UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

FACULTAD DE INGENIERÍA Y GESTIÓN

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

"PLAN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2014 PARA EL CENTRO DE SALUD MENTAL COMUNITARIO SAN GABRIEL ALTO"

TRABAJO DE SUFICIENCIA PROFESIONAL
Para optar el Título Profesional de

INGENIERO DE SISTEMAS

PRESENTADO POR EL BACHILLER

ALBERTO ALE, MIGUEL ANGEL

Villa El Salvador
2016

DEDICATORIA

A mis padres por su apoyo incansable y cada uno de mis proyectos a lo largo de mi vida. A mi hermana Olga por todos sus consejos. A mi esposa Cristina que con su aliento diario permite seguir día a día en la búsqueda de nuevos retos y alcanzar mis metas con optimismo y excelencia. A mi hijo Piero por ser una motivación en todos los ámbitos de mi vida. En especial a Margarita Gutiérrez Lizárraga que con su amor y apoyo día a día hizo que este proyecto salga a la luz

Miguel Ángel Alberto Ale

AGRADECIMIENTO

Agradezco a Dios por siempre estar allí.

A mis padres, por inculcarme el hermoso hábito de la lectura y la exigencia en el estudio.

A mi esposa Cristina por todo su apoyo.

A mis profesores de la carrera.

A mis amigos y compañeros por todos los conocimientos compartidos en las aulas.

Miguel Ángel Alberto Ale

ÍNDICE

LISTADO DE FIGURAS

LISTADO DE TABLAS

ÍNDICE DE ANEXOS

INTRODUCCIÓN

El Centro de Salud Mental Comunitario San Gabriel Alto tiene como función fortalecer la salud mental de la población a través del desarrollo de estrategias aplicadas a resolver los principales problemas que aquejan a la salud mental en el distrito de Villa María del Triunfo, tales como: Violencia familiar, trastorno de depresión, trastorno de ansiedad, intento de suicidio y abuso de alcohol sin distinción de género, raza, edad, nivel cultural y socio – económico.

Como entidad pública prestadora de servicios de salud, se dedica a la atención del paciente mediante consulta psiquiátrica, psicológica y terapia de lenguaje a cargo de profesionales de la salud (psiquiatra, psicólogo, terapista ocupacional).

Para acceder a estos servicios en las diversas especialidades del Centro de Salud Mental Comunitario San Gabriel Alto, es necesaria la creación física de la Historia Clínica del paciente. Este documento legal que permite almacenar los datos personales del paciente, contiene información privada que incluye nombres completos, datos biométricos, resultados de exámenes y derivaciones a otros centros de mayor complejidad mediante la hoja de referencia.

En el contexto del presente proyecto “Plan de seguridad de la información en el Centro de Salud Mental Comunitario San Gabriel alto” se

debe tener en cuenta que el activo de información más importante que maneja el establecimiento de salud es la Historia Clínica, la misma que debe ser resguardada por la institución manteniendo su integridad, disponibilidad y confidencialidad. Para ello, es necesario planificar uso de diferentes herramientas que nos permitan mantener estas tres condiciones fundamentales en la seguridad de la información.

CAPÍTULO I

PLANTEAMIENTO DEL PROBLEMA

1.1. DESCRIPCIÓN DE LA REALIDAD PROBLEMÁTICA

La atención de los pacientes en los establecimientos de salud públicos es un derecho que tiene todo ciudadano (PODER EJECUTIVO, 2015). Las instituciones prestadoras de servicios de salud tienen como finalidad, atender a los pacientes, registrando la información de estos mediante la historia clínica (MINSA, 2005). Este documento legal que almacena información confidencial del paciente, es manipulada diariamente por el personal de salud vinculado a la atención de pacientes (MINSA, 2005).

Todo establecimiento de salud público tiene como finalidad salvaguardar este activo crítico mediante la implementación de directivas descritos según la Norma Técnica de Historias Clínicas (MINSA, 2005). Además, la obligación legal de proceder con la aplicación de la Norma Técnica ISO 27001: 2014 cumpliendo con la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) que pueda garantizar la Integridad, Confidencialidad y Disponibilidad de la información que usa en sus diferentes procesos de negocio. (CNB - INDECOPI, 2014)

Dentro del Centro de Salud Mental Comunitario San Gabriel Alto, el manejo de la documentación formal - Historias Clínicas - no está clasificado por unidades de atención o nivel de criticidad (Gonzáles Aguado & Castejón Bellmunt, 2016). Este factor sumado a la búsqueda manual que realiza el personal a cargo de la unidad de admisión (MINSA, 2005), produce una demora en la ubicación de la historia clínica, generando incomodidad en el paciente durante la espera en la cola. Y este factor puede agravarse si llega un paciente que necesita atención médica urgente (intento de suicidio). No existe un apropiado control de accesos al área de admisión, el personal de otras unidades administrativas y/o de atención a pacientes puede ingresar, infringiendo la confidencialidad que todo ambiente de admisión debe necesariamente tener.

