas han sido llamadas a realizar la implementación de diversos controles a través de un Sistema de Gestión de Seguridad de la Información en base a estándares y normas como la NTP ISO/IEC 27001 con la finalidad de asegurar el buen uso y protección de la información crítica que manejen, ya sea de clientes o información estratégica interna buscando cumplir con la normativa vigente relativa a Seguridad de la Información, esta investigación coincide con el tipo de desarrollo que se pretende hacer en nuestra investigación aplicando la Norma Técnica Peruana y refuerza la concepción de ser aplicada en una entidad de Salud determinando los riesgos internos y externos a los que podría estar expuesta la información sensible de la entidad.

Entre los principales antecedentes locales se cuenta con:

En la tesis de maestría titulada “Repercusión de la gestión de las historias clínicas en la seguridad de la información del Hospital Regional Cajamarca, marzo – agosto 2015” (Cruz Malca, 2015) publicada por la Universidad Privada del Norte, Sucursal Cajamarca, presentó como objetivo general aplicar una evaluación normativa al proceso de Gestión de Historias Clínicas y una auditoría informática a la Seguridad de la Información del Hospital

Regional Cajamarca, donde hace un análisis del uso de la NT N° 022-MINSA/DGSP-V.02 “Norma Técnica de Salud para la Gestión de la Historia Clínica” y de la NTP ISO/IEC 27001:2008 “Tecnología de la información, Técnicas de Seguridad, Sistemas de gestión de seguridad de la Información” 1ra Edición (11-Ene-2009); el autor concluye que mediante el análisis efectuado a la gestión de las historias clínicas que realiza el Hospital Regional Cajamarca y mediante el desarrollo una auditoria informática a la seguridad de la información del Hospital Regional Cajamarca, donde realiza un análisis detallado de riesgos a los activos informáticos involucrados en el proceso de gestión de las historias clínicas, constató que la gestión de las historias clínicas que realiza el Hospital Regional Cajamarca, únicamente da cumplimiento al 44% del total de disposiciones de la normativa evaluada, repercutiendo directamente en la confidencialidad, integridad y disponibilidad de la información de los pacientes. En tal sentido se establecieron los mecanismos necesarios para fortalecer la seguridad de la información y proteger los activos relacionados al proceso de la Gestión de las Historias Clínicas, mediante la priorización de los controles aplicables para la ejecución de pruebas de cumplimiento y pruebas sustantivas.

Investigación bastante relacionada a la Gestión de las Historias Clínicas en el Hospital Regional de Cajamarca, usando una norma anterior sobre Sistema de Gestión de la Seguridad de la Información, es un antecedente de investigación muy cercano porque involucra el Análisis de Riesgos sobre el principal activo de información del Hospital.

El proyecto profesional denominado “Análisis de Riesgos de TI para la Implementación de un Sistema de Seguridad de la Información en el Gobierno Regional de Cajamarca.” (Aliaga Infante, 2014) publicado por la Universidad Nacional de Cajamarca, Perú, se analiza la obligatoriedad de implementar procesos para proteger la información del negocio y todo aquello que tenga relación con la creación y procesamiento de información (personas, equipamiento, infraestructura), se utiliza una metodología de análisis de riesgos, como MAGERIT, OCTAVE, ISQ 27005 teniendo en cuenta la normativa exigida por la Oficina Nacional de Gobierno Electrónico e Informática a través de la NTP-ISO/IEC 27005;2009, el desarrollo metodológico se realiza analizando los macro procesos del Gobierno Regional de Cajamarca y posteriormente centrarse en el proceso Core del

negocio (Gestión de Proyectos de Inversión Pública), luego de ello se identifica los activos de información y luego se centra en los activos de TI relevantes para el proceso Core estos activos han sido definidos teniendo en cuenta los pilares de la seguridad de la información (Integridad, Confidencialidad y Disponibilidad) para luego identificar y valorar amenazas y vulnerabilidades y finalmente, con ayuda de la NTP-ISO/IEC 27001:2008 y NTP-ISO/IEC 17799:2007 se identificaron los controles a implementar para cada riesgo, esta tesis apoya la presente investigación en el sentido de que establece la necesidad de determinar las actividades principales relacionadas a la seguridad de la Información para buscar todos los activos y riesgos de seguridad relacionados a estos procesos Core, en nuestra investigación el proceso central de estudio es el resguardo adecuado de la Historia Clínica sobre el cual se debe establecer que aspectos se deben de proteger y resguardar de manera adecuada siguiendo las normas establecidas para ello.

III.2 Bases teóricas

II.2.1. Historia Clínica

La Historia Clínica y en general todos los registros médicos, constituyen documentos de alto valor médico, gerencial, legal y académico, su correcta administración y gestión contribuyen de manera directa a mejorar la calidad de atención de los pacientes, así como también a optimizar la gestión de los establecimientos de salud, proteger los intereses legales del paciente, del personal de salud y del establecimiento, así como proporcionar información con fines de investigación y docencia (Dirección General de Salud de las Personas MINSA, 2005, p.3)

II.2.1.1. Definición de la Historia Clínica

Es un documento físico de registro único y válido desde el punto de vista clínico y legal. Registra los datos de identificación, datos clínicos relacionados a la situación de un paciente, las intervenciones practicadas, su proceso evolutivo, tratamiento y recuperación de la atención que el profesional de la salud brinda al paciente. Se presenta como narración o exposición de hechos e incluye juicios, documentos, procedimientos, informaciones, consentimiento informado entre otros; estos se registran en el tiempo de forma ordenada, integrada, secuencial e inmediata, documentando fundamentalmente la relación médico-paciente. (Gerencia General de EsSalud, 2014, p.19)

"Es el documento médico legal, que registra los datos, de identificación y de los procesos relacionados con la atención del paciente, en forma ordenada, integrada, secuencial e inmediata de la atención que el médico u otros profesionales brindan al paciente." (Dirección General de Salud de las Personas MINSA, 2005, p.6)

Definición consideraba para la Historia Clínica que será pilar para el desarrollo de la tesis teniendo en consideración las normas principales de EsSalud y del Ministerio de Salud.

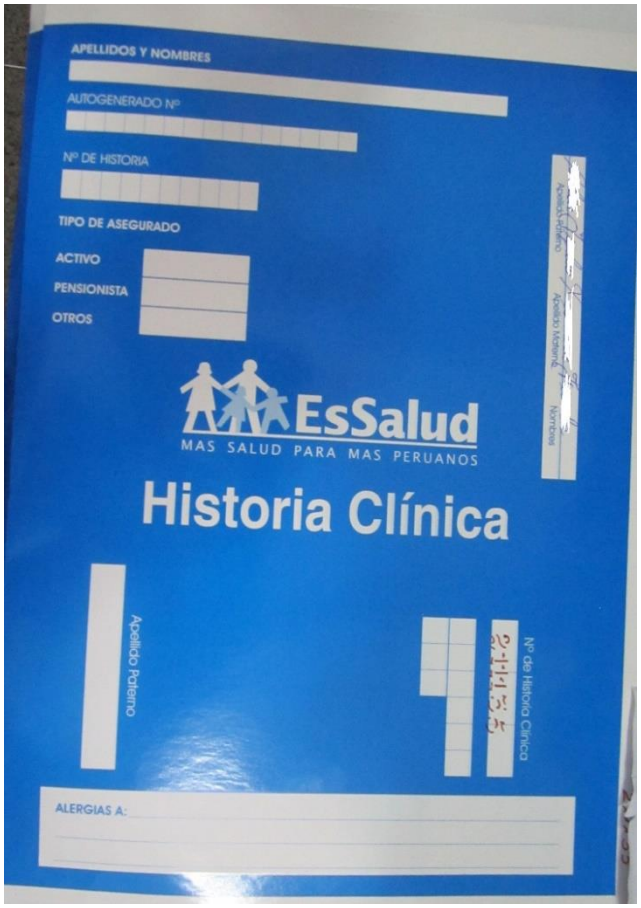


Figura 2. Ejemplo de Historia Clínica ESSALUD Hospital II Cajamarca

II.2.1.2. Estructura de la Historia Clínica

1. Identificación del paciente. - Aquí se registran los datos que permiten la identificación del paciente, en la que se incluye la hora y fecha del inicio de la atención, datos del establecimiento, número de historia clínica, etc.
2. Registro de la atención de salud. - Se registran las evaluaciones y procedimientos a que fue sometido el paciente, además del diagnóstico, estos registros deben estar suscritos por el profesional que brindó la atención de salud.
3. Información complementaria. - Aquí se registran o se adjuntan los resultados de los exámenes auxiliares que se practicó al paciente, además, del consentimiento informado, hojas de referencia o transferencia, etc. (Dirección General de Salud de las Personas MINSA, 2005, p.5)

En el Hospital II Cajamarca, todos los profesionales médicos y no médicos registran las atenciones en el Sistema de Gestión Hospitalaria previa cita que contiene un acto médico y que parcialmente los profesionales imprimen la atención para poder firmarla y agregar al archivo físico para situaciones legales, no se realiza este proceso de impresión por falta de papel.

II.2.1.3. Gestión de la Historia Clínica

"El Seguro Social de Salud – ESSALUD, busca establecer los mecanismos y procedimientos de la gestión del uso, manejo, conservación y depuración de la Historia Clínica física y electrónica en los Centros Asistenciales del Seguro Social de Salud – ESSALUD (Gestión de la Historia Clínica en los centros asistenciales del seguro social de salud – ESSALUD)" (Gerencia General de EsSalud, 2014, p.6)

"El proceso de administración y gestión de la Historia Clínica se realiza en los componentes técnicos administrativos y técnicos asistencial". (Gerencia General de EsSalud, 2014, p.8)

La necesidad de proteger su mejor activo de información se crea esta norma y que al evaluarlo sus componentes serán las dimensiones necesarias para ver otras perspectivas de su cumplimiento.

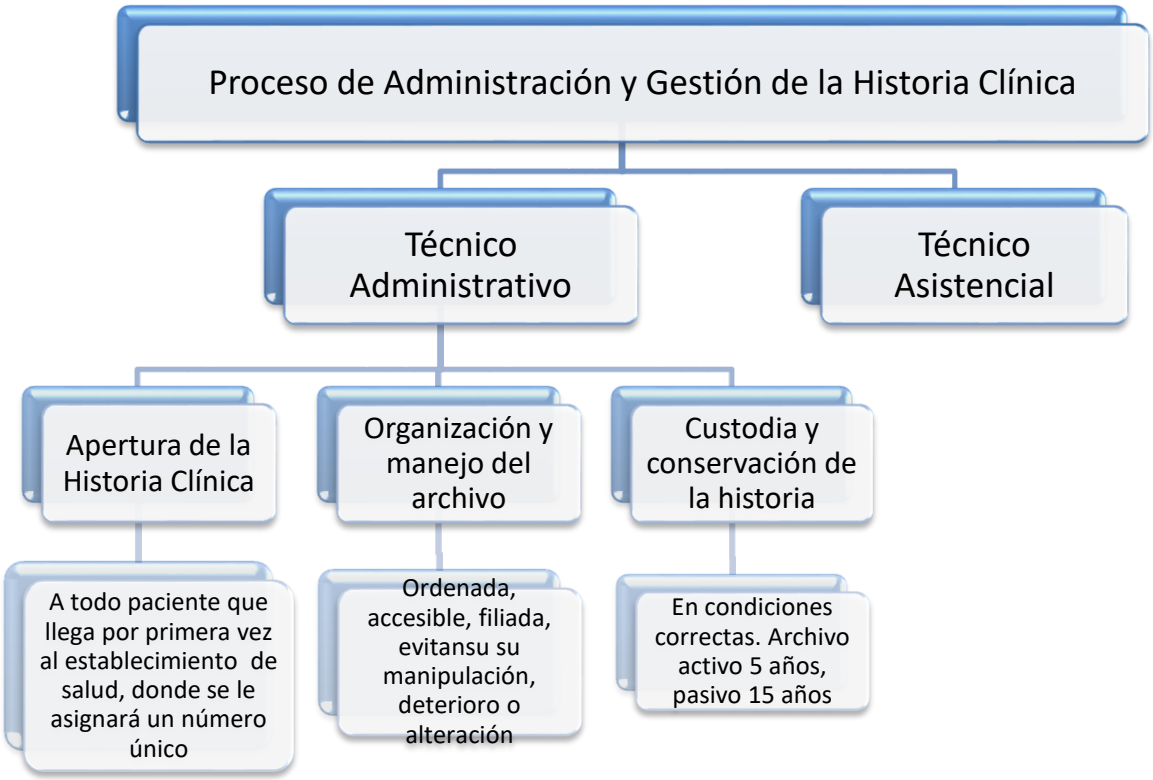


Figura 3 Proceso de Administración y Gestión de la Historia Clínica. Jefatura de Admisión y Registro ESSALUD-Cajamarca

II.2.1.4. Proceso Técnico Administrativo

a) Apertura de la historia clínica:

1. "Se realiza a todo paciente que llega por primera vez al Centro Asistencial, donde el personal verifica que el paciente no cuente con Historia Clínica Anterior. Ver Anexo VIII.1" (Gerencia General de EsSalud, 2014, p.8)
2. "A cada usuario que se le apertura una Historia Clínica, se le asigna el número de su documento de identidad nacional (DNI), el cual lo identifica y debe ser registrado en toda documentación que se genere". (Gerencia General de EsSalud, 2014, p.8)
3. "En los Centros Asistenciales del Primer nivel de atención se apertura la Historia Clínica a todos los recién nacidos asignándole como número de su DNI y en caso de que aún no lo tuviera se archiva la ficha de las atenciones en la Historia Clínica de la madre, en forma provisional hasta la expedición de su DNI". (Gerencia General de EsSalud, 2014, p.8)

4. En los Centros Asistenciales del II y III nivel de atención, solo se apertura la HC a los recién nacidos con patología; la documentación e información clínica de los recién nacidos normales o de los natimuertos son archivados en la Historia Clínica de la madre. (Gerencia General de EsSalud, 2014, p.8)

   La creación de Historias Clínicas se realiza en el Sistema de Gestión Hospitalaria por parte del personal de Módulos e igualmente de EsSalud en Línea.

b) Organización y manejo del archivo.

1. "Las Historias Clínicas deben conservarse en forma íntegra, asegurando su orden cronológico completo y pulcro de todos los formatos usados durante el proceso de atención de salud." (Gerencia General de EsSalud, 2014, p.9)
2. "El archivo de Historia Clínica es centralizado, organizado en un archivo activo y uno pasivo, accesibles al uso." (Gerencia General de EsSalud, 2014, p.9)
3. "Todo CAS debe disponer de un ambiente acondicionado para archivo de Historias Clínicas especiales, que por su contenido son potencialmente de implicancia médico legal, debiendo estar foliadas y adecuadamente conservadas. Dicho archivo funciona en ambientes físicos separados." (Gerencia General de EsSalud, 2014, p.9)
4. "Es responsabilidad del Gerente y/o Director de la Red, en coordinación con el Director del CAS, implementar este archivo especial, disponiendo que se aplique las medidas de seguridad de orden físico, en conformidad con el Sistema Nacional de Archivo para evitar su deterioro, manipulación y/o alteración de las mismas." (Gerencia General de EsSalud, 2014, p.9)

El boom minero dado en la Ciudad de Cajamarca ha generado un crecimiento desproporcionado de la demanda en comparación a la media a nivel nacional ocasionando el colapso en infraestructura, recursos y logística para la atención de sus pacientes adscritos.

c) Codificación y sistema de archivamiento de las historias clínicas.

1. "Los Centros Asistenciales que cuenten con menos de 10 000 Historias Clínicas deben usar el método convencional (correlativo) para archivar sus historias clínicas." (Gerencia General de EsSalud, 2014, p.9)
2. Los Centros Asistenciales que cuenten entre 10 000 y 100 000 Historias Clínicas deben usar el método dígito terminal simple. (Gerencia General de EsSalud, 2014, p.9)
3. Los Centros Asistenciales que cuenten con más de 100 000 historias clínicas deben usar el método dígito terminal compuesto.
4. Las historias clínicas en el archivo pasivo y en archivo especial, se archivan según el mismo método que se usa para el archivo activo. (Gerencia General de EsSalud, 2014, p.9)
5. En los CAS del I nivel de atención con población adscrita, las Historias Clínicas se archivan teniendo en cuenta el proceso de sectorización definido. (Gerencia General de EsSalud, 2014, p.9)

   En la mayoría de Centros Asistenciales de EsSalud cuentan con el Sistema de Gestión Hospitalaria que se encarga de la administración y "gestión" de las historias clínicas.

d) Custodia y conservación de la historia

1. La Dirección del CAS, es responsable de gestionar la implementación de los recursos humanos, físico y apoyo logístico de forma continua, que garantice la conservación de la documentación clínica en condiciones adecuadas que permitan el correcto mantenimiento y uso para la asistencia oportuna del paciente. (Gerencia General de EsSalud, 2014, p.10)
2. El responsable de la Unidad / Coordinador de la Unidad de Archivo tiene dentro de sus funciones la custodia de las Historias Clínicas en el CAS, mientras estas no registren movimientos y se encuentren archivadas. (Gerencia General de EsSalud, 2014, p.10).
3. "Los CAS de acuerdo a su complejidad deben mantener actualizado los dos en el sistema informático vigente, que facilite

el registro, control y monitoreo de la HC, para el seguimiento y ubicación (Ver Anexo VIII.4)" (Gerencia General de EsSalud, 2014, p.10)

4. "Cuando las HC permanezcan fuera del archivo, corresponde su custodia y conservación a la persona que solicitó la HC y de forma subsidiaria al responsable del servicio asistencial o administrativo al que pertenezca". (Gerencia General de EsSalud, 2014, p.10)
5. "Cuando se requiera la atención de solicitudes de copia de la historia clínica de un paciente hospitalizado, ésta debe ser realizada por la Jefatura del Servicio Médico / Jefatura Médico Quirúrgico correspondiente para la entrega completa y oportuna de la misma, en cumplimiento de las normas legales vigentes." (Gerencia General de EsSalud, 2014, p.10)
6. "Cuando el paciente hospitalizado con orden médica es transferido para atención específica, la enfermera responsable del servicio de origen entrega al paciente con su respectiva historia clínica (ordenada y completa) a la enfermera del Servicio de destino". (Gerencia General de EsSalud, 2014, p.10)
7. "Cuando el paciente hospitalizado requiera otras prestaciones quirúrgicas, médicas o de ayuda al diagnóstico y tratamiento, el personal asistencial del servicio destino es responsable de la custodia y devolución de la historia clínica al servicio de origen." (Gerencia General de EsSalud, 2014, p.10)
8. "En los Servicios de Hospitalización, la enfermera es responsable de la administración de la historia clínica, así como de su devolución completa y ordenada al área de archivo dentro de las 48 horas siguientes, al momento del alta". (Gerencia General de EsSalud, 2014, p.10)
9. "Las historias clínicas de pacientes fallecidos durante la hospitalización, son entregadas al personal del mortuorio (completas y ordenadas), conjuntamente al cadáver, debiendo responsabilizarse de su custodia hasta su entrega final al archivo o al área de epidemiología correspondiente." (Gerencia General de EsSalud, 2014, p.10)
10. "Todas las historias clínicas de pacientes fallecidos durante la hospitalización evaluadas en el área de epidemiología deben ser

devueltas (completas y ordenadas) al archivo dentro de las 72 horas siguientes a su recepción". (Gerencia General de EsSalud, 2014, p.10)

11. "Las historias clínicas en custodia por motivos legales solicitadas para atención médica deben ser entregadas en fotocopia, quedando el original en el área de custodia". (Gerencia General de EsSalud, 2014, p.11)
12. "Ninguna historia clínica original debe salir del CAS salvo exista mandato judicial que lo ordene, de ser así es trasladada por un personal de archivo con custodia y bajo responsabilidad de la dirección del CAS". (Gerencia General de EsSalud, 2014, p.11)
13. "Los locales y ambientes designados para archivo deben ser fumigados por lo menos trimestralmente". (Gerencia General de EsSalud, 2014, p.11)
14. "Los locales y ambientes designados para archivo deben contar con ventilación adecuada ya sea natural o artificial, sobre la base de la utilización racional de puertas y ventanas, empleo de ventiladores, aire acondicionado, extractores e inyectores de aire, deshumedecedores, etc". (Gerencia General de EsSalud, 2014, p.11)
15. "Se debe evitar la incidencia directa o perpendicular de la luz natural o artificial sobre las historias clínicas y demás documentos pertinentes". (Gerencia General de EsSalud, 2014, p.11)
16. "Los locales y ambientes designados para archivo deben contar con iluminación, según normativa". (Gerencia General de EsSalud, 2014, p.11)
17. "La historia clínica debe ser protegida, mediante folders según especificaciones del anexo VIII.2." (Gerencia General de EsSalud, 2014, p.11)
18. "Las historias clínicas depuradas deben estar almacenadas en cajas de cartón y/o según normatividad vigente." (Gerencia General de EsSalud, 2014, p.11)
19. "Las áreas de archivo deben contar con señalización pertinente." (Gerencia General de EsSalud, 2014, p.11)
20. "Las áreas de archivo deben estar implementadas con sistemas contraincendios, extintores y detectores de humo según normas

de arquitectura sanitaria y de defensa civil.” (Gerencia General de EsSalud, 2014, p.11)

21. “Es responsabilidad del Director del CAS implementar medidas de seguridad dirigidas a evitar la sustracción indebida de las historias clínicas por medio de un sistema de videocámara.” (Gerencia General de EsSalud, 2014, p.11)
22. “La Unidad de Archivo de HC debe contar con Sala de trabajo, sala de Lectura y sala de evacuación, debiendo estar implementadas con sistema de video cámara y de vigilancia de ingreso y salida para el control.” (Gerencia General de EsSalud, 2014, p.11)
23. “En caso de cierre de un Centro Asistencial las Historias Clínicas pasan al nuevo Centro Asistencial de readscripción del asegurado.” (Gerencia General de EsSalud, 2014, p.11)

En la actualidad el uso del Sistema de Gestión Hospitalaria hace que los principales procesos para el acceso se hagan por medio de él y no sea necesaria la salida de la copia física del archivo de historias clínicas, por razones de espacios no cuentan con las salas complementarias indicadas.

e) De la confidencialidad y acceso a la historia

24. “El paciente tiene derecho a que se le entregue a su solicitud copia de epicrisis y de su Historia Clínica, para lo cual el recurrente abona el costo establecido de acuerdo al TUPA de ESSALUD vigente y la Ley General de Salud artículo 15° inciso i, debiendo llenar la solicitud del anexo VIII.7).” (Gerencia General de EsSalud, 2014, p.11)
25. “Toda persona usuaria de los servicios de salud, tiene derecho a exigir la reserva de la información relacionada con el acto médico y su Historia Clínica, con las excepciones que la Ley establece (Ley General de Salud artículo 15° inciso b, artículo 25).“ (Gerencia General de EsSalud, 2014, p.12)
26. “La información sobre el diagnóstico de las lesiones o daños en los casos de herida por arma blanca, herida de bala, accidente de tránsito o por causa de otro tipo de violencia que constituya delito

perseguido de oficio o cuando existan indicios de aborto criminal; debe ser proporcionada a la autoridad policial o al Ministerio Público a su requerimiento (artículo 25° y 30° de la Ley General de Salud).” (Gerencia General de EsSalud, 2014, p.12)

27. “En los casos de entrega de información a terceros, se debe presentar la carta poder notarial con la autorización del paciente. Esto no se aplica a la información que el establecimiento tiene la obligación legal y administrativa de proporcionar.
    La autorización o carta poder debe incluir:
    - El nombre del hospital que debe brindar la información.
    - El nombre de la persona o institución que debe recibir la información.
    - El nombre completo del paciente, su fecha de nacimiento y dirección.
    - Copia simple del DNI del paciente y solicitante.
    - El motivo por el cual se requiere la información.
    - La naturaleza de la información que se desea y la magnitud que abarca.
    - La fecha en que se firmó la autorización.
    - La firma del paciente o del familiar responsable y del tercero al que delega poder.

    La autorización debidamente firmada, se conserva en la Historia Clínica.
    En caso de pacientes fallecidos los familiares directos en grado de consanguinidad pueden solicitar la copia de la historia clínica cumpliendo los requisitos del TUPA de ESSALUD.” (Gerencia General de EsSalud, 2014, p.12)

Los procesos indicados en esta sección hablan sobre la confidencialidad de la información almacenada en las historias clínicas y con pueden darse su disponibilidad mediante el TUPA.

f) Depuración de las historias clínicas

1. “La depuración del archivo de Historias Clínicas debe ser un proceso constante, debiendo evaluarse anualmente el

movimiento de las historias (ver anexo VIII.6).” (Gerencia General de EsSalud, 2014, p.12)

2. “El tiempo de conservación de las Historias Clínicas en el archivo activo es de cinco años, considerando la fecha de última atención al paciente, debiendo trasladarse al archivo pasivo en forma regular y permanente, conservando su número original.” (Gerencia General de EsSalud, 2014, p.12)
3. “Después de encontrarse la historia clínica 10 años en el archivo pasivo, se levante un ACTA dirigida por el Comité de historias clínicas, antes de proceder a su destrucción selectiva para aquellos episodios de hospitalización; y destrucción total para aquellos que sólo tenga consultas externas.” (Gerencia General de EsSalud, 2014, p.13)
4. “Para el caso de la destrucción selectiva de las historias clínicas físicas, se conserva de manera definitiva en forma original o en medio digital codificado que permita el acceso de los siguientes formatos:
    - Hojas de consentimiento informado.
    - Hoja de exoneración de responsabilidad por alta voluntaria.
    - Informes quirúrgicos y/o registros de parto.
    - Informes de anestesia.
    - Informes de procedimientos complementarios.
    - Ficha Clínica Estomatológica (Odontograma).
    - Epicrisis
    - Informe de necropsia.
    - Hoja de indicación terapéutica médica.
    - Hoja de evolución y de planificación de cuidados de enfermería.” (Gerencia General de EsSalud, 2014, p.13)
5. “El proceso de conservación en medio digital usa el soporte tecnológico necesario según el número de asegurados adscritos y/o referidos al CAS y software de gestión de documentos con soporte para validación de las copias generadas.” (Gerencia General de EsSalud, 2014, p.13)
6. “El proceso de destrucción parcial o selectiva de Historias Clínicas, es evaluado y verificado e informado por el Comité de

Historias Clínicas de la Red Asistencial, cuyas actas elevadas por el Gerente o Director de la Red Asistencial para ser avalado por el Comité Nacional de Historias Clínicas, proceso que es registrado en una Acta, así como la lista de Historias Clínicas a ser destruidas, donde se determina su destino final." (Gerencia General de EsSalud, 2014, p.13)

7. "Es obligación de los Órganos Desconcentrados mantener activo al Comité de Historias Clínicas de su ámbito, de acuerdo a normatividad vigente." (Gerencia General de EsSalud, 2014, p.13)
8. "En caso de que los pacientes demanden atención de salud posterior a la destrucción de su historia clínica, los formatos conservados son los documentos que reinician su Historia Clínica manteniendo el número asignado originalmente." (Gerencia General de EsSalud, 2014, p.13)
9. *Conformación del Comité de HHCC*

   Estará conformado por:

   - *Nivel Central: designado por la GCPS.*
   - *Nivel de Redes Asistenciales y Hospitales conformado por:*
     - *Gerente o Director de la Red Asistencial o representante.*
     - *Gerente Quirúrgico o representante.*
     - *Gerente Clínico o representante.*
     - *Jefe de la Oficina de Admisión.*
     - *Representante de la Oficina de Asesoría Jurídica.*
     - *Jefe de Archivo de Historias Clínicas.*
     - *Administrador.*

   (Gerencia General de EsSalud, 2014, p.14)

Esto describe la forma de realizar el proceso de depuración de las historias clínicas y quien es el responsable de realizarlo, quienes conforman el comité y el periodo a realizarse.

g) Propiedad de la historia clínica

1. "La Historia Clínica y la base de datos, es de propiedad física del Centro Asistencial." (Gerencia General de EsSalud, 2014)

2. “La información contenida en la historia clínica es propiedad del paciente, por lo tanto, tiene derecho a ella, según lo estipula la Ley General de Salud.” (Gerencia General de EsSalud, 2014, p.14)
3. “El personal asistencial que elabora la historia clínica tiene derecho de propiedad intelectual respecto a sus registros.” (Gerencia General de EsSalud, 2014, p.14)

Para los casos legales que tienen que ver con los derechos de autor, en esta sección se determina los propietarios de la información.

II.2.1.5. Proceso Asistencial

a) Elaboración y registro

1. Todo acto médico debe estar sustentado en una Historia Clínica veraz y suficiente que contenga las prácticas y procedimientos aplicados al paciente. (Artículo 29° de la Ley General de Salud). (Congreso de la República , 1997) (Gerencia General de EsSalud, 2014, p.14)
2. Los registros de los diagnósticos y las anotaciones contenidas deben ser legibles incluyendo el código y la descripción según la Clasificación Internacional de Enfermedades – CIE 10 vigente y Problemas Relacionados con la Salud. (Gerencia General de EsSalud, 2014, p.14)
3. El registro de los procedimientos se realiza aplicando el Código de Procedimientos Terapéuticos actual, según normatividad vigente. (Gerencia General de EsSalud, 2014, p.14)
4. Los errores en la Historia Clínica se corrigen trazando una línea sobre el error y anotando al lado de la corrección la fecha, firma y sello del profesional de la salud responsable, y consignando el fundamento de la corrección. (Gerencia General de EsSalud, 2014, p.14)
5. Todas las anotaciones en la Historia Clínica deben ser fechadas y firmadas por quién realizó el acto médico, consignándose

claramente, el nombre y apellido, el número de colegio profesional y sello. (Gerencia General de EsSalud, 2014, p.14)

6. Otros profesionales no médicos que realizan anotaciones en la Historia Clínica lo hacen en las condiciones arriba señaladas. (Gerencia General de EsSalud, 2014, p.14)
7. Cada anotación realizada por internos y/o residentes de medicina y otros profesionales de la salud debe ser refrendada con la firma y sello de los profesionales asistentes pertenecientes al servicio asignado responsable a dicha actividad docente. (Gerencia General de EsSalud, 2014, p.15)

En esta sección se encuentran las buenas prácticas a realizar por el personal asistencial que tiene acceso a la información de la historia clínica.

b) Orden de los formatos

- "Los formatos de la Historia Clínica deben estar de acuerdo a los Anexos de la Norma Gestión de La Historia Clínica en los Centros Asistenciales del Seguro Social De Salud – ESSALUD." (Gerencia General de EsSalud, 2014, p.15)
- "Toda hoja de la Historia Clínica debe ser identificada con el nombre completo y número de Historia Clínica del paciente, en lugar uniforme y de fácil visibilidad." (Gerencia General de EsSalud, 2014, p.15)
- "En el caso de pacientes hospitalizados en la HC manual se registra además el servicio y el número de cama, con letra legible." (Gerencia General de EsSalud, 2014, p.15)
- "El orden de los formatos de acuerdo al servicio de atención debe seguir una secuencia lógica definida a partir de los procesos de atención en las diversas unidades productoras de salud". (Gerencia General de EsSalud, 2014, p.15)
- "En los casos que el paciente requiera del formato de Consentimiento Informado, éste se adiciona en la HC y se procede de acuerdo a lo establecido en la normatividad vigente". (Gerencia General de EsSalud, 2014, p.15)

- "En las diferentes Especialidades Médicas, PADOMI entre otros que usan formatos complementarios, debidamente validados por el área de calidad y el comité de historias clínicas, estos deben ser adicionados a la historia clínica básica". (Gerencia General de EsSalud, 2014, p.15)

  Se indican los documentos que son parte de la historia clínica y el orden en el cual deben ser almacenados para ser accesibles para las profesionales asistenciales en las consultas médicas o administrativas como las auditorias o temas de investigación.

c) Uso y manejo de la historia clínica

1. Objetivos
   - Proporcionar evidencia documentada sobre el curso de la enfermedad y tratamiento del paciente.
   - Servir como base para el estudio y evaluación de la calidad de la atención prestada al paciente.
   - Proporcionar información para usos de investigación y docencia.
   - Contribuir al sistema de información proporcionando datos para la programación, y evaluación de actividades de salud local, regional y nacional.
   - Ayudar a proteger los intereses legales del paciente, del establecimiento de salud y del personal de salud. (Gerencia General de EsSalud, 2014, p.3)
2. Solicitud de HHCC para docencia e investigación
   - Los requerimientos de historias clínicas son solicitados por escrito, o por correo electrónico del Gerente / Director / Jefes de Departamento / Servicio y son revisadas en la Sala de lectura del archivo de historias clínicas.
   - La información obtenida de la Historia Clínica se consigna de forma anónima para salvaguardar la confidencialidad. (Gerencia General de EsSalud, 2014, p.16)
3. Uso y manejo de la historia clínica

- Para la atención a los usuarios de consulta externa el Responsable de la Unidad de Archivo obtiene del Sistema Informático vigente la relación de pacientes citados. (Gerencia General de EsSalud, 2014, p.16)
- Para los casos de citas adicionales en consulta externa, el personal técnico de enfermería solicita la HC al personal de archivo, quien se encarga de llevar la HC al consultorio solicitante. (Gerencia General de EsSalud, 2014, p.16)
- Para la atención a los usuarios en hospitalización las Historias Clínicas deben ser solicitadas a la Unidad de Archivo por la enfermera de dichos servicios. (Gerencia General de EsSalud, 2014, p.16)
- Todas las historias que salen del archivo a consulta externa deben ser devueltas el mismo día de la atención con excepción de los pacientes que hayan sido hospitalizados. (Gerencia General de EsSalud, 2014, p.16)
- En las unidades de emergencia u hospitalización, las historias clínicas deben ser retornadas al archivo del CAS al alta del paciente dentro de las 24 ó 48 horas respectivamente. (Gerencia General de EsSalud, 2014, p.16)
- Toda retención por causa absolutamente justificada, debe ser reportada por escrito y con autorización del Jefe del Servicio / Jefe Médico Quirúrgico, el mismo día a la unidad de archivo, precisando el motivo y la fecha de devolución no mayor a 72 horas (Gerencia General de EsSalud, 2014, p.16)
- Está prohibido guardar Historias Clínicas en casilleros del personal de la salud. (Gerencia General de EsSalud, 2014, p.16)
- Las Historias Clínicas deben permanecer almacenadas dentro de la unidad de archivo, cuando no están siendo utilizados en la atención del paciente. (Gerencia General de EsSalud, 2014, p.16)
- Las historias de pacientes hospitalizados deben retornar a la unidad de archivo en un plazo no mayor a las 24 horas posterior al alta, con su epicrisis respectiva, para el procesamiento de la

misma (compaginación, codificación, indización, preparación de informes estadísticos, etc.). (Gerencia General de EsSalud, 2014, p.16)

- Las historias solicitadas por el Servicio de Emergencia deben ser devueltas dentro de las 48 horas siguientes, salvo que el paciente permanezca en sala de observación o haya sido hospitalizado. (Gerencia General de EsSalud, 2014, p.16)
- Los formatos de atención de emergencia deben ser incorporados a la Historia Clínica de los pacientes adscritos al CAS. Los no adscritos son remitidos a su respectivo CAS. (Gerencia General de EsSalud, 2014, p.16)
- Las historias clínicas entregadas a los diferentes Departamentos o Servicios para informes médicos que requieran de opinión especializada o para auditorías médicas, deben ser devueltas al archivo en un plazo no mayor a 72 horas. (Gerencia General de EsSalud, 2014, p.17)
- Toda Historia Clínica que se retira de su lugar en el archivo debe ser registrado en el sistema informático pertinente, de manera tal, que permita el seguimiento de cada historia y agilice su archivo cuando sea devuelta. (Gerencia General de EsSalud, 2014, p.17)
- Toda historia que se retira de su lugar en el archivo para cualquiera de sus diferentes usos, debe necesariamente ser registrada en el formato: solicitud de historia clínica; consignando la salida, la recepción por los diferentes “usuarios” internos y su posterior devolución, con las firmas autorizadas (ver anexo VIII.5). (Gerencia General de EsSalud, 2014, p.17)

Uso, procesos, formatos, registro, consulta, etc. de la información de las historias clínicas y el entorno en el cual se da su presencia para el manejo por el personal administrativo y asistencial.

II.2.2. Seguridad de la Información

Toda persona tiene "el derecho fundamental a la protección de los datos personales, previsto en el artículo 2 numeral 6 de la Constitución Política del Perú, a través de su adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales que en ella se reconocen." (Ley Nº 29733, 2011) Por lo mismo cualquier institución, persona o empresa está en la obligación de proteger la información personal que sea recabada como parte de un servicio brindado a cualquier ciudadano.

"La información es un recurso que, como el resto de los activos empresariales, tiene valor para una organización y por consiguiente debe ser debidamente protegida. La seguridad de la información protege ésta de una amplia gama de amenazas, a fin de garantizar la continuidad institucional, minimizar el daño y maximizar el retorno sobre las inversiones y las oportunidades." (OPTIC, 2013, p.3) Esta seguridad por tanto debe estar a cargo de la institución y ella debe de establecer los mecanismos adecuados para poder resguardarla de manera adecuada.

"La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información" (Donato, 2013, p.47), esta protección debe ser por tanto efectiva en sus controles permitiendo así lograr los objetivos institucionales.

"Para que un sistema de información sea seguro se debe garantizar la disponibilidad, para permitir el acceso a la información para las personas autorizadas cuando sea requerida, integridad para el mantenimiento de la información tal cual como fue generada y confidencialidad para asegurar el acceso a la información solo para aquellas personas que cuenten con la debida autorización" (Donato, 2013, p.47), de esta manera se cumple con los tres objetivos de la seguridad de la información, disponibilidad, integridad y confidencialidad.