Además, el personal asistencial no devuelve inmediatamente la historia clínica después de concluida la atención. Por último, no se cuenta con planes de evacuación y emergencias ante desastres, sumado a ello la inexistencia de extintores en el establecimiento (ver Anexo 1).

1.2. JUSTIFICACIÓN DEL PROYECTO

El proyecto permitirá identificar los procesos que manejan los activos de información del Centro de Salud Mental comunitario San Gabriel Alto, así mismo, cumplir con las normas vigentes que vinculen el principal activo de los establecimientos de salud (Las historias clínicas de los pacientes) asegurando de esta manera que nuestro plan de seguridad de la información se mantenga alineado con las políticas vigentes que exigen un cuidado en el manejo de los datos personales, ayudando al personal de los establecimientos a proteger la información mediante el uso de políticas y controles evitando la pérdida de la información.

1.3. DELIMITACIÓN DEL PROYECTO

El presente proyecto de tesis se desarrollará en el Centro de Salud Mental Comunitario San Gabriel Alto perteneciente a la Red de Salud SJM – VMT, ubicado en el distrito de Villa María del Triunfo.

1.4. FORMULACIÓN DEL PROBLEMA

- ¿El centro de salud mental comunitario cuenta con el modelado de procesos que manejan información crítica de la organización?
- ¿El centro de salud mental comunitario cuenta con una metodología de análisis de riesgos y valoración de activos?
- ¿El centro de salud mental comunitario cuenta con un mapa de riesgos de los procesos críticos?
- ¿El centro de salud mental comunitario cuenta con declaración de aplicabilidad?

1.5. OBJETIVOS

1.5.1. Objetivo General

Elaborar el plan de Seguridad de la Información basado en la Norma Técnica Peruana NTP/IEC 27001: 2014 para el Centro de Salud Mental Comunitario San Gabriel Alto.

1.5.2. Objetivos Específicos

- Identificar los procesos que manejan el activo crítico de la organización.
- Elaborar el análisis de riesgos y valoración de activos.
- Elaborar un mapa de riesgos para el proceso de Admisión.
- Elaborar la declaración de aplicabilidad con los controles necesarios para tratar los riesgos de seguridad de la información.

CAPÍTULO II

MARCO TEÓRICO

2.1. ANTECEDENTES DE LA INVESTIGACIÓN

2.1.1. Diseño de un Sistema de Gestión de Seguridad de la Información para una empresa inmobiliaria alineado a la norma ISO/IEC 27001:2013 (2015)

En la tesis de grado, se hace referencia al diseño de un Sistema de Gestión de seguridad para una empresa inmobiliaria en la cual se evidencia el importante rol de la alta dirección en la aprobación y difusión de las políticas para el conocimiento del

personal responsable y su compromiso con el cumplimiento de dicha política.

Para este caso de negocio, se hizo evidente las amenazas tanto externas como internas a las que se expone diariamente la inmobiliaria durante la ejecución de sus diversos procesos de negocio. Por ello, es necesario establecer roles y responsabilidades dentro de la empresa relacionados a Seguridad de la Información para asegurar el cumplimiento de las políticas de seguridad establecidas así como el monitoreo y seguimiento de los riesgos hasta reducirlos a lo mínimo permitido.

Al no contar con un marco regulatorio, la inmobiliaria deberá trabajar el aspecto de la cultura de seguridad a todo nivel para concientizar al personal vinculado con la gestión de seguridad de la información.

2.1.2. Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001 para la Superintendencia de Transporte Terrestres de personas, carga y mercancías (SUTRAN) – Región Lambayeque (2015)

En la tesis de grado, se visualizó con mayor nitidez la importancia de la protección de datos en las organizaciones

mediante la información de todos los activos involucrados en los procesos de negocio, permitiendo de esta manera ver las falencias en seguridad de la información a los cuales están expuestos.

Otro alcance importante en el estudio de la Norma ISO 27001 es la calidad, la organización puede aplicar un proceso de mejora continua mediante el uso del ciclo de Deming, además; mediante la creación del Sistema de Gestión de Seguridad de la Información se logrará concientizar a los trabajadores creando así una cultura de seguridad de la información en cada uno de los departamentos encargados de los procesos de negocio.

2.1.3. Implementación de un Sistema de Gestión de Seguridad de la Información en el Ministerio de Desarrollo e Inclusión Social (2016)

Hace referencia al cumplimiento de la norma ISO/IEC 27001:2014 llevada a cabo en el centro de datos de este ministerio que custodia la información relacionada al Padrón General de Hogares, administrado por el Sistema de Focalización de Hogares (SISFOH), instrumento fundamental para conocer la clasificación socioeconómica de las familias de pobreza y pobreza

extrema que puedan acceder a los programas sociales del estado (MIDIS, 2016).