También son importantes las políticas, estándares y medidas que se implementen en la organización buscando asegurar además de las tres propiedades principales de la información la autenticación la cual "permite identificar a la persona o personas que han generado la

información" y el no repudio que "permite que la información sea validada a través de algún mecanismo que compruebe su integridad y contenido, declarándola como genuina" (Talavera Álvarez , 2015, p.36)

"Seguridad es la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles." (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012, p8), por lo mismo la seguridad no es el hecho de impedir cualquier riesgo al que estén asociados los activos si no saber resistir o sobrellevar dicho riesgo a un nivel determinado.

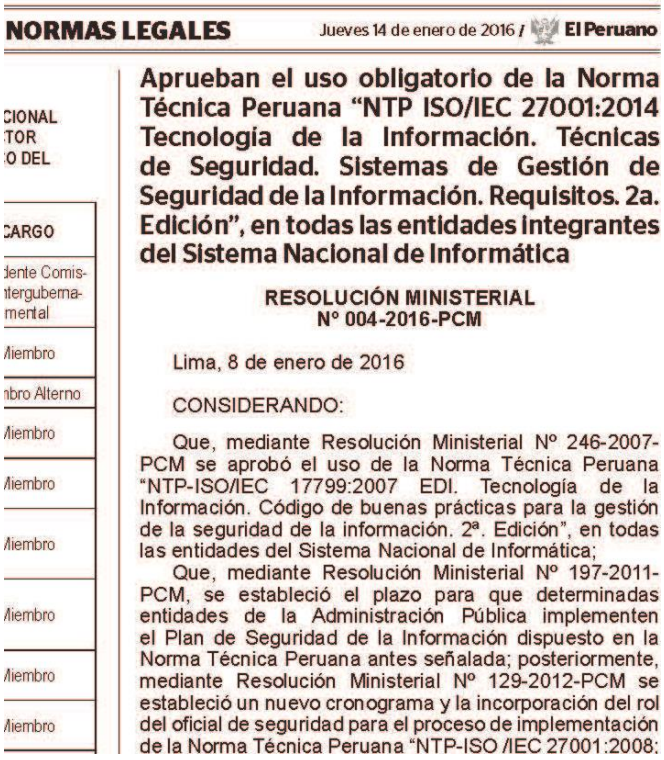
"Se requiere para gestionar eficientemente la seguridad de la información que, todos los miembros de la Organización tomen conciencia de su importancia y el papel que juegan en generar aportes de calidad y eficacia en los servicios críticos de la Entidad" (Seclén Arana, 2016) para ello es importante que los temas de la seguridad de la información se difundan entre los miembros de la organización a fin de que este tema forme parte de la cultura organizacional de cada empresa o institución como es el caso de EsSalud en donde a través de la Gerencia Central de Tecnologías de Información y Comunicación difunde a sus empleados los temas relacionados a la seguridad de la Información de manera tal que partiendo de temas sencillos se pueda llegar a objetivos solidos institucionalmente.

Figura 4. Difusión de temas relacionados a la seguridad de la Información, accesos no autorizados

Figura 5. Difusión de temas relacionados a la seguridad de la Información, conexiones eléctricas.

II.2.2.1. Seguridad de la Información en el Perú

La Presidencia del Consejo de Ministros del Perú ha dispuesto por medio de la Resolución Ministerial N° 004-2016-PCM la aprobación del uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática a donde pertenece también EsSalud, y establece que cada entidad debe de designar un Comité de Gestión de Seguridad de la Información, cuyas funciones serán establecidas por cada entidad de acuerdo a la norma estableciendo los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) de acuerdo al ciclo Planificar, Hacer, Verificar y Actuar. (Presidencia del Consejo de Ministros, 2016, p.2)



NORMAS LEGALES Jueves 14 de enero de 2016 / El Peruano

Aprueban el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática

RESOLUCIÓN MINISTERIAL N° 004-2016-PCM

Lima, 8 de enero de 2016

CONSIDERANDO:

Que, mediante Resolución Ministerial Nº 246-2007-PCM se aprobó el uso de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2ª. Edición", en todas las entidades del Sistema Nacional de Informática;

Que, mediante Resolución Ministerial Nº 197-2011-PCM, se estableció el plazo para que determinadas entidades de la Administración Pública implementen el Plan de Seguridad de la Información dispuesto en la Norma Técnica Peruana antes señalada; posteriormente, mediante Resolución Ministerial Nº 129-2012-PCM se estableció un nuevo cronograma y la incorporación del rol del oficial de seguridad para el proceso de implementación de la Norma Técnica Peruana "NTP-ISO /IEC 27001:2008:

Figura 6. Aprobación de uso obligatorio de la NTP ISO/IEC 27001:2014. Recuperado de Normas Legales Diario Oficial El Peruano

II.2.2.2. Análisis de Riesgos Informáticos

Un riesgo viene a ser una "estimación del grado de exposición de un activo, a que una amenaza se materialice sobre él causando daños a la

organización. El riesgo indica lo que le podría pasar a los activos si no se protegen adecuadamente" (Instituto Nacional de Tecnologías de la Comunicación, 2014, p.9) es una estimación que debe realizar cada organización o empresa en base a los conocimientos y experiencia que posee.

"El análisis de riesgos es una aproximación metódica para determinar el riesgo siguiendo unos pasos pautados:

1. Determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación." La organización debe de realizar un listado de los activos de Información que posee.
2. "Determinar a qué amenazas están expuestos aquellos activos", en base a un análisis y entrevistas con el personal responsable de los activos el cual posee la experiencia y conocimientos.
3. "Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo.", este punto también se debe de realizar en base a la información de los expertos que conocen a estos activos.
4. "Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza", se debe asignar valores para poder determinar el impacto ante la posible materialización de la amenaza.
5. Estimar el riesgo, definido como el impacto". (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012, p.22)

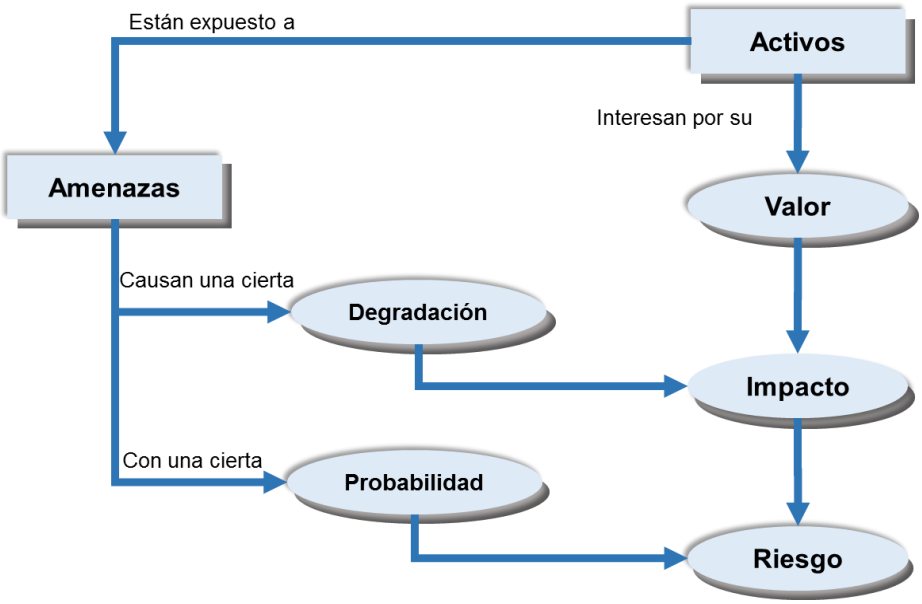


Figura 7. Elementos del análisis de riesgos potenciales. Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, (2012)

II.2.2.3. Metodología de Análisis de Riesgos Informáticos.

Se debe emplear una metodología para el análisis de los riesgos informáticos que permita poder determinar qué tan probable vendría a ser el desarrollo de una amenaza y el impacto que se produciría en la organización, para este fin es necesario identificar los activos de información, las amenazas y vulnerabilidades a las que está expuesta asignando valores que permitan estimar el riesgo al que estaría expuesto.

Luego de conocer estos resultados la organización debe de establecer las acciones y controles necesarios que se deben de implementar para mitigar, controlar o simplemente asumir los riesgos a los que estaría expuesta.

Una metodología desarrollada por el gobierno español para poder realizar este proceso es Magerit.

II.2.2.4. Magerit

"Siguiendo la terminología de la normativa ISO 31000, Magerit responde a lo que se denomina "Proceso de Gestión de los Riesgos", sección 4.4

("Implementación de la Gestión de los Riesgos") dentro del "Marco de Gestión de Riesgos". En otras palabras, MAGERIT implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información." (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012, p.7), esta metodología que inicialmente fue desarrollada para las entidades estatales españolas es ahora utilizada tanto en el sector público como en el privado y ayuda a poder realizar un análisis de los riesgos informáticos a través de un conjunto organizado de pasos que están descritos en tres libros los cuales son de libre acceso, esto ha ayudado a que se difunda la metodología convirtiéndola en una de las más utilizadas.

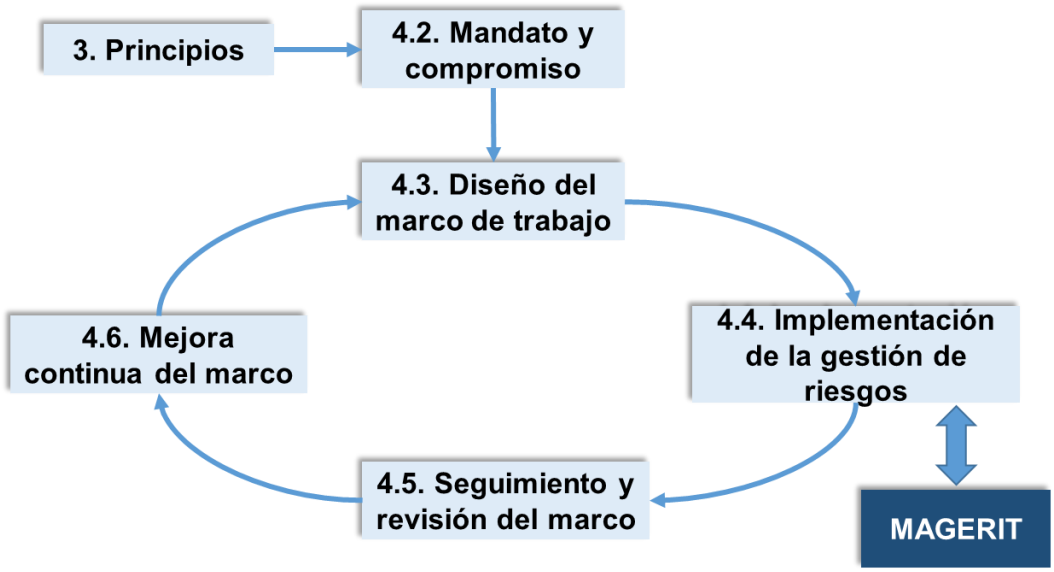


Figura 8. ISO 31000 Marco de trabajo para la gestión de riesgos. Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, (2012).

"Magerit persigue los siguientes objetivos:

Directos

- Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos
- Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC)

- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control

Indirectos

- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso" (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012),

II.2.2.5. Tipos de Activos de Información:

"La tipificación de los activos es tanto una información documental de interés como un criterio de identificación de amenazas potenciales y salvaguardas apropiadas a la naturaleza del activo." (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012, p.7), Magerit en su libro de Catalogo de elementos sugiere clasificar los activos de información de la siguiente manera:

[D] Datos/Información

Los datos son el corazón que permite a una organización prestar sus servicios. La información es un activo abstracto que será almacenado en equipos o soportes de información (normalmente agrupado como ficheros o bases de datos) o será transferido de un lugar a otro por los medios de transmisión de datos.

[K] Claves criptográficas

Se emplea para proteger el secreto o autenticar a las partes. Las claves criptográficas, combinando secretos e información pública, son esenciales para garantizar el funcionamiento de los mecanismos criptográficos.

[S] Servicios

Función que satisface una necesidad de los usuarios

[SW] Software - Aplicaciones informáticas

Con múltiples denominaciones (programas, aplicativos, desarrollos, etc.) se refiere a tareas que han sido automatizadas para su desempeño por un equipo informático.

[HW] Equipamiento informático

Medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización, siendo depositarios temporales o permanentes de los datos.

[COM] Redes de comunicaciones

Incluye tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros; pero siempre centrándose en que son medios de transporte que llevan datos de un sitio a otro.

[Media] Soportes de información

Se consideran dispositivos físicos que permiten almacenar información de forma permanente o, al menos, durante largos periodos de tiempo.

[AUX] Equipamiento auxiliar

Se consideran otros equipos que sirven de soporte a los sistemas de información,

[L] Instalaciones

Lugares donde se hospedan los sistemas de información y comunicaciones.

[P] Personal

Personas relacionadas con los sistemas de información.

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

Existen muchas definiciones sobre los sistemas de Gestión de la seguridad de la información, sin embargo, para la presente investigación se tomará el definido en la ley 30024 que crea el Registro Nacional de Historias Clínicas Electrónicas y lo define como “Parte de un sistema

global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitorea, revisa, mantiene y mejora la seguridad de la información. El sistema de gestión incluye una estructura de organización, políticas, planificación de actividades, responsabilidades, procedimientos, procesos y recursos." (Ley N° 30024, 2013, p.2).

"El sistema de gestión de la seguridad de información 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 riesgos se manejan adecuadamente." (INDECOPI, 2014, p.vii) luego del análisis es la institución la encargada de realizar las acciones que sean más convenientes para manejar los riesgos encontrados.

La información es un activo para cualquier organización y aunque existen muchos soportes documentales diferentes, como la información en papel, en imágenes, almacenada electrónicamente, transmitida por correo electrónico, etc, "lo cierto es que, en la actualidad, la mayor parte de la información gestionada por una empresa se sustenta en la información automatizada (informatizada) a través de las nuevas herramientas de las Tecnologías de la Información y la Comunicación (TICs). Por este motivo, la tendencia de la norma ISO 27001 es tratar aspectos mayoritariamente del rango informático" (ISOTools Excellence, 2014, p.4)

"La definición y puesta en marcha de un SGSI basado en la norma ISO es especialmente atractiva para las organizaciones médicas, tanto públicas como privadas, por los siguientes motivos:

- La información que manejan es especialmente crítica y confidencial.
- Los requisitos y medidas planteados por la ISO 27001 garantizan la confidencialidad y seguridad de la información de los pacientes y trabajadores ante cualquier amenaza.
- En todo momento se preserva la confidencialidad, integridad y disponibilidad de la información.
- Con la aplicación de este sistema se consiguen ventajas adicionales como: mejorar la calidad de los servicios, disminuir los tiempos de espera o agilizar las comunicaciones internas y externas del hospital

o centro de salud." (ISOTools Excellence, 2014, p21), este análisis refuerza el fin de la investigación al ser aplicado a una institución relacionada con el tema de la salud de las personas y la relevancia de custodias la información personal bajo todas las medidas necesarias.

II.2.2.7. SGSI basado en la Norma ISO 27001

"La norma ISO 27001 es una solución de mejora continua en base a la cual puede desarrollarse un Sistema de Gestión de Seguridad de la Información (SGSI) que permita evaluar todo tipo de riesgos o amenazas susceptibles de poner en peligro la información de una organización tanto propia como datos de terceros. Además, también permite establecer los controles y estrategias más adecuadas para eliminar o minimizar dichos peligros." (ISOTools Excellence, 2014, p.4) Es decir, es un estándar que permite el desarrollo de un SGSI en un entorno empresarial o institucional y como todo estándar provee de las mejores prácticas en esta área.

ISO 27001 es un sistema basado en el ciclo de mejora continua o de Deming (Planificar-Hacer-Verificar-Actuar) también conocido como ciclo PDCA por sus siglas en inglés (Plan-Do-Check-Act).

"Estableciendo las necesidades de un SGSI y haciendo la comparación con el ciclo PDCA planteado por la ISO 27001 se dividiría en los siguientes pasos, cada uno de ellos ligado a una serie de acciones:" (ISOTools Excellence, 2014, p4)

Tabla 3

Ciclo PDCA y requisitos de un SGSI

Etapas PDCA	Requisitos SGSI
PLANIFICAR	Definir la política de seguridad
	Establecer al alcance del SGSI
	Realizar el análisis de riesgo
	Seleccionar los controles
	Definir competencias
	Establecer un mapa de procesos
	Definir autoridades y responsabilidades

HACER	Implantar el plan de gestión de riesgos Implantar el SGSI Implantar los controles
VERIFICAR	Revisar internamente el SGSI Realizar auditorías internas del SGSI Poner en marcha indicadores y métricas Hacer una revisión por parte de la Dirección
ACTUAR	Adoptar acciones correctivas Adoptar acciones de mejora

Nota. Ciclo estándar PDCA. Fuente: ISOTools Excellence, (2014)

II.2.2.8. Fases de un SGSI basado en la norma ISO 27001

En base al ciclo de la mejora continua PDCA, la norma ISO 27001 establece las siguientes fases para elaborar un SGSI

1. Análisis y evaluación de riesgos. "Es decir, un SGSI basado en la norma ISO 27001 se fundamenta principalmente en la identificación y análisis de las principales amenazas para, a partir de este punto de partida, poder establecer una evaluación y planificación de dichos riesgos. En definitiva, se trata de elaborar una adecuada gestión de riesgos que permita a las organizaciones conocer cuáles son las principales vulnerabilidades de sus activos de información." (ISOTools Excellence, 2014, p.7) este punto de partida es fundamental y para lograrlo se puede hacer uso de las metodologías de análisis de riesgos Informáticos que existen en la actualidad, en el caso de la presente investigación se ha optado por MAGERIT en su versión 3.0, previamente detallado en el apartado II.2.2.4.

2. Implementación de controles. "Con el objetivo de que cada riesgo identificado previamente quede cubierto y pueda ser auditable, la norma ISO 27001 establece en su última versión: ISO/IEC 27001:2013 hasta 113 puntos de control" (ISOTools Excellence, 2014) en el caso del Perú se tiene la NTP ISO/IEC 27001:2014 que se basa en la ISO 27001:2013

y que es de uso obligatorio en todas las entidades del estado y en la cual se establecen un total de 114 controles.

3. Definición de un plan de tratamiento de los riesgos o esquema de mejora. "Una vez realizado el análisis, se debe definir un plan de tratamiento o esquema de mejora, en el que se tengan en cuenta las distintas consecuencias potenciales de esos riesgos, estableciendo una criticidad para cada uno de ellos y así poder evaluar con objetividad las diferentes amenazas." (ISOTools Excellence, 2014)

4. Alcance de la gestión. "Teniendo en cuenta que existen organizaciones que difieren en tamaño por el número de empleados, volumen de información manejada, número de clientes, volúmenes de activos físicos y lógicos, número de sedes u oficinas, entre otros elementos, se hace necesario determinar cómo se debe implantar un SGSI. Por lo general, las primeras áreas que se deben considerar son aquellas que, por sus funciones y responsabilidades, ayudan en primera instancia a dar cumplimiento a la misión institucional." (ISOTools Excellence, 2014, p13)

5. Contexto de organización. "El análisis de contexto de la organización es fundamental para el SGSI, ya que nos permite determinar los problemas internos y externos de la organización, así como sus debilidades, amenazas, fortalezas y oportunidades que nos puedan afectar.

La norma ISO no especifica el método a utilizar para el análisis del contexto, siendo del método DAFO uno de los más comunes y aceptados. Sea cual sea el sistema elegido, es fundamental someter a valoración tanto el contexto interno (productos y servicios) como externos (logística o clima organizacional)." (ISOTools Excellence, 2014)

6. Partes interesadas. "Para poder realizar un correcto análisis de riesgo es preciso definir un contexto de la organización y comprender las necesidades y expectativas de todas las partes interesadas:

- Proveedores de servicios de información y de equipamientos de Tecnologías de la Información (TICs).

- Clientes, poniendo especial cuidado en la gestión de datos de protección personal.
- Fuerzas de seguridad de cada estado y autoridades jurídicas para tratar los aspectos legales.
- Participación en foros profesionales.
- La sociedad en general." (ISOTools Excellence, 2014)

7. Fijación y medición de objetivos. "Es necesario fijar unos objetivos para la gestión de riegos, los cuales deben poder ser medibles, aunque no es necesario que sean cuantificables. Otro aspecto básico es que estos objetivos deben ser eficientemente comunicados al conjunto de los empleados de la empresa, puesto que todos los profesionales deben ser conscientes de que participan en un objetivo común, y que un descuido o una mala actitud pueden acarrear consecuencias muy negativas." (ISOTools Excellence, 2014, p.16)

8. Proceso documental. "La norma ISO 27001 da mucha importancia a la documentación, estableciendo de manera muy estricta cómo se debe gestionar la documentación y exigiendo que la organización cuente con un procedimiento documentado para gestionar toda la información. Esta cuestión es fundamental para la obtención de la certificación.

La documentación puede ser presentada en diversos formatos: documentos en papel, archivos de texto, hojas de cálculo, archivos de vídeo o audio, etc. Pero en cualquier caso constituye un marco de referencia fundamental y debe estar lista en todo momento para que pueda ser consultada." (ISOTools Excellence, 2014, p.17)

9. Auditorías internas y revisión por la Dirección. "Para garantizar el correcto funcionamiento y mantenimiento de un SGSI basado en la norma ISO 27001, se hace necesario llevar a cabo auditorías internas cada cierto tiempo para poder comprobar que el sistema se encuentra en un estado idóneo." (ISOTools Excellence, 2014)

II.2.3. Marco Conceptual

- **Activo**: Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos,

servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos. (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012)

- **Amenaza**: Posible causa de un incidente no deseado, que puede resultar en daño a un sistema u organización (ISO/IEC 27000, 2016)
- **Análisis de Riesgo**: Proceso para comprender la naturaleza del riesgo y para determinar el nivel de riesgo (ISO/IEC 27000, 2016).
- **Ataque**: Intentar destruir, exponer, alterar, inhabilitar, robar u obtener acceso no autorizado o hacer uso no autorizado de un activo (ISO/IEC 27000, 2016)**.**
- **Confidencialidad**: La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados (ISO/IEC 27000, 2016).
- **Contexto externo**: Entorno externo en el que la organización persigue alcanzar sus objetivos (ISO/IEC 27000, 2016).
- **Contexto interno**: Ambiente interno en el que la organización busca alcanzar sus objetivos (ISO/IEC 27000:2016, 2016).
- **Control**: Medida que está modificando el riesgo (ISO/IEC 27000, 2016).
- **Control de Acceso**: Medios para asegurar que el acceso a los activos esté autorizado y restringido en base a los requisitos de negocios y seguridad (ISO/IEC 27000, 2016).
- **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.

  Propiedad de ser accesible y utilizable a petición de una entidad autorizada (ISO/IEC 27000, 2016).
- **Evaluación de riesgos**: El proceso global de la identificación del riesgo, el análisis de riesgo y la evaluación del riesgo (ISO/IEC 27000, 2016).

Proceso de comparación de los resultados del análisis de riesgo con criterios de riesgo para determinar si el riesgo y / o su magnitud es aceptable o tolerable (ISO/IEC 27000, 2016).

- **Evento**: Ocurrencia o cambio de un conjunto particular de circunstancias (ISO/IEC 27000, 2016).
- **Evento de seguridad de la información**: Identificó la ocurrencia de un estado del sistema, servicio o red que indica una posible violación de la política de seguridad de la información o fallo de los controles, o una situación previamente desconocida que puede ser relevante para la seguridad (ISO/IEC 27000, 2016).
- **Fuente de riesgo**: Elemento que, por sí solo o en combinación, tiene el potencial intrínseco de generar riesgo (ISO/Guide 73:2009, 2009).
- **Gestión de incidentes de seguridad de la información**: Procesos para detectar, informar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información (ISO/IEC 27000, 2016).
- **Gestión de Riesgos**: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo (ISO/IEC 27000, 2016).
- **Gestión ejecutiva**: Persona o grupo de personas que han delegado la responsabilidad del cuerpo directivo para la implementación de estrategias y políticas para lograr el propósito de la organización (ISO/IEC 27000, 2016).
- **Identificación de Riesgos**: Proceso de encontrar, reconocer y describir los riesgos (ISO/IEC 27000, 2016).
- **Incidente de seguridad de la información:** Es única o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones comerciales y amenazar la seguridad de la información (ISO/IEC 27000, 2016).
- **Integridad**: Mantenimiento de la exactitud y completitud de la información y sus métodos de procesos.
  Propiedad de exactitud y completo (ISO/IEC 27000, 2016).
- **Nivel de riesgo**: Magnitud de un riesgo expresada en términos de la combinación de consecuencias y su probabilidad (ISO/IEC 27000, 2016).

- **Objetivo de Control**: Declaración que describe lo que se logrará como resultado de la implementación de controles (ISO/IEC 27000:2016, 2016).
- **Políticas**: Intenciones y dirección de una organización expresada formalmente por su alta dirección (ISO/IEC 27000:2016, 2016).
- **Políticas de Seguridad de la Información**: Sistema por el cual las actividades de una organización dirigidas y controladas en seguridad de la información (ISO/IEC 27000:2016, 2016).
- **Probabilidad**: Posibilidad de que algo suceda (ISO/IEC 27000, 2016).
- **Proceso de Gestión de Riesgo**: La aplicación sistemática de políticas, procedimientos y prácticas de gestión a las actividades de comunicación, consulta, establecimiento del contexto e identificación, análisis, evaluación, tratamiento, seguimiento y revisión del riesgo (ISO/IEC 27000, 2016).
- **Propietario de riesgo**: Persona o entidad con la responsabilidad y autoridad para manejar un riesgo (ISO/IEC 27000, 2016).
- **Riesgo**: Es el efecto de la incertidumbre sobre los objetivos (ISO/IEC 27000, 2016).
- **Riesgo Aceptado**: Decisión informada de tomar un riesgo particular (ISO/IEC 27000, 2016).
- **Riesgo Residual**: Riesgo restante después del tratamiento de riesgo (ISO/IEC 27000, 2016).
- **Sistema de Gestión**: Conjunto de elementos interrelacionados o interactuantes de una organización para establecer políticas, objetivos y procesos para lograr esos objetivos (ISO/IEC 27000, 2016).
- **Sistema de información**: Aplicaciones, servicios, activos de tecnología de la información u otros componentes de manejo de información (ISO/IEC 27000, 2016).
- **Stakeholder**: Persona u organización que pueda afectar, verse afectada o percibirse afectada por una decisión o actividad (ISO/IEC 27000, 2016).
- **Supervisión**: Determinar el estado de un sistema, un proceso o una actividad (ISO/IEC 27000, 2016).

- **Tratamiento de riesgo**: Proceso para modificar el riesgo (ISO/IEC 27000, 2016).
- **Vulnerabilidad**: Debilidad de un activo o control que puede ser explotada por una o más amenazas (ISO/IEC 27000, 2016).

III. HIPÓTESIS

III.1 Declaración de hipótesis

La dimensión Administrativa de la Gestión de la Historia Clínica es la más relevante en la Seguridad de la Información

Variables

III.1.1 Variable Independiente

Gestión de la Historia Clínica

III.1.2 Variable dependiente

Seguridad de la Información

III.2 Operacionalización de variables

Tabla 4

Operacionalización de Variable Independiente

VARIABLE	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIONES	INDICADORES	Items
Gestión de la Historia Clínica	Documento físico de registro único y válido desde el punto de vista clínico y legal. Registra los datos de identificación, datos clínicos relacionados a la situación de un paciente, las intervenciones practicadas, su proceso evolutivo, tratamiento y recuperación de la atención que el profesional de la salud brinda al paciente, Se presenta como narración o exposición de hechos e incluye	Documento físico, electrónico, Médico legal, que cumple con los mecanismos y procedimientos de la gestión del uso, manejo, conservación y depuración de las Historias Clínicas. El proceso de gestión y administración de la Historia Clínica se realiza en los componentes técnico administrativos y asistenciales (MINSA, 2015)	Administrativo	Historia clínica debe ser: ● Única ● Cronológica ● Pulcra ● Secuencial Debe estar: ● Segura ● Disponible ● Integra ● Depurada Debe estar organizado: ● Activas ● Pasivas ● Especiales	**Técnicos Administrativas** 1. ¿Se verifica que al momento de crear la historia clínica sea única en la institución? 2. ¿Se crea una historia física al crear la Historia Clínica en el Sistema de Gestión Hospitalaria? 3. ¿Toda documentación en la atención médica que se genera tiene el DNI como identificación? 4. ¿A los neonatos con patología se le crea una Historia Clínica propia? 5. ¿A los neonatos nacidos normales o natimuertos se le archiva en la Historia Clínica de la madre? 6. ¿Se conserva en forma íntegra, garantizando el orden cronológico y todos los formatos de la atención de salud? 7. ¿El archivo de historias clínicas está diferenciado en activos y pasivos? 8. ¿Se cuenta con un ambiente separado para las Historias Clínicas especiales con contenido potencial de implicancia médico legal? 9. ¿Cuenta con medidas de seguridad este archivo especial de Historias Clínicas con implicancia médico legal? 10. ¿Se ha gestionado los recursos humanos, físicos y apoyo logístico de forma continua para la

Continúa

	juicios, documentos, procedimientos, informaciones, consentimiento informado entre otros. (Gerencia General de EsSalud, 2014)	conservación de la documentación? 11. ¿Se encuentra establecido quien es el responsable de la custodia de las HC físicas en el archivo? 12. ¿Se encuentra establecido quien es el responsable de la custodia de las HC físicas en caso de salir del archivo? 13. ¿Se encuentra actualizado los datos el sistema informático para el registro, control y monitoreo de la Historia Clínica, para el seguimiento y ubicación? 14. ¿Se atienden las copias de solicitudes de las Historias Clínicas solicitadas por los pacientes o por mandato judicial? 15. ¿En el servicio de Hospitalización la enfermera de cada servicio donde está en paciente es responsable de la Historia Clínica? 16. ¿En el servicio de Hospitalización la enfermera entrega la historia clínica completa y ordenada al archivo dentro de las 48 horas siguientes al momento del alta? 17. ¿La historia de los pacientes fallecidos son entregados al área de Epidemiología? 18. ¿El área de Epidemiología entrega la historia clínica al archivo dentro de las 72 horas de su recepción? 19. ¿Las historias clínicas usadas en la Consulta Externa son devueltas el mismo día? 20. ¿Las historias clínicas usadas en la Hospitalización o Emergencia son devueltas a las 48 horas del alta del paciente? 21. ¿Las historias clínicas usadas para informes médicos o auditorias médicas son devueltas en un plazo menor a 72 horas?

22. ¿El archivo de historias cuenta con un Plan de Fumigaciones al menos trimestralmente?
23. ¿Cuenta con ventilación adecuada, ventiladores, aire acondicionado, extractores e inyectores de aire, deshumedecedores el archivo de historias físicas?
24. ¿La historia clínica se encuentra protegida mediante fólderes?
25. ¿Las historias clínicas depuradas se encuentran almacenadas en cajas de cartón o según normatividad vigente?
26. ¿El área de archivo cuenta con señalización?
27. ¿El área de archivo cuenta con sistemas contraincendios, extintores y detectores de humo?
28. ¿El área de archivo cuenta con sistema de videocámaras?
29. ¿El área de archivo cuenta con sala de trabajo, sala de lectura y cuentan con videocámara?
30. ¿Se realiza el proceso de depuración anual de las HC de archivo?
31. ¿El archivo activo cuenta con información de historias clínicas con su última atención menor a cinco años?
32. ¿Se realiza la destrucción total de las historias clínicas del archivo pasivo mayores a 10 años y que sólo cuenten con atenciones de consulta externa?
33. ¿Se realiza la destrucción selectiva de las historias clínicas del archivo pasivo mayores a 10 años y que contienen atenciones de hospitalización?

En caso de contar con un Comité de Auditoría de Historias Clínicas

34. ¿Se informa al Comité de Historias Clínicas con acta de la destrucción total y selectiva de las historias clínicas mayores a 10 años del archivo pasivo?
35. ¿El Comité de Auditoría de Historias Clínicas informa los hallazgos encontrados?
36. ¿Cuenta con un Sistema de Historia Clínica informatizada?

En caso de contar con un Sistema de Historia Clínica Informatizada

37. ¿Se hacen auditorias regulares al Sistema de Historia Clínica Informatizada?
38. ¿Cuenta con un servidor apropiado para almacenar las HC electrónicas?
39. ¿Se cuenta con copias de seguridad diarias de las HC?
40. ¿Se cuenta con seguridad el acceso a los Servidores de las HC?
41. ¿Se cuenta con señalización el Centro de Cómputo de la Red Asistencial Cajamarca?
42. ¿Se cuenta con sistemas contra incendios, extintores y detectores de humo?

Otros

43. ¿Cuenta con el Plan de continuidad del Negocio?
44. ¿Realiza las pruebas del Plan de Continuidad del Negocio?

			Asistencial	La Historia Clínica debe tener: ● Acto Médico ● Prácticas y procedimientos aplicados al paciente. ● Código CIE10 ● Firma y Sello del Profesional Asistencial	**Técnicos Asistenciales** 45. ¿Se tiene la reserva de la información relacionada con el acto médico y su historia clínica? 46. ¿El registro por parte de los profesionales de la salud contiene las prácticas y procedimientos aplicados al paciente? 47. ¿Todas las atenciones médicas y no médicas cuentan con acto médico? 48. ¿Cada atención tienen registrado el código CIE-10? 49. ¿Todas las atenciones tienen la firma y sello del profesional asistencial? 50. ¿Cuenta con un Comité de Auditoría de Historias Clínicas?

Nota. De acuerdo a formato UPN.

Tabla 5

Operacionalización de Variable dependiente

VARIABLE	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIONES	INDICADORES	Items
Seguridad de la Información	Conjunto de buenas prácticas para garantizar el resguardo y protección de la información, asegurando que los riesgos asociados sean	Según la NTP-ISO/IEC 27001:2014 se refiere a la confidencialidad, la integridad y la disponibilidad de la información y los datos importantes para la organización, independientemente del	Protección	Confidencialidad	A.5 Políticas de Seguridad en la Información. A.6 Organización de la seguridad de la información. A.7 Seguridad de los recursos humanos. A.8 Gestión de Activos A.9 Control de acceso. A.10 Criptografía A.11 Seguridad física y ambiental. A.12 Seguridad de las operaciones A.13 Seguridad de las comunicaciones A.14 Adquisición, desarrollo y mantenimiento de sistemas.

conocidos, asumidos, gestionados y minimizados. (ISO/IEC 27000, 2016, p.14)	formato que tengan, estos pudiendo ser: Electrónicos, en papel, audio y vídeo, etc.	Exactitud	Integridad	A.15 Relación con los proveedores A.16 Gestión de incidentes de seguridad de la información A.17 Aspectos de seguridad de la información en la gestión de la continuidad del negocio. A.18 Cumplimiento.
		Acceso a la Información	Disponibilidad	

Nota. De acuerdo a formato UPN

III.3 Propuesta de solución

III.3.1 Mejora de los procesos de la Gestión de la Historia Clínica

III.3.1.1 Actualización de la Norma Gestión de las Historias Clínicas por:

- No se profundiza sobre las TIC en la Gestión de las Historias Clínicas.
- Uso de Sistemas Informáticos para la Gestión Hospitalaria y actualización de los Manuales de Usuario.
- Adaptar las recomendaciones dadas teniendo en consideración la Ley 30024 sobre el "Registro Nacional de Historias Clínicas Electrónicas".

III.3.1.2 Incluir en el Plan de Capacitación Local de la Red Asistencial Cajamarca las siguientes actividades:

- Charla sobre Gestión de las Historias Clínicas uso y recomendaciones para todo el personal involucrado directa e indirectamente.
- Charla de los Sistema de Gestión de la Seguridad de la Información en instituciones públicas.
- Gobierno electrónico y uso de la Norma Técnica Peruana sobre Seguridad de la Información

III.3.1.3 Seguir realizando de acuerdo a norma la depuración de las historias clínicas anualmente.

III.3.1.4 Realizar el requerimiento dentro del Presupuesto Institucional de Apertura PIA del siguiente año para la adquisición de los siguientes bienes y servicios:

- Construcción de Archivo de Historias Clínicas Especiales.
- Contratación de los Servicios para Fumigación trimestralmente.
- Compra de equipos necesarios para salvaguardar el archivo de historias clínicas y el centro de cómputo de la Red Asistencial Cajamarca como ventiladores, aire acondicionado, extractores o inyectores de aire, deshumedecedores, sistemas contraincendios, extintores y detectores de humo.
- Elaboración de señalización para el archivo de Historias Clínicas y el Centro de Cómputo donde se ubican los servidores de los Sistemas Informáticos.

- Construcción de salas de trabajo y lectura.
- Adquisición de circuito cerrado para el archivo de Historias Clínicas, el Centro de Cómputo de la Red Asistencial Cajamarca y las futuras Salas de Trabajo y Lectura del Archivo de Historias Clínicas.

III.3.2 Análisis de Brechas (GAP Análisis)

Para el desarrollo de nuestra propuesta en el aspecto de la seguridad de la información, nos basamos en los requisitos que establece la NTP-ISO/IEC 27001 2014 y realizamos sobre ello un análisis de brechas en base a los controles y objetivos de control que establece dicha norma y lo que la institución regula o tiene implementado para cumplir con tal fin, además de ello se ha realizado un análisis de riesgos informáticos siguiendo la metodología Magerit, el cual se adjunta a la lista de anexos y ha permitido complementar al análisis de brechas en temas de seguridad.

A) OBJETIVO

Evaluar la implementación actual de cada control de la NTP-ISO/IEC 27001 2014 en lo referente a la gestión de la seguridad de la Información en el Hospital II Cajamarca - EsSalud, con el fin de determinar el grado de cumplimiento de éstos y luego de analizar los resultados realizar una propuesta para las mejoras relacionadas con la Seguridad de la Información.

B) METODOLOGÍA

El análisis se lleva a cabo mediante el uso de instrumentos de recolección de datos (entrevistas) así como de visitas presenciales al Hospital II Cajamarca - EsSalud, para poder observar y analizar el proceso de gestión de las Historias Clínicas.

Las actividades llevadas a cabo durante esta fase son las siguientes:

- Entrevistas en sitio realizadas al responsable del área de Informática, responsable del área de admisión, personal del área de admisión encargados del resguardo y gestión de las historias clínicas físicas lo que se busca con estas tareas es completar el cuestionario

relacionado al cumplimiento de los controles de la NTP ISO/IEC 27001 2014.

- Revisión de la documentación de las políticas y procedimientos definidos en la organización.
- Calificación general en Seguridad de la Información.
- Propuesta de mejora y recomendaciones a la Institución.

C) MÉTODO DE VALORACIÓN

La valoración se hace en base a un análisis del cumplimiento o no de cada control que esté relacionado al proceso de estudio de la presente investigación que es la Gestión de las Historias Clínicas.

Para los fines del presente análisis se determinó la siguiente clasificación:

- NO (0%- 30%): El control no se encuentra implantado, o su nivel de implantación y gestión es muy débil;
- PARCIAL (31% - 70%): Se tienen algún nivel de implantación con relación a los controles que el dominio establece, pero no se hace en su totalidad.
- SI (71% - 100%): El dominio se encuentra implantado.

Los valores dados a cada control se suman y se promedian agrupados en el objetivo de control al cual pertenecen, y se calcula un valor numérico que indica el porcentaje de cumplimiento con la norma. Para obtener el promedio de cumplimiento de la norma por dominio, se suman y se promedian todos los controles pertenecientes al dominio.

Este mismo ejercicio se hace para el total de los controles y se obtiene el porcentaje de cumplimiento frente al estándar NTP-ISO/IEC 27001 2014.

D) APLICACIÓN

Luego de la evaluación de los controles de cada dominio se procedió a llenar los valores siguiendo las indicaciones del método de valoración, estos resultados son los que se presentan a continuación.

Los objetivos de control y controles listados a continuación son directamente derivados desde y alineados con los listados en ISO/IEC 27001:2014, Cláusulas 5 a 18 (INDECOPI, 2014)

5. POLÍTICA DE SEGURIDAD

5.1. Política de seguridad de la información

EsSalud cuenta con una política de seguridad de la información elaborada por la Gerencia Central de Organización e Informática, sin embargo no es aplicada en su totalidad por las diferentes redes asistenciales.

Tabla 6

Política de seguridad de la información

CONTROL		PREGUNTA	SI	PARCIAL	NO	N/A	CONCLUSIÓN
5.1.1.	Documento de política de Seguridad de la Información	¿Ha sido aprobado por la dirección un documento que contenga la política de seguridad de la información, y ha sido publicado y comunicado a todos los empleados y terceras partes relevantes?	X 100%				ESSALUD tiene definida sus Políticas para la seguridad de la información y están publicadas en la Intranet institucional
5.1.2.	Revisión de la política de Seguridad de la Información	¿La política de seguridad de la información se revisa en intervalos planificados, o si ocurren cambios significativos, para asegurar que sigue siendo conveniente, suficiente y efectiva?			X 30%		ESSALUD no tiene implementada la revisión de las políticas a intervalos regulares de tiempo.

Nota. Adaptación de la NTP ISO/IEC 27001:2014 Fuente: INDECOPI, (2014)

6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

6.1. Organización Interna

ESSALUD Debería elaborar un inventario de activos con sus responsables y el estado en el que se encuentran.

Debe tener cuidado de que ninguna persona pueda acceder, modificar o utilizar activos sin autorización o detección de acuerdo a la estructura de segregación de funciones que la institución debe también determinar.

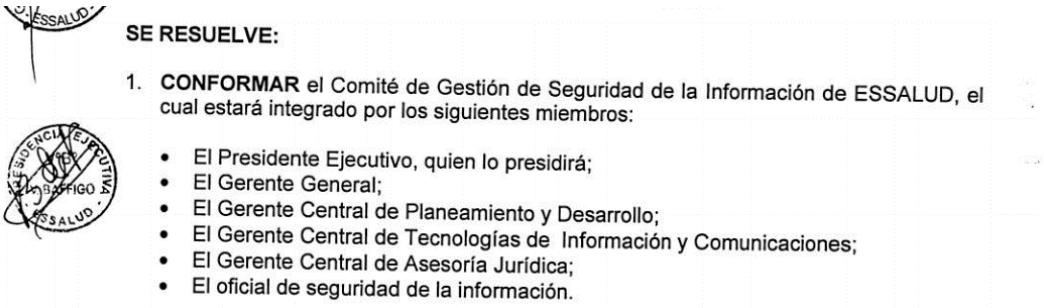
Lo proyectos que debe llevar a cargo la institución deben tener una metodología para su administración que permita identificar el activo para poder utilizarlo y resguardar su valor e integridad.

Tabla 7

Organización Interna

	CONTROL	PREGUNTA	SI	PARCIAL	NO	N/A	CONCLUSIÓN
6.1.1.	Roles y responsabilidades en la Seguridad de Información	¿Se han definido y asignado claramente todas las responsabilidades de seguridad de la información?	x 100%				ESSALUD tiene establecidas las responsabilidades funcionales y por uso.
6.1.2.	Segregación de funciones	¿Se tienen adecuadamente separados los deberes y áreas, minimizando las oportunidades de mal uso de los activos de información?	x 75%				Se tiene una segregación de funciones individuales por mejorar aún.
6.1.3.	Contacto con autoridades	¿Se mantiene una relación apropiada con las autoridades relevantes (p.e. Policía, Bomberos)?	x 100%				ESSALUD cuenta con un directorio nacional y local con todas las instituciones relevantes.
6.1.4.	Contacto con grupos de interés	¿La organización mantiene contacto con grupos de interés, foros de especialistas en seguridad o en asociaciones profesionales?			x 30%		ESSALUD, cuenta con grupo de profesionales interno pero hace falta generar nexos con grupos externo para temas de seguridad de la información.
6.1.5.	Seguridad de información en la gestión de proyectos	¿Se incluyen y conducen aspectos de seguridad de información en la gestión de proyectos, de acuerdo al tipo de proyecto?			x 0%		No se contemplan temas de seguridad de la información en la gestión de proyectos.

Nota**.** Adaptación de la NTP ISO/IEC 27001:2014 Fuente: INDECOPI, (2014)



SE RESUELVE:

1. **CONFORMAR** el Comité de Gestión de Seguridad de la Información de ESSALUD, el cual estará integrado por los siguientes miembros:

- El Presidente Ejecutivo, quien lo presidirá;
- El Gerente General;
- El Gerente Central de Planeamiento y Desarrollo;
- El Gerente Central de Tecnologías de Información y Comunicaciones;
- El Gerente Central de Asesoría Jurídica;
- El oficial de seguridad de la información.

Figura 9. Conformación de Comité de Seguridad de la Información. Resolución de Presidencia Ejecutiva Nº 180-PE-ESSALUD-2016

6.2. Dispositivos Móviles y Teletrabajo

ESSALUD debe complementar la norma sobre el uso de los dispositivos móviles para protegerlos de los riesgos a los que estarían expuesto.

La institución debería realizar un análisis de los puestos de trabajo en los que se podría aplicar el teletrabajo y en base a este análisis se tendría que desarrollar las políticas, procedimientos y normas que se deberían tener en cuenta para la contratación de personal bajo esta modalidad.

Tabla 8

Dispositivos Móviles y Teletrabajo

	CONTROL	PREGUNTA	SI	PARCIAL	NO	N/A	CONCLUSIÓN
6.2.1.	Política para dispositivo móvil	¿Existe una política formal y se han adoptado las medidas de seguridad necesarias para protegerse en contra de los riesgos de utilizar computadores móviles e infraestructura de comunicaciones?			X 0%		No existe una política de la institución al respecto
6.2.2.	Teletrabajo	¿Se ha desarrollado una política, unos planes operativos, y unos procedimientos para regular las actividades del teletrabajo?			X 0%		No se tiene implementado el Teletrabajo de acuerdo a la Ley No. 30036

Nota**.** Adaptación de la NTP ISO/IEC 27001:2014 Fuente: INDECOPI, (2014)

7. SEGURIDAD DE LOS RECURSOS HUMANOS

7.1. Previo al empleo

Tabla 9

Seguridad de la Información Previo al empleo de personal en ESSALUD

CONTROL		PREGUNTA	SI	PARCIAL	NO	N/A	CONCLUSIÓN
7.1.1.	Investigación de antecedentes	¿Se realizan las verificaciones oportunas de los antecedentes de todos los candidatos para un empleo, de los contratistas y terceras partes, siempre de acuerdo a las leyes y regulaciones vigentes, la ética y siempre de manera proporcional a los requerimientos del negocio, la clasificación de la información a la que accederá y los riesgos percibidos?		X 70%			Se realiza el proceso de acuerdo a los siguientes pasos: Evaluación Pre curricular. Evaluación Psicotécnica. Evaluación de conocimientos. Evaluación curricular. Entrevista personal.
7.1.2.	Términos y condiciones del empleo	¿Se les exige a los empleados, contratistas y terceras partes estar de acuerdo y firmar los términos y condiciones de su contrato de empleo, y este contrato establece las responsabilidades tanto del empleado como las de la organización, en materia de seguridad de la información?		X 60%			Se establece en el contrato los términos y condiciones los cuales abarcan en general tres aspectos: • Seguridad en el trabajo. • Ética pública. • Resguardo de los bienes patrimoniales.

Nota. Adaptación de la NTP ISO/IEC 27001:2014 Fuente: INDECOPI, (2014)

7.2. Durante el empleo

ESSALUD debería establecer visitas de verificación inopinadas para comprobar los aspectos de seguridad de acuerdo a las políticas establecidas.

Cada empleado debería de tener un mínimo de seis horas de capacitación al año sobre temas de seguridad de la información.

Se debe incluir dentro de la inducción al personal nuevo aspectos relacionados a la seguridad de la información.

Se debe desarrollar material impreso y digital sobre aspectos relevantes a la seguridad de la información y socializarlo con los empleados y contratistas.

Se debería modificar el reglamento interno de trabajo creando normas y controles relacionados a las infracciones en temas de seguridad de la información para todos los tipos de regímenes laborales.

Tabla 10

Durante el empleo

	CONTROL	PREGUNTA	SI	PARCIAL	NO	N/A	CONCLUSIÓN
7.2.1.	Responsabilidades de la gerencia	¿La dirección exige a los empleados, contratistas y terceras partes aplicar seguridad de acuerdo con las políticas y procedimientos establecidos por la organización?			X 30%		Se emiten cada cierto tiempo (por lo general anualmente) documentos que son remitidos por la gerencia sobre temas referidos a uso de fotochecks, uniforme, seguridad informática, escritorio limpio, etc.
7.2.2.	Concientización, educación y entrenamiento en la seguridad de la información.	¿Los empleados y, cuando es relevante, contratistas y terceras partes, reciben el entrenamiento adecuado sobre concientización en seguridad de la información y se les mantiene actualizados sobre las políticas y procedimientos de la organización que son relevantes para el cumplimiento de las			X 0%		Falta de asignación presupuestal para entrenamiento en temas de seguridad de la Información tanto para empleados como contratistas.

		funciones de su trabajo?				
7.2.3.	Proceso disciplinario	¿Existe algún proceso disciplinario formal para tratar con los empleados que infringen la seguridad de la organización?		X 70%		Hay procesos para temas de incumplimiento de contrato pero no está especificado para temas de seguridad de la información en la organización.

Nota**.** Adaptación de la NTP ISO/IEC 27001:2014 Fuente: INDECOPI, (2014)

7.3. Finalización o cambio de empleo

ESSALUD para el término de contrato por cualquier modalidad debe establecer las cláusulas que prohíban el uso, difusión u otros aspectos con fines personales o comerciales sobre la información con la cual el personal tuvo contacto durante su tiempo de trabajo dentro de la institución

Tabla 11

Finalización o cambio de empleo

	CONTROL	PREGUNTA	SI	PARCIAL	NO	N/A	CONCLUSIÓN
7.3.1.	Finalización de responsabilidades	¿Han sido claramente definidas y asignadas las responsabilidades para realizar la finalización de un contrato de trabajo o cambios en el empleo?			X 0%		No se realiza ni hay control de esta actividad dentro de la institución

Nota**.** Adaptación de la NTP ISO/IEC 27001:2014 Fuente: INDECOPI, (2014)

8. GESTION DE ACTIVOS

8.1. Responsabilidad de los activos

ESSALUD debe implementar el inventario de activos de información y definir a los responsables para cada activo, además cada activo debería tener asociado los procedimientos, manuales de uso u otra documentación necesaria para garantizar su uso adecuado. En la presente investigación se ha realizado un inventario de activos de información el cual está más ligado a la gestión de la Historia Clínica, pero puede servir como una primera versión sobre la cual se agregarían los demás activos con los que cuenta la institución.

Se debe normar además las devoluciones de activos y asegurar así la información almacenada en ellos.

Tabla 12

Responsabilidad de los activos

CONTROL		PREGUNTA	SI	PARCIAL	NO	N/A	CONCLUSIÓN
8.1.1.	Inventario de activos	¿Todos los activos están identificados de forma clara, y se ha elaborado y mantenido un inventario de todos los activos importantes?		X 60%			Se tiene un inventario de equipos informáticos, pero no se ha realizado la clasificación. Se tiene inventariado el parque informático a través de un registro de bienes patrimoniales.
8.1.2.	Propiedad de activos	¿Toda la información y activos asociados con la infraestructura para el procesamiento de la información, han sido asignados a un área específica de la organización?			X 30%		Los bienes patrimoniales están asignado al personal pero no están clasificados como activos.
8.1.3.	Uso adecuado de activos	¿Las reglas para el uso correcto de la información y de los activos asociados a la infraestructura para el procesamiento de la información, han sido identificadas, documentadas e implementadas?	X 75%				Se cuenta con algunas reglas, políticas, documentación y en algunos casos manuales de uso de información.
8.1.4.	Devolución de activos	¿Se requiere que todos los empleados, contratistas y usuarios de terceras partes, devuelvan todos los	X 75%				Existe una norma para devolución de bienes patrimoniales.

		activos de la organización que se encuentren en su posesión en el momento de la terminación del empleo, contrato o acuerdo?					

Nota**.** Adaptación de la NTP ISO/IEC 27001:2014 Fuente: INDECOPI, (2014)

8.2. CLASIFICACIÓN DE LA INFORMACIÓN

ESSALUD debe mejorar la clasificación de la información de acuerdo a los requisitos legales, valor y criticidad de la misma así mismo definir un esquema que lleve a mejorar los procedimientos necesarios para su etiquetado y separación.

Tabla 13

Clasificación de la información

CONTROL		PREGUNTA	SI	PARCIAL	NO	N/A	CONCLUSIÓN
8.2.1.	Clasificación de la información	¿Se ha clasificado la información con base en su valor, requerimientos legales vigentes, sensibilidad y que tan crítica es para la organización?	X 75%				Se tiene implementada de cierta manera una clasificación de la información médica asistencial y administrativa.
8.2.2.	Etiquetado de la información	¿Existen adecuados procedimientos de etiquetamiento de la información de acuerdo al esquema de clasificación de la organización?			X 0%		La organización no ha definido los procedimientos de clasificación de la información.
8.2.3.	Manejo de activos	¿Se ha desarrollado e implantado un conjunto de procedimientos apropiado para el manejo de activos de información, de acuerdo con el			X 0%		No se han definido e identificado los activos de información como tal y no se tienen procedimientos para el manejo de información.

		esquema de clasificación adoptado por la organización?					

Nota**.** Adaptación de la NTP ISO/IEC 27001:2014 Fuente: INDECOPI, (2014)

8.3. Manejo de medios

ESSALUD debe establecer un procedimiento para el control y uso de los medios removibles de acuerdo a las políticas y perfiles de usuarios.

Se debe formalizar el proceso de desecho o reutilización de los medios removibles y asegurar el control de los datos que estos podrían almacenar.

Tabla 14

Manejo de medios

CONTROL		PREGUNTA	SI	PARCIAL	NO	N/A	CONCLUSIÓN
8.3.1.	Gestión de los medios removibles	¿Existen procedimientos para la administración de los medios removibles?	X 75%				Se han implementado algunos procedimientos para el control de medios removibles
8.3.2.	Eliminación de medios	¿Se revisan todos los medios, para asegurarse que ningún tipo de dato sensible o software licenciado haya sido eliminado o sobrescrito con seguridad antes del desecho o reutilización del medio?	X 75%				Se sigue la norma de procedimiento de bienes de baja a través de control patrimonial pero se debe incidir en la verificación la información contenida en los activos de información.
8.3.3.	Transferencia de medios físicos	¿Los medios que contienen información, están protegidos en contra del acceso no autorizado, el mal uso o su alteración durante el transporte más allá			X 20%		No se tiene control sobre el traslado de cualquier medio de información.

		de los límites físicos de la organización?				

Nota**.** Adaptación de la NTP ISO/IEC 27001:2014 Fuente: INDECOPI, (2014)

9. CONTROL DE ACCESO

9.1. Requerimientos de negocio para el control del acceso

Tabla 15

Requerimientos de negocio para el control del acceso

CONTROL		PREGUNTA	SI	PARCIAL	NO	N/A	CONCLUSIÓN
9.1.1.	Política de control de acceso	¿Se ha establecido y documentado una política de control de acceso con base en los requisitos de seguridad y del negocio, y ésta política ha sido revisada de forma regular?	X 75%				Se tiene normas para el acceso a la Institución, algunas áreas por parte de los usuarios y del personal de la Institución son controladas por vigilancia, igualmente el acceso a los sistemas informáticos se da de acuerdo al perfil y responsabilidades.
9.1.2.	Acceso a redes y servicios de red	¿Los usuarios tienen acceso exclusivamente a los servicios a los que se les ha autorizado específicamente?	X 80%				Todo está en una red interna y se tiene acceso de acuerdo a los tipos de usuario de los sistemas de información.

Nota**.** Adaptación de la NTP ISO/IEC 27001:2014 Fuente: INDECOPI, (2014)

9.2. Gestión de accesos de usuarios

Tabla 16

Gestión de accesos de usuarios

CONTROL		PREGUNTA	SI	PARCIAL	NO	N/A	CONCLUSIÓN
9.2.1.	Registro de usuarios	¿Existe un procedimiento formal	X 90%				Se realiza en los mismos sistemas pero

		de registro y de salida del registro para los usuarios de la organización con el fin de garantizar o revocar el acceso a todos los sistemas de información y servicios?			no se gestiona a nivel global
9.2.2.	Gestión de acceso de usuarios	¿Se restringe y controla la asignación y retiro accesos?	X 75%		No existe proceso formal para la gestión de los usuarios en las altas, bajas y/o modificaciones de accesos y privilegios, pero se hace en base a la información que es alcanzada al área de informática.
9.2.3.	Gestión de los accesos privilegiados	¿Se restringe y controla la asignación y uso de accesos privilegiados?	X 100%		Se le da en las funciones (MOF) y en los accesos que se crean por el administrador de los sistemas.
9.2.4.	Gestión de la información secreta de autenticación	¿Existen procesos formales de gestión y control de la información de autenticación asignada?		X 50%	Los sistemas contemplan la gestión como: - cambio de clave por primera vez - renovación de claves por periodos.
9.2.5.	Revisión de los derechos de acceso de los usuarios	¿Los derechos de acceso de los usuarios, se revisan en intervalos regulares de tiempo siguiendo un proceso formal?	X 80%		Se realiza cada cierto tiempo un control y depuración de privilegios, también se ejecuta luego de la realización de cambios en las áreas de la institución.
9.2.6.	Retiro de los permisos de acceso	¿Una vez se termina el contrato, se retiran inmediatamente todos los derechos de acceso a la información y a la infraestructura para el	X 75%		Se controla y se restringe los accesos físicos y de sistema, pero no se hace de manera inmediata, existe un poco de

		procesamiento de la información de los empleados, contratistas y terceras partes, o si fuese el caso, se ajustan si hay cambios?					retraso en el alcance de información. Los terceros son: - EsSalud en Línea - Módulo de Atención al Asegurado - Mantenimiento - Limpieza - Vigilancia

Nota**.** Adaptación de la NTP ISO/IEC 27001:2014 Fuente: INDECOPI, (2014)

9.3. Responsabilidades de usuario

Tabla 17

Responsabilidades de usuario

CONTROL		PREGUNTA	SI	PARCIAL	NO	N/A	CONCLUSIÓN
9.3.1.	Uso de información secreta de autenticación	¿Se requiere que los usuarios sigan buenas prácticas de seguridad en la selección y el uso de información secreta de autenticación?	X 100%				Se controla a través del contrato de los trabajadores que acceden a sistemas informáticos. Se cumplen políticas de claves de acceso.

Nota**.** Adaptación de la NTP ISO/IEC 27001:2014 Fuente: INDECOPI, (2014)

9.4. Control de acceso a la información y las aplicaciones

Tabla 18

Control de acceso a la información y las aplicaciones

CONTROL		PREGUNTA	SI	PARCIAL	NO	N/A	CONCLUSIÓN
9.4.1.	Restricción de acceso a la información	¿El acceso a las funciones del sistema de información y	X 90%				Los sistemas tienen perfiles de usuarios para restringir el

		aplicación, es restringido para los usuarios y personal de soporte, de acuerdo con la política de control de acceso?			acceso de acuerdo al perfil. Ambientes físicos resguardados físicamente con cámaras de video vigilancia. Historias clínicas resguardadas por medio de un procedimiento normado (Acceso, devolución)
9.4.2.	Procedimientos de inicio seguro de sesión	¿El acceso a los sistemas operativos está controlado por un procedimiento de inicio de sesión seguro?		X 30%	Capa persona utiliza un usuario y clave para ingreso a cualquier equipo de cómputo. Se debe establecer un mejor control de acceso.
9.4.3.	Sistema de gestión de contraseñas	¿Los sistemas de gestión de contraseñas son interactivos y aseguran igualmente la calidad de las contraseñas?	X 100%		Existe una consola de administración y las contraseñas cumplen con características de complejidad (longitud, uso de caracteres especiales, historicidad de claves, etc)
9.4.4.	Uso de las utilidades del sistema	¿El uso de programas de usuario capaces de modificar el sistema y los controles de las aplicaciones, está restringido y fuertemente controlado?		X 30%	Se prohíbe la instalación de cualquier tipo de software, pero no siempre se hace efectivo al tener algunos perfiles de usuario con privilegios.
9.4.5.	Control de acceso al código fuente del programa	¿Está restringido el acceso al código fuente de los programas?	X 100%		No se cuenta con los códigos fuentes de los sistemas principales de EsSalud

						- Sistema de Gestión Hospitalaria - SAP R/4

Nota**.** Adaptación de la NTP ISO/IEC 27001:2014 Fuente: INDECOPI, (2014)

10. CRIPTOGRAFÍA

10.1. Controles criptográficos

Definir dentro de la Política de Seguridad Informática los aspectos sobre el uso de controles criptográficos para toda la organización

Incluir dentro de la Política de Seguridad Informática los procedimientos y normas para la gestión de claves.

Tabla 19

Controles criptográficos

CONTROL		PREGUNTA	SI	PARCIAL	NO	N/A	CONCLUSIÓN
10.1.1.	Política en el uso de controles de cifrado	¿Se ha desarrollado e implementada una política sobre el uso de controles criptográficos para la protección de la información?	X 75%				Se tiene implementada la encriptación a nivel de equipos de comunicación y algunos sistemas.
10.1.2.	Administración de llaves	¿Se encuentra implantada una gestión de claves para soportar el uso de técnicas criptográficas por parte de la organización?			X 0%		La institución no cuenta con una administración centralizada de claves de encriptación.

Fuente: Adaptación de la NTP ISO/IEC 27001:2014 (INDECOPI, 2014)

11. SEGURIDAD FÍSICA Y AMBIENTAL

11.1. Áreas seguras

Tabla 20

Áreas seguras

CONTROL	PREGUNTA	SI	PARCIAL	NO	N/A	CONCLUSIÓN
11.1.1. Perímetro de seguridad física	¿Se utilizan perímetros de seguridad (barreras como: paredes, puertas de acceso controladas por tarjetas de identidad, puestos de recepción, etc.) para proteger áreas que contengan información e infraestructura para el procesamiento de la información?			X 30%		Se tienen áreas definidas para el Data Center (servidores), Equipos Biomédicos, Almacenes, los cuales deberían estar mejor protegidos.
11.1.2. Controles físicos de entrada	¿Están protegidas las áreas seguras por los controles de entrada apropiados para asegurarse de que solamente permiten el acceso de personal autorizado?			X 30%		El personal encargado maneja las llaves físicas de los ambientes, no existe un control automatizado, se cuentan con algunas cámaras de videovigilancia.
11.1.3. Seguridad en oficinas, cuartos y edificios	¿Se ha diseñado e implantado un sistema de seguridad física para las oficinas, salas y resto de instalaciones?		X 50%			Se cuenta con Videovigilancia para algunas zonas y personal de seguridad en la entrada de todos los locales.
11.1.4. Protección contra amenazas externas y ambientales	¿Se ha sido diseñado y aplicado un sistema de protección física en contra de daños causados por incendios, inundaciones, terremotos, explosiones, ataques provocados por personas y/o			X 30%		Se tiene señalización, áreas seguras, extintores. No se tienen sistemas contra incendios, protección contra inundaciones, las

		otras formas de desastre natural o artificial?				edificaciones son relativamente antiguas.
11.1.5.	Trabajo en áreas seguras	¿Se han diseñado y aplicado las guías y medidas de protección adecuadas para trabajar en las áreas seguras?	x 75%			Existen los procedimientos administrativos y procedimientos asistenciales. Se deben actualizar y mejorar.
11.1.6.	Áreas de acceso pública, carga y entrega	¿Los puntos de acceso, tales como áreas de entrega y/o carga, y otros puntos donde personas no autorizadas puedan tener acceso, son controlados y, si es posible, aislados de las instalaciones para el procesamiento de la información, con el fin de evitar accesos no autorizados?		x 50%		El almacén se encuentra separado del resto de la infraestructura y se lleva un control de acceso a él, sin embargo otras áreas son de acceso público por parte de los usuarios

Nota**.** Adaptación de la NTP ISO/IEC 27001:2014 Fuente: INDECOPI, (2014)

11.2. Equipamiento

Tabla 21

Equipamiento

CONTROL		PREGUNTA	SI	PARCIAL	NO	N/A	CONCLUSIÓN
11.2.1.	Ubicación y protección de equipamiento	¿Los equipos están aislados o protegidos con la finalidad de reducir el riesgo de daños, amenazas y accesos no autorizados?		x 50%			Se ha inventariado y ubicado cada equipo dentro de las instalaciones. Falta protección ambiental sobre todo en los equipos ubicados en los módulos.
11.2.2.	Suministros de soporte	¿Los equipos se encuentran protegidos ante los posibles fallos de electricidad y otras perturbaciones causadas	x 80%				Se cuenta con generador eléctrico para cada Hospital y el área administrativa.

		por los fallos en los sistemas de soporte (UPS, Planta eléctrica)?			Los equipos médicos críticos cuentan con su propio UPS. Se cuenta con pozo a tierra. Faltan generadores para algunos locales.
11.2.3.	Seguridad en el cableado	¿El cableado eléctrico y el de telecomunicaciones, que transmiten datos o soportan servicios de información, están protegidos contra la intercepción o daño?		X 30%	Se cuenta con cableado estructurado categoría 6 (certificado). El cableado se rige a estándares y está aislado del cableado eléctrico. No hay una protección mayor que el de las canaletas por donde pasa.
11.2.4.	Mantenimiento de equipos	¿Se hace un mantenimiento correcto de los equipos para asegurar su continua disponibilidad e integridad?	X 100%		Existen planes de mantenimiento preventivo de equipos informáticos y equipos médicos.
11.2.5.	Retiro de activos	¿Se requiere autorización previa para sacar de la organización equipos, información o software?	X 100%		Cualquier equipo sólo puede ser trasladado por medio de una papeleta de desplazamiento o de mantenimiento con la debida autorización.
11.2.6.	Seguridad de los equipos fuera de las instalaciones	¿Se aplica la seguridad adecuada los equipos que se encuentran fuera de las áreas pertenecientes a la organización, considerando los riesgos que implica trabajar fuera de las instalaciones de la organización?		X 30%	Se asigna el equipo a una persona responsable. En campañas se sacan equipos médicos.
11.2.7.	Desecho y/o “reutilización” seguro de los equipos	¿Se revisan todos los equipos que tengan capacidad de almacenamiento, para asegurarse que ningún tipo de dato sensible y/o software licenciado haya sido eliminado o sobrescrito con seguridad	X 100%		Se formatean los equipos y/o resetea la información. Se sigue un proceso formal

		antes del desecho o reutilización del equipo?				
11.2.8.	Equipos de usuarios desatendidos	¿Se requiere que los usuarios se aseguren que los equipos desatendidos tengan la protección adecuada?		X 50%		Se tiene usuarios de SO estándar que no tienen implementadas políticas de bloqueo de equipos. Se sugiere a los usuarios bloquear sus equipos.
11.2.9.	Política de escritorio y pantalla limpia	¿Se ha adoptado una política de "escritorio despejado" para los papeles, medios de almacenamiento removibles y una política de "pantalla limpia" en la infraestructura para el procesamiento de información?		X 50%		Se cuenta con una política de escritorio limpio pero no se aprecia su aplicación por parte de los usuarios.

Nota**.** Adaptación de la NTP ISO/IEC 27001:2014 Fuente: INDECOPI, (2014)

12. SEGURIDAD DE LAS OPERACIONES

12.1. Responsabilidad y procedimientos operacionales

Tabla 22

Responsabilidad y procedimientos operacionales

CONTROL		PREGUNTA	SI	PARCIAL	NO	N/A	CONCLUSIÓN
12.1.1.	Procedimientos operacionales documentados	¿Los procedimientos operativos están documentados, mantenidos y puestos a disposición de todos los usuarios que los necesitan?	X 80%				Se cuenta con procedimientos asistenciales, administrativos, manuales de usuario, operador. Faltan para algunos procesos nuevos o se deben actualizar.
12.1.2.	Administración de cambios	¿Se controlan los cambios a la infraestructura para el tratamiento de la		X 40%			Se gestiona la actualización de la infraestructura de acuerdo a los avances

		información y los sistemas?				técnológicos y medicos. Se maneja a nivel corporativo y a veces no llega a todas las redes asistenciales.
12.1.3.	Gestión de la Capacidad	¿El uso de recursos es monitoreado, afinado y se realizan proyecciones de futuros requisitos de capacidad para asegurar el rendimiento del sistema?		X 70%		Se hace una proyección al inicio de la adquisición de equipamiento y se debe tener presente una proyección hacia 7 años de uso.
12.1.4.	Separación de ambientes	¿Las instalaciones de desarrollo, producción y pruebas están separadas para reducir los riesgos de accesos o cambios en los sistemas operativos no autorizados?			X	El desarrollo de sistemas se realiza de manera centralizada en Lima.

Nota**.** Adaptación de la NTP ISO/IEC 27001:2014 Fuente: INDECOPI, (2014)

12.2. Protección contra código malicioso

Tabla 23

Protección contra código malicioso

CONTROL		PREGUNTA	SI	PARCIAL	NO	N/A	CONCLUSIÓN
12.2.1.	Controles contra software malicioso	¿Se han implementado controles de detección, prevención y recuperación para protegerse de código malicioso, así como procedimientos	X 80%				Se cuenta con equipamiento activo de seguridad (Firewall, IDS, IPS) Las redes estan conectadas mediante VPN. Los servidores y estaciones de trabajo

	apropiados para la concientización de los usuarios sobre éste?	cuentan con software antivirus. La salida a Internet es mediante proxy.

Nota**.** Adaptación de la NTP ISO/IEC 27001:2014 Fuente: INDECOPI, (2014)

12.3. Copias de respaldo

Tabla 24

Copias de respaldo

CONTROL	PREGUNTA	SI	PARCIAL	NO	N/A	CONCLUSIÓN
12.3.1. Copia de respaldo de información	¿Se realizan las copias de seguridad y se comprueban regularmente conforme a lo establecido en la política acordada?	X 100%				Se realizan Backups de aplicaciones rigiendose a una política.

Nota**.** Adaptación de la NTP ISO/IEC 27001:2014 Fuente: INDECOPI, (2014)

12.4. Registro y monitoreo

Tabla 25

Registro y monitoreo

CONTROL	PREGUNTA	SI	PARCIAL	NO	N/A	CONCLUSIÓN
12.4.1. Registro de eventos	¿Los logs de auditoría registran y mantienen las actividades de los usuarios, las excepciones y los eventos de seguridad de la información, durante un periodo de tiempo acordado, con el		X 60%			Se manejan logs de acceso a las principales aplicaciones. Vigilancia registra el acceso a las instalaciones.

		fin de ser utilizados en investigaciones futuras y monitorear el control de acceso?			Las PC y los equipos médicos no guardan registros de acceso.
12.4.2.	Protección de la información de registros	¿La infraestructura para los registros y la información de estos registros, son protegidos en contra de acceso forzoso o no autorizado?		X 50%	La infraestructura en donde se guardan los registros está protegida, sin embargo se han presentado casos de pérdidas o adulteración en algunas historias clínicas físicas.
12.4.3.	Registros del administrador y operador	¿Las actividades del administrador y del operador del sistema, son registradas?	X 80%		Se registras todas las actividades realizadas en los sistemas de Información. Falta el registro en equipos biomédicos
12.4.4.	Sincronización de relojes	¿Se encuentran sincronizados todos los relojes de todos los sistemas relevantes de procesamiento de información en la organización o contenidos en el dominio de seguridad, conforme a una fuente de tiempo de confianza?	X 80%		Se tiene implementado a nivel de la sede central y la mayoría de sedes pero a veces puede fallar con regiones aisladas

Nota**.** Adaptación de la NTP ISO/IEC 27001:2014 Fuente: INDECOPI, (2014)

12.5. Control de software operacional

Tabla 26

Control de software operacional

CONTROL	PREGUNTA	SI	PARCIAL	NO	N/A	CONCLUSIÓN
12.5.1. Instalación de software sobre el sistema operativo	¿Existen procedimientos para el control de la instalación de software sobre sistemas operacionales?	X 100%				Se cuenta con manual de usuario y operador de los Sistemas Operativos y se restringe la instalación de software

Nota**.** Adaptación de la NTP ISO/IEC 27001:2014 Fuente: INDECOPI, (2014)

12.6. Gestión de vulnerabilidades técnicas

Tabla 27

Gestión de vulnerabilidades técnicas

CONTROL	PREGUNTA	SI	PARCIAL	NO	N/A	CONCLUSIÓN
12.6.1. Gestión de vulnerabilidades técnicas	¿Se obtiene oportunamente información sobre las vulnerabilidades técnicas de los sistemas de información que están en uso, la exposición a dichas vulnerabilidades es evaluada y se toman las medidas oportunas para tratar el riesgo asociado?			X 10%		No se lleva un control de las vulnerabilidades.

12.6.2.	Restricciones en la instalación de software	¿Se establecieron e implementaron reglas para la instalación de software por parte de los usuarios?			X 100%		Los usuarios no tienen opción para instalar software

Nota**.** Adaptación de la NTP ISO/IEC 27001:2014 Fuente: INDECOPI, (2014)

12.7. Consideraciones de auditoria de sistemas de información

Tabla 28

Consideraciones de auditoria de sistemas de información

	CONTROL	PREGUNTA	SI	PARCIAL	NO	N/A	CONCLUSIÓN
12.7.1.	Controles de auditoría de los sistemas de información	¿Los requerimientos y las actividades de auditoría sobre los sistemas operativos, que involucran revisiones, son cuidadosamente planeados y acordados para minimizar el riesgo de perturbar los procesos del negocio?			X 0%		No se realiza en la sede de Cajamarca.

Nota**.** Adaptación de la NTP ISO/IEC 27001:2014 Fuente: INDECOPI, (2014)

13. SEGURIDAD DE LAS COMUNICACIONES

13.1. Controles en la red

Tabla 29

Controles en la red

CONTROL	PREGUNTA	SI	PARCIAL	NO	N/A	CONCLUSIÓN
13.1.1. Controles en la red	¿La red está adecuadamente administrada y controlada, con el fin de protegerla de las amenazas y mantener la seguridad de los sistemas y aplicaciones que usa la red, incluida la información en tránsito?	X 100%				El personal de sistemas administra y monitorea la red. Los equipos de comunicación son administrables y configurados con políticas de seguridad de acceso. Se tiene enlaces punto a punto protegidos con claves seguras.
13.1.2. Seguridad de servicios de red	¿Las características de seguridad, los niveles de servicio, y los requerimientos de administración de todos los servicios de red, están identificados e incluidos en los acuerdos con los diferentes proveedores de servicios de red, bien sean internos o externos?	X 100%				Se cuenta con acuerdos de nivel de servicio con el proveedor de servicio de Internet. Se cuenta con equipos de red de respaldo en caso falle algún equipo. Se revisan periódicamente las instalaciones de equipos de red.
13.1.3. Segregación en redes	¿Los controles para segregar grupos de dispositivos de información, usuarios y sistemas de información son adecuados?	X 80%				Se tienen segmentos de red asignados por áreas. No se cuenta con aislamiento del

							segmento en donde están los servidores.

Nota**.** Adaptación de la NTP ISO/IEC 27001:2014 Fuente: INDECOPI, (2014)

13.2. Transferencia de información

Tabla 30

Transferencia de información

	CONTROL	PREGUNTA	SI	PARCIAL	NO	N/A	CONCLUSIÓN
13.2.1.	Políticas y procedimientos de transferencia de información	¿Hay establecida una política formal de intercambio, procedimientos y controles para proteger el intercambio de información a través de los servicios de comunicación?	X 100%				Existen políticas establecidas para la transferencia de información. La intercomunicación se da punto a punto.
13.2.2.	Acuerdos de transferencia	¿Se han establecido acuerdos para el intercambio de información y software dentro de la organización y con organizaciones externas?				X	
13.2.3.	Mensajería electrónica	¿Está adecuadamente protegida la información involucrada en la mensajería electrónica?	X 100%				Se cuenta con un servidor propio de correo electrónico. Se filtran mensajes SPAM.
13.2.4.	Acuerdos de confidencialidad y no revelación.	¿Los acuerdos de confidencialidad y no revelación reflejan las necesidades de la organización, se documentan y revisan?		X 50%			Se encuentran establecidos los acuerdos de confidencialidad en los contratos, más no se encuentran

							revisados ni documentados.