Para llevar a cabo esta implementación, la alta dirección del MIDIS constituyo el Comité de Gestión de Seguridad de la Información (MIDIS, 2016) y estableció las siguientes funciones:

- Asegurar que la Política de Seguridad de la información y los objetivos de seguridad de la información sean compatibles con la dirección estratégica del MIDIS.
- Revisar la Política de seguridad de la información, si ocurren cambios significativos, asegurar su adecuación y efectividad continua.
- Asegurar que los recursos necesarios para el sistema de gestión de seguridad de la información estén disponibles.
- Proponer planes y programas para mantener la conciencia en seguridad de la información entre el personal del MIDIS.
- Patrocinar auditorías internas y externas del Sistema de gestión de seguridad de la información a intervalos planificados (por lo menos una vez al año).
- Supervisas el cumplimiento de las exigencias legales en materias de seguridad de la información y de protección de datos personales (MIDIS, 2016).

2.1.4. Diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) para el área de informática de la cooperativa del magisterio de Túquerres bajo la Norma ISO 27001:2013 (2015)

En la tesis de grado, durante el levantamiento de los activos de la información, se vio algunas debilidades que debemos salvaguardar para evitar una pérdida o robo de la información. Una vez realizado el inventario de activos se continúa con un análisis de riesgo, midiendo el impacto de los eventos que atenten contra la seguridad de la información, esto nos permite aplicar controles para prevenir estos eventos. Una vez encontrados los riesgos, mediremos el impacto a los tres niveles, confidencialidad, integridad y disponibilidad de la información, mejorando los controles que ya estén implementados mediante el uso de políticas. Luego de la realización del diseño del SGSI, es imprescindible contar con el apoyo de la alta dirección para el desarrollo de mejoras y medidas a tomar para todos los trabajadores respecto a las buenas prácticas en seguridad de la información.

2.2. BASES TEÓRICAS

2.2.1 Norma ISO/IEC 27001: 2013

Es un estándar Internacional orientado a procesos de negocio en las organizaciones basada en el ciclo de Deming (Plan, Do, Check, Act) que permite el análisis, implementación, control y mantenimiento de un Sistema de Gestión de Seguridad de la Información enfocado al manejo de los activos de la información (ISO 27001, 2013). El uso de esta herramienta permitirá establecer:

- El alcance que tendrá el SGSI sobre los procesos.
- La política general de seguridad de la información.
- La identificación y valoración de los activos de información.
- La exposición de los activos a los riesgos en la organización.
- La selección de controles para mitigar los riesgos detectados. (CNB - INDECOPI, 2014).

2.2.2 Norma ISO/IEC 27002: 2013

Permite elaborar la declaración de aplicabilidad basada en la Norma ISO/IEC 27002, documento en el cual se detallan los

controles seleccionados así como también los implementados y excluidos, se detallara además el objetivo del control, la justificación de su elección y la justificación de su exclusión. (ISO 27002, 2013).

2.2.3 Norma ISO/IEC 27799: 2008

Es una norma que brinda directivas para la interpretación y aplicación de la norma ISO/IEC 27002 sobre los datos de pacientes en el sector salud, hace hincapié en la sensibilización y formación constante de los colaboradores en la gestión adecuada de los riesgos de seguridad mediante el análisis y diseño de un Sistema de Gestión de Seguridad de la Información en un entorno hospitalario. (ISO 27799, 2008) (Henarejos, Fernández Alemán, & Toval, 2013).

2.2.4 Norma ISO/IEC 31000: 2009

Estándar internacional que brinda recomendaciones para la implementación de un sistema de gestión de riesgos a cualquier organización sin importar su tamaño o tipo, de tal manera que pueda gestionarlos en cada una de sus actividades (ISO 31000, 2013). Para ello utiliza el ciclo de Deming o de mejora continua (Plan-Do-

Check-Act) como metodología de análisis de riesgos y valoración de activos. Se basa en 3 acciones:

- Establecer las políticas de riesgo para la organización.
- Análisis, valoración y manejo del riesgo.
- Análisis de las estrategias en el manejo de riesgos actuales y la implementación ante posibles riesgos futuros. (ISO 31000, 2013) (Delgado, 2014) (CNB - INDECOPI, 2014).

2.2.5 Business Process Model and Notation (BPMN 2.0)

BPMN 1.0 fue lanzado en mayo de 2004. Pone a disposición una notación gráfica, estandarizada, que permite automatizar los procesos a partir del diseño gráfico. (Briceño Ortega, 2009). Además de la notación gráfica, BPMN incorporó un número de mecanismos específicos para el modelado de procesos tales como eventos y mensajes.

La versión 2.0, completamente nueva y ampliada, se terminó a mediados del 2010 y fue desarrollado por BPMI (Business Process Management Initiative) con la finalidad de adoptar técnicas empleadas en las herramientas de esquematización así como unificar y extender los gráficos utilizados en ellas para expresar el significado de los símbolos y

patrones útiles para modelar la semántica de los procesos. (Freund , Rucker, & Hitpass, 2014).