Nota**.** Adaptación de la NTP ISO/IEC 27001:2014 Fuente: INDECOPI, (2014)

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

14.1. Requerimientos de seguridad de los sistemas de información

Tabla 31

Requerimientos de seguridad de los sistemas de información

	CONTROL	PREGUNTA	SI	PARCIAL	NO	N/A	CONCLUSIÓN
14.1.1.	Análisis y especificaciones de los requerimientos de seguridad	¿Las declaraciones de los requerimientos del negocio para nuevos sistemas de información o para la mejora de los ya existentes, especifican los requerimientos de los controles de seguridad?		X 40%		X	Lo realiza la sede central
14.1.2.	Seguridad de servicios aplicativos sobre redes públicas	¿La información disponible a través de un sistema público, se encuentra protegida para asegurar su integridad y prevenir modificaciones no autorizadas?		X 40%			Sede central y Soporte informático.
14.1.3.	Protección de transacciones aplicativas	¿La información involucrada en transacciones on-line, está protegida para prevenir transmisiones incompletas, desvío, modificación no autorizada del mensaje, divulgación no autorizada y para	X 100%				Las comunicaciones están protegidas y encriptadas.

		evitar la duplicación o reproducción?				

Nota**.** Adaptación de la NTP ISO/IEC 27001:2014 Fuente: INDECOPI, (2014)

14.2. Seguridad en el desarrollo y soporte de procesos

Tabla 32

Seguridad en el desarrollo y soporte de procesos

CONTROL		PREGUNTA	SI	PARCIAL	NO	N/A	CONCLUSIÓN
14.2.1.	Política de desarrollo seguro	¿Existen reglas de seguridad para el desarrollo de software?		X 40%			No se tiene una política de desarrollo de software implementada a nivel nacional.
14.2.2.	Procedimientos de control de cambios	¿Se utilizan procedimientos de control de cambios formales para controlar la implementación de cambios?		X 40%			No se tiene política y se realiza a demanda en todas las redes.
14.2.3.	Revisión técnica de aplicaciones después de cambios al sistema operativo	¿Cuándo los sistemas operativos son cambiados, todas las aplicaciones críticas del negocio son revisadas y comprobadas para asegurar que no haya un impacto adverso en las operaciones y/o la seguridad de la organización?	X 80%				Cuenta con políticas de software legal
14.2.4.	Restricciones en los cambios a los paquetes de software	¿Las modificaciones de los paquetes de software, son desalentadas, limitadas a los cambios necesarios y todos los cambios son estrictamente controlados?	X 80%				Cuenta con políticas de software legal
14.2.5.	Principios de ingeniería de sistemas segura	¿Se han establecido, documentados, mantenidos y aplicados principios de		X 40%			No se retroalimenta ni verifica lo requerido.

		ingeniería de sistemas segura?				
14.2.6.	Ambiente de desarrollo seguro	¿El ambiente de desarrollo está adecuadamente protegido durante el ciclo completo de codificación?		X 40%		No se tiene políticas de desarrollo
14.2.7.	Desarrollo de software en outsourcing	¿El desarrollo de software realizado en outsourcing, está siendo supervisado y monitoreado por la organización?			X	Lo realiza la sede central
14.2.8.	Prueba de seguridad del sistema	¿Se prueban las funcionalidades de seguridad durante el desarrollo?		X 50%	X	Se verifica funcionalidades básicas
14.2.9.	Prueba de aceptación del sistema	¿Se programan pruebas de aceptación para sistemas nuevos o actualizados?	X 80%			Lo realiza la sede central

Nota**.** Adaptación de la NTP ISO/IEC 27001:2014 Fuente: INDECOPI, (2014)

14.3. Datos de prueba

Tabla 33

Datos de prueba

CONTROL		PREGUNTA	SI	PARCIAL	NO	N/A	CONCLUSIÓN
14.3.1.	Protección de los datos de prueba del sistema	¿Los datos de prueba del sistema están seleccionados cuidadosamente, protegidos y controlados?		X 60%		X	No siempre se realizan los test de prueba de datos.

Nota**.** Adaptación de la NTP ISO/IEC 27001:2014 Fuente: INDECOPI, (2014)

15. RELACIONES CON PROVEEDORES

15.1. Seguridad de información en relaciones con el proveedor

Tabla 34

Seguridad de información en relaciones con el proveedor

	CONTROL	PREGUNTA	SI	PARCIAL	NO	N/A	CONCLUSIÓN
15.1.1.	Políticas de seguridad de información en las relaciones con el proveedor	¿Los requerimientos de seguridad de información para mitigar los accesos de proveedores a recursos de la organización están acordados y documentados?	X 100%				Se tienen acuerdos de seguridad establecidos en los contratos con los proveedores.
15.1.2.	Gestión de la seguridad en los acuerdos con el proveedor	¿Todos los requerimientos relevantes de seguridad de información están establecidos y acordados con cada proveedor que usa componentes de la infraestructura de TI?	X 100%				Se tienen acuerdos de seguridad establecidos en los contratos con los proveedores.
15.1.3.	Cadena de suministro de tecnología de información y comunicaciones	¿Los acuerdos con proveedores incluyen requerimientos para gestionar los riesgos de seguridad en la cadena del suministro del servicio o producto?	X 100%				El proveedor debe asegurar el aprovisionamiento de suministros siguiendo los acuerdos del servicio.

Fuente: Adaptación de la NTP ISO/IEC 27001:2014 (INDECOPI, 2014)

15.2. Gestión de servicios por terceras partes

Tabla 35

Gestión de servicios por terceras partes

	CONTROL	PREGUNTA	SI	PARCIAL	NO	N/A	CONCLUSIÓN
15.2.1.	Monitoreo y revisión de los servicios de terceros	¿Los servicios, informes y registros proporcionados por terceras partes, se monitorizan y revisan de forma regular, y se llevan a cabo auditorias de forma regular?	X 100%				Cualquier producto o servicio debe ser verificado y tener el visto bueno del área usuaria
15.2.2.	Administración de cambios en los servicios de terceros	¿Se gestionan los cambios de provisión de los servicios (incluyendo el mantenimiento y mejora de las políticas existentes, procedimientos y controles de seguridad de la información) tomando en cuenta la criticidad de los sistemas y procesos del negocio implicados y la reevaluación del riesgo?	X 100%				Los proveedores se deben seguir a lo establecido en los contratos o especificaciones técnicas de los productos.

Nota**.** Adaptación de la NTP ISO/IEC 27001:2014 Fuente: INDECOPI, (2014)

16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

16.1. Informes de los eventos de seguridad de la información y vulnerabilidades

Implementar los aspectos definidos en la Política de Seguridad de la Información sobre las responsabilidades y procedimientos de gestión a los incidentes de seguridad de la información.

Implementar un sistema de seguimiento de incidencias de seguridad de la información, que clasifique la criticidad de dichas incidencias.

Capacitar a todos los involucrados sobre el procedimiento a seguir en el caso de reporte de incidencias de seguridad de la información.

Definir un proceso para reporte de vulnerabilidades detectadas en temas de seguridad.

Capacitar al personal interno y externo sobre temas relacionados a las vulnerabilidades de seguridad.

Definir un proceso de respuesta y escalamiento para la atención de incidentes de acuerdo con el nivel de complejidad.

Verificar el cumplimiento del procedimiento de respuesta ante indigentes

Realizar informes mensuales de atención de incidentes.

Establecer periodos de verificación de incidentes detectados y determinar acciones necesarias para evitar su ocurrencia futura (proceso de mejora continua)

Normar que se documente toda la evidencia de los incidentes de seguridad (fotos, capturas de pantallas, mensajes, los, etc), definiendo un lugar seguro para su almacenamiento

Tabla 36

Informes de los eventos de seguridad de la información y vulnerabilidades

CONTROL	PREGUNTA	SI	PARCIAL	NO	N/A	CONCLUSIÓN
16.1.1. Responsabilidades y procedimientos	¿Se encuentran establecidos las responsabilidades y los procedimientos necesarios para establecer una respuesta rápida, efectiva y ordenada cuando se presentan			X 30%		No se cuenta con planes de acción en temas de incidencias relacionadas a la seguridad de la Información. Se tienen funciones del

		incidentes de seguridad de la información?			área de sistemas definidas.
16.1.2.	Reporte de eventos de seguridad de la información	¿Los eventos de seguridad de la información están siendo reportados a los canales de gestión adecuados tan pronto como sea posible?	X 40%		Surgen eventos que son reportados de manera verbal, pero no son almacenados en algún tipo de repositorio.
16.1.3.	Reporte de debilidades de seguridad	¿Se requiere que los empleados contratistas y terceras partes, usuarios de sistemas de información, tomen nota y denuncien cualquier vulnerabilidad de seguridad en los sistemas o en los servicios, que observen o sospechen?		X 0%	No se han realizado hasta la fecha.
16.1.4.	Evaluación y decisión sobre los incidentes de seguridad de información	¿Los eventos de seguridad de información son evaluados para ver si son clasificados como incidentes?		X 30%	En los eventos reportados se procura realizar una evaluación para su tratamiento mas no son registrados para luego clasificarlos.
16.1.5.	Respuesta a incidentes de seguridad de información	¿La respuesta a los incidentes de seguridad está de acuerdo a los procedimientos documentados?		X 0%	No existen procedimientos documentados
16.1.6.	Aprender de los incidentes de seguridad de la información	¿Existen mecanismos para establecer los tipos, volúmenes y costos		X 0%	No se lleva un control documentado de los incidentes de

		referidos a incidentes de seguridad de la información, que deban ser cuantificados y monitorizados?		seguridad de la información
16.1.7.	Recolección de evidencia	Cuando se presenta una acción de seguimiento en contra de una persona u organización después que un incidente de seguridad de la información implica una acción legal (ya sea criminal o civil): ¿La evidencia, es recogida, retenida y presentada conforme a las reglas para la evidencia colocada en la jurisdicción relevante?	X 0%	No se realiza, debido a que no hay registros.

Nota**.** Adaptación de la NTP ISO/IEC 27001:2014 Fuente: INDECOPI, (2014)

17. ASPECTOS DE SEGURIDAD DE INFORMACIÓN EN LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO

17.1. Gestión de los aspectos de seguridad de la continuidad del negocio

Ejecutar un análisis de riesgos que contemple el impacto sobre la continuidad del negocio.

La organización debe incluir dentro de la Política de Continuidad del Negocio los lineamientos sobre la continuidad de la seguridad de la información, detallando pasos y recomendaciones necesarias.

Se debe actualizar e implementar el Plan de Recuperación ante Desastres.

El área de TI debe documentar un manual de continuidad de TI.

Establecer un cronograma de capacitación a todas las unidades sobre Continuidad de Negocio.

Establecer un cronograma de pruebas de continuidad del negocio con la emisión de un informe.

Establecer un proceso de verificación, revisión y evaluación en la continuidad de la seguridad de la Información.

Tabla 37

Gestión de los aspectos de seguridad de la continuidad del negocio

CONTROL		PREGUNTA	SI	PARCIAL	NO	N/A	CONCLUSIÓN
17.1.1.	Planeamiento de la continuidad de la seguridad de información	¿Se ha desarrollado y mantenido un proceso de gestión para la continuidad del negocio de toda la organización que trate los requerimientos de seguridad de la información que se necesitan para la continuidad del negocio de la organización?			X 30%		Se han tomado medidas para mitigar algunos incidentes que se han presentado buscando mantener la continuidad del negocio sin embargo no se ha contemplado temas relacionados a la continuidad del negocio.
17.1.2.	Implementación de la continuidad de la seguridad de información	¿Se han identificados todos los eventos que pueden causar interrupciones a los procesos de negocio, junto con la probabilidad y el impacto de dichas interrupciones, y sus consecuencias para la seguridad de la información?			X 20%		Se han identificado algunos eventos que podrían causar interrupciones a los procesos de negocio, sin embargo no se ha definido su probabilidad de ocurrencia ni el impacto sobre la seguridad de la información
17.1.3.	Verificación, revisión y evaluación de la continuidad de la seguridad de información	¿Los planes de continuidad de negocio son probados y modificados para asegurar que son efectivos y se encuentran al día?			X 0%		No hay planes formales de contingencia

Nota**.** Adaptación de la NTP ISO/IEC 27001:2014 Fuente: INDECOPI, (2014)

17.2. Redundancias

Realizar un análisis a la infraestructura actual para definir las necesidades de respaldo de información.

Definir el lugar más adecuado para implementar la redundancia de la información

Implementar la infraestructura necesaria para la replicación de la información

Realizar pruebas de funcionamiento

Tabla 38

Redundancias

CONTROL	PREGUNTA	SI	PARCIAL	NO	N/A	CONCLUSIÓN
17.2.1. Disponibilidad de centro de procesamiento de datos	¿Las instalaciones para el procesamiento de datos cuentan con la suficiente redundancia para cumplir con los requerimientos de disponibilidad?			X 30%		Se cuentan con equipos de respaldo pero no hay una replicación, en caso de tener que reemplazar un equipo por otro primero se tendría que preparar y pasar la información.

Nota. Adaptación de la NTP ISO/IEC 27001:2014 Fuente: INDECOPI, (2014)

18. CUMPLIMIENTO

18.1. Cumplimiento de los requerimientos legales

Tabla 39

Cumplimiento de los requerimientos legales

CONTROL	PREGUNTA	SI	PARCIAL	NO	N/A	CONCLUSIÓN
18.1.1. Identificación de la legislación aplicable	¿Todos los requerimientos estatutarios,	X 100%				La organización se rige a las normas que establecen para

		regulatorios y contractuales, y el enfoque de la organización para cumplir con estos requerimientos, se encuentran explícitamente definidos, documentados y mantenidos al día para cada uno de los sistemas de información y para la organización?			las entidades del estado. La misma entidad también establece normas para el trabajo interno de todos sus trabajadores.
18.1.2.	Derechos de propiedad intelectual (IPR)	¿Se han implementado los procedimientos apropiados para asegurar el cumplimiento de los requerimientos legales, regulatorios y contractuales respecto al uso de materiales que pudieran estar protegidos por los derechos de propiedad intelectual, e igualmente respecto al uso de productos software propietario?	X 100%		La entidad se rige a las normas de propiedad intelectual y prohíbe a sus usuarios la instalación de cualquier software no licenciado.
18.1.3.	Protección de los registros	¿Los registros importantes están protegidos de pérdida, destrucción y falsificación, de acuerdo con los requerimientos estatutarios, regulatorios, contractuales y del negocio?		X 70%	La protección de los registros del sistema está asegurada sin embargo algunos datos como las historias clínicas físicas todavía se encuentran expuestas a sufrir cambios no registrados en los sistemas.

18.1.4.	Protección y privacidad de la información personal	¿Se están aplicando controles para asegurar la protección y la privacidad de los datos, tal y como se requiere por la legislación, regulaciones aplicables y, si fuera el caso, cláusulas contractuales?	X 100%			Se aplica una normativa para llevar un control de la información almacenada en los sistemas de información.
18.1.5.	Regulación de controles de cifrado	¿Se están utilizando controles criptográficos de acuerdo con las leyes, regulaciones y acuerdos relevantes?			X 0%	No se tiene implementado controles criptográficos

Nota. Adaptación de la NTP ISO/IEC 27001:2014 Fuente: INDECOPI, (2014)

18.2. Revisiones a la seguridad de información

Tabla 40

Revisiones a la seguridad de información

CONTROL		PREGUNTA	SI	PARCIAL	NO	N/A	CONCLUSIÓN
18.2.1.	Revisión independiente de la seguridad de información	¿Los requerimientos y las actividades de auditoría sobre los sistemas operativos, que involucran revisiones, son cuidadosamente planeados y acordados para minimizar el riesgo de perturbar los procesos del negocio?		X 70%			Se cuenta con políticas referidas a la seguridad de la información pero falta mejorar su implementación.
18.2.2.	Cumplimiento de políticas y estándares de seguridad	¿Los directivos se aseguran que todos los procedimientos de seguridad dentro de su área de responsabilidad, se realizan correctamente		X 50%			Se realiza la revisión de manera parcial por parte de los directivos, no se tienen procedimientos

		para asegurar el cumplimiento con los estándares y políticas de seguridad de la organización?		definidos de revisión.
18.2.3.	Verificación del cumplimiento técnico	¿Los sistemas de información son revisados regularmente en cumplimiento de los estándares de implementación de la seguridad?	X 20%	Se realizan revisiones de los sistemas pero no basados en cumplimiento de estandares de seguridad

Nota**.** Adaptación de la NTP ISO/IEC 27001:2014 Fuente: INDECOPI, (2014)

III.3.1 Análisis de cumplimiento

Luego de realizado el análisis de brechas entre lo que la institución tiene implementado y los controles que establece la Norma Técnica Peruana se ha resumido en el siguiente cuadro los resultados, para temas de interpretación se ha considerado la cantidad de puntos que se cumplen de manera positiva es decir Si son aplicados, la cantidad de los que se cumplen parcialmente o están en desarrollo, los que no se cumplen o su porcentaje de avance es aún insuficiente y los controles que no serían aplicables a la institución, la suma total por cada control es la que vendría a significar el 100% de cumplimiento.

Tabla 41

Resumen de cumplimiento de Controles de la NTP

Clausula	Controles de Referencia	SI	Parcial	No	No Aplica
A.5	Políticas de seguridad de la información	50%	0%	50%	0%
A.6	Organización de la seguridad de la información	43%	0%	57%	0%
A.7	Seguridad de los recursos humanos	0%	50%	50%	0%
A.8	Gestión de activos	50%	10%	40%	0%
A.9	Control de acceso	79%	7%	14%	0%
A.10	Criptografía	50%	0%	50%	0%
A.11	Seguridad física y ambiental	33%	33%	33%	0%
A.12	Seguridad de las operaciones	50%	29%	14%	7%
A.13	Seguridad de las comunicaciones	71%	14%	0%	14%

A.14	Adquisición, desarrollo y mantenimiento de sistema	54%	0%	38%	8%
A.15	Relaciones con los proveedores	40%	0%	60%	0%
A.16	Gestión de incidentes de seguridad de la información	57%	0%	43%	0%
A.17	Aspectos de seguridad de la información en la gestión de continuidad del negocio	50%	0%	50%	0%
A.18	Cumplimiento	88%	0%	13%	0%
	Promedio	51%	10%	33%	2%

Nota. Cumplimiento de controles en EsSalud Cajamarca

En base al desarrollo de este análisis, tenemos una mayor cantidad de cumplimientos positivos que en promedio representan el 51% estos cumplimientos se aplican de manera completa o están en una etapa de maduración adecuada, el 10% se encuentran en una etapa de maduración y por el momento se cumple de manera parcial, el 33% no se está cumpliendo o su implementación es aún insuficiente y sólo el 2% no es aplicable a la institución para lo que corresponde a la red asistencial de Cajamarca.

Se cuenta con políticas de seguridad, pero se deben de revisar de manera continua por eso se cumple el 50%, la organización de la seguridad es uno de los puntos a mejorar ya que sólo se llega a cumplir el 43%, en cuanto a los recursos humanos se debe de mejorar la seguridad ya que no se cumple el 50% y además el resto se encuentra en una etapa de cumplimiento parcial, la gestión de activos que es un aspecto importante todavía está en un cumplimiento del 50%, en cuanto al control de acceso se puede apreciar un mayor cuidado debido al servicio del personal de seguridad y videocámaras, la criptografía es un tema que se está empezando a ser tomado en cuenta en la institución, la seguridad física y ambiental tiene problemas debido a la antigüedad del Hospital II Cajamarca y se espera sea notablemente mejorada con la construcción del nuevo hospital, la seguridad de las operaciones también es un aspecto clave que tiene que mejorarse debido a que por ahora se cumple el 50% de controles, las comunicaciones se encuentran adecuadamente resguardadas y cumplen e 71%, en cuanto a las mejoras de los sistemas, adquisiciones y nuevos desarrollos mayormente recae la tarea en la sede central pero aun así se desarrollan algunas actividades para resguardar la información, la seguridad con los proveedores también enfrenta algunas dificultades a veces ligadas a la informalidad y en otros casos ligadas al tema de que se trata de una institución de atención pública lo que la hace más expuesta al riesgo, se lleva un

registro de los incidentes de seguridad pero se tiene deficiencias en este punto debido a que no se ha establecido con claridad algunas responsabilidades y a la falta de personal para dar seguimiento a estos eventos, los aspectos de la seguridad de la información deben desarrollar un plan de continuidad de negocio para poder estar en una condición adecuada, en cuanto al cumplimiento se tiene un 80% debido a que se trata de una institución que debe contemplar muchas normas de seguridad.

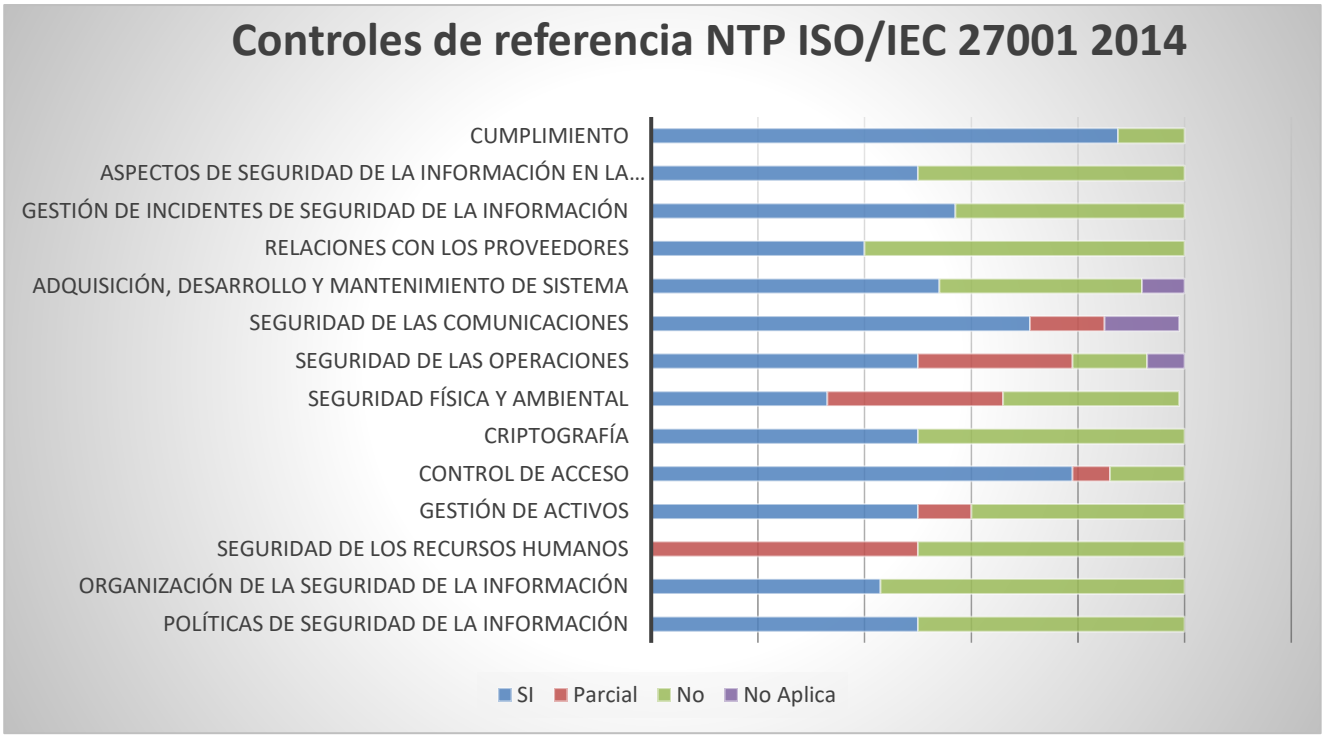


Figura 10. Análisis de cumplimiento de controles de referencia

III.3.2 Plan de acción

Tabla 42

Plan de Acciones a Ejecutar por ESSALUD

Dominio	Código	Acción	Mes 1	Mes 2	Mes 3	Mes 4	Mes 5	Mes 6	Mes 7	Mes 8	Mes 9	Mes 10	Mes 11	Mes 12	Responsable
17. Aspectos de seguridad de información en la gestión de continuidad del negocio	17.1.1	Ejecutar un análisis de riesgos que contemple el impacto sobre la continuidad del negocio.	X												DIRECCIÓN MÉDICA
		Incluir dentro de la Política de Continuidad del Negocio los lineamientos sobre la continuidad de la seguridad de la información, detallando pasos y recomendaciones necesarias	X	X	X	X									GERENCIA DE PLANEAMIENTO Y DESARROLLO
		Actualizar e implementar el Plan de Recuperación ante Desastres.	X	X											JEFE DE ADMINISTRACION
		TI debe documentar un manual de continuidad de negocio en temas de TI.				X	X	X							JEFE DE UNIDAD DE SOPORTE INFORMÁTICO
	17.1.2	Establecer un cronograma de capacitación a todas las unidades sobre Continuidad de Negocio.	X												JEFE DE OF. ADMINISTRACIÓN
		Establecer un cronograma de pruebas de continuidad del negocio con la emisión de un informe.		X											JEFE DE OFICINA ADMINISTRACION
	17.1.3	Establecer un proceso de verificación, revisión y evaluación en la continuidad de la seguridad de la Información.	X												DIRECCIÓN MÉDICA

	17.2.1	Realizar un análisis a la infraestructura actual para definir las necesidades de respaldo de información.	X	X					JEFE DE UN. DE INGENIERIA HOSPITALARIA
		Definir el lugar más adecuado para implementar la redundancia de la información		X					JEFE DE UNIDAD DE INGENIERIA HOSPITALARIA
		Implementar la infraestructura necesaria para la replicación de la información			X	X	X		JEFE DE UNIDAD DE INGENIERIA HOSPITALARIA
		Realizar pruebas de funcionamiento a la infraestructura de replicación.						X	JEFE DE UNIDAD DE SOPORTE INFORMÁTICO
10. Criptografía	10.1.1	Incluir dentro de la Política de Seguridad Informática los aspectos sobre el uso de controles criptográficos para toda la organización						X	GERENCIA CENTRAL DE TECNOLOGIAS DE INFORMACIÓN
	10.1.2	Incluir dentro de la Política de Seguridad Informática los procedimientos y normas para la gestión de claves.						X	GERENCIA CENTRAL DE TECNOLOGÍAS DE INFORMACIÓN
8. Gestión de activos	8.1.1	Identificar los activos de Información	X	X					DIRECCIÓN MÉDICA
	8.1.2	Implementar el inventario de activos de información.			X				
	8.1.4	Definir a los responsables para cada activo			X				
	8.1.3	Asociar a cada activo los procedimientos, manuales de uso u otra documentación necesaria				X			
	8.1.4	Desarrollar y establecer una política de devolución de activos de información.				X			

16. Gestión de incidentes de seguridad de la información	8.2.1 8.2.2	Inventario, clasificación y priorización de la información	X							JEFE DE OFICINA DE ADMINISTRACIÓN
	8.2.3	Implementar procedimientos y gestión de la información de acuerdo a la clasificación		X						DIRECCIÓN MÉDICA
	8.3.1 8.3.2	Normar el proceso de gestión y eliminación de medios removibles de acuerdo a las incidencias y políticas de seguridad de la información	X							DIRECCIÓN MÉDICA
	16.1.1	Implementar las aspectos definidos en la Política de Seguridad de la Información sobre las responsabilidades y procedimientos de gestión a los incidentes de seguridad de la información.			X					JEFE DE OFICINA DE ADMINISTRACIÓN
	16.1.2	Implementar un sistema de seguimiento de incidencias de seguridad de la información, que clasifique la criticidad de dichas incidencias.			X	X	X			JEFE DE UNIDAD DE SOPORTE INFORMÁTICO
		Capacitar a todos los involucrados sobre el procedimiento a seguir en el caso de reporte de incidencias de seguridad de la información.				X		X		JEFE DE UNIDAD DE SOPORTE INFORMÁTICO
	16.1.3	Definir un proceso para reporte de vulnerabilidades detectadas en temas de seguridad.					X			JEFE DE UNIDAD DE SOPORTE INFORMÁTICO
		Capacitar al personal interno y externo sobre temas relacionados a las vulnerabilidades de seguridad.						X	X	JEFE DE UNIDAD DE SOPORTE INFORMÁTICO
	16.1.4	Definir un proceso de respuesta y escalamiento para la atención de incidentes de acuerdo con el nivel de complejidad.					X			JEFE DE UNIDAD DE SOPORTE INFORMÁTICO

16.1.5	Verificar el cumplimiento del procedimiento de respuesta ante incidentes			X		JEFE DE UNIDAD DE SOPORTE INFORMÁTICO
	Realizar informes mensuales de atención de incidentes.	X	X	X	X	JEFE DE UNIDAD DE SOPORTE INFORMÁTICO
16.1.6	Establecer periodos de verificación de incidentes detectados y determinar acciones necesarias para evitar su ocurrencia futura (proceso de mejora continua)	X				JEFE DE UNIDAD DE SOPORTE INFORMÁTICO
16.1.7	Normar que se documente toda la evidencia de los incidentes de seguridad (fotos, capturas de pantallas, mensajes, los, etc.), definiendo un lugar seguro para su almacenamiento		X			DIRECCIÓN MÉDICA

Nota. Las acciones deberán ser programadas para el siguiente año teniendo en cuenta el tema del presupuesto institucional.

IV. DESCRIPCIÓN DE MÉTODOS Y ANÁLISIS

IV.1 Tipo de Investigación

A. Según su fin

Aplicada

B. Según su alcance o nivel de profundidad del conocimiento

Descriptiva

IV.2 Diseño de la Investigación:

No experimental

IV.3 Unidad de Análisis:

Gestión de la Historia Clínica

IV.4 Población:

Archivo de Historias Clínicas y Base de Datos de Historias Clínicas Electrónicas.

IV.5 Muestra:

Archivo de Historias Clínicas y Base de Datos de Historias Clínicas Electrónicas.

IV.6 Técnicas:

- Análisis Documental
- Entrevista.

IV.7 Instrumentos:

- Ficha de entrevista/cuestionario.

IV.8 Método:

Inductivo – Deductivo.

IV.9 Procedimiento:

El procedimiento que se seguirá para el análisis de la Gestión de las Historias Clínicas en el Hospital II de ESSALUD en Cajamarca será primero el de observar la manipulación y desplazamiento de las Historias Clínicas de los pacientes, así como el resguardo de las mismas en el archivo de historias clínicas y también se aplicará una entrevista al personal que tiene injerencia o responsabilidad sobre las Historias Clínicas (muestra), esta información servirá para realizar la evaluación del grado de cumplimiento de la directiva de manejo de Historias Clínicas.

V. RESULTADOS

Presentamos en este apartado los resultados esperados en concordancia a cada objetivo planteado y las actividades realizadas.

- La Gestión de la Historia Clínica está compuesta de mayores actividades del tipo Administrativas en comparación con las Asistenciales y llega a estar relacionada con los controles definidos en la NTP-ISO/IEC 27001:2014 en aproximadamente una tercera parte del total de controles que la componen, siendo la continuidad del negocio la categoría con mayor relación.
- Se ha encontrado que la norma de EsSalud sobre Gestión de la Historias Clínicas del Hospital II Cajamarca se ha implementado de manera general en un 60%, en cuanto los Procedimientos Asistenciales referente a la historia clínica se observa que se tiene implementado al 100%, en cuanto a la Continuidad del Negocio no se encuentran evidencias de implementación, siendo este un aspecto a mejorar en la institución.
- Del análisis de los controles realizados para la Seguridad de la Información usando la NTP ISO/IEC 27001:2014, se ha encontrado un cumplimiento de 51% del total de controles, un 10% se encontraría en una etapa de cumplimiento parcial y 33% no se está cumpliendo aún. El aspecto con menor grado de desarrollo es el de la Seguridad de los Recursos Humanos y el mejor valorado es el de Cumplimiento debido a todas las normas y regulaciones con las que cuenta ESSALUD, dentro de los aspectos que se deben mejorar tenemos a la Gestión de Activos 50%, la Seguridad Física y Ambiental que sólo cumple el 33% y la Relación con los Proveedores con un 40% de cumplimiento.

Las actividades realizadas para encontrar los resultados fueron:

- Se realizó una evaluación de la aplicación de la norma Resolución de Gerencia General Nº 107-GG-ESSALUD-2014 que aprueba la Directiva Nº 001-GG-ESSALUD-2014 “Gestión de la Historia Clínica en los Centros Asistenciales del Seguro Social de Salud - ESSALUD” en el Hospital II Cajamarca de la Red Asistencial Cajamarca.
- Utilizando la metodología Magerit versión 3, se realizó el Análisis de Riesgos de las TIC para la identificación y priorización de riesgos asociados al proceso de la Gestión de las Historias Clínicas, con la finalidad de evaluar la Seguridad de la Información del Hospital II Cajamarca de la Red

Asistencial Cajamarca de EsSalud mediante al análisis del nivel de cumplimiento de la NTP-ISO/IEC 27001:2014 – "Norma Técnica Peruana Tecnología de la Información. Técnicas de seguridad. Sistemas de Gestión de Seguridad de la información. Requisitos".

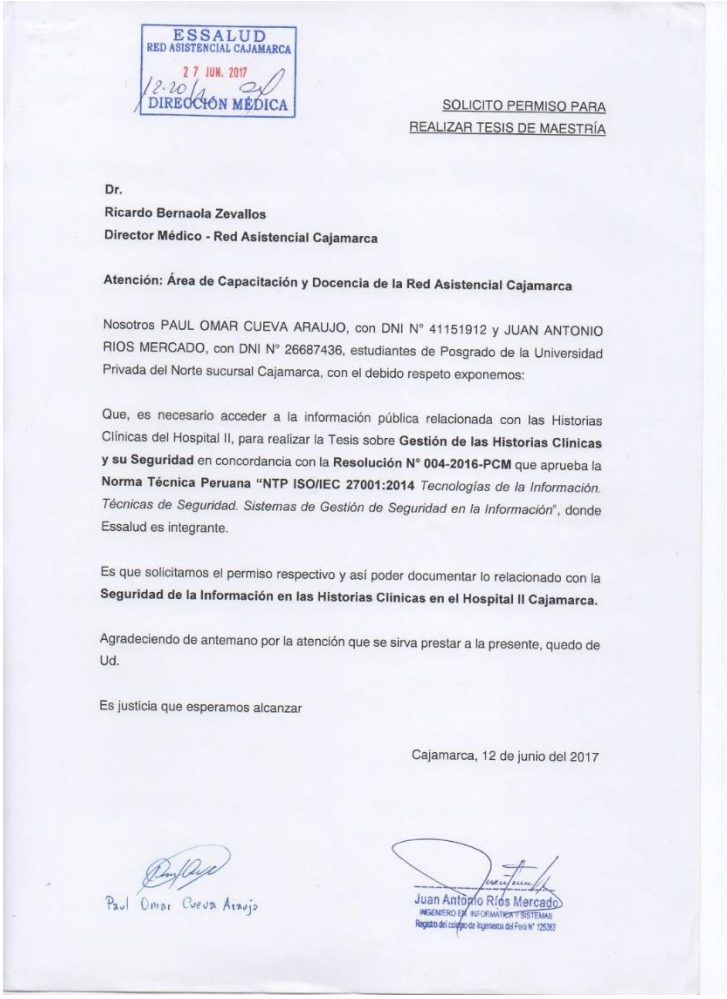
- Los Resultados de ambas evaluaciones fueron:
  a. La identificación de las disposiciones en las que se posee deficiencias para la Gestión de las Historias Clínicas
  b. La priorización de riesgos de las TIC asociados al proceso de la gestión de historias clínicas e identificación de controles aplicables de la NTP-ISO/IEC 27001:2014

  Los resultados obtenidos fueron los insumos indispensables para la elaboración de la propuesta, la cual se detalla en el punto III de la presente investigación.

V.1 Diagnóstico de la Gestión de la Historia Clínica

Uso de la información institucional

- Para poder realizar la investigación en el Hospital II Cajamarca de la Red Asistencial Cajamarca de EsSalud se presentó una solicitud al Director de la Red, el Dr. Ricardo Bernaola Zevallos con Número de Identificación de Trámite NIT 1607-2017-1366 con atención al Área de Capacitación y Docencia solicitando la autorización para uso de la información pública de las Historias Clínicas del Hospital II Cajamarca - EsSalud.



ESSALUD
RED ASISTENCIAL CAJAMARCA
27 JUN. 2017
12:20
DIRECCIÓN MÉDICA

SOLICITO PERMISO PARA
REALIZAR TESIS DE MAESTRÍA

Dr.
Ricardo Bernaola Zevallos
Director Médico - Red Asistencial Cajamarca

Atención: Área de Capacitación y Docencia de la Red Asistencial Cajamarca

Nosotros PAUL OMAR CUEVA ARAUJO, con DNI N° 41151912 y JUAN ANTONIO RIOS MERCADO, con DNI N° 26687436, estudiantes de Posgrado de la Universidad Privada del Norte sucursal Cajamarca, con el debido respeto exponemos:

Que, es necesario acceder a la información pública relacionada con las Historias Clínicas del Hospital II, para realizar la Tesis sobre **Gestión de las Historias Clínicas y su Seguridad** en concordancia con la **Resolución N° 004-2016-PCM** que aprueba la **Norma Técnica Peruana "NTP ISO/IEC 27001:2014** *Tecnologías de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad en la Información*", donde Essalud es integrante.

Es que solicitamos el permiso respectivo y así poder documentar lo relacionado con la **Seguridad de la Información en las Historias Clínicas en el Hospital II Cajamarca.**

Agradeciendo de antemano por la atención que se sirva prestar a la presente, quedo de Ud.