Este modelado se realizará en la herramienta Bizagi, la cual nos permitirá ver de forma gráfica las tareas y la documentación obtenidas de los dueños del negocio.

2.2.6 Alcance organizacional del proyecto

Este proyecto tiene como alcance realizar el plan de seguridad de la información utilizando la Norma Técnica Peruana ISO/IEC 27001:2014 (CNB - INDECOPI, 2014), alineando su aplicación con la Ley de Protección de Datos Personales (CONGRESO DE LA REPUBLICA, 2011) enfocado en el Proceso de Admisión de Pacientes del Centro de Salud Mental Comunitario.

a. Necesidades del Negocio

Toda organización que brinda servicios de salud prestan un servicio critico que puede definir la vida de los pacientes en minutos (PODER EJECUTIVO, 2015) por ello; según mandato legal, la atención de los pacientes debe ser registrada y almacenada físicamente en la Historia Clínica

(MINSA, 2005). El establecimiento de salud debe garantizar la disponibilidad de esta información ante cualquier situación que ponga en riesgo la vida del paciente. (PODER EJECUTIVO, 2015).

La información contenida en los formatos para registrar la atención del paciente en los diversos módulos se encuentra descrito en la Norma Técnica Peruana de Historias Clínicas (MINSA, 2005). Esta norma ofrece directivas en el manejo de las historias clínicas respecto a la custodia, almacenamiento y depuración de las mismas. (MINSA, 2005).

Otra necesidad del Centro de Salud Mental Comunitario San Gabriel Alto es cumplir con la Norma Técnica Peruana NTP – ISO/IEC 27001:2014 en cuya publicación establece que dicha institución al pertenecer al ministerio de salud y por ende al sistema nacional de salud debe proceder con la implementación de un Sistema de Gestión de Seguridad de la Información garantizando la confidencialidad, integridad y disponibilidad de la información que utilice en sus procesos de negocio (PRESIDENCIA DEL CONSEJO DE MINISTROS, 2016).

Por último, la necesidad de cumplir con la Ley de Protección de Datos Personales (CONGRESO DE LA

REPUBLICA, 2011) (PODER EJECUTIVO, 2013). Se debe tener en cuenta que el activo más importante que maneja el establecimiento de salud es la historia clínica (María Fátima Cueva Murillo, 2015), la cual contiene información personal y debe ser resguardada. (CNB - INDECOPI, 2014).

b. Alcance organizacional en la Seguridad de la Información

Como toda entidad de salud, el ingreso al público en los establecimientos es caótico debido a la gran demanda de atención en salud mental. El establecimiento no es ajeno a esta realidad, siendo el servicio más solicitado el de Admisión.

La unidad de Admisión está a cargo de la creación, mantenimiento, custodia, archivo, entrega y recepción de las Historias Clínicas de los pacientes (MINSA, 2005).

Las funciones de la Unidad de Admisión son;

a) Gestionar el ingreso de los usuarios al establecimiento de salud.
b) Brindar orientación al usuario sobre el flujo de atención de acuerdo a su necesidad (Ver Anexo 2).
c) Identificar y registrar al paciente, buscando al paciente continuador y creando una historia clínica al paciente nuevo.

d) Orientar al paciente sobre la cartera de servicios que provee el Centro de Salud Mental Comunitario; se brinda información sobre la ubicación de los servicios donde acudirán los pacientes y los procedimientos a seguir por los profesionales a cargo de la atención (MINSA, 2016).

La unidad de Admisión se encuentra muy próxima al punto de ingreso de los usuarios. Su infraestructura permite una fácil y adecuada comunicación con ellos, así como garantizar la privacidad y confidencialidad de los activos de información que ella custodia (MINSA, 2016). Esta Unidad contiene además los siguientes módulos:

Módulo de Caja. Espacio donde se identifica el precio de la atención (Ver Anexo 3), cobro de la tarifa, emisión y archivo del comprobante de pago (Ver Anexo 4) y el control de ingresos y egresos (Ver Anexo 5) (MINSA, 2016).

Módulo de Seguro. Espacio donde se acredita de la condición de aseguramiento en salud que posee, si está activo o no SISFOH (Anexo 6) (MINSA, 2016).

c. Alcance en Tecnologías de Información y Comunicación

En el Centro de Salud Mental Comunitario como en cualquier establecimiento de salud, el manejo de las Historias Clínicas es manual (MINSA, 2005), soportándose en el programa informático Excel que permite la creación de los números correlativos de Historia Clínica, información básica del usuario y control de citas. (MINSA, 2005).

Es necesario establecer una Política de Seguridad de la Información para determinar los lineamientos que deben ser cumplidos en la organización. (CNB - INDECOPI, 2014) (ISO 27001, 2013). Esta política debe ser aprobada por la Alta Dirección y comunicar a la institución su importancia y los objetivos trazados. (CNB - INDECOPI, 2014)

d. Política de Seguridad de la Información

La política de Seguridad de la Información propuesta en este proyecto será:

“La atención de los servicios de salud pública son soportados en sistemas de información basados en software o de manera manual para gestionar la información de los pacientes.

Como institución pública dedicada a la atención de pacientes con depresión, trastornos psicóticos, violencia familiar, el Centro de Salud Mental Comunitario San Gabriel Alto (CSMC - SGA) tiene la obligación de proteger la información almacenada y adjuntar la información actualizada generada por los pacientes para brindar así un servicio de calidad, caso contrario, un incidente que afecte la información podría dificultar el acto médico o tratamiento poniendo en riesgo la salud del paciente como su entorno más cercano (feminicidio, suicidios).

Es obligación del CSMC – SGA garantizar la confidencialidad de los datos personales de los pacientes en el uso diario siguiendo las disposiciones de ley vigentes.

Los colaboradores del CSMC – SGA serán comunicados de esta política de seguridad asumiendo la responsabilidad individual manteniendo la integridad, disponibilidad y confidencialidad de la información.

Los colaboradores deben comprometerse con el cumplimiento de las políticas y procedimientos vigentes o que se implementen posteriormente.”

2.3 MARCO CONCEPTUAL

2.3.1 Conceptos relacionados al área de ciencias de la salud

a. Atención de salud

Acciones que se brinda a los pacientes como procedimiento para promover, prevenir, recuperar o rehabilitar la salud de una persona. (MINSA, 2005).

b. Acto médico

Es cualquier atención o acción que realice el personal médico como parte del ejercicio continuo de su profesión. Esto comprende el diagnóstico, terapia y pronóstico que realice el médico durante la atención de sus pacientes. (MINSA, 2005).

c. Historia Clínica

Es el documento médico donde se registra los datos de identificación y los procesos relacionados con las atenciones de salud recibidas por el paciente. Este documento legal se redacta de manera secuencial por los profesionales de la salud (MINSA, 2005).

La historia clínica tiene la siguiente estructura:

i. Identificación del paciente

Contiene los datos personales que identifican al paciente, incluye además los datos del establecimiento de salud y el número de Historia Clínica generado. (MINSA, 2005)

ii. Registro de la atención de salud

Contiene los registros de todas las atenciones de salud recibido por el paciente a lo largo de su vida clínica, incluye los diversos tratamientos ambulatorios en la entidad prestadora de salud. (MINSA, 2005).

iii. Información complementaria

Se registran en esta sección los resultados de exámenes, análisis, documentos y consentimientos del paciente que se encuentren relacionados con su tratamiento o consultas en la entidad prestadora de salud. (MINSA, 2005).

d. Métodos de archivo de Historia Clínica

Se denomina así a las diferentes técnicas que se utilizan para organizar el archivo clínico del establecimiento de salud.

Tiene por objetivo mantener un orden y reconocimiento rápido de la ubicación física de las historias clínicas de los pacientes. (MINSA, 2005).

e. Información personal de salud

Este concepto se refiere a toda aquella información perteneciente a una persona usuaria de los servicios de salud y que describe sus características físicas o mentales (MINSA, 2016), además; es el registro de sus tratamientos, operaciones, medicaciones o servicios que ha recibido por parte de la institución médica correspondiente (MINSA, 2005). Se considera que la información personal de salud puede incluir los siguientes datos:

- Información del registro del paciente.
- Información sobre los pagos o elegibilidad del paciente para utilizar los servicios de salud de la institución.
- El registro de identificación único del paciente en los sistemas de la institución.
- Cualquier información sobre el paciente que haya sido recolectada a lo largo del uso de los servicios de salud.
- Información derivada de los análisis o exámenes que se realicen al paciente o a sustancias o tejidos pertenecientes al mismo.

- Identificación de una persona como profesional de la salud al paciente. (ISO 27799, 2008)

El concepto de Información personal de salud se aplica sin tener en cuenta el medio – ya sea digital, físico o audible – en el que los datos se encuentren almacenados (MINSA, 2005). Es por este motivo que el presente plan de seguridad de la información no tendrá un alcance exclusivo hacia la información digital puesto que en las entidades prestadoras de salud aún son muchos los datos que se almacenan físicamente. (ISO 27799, 2008) (ISO 27001, 2013) (MINSA, 2005).

f. Sistema de Información de salud

Es cualquier sistema, repositorio o conjunto de datos (bases de datos, datawarehouse) que almacena información relevante sobre uno o más pacientes, se encuentra almacenada de tal forma que pueda ser transmitida de forma segura por parte de usuarios autorizados según su nivel de acceso a la misma. (ISO 27799, 2008).

2.3.2 Conceptos relacionados al proyecto

a. Activo de la Información

Es su definición básica, es cualquier cosa que tenga valor para la organización, esta puede ser de dos tipos, activos tangibles (muebles, edificios, autos) y activos intangibles (software, patentes, dato). (ISO 27000, 2016) (Delgado, 2014).