Es justicia que esperamos alcanzar

Cajamarca, 12 de junio del 2017

Paul Omar Cueva Araujo

Juan Antonio Ríos Mercado
INGENIERO EN INFORMÁTICA Y SISTEMAS
Registro del colegio de Ingenieros del Perú N° 125363

Figura 11. Solicitud para poder realizar la investigación

- Según la Resolución de Gerencia General Nº 107-GG-ESSALUD-2014 que aprueba la Directiva Nº 001-GG-ESSALUD-2014 "Gestión de la Historia Clínica en los Centros Asistenciales del Seguro Social de Salud - ESSALUD", y de acuerdo a la categoría del Hospital II Cajamarca, fueron **50** las disposiciones a las que correspondió evaluar el nivel de cumplimiento para la Gestión de las Historias Clínicas. Ver el instrumento en el anexo VIII.1

La responsable de las Historias Clínicas es el Jefe de la Unidad de Admisión, Registros Médicos, Referencias y Contrareferencias, del Hospital II quien a su vez es el responsable principal de la gestión de las mismas y su cumplimiento de la norma, aplicando la entrevista preparada se obtuvo los siguientes resultados:

Figura 12. Entrevista a Jefe de la Unidad de Admisión, Registros Médicos

Figura 13. Entrevista a Jefe de la Unidad de Admisión, Registros Médicos

Tabla 43

Cuestionario en base a la Directiva N° 001-GG-ESSALUD-2014 y su relación con los controles de la NTP-ISO/IEC 27001:2014

DISPOSICIONES		Jefe Unidad de Admisión y Registros Médicos	Control NTP
N°	MANDATO		
TÉCNICO ADMINISTRATIVOS			
1	¿Se verifica que al momento de crear la historia clínica sea única en la institución?	SI	8.2.3
2	¿Se crea una historia física al crear la Historia Clínica en el Sistema de Gestión Hospitalaria?	SI	8.2.1
3	¿Toda documentación en la atención médica que se genera tiene el DNI como identificación?	NO	8.2.2
4	¿A los neonatos con patología se le crea una Historia Clínica propia?	SI	8.2.3
5	¿A los neonatos nacidos normales o natimuertos se le archiva en la Historia Clínica de la madre?	SI	8.2.2
6	¿Se conserva en forma íntegra, garantizando el orden cronológico y todos los formatos de la atención de salud?	SI	8.2.2
7	¿El archivo de historias clínicas está diferenciado en activos y pasivos?	SI	8.2.1
8	¿Se cuenta con un ambiente separado para las Historias Clínicas especiales con contenido potencial de implicancia médico legal?	SI	8.2.1
9	¿Cuenta con medidas de seguridad este archivo especial de Historias Clínicas con implicancia médico legal?	NO	9.2.2 9.2.3
10	¿Se ha gestionado los recursos humanos, físicos y apoyo logístico de forma continua para la conservación de la documentación?	SI	7.1.2 11.1.4 11.2.1
11	¿Se encuentra establecido quien es el responsable de la custodia de las Historia Clínica físicas en el archivo?	SI	5.1.1 9.1.1
12	¿Se encuentra establecido quien es el responsable de la custodia de las Historias Clínicas físicas en caso de salir del archivo?	SI	5.1.1 11.2.6
13	¿Se encuentra actualizado los datos el sistema informático para el registro, control y monitoreo de la Historia Clínica, para el seguimiento y ubicación?	SI	8.1.1 12.4.1
14	¿Se atienden las copias de solicitudes de las Historias Clínicas solicitadas por los pacientes o por mandato judicial?	SI	
15	¿En el servicio de Hospitalización la enfermera de cada servicio donde está el paciente es responsable de la Historia Clínica?	SI	7.1.2 8.1.3 6.1.1
16	¿En el servicio de Hospitalización la enfermera entrega la historia clínica completa y ordenada al archivo dentro de las 48 horas siguientes al momento del alta?	NO	8.1.4
17	¿La historia de los pacientes fallecidos es entregada al área de Epidemiología?	SI	8.1.4 8.2.3 8.3.2
18	¿El área de Epidemiología entrega la historia clínica al archivo dentro de las 72 horas de su recepción?	NO	8.1.4 8.2.3 8.3.2
19	¿Las historias clínicas usadas en la Consulta Externa son devueltas el mismo día?	NO	8.1.4 8.2.3

20	¿Las historias clínicas usadas en la Hospitalización o Emergencia son devueltas el las 48 horas de la alta del paciente?	NO	8.1.4 8.2.3
21	¿Las historias clínicas usadas para informes médicos o auditorias médicas son devueltas en un plazo menor a 72 horas?	SI	8.1.4 8.2.3
22	¿El archivo de historias cuenta con un Plan de Fumigaciones al menos trimestralmente?	NO	11.1.4 11.1.5
23	¿Cuenta con ventilación adecuada, ventiladores, aire acondicionado, extractores e inyectores de aire, deshumedecedores el archivo de historias físicas?	NO	11.1.4 11.1.5
24	¿La historia clínica se encuentra protegida mediante fólderes?	SI	8.2.2
25	¿Las historias clínicas depuradas se encuentran almacenadas en cajas de cartón o según normatividad vigente?	SI	8.3.2
26	¿El área de archivo cuenta con señalización?	NO	11.1.5
27	¿El área de archivo cuenta con sistemas contraincendios, extintores y detectores de humo?	NO	11.1.5 11.2.1
28	¿El área de archivo cuenta con sistema de videocámaras?	NO	11.1.3 11.1.4
29	¿El área de archivo cuenta con sala de trabajo, sala de lectura y cuentan con videocámara?	NO	11.1.5
30	¿Se realiza el proceso de depuración anual de las HC de archivo?	NO	8.2.3
31	¿El archivo activo cuenta con información de historias clínicas con su última atención menor a cinco años?	SI	8.2.1 8.2.3
32	¿Se realiza la destrucción total de las historias clínicas del archivo pasivo mayores a 10 años y que sólo cuenten con atenciones de consulta externa?	NO	8.3.2
33	¿Se realiza la destrucción selectiva de las historias clínicas del archivo pasivo mayores a 10 años y que contienen atenciones de hospitalización?	NO	8.2.3
COMITÉ DE HISTORIAS CLÍNICAS			
34	¿Cuenta con un Comité de Auditoría de Historias Clínicas?	SI	6.1.1
35	¿Se informa al Comité de Historias Clínicas con acta de la destrucción total y selectiva de las historias clínicas mayores a 10 años del archivo pasivo?	NO	8.2.3
36	¿El Comité de Auditoría de Historias Clínicas informa los hallazgos encontrados?	SI	17.1.3
SISTEMA DE HISTORIAS CLÍNICAS INFORMATIZADAS			
37	¿Cuenta con un Sistema de Historia Clínica informatizada?	SI	12.5.1
38	¿Se hacen auditorias regulares al Sistema de Historia Clínica Informatizada?	SI	18.2.3
39	¿Cuenta con un servidor apropiado para almacenar las Historias Clínicas electrónicas?	SI	
40	¿Se cuenta con copias de seguridad diarias de las Historias Clínicas?	SI	12.3.1 12.4.1

41	¿Se cuenta con seguridad el acceso a los Servidores de las Historias Clínicas?	SI	9.4.1 9.4.2 9.4.3 10.1.2 11.1.1
42	¿Se cuenta con señalización el Centro de Cómputo de la Red Asistencial Cajamarca?	NO	13.1.1
43	¿Se cuenta con sistemas contra incendios, extintores y detectores de humo en el Centro de Cómputo?	NO	11.1.5 11.2.1
OTROS			
44	¿Cuenta con el Plan de continuidad del Negocio?	NO	17.1.1
45	¿Realiza las pruebas del Plan de Continuidad del Negocio?	NO	17.1.2
TECNICO ASISTENCIALES			
46	¿Se tiene la reserva de la información relacionada con el acto médico y su historia clínica?	SI	13.2.4 18.1.3 18.1.4
47	¿El registro por parte de los profesionales de la salud contiene las prácticas y procedimientos aplicados al paciente?	SI	
48	¿Todas las atenciones médicas y no médicas cuentan con acto médico?	SI	8.2.3
49	¿Cada atención tienen registrado el código CIE-10?	SI	8.2.3
50	¿Todas las atenciones tienen la firma y sello del profesional asistencial?	SI	8.2.3
	TOTAL DE CUMPLIMIENTO DE DISPOSICIONES	30	

Nota. Disposiciones y su incidencia sobre los controles de la seguridad de la Información

De acuerdo al análisis de la implementación de la Directiva indicada para el proceso de Gestión de la Historia Clínica en el Hospital II Cajamarca - EsSalud, se presenta el siguiente resumen:

Tabla 44

Porcentaje de cumplimiento de la Gestión de la Historia Clínica en el Hospital II Cajamarca - EsSalud

Cumplimiento	Disposiciones	Porcentaje
SI	30	60%
NO	20	40%
TOTAL	**50**	**100%**

Nota. Las disposiciones relacionadas a la parte asistencial tienen un cumplimiento del 100%

En el Hospital II de EsSalud Cajamarca se evidencia que al aplicar la Directiva 001-GG-ESSALUD-2014 sobre Gestión de las Historias Clínicas en los Centros Asistenciales del Seguro Social de Salud EsSalud, se tiene un 60% de disposiciones o buenas prácticas implementadas, al evaluar la información por dimensiones o categorías se obtuvo lo siguiente:

Tabla 45

Resumen de aplicación de entrevistas

Gestión de la Historia Clínica	Técnico Administrativo	Técnico Asistencial	Total
TOTAL RESPUESTAS			
TOTAL Respuestas	45	5	50
SI	25	5	30
NO	20	0	20
PORCENTAJES			
SI	55,5%	100,0%	60,0%
NO	44,5%	0,0%	40,0%

Nota. Las disposiciones relacionadas a la parte asistencial tienen un cumplimiento del 100%

Se aprecia que en los Procesos Técnico Asistenciales hay un cumplimiento del 100% de las indicaciones, luego en el cumplimiento para los Procesos Administrativos en la Gestión de la Historia Clínica es de un 55.5%.

V.2 Análisis de la relación entre la Gestión de la Historia Clínica y la NTP-ISO/IEC 27001:2014

Relación de la Gestión de la Historia Clínica con la NTP-ISO/IEC 27001:2014

La evaluación de las disposiciones de la Gestión de la Historia Clínica ha permitido identificar una relación entre esta norma y los controles de la NTP-ISO/IEC 27001:2014 encontrándose que 47 de las 50 disposiciones tienen una relación con algún o algunos controles relacionados a la Seguridad de la Información.

$$\frac{47}{50} * 100 = 94\%$$

Porcentaje de controles de NTP-ISO/IEC 27001:2014 con implicancia en la Gestión de la Historia Clínica

De los 114 controles que tiene la NTP-ISO/IEC 27001:2014, se han identificado 34 relacionados con la Gestión de la Historia Clínica.

$$\frac{34}{114} * 100 = 29.8\%$$

Control de la NTP-ISO/IEC 27001:2014 que tiene mayor relación con las disposiciones de la Gestión de las Historias Clínicas

El control de la NTP que mayor coincidencia tiene en las preguntas de la Gestión de la Historia Clínica es decir es el control que más veces aparece en las disposiciones de la Gestión de la Historia Clínica es el 8.2.3 el cual tiene que ver con el Manejo de activos, este control está relacionado con 14 de las 50 actividades de la Gestión de la Historia Clínica.

Categorías de controles de la NTP-ISO/IEC 27001:2014 que mayor relación tiene con las disposiciones de la Gestión de las Historias Clínicas

De acuerdo a las categorías de la NTP-ISO/IEC 27001:2014 desde la 5 a la 18, la categoría 17 relacionada a la Continuidad de la Seguridad de la Información está relacionada en un 75% con la Gestión de las Historias clínicas, seguida de la categoría 8 relacionada a la Clasificación de la Información y la que se relaciona en menor medida sería la categoría 6 Organización de la seguridad de la información con un 14% de relación, las categorías 14 Seguridad en los Procesos de Desarrollo y Soporte, 15 Relaciones con los Proveedores y 16 relacionada a la Gestión de incidentes de seguridad de la información no están relacionadas con la Gestión de la Historia Clínica.

Tabla 46

Relación entre los Controles de la NTP y la Gestión de la Historia Clínica

Control		Porcentaje
5	Políticas de Seguridad de la Información	50%
6	Organización de la Seguridad de la información	14%
7	Seguridad de los recursos humanos	17%

8	Gestión de Activos	70%
9	Control de acceso	43%
10	Criptografía	50%
11	Seguridad física y ambiental	33%
12	Seguridad de las operaciones	21%
13	Seguridad de las comunicaciones	29%
17	Aspectos de la seguridad de la información en la gestión de la continuidad del negocio	75%
18	Cumplimiento	38%

Nota. El aspecto que tiene mayor incidencia es el relacionado con la Continuidad del Negocio.

V.3 Propuesta de mejora sobre las Deficiencias de la Gestión de las Historias Clínicas

Del análisis del cumplimiento del uso de la Directiva 001-GG-ESSALUD-2014 sobre Gestión de las Historias Clínicas en los Centros Asistenciales del Seguro Social de Salud EsSalud, en el Hospital II Cajamarca del Seguro Social de Salud EsSalud, se realiza el análisis de las acciones no realizadas para tener propuestas de solución:

Las que no son efectuadas son:

Tabla 47

Disposición N° 3

Disposiciones		Cumple
N°	Mandato	
3	¿Toda documentación en la atención médica que se genera tiene el DNI como identificación?	NO

Nota. Se debería usar el Documento Nacional de Identidad.

De lo conversado con el personal indican que **nunca** han usado como identificador principal el Documento de Identidad para los pacientes atendidos, usan el Sistema de Gestión Hospitalaria para otorgar la cita, el médico registra en el Sistema de Gestión Hospitalaria y tiene en cuenta el **acto médico e historia clínica** para realizar el llenado de exámenes auxiliares de ser necesario, por lo que se debería actualizar la norma sobre esta disposición.

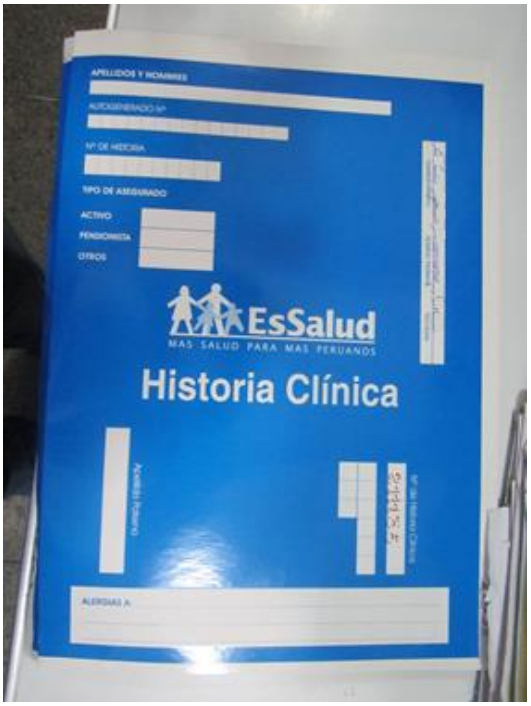


Figura 14. Historia Clínica física

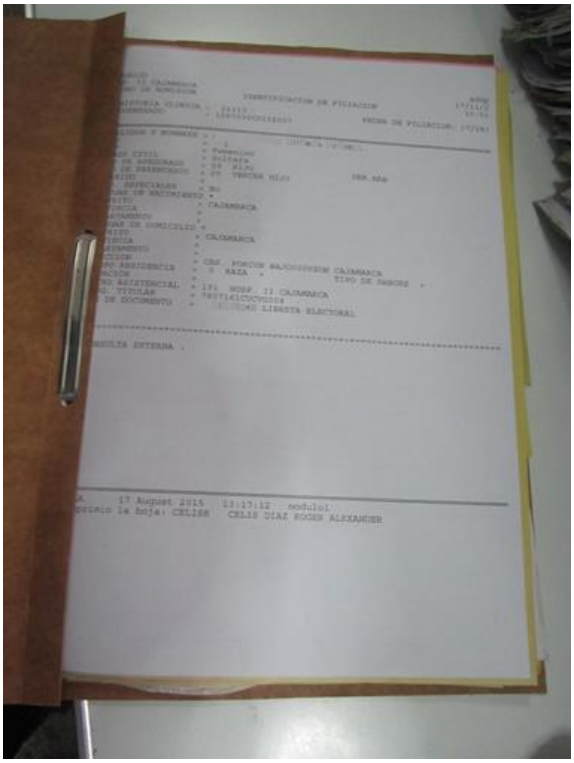


Figura 15. Datos de asegurado en Historia Clínica

Tabla 48

Disposición N° 9

Disposiciones		Cumple
N°	Mandato	
9	¿Cuenta con medidas de seguridad este archivo especial de Historias Clínicas con implicancia médico legal?	NO

Nota. Referido a las Historias Clínicas solicitadas para temas legales.

No se cuenta con un archivo especial de Historias Clínicas, en consecuencia, no se tienen medidas de seguridad asignadas.

Tabla 49

Disposición N° 16 y 20

Disposiciones		Cumple
N°	Mandato	
16	¿En el servicio de Hospitalización la enfermera entrega la historia clínica completa y ordenada al archivo dentro de las 48 horas siguientes al momento del alta?	NO
20	¿Las historias clínicas usadas en la Hospitalización o Emergencia son devueltas a las 48 horas de la alta del paciente?	NO

Nota. Tiempo establecido en la norma.

Según el personal de archivo, la entrega de las historias clínicas se demoran debido a que la infraestructura que tiene el Hospital II Cajamarca del Seguro Social de Salud EsSalud, el local de Hospitalización está a una distancia de 3 Km aprox. del Archivo de Historias que está en el local de Consultorios Externos, se tiene que coordinar la movilidad, el chofer de la movilidad tiene más funciones que no siempre entrega las historias en el mismo día de su entrega, a veces la falta de personal permanente en el archivo para entrega de las Historias Clínicas, no existen cargos, ni listados de las historias clínicas que son trasladadas.

Tabla 50

Disposición N° 18

Disposiciones		Cumple
N°	Mandato	
18	¿El área de Epidemiología entrega la historia clínica al archivo dentro de las 72 horas de su recepción?	NO

Nota. Tiempo establecido en la norma.

El área de Epidemiología se encuentra en el mismo local de Hospitalización y Emergencia y como en el punto anterior, la entrega de las historias clínicas al área

de Epidemiología demora a veces hasta una semana por parte de los Servicios de Emergencia o del Servicio de Hospitalización, donde no se acepta la responsabilidad de la custodia de las historias clínicas por parte del personal de Enfermería.

Tabla 51

Disposición N° 19

Disposiciones		Cumple
N°	Mandato	
19	¿Las historias clínicas usadas en la Consulta Externa son devueltas el mismo día?	NO

Nota. Se cuenta con un Sistema de Gestión Hospitalaria que registra los datos de los pacientes.

Con el uso del Sistema de Gestión Hospitalaria no se sacan historias clínicas del día en la consulta externa al tener el profesional asistencial acceso el histórico de la información en el sistema, esta información se tiene desde el 2012, por lo que no aplica esta disposición actualmente y se debería actualizar la norma.

Tabla 52

Disposición N° 22

Disposiciones		Cumple
N°	Mandato	
22	¿El archivo de historias cuenta con un Plan de Fumigaciones al menos trimestralmente?	NO

Nota. Plan exigido al menos trimestralmente..

No se cuenta con un Plan de Fumigaciones para el archivo de historias clínicas del Hospital II Cajamarca del Seguro Social de Salud, EsSalud

Tabla 53

Disposición N° 23

Disposiciones		Cumple
N°	Mandato	
23	¿Cuenta con ventilación adecuada, ventiladores, aire acondicionado, extractores e inyectores de aire, deshumedecedores el archivo de historias físicas?	NO

Nota. Importante para poder conservar las Historias Clínicas.

El archivo de historias clínicas no tiene instalados ventiladores, aire acondicionado, extractores e inyectores de aire, deshumedecedores.

Figura 16. Ductos de ventilación natural en el Archivo de Historias Clínicas

Tabla 54

Disposición N° 26

Disposiciones		Cumple
N°	Mandato	
26	¿El área de archivo cuenta con señalización?	NO

Nota. Implementación de señalética

El archivo no cuenta con señalización de áreas más si cuenta en los anaqueles donde se archivan las historias el rango de las historias clínicas que están en esa fila.

Figura 17. Anaqueles de Historias Clínicas

Figura 18. Entrevistas a Personal encargado de administración de Historias Clínicas

Tabla 55

Disposición N° 27

Disposiciones		Cumple
N°	Mandato	
27	¿El área de archivo cuenta con sistemas contraincendios, extintores y detectores de humo?	NO

Nota. Importante para casos de incendios

El archivo de historias clínicas evidencia que cuenta con extintores, no cuenta con sistemas contraincendios y detectores de humo.

Figura 19. Extintores en diferentes ambientes del archivo de historias clínicas

Figura 20. Extintores cerca a anaqueles de historias clínicas

Tabla 56

Disposición N° 28

Disposiciones		Cumple
N°	Mandato	
28	¿El área de archivo cuenta con sistema de videocámaras?	NO

Nota. Existe en la institución, pero no específicamente en el Archivo de Historias Clínicas.

El archivo de historias clínicas no cuenta con videocámaras instaladas.

Tabla 57

Disposición N° 29

Disposiciones		Cumple
N°	Mandato	
29	¿El área de archivo cuenta con sala de trabajo, sala de lectura y cuentan con videocámara?	NO

Nota. El área ha quedado insuficiente para la cantidad de historias clínicas.

Figura 21. Ausencia de salas de trabajo y lectura

El archivo de historias clínicas del Hospital II Cajamarca del Seguro Social de Salud EsSalud no cuenta con salas de trabajo, lectura y por consiguiente no tienen instalados videocámaras.

Tabla 58

Disposición N° 30

Disposiciones		Cumple
N°	Mandato	
30	¿Se realiza el proceso de depuración anual de las HC de archivo?	NO

La depuración del archivo de historias clínicas de acuerdo a normas no se ha depurado regularmente, el último realizado es el 2015 y para este año se tiene planificado en noviembre 2017.

Tabla 59

Disposición N° 32

Disposiciones		Cumple
N°	Mandato	
32	¿Se realiza la destrucción total de las historias clínicas del archivo pasivo mayores a 10 años y que sólo cuenten con atenciones de consulta externa?	NO

Al no realizarse regularmente la depuración de historias clínicas del pasivo mayores a 10 años, no se está destruyendo, pero las veces que se ha realizado se cumplió con la destrucción total de las historias clínicas que cuentan con atenciones solo de consulta externa.

Tabla 60

Disposición N° 33

Disposiciones		Cumple
N°	Mandato	
33	¿Se realiza la destrucción selectiva de las historias clínicas del archivo pasivo mayores a 10 años y que contienen atenciones de hospitalización?	NO

Al no realizarse regularmente la depuración de historias clínicas del pasivo mayores a 10 años, no se está destruyendo, pero las veces que se ha realizado se cumplió con la destrucción selectiva de las historias clínicas que cuentan con atenciones de hospitalización.

Tabla 61

Disposición N° 40

Disposiciones		Cumple
N°	Mandato	
40	¿Se informa al Comité de Historias Clínicas con acta de la destrucción total y selectiva de las historias clínicas mayores a 10 años del archivo pasivo?	NO

No se tiene constancia de informar al Comité de Historias Clínicas el acta de destrucción total y selectiva de las historias clínicas mayores a 10 años del archivo pasivo.

Tabla 62

Disposición N° 47

Disposiciones		Cumple
N°	Mandato	
47	¿Se cuenta con señalización el Centro de Cómputo de la Red Asistencial Cajamarca?	NO

El Centro de Cómputo de la Red Asistencial y que almacena los servidores del Hospital II Cajamarca para el Sistema de Gestión Hospitalaria y otros sistemas, no cuenta con las señalizaciones respectivas en su totalidad de ambientes y equipos.

Figura 22. Ausencia de señalización en Centro de Cómputo

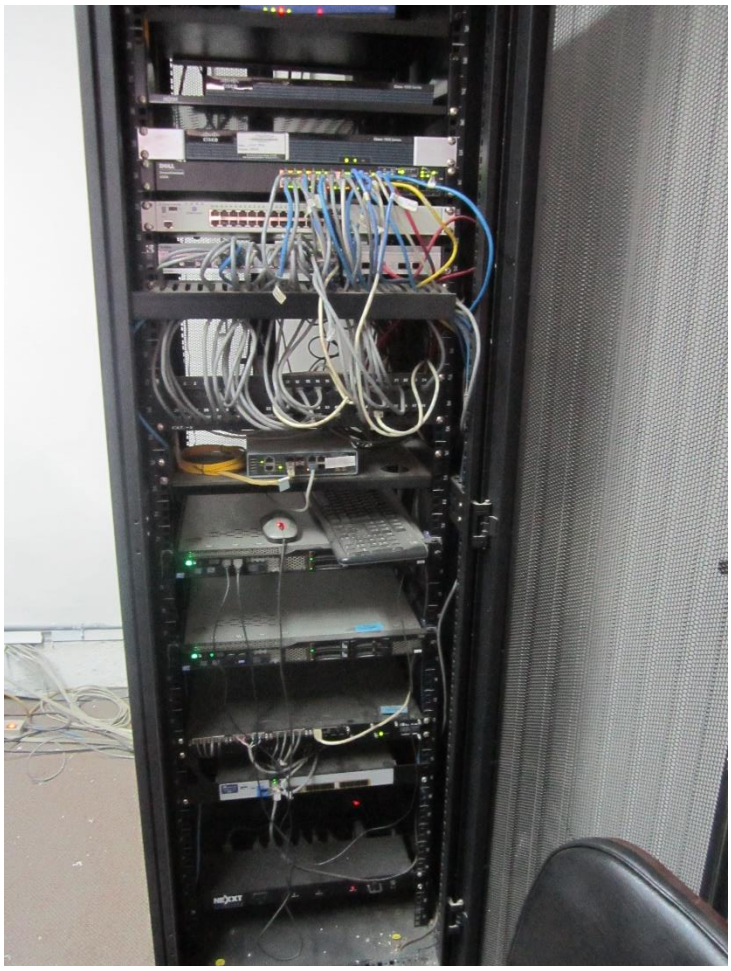


Figura 23. Necesidad de señalización en Data Center

Tabla 63

Disposición N° 48

Disposiciones		Cumple
N°	Mandato	
48	¿Se cuenta con sistemas contra incendios, extintores y detectores de humo en el Centro de Cómputo?	NO

El Centro de Cómputo de la Red Asistencial cuenta con extintores mas no detectores de humo y sistemas contraincendios.

Figura 24. Extintores en Data Center

VI. DISCUSIÓN Y CONCLUSIONES

El Hospital II de ESSALUD Cajamarca enfrenta algunas deficiencias dentro de las cuales se incluye el cumplimiento parcial de la Directiva N° 001-GG-ESSALUD-2014 “Gestión de la Historia Clínica en los Centros Asistenciales del Seguro Social de Salud - EsSalud”, razón por la cual se hace necesario mejorar su gestión debido a que la Historia Clínica constituye el activo principal de información que maneja esta institución y debe ser resguardado de una manera adecuada ello también debido a que en el Perú las entidades estatales deben tener implementado un Sistema de Gestión de la Seguridad de la Información basado en la NTP ISO /IEC 27001, estas dos variables de gestión según el análisis realizado en la presente investigación se encuentran interrelacionadas descriptivamente y permiten determinar que al incrementar una mejor Gestión a la Historia Clínica se mejora también de manera directa y significativamente la seguridad de la Información y se puede cumplir con las diferentes normativas propias del sector salud y otras transversales a todas las entidades estatales.

Para lograr obtener la información necesaria sobre la gestión de Historias Clínicas análisis ha sido necesario observar los procesos que inciden con esta y ver cómo se lleva a cabo más allá de los procedimientos que puedan estar normados y documentados de manera tal que se pueda obtener una información objetiva que permita hacer un buen análisis el cual muestra un cumplimiento parcial y algunas deficiencias sobre las que la institución debe trabajar en el tiempo.

La seguridad de la información ha sido posible de evaluar a través de un análisis de brechas en base a los controles que establece la NTP ISO/IEC 27001:2014, para tal fin también ha sido necesario revisar la documentación pertinente, realizar una entrevista al personal responsable y hacer una observación de todo proceso ligado a la Seguridad de la Información y que tenga relación con la gestión de las Historias Clínicas.

Se logró Identificar las brechas de seguridad de la información que debe tomar en cuenta ESSALUD Cajamarca para poder estar acorde a lo que establece la norma técnica peruana y los estándares internacionales, los cuales se siguen desarrollando y mejorando, siendo necesario señalar que el tema de la seguridad de la información en nuestro país se encuentra en una etapa de desarrollo.

Se aplicó una evaluación de la Directiva N° 001-GG-ESSALUD-2014 “Gestión de la Historia Clínica en los Centros Asistenciales del Seguro Social - ESSALUD”, aprobada por la Resolución de Gerencia General N° 107-GG-ESSALUD-2014 (21-Ene-2014), igualmente una auditoría informática basada en la Norma Técnica Peruana NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos 2da Edición (08-Ene-2016) para el Hospital II Cajamarca del Seguro Social de Salud, EsSalud.

Del análisis realizado a la Gestión de la Historia Clínica en el Hospital II Cajamarca del Seguros Social, se encontró que el uso del Sistema de Gestión Hospitalaria permite utilizar Historias Clínicas Informatizadas en la mayoría de las Actividades Asistenciales pero que al no cumplir con la firma digital del profesional y no profesional no es completa la implementación siendo ambigua la implementación y se tiene deficiencias importantes como la demora en la entrega de las Historias Clínicas por parte de los Servicios (Hospitalización, Emergencia, etc.) por encima del periodo permitido, no está aceptada la responsabilidad de las Enfermeras de las

Historias Clínicas cuando están fuera del Archivo en la Hospitalización, falta de seguimiento de las Historias Clínicas que salen del Archivo.

De los hallazgos en la auditoría informática a la Seguridad de la Información del Hospital II Cajamarca del Seguro Social de EsSalud, se realizó un análisis detallado de riesgos a los activos informáticos involucrados en el proceso de gestión de las historias clínicas, identificándose todos aquellos riesgos que atentan contra la continuidad del servicio.

De la Gestión de la Historia Clínica que se realiza en el Hospital II Cajamarca del Seguro Social de Salud EsSalud, se llega a cumplir en un 40% del total de disposiciones contempladas en la Directiva evaluada, ocasionando que se afecte directamente en la Confidencialidad, Integridad y Disponibilidad de la información de los pacientes. A consecuencia de la evaluación se dieron las acciones necesarias para fortalecer la Seguridad de la Información y proteger los activos relacionados al proceso de la Gestión de las Historias Clínicas, mediante la priorización de los controles aplicables para la ejecución de pruebas de cumplimiento y pruebas sustantivas.

CONCLUSIONES

1. Las características más importantes de la Gestión de la Historia Clínica y la Seguridad de la Información en el Hospital II Cajamarca – EsSalud bajo la NTP-ISO/IEC 27001:2014 son:
   - Característica Administrativa, en referencia al Manejo de Activos de la NTP-ISO/IEC 27001:2014, al abarcar el 90% de las dimensiones que se deben cumplir.
   - Característica Asistencial, que al cumplirse en un 100% hace mayor referencia al Manejo de Activos de la NTP-ISO/IEC 27001:2014.
2. El análisis de la Gestión de la Historias Clínicas en el Hospital II Cajamarca nos ha llevado a observar que la dimensión Técnico Administrativo tiene un total de 45 disposiciones que debe cumplir sobre un total de 50 es decir abarca el 90% de dimensiones, de las cuales se están cumpliendo en la actualidad un total de 25 que representan el 55,5% y por lo mismo se ha desarrollado una serie de sugerencias de mejoras que se deben de implementar con la finalidad de resguardar de la manera más adecuada este importante activo de información.

Esta dimensión administrativa también abarca 7 disposiciones relacionadas con la informatización de las Historias Clínicas, un aspecto muy ligado con la seguridad de la Información, de las cuales 5 se vienen cumpliendo en la actualidad.

3. El análisis de la seguridad de la Información en el Hospital II Cajamarca - EsSalud tomando como base los controles definidos en la NTP ISO/IEC 27001:2014 determino que se está cumpliendo en un 51% con los controles debiéndose tomar acciones para mejorar este aspecto, sin embargo, un 10% se encuentra en etapa de maduración y por lo tanto por ahora se cumple de manera parcial, sin embargo, hay un porcentaje del 33% de controles que aún no se cumplen o su implementación se encuentra en una etapa inicial. Dentro de los controles de referencia para la seguridad de la Información el que se encuentra en una etapa alta de implementación es el concerniente al Cumplimiento, esto debido a que EsSalud debe cumplir con muchas exigencias normativas del estado peruano y por otro lado el control con menor grado de implementación es el referido a la seguridad de los Recursos Humanos relacionados a la seguridad de la Información debido a la falta de cultura organizacional relacionada al tema de la seguridad de la Información y que EsSalud debe implementar en su personal.

RECOMENDACIONES

A consecuencia del análisis realizado en la presente investigación y de la relevancia administrativa de la Gestión de la Historia Clínica en el Hospital II EsSalud Cajamarca, se plantea como recomendación desarrollar las siguientes actividades:

RECOMENDACIÓN	RESPONSABILIDAD
Mejorar la seguridad y el acceso al Archivo de Historias Clínicas del Hospital II Cajamarca del Seguro Social de Salud, EsSalud.	• Unidad de Admisión, Registros Médicos, Referencias y Contrarreferencias. • Oficina de Administración.
Continuar realizando los procesos de depuración y eliminación de Historias Clínicas.	• Unidad de Admisión, Registros Médicos, Referencias y Contrarreferencias • Oficina de Administración

	• Dirección Médica
Considerar en el Plan de Capacitaciones Local de la Red Asistencial Cajamarca, las inducciones continuas sobre: • Gestión de la Historia Clínica. • Gestión de Riesgos de los principales activos de la Institución. • Gestión de continuidad del negocio.	• Unidad de Admisión, Registros Médicos, Referencias y Contrarreferencias. • Área de Capacitación y Docencia • Oficina de Planeamiento y Calidad
Desarrollar y ejecutar un plan de mantenimientos preventivos / correctivos de los equipos informáticos.	• Unidad de Soporte Informático, • Oficina de Administración
Implementar una herramienta para la gestión de vulnerabilidades.	• Unidad de Soporte Informático

VII. Lista de referencias

Aliaga Infante, R. J. (2014). Analisis de riesgos de TI para la implementación de un sistema de seguridad de la informacion en el gobierno regional de Cajamarca. Cajamarca, Perú: Universidad Nacional de Cajamarca.

Atienza, O. A. (2013). Historia Clínica informática única una herramienta en la mejora de procesos en salud pública. Córdoba, Argentina: Universidad Nacional de Córdoba.

Calderón Merchán, D. O., & Sanchez Meza, D. A. (Octubre de 2012). "Desarrollo de un Sistema de Gestión de Seguridad de la Información (SGSI) para la Empresa Comware S.A. en la Ciudad de Quito, Aplicando la Norma ISO/IEC 27001". Quito, Ecuador: Universidad Politécnica Salesiana.

Congreso de la República . (09 de julio de 1997). Ley General de Salud Ley Nº 26842. Lima, Perú.

Córdoba, J. C. (2007). *Modelo de Calidad para Portales Bancarios.* San José, Costa Rica.

Cruz Malca, M. L. (2015). Repercusión de la gestión de las historias clínicas en la seguridad de la información del Hospital Regional Cajamarca, marzo – agosto 2015. Cajamarca, Perú: Universidad Privada del Norte.

Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. (octubre de 2012). MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I - Método. Madrid, España: Ministerio de Hacienda y Administraciones Públicas.

Dirección General de Salud de las Personas MINSA. (2005). N.T. No 022-MINSA/DGSP-V.02. *Norma Técnica de la Historia Clínica de los Establecimientos del Sector Salud*. Lima, Perú.

Donato, B. (11 de noviembre de 2013). La Historia Clínica Electrónica centrada en el paciente como componente fundamental para la gestión de un Sistema de Información de Salud. Argentina: Universidad de San Andrés.

Gartner. (03 de febrero de 2014). *Gartner Blog Network.* Obtenido de http://blogs.gartner.com/ben-tomhave/new-research-on-it-risk-assessment-and-analysis-methods/

Gerencia Central de Prestaciones de Salud. (2013). Directiva N° 018-GG-ESSALUD-2013. *Definición, características y funciones generales de los establecimientos de salud del Seguro Social de Salud (ESSALUD)*. Perú.

Gerencia General de EsSalud. (2014). Directiva de Gerencia General Nº 001-GG-ESSALUD-2014. *Gestión de la Historia Clínica en los Centros Asistenciales del Seguro Social de Salud - ESSALUD*. Lima.

Gerencia General de EsSalud. (21 de 01 de 2014). Directiva de Gerencia General Nº 001-GG-ESSALUD-2014. *Gestión de la Historia Clínica en los Centros Asistenciales del Seguro Social de Salud - ESSALUD*. Lima.

Huamán Monzón, F. M. (12 de Setiembre de 2014). Diseño de Procedimientos de auditoría de cumplimiento de la norma NTP-ISO/IEC 17799:2007 como parte del proceso de implantación de la norma técnica NTP-ISO/IEC 27001:2008 en Instituciones del Estado Peruano. Lima, Perú: Pontificia Universidad Católica del Perú.

INDECOPI. (2014). Norma Técnica Peruana NTP-ISO/IEC 27001. *TECNOLOGÍA DE LA INFORMACIÓN. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos*. Lima, Perú.

Instituto Nacional de Tecnologías de la Comunicación. (2014). Implantación de un SGSI en la Empresa.

ISACA. (2009). An Introduction to the Business Model For Information Security. Illinois, USA.

ISO/IEC 27000. (15 de 02 de 2016). Information technology — Security techniques — Information security management systems — Overview and vocabulary. Suiza: ISO copyright office.

ISOTools Excellence. (2014). La norma ISO 27001 Aspectos clave de su diseño e implantación.

Ley N° 30024. (07 de Abril de 2013). *Ley que crea el registro nacional de historias clínicas electrónicas*. Lima, Perú: Diario Oficial El Peruano.

Ley Nº 29733. (02 de Julio de 2011). Ley de protección de datos personales. Lima, Perú: Diario Oficial El Peruano.

OPTIC, O. P. (2013). Normas y Estándares: Seguridad Informática. Gobierno Electrónico Republica Dominicana.

Presidencia del Consejo de Ministros. (08 de Enero de 2016). RESOLUCIÓN MINISTERIAL Nº 004-2016-PCM. *Uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición"*. Lima, Perú: Diario Oficial El Peruano.

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: Universidad Nacional Mayor de San Marcos.

Talavera Álvarez , V. R. (2015). Diseño de un Sistema de Gestión de Seguridad de la Información para una Entidad Estatal de Salud de Acuerdo a la ISO/IEC 27001:2013. Lima, Perú: Pontificia Universidad Católica del Perú.

Tomhave, B. (24 de octubre de 2014). *How to Achieve Success with Cyber Risk Assessment and Analysis.* Orlando, Florida. Obtenido de Information Systems Security Association: www.issa.org/resource/resmgr/2014_October_CISO/Ben_Tomhave.pdf

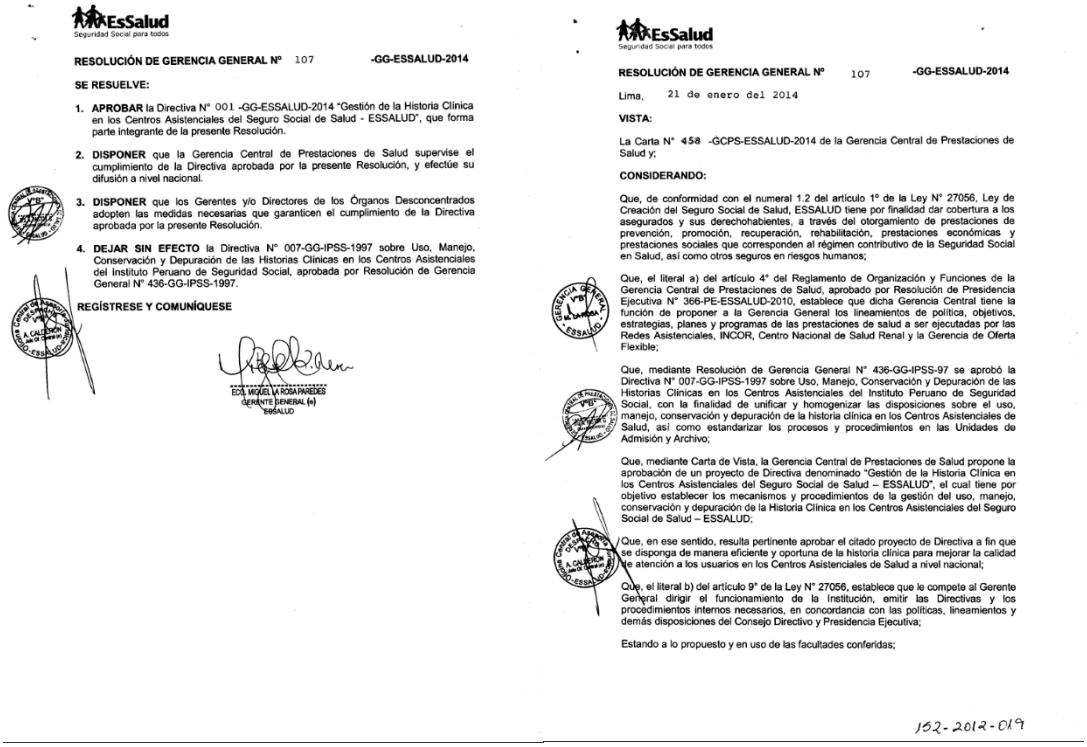
Valdunciel, L. M. (2007). Análisis de la Calidad de Servicio que prestan las Entidades Bancarias y su repercusión en la satisfacción del cliente y la lealtad hacia la Entidad. . *Revista Asturiana de Economía*, 85.

Valencia, A. (2012). Una visión para hacer mas eficiente el desempeño del Sector Bancario en América Latina. *IDC- Analyze The Future*, 1.

VIII. ANEXOS

VIII.1 Resolución de Gerencia General Nº 107-GG-ESSALUD - 2014

Esta resolución aprueba la Directiva Nº 001-GG-ESSALUD-2014 "Gestión de la Historia Clínica en los Centros Asistenciales del Seguir Social de Salud – ESSALUD"



EsSalud
Seguridad Social para todos

RESOLUCIÓN DE GERENCIA GENERAL Nº 107 **-GG-ESSALUD-2014**

SE RESUELVE:

1. **APROBAR** la Directiva N° 001 -GG-ESSALUD-2014 "Gestión de la Historia Clínica en los Centros Asistenciales del Seguro Social de Salud - ESSALUD", que forma parte integrante de la presente Resolución.
2. **DISPONER** que la Gerencia Central de Prestaciones de Salud supervise el cumplimiento de la Directiva aprobada por la presente Resolución, y efectúe su difusión a nivel nacional.
3. **DISPONER** que los Gerentes y/o Directores de los Órganos Desconcentrados adopten las medidas necesarias que garanticen el cumplimiento de la Directiva aprobada por la presente Resolución.
4. **DEJAR SIN EFECTO** la Directiva N° 007-GG-IPSS-1997 sobre Uso, Manejo, Conservación y Depuración de las Historias Clínicas en los Centros Asistenciales del Instituto Peruano de Seguridad Social, aprobada por Resolución de Gerencia General N° 436-GG-IPSS-1997.

REGÍSTRESE Y COMUNÍQUESE

EDIL MIGUEL LA ROSA PAREDES
GERENTE GENERAL (e)
ESSALUD

EsSalud
Seguridad Social para todos

RESOLUCIÓN DE GERENCIA GENERAL Nº 107 **-GG-ESSALUD-2014**

Lima, 21 de enero del 2014

VISTA:

La Carta N° 458 -GCPS-ESSALUD-2014 de la Gerencia Central de Prestaciones de Salud y;

CONSIDERANDO:

Que, de conformidad con el numeral 1.2 del artículo 1° de la Ley N° 27056, Ley de Creación del Seguro Social de Salud, ESSALUD tiene por finalidad dar cobertura a los asegurados y sus derechohabientes, a través del otorgamiento de prestaciones de prevención, promoción, recuperación, rehabilitación, prestaciones económicas y prestaciones sociales que corresponden al régimen contributivo de la Seguridad Social en Salud, así como otros seguros en riesgos humanos;

Que, el literal a) del artículo 4° del Reglamento de Organización y Funciones de la Gerencia Central de Prestaciones de Salud, aprobado por Resolución de Presidencia Ejecutiva N° 366-PE-ESSALUD-2010, establece que dicha Gerencia Central tiene la función de proponer a la Gerencia General los lineamientos de política, objetivos, estrategias, planes y programas de las prestaciones de salud a ser ejecutadas por las Redes Asistenciales, INCOR, Centro Nacional de Salud Renal y la Gerencia de Oferta Flexible;

Que, mediante Resolución de Gerencia General N° 436-GG-IPSS-97 se aprobó la Directiva N° 007-GG-IPSS-1997 sobre Uso, Manejo, Conservación y Depuración de las Historias Clínicas en los Centros Asistenciales del Instituto Peruano de Seguridad Social, con la finalidad de unificar y homogenizar las disposiciones sobre el uso, manejo, conservación y depuración de la historia clínica en los Centros Asistenciales de Salud, así como estandarizar los procesos y procedimientos en las Unidades de Admisión y Archivo;

Que, mediante Carta de Vista, la Gerencia Central de Prestaciones de Salud propone la aprobación de un proyecto de Directiva denominado "Gestión de la Historia Clínica en los Centros Asistenciales del Seguro Social de Salud – ESSALUD", el cual tiene por objetivo establecer los mecanismos y procedimientos de la gestión del uso, manejo, conservación y depuración de la Historia Clínica en los Centros Asistenciales del Seguro Social de Salud – ESSALUD;

Que, en ese sentido, resulta pertinente aprobar el citado proyecto de Directiva a fin que se disponga de manera eficiente y oportuna de la historia clínica para mejorar la calidad de atención a los usuarios en los Centros Asistenciales de Salud a nivel nacional;

Que, el literal b) del artículo 9° de la Ley N° 27056, establece que le compete al Gerente General dirigir el funcionamiento de la Institución, emitir las Directivas y los procedimientos internos necesarios, en concordancia con las políticas, lineamientos y demás disposiciones del Consejo Directivo y Presidencia Ejecutiva;

Estando a lo propuesto y en uso de las facultades conferidas;

152-2012-019

VIII.2 Procedimiento Generación del fólder de la historia clínica

Red Asistencial _____ **Unidad de Archivo e Historias Clínicas**	**Nombre del Procedimiento:** **GENERACIÓN DEL FÓLDER DE LA HISTORIA CLÍNICA**	**VERSION: 01** **FECHAS:** **Elaboración: Setiembre 2012** **Revisado: diciembre 2012** **Página: 1 de 2**

OBJETIVO:

- **Aperturar el fólder de la HC por asegurado, asignándole un número de Ubicación en el Sistema Informático vigente, para su ubicación en el archivo a fin de conservar, almacenar y proteger el contenido de la Historia Clínica (H:C).**

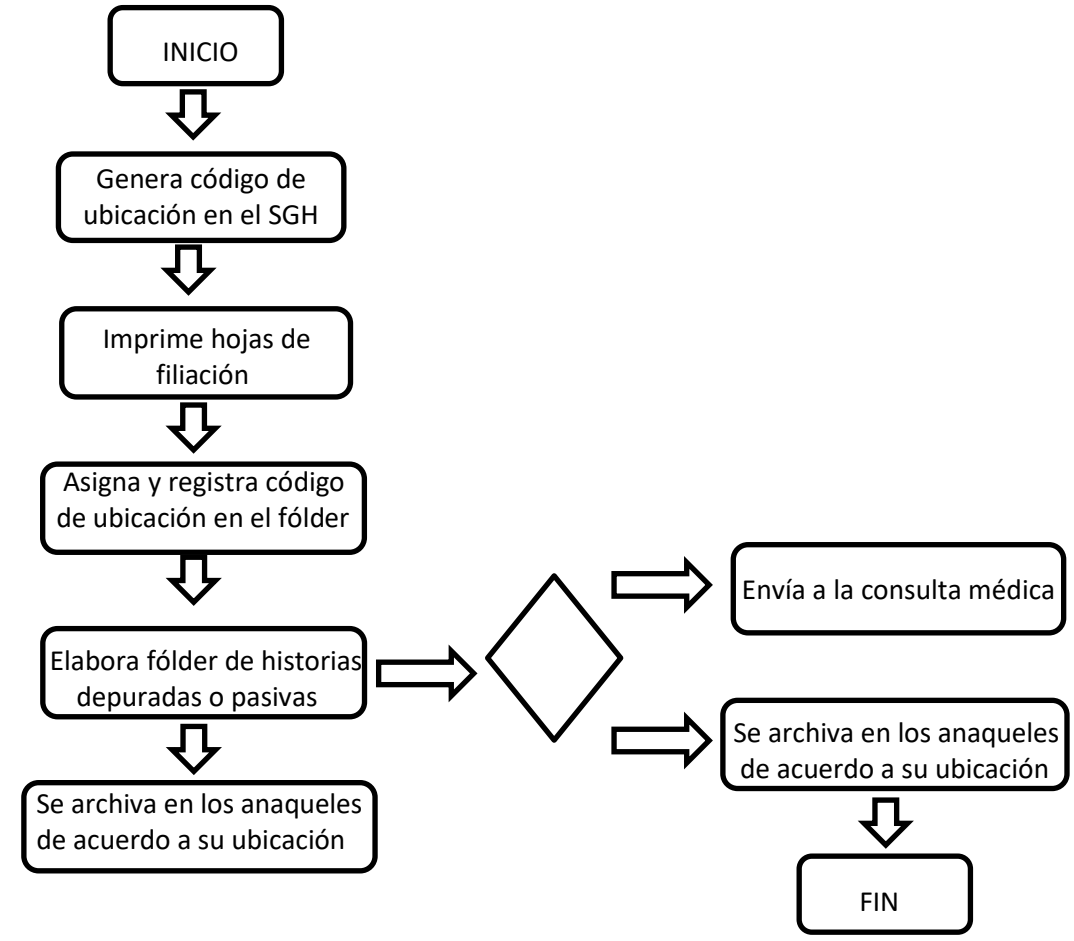
ALCANCE:

El procedimiento tiene aplicación en la Unidad de Archivo bajo supervisión del Jefe de la Unidad Orgánica y/o Encargado Funcional de Archivo e Historias Clínicas, y aplicación por el personal de la Unidad de Archivo en toda la Red Asistencial.

PASO N°	DESCRIPCIÓN DEL PROCEDIMIENTO	RESPONSABLE
1	Genera código de ubicación de los pacientes nuevos en el Sistema Informático vigente	Asistente Administrativo
2	Imprime las hojas de afiliación de los pacientes nuevos.	Asistente Administrativo
3	Asigna y registra manualmente el número de ubicación en el fólder de acuerdo al cuaderno de control.	Asistente Administrativo
4	Elaboración también fólder de las H.C. pasiva o depuradas, para la consulta médica.	Asistente Administrativo
5	Envía las H.C. de los pacientes nuevos a la Consulta Médica (Adicionales).	Asistente Administrativo
6	En caso no tuviera cita el paciente nuevo, la H.C. se envía al archivo para ser almacenada en su código de ubicación asignado.	Asistente Administrativo
7	Fin de Procedimiento.	

GENERACIÓN DEL FOLDER DE HISTORIA CLÍNICA

Asistente Administrativo



VIII.3 Procedimiento archivo de las historias clínicas

Red Asistencial _____ **Unidad de Archivo e Historias Clínicas**	**Nombre del Procedimiento:** ARCHIVO DE LAS HISTORIAS CLÍNICAS	**VERSION: 01** **FECHAS:** **Elaboración: Setiembre 2012** **Revisado: diciembre 2012** **Página: 1 de 2**

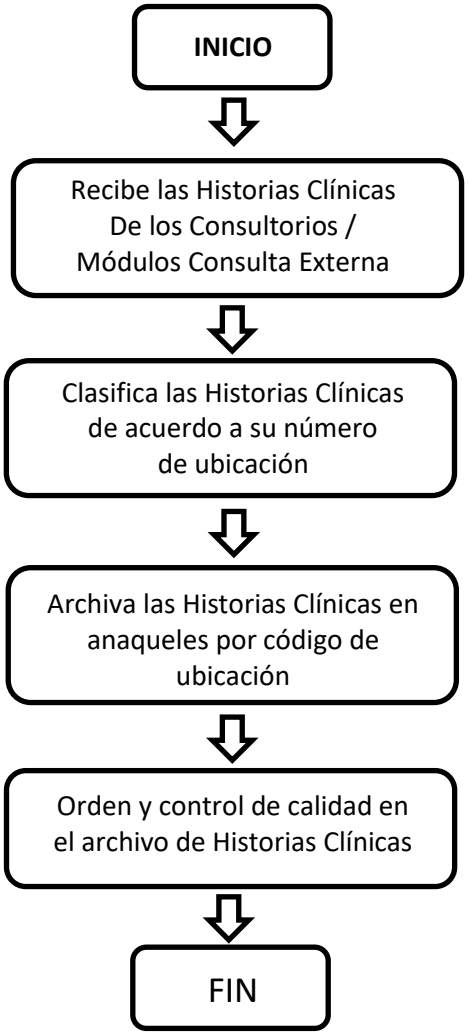
OBJETIVO:

- **Mantener el orden de las historias clínicas en el archivo.**
- **Ubicar con facilidad las historias clínicas.**
- **Garantizar la accesibilidad del archivo las 24 horas del día para sus diferentes requerimientos (Hospitalización, Emergencia).**
- **Custodiar el contenido de la historia en el código de ubicación asignado.**

ALCANCE:
Supervisión del procedimiento por el Jefe de la Unidad Orgánica y/o Encargado funcional de Archivo e Historias Clínicas y ejecución por el personal de la Unidad de Archivo en toda la Red Asistencial.

PASO N°	DESCRIPCIÓN DEL PROCEDIMIENTO	RESPONSABLE
1	Recibe las Historias Clínicas de los Consultorios / Módulos de Consulta Externa.	Técnico Administrativo
2	Clasifica las historias clínicas de acuerdo al número de ubicación	Técnico Administrativo
3	Archiva las historias clínicas en los anaqueles de acuerdo a su código de ubicación.	Técnico Administrativo
4	Garantiza el orden y la fácil ubicación de las historias en el archivo.	Técnico Administrativo
5	Busca los reclamos con relación a las historias clínicas no ubicadas en el archivo.	Técnico Administrativo
6	Realiza el control de calidad en el archivo, asegura el adecuado almacenamiento cambiando los sobres deteriorados.	Técnico Administrativo
7	Fin de procedimiento	Técnico Administrativo

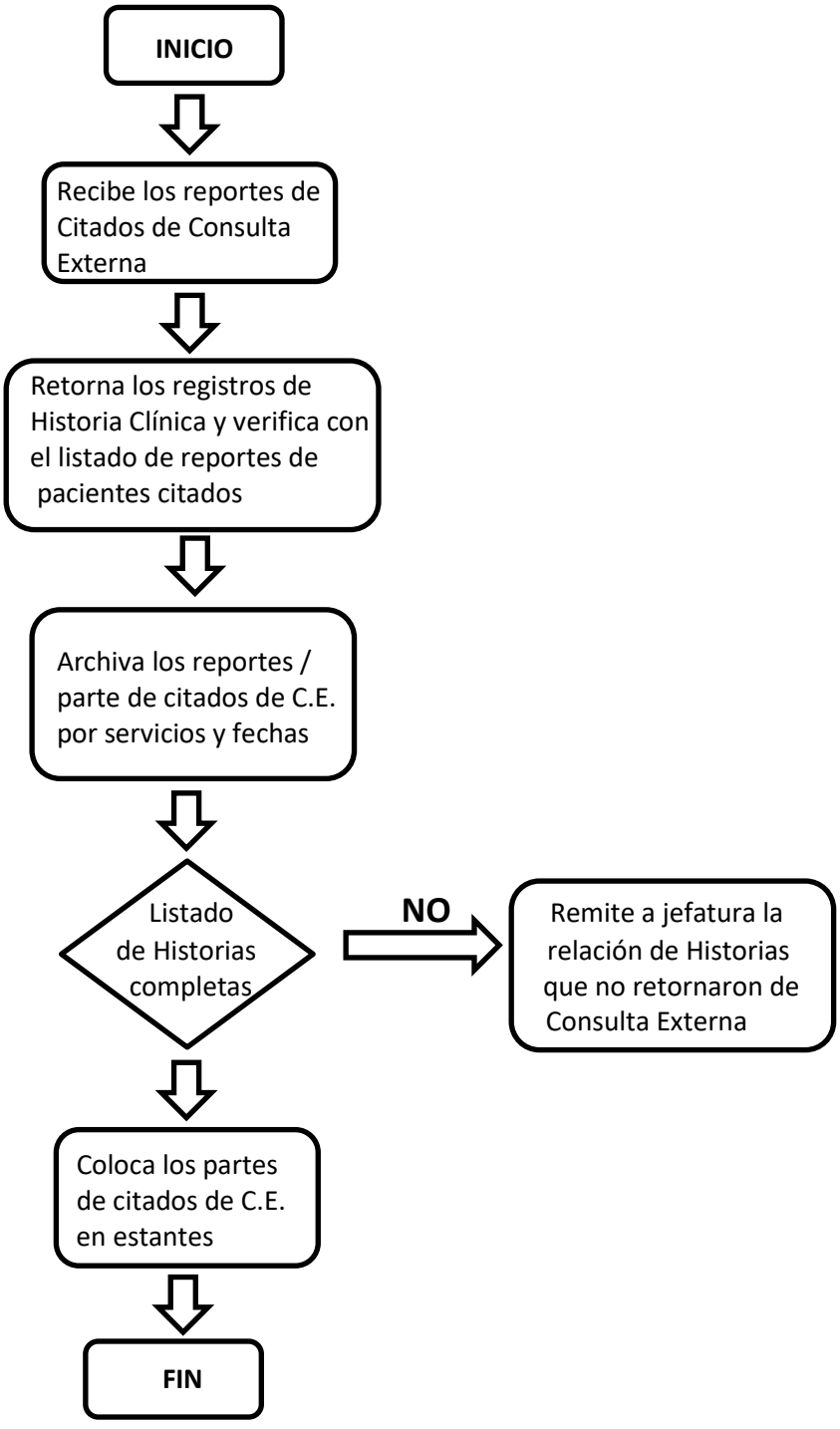
ARCHIVO DE HISTORIAS CLÍNICAS



VIII.4 Procedimiento retorno de historias clínicas a través del sistema de gestión hospitalaria

Red Asistencial _____ **Unidad de Archivo e Historias Clínicas**	**Nombre del Procedimiento:** RETORNO DE HISTORIAS CLÍNICAS A TRAVÉS DEL SISTEMA DE GESTIÓN HOSPITALARIA	**VERSION: 01** **FECHAS:** **Elaboración: Setiembre 2012** **Revisado: diciembre 2012** **Página: 1 de 2**
OBJETIVO: **Prevenir pérdidas controlando el retorno completo de las historias entregadas a los servicios usuarios descargando en el Sistema de Gestión Hospitalaria.**		
ALCANCE: **Supervisión del procedimiento por el Jefe de la Unidad Orgánica y/o Encargado funcional de Archivo e Historias Clínicas y ejecución por el personal de la Unidad de Archivo en toda la Red Asistencial.**		
PASO N°	DESCRIPCIÓN DEL PROCEDIMIENTO	RESPONSABLE
1	Recibe los reportes de citados de la consulta externa, verificados manualmente por el mensajero.	Digitador Asistencial
2	Retorna los registros de la historia clínica y verifica inmediatamente con el listado de reportes de pacientes citados.	Digitador Asistencial
3	Proceden a archivar el reporte de citados o el parte de citados por módulos de atención por fechas	Digitador Asistencial
4	Informe a la Jefatura las historias que no retornaron adjuntando cargo de las Historias Clínicas no retornadas	Digitador Asistencial
5	Coloca manualmente las partes de pacientes citados en los estantes	Digitador Asistencial
6	Fin de Procedimiento	

RETORNO DE HISTORICAS CLÍNICAS A TRAVÉS DEL SISTEMA INFORMÁTICO



VIII.5 Procedimiento préstamo de historias clínicas

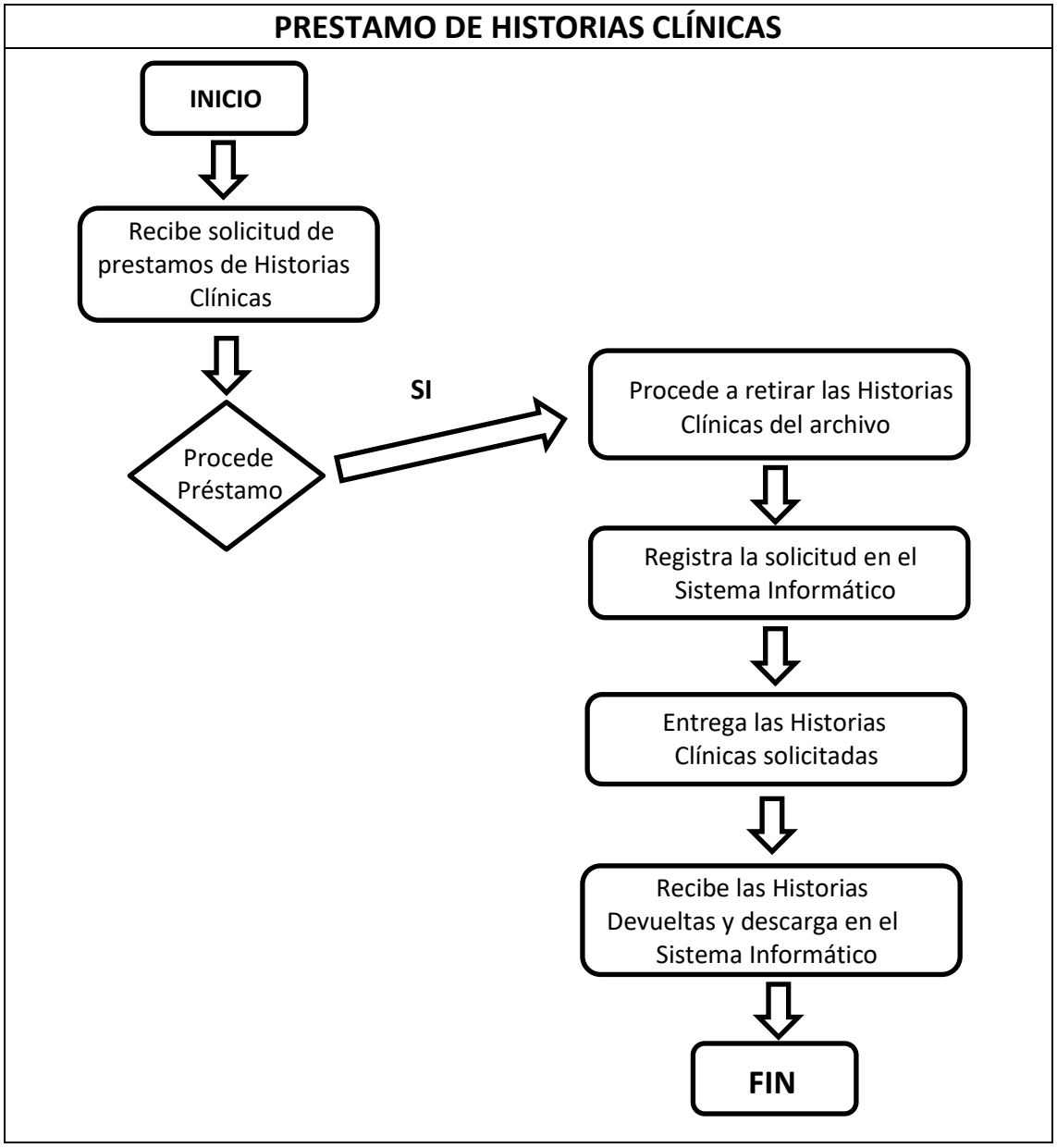
Red Asistencial **Unidad de Archivo e Historias Clínicas**	**Nombre del Procedimiento:** PRESTAMO DE HISTORIAS CLÍNICAS	**VERSION: 01** **FECHAS:** **Elaboración: Setiembre 2012** **Revisado: Diciembre 2012** **Página: 1 de 2**

OBJETIVO:

- **Remitir dentro de los plazos establecidos las solicitudes de historias clínicas para auditoría, investigación, junta médica, etc. a las diferentes Jefaturas u otros órganos del Centro Asistencial.**
- **Llevar el control de dichas historias prestadas a través del Sistema de Gestión Informático vigente (SGH/SGSS) y/o registro manual**

ALCANCE:
Supervisión del procedimiento por el Jefe de la Unidad Orgánica y/o Encargado funcional de Archivo e Historias Clínicas y ejecución por el personal de la Unidad de Archivo en toda la Red Asistencial.

PASO N°	DESCRIPCIÓN DEL PROCEDIMIENTO	RESPONSABLE
1	Recibe las solicitudes presentadas en la Unidad de Archivo por las distintas Jefaturas Médicas.	Técnico Administrativo
2	Procede a sacar las historias del archivo para el préstamo respectivo.	Técnico Administrativo
3	Registra las solicitudes por servicio en el sistema de Gestión Hospitalaria.	Técnico Administrativo
4	Entrega las solicitudes con las historias clínicas ubicadas a las secretarias y/o técnicos de enfermería de las diferentes Jefaturas	Técnico Administrativo
5	Recibe las H.C. devueltas de las diferentes Jefaturas las verifica y firma el cargo de retorno al archivo.	Técnico Administrativo
6	Retorna en el Sistema Informático vigente las HC devueltas de los diferentes servicios.	Técnico Administrativo
7	Fin de procedimiento.	


PRESTAMO DE HISTORIAS CLÍNICAS
INICIO
Recibe solicitud de prestamos de Historias Clínicas
Procede Préstamo
SI
Procede a retirar las Historias Clínicas del archivo
Registra la solicitud en el Sistema Informático
Entrega las Historias Clínicas solicitadas
Recibe las Historias Devueltas y descarga en el Sistema Informático
FIN

VIII.6 Procedimiento depuración de historias clínicas

Red Asistencial _____ **Unidad de Archivo e Historias Clínicas**	**Nombre del Procedimiento:** DEPURACION DE HISTORIAS CLÍNICAS	**VERSION: 01** **FECHAS:** **Elaboración: Setiembre 2012** **Revisado: diciembre 2012** **Página: 1 de 2**

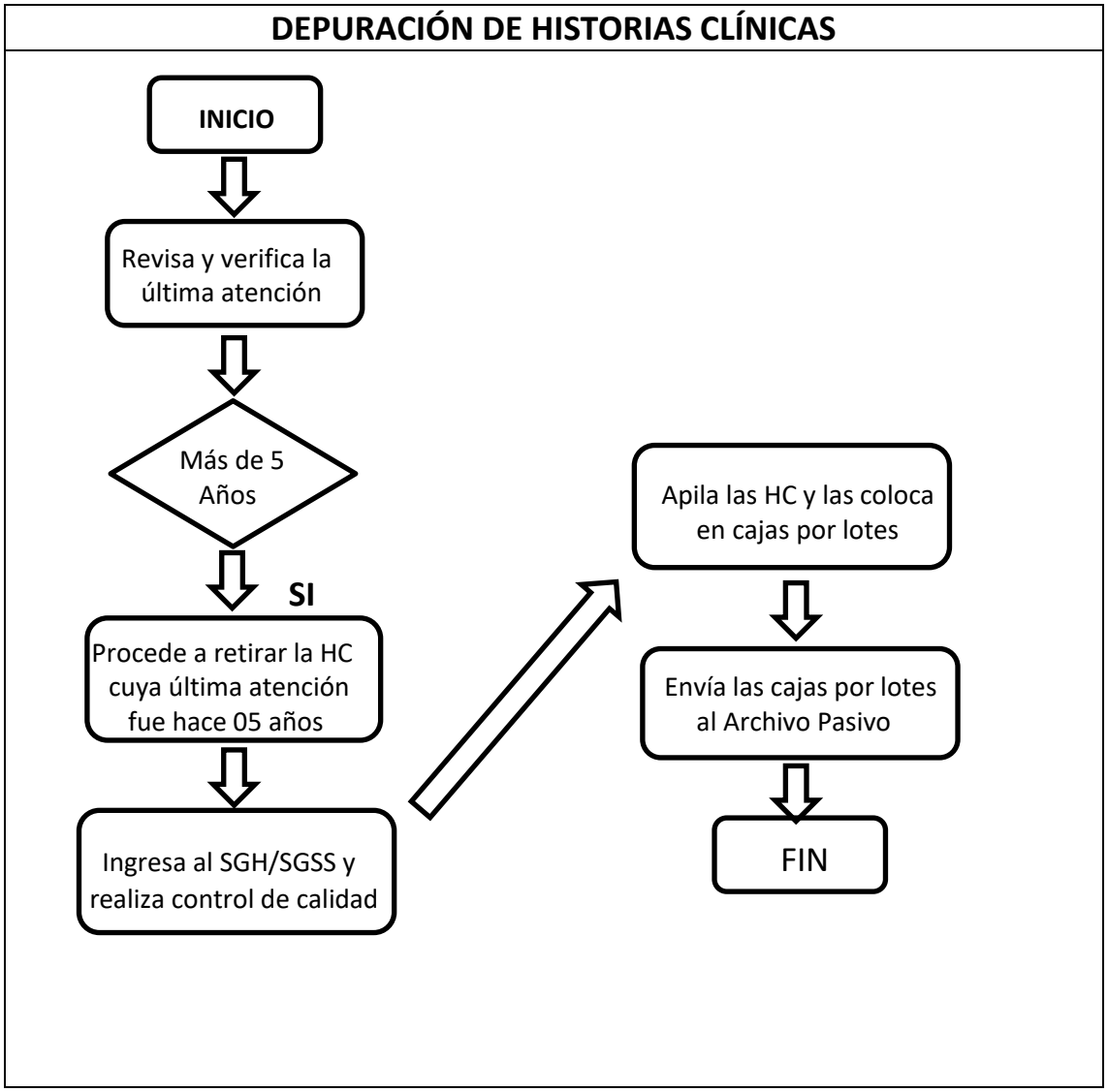
OBJETIVO:

- **Retirar las historias clínicas pasivas del archivo activo de acuerdo a las normativas y directivas vigentes.**
- **Mantener el archivo de historias clínicas de forma ordenada con espacios físicos adecuados, para realizar el trabajo diario.**

ALCANCE:
Supervisión del procedimiento por el Jefe de la Unidad Orgánica y/o Encargado funcional de Archivo e Historias Clínicas y ejecución por el personal de la Unidad de Archivo en toda la Red Asistencial.

PASO N°	DESCRIPCIÓN DEL PROCEDIMIENTO	RESPONSABLE
1	Revisa las Historias Clínicas (H.C.) y verifica la última atención dentro de los 05 años en el CAS.	Técnico Administrativo
2	Procede a retirar la Historia Clínica cuya última atención fue hace 05 años.	Técnico Administrativo
3	Registra en el Sistema de Gestión informático vigente la condición de historia pasiva.	Técnico Administrativo
4	Embalan y apilan en cajas las historias clínicas depuradas por lotes.	Técnico Administrativo
5	Envía las historias clínicas a los almacenes designadas por la Red Asistencial o nivel central.	Técnico Administrativo
6	Fin de procedimiento	

DEPURACIÓN DE HISTORIAS CLÍNICAS



VIII.7 Solicitud de Historias Clínicas

EsSalud
Seguridad Social para todos

ANEXO

Red Asistencial: .....

Centro Asistencial: .....

SOLICITUD DE HISTORIAS CLÍNICAS

FECHA | | |

SERVICIO O CONSULTORIOS | | ANEXO | |

N° DE HISTORIA CLÍNICA / CÓDIGO DE UBICACIÓN	APELLIDOS Y NOMBRES

1.-	AUDITORIA MEDICA	6.-	EVALUACIÓN MÉDICA
2.-	PACIENTES HOSPITALIZADOS	7.-	EXPEDIENTES
3.-	REUNIÓN CLÍNICA	8.-	ASESORÍA LEGAL
4.-	REGULARIZACIÓN DE CITT	9.-	SALUD OCUPACIONAL
5.-	INVESTIGACIÓN	10.-	OTROS

FIRMA Y SELLO DEL JEFE DE SERVICIO

FIRMA Y SELLO DEL SOLICITANTE

VIII.8 Encuesta Al personal de ESSALUD para medición de variable Gestión de la Historia Clínica

UNIVERSIDAD PRIVADA DEL NORTE
Gestión de la Historia Clínica y la Seguridad de la Información del Hospital II Cajamarca, ESSALUD bajo la NTP-ISO/IEC 27001:2014

FICHA DE ENTREVISTA AL PERSONAL DE ESSALUD

VARIABLE: Gestión de la Historia Clínica

Nombre y Apellidos: _____

Cargo que desempeña: _____

Años de experiencia en la institución: _____

Fecha: _____

Entrevistadores: Paul Omar Cueva Araujo – Juan Antonio Ríos Mercado

Entrevista para evaluación de la Gestión de las Historias Clínicas en el Hospital II de ESSALUD

ITEMS

Técnicos Administrativas

ITEM	SI	NO	NO APLICA
Técnicos Administrativas			
1. ¿Se verifica que al momento de crear la historia clínica sea única en la institución?			
2. ¿Se crea una historia física al crear la Historia Clínica en el Sistema de Gestión Hospitalaria?			
3. ¿Toda documentación en la atención médica que se genera tiene el DNI como identificación?			
4. ¿A los neonatos con patología se le crea una Historia Clínica propia?			
5. ¿A los neonatos nacidos normales o natimuertos se le archiva en la Historia Clínica de la madre?			
6. ¿Se conserva en forma íntegra, garantizando el orden cronológico y todos los formatos de la atención de salud?			
7. ¿El archivo de historias clínicas está diferenciado en activos y pasivos?			
8. ¿Se cuenta con un ambiente separado para las Historias Clínicas especiales con contenido potencial de implicancia médico legal?			
9. ¿Cuenta con medidas de seguridad este archivo especial de Historias Clínicas con implicancia médico legal?			
10. ¿Se ha gestionado los recursos humanos, físicos y apoyo logístico de forma continua para la conservación de la documentación?			
11. ¿Se encuentra establecido quien es el responsable de la custodia de las HC físicas en el archivo?			
12. ¿Se encuentra establecido quien es el responsable de la custodia de las HC físicas en caso de salir del archivo?			
13. ¿Se encuentra actualizado los datos el sistema informático para el registro, control y monitoreo de la Historia Clínica, para el seguimiento y ubicación?			
14. ¿Se atienden las copias de solicitudes de las Historias Clínicas solicitadas por los pacientes o por mandato judicial?			