Para el desarrollo del presente trabajo, es necesario estudiar todos los activos que intervienen en el funcionamiento de la organización, centrándose en aquellos que generen, contengan o procesen información (ISO 31000, 2013). Para el sector salud encontraremos los siguientes:

1. Información de salud
2. Servicios y equipos de tecnologías de información
3. Hardware y Software de la organización
4. Servicios y equipos de comunicación
5. Dispositivos médicos que graben o generen reportes. (ISO 27000, 2016)

b. Riesgo

Un riesgo es la probabilidad de que una amenaza se aproveche de la vulnerabilidad para materializarse e impactar positiva o negativamente sobre algún evento o proceso. (ISO 31000, 2013) (ISO 27000, 2016).

A continuación reconoceremos alguno de los componentes del riesgo:

i. Evento o incidente (situación)

Referido a un evento del cual no se tiene la certeza que ocurrirá o no, identificar los posibles eventos es un factor crítico en el estudio del control de riesgos (Delgado, 2014).

ii. Activo (objeto)

Es algo que tiene valor para la organización, es el objetivo de un evento y se verá afectado por lo que ocurra dentro de este (ISO 27005, 2011).

iii. Consecuencia (daño)

Es el impacto que tiene sobre el activo, supone un daño o potencial pérdida parcial o total del activo (ISO 27005, 2011)

iv. Probabilidad

Es la medición que se realiza sobre el riesgo y tiene como resultado un valor que nos brinda una métrica para catalogar y priorizar los riesgos para definir cuál es el riesgo crítico y así generar los controles necesarios. (ISO 31000, 2013) (ISO 27001, 2013)

En el presente plan de seguridad de la información se realizará un Análisis de Riesgos el cual presenta las siguientes etapas:

1. **Identificación y valoración de activos**

Se realiza el estudio de los procesos críticos del negocio y se determinan los activos q cubren el alcance establecido. (ISO 31000, 2013). Para definir el alcance y activos críticos utilizaremos entrevistas con los dueños del proceso y documentación existente. Al culminar esta etapa se tendrá identificado los procesos y los activos sobre los cuales trabajará el Análisis de Riesgos.

2. **Identificación y valoración de riesgos**

Para este fin, se pueden utilizar el checklist, revisión de eventos e incidentes ocurridos y lluvia de ideas. Determinadas las amenazas existentes, se procede a establecer la probabilidad de ocurrencia de cada uno así como el impacto que generaría su materialización sobre los activos de información. (ISO 31000, 2013). Este último paso nos permitirá priorizar los riesgos según su criticidad o impacto en el negocio.

3. **Controles a implementar**

Establecer controles que minimicen el impacto del riesgo, o disminuyan la probabilidad de ocurrencia del mismo (ISO 27002, 2013). Mientras más controles se identifiquen para un riesgo la mitigación del mismo será mayor.

c. Seguridad de la Información

Es la protección de la información ante una gran variedad de amenazas con el fin de asegurar la continuidad del negocio, minimizar el riesgo, maximizar el retorno de inversiones y

oportunidades de negocio (Palacios Portilla, 2015). Todo ello con la finalidad de mantener las siguientes propiedades de la información:

i. Confidencialidad

Protección de la información reservada o confidencial del acceso o difusión por parte de personas naturales o jurídicas no autorizadas tanto por el dueño de la información como por parte de la entidad pública o privada que maneja la misma. (ISO 27000, 2016)

ii. Integridad

Protección de la información ante cualquier modificación o eliminación sin autorización. Con ello lograremos que la información sea la correcta en el momento que sea necesario. (ISO 27000, 2016).

iii. Disponibilidad

Es la propiedad que brindamos a la información por estar accesible en todo momento para los usuarios que puedan acceder a la misma. (ISO 27000, 2016)

iv. Autenticación

Permite la identificación de la persona que genera información, permite validar la autoría de la información por parte de un usuario específico. (ISO 27000, 2016)

En un sistema de información se suele conseguir este factor con el uso de cuentas de usuario y contraseñas de acceso (Pacheco Vargas & Fernández Peñaloza, 2014) (CNB - INDECOPI, 2007).

v. No Repudio

Asegura que las entidades no puedan negar una acción realizada, validando la acción mediante algún mecanismo que compruebe su integridad y contenido, declarándola como genuina (CNB - INDECOPI, 2014) (ISACA, 2012) (CNB - INDECOPI, 2007)

d. Sistema de Gestión de Seguridad de la Información (SGSI)

Es un modelo de gestión de seguridad basado en los tres pilares de la seguridad de la información: integridad, disponibilidad y confidencialidad, permite establecer procedimientos adecuados mediante la planificación e implantación de controles de seguridad

basados en el análisis y evaluación de riesgos (ISO 27001, 2013) además; posee un enfoque basado en procesos adoptando el ciclo de mejora continua (Palacios Portilla, 2015) (CNB - INDECOPI, 2014).