1

Elaborado por Paul Omar Cueva Araujo – Juan Antonio Ríos Mercado

UNIVERSIDAD PRIVADA DEL NORTE
Gestión de la Historia Clínica y la Seguridad de la Información del Hospital II Cajamarca, ESSALUD bajo la NTP-ISO/IEC 27001:2014

ITEM	SI	NO	NO APLICA
15. ¿En el servicio de Hospitalización la enfermera de cada servicio donde está en paciente es responsable de la Historia Clínica?			
16. ¿En el servicio de Hospitalización la enfermera entrega la historia clínica completa y ordenada al archivo dentro de las 48 horas siguientes al momento del alta?			
17. ¿La historia de los pacientes fallecidos son entregados al área de Epidemiología?			
18. ¿El área de Epidemiología entrega la historia clínica al archivo dentro de las 72 horas de su recepción?			
19. ¿Las historias clínicas usadas en la Consulta Externa son devueltas el mismo día?			
20. ¿Las historias clínicas usadas en la Hospitalización o Emergencia son devueltas el las 48 horas de la alta del paciente?			
21. ¿Las historias clínicas usadas para informes médicos o auditorias médicas son devueltas en un plazo menor a 72 horas?			
22. ¿El archivo de historias cuenta con un Plan de Fumigaciones al menos trimestralmente?			
23. ¿Cuenta con ventilación adecuada, ventiladores, aire acondicionado, extractores e inyectores de aire, deshumedecedores el archivo de historias físicas?			
24. ¿La historia clínica se encuentra protegida mediante fólderes?			
25. ¿Las historias clínicas depuradas se encuentran almacenadas en cajas de cartón o según normatividad vigente?			
26. ¿El área de archivo cuenta con señalización?			
27. ¿El área de archivo cuenta con sistemas contraincendios, extintores y detectores de humo?			
28. ¿El área de archivo cuenta con sistema de videocámaras?			
29. ¿El área de archivo cuenta con sala de trabajo, sala de lectura y cuentan con videocámara?			
30. ¿Se realiza el proceso de depuración anual de las HC de archivo?			
31. ¿El archivo activo cuenta con información de historias clínicas con su última atención menor a cinco años?			
32. ¿Se realiza la destrucción total de las historias clínicas del archivo pasivo mayores a 10 años y que sólo cuenten con atenciones de consulta externa?			
33. ¿Se realiza la destrucción selectiva de las historias clínicas del archivo pasivo mayores a 10 años y que contienen atenciones de hospitalización?			
En caso de contar con un Comité de Auditoría de Historias Clínicas			
34. ¿Se informa al Comité de Historias Clínicas con acta de la destrucción total y selectiva de las historias clínicas mayores a 10 años del archivo pasivo?			

2

Elaborado por Paul Omar Cueva Araujo – Juan Antonio Ríos Mercado

Gestión de la Historia Clínica y la Seguridad de la Información del Hospital II Cajamarca, ESSALUD bajo la NTP-ISO/IEC 27001:2014

35. ¿El Comité de Auditoría de Historias Clínicas informa los hallazgos encontrados?			
36. ¿Cuenta con un Sistema de Historia Clínica informatizada?			
En caso de contar con un Sistema de Historia Clínica Informatizada			
37. ¿Se hacen auditorias regulares al Sistema de Historia Clínica Informatizada?			
38. ¿Cuenta con un servidor apropiado para almacenar las HC electrónicas?			
39. ¿Se cuenta con copias de seguridad diarias de las HC?			
40. ¿Se cuenta con seguridad el acceso a los Servidores de las HC?			
41. ¿Se cuenta con señalización el Centro de Cómputo de la Red Asistencial Cajamarca?			
42. ¿Se cuenta con sistemas contra incendios, extintores y detectores de humo?			
Otros			
43. ¿Cuenta con el Plan de continuidad del Negocio?			
44. ¿Realiza las pruebas del Plan de Continuidad del Negocio?			
Técnicos Asistenciales			
45. ¿Se tiene la reserva de la información relacionada con el acto médico y su historia clínica?			
46. ¿El registro por parte de los profesionales de la salud contiene las prácticas y procedimientos aplicados al paciente?			
ITEM	SI	NO	NO APLICA
47. ¿Todas las atenciones médicas y no médicas cuentan con acto médico?			
48. ¿Cada atención tienen registrado el código CIE-10?			
49. ¿Todas las atenciones tienen la firma y sello del profesional asistencial?			
50. ¿Cuenta con un Comité de Auditoría de Historias Clínicas?			

De acuerdo con su experiencia que aspectos son los que considera se deberían mejorar en torno al proceso de Gestión de las Historias Clínicas en el Hospital II de ESSALUD Cajamarca.

_____

_____

_____

_____

Gestión de la Historia Clínica y la Seguridad de la Información del Hospital II Cajamarca, ESSALUD bajo la NTP-ISO/IEC 27001:2014

¿Considera que la seguridad de las Historias Clínicas es adecuada? Comente su respuesta.

Conoce algún caso en el que se haya sido expuesta la información de las Historias Clínicas a personal no autorizado.

VIII.9 Encuesta Al personal de ESSALUD para medición de variable Seguridad de la Información

UNIVERSIDAD PRIVADA DEL NORTE
Gestión de la Historia Clínica y la Seguridad de la Información del Hospital II Cajamarca, ESSALUD bajo la NTP-ISO/IEC 27001:2014

FICHA DE ENTREVISTA AL PERSONAL DE ESSALUD

VARIABLE: Seguridad de la Información

Nombre y Apellidos: _____

Cargo que desempeña: _____

Años de experiencia en la institución: _____

Fecha: _____

Entrevistadores: Paul Omar Cueva Araujo – Juan Antonio Ríos Mercado

Entrevista para evaluación de la Seguridad de la Información ligada a los procesos de Gestión de las Historias Clínicas en el Hospital II Cajamarca - EsSalud

POLÍTICA DE SEGURIDAD

	ITEM	SI	PARCIAL	NO	NO APLICA
	Política de seguridad de la información				
1.	¿Ha sido aprobado por la dirección un documento que contenga la política de seguridad de la información, y ha sido publicado y comunicado a todos los empleados y terceras partes relevantes?				
2.	¿La política de seguridad de la información se revisa en intervalos planificados, o si ocurren cambios significativos, para asegurar que sigue siendo conveniente, suficiente y efectiva?				

ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

	ITEM	SI	PARCIAL	NO	NO APLICA
	Organización Interna				
1.	¿Se han definido y asignado claramente todas las responsabilidades de seguridad de la información?				
2.	¿Se tienen adecuadamente separados los deberes y áreas, minimizando las oportunidades de mal uso de los activos de información?				
3.	¿Se mantiene una relación apropiada con las autoridades relevantes (p.e. Policía, Bomberos)?				
4.	¿La organización mantiene contacto con grupos de interés, foros de especialistas en seguridad o en asociaciones profesionales?				
5.	¿Se incluyen y conducen aspectos de seguridad de información en la gestión de proyectos, de acuerdo al tipo de proyecto?				
	Dispositivos Móviles y Teletrabajo				
6.	¿Existe una política formal y se han adoptado las medidas de seguridad necesarias para protegerse en contra de los riesgos de utilizar computadores móviles e infraestructura de comunicaciones?				
7.	¿Se ha desarrollado una política, unos planes operativos, y unos				

1 Elaborado por Paul Omar Cueva Araujo – Juan Antonio Ríos Mercado

Gestión de la Historia Clínica y la Seguridad de la Información del Hospital II Cajamarca, ESSALUD bajo la NTP-ISO/IEC 27001:2014

procedimientos para regular las actividades del teletrabajo?				
8. ¿Los acuerdos con terceros relacionados con acceso, procesamiento, comunicación o manejo de la información o infraestructura para el procesamiento de información, o adición de productos o servicios a la infraestructura para el procesamiento de la información, cubren todos los requerimientos de seguridad relevantes?				

SEGURIDAD DE LOS RECURSOS HUMANOS

ITEM	SI	PARCIAL	NO	NO APLICA
Previo al empleo				
9. ¿Se realizan las verificaciones oportunas de los antecedentes de todos los candidatos para un empleo, de los contratistas y terceras partes, siempre de acuerdo a las leyes y regulaciones vigentes, la ética y siempre de manera proporcional a los requerimientos del negocio, la clasificación de la información a la que accederá y los riesgos percibidos?				
10. ¿Se les exige a los empleados, contratistas y terceras partes estar de acuerdo y firmar los términos y condiciones de su contrato de empleo, y este contrato establece las responsabilidades tanto del empleado como las de la organización, en materia de seguridad de la información?				
Durante el empleo				
11. ¿La dirección exige a los empleados, contratistas y terceras partes aplicar seguridad de acuerdo con las políticas y procedimientos establecidos por la organización? 12. ¿Los empleados y, cuando es relevante, contratistas y terceras partes, reciben el entrenamiento adecuado sobre concientización en seguridad de la información y se les mantiene actualizados sobre las políticas y procedimientos de la organización que son relevantes para el cumplimiento de las funciones de su trabajo?				
13. ¿Existe algún proceso disciplinario formal para tratar con los empleados que infringen la seguridad de la organización?				
Finalización o cambio de empleo				
14. ¿Han sido claramente definidas y asignadas las responsabilidades para realizar la finalización de un contrato de trabajo o cambios en el empleo?				

UNIVERSIDAD PRIVADA DEL NORTE
Gestión de la Historia Clínica y la Seguridad de la Información del Hospital II Cajamarca, ESSALUD bajo la NTP-ISO/IEC 27001:2014

GESTION DE ACTIVOS

	ITEM	SI	PARCIAL	NO	NO APLICA
	Responsabilidad de los activos				
1.	¿Todos los activos están identificados de forma clara, y se ha elaborado y mantenido un inventario de todos los activos importantes?				
2.	¿Toda la información y activos asociados con la infraestructura para el procesamiento de la información, han sido asignados a un área específica de la organización?				
3.	¿Las reglas para el uso correcto de la información y de los activos asociados a la infraestructura para el procesamiento de la información, han sido identificadas, documentadas e implementadas?				
4.	¿Se requiere que todos los empleados, contratistas y usuarios de terceras partes, devuelvan todos los activos de la organización que se encuentren en su posesión en el momento de la terminación del empleo, contrato o acuerdo?				
	Clasificación de la Información				
5.	¿Se ha clasificado la información con base en su valor, requerimientos legales vigentes, sensibilidad y que tan crítica es para la organización?				
6.	¿Existen adecuados procedimientos de etiquetamiento de la información de acuerdo al esquema de clasificación de la organización?				
7.	¿Se ha desarrollado e implantado un conjunto de procedimientos apropiado para el etiquetado y manejo de la información, de acuerdo con el esquema de clasificación adoptado por la organización?				
	Manejo de medios				
8.	¿Existen procedimientos para la administración de los medios removibles?				
9.	¿Se revisan todos los medios, para asegurarse que ningún tipo de dato sensible o software licenciado haya sido eliminado o sobrescrito con seguridad antes del desecho o reutilización del medio?				
10.	¿Los medios que contienen información, están protegidos en contra del acceso no autorizado, el mal uso o su alteración durante el transporte más allá de los límites físicos de la organización?				

CONTROL DE ACCESO

	ITEM	SI	PARCIAL	NO	NO APLICA
	Requerimientos de negocio para el control del acceso				
1.	¿Se ha establecido y documentado una política de control de acceso con base en los requisitos de seguridad y del negocio, y ésta política ha sido ha sido revisada de forma regular?				
2.	¿Los usuarios tienen acceso exclusivamente a los servicios a los que se les ha autorizado específicamente?				

Gestión de la Historia Clínica y la Seguridad de la Información del Hospital II Cajamarca, ESSALUD bajo la NTP-ISO/IEC 27001:2014

	Gestión de accesos de usuarios				
3.	¿Existe un procedimiento formal de registro y de salida del registro para los usuarios de la organización con el fin de garantizar o revocar el acceso a todos los sistemas de información y servicios?				
4.	¿Se restringe y controla la asignación y retiro accesos?				
5.	¿Se restringe y controla la asignación y uso de accesos privilegiados?				
6.	¿Existen procesos formales de gestión y control de la información de autenticación asignada?				
7.	¿Los derechos de acceso de los usuarios, se revisan en intervalos regulares de tiempo siguiendo un proceso formal?				
8.	¿Una vez se termina el contrato, se retiran inmediatamente todos los derechos de acceso a la información y a la infraestructura para el procesamiento de la información de los empleados, contratistas y terceras partes, o si fuese el caso, se ajustan si hay cambios?				
	Responsabilidades de usuario				
9.	¿Se requiere que los usuarios sigan buenas prácticas de seguridad en la selección y el uso de información secreta de autenticación?				
	Control de acceso a la información y las aplicaciones				
10.	¿El acceso a las funciones del sistema de información y aplicación, es restringido para los usuarios y personal de soporte, de acuerdo con la política de control de acceso?				
11.	¿El acceso a los sistemas operativos está controlado por un procedimiento de inicio de sesión seguro?				
12.	¿Los sistemas de gestión de contraseñas son interactivos y aseguran igualmente la calidad de las contraseñas?				
13.	¿El uso de programas de usuario capaces de modificar el sistema y los controles de las aplicaciones, está restringido y fuertemente controlado?				
14.	¿Está restringido el acceso al código fuente de los programas?				

CRIPTOGRAFÍA

	ITEM	SI	PARCIAL	NO	NO APLICA
	Controles criptográficos				
1.	¿Se ha desarrollado e implementada una política sobre el uso de controles criptográficos para la protección de la información?				
2.	¿Se encuentra implantada una gestión de claves para soportar el uso de técnicas criptográficas por parte de la organización?				

UNIVERSIDAD PRIVADA DEL NORTE
Gestión de la Historia Clínica y la Seguridad de la Información del Hospital II Cajamarca, ESSALUD bajo la NTP-ISO/IEC 27001:2014

SEGURIDAD FÍSICA Y AMBIENTAL

	ITEM	SI	PARCIAL	NO	NO APLICA
	Áreas seguras				
1.	¿Se utilizan perímetros de seguridad (barreras como: paredes, puertas de acceso controladas por tarjetas de identidad, puestos de recepción, etc.) para proteger áreas que contengan información e infraestructura para el procesamiento de la información?				
2.	¿Están protegidas las áreas seguras por los controles de entrada apropiados para asegurarse de que solamente permiten el acceso de personal autorizado?				
3.	¿Se ha diseñado e implantado un sistema de seguridad física para las oficinas, salas y resto de instalaciones?				
4.	¿Se ha sido diseñado y aplicado un sistema de protección física en contra de daños causados por incendios, inundaciones, terremotos, explosiones, ataques provocados por personas y/o otras formas de desastre natural o artificial?				
5.	¿Se han diseñado y aplicado las guías y medidas de protección adecuadas para trabajar en las áreas seguras?				
6.	¿Los puntos de acceso, tales como áreas de entrega y/o carga, y otros puntos donde personas no autorizadas puedan tener acceso, son controlados y, si es posible, aislados de las instalaciones para el procesamiento de la información, con el fin de evitar accesos no autorizados?				
	Equipamiento				
7.	¿Los equipos están aislados o protegidos con la finalidad de reducir el riesgo de daños, amenazas y accesos no autorizados?				
8.	¿Los equipos se encuentran protegidos ante los posibles fallos de electricidad y otras perturbaciones causadas por los fallos en los sistemas de soporte (UPS, Planta eléctrica)?				
9.	¿El cableado eléctrico y el de telecomunicaciones, que transmiten datos o soportan servicios de información, están protegidos contra la intercepción o daño?				
10.	¿Se hace un mantenimiento correcto de los equipos para asegurar su continua disponibilidad e integridad?				
11.	¿Se requiere autorización previa para sacar de la organización equipos, información o software?				
12.	¿Se aplica la seguridad adecuada los equipos que se encuentran fuera de las áreas pertenecientes a la organización, considerando los riesgos que implica trabajar fuera de las instalaciones de la organización?				
13.	¿Se revisan todos los equipos que tengan capacidad de almacenamiento, para asegurarse que ningún tipo de dato sensible y/o software licenciado haya sido eliminado o sobrescrito con seguridad antes del desecho o reutilización del equipo?				
14.	¿Se requiere que los usuarios se aseguren que los equipos desatendidos tengan la protección adecuada?				
15.	¿Se ha adoptado una política de "escritorio despejado" para los				

5 Elaborado por Paul Omar Cueva Araujo – Juan Antonio Ríos Mercado

Gestión de la Historia Clínica y la Seguridad de la Información del Hospital II Cajamarca, ESSALUD bajo la NTP-ISO/IEC 27001:2014

	papeles, medios de almacenamiento removibles y una política de "pantalla limpia" en la infraestructura para el procesamiento de información?				

SEGURIDAD DE LAS OPERACIONES

	ITEM	SI	PARCIAL	NO	NO APLICA
	Responsabilidad y procedimientos operacionales				
1.	¿Los procedimientos operativos están documentados, mantenidos y puestos a disposición de todos los usuarios que los necesitan?				
2.	¿Se controlan los cambios a la infraestructura para el tratamiento de la información y los sistemas?				
3.	¿El uso de recursos es monitoreado, afinado y se realizan proyecciones de futuros requisitos de capacidad para asegurar el rendimiento del sistema?				
4.	¿Las instalaciones de desarrollo, producción y pruebas están separadas para reducir los riesgos de accesos o cambios en los sistemas operativos no autorizados?				
	Protección contra código malicioso				
5.	¿Se han implementado controles de detección, prevención y recuperación para protegerse de código malicioso, así como procedimientos apropiados para la concientización de los usuarios sobre éste?				
	Copias de respaldo				
6.	¿Se realizan las copias de seguridad y se comprueban regularmente conforme a lo establecido en la política acordada?				
	Registro y monitoreo				
7.	¿Los logs de auditoría registran y mantienen las actividades de los usuarios, las excepciones y los eventos de seguridad de la información, durante un periodo de tiempo acordado, con el fin de ser utilizados en investigaciones futuras y monitorear el control de acceso?				
8.	¿La infraestructura para los registros y la información de estos registros, son protegidos en contra de acceso forzoso o no autorizado?				
9.	¿Las actividades del administrador y del operador del sistema, son registradas?				
10.	¿Se encuentran sincronizados todos los relojes de todos los sistemas relevantes de procesamiento de información en la organización o contenidos en el dominio de seguridad, conforme a una fuente de tiempo de confianza?				
	Control de software operacional				
11.	¿Existen procedimientos para el control de la instalación de software sobre sistemas operacionales?				

Gestión de la Historia Clínica y la Seguridad de la Información del Hospital II Cajamarca, ESSALUD bajo la NTP-ISO/IEC 27001:2014

	Gestión de vulnerabilidades técnicas				
12.	¿Se obtiene oportunamente información sobre las vulnerabilidades técnicas de los sistemas de información que están en uso, la exposición a dichas vulnerabilidades es evaluada y se toman las medidas oportunas para tratar el riesgo asociado?				
13.	¿Se establecieron e implementaron reglas para la instalación de software por parte de los usuarios?				
	Consideraciones de auditoria de sistemas de información				
14.	¿Los requerimientos y las actividades de auditoría sobre los sistemas operativos, que involucran revisiones, son cuidadosamente planeados y acordados para minimizar el riesgo de perturbar los procesos del negocio?				

SEGURIDAD DE LAS COMUNICACIONES

	ITEM	SI	PARCIAL	NO	NO APLICA
	Controles en la red				
1.	¿La red está adecuadamente administrada y controlada, con el fin de protegerla de las amenazas y mantener la seguridad de los sistemas y aplicaciones que usa la red, incluida la información en tránsito?				
2.	¿Las características de seguridad, los niveles de servicio, y los requerimientos de administración de todos los servicios de red, están identificados e incluidos en los acuerdos con los diferentes proveedores de servicios de red, bien sean internos o externos?				
3.	¿Los controles para segregar grupos de dispositivos de información, usuarios y sistemas de información son adecuados?				
	Transferencia de información				
4.	¿Hay establecida una política formal de intercambio, procedimientos y controles para proteger el intercambio de información a través de los servicios de comunicación?				
5.	¿Se han establecido acuerdos para el intercambio de información y software dentro de la organización y con organizaciones externas?				
6.	¿Está adecuadamente protegida la información involucrada en la mensajería electrónica?				
7.	¿Los acuerdos de confidencialidad y no revelación reflejan las necesidades de la organización, se documentan y revisan?				

UNIVERSIDAD PRIVADA DEL NORTE
Gestión de la Historia Clínica y la Seguridad de la Información del Hospital II Cajamarca, ESSALUD bajo la NTP-ISO/IEC 27001:2014

ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

	ITEM	SI	PARCIAL	NO	NO APLICA
	Requerimientos de seguridad de los sistemas de información				
1.	¿Las declaraciones de los requerimientos del negocio para nuevos sistemas de información o para la mejora de los ya existentes, especifican los requerimientos de los controles de seguridad?				
2.	¿La información disponible a través de un sistema público, se encuentra protegida para asegurar su integridad y prevenir modificaciones no autorizadas?				
3.	¿La información involucrada en transacciones on-line, está protegida para prevenir transmisiones incompletas, desvío, modificación no autorizada del mensaje, divulgación no autorizada y para evitar la duplicación o reproducción?				
	Seguridad en el desarrollo y soporte de procesos				
4.	¿Existen reglas de seguridad para el desarrollo de software?				
5.	¿Se utilizan procedimientos de control de cambios formales para controlar la implementación de cambios?				
6.	¿Cuándo los sistemas operativos son cambiados, todas las aplicaciones críticas del negocio son revisadas y comprobadas para asegurar que no haya un impacto adverso en las operaciones y/o la seguridad de la organización?				
7.	¿Las modificaciones de los paquetes de software, son desalentadas, limitadas a los cambios necesarios y todos los cambios son estrictamente controlados?				
8.	¿Se han establecido, documentados, mantenidos y aplicados principios de ingeniería de sistemas segura?				
9.	¿El ambiente de desarrollo está adecuadamente protegido durante el ciclo completo de codificación?				
10.	¿El desarrollo de software realizado en outsourcing, está siendo supervisado y monitoreado por la organización?				
11.	¿Se prueban las funcionalidades de seguridad durante el desarrollo?				
12.	¿Se programan pruebas de aceptación para sistemas nuevos o actualizados?				
	Datos de prueba				
13.	¿Los datos de prueba del sistema están seleccionados cuidadosamente, protegidos y controlados?				

Gestión de la Historia Clínica y la Seguridad de la Información del Hospital II Cajamarca, ESSALUD bajo la NTP-ISO/IEC 27001:2014

RELACIONES CON PROVEEDORES

	ITEM	SI	PARCIAL	NO	NO APLICA
	Seguridad de información en relaciones con el proveedor				
1.	¿Los requerimientos de seguridad de información para mitigar los accesos de proveedores a recursos de la organización están acordados y documentados?				
2.	¿Todos los requerimientos relevantes de seguridad de información están establecidos y acordados con cada proveedor que usa componentes de la infraestructura de TI?				
3.	¿Los acuerdos con proveedores incluyen requerimientos para gestionar los riesgos de seguridad en la cadena del suministro del servicio o producto?				
	Gestión de servicios por terceras partes				
4.	¿Los servicios, informes y registros proporcionados por terceras partes, se monitorizan y revisan de forma regular, y se llevan a cabo auditorias de forma regular?				
5.	¿Se gestionan los cambios de provisión de los servicios (incluyendo el mantenimiento y mejora de las políticas existentes, procedimientos y controles de seguridad de la información) tomando en cuenta la criticidad de los sistemas y procesos del negocio implicados y la reevaluación del riesgo?				

GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

	ITEM	SI	PARCIAL	NO	NO APLICA
	Informes de los eventos de seguridad de la información y vulnerabilidades				
1.	¿Se encuentran establecidos las responsabilidades y los procedimientos necesarios para establecer una respuesta rápida, efectiva y ordenada cuando se presentan incidentes de seguridad de la información?				
2.	¿Los eventos de seguridad de la información están siendo reportados a los canales de gestión adecuados tan pronto como sea posible?				
3.	¿Se requiere que los empleados contratistas y terceras partes, usuarios de sistemas de información, tomen nota y denuncien cualquier vulnerabilidad de seguridad en los sistemas o en los servicios, que observen o sospechen?				
4.	¿Los eventos de seguridad de información son evaluados para ver si son clasificados como incidentes?				
5.	¿La respuesta a los incidentes de seguridad está de acuerdo a los procedimientos documentados?				
6.	¿Existen mecanismos para establecer los tipos, volúmenes y costos referidos a incidentes de seguridad de la información, que deban ser cuantificados y monitorizados?				

Gestión de la Historia Clínica y la Seguridad de la Información del Hospital II Cajamarca, ESSALUD bajo la NTP-ISO/IEC 27001:2014

7.	Cuando se presenta una acción de seguimiento en contra de una persona u organización después que un incidente de seguridad de la información implica una acción legal (ya sea criminal o civil): ¿La evidencia, es recogida, retenida y presentada conforme a las reglas para la evidencia colocada en la jurisdicción relevante?				

ASPECTOS DE SEGURIDAD DE INFORMACIÓN EN LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO

	ITEM	SI	PARCIAL	NO	NO APLICA
	Gestión de los aspectos de seguridad de la continuidad del negocio				
1.	¿Se ha desarrollado y mantenido un proceso de gestión para la continuidad del negocio de toda la organización que trate los requerimientos de seguridad de la información que se necesitan para la continuidad del negocio de la organización?				
2.	¿Se han identificados todos los eventos que pueden causar interrupciones a los procesos de negocio, junto con la probabilidad y el impacto de dichas interrupciones, y sus consecuencias para la seguridad de la información?				
3.	¿Los planes de continuidad de negocio son probados y modificados para asegurar que son efectivos y se encuentran al día?				
	Redundancias				
4.	¿Las instalaciones para el procesamiento de datos cuentan con la suficiente redundancia para cumplir con los requerimientos de disponibilidad?				

CUMPLIMIENTO

	ITEM	SI	PARCIAL	NO	NO APLICA
	Cumplimiento de los requerimientos legales				
1.	¿Todos los requerimientos estatutarios, regulatorios y contractuales, y el enfoque de la organización para cumplir con estos requerimientos, se encuentran explícitamente definidos, documentados y mantenidos al día para cada uno de los sistemas de información y para la organización?				
2.	¿Se han implementado los procedimientos apropiados para asegurar el cumplimiento de los requerimientos legales, regulatorios y contractuales respecto al uso de materiales que pudieran estar protegidos por los derechos de propiedad intelectual, e igualmente respecto al uso de productos software propietario?				
3.	¿Los registros importantes están protegidos de pérdida, destrucción y falsificación, de acuerdo con los requerimientos				

Gestión de la Historia Clínica y la Seguridad de la Información del Hospital II Cajamarca, ESSALUD bajo la NTP-ISO/IEC 27001:2014

	estatutarios, regulatorios, contractuales y del negocio?				
4.	¿Se están aplicando controles para asegurar la protección y la privacidad de los datos, tal y como se requiere por la legislación, regulaciones aplicables y, si fuera el caso, cláusulas contractuales?				
5.	¿Se están utilizando controles criptográficos de acuerdo con las leyes, regulaciones y acuerdos relevantes?				
	Revisiones a la seguridad de información				
6.	¿Los requerimientos y las actividades de auditoría sobre los sistemas operativos, que involucran revisiones, son cuidadosamente planeados y acordados para minimizar el riesgo de perturbar los procesos del negocio?				
7.	¿Los directivos se aseguran que todos los procedimientos de seguridad dentro de su área de responsabilidad, se realizan correctamente para asegurar el cumplimiento con los estándares y políticas de seguridad de la organización?				
8.	¿Los sistemas de información son revisados regularmente en cumplimiento de los estándares de implementación de la seguridad?				

VIII.10 Análisis de riesgos informáticos

Para la correcta evaluación de la seguridad de la información del Hospital II EsSalud Cajamarca correspondiente al proceso de Gestión de Historias Clínicas, se aplicó la metodología Magerit 3.0 para el Análisis y Gestión de Riesgos Informáticos.

Para el análisis de Riesgos se parte de la identificación de los activos de información para luego realizar la valora del impacto, probabilidad y riesgo por medio de escalas cualitativas.

Tabla 64

Escalas de Impacto, Probabilidad y Riesgo

Escalas		
Impacto	Probabilidad	Riesgo
MA: muy alto	MA: casi seguro	MA: crítico
A: alto	A: Muy alto	A: importante (grave)
M: medio	M: posible	M: apreciable
B: bajo	B: poco probable	B: bajo
MB: muy bajo	MB: muy raro	MB: despreciable

Nota. Escalas de impacto. Adaptado de la Metodología Magerit 3.0

Donde se combinan impacto con frecuencia en una tabla para el cálculo de riesgo:

Riesgo		**Probabilidad**[1]				
		MB	B	M	A	MA
Impacto[2]	MA	B	M	MA	MA	MA
	A	B	A	A	MA	MA
	M	MB	B	M	A	MA
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Figura 25. Matriz de Valoración Cualitativa de Riesgos (probabilidad e impacto) Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, (2012)

[1] Cuán probable o improbable es que se materialice la amenaza
[2] Medida del daño sobre el activo derivado de la materialización de una amenaza.

Riesgo		Probabilidad				
		MB	B	M	A	MA
Impacto	MA	5	10	15	20	25
	A	4	8	12	16	20
	M	3	6	9	12	15
	B	2	4	6	8	10
	MB	1	2	3	4	5

Figura 26. Matriz de Valoración Cuantitativa de Riesgos (Probabilidad e Impacto) Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, (2012)

Activos de Tecnología de Información

Siguiendo los pasos de la metodología MAGERIT a continuación se presentan los activos de información que están ligados a la gestión de las Historias Clínicas según la clasificación que la metodología sugiere.

- [D] Datos/Información
- [S] Servicios
- [SW] Software - Aplicaciones informáticas
- [HW] Equipamiento informático
- [COM] Redes de comunicaciones
- [Media] Soportes de información
- [AUX] Equipamiento auxiliar
- [L] Instalaciones
- [P] Personal

.

INFORMACIÓN DEL ACTIVO					Valoración del Activo de Información (1 - 5)					Ubicación				Propiedad		Clasificación de la Información		
Nº	Clase	Código	Activo de Información	Descripción	Confidencialidad	Integridad	Disponibilidad	TOTAL		Física	Electrónica	Otro		Propietario		Confidencialidad	Integridad	Disponibilidad
1	Datos Información	D001	Historias Clínicas Físicas	Documento físico de registro único y válido desde el punto de vista clínico y legal	5	5	4	5		x				Unidad de Admisión, Archivo y Referencias		Crítica	Crítica	Crítica
2	Datos Información	D002	Copias de seguridad – Backup	Copia de datos para proteger los originales ante fallas o pérdidas.	5	5	4	5		x				Unidad de Soporte Informático		Crítica	Crítica	Crítica
3	Datos Información	D003	Inventario de Aplicativos	Registro de los aplicativos existentes en la institución.	5	3	3	4			x			Unidad de Soporte Informático		Crítica	No crítica	No Crítica
4	Software - Aplicaciones informáticas	SW001	Sistema Operativo Cliente	Programa de software que hace que el hardware de la computadora interactúe con el software para realizar varias acciones asignadas	2	4	2	3			x			Diferentes áreas		No Crítica	Crítica	No Crítica

5	Software - Aplicaciones informáticas	SW002	Sistema Operativo Servidores	Programa de software especializado para equipos servidores que hace que el hardware de la computadora interactúe con el software para realizar varias acciones asignadas	3	4	4	4			x			Unidad de Soporte Informático		No Crítica	Crítica	Crítica
6	Software - Aplicaciones informáticas	SW003	Software Antivirus	Programa informático que ha sido diseñado como medida de protección y seguridad para resguardar los datos y el funcionamiento de sistemas informáticos de la institución.	4	4	4	4			x			Unidad de Soporte Informático		Crítica	Crítica	Crítica
7	Software - Aplicaciones informáticas	SW004	Software de Ofimática	Conjunto de programas informáticos que son de uso habitual en las oficinas, incluye al menos procesador de texto, hoja de cálculo y administrador de presentaciones o diapositivas.	3	3	3	3			x			Unidad de Soporte Informático		No Crítica	No crítica	No Crítica
8	Software - Aplicaciones informáticas	SW005	Sistema de Gestión Hospitalaria	Programa Informático diseñado por la institución para llevar el registro de las incidencias médicas de los pacientes	5	5	5	5			x			Unidad de Soporte Informático		Crítica	Crítica	Crítica

9	Equipamiento informático	HW001	Servidor Sistema de Gestión Hospitalaria.	Equipo informático conectado a la red el cuál provee servicios a otros computadores denominados clientes. Computadora física en la cual se encuentra instalado el Sistema de Gestión Hospitalaria	5	5	5	5		x				Unidad de Soporte Informático		Crítica	Crítica	Crítica
10	Equipamiento informático	HW002	PC's	Equipo de cómputo diseñado para ser usado en una ubicación fija, como un escritorio.	4	4	4	4		x				Usado en diferentes áreas		Crítica	Crítica	Crítica
11	Equipamiento informático	HW003	Laptop	Equipo de cómputo que permite la movilidad del equipo.	4	4	4	4		x				Usado en diferentes áreas		Crítica	Crítica	Crítica
12	Equipamiento informático	HW004	Servidor Central IP	Equipo informático que forma parte de una red y provee el servicio de telefonía a través del protocolo IP.	4	4	5	4		x				Unidad de Soporte Informático		Crítica	Crítica	Crítica
13	Equipamiento informático	HW005	Central Telefónica	Equipo informático conectado a la red el cual permite la conexión hacia el servicio de telefonía.	4	4	4	4		x				Unidad de Soporte Informático		Crítica	Crítica	Crítica
14	Equipamiento informático	HW006	Servidor de Aplicaciones	Equipo informático conectado a la red el cuál provee servicios a otros computadores denominados clientes. Computadora física en la cual se encuentra instaladadas algunas de las aplicaciones informáticas de uso de EsSalud	4	5	4	5		x				Unidad de Soporte Informático		Crítica	Crítica	Crítica

15	Redes de comunicaciones	COM001	Equipos de Comunicaciones	Equipo Hardware que permite establecer las comunicaciones entre el local de la administración y el resto de locales	4	4	5	4		x				Unidad de Soporte Informático		Crítica	Crítica	Crítica
16	Redes de comunicaciones	COM002	Switch Core	Equipo central de distribusión de las comunicaciones de voz y datos	5	5	5	5		x				Unidad de Soporte Informático		Crítica	Crítica	Crítica
17	Redes de comunicaciones	COM003	Switches de Borde	Equipo secundario de distribusión de las comunicaciones de voz y datos	4	4	5	4		x				Unidad de Soporte Informático		Crítica	Crítica	Crítica
18	Redes de comunicaciones	COM004	Servicio de Internet	Servicio brindado por un ISP para que la institución pueda acceder a Internet	3	3	4	3		x				ISP		No Crítica	No crítica	Crítica
19	Redes de comunicaciones	COM005	Router de Internet	Equipo de red cuya finalidad es conectar la red de la institución al servicio de Internet	3	3	4	3		x				ISP		No Crítica	No crítica	Crítica
20	Redes de comunicaciones	COM006	Servicio de Telefonía	Servicio contratado con un proveedor de Servicios para poder acceder a llamadas telefónicas	3	5	4	4		x				IPS		No Crítica	Crítica	Crítica

21	Equipamiento auxiliar	AUX001	UPS para Data Center	Es un dispositivo que gracias a sus baterías almacena energía, para luego proporcionarla por un tiempo limitado a todos los dispositivos que estén conectados	4	4	4	4		x				Unidad de Soporte Informático		Crítica	Crítica	Crítica
22	Equipamiento auxiliar	AUX002	Aire Acondicionado Data Center	Dispositivos de hardware que permiten mantener una temperatura adecuada en el Data Center.	3	4	4	4		x				Unidad de Soporte Informático		No Crítica	Crítica	Crítica
23	Equipamiento auxiliar	AUX003	Extintores del archivo de Historias Clínicas	Equipo portátil para apagar fuego o incendios de pequeña magnitud.	2	4	5	4		x				Oficina de Administración		Pública	Crítica	Crítica
24	Instalaciones	L001	Archivo de Historias clínicas	Instalación en donde se encuentran ubicadas las Historias Clínicas físicas.	5	5	5	5		x				Oficina de Administración		Crítica	Crítica	Crítica
25	Instalaciones	L002	Data Center	Centro de procesamiento de datos, el cual alberga los sistemas de información del Hospital II de ESSALUD Cajamarca, incluye los equipos de telecomunicaciones y servidores con todos sus accesorios.	5	5	5	5		x				Unidad de Soporte Informático		Crítica	Crítica	Crítica
26	Instalaciones	L003	Oficinas Área de TI	Oficinas ubicadas en el local de la Administración en donde se encuentra ubicado el personal de la unidad de soporte informático.	2	2	4	3		x				Unidad de Soporte Informático		Pública	No crítica	No Crítica

27	Intangible	I001	Experiencia del personal (Gestión de la HC)	Experiencia en el uso y gestión de las Historias Clínicas del personal Asistencial y Administrativo	3	3	3	3				x		Diferentes áreas		No Crítica	No crítica	No Crítica
28	Intangible	I002	Imagen Corporativa	Forma en que es percibida la institución en el ámbito público.	4	4	4	4				x		Oficina de Administración		Crítica	Crítica	Crítica

Figura 27. Activos de Información EsSalud Cajamarca. Adaptación de metodología Magerit

Valoración de la Probabilidad, Impacto y Aceptación de Riesgo

Tabla 65

Estimación de la Probabilidad

VALOR CUALITATIVO	VALOR CUANTITATIVO	DESCRIPCIÓN
MA: casi seguro	5	La amenaza se materializa tres veces a la semana
A: Muy alto	4	La amenaza se materializa a lo sumo una vez cada semana.
M: posible	3	La amenaza se materializa a lo sumo una vez cada mes.
B: poco probable	2	La amenaza se materializa a lo sumo una vez cada año.
MB: muy raro	1	La amenaza no se ha materializado o máximo lo ha hecho una vez.

Tabla 66

Estimación del Impacto

VALOR CUALITATIVO	VALOR CUANTITATIVO	DESCRIPCIÓN
MA: muy alto	5	El daño derivado de la materialización de la amenaza tiene consecuencias muy graves para la organización.
A: alto	4	El daño derivado de la materialización de la amenaza tiene consecuencias graves para la organización.
M: medio	3	El daño derivado de la materialización de la amenaza tiene consecuencias para la organización.
B: bajo	2	El daño derivado de la materialización de la amenaza no tiene consecuencias relevantes para la organización.
MB: muy bajo	1	El daño derivado de la materialización de la amenaza es totalmente inapreciable para la organización.