Establece políticas y procedimientos en relación a los objetivos de negocio de la organización, la decisión de su uso es una decisión estratégica de la organización para mantener un nivel menor de riesgo que la propia organización decida asumir (CNB - INDECOPI, 2014) (Palacios Portilla, 2015) (Chang Ampuero, 2011). (ISACA, 2012).

Beneficios de un SGSI:

-Involucrar a la Dirección en la seguridad de la información.
-Desarrollar políticas de cumplimiento obligatorio.
-Conocer realmente los activos de la organización.
-Cumplir con la legislación vigente ligada al proyecto.
-Realizar el análisis de riesgo para la organización.

2.4 MARCO LEGAL

El presente marco legal se sustenta por la introducción de nuevas leyes que regulan la seguridad de la información en los procesos críticos de las instituciones públicas prestadoras de servicios en salud.

Este marco legal se compone por dos documentos aprobados y vigentes:

2.4.1 Políticas de Seguridad de la Información del Ministerio de Salud.

Estas políticas se encuentran aprobados mediante Resolución Ministerial Nª 520-2006/MINSA y se alinea con la “Norma Técnica Peruana (NTP) ISO/IEC 17799:2007 Código de buenas prácticas para la gestión de la seguridad de la información” (CNB - INDECOPI, 2007) que sirvió de precedente a la Norma Técnica Peruana ISO/IEC 27001:2008 y esta a su vez a la última Norma Técnica Peruana ISO/IEC 27001: 2014.

Esta Norma Técnica (CNB - INDECOPI, 2007) presenta la información como un activo que puede ser almacenado de manera física o digital, considerando además que todo activo tiene un valor y está sujeto a riesgos que deben ser controlados mediante el uso de mecanismos adecuados que permitan mitigarlos en caso se presenten de manera concreta (Delgado, 2014) (ISO 27000, 2016).

Esta norma es un precedente a las normas que regulan en la actualidad la gestión de la seguridad de la información en el sector salud.

2.4.2 Familia de Normas ISO/IEC 27000

Este grupo o familia se enfocan en aspectos relacionados a la seguridad de la información en cualquier tipo de organización. A continuación detallaremos las normas que pertenecen a la serie 27000.

- **ISO/IEC 27001:2013**. Publicada el primero de octubre del 2013, es la norma principal de la familia de la ISO 27000, y contiene los requisitos básicos que debe tener todo sistema de gestión de seguridad de la información, especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un SGSI basado en el uso del Plan-Do-Check-Act. Incluye también los requisitos para la evaluación y tratamiento de riesgos de seguridad de la información, adaptados a las necesidades de la organización (ISO 27001, 2013) tiene 14 cláusulas que contienen 35 objetivos de control y 114 controles.

- **ISO 27002:2013**. Proporciona directivas en la gestión de seguridad de la información, incluyendo la selección e implementación de controles, describiendo sus objetivos y recomendaciones para asegurar la información. Para ello especifica 14 cláusulas, 35 objetivos de control y 114 controles. Cabe destacar que esta norma no es certificable. También se le conoce como ISO 17799 (ISO 27002, 2013) (Chávez Paz & Nepo López , 2015).

- **ISO 27005:2009**. Presenta una metodología para el análisis de riesgos, brinda información sobre cómo llevar a cabo la evaluación y el tratamiento de riesgos, quizá la etapa más difícil durante el proceso de implementación. Surge de la norma británica BS 7799-3. (ISO 27005, 2011). (Chávez Paz & Nepo López , 2015)

- **ISO 27799:2008**. Publicada el 12 de junio del 2008, es un estándar de gestión de seguridad de la información en el sector salud, aplicando la norma ISO 17799 (Actual ISO 27002). Especifica un conjunto detallado de controles para la seguridad de la información en organizaciones sanitarias. Garantiza un mínimo nivel de seguridad para mantener la confidencialidad, integridad y disponibilidad de información personal en el sector salud (ISO 27799, 2008).

Esta norma se aplica a la información de la salud en cualquiera de sus formas (grabaciones sonoras, dibujos, videos, imágenes radiológicas) sin importar la forma como son almacenados (impreso en papel, medios electrónicos) (ISO 27000, 2016)

2.4.3 NTP ISO/IEC 27001:2014

El objetivo principal de esta norma es establecer los requisitos a cumplir para la implementación del Sistema de Gestión de Seguridad de la Información basado en un enfoque a procesos. (CNB - INDECOPI, 2014)

La norma utiliza la metodología Plan-Do-Check-Act conocido también como ciclo de Daming o de mejora continua, el cual permite el mantenimiento de los controles y futuros cambios para mitigar posibles riesgos luego de la implementación del Sistema de Seguridad de la Información.