Tabla 67

Criterios de Aceptación del Riesgo

RANGO	DESCRIPCIÓN
Riesgo <= 9	La organización considera el riesgo poco considerable
Riesgo > 9	La organización considera el riesgo considerable y debe proceder a su tratamiento.

Amenazas

Tabla 68

Amenazas de acuerdo a su origen

Código	Origen	Descripción
A001	Desastres naturales	Daños por agua
A002		Desastres naturales
A003	De origen industrial	Fuego
A004		Desastres industriales (contaminación química)
A005		Contaminación electromagnética (interferencia o carga electromagnética)
A006		Avería de origen físico o lógico
A007		Corte del suministro eléctrico
A008		Condiciones inadecuadas de temperatura o humedad
A009		Fallo de servicios de comunicaciones
A010		Avería de origen físico o lógico
A011	Errores y fallos no intencionados	Errores y fallos no intencionados (Introducción de información Incorrecta)
A012		Errores de los usuarios
A013		Difusión de software dañino
A014		Alteración accidental de la información (mezcla con otras Historias)

A015		Destrucción de información
A016		Fugas de información
A017		Errores de mantenimiento / actualización de programas
A018		Caída del sistema por agotamiento de recursos
A019		Pérdida de equipos
A020		Indisponibilidad del personal
A021		Deterioro por manejo y uso
A022		Corrupción de la información
A023		Degradación de los soportes de almacenamiento de la información
A024		Destrucción de información
A025		Instalación no estándar
A026		Errores de configuración
A027		Falta de pago
A028		Caída de los servicios del Proveedor
A029		Falta de mantenimiento
A030		Errores de mantenimiento / actualización de equipos
A031		Deficiencias en la organización
A032	Ataques intencionados	Difusión de software dañino
A033		Acceso no autorizado
A034		Divulgación de información
A035		Denegación de servicio
A036		Robo
A037		Indisponibilidad del personal (Huelgas)

A038	Fuga de información
A039	Manipulación de los equipos
A040	Ataque destructivo

Análisis de Riesgos

ANÁLISIS DE RIESGOS					
Código	**Activo**	Amenaza	Prob.	Impacto	RIESGO
D001	Historias Clínicas Físicas	Fuga de información	***2***	***3***	***6***
		Divulgación de información	***2***	***4***	***8***
		Destrucción de información	***2***	***4***	***8***
		Deterioro por manejo y uso de las Historias Clínicas	***4***	***3***	***12***
		Errores y fallos no intencionados (Introducción de información Incorrecta)	***3***	***4***	***12***
		Alteración accidental de la información (mezcla con otras Historias)	***3***	***4***	***12***
D002	Copias de seguridad – Backup	Divulgación de información	***1***	***2***	***2***
		Corrupción de la información	***2***	***3***	***6***
		Degradación de los soportes de almacenamiento de la información	***2***	***3***	***6***
		Destrucción de información	***2***	***4***	***8***
D003	Inventario de Aplicativos	Fuga de información	***2***	***1***	***2***
		Destrucción de información	***2***	***3***	***6***
SA001	Sistema Operativo Cliente	Instalación no estándar	***3***	***2***	***6***
		Difusión de software dañino (No Intencionado)	***3***	***5***	***15***
		Difusión de software dañino (Intencionado)	***2***	***5***	***10***
		Errores de mantenimiento / actualización de programas	***3***	***3***	***9***

		Errores de configuración	4	3	12
SA002	Sistema Operativo Servidores	Instalación no estándar	1	5	5
		Difusión de software dañino (No Intencionado)	2	5	10
		Difusión de software dañino (Intencionado)	1	5	5
		Errores de mantenimiento / actualización de programas	3	4	12
		Errores de configuración	2	5	10
SA003	Software Antivirus	Instalación no estándar	2	4	8
		Errores de mantenimiento / actualización de programas	3	4	12
		Errores de configuración	3	4	12
SA004	Software de Ofimática	Instalación no estándar	3	2	6
		Errores de mantenimiento / actualización de programas	1	2	2
		Errores de configuración	3	2	6
SA005	Sistema de Gestión Hospitalaria	Errores de los usuarios	4	4	16
		Avería de origen físico o lógico	3	4	12
		Suplantación de la identidad del usuario	2	4	8
		Acceso no autorizado	2	4	8
		Errores de mantenimiento / actualización de programas	2	4	8
		Errores de configuración	2	4	8
EI001	Servidor Sistema de Gestión Hospitalaria.	Denegación de servicio	2	5	10
		Avería de origen físico o lógico	2	4	8
		Acceso no autorizado	2	4	8
		Condiciones inadecuadas de temperatura o humedad	2	4	8
		Errores de mantenimiento / actualización de equipos	2	4	8
		Corte del suministro eléctrico	3	4	12

		Pérdida de Información	***2***	***5***	***10***
		Caída del sistema por agotamiento de recursos	***2***	***4***	***8***
EI002	PC's	Corte del suministro eléctrico	***3***	***3***	***9***
		Condiciones inadecuadas de temperatura o humedad	***2***	***3***	***6***
		Pérdida de equipos	***2***	***3***	***6***
		Avería de origen físico o lógico	***2***	***2***	***4***
EI003	Laptop	Robo	***2***	***3***	***6***
		Condiciones inadecuadas de temperatura o humedad	***2***	***3***	***6***
		Pérdida de equipos	***2***	***3***	***6***
		Avería de origen físico o lógico	***2***	***2***	***4***
EI004	Servidor Central IP	Denegación de servicio	***2***	***4***	***8***
		Avería de origen físico o lógico	***3***	***3***	***9***
		Acceso no autorizado	***2***	***4***	***8***
		Condiciones inadecuadas de temperatura o humedad	***2***	***3***	***6***
		Corte del suministro eléctrico	***3***	***3***	***9***
EI005	Central Telefónica	Avería de origen físico o lógico	***3***	***3***	***9***
		Condiciones inadecuadas de temperatura o humedad	***2***	***3***	***6***
		Corte del suministro eléctrico	***3***	***3***	***9***
EI006	Servidor de Aplicaciones	Denegación de servicio	***2***	***4***	***8***
		Avería de origen físico o lógico	***3***	***3***	***9***
		Acceso no autorizado	***2***	***4***	***8***
		Condiciones inadecuadas de temperatura o humedad	***2***	***3***	***6***
		Corte del suministro eléctrico	***3***	***3***	***9***
COM001	Equipos de Comunicaciones	Corte del suministro eléctrico	***3***	***3***	***9***

		Condiciones inadecuadas de temperatura o humedad	2	3	6
		Falta de mantenimiento	3	3	9
		Contaminación electromagnética (interferencia o carga electromagnética)	2	3	6
		Fallo de servicios de comunicaciones	3	3	9
COM002	Switch Core	Corte del suministro eléctrico	3	3	9
		Condiciones inadecuadas de temperatura o humedad	2	3	6
		Fallo de servicios de comunicaciones	3	3	9
		Falta de mantenimiento	3	3	9
COM003	Switches de Borde	Corte del suministro eléctrico	3	3	9
		Condiciones inadecuadas de temperatura o humedad	2	3	6
		Falta de mantenimiento	3	3	9
		Fallo de servicios de comunicaciones	3	3	9
COM004	Servicio de Internet	Falta de pago	2	3	6
		Caída de los servicios del Proveedor	3	3	9
COM005	Router de Internet	Corte del suministro eléctrico	3	3	9
		Condiciones inadecuadas de temperatura o humedad	2	3	6
		Fallo de servicios de comunicaciones	3	3	9
		Falta de mantenimiento	3	3	9
COM006	Servicio de Telefonía	Falta de pago	2	3	6
		Caída de los servicios del Proveedor	3	3	9
EA001	UPS para Data Center	Avería de origen físico o lógico	2	3	6
		Falta de mantenimiento	3	3	9
		Condiciones inadecuadas de temperatura o humedad	2	3	6

EA002	Aire Acondicionado Data Center	Corte del suministro eléctrico	3	3	9
		Falta de mantenimiento	3	3	9
		Avería de origen físico o lógico	2	3	6
EA003	Extintores del archivo de Historias Clínicas	Manipulación de los equipos	1	4	4
		Falta de mantenimiento	3	3	9
		Pérdida de equipos	1	4	4
I001	Archivo de Historias clínicas	Acceso No Autorizado	2	5	10
		Desastres naturales	1	5	5
		Fuego	2	5	10
		Daños por agua	2	5	10
		Desastres industriales (contaminación química)	1	5	5
		Ataque destructivo	1	5	5
I002	Data Center	Acceso No Autorizado	2	5	10
		Desastres naturales	2	5	10
		Fuego	1	5	5
		Daños por agua	1	5	5
I003	Oficinas Área de TI	Desastres naturales	2	5	10
		Fuego	1	5	5
		Daños por agua	1	5	5
IN001	Experiencia del personal (Gestión de la HC)	Indisponibilidad del personal (permisos o urgencias)	4	3	12
		Indisponibilidad del personal (Huelgas)	2	5	10
		Deficiencias en la organización	2	4	8
IN002	Imagen Corporativa	Negligencias	2	5	10

Figura 28. Análisis de Riesgos de Los Activos de Información. Adaptación de metodología Magerit

Acciones frente a amenazas

Permiten hacer frente a las amenazas, especialmente las técnicas, varían con el avance tecnológico, por lo que deben ser revisadas cada cierto tiempo.

Tabla 69

Amenazas de acuerdo a su origen

Código	Activo	Vulnerabilidad	Amenaza	ACCIONES
D001	Historias Clínicas Físicas	Ausencia de una política de Seguridad de la Información establecida para EsSalud Cajamarca, ausencia de un controles eficaces para la protección de la información de la HC.	Fuga de información	Establecer en toda la gestión de la información un procedimiento de Identificación y autenticación. Establecer una política de Seguridad de la Información que norme el uso adecuado de la información de la institución y las sanciones en caso de uso inadecuado
			Divulgación de información	Establecer Roles y Responsabilidades. Establecer una política de Seguridad de la Información.
		No se tiene toda la Información de las Historias Clínicas respaldadas en el Sistema de Gestión Hospitalaria	Destrucción de información	Realizar según lo programado copias de seguridad de los datos (backup)
			Deterioro por manejo y uso de las Historias Clínicas	Respaldar toda la información de manera electrónica. Establecer una política de Seguridad de la Información. Establecer un procedimiento de etiquetado y clasificación de la información.
		Ausencia de capacitación constante al personal y falta de auditorías a las Historias Clínicas o una revisión al azar para verificar su correcto llenado. Escasez de personal en el área de archivo de Historias Clínicas	Errores y fallos no intencionados (Introducción de información Incorrecta)	Instruir mejor al personal y establecer documentación necesaria. Segregar funciones y responsabilidades entre el personal asistencial y administrativo. Auditoria constante a las Historias Clínicas.
			Alteración accidental de la información (mezcla con otras Historias)	Establecer una política de Seguridad de la Información. Establecer un procedimiento de etiquetado y clasificación de la información. Auditoria constante a las Historias Clínicas.

D002	Copias de seguridad - Backup	Ausencia de política de seguridad. Las copias de seguridad son almacenadas en el mismo local en donde se encuentra ubicado el Data Center. No se realizan pruebas periódicas de restauración de información a partir de las copias de seguridad. Se debe mejorar la segregación de funciones y responsabilidades.	Divulgación de información Corrupción de la información Degradación de los soportes de almacenamiento de la información Destrucción de información	Protección criptográfica del contenido. Establecer Roles y Responsabilidades. Establecer una política de Seguridad de la Información. Verificación de las copias de seguridad, establecer una política que ejecute de manera periódica una restauración de la información a partir de las copias de seguridad Establecer un procedimiento para la destrucción de soportes de información y renovar estos medios en un espacio de tiempo acorde a las necesidades y realidad de la institución. Resguardo de las copias de seguridad en otro de los locales de EsSalud en Cajamarca asegurando su protección contra accesos no autorizados inclusive durante su transporte.
D003	Inventario de Aplicativos	Ausencia de una politica de Seguridad de la Información establecida para EsSalud Cajamarca	Fuga de información Destrucción de información	Establecer en toda la gestión de la información un procedimiento de Identificación y autenticación. Establecer una política de Seguridad de la Información que norme el uso adecuado de la información de la institución y las sanciones en caso de uso inadecuado Realizar según lo programado copias de seguridad de los datos (backup)
SA001	Sistema Operativo Cliente	Falta de personal para tareas de soporte y mantenimiento de equipos de computo Por necesidad no se restringen todos los permisos a los usuarios. Privilegios de Administrador del sistema en algunos equipos de la institución	Instalación no estándar Difusión de software dañino (No Intencionado) Difusión de software dañino (Intencionado)	La organización debe asegurar los recursos necesarios de personal para las tareas que tengan que ver con los sistemas Informáticos Se deben aplicar perfiles de seguridad y establecer controles para la detección, prevención y recuperación contra códigos o software malicioso.

		Falta de personal para tareas de soporte y mantenimiento de equipos de computo	Errores de mantenimiento / actualización de programas Errores de configuración	Se deben establecer los procedimientos adecuados a fin de llevar un control de cambios (actualizaciones y mantenimiento) a los sistemas operativos cliente realizando pruebas iniciales antes de replicar la configuración a todos los equipos de cómputo. Establecer una revisión periódica de los sistemas Operativos a fin de verificar si cumplen con las políticas y normas de seguridad de la Información.
SA002	Sistema Operativo Servidores	Proceso depende de la experiencia del personal a cargo.	Instalación no estándar	La organización debe brindar capacitación especializada sobre temas técnicos propios de los sistemas operativos servidores y sobre los temas de seguridad de la Información que se deben contemplar en la instalación.
		Diferentes usuarios de sistemas pueden acceder a recursos de los equipos servidores pudiendo desencadenar algún tipo de infección.	Difusión de software dañino (No Intensionado) Difusión de software dañino (Intensionado)	Se deben aplicar perfiles de seguridad y establecer controles para la detección, prevención y recuperación contra códigos o software malicioso.
		Falta de personal para tareas de soporte y mantenimiento. Poca capacitación en temas especializados al personal a cargo de soporte.	Errores de mantenimiento / actualización de programas Errores de configuración	Se deben establecer los procedimientos adecuados a fin de llevar un control de cambios (actualizaciones y mantenimiento) a los sistemas operativos servidor realizando pruebas iniciales antes de ser desplegados en equipos que se encuentren en producción. Establecer una revisión periódica de los sistemas Operativos a fin de verificar si cumplen con las políticas y normas de seguridad de la Información.
SA003	Software Antivirus	Falta de personal para tareas de soporte y mantenimiento de equipos de computo	Instalación no estándar	La organización debe asegurar los recursos necesarios de personal para las tareas que tengan que ver con los sistemas Informáticos
			Errores de mantenimiento /	Se deben establecer los procedimientos adecuados a

		Falta de personal para tareas de soporte y mantenimiento de equipos de computo	actualización de programas Errores de configuración	fin de llevar un control de cambios (actualizaciones y mantenimiento) a las herramientas informaticas antivirus, asegurando su actualización siempre a la última versión emitida por el fabricante. Establecer una política que asegure la actualización diaria o cuando sea necesario de la herramienta antivirus y llevar un control sobre ello.
SA004	Software de Ofimática	Falta de personal para tareas de soporte y mantenimiento de equipos de computo	Instalación no estándar	La organización debe asegurar los recursos necesarios de personal para las tareas que tengan que ver con los sistemas Informáticos
		Falta de personal para tareas de soporte y mantenimiento de equipos de computo	Errores de mantenimiento / actualización de programas Errores de configuración	Se deben establecer los procedimientos adecuados a fin de llevar un control de cambios (actualizaciones y mantenimiento) al software Ofimático realizando pruebas iniciales antes de ser desplegadas las actualizaciones o nuevas versiones en equipos siempre que sea necesario, en caso contrario se deben de limitar los cambios. Establecer una revisión periodica de los sistemas Operativos a fin de verificar si cumplen con las políticas y normas de seguridad de la Información.
SA005	Sistema de Gestión Hospitalaria	El sistema no valida la información ingresada por el usuario. Usuarios rutinizados en el uso del sistema.	Errores de los usuarios	La organización debe brindar capacitación constante en el uso correcto del Sistema de Gestión Hospitalaria.
		No existe una persona dedicada a monitorear el desempeño del sistema de manera constante, no se registran adecuadamente incidentes y eventos.	Avería de origen físico o lógico	Se debe establecer un plan de mantenimiento del sistemas tomando en cuenta la criticidad de la información del negocio, sistemas y procesos involucrados y una reevaluación de riesgos, asimismo se debe establecer una política para registrar cualquier tipo de evento para

				luego ser estudiado y determinar su causa a fin de que se tomen acciones correctivas.
		Usuarios minimizan o no toman en cuenta la gravedad de compartir claves y usuarios con otras personas. Inadecuado resguardo de claves y usuarios.	Suplantación de la identidad del usuario Acceso no autorizado	Se debe establecer una política de vencimiento de contraseñas y capacitar al personal para saber cómo establecer contraseñas de calidad Establecer el acceso a los sistemas y a las aplicaciones controladas por un procedimiento de ingreso seguro.
		Falta de personal para tareas de soporte y mantenimiento de equipos de computo	Errores de mantenimiento / actualización de programas Errores de configuración	Se deben establecer los procedimientos adecuados a fin de realizar un mantenimiento periódico del Sistema de Gestión Hospitalaria, se debe evaluar cualquier cambio de configuración y limitar los cambios a menos que sea necesario, se debe llevar un control de esta tarea. Establecer una revisión periódica del sistema en los equipos clientes verificando su correcto funcionamiento.
EI001	Servidor Sistema de Gestión Hospitalaria.	Desde la red interna se podría desarrollar un ataque hacia el servidor del Sistema de Gestión Hospitalaria	Denegación de servicio	Los usuarios deben tener acceso solamente a la red y a servicios de red que hayan sido específicamente autorizados a usar. Se deben aplicar perfiles de seguridad de acceso a los equipos servidores.
		No existe una persona y procedimientos o políticas dedicadas a monitorear el desempeño de los equipos servidores de manera constante, no se registran adecuadamente incidentes y eventos.	Avería de origen físico o lógico	Los equipos deben mantenerse de manera correcta para asegurar su continua disponibilidad e integridad. Se debe tener equipos de respaldo y algunos repuestos esenciales adecuados para los modelos de equipos con los que cuenta la institución.

	No se ejecutan procedimientos de remoción de privilegios y actualización constante de usuarios y claves.	Acceso no autorizado	Establecer el acceso a los sistemas y a las aplicaciones controladas por un procedimiento de ingreso seguro.
	La ubicación del Data Center es en las instalaciones antiguas del local de administración.	Condiciones inadecuadas de temperatura o humedad	Los equipos deben ser ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales, así como las oportunidades para el acceso no autorizado. Se debe evaluar a futuro la construción o traslado del Data Center a una mejor ubicación.
	Falta de mantenimiento constante y programado del Hardware, cambios o actualizaciones realizadas directamente en el equipo sin hacer sido probados previamente.	Errores de mantenimiento / actualización de equipos	Los equipos deben mantenerse de manera correcta para asegurar su continua disponibilidad e integridad. Se debe cumplir y revisar el cumplimiento del plan de mantenimiento.
	Aun cuando se cuenta con un UPS en ocasiones se presentan cortes de energía electríca que superan el tiempo de duración del UPS	Corte del suministro eléctrico	Los equipos deben ser protegidos contra fallas de electricidad y otras alteraciones causadas por fallas en los servicios de suministro. Se debe evaluar las adquisición de un generador de energía para el data center.
	No se cuenta con equipos de respaldo o con repuestos de componentes del servidor	Pérdida de Información	Copias de respaldo de la información, del software y de las imágenes del sistema deben ser tomadas y probadas regularmente en concordancia con una política de respaldo acordada.
	No se ha establecido una línea base de desempeño del equipo además de que no se tiene establecida una medición de las necesidades a futuro.	Caída del sistema por agotamiento de recursos	Los equipos deben mantenerse de manera correcta para asegurar su continua disponibilidad e integridad. Se debe establecer una línea base de uso de los recursos a fin de determinar las necesidades de crecimiento o agotamiento de recursos a futuro.

EI002	PC's	Se producen cortes de energía que pueden ser prolongados en el tiempo.	Corte del suministro eléctrico	Los equipos deben ser protegidos contra fallas de electricidad y otras alteraciones causadas por fallas en los servicios de suministro. Se debe evaluar las adquisición de un generador de energía para el data center.
		La mayoría de las instalaciones son antiguas e inapropiadas para el trabajo de los equipos.	Condiciones inadecuadas de temperatura o humedad	Los equipos deben ser ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales, así como las oportunidades para el acceso no autorizado. Se tiene previsto la construcción de un nuevo hospital moderno que tiene en consideración estos aspectos para la parte de equipos del personal asistencial.
		Al ser trasladados de un local a otro se podrían estraviar dentro de las instalaciones de EsSalud	Pérdida de equipos	Establecer mejores controles de seguridad y restringir el acceso a zonas no autorizadas. Se debe llevar un control del inventario de equipos.
		Por el tiempo de uso los recursos podrían fallar, también debido a un falta de mantenimiento preventivo.	Avería de origen físico o lógico	Se debe establecer un tiempo de uso adecuado para los equipos y ejecutar el reemplazo pasado ese tiempo.
EI003	Laptop	Por ser una institución pública se permite el acceso al público en general a la mayoría de sus instalaciones, sobre todo en la parte asistencial	Robo	Establecer mejores controles de seguridad y restringir el acceso a zonas no autorizadas, se puede tambien pensar en una reestructutración de la ubicación de ciertas areas
		La mayoría de las instalaciones son antiguas e inapropiadas para el trabajo de los equipos.	Condiciones inadecuadas de temperatura o humedad	Los equipos deben ser ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales, así como las oportunidades para el acceso no autorizado. Se tiene previsto la construcción de un nuevo hospital moderno que tiene en consideración estos aspectos para la parte de equipos del personal asistencial.
		Debido a la portabilidad se podrían estraviar dentro de	Pérdida de equipos	Se debe llevar un control del inventario de equipos.

		alguna de las instalaciones de EsSalud.		
		Por el tiempo de uso los recursos podrían fallar, también debido a un falta de mantenimiento preventivo.	Avería de origen físico o lógico	Se debe establecer un tiempo de uso adecuado para los equipos y ejecutar el reemplazo pasado ese tiempo.
EI004	Servidor Central IP	Desde la red interna se podría desarrollar un ataque hacia el servidor de la Central IP	Denegación de servicio	Los usuarios deben tener acceso solamente a la red y a servicios de red que hayan sido específicamente autorizados a usar. Se deben aplicar perfiles de seguridad de acceso a los equipos servidores.
		No existe una persona y procedimientos o políticas dedicadas a monitorear el desempeño de los equipos servidores de manera constante, no se registran adecuadamente incidentes y eventos.	Avería de origen físico o lógico	Los equipos deben mantenerse de manera correcta para asegurar su continua disponibilidad e integridad. Se debe tener equipos de respaldo y algunos repuestos esenciales adecuados para los modelos de equipos con los que cuenta la institución.
		No se ejecutan procedimientos de remoción de privilegios y actualización constante de usuarios y claves.	Acceso no autorizado	Establecer el acceso a los sistemas y a las aplicaciones controladas por un procedimiento de ingreso seguro.
		La ubicación del Data Center es en las instalaciones antiguas del local de administración.	Condiciones inadecuadas de temperatura o humedad	Los equipos deben ser ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales, así como las oportunidades para el acceso no autorizado. Se debe evaluar a futuro la construcción o traslado del Data Center a una mejor ubicación.
		Aun cuando se cuenta con un UPS en ocasiones se presentan cortes de energía electríca que superan el tiempo de duración del UPS	Corte del suministro eléctrico	Los equipos deben ser protegidos contra fallas de electricidad y otras alteraciones causadas por fallas en los servicios de suministro. Se debe evaluar las adquisición de un generador de energía para el data center.

EI005	Central Telefónica	No existe una persona y procedimientos o políticas dedicadas a monitorear el desempeño de los equipos servidores de manera constante, no se registran adecuadamente incidentes y eventos.	Avería de origen físico o lógico	Los equipos deben mantenerse de manera correcta para asegurar su continua disponibilidad e integridad. Se debe tener equipos de respaldo y algunos repuestos esenciales adecuados para los modelos de equipos con los que cuenta la institución.
		La ubicación del Data Center es en las instalaciones antiguas del local de administración.	Condiciones inadecuadas de temperatura o humedad	Los equipos deben ser ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales, así como las oportunidades para el acceso no autorizado. Se debe evaluar a futuro la construción o traslado del Data Center a una mejor ubicación.
		Aun cuando se cuenta con un UPS en ocasiones se presentan cortes de energía eléctrica que superan el tiempo de duración del UPS	Corte del suministro eléctrico	Los equipos deben ser protegidos contra fallas de electricidad y otras alteraciones causadas por fallas en los servicios de suministro. Se debe evaluar las adquisición de un generador de energía para el data center.
EI006	Servidor de Aplicaciones	Desde la red interna se podría desarrollar un ataque hacia el servidor de Aplicaciones	Denegación de servicio	Los usuarios deben tener acceso solamente a la red y a servicios de red que hayan sido específicamente autorizados a usar. Se deben aplicar perfiles de seguridad de acceso a los equipos servidores.
		No existe una persona y procedimientos o políticas dedicadas a monitorear el desempeño de los equipos servidores de manera constante, no se registran adecuadamente incidentes y eventos.	Avería de origen físico o lógico	Los equipos deben mantenerse de manera correcta para asegurar su continua disponibilidad e integridad. Se debe tener equipos de respaldo y algunos repuestos esenciales adecuados para los modelos de equipos con los que cuenta la institución.
		No se ejecutan procedimientos de remoción de privilegios y actualización constante de usuarios y claves.	Acceso no autorizado	Establecer el acceso a los sistemas y a las aplicaciones controladas por un procedimiento de ingreso seguro.

		La ubicación del Data Center es en las instalaciones antiguas del local de administración.	Condiciones inadecuadas de temperatura o humedad	Los equipos deben ser ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales, así como las oportunidades para el acceso no autorizado. Se debe evaluar a futuro la construcción o traslado del Data Center a una mejor ubicación.
		Aun cuando se cuenta con un UPS en ocasiones se presentan cortes de energía eléctrica que superan el tiempo de duración del UPS	Corte del suministro eléctrico	Los equipos deben ser protegidos contra fallas de electricidad y otras alteraciones causadas por fallas en los servicios de suministro. Se debe evaluar las adquisición de un generador de energía para el data center.
COM001	Equipos de Comunicaciones	Aun cuando se cuenta con un UPS en ocasiones se presentan cortes de energía eléctrica que superan el tiempo de duración del UPS	Corte del suministro eléctrico	Los equipos deben ser protegidos contra fallas de electricidad y otras alteraciones causadas por fallas en los servicios de suministro. Se debe evaluar las adquisición de un generador de energía para el data center.
		La ubicación del Data Center es en las instalaciones antiguas del local de administración.	Condiciones inadecuadas de temperatura o humedad	Los equipos deben ser ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales, así como las oportunidades para el acceso no autorizado. Se debe evaluar a futuro la construcción o traslado del Data Center a una mejor ubicación.
		Falta de personal para tareas de soporte y mantenimiento de equipos de computo	Falta de mantenimiento	Se debe establecer y cumplir un plan de mantenimiento anual verificando que la tarea se haya cumplido de manera correcta
		Creciente uso de señales electromagnética en toda la ciudad	Contaminación electromagnética (interferencia o carga electromagnética)	Se debe medir el funcionamiento de la red y establecer los niveles de servicio adecuados a fin de detectar posibles caídas o degradaciones del servicio.

		Ausencia de equipos de respaldo	Fallo de servicios de comunicaciones	Se debe establecer una política de mantenimiento de stock de equipos de respaldo en caso de avería de los equipos en producción
COM002	Switch Core	Aun cuando se cuenta con un UPS en ocasiones se presentan cortes de energía eléctrica que superan el tiempo de duración del UPS	Corte del suministro eléctrico	Los equipos deben ser protegidos contra fallas de electricidad y otras alteraciones causadas por fallas en los servicios de suministro. Se debe evaluar las adquisición de un generador de energía para el data center.
		La ubicación del Data Center es en las instalaciones antiguas del local de administración.	Condiciones inadecuadas de temperatura o humedad	Los equipos deben ser ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales, así como las oportunidades para el acceso no autorizado. Se debe evaluar a futuro la construcción o traslado del Data Center a una mejor ubicación.
		Ausencia de equipos de respaldo	Fallo de servicios de comunicaciones	Se debe establecer una política de mantenimiento de stock de equipos de respaldo en caso de avería de los equipos en producción
		Falta de personal para tareas de soporte y mantenimiento de equipos de computo	Falta de mantenimiento	Se debe establecer y cumplir un plan de mantenimiento anual verificando que la tarea se haya cumplido de manera correcta
COM003	Switches de Borde	Aun cuando se cuenta con un UPS en ocasiones se presentan cortes de energía eléctrica que superan el tiempo de duración del UPS	Corte del suministro eléctrico	Los equipos deben ser protegidos contra fallas de electricidad y otras alteraciones causadas por fallas en los servicios de suministro. Se debe evaluar las adquisición de un generador de energía para el data center.
		La ubicación del Data Center es en las instalaciones antiguas del local de administración.	Condiciones inadecuadas de temperatura o humedad	Los equipos deben ser ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales, así como las oportunidades para el acceso no autorizado. Se debe evaluar a futuro la construcción o traslado del

				Data Center a una mejor ubicación.
		Falta de personal para tareas de soporte y mantenimiento de equipos de computo	Falta de mantenimiento	Se debe establecer y cumplir un plan de mantenimiento anual verificando que la tarea se haya cumplido de manera correcta
		Ausencia de equipos de respaldo	Fallo de servicios de comunicaciones	Se debe establecer una política de mantenimiento de stock de equipos de respaldo en caso de avería de los equipos en producción
COM004	Servicio de Internet	Se puede producir huelgas en la parte administrativa o por temas relacionados al funcionamiento de la parte administrativa se podría dejar de pagar el servicio ocasionando un corte del servicio.	Falta de pago	Establecer un procedimiento de monitoreo, revisión y auditoría regularmente de la entrega del servicio por parte del proveedor y el estado del cumplimiento de pagos y demás deberes de la institución.
		Posible caída de los servicios del proveedor a nivel nacional o mundial originando una indisponibilidad de acceso a su red de datos.	Caída de los servicios del Proveedor	Se debe establecer en el contrato con el proveedor los temas relacionados a la seguridad de la información como parte de los acuerdos y el nivel de servicio que se espera, además también se deben establecer los datos de contacto del personal de la institución a los que el proveedor deberá de comunicar cualquier inconveniente con el servicio.
COM005	Router de Internet	Aun cuando se cuenta con un UPS en ocasiones se presentan cortes de energía electríca que superan el tiempo de duración del UPS	Corte del suministro eléctrico	Los equipos deben ser protegidos contra fallas de electricidad y otras alteraciones causadas por fallas en los servicios de suministro. Se debe evaluar las adquisición de un generador de energía para el data center.

		La ubicación del Data Center es en las instalaciones antiguas del local de administración.	Condiciones inadecuadas de temperatura o humedad	Los equipos deben ser ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales, así como las oportunidades para el acceso no autorizado. Se debe evaluar a futuro la construcción o traslado del Data Center a una mejor ubicación.
		Ausencia de equipos de respaldo	Fallo de servicios de comunicaciones	Se debe establecer una política de mantenimiento de stock de equipos de respaldo en caso de avería de los equipos en producción
		Falta de personal para tareas de soporte y mantenimiento de equipos de computo	Falta de mantenimiento	Se debe establecer y cumplir un plan de mantenimiento anual verificando que la tarea se haya cumplido de manera correcta
COM006	Servicio de Telefonía	Se puede producir huelgas en la parte administrativa o por temas relacionados al funcionamiento de la parte administrativa se podría dejar de pagar el servicio ocasionando un corte del servicio.	Falta de pago	Establecer un procedimiento de monitoreo, revisión y auditoría regularmente de la entrega del servicio por parte del proveedor y el estado del cumplimiento de pagos y demás deberes de la institución.
		Posible caída de los servicios del proveedor a nivel nacional o mundial originando una indisponibilidad de acceso a su red de telefonía.	Caída de los servicios del Proveedor	Se debe establecer en el contrato con el proveedor los temas relacionados a la seguridad de la información como parte de los acuerdos y el nivel de servicio que se espera, además también se deben establecer los datos de contacto del personal de la institución a los que el proveedor deberá de comunicar cualquier inconveniente con el servicio.
EA001	UPS para Data Center	Falta de personal para tareas de soporte y mantenimiento del equipo UPS, además de expiración de tiempo de garantía.	Avería de origen físico o lógico	Los equipos deben mantenerse de manera correcta para asegurar su continua disponibilidad e integridad. Se debe tener equipos de respaldo y algunos repuestos esenciales adecuados para los modelos de equipos con los que cuenta la institución.

			Falta de mantenimiento	Se debe establecer y cumplir un plan de mantenimiento anual verificando que la tarea se haya cumplido de manera correcta
		La ubicación del Data Center es en las instalaciones antiguas del local de administración.	Condiciones inadecuadas de temperatura o humedad	Los equipos deben ser ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales, así como las oportunidades para el acceso no autorizado. Se debe evaluar a futuro la construcción o traslado del Data Center a una mejor ubicación.
EA002	Aire Acondicionado Data Center	Aun cuando se cuenta con un UPS en ocasiones se presentan cortes de energía eléctrica que superan el tiempo de duración del UPS	Corte del suministro eléctrico	Los equipos deben ser protegidos contra fallas de electricidad y otras alteraciones causadas por fallas en los servicios de suministro. Se debe evaluar las adquisición de un generador de energía para el data center.
		Falta de personal para tareas de soporte y mantenimiento del equipo de aire acondicionado, además de expiración de tiempo de garantía.	Falta de mantenimiento	Los equipos deben mantenerse de manera correcta para asegurar su continua disponibilidad e integridad. Se debe tener equipos de respaldo y algunos repuestos esenciales adecuados para los modelos de equipos con los que cuenta la institución.
			Avería de origen físico o lógico	Se debe establecer y cumplir un plan de mantenimiento anual verificando que la tarea se haya cumplido de manera correcta
EA003	Extintores del archivo de Historias Clínicas	Equipos por naturaleza expuestos a ser manipulados por cualquier persona que acceda a ellos.	Manipulación de los equipos	Se deben publicar carteles que adviertan el uso inadecuado de los equipos y la advertencia de sanciones Se debe capacitar al personal en el uso adecuado de los equipos.
		No se programan los mantenimientos en base a fechas de vencimiento.	Falta de mantenimiento	Se deben hacer pruebas de funcionamiento cada cierto tiempo.
		Por su naturaleza deben ser fáciles de extraer de su lugar para poder ser utilizados	Pérdida de equipos	Se deben proteger de la mejor manera posible los equipos de manera que se proteja el

				equipo pero no se dificulte su uso ante una emergencia.
I001	Archivo de Historias clínicas	No existe un control o protección adecuada para acceder al ambiente en donde está ubicado el archivo central de Historias Clínicas.	Acceso no autorizado	Las áreas importantes deben ser protegidas por medio de controles apropiados de ingreso para asegurar que se le permite el acceso sólo al personal autorizado.
		No es muy frecuente pero se podría presentar algún tipo de desastre natural que podría afectar las instalaciones del archivo.	Desastres naturales	Se debe diseñar y aplicar una protección física contra desastres naturales, ataque malicioso o accidentes.
		Se podría originar un incendio en el estacionamiento que está al costado del archivo.	Fuego	
		Se han presentado ya problemas por inundación en épocas de lluvias intensas.	Daños por agua	
		Debido al manejo de sustancias químicas es posible la contaminación de las instalaciones o el desarrollo de alguna epidemia.	Desastres industriales (contaminación química)	
		Debido a la cercanía del ambiente con el exterior del Hospital se podría ver afectadas las instalaciones debido a un ataque intencionado.	Ataque destructivo	
I002	Data Center	Se controla el ingreso a la edificación pero no hay un control restringido para acceder al Data Center	Acceso no autorizado	Las áreas seguras deben ser protegidas por medio de controles apropiados de ingreso para asegurar que se le permite el acceso sólo al personal autorizado.
		Edificación antigua	Desastres naturales	Se debe diseñar y aplicar una protección física contra desastres naturales, ataque malicioso o accidentes.
		Los equipos pueden producir un exceso de calor que podría ocasionar la aparición de fuego.	Fuego	
		En épocas de lluvia se podría presentar precipitaciones altas.	Daños por agua	
I003	Oficinas Área de TI	Edificación antigua	Desastres naturales	Se debe diseñar y aplicar una protección física contra
		Los equipos pueden producir un exceso de calor que podría	Fuego	

		ocasionar la aparición de fuego.		desastres naturales, ataque malicioso o accidentes.
		Los equipos pueden producir un exceso de calor que podría ocasionar la aparición de fuego.	Daños por agua	
IN001	Experiencia del personal (Gestión de la HC)	Permisos o urgencias que se pueden presentar en el personal. Huelgas o reclamos por temas de salarios y otros Desorganización o cambios políticos en la organización.	Indisponibilidad del personal (permisos o urgencias) Indisponibilidad del personal (Huelgas) Deficiencias en la organización	Establecer políticas y procedimientos en caso de ausencias o cambios de personal.
IN002	Imagen Corporativa	Posibilidad de incumplimiento de normas de seguridad y procedimientos.	Negligencias médicas.	Establecer auditorias médicas inopinadas para verificar que en todos los procedimientos médicos se estén tomando en cuenta todas las normas y medidas de seguridad