Las fases del ciclo de Deming comprenden las siguientes etapas:

1. **PLAN: Establecer el SGSI**

   Permite establecer el alcance que debe tener nuestro sistema de seguridad de la información en la organización, el cual

consiste en decidir que parte de la organización será protegida. Luego se realiza la identificación y valoración tanto de los activos como de los riesgos y amenazas a los que están expuestos. Por último, los posibles controles para mitigarlos (ISO 27001, 2013) (CNB - INDECOPI, 2014).

2. **DO (Hacer): Implementar y utilizar el SGSI**

Se detallan todas las acciones de corte técnico que se deben realizar como parte de la mitigación de los riesgos identificados (ISO 27001, 2013) (CNB - INDECOPI, 2014). Una tarea importante es la formación e información continua al personal dentro del proyecto y además se debe involucrar a todos aquellos que sean afectados por el SGSI de forma directa e indirecta (Chávez Paz & Nepo López , 2015).

3. **CHECK (Comprobar): Monitoreo y Revisión del SGSI**

Se establecen métricas que permiten evaluar la eficiencia de nuestro Sistema de Gestión de Seguridad de la Información, detectando posibles desviaciones y si es necesario, realizar cambios para mejorar su desempeño. (ISO 27001, 2013) (CNB - INDECOPI, 2014)

4. **ACT (Actuar): Mantenimiento y mejora continua**

Luego de ver los indicadores de desempeño, se identifican los cambios necesarios adoptando acciones correctoras basadas en la identificación precisa de la causa del problema, las acciones preventivas permitirán saber cuál es la fuente del problema con el objetivo de eliminarlo, y por último, definir las acciones de mejora que nos brinden una dinámica para refinar procesos y superar objetivos de seguridad continuamente (ISO 27001, 2013) (CNB - INDECOPI, 2014).

2.4.4 Ley de Protección de Datos Personales

Se refiere a la Ley Nª 29733 de Protección de datos personales, publicada en el mes de julio del 2011 (CONGRESO DE LA REPUBLICA, 2011) y aprobada su aplicación en marzo del año 2013, surge ante la necesidad de contar con un documento que regule el uso de la información personal en los procesos de negocio de todas las organizaciones en el Perú. (PODER EJECUTIVO, 2013).

Se considera dato personal a cualquier dato q puede ser utilizado para identificar a una persona natural (PODER EJECUTIVO,

2013), como ejemplo, el nombre de una persona, su sexo, origen racial, religión, etc.

El titular de los datos tiene los siguientes derechos:

- Solicitar información sobre el uso que se dará a la información que facilite.
- Solicitar acceso a la información que la organización tiene.
- Solicitar actualización, rectificación, adición o supresión de datos.
- Solicitar que su información personal no se suministre a terceros.

El principal objetivo de la norma es que las personas naturales tengan conocimiento de quien tiene acceso a su información personal, además de saber cuál es el tipo de uso que se le dará. (PODER EJECUTIVO, 2013) (PRESIDENCIA DEL CONSEJO DE MINISTROS, 2013)

CAPÍTULO III

DESARROLLO DEL PLAN DE SEGURIDAD DE LA INFORMACIÓN

En este capítulo, se describe los pasos realizados según la Norma Técnica Peruana ISO 27001:2014 para la elaboración de un plan de Seguridad de la Información para el Centro de Salud Mental Comunitario. Este plan identifica el proceso de negocio, identificación y valoración de activos y riesgos, la elaboración de un mapa de riesgos y la declaración de aplicabilidad.

3.1 Identificación del Proceso de Admisión

Un proceso es el conjunto de tareas lógicamente relacionadas que existen para obtener un resultado definido por el negocio, toman una

entrada y agregan valor para producir una salida. Estos procesos tienen clientes que pueden ser internos o externos y reciben a la salida un producto físico o un servicio. (Barros, Oscar, 1994).

El Centro de Salud Mental Comunitario San Gabriel Alto, es un establecimiento inaugurado el 14 de Julio del año 2015 y como ente prestador de servicios de salud, debe contar con todos sus procesos debidamente documentados, sin embargo, al no encontrarse dicha información en la Norma Técnica que rige al establecimiento en su última versión actualizada al mes de Julio (MINSA, 2016), urge la necesidad de levantar información para realizar el modelado del proceso de admisión acorde a la situación real de la institución.

Al analizar los procesos presentados a continuación, se puede evidenciar que la información contenida en la historia clínica es utilizada en las diversas unidades de atención (psiquiatría, psicología), enviando la historia clínica del paciente de la unidad de admisión hacia los consultorios. (MINSA, 2005).

Cabe resaltar además, la responsabilidad en la seguridad de este activo critico por parte del personal del área de admisión, área con la cual se realizó la identificación de los activos de información (ver Anexo 4 - 9) importante para el desarrollo del análisis de riesgo y determinar los controles requeridos para garantizar la seguridad de la información en el proceso de admisión de pacientes.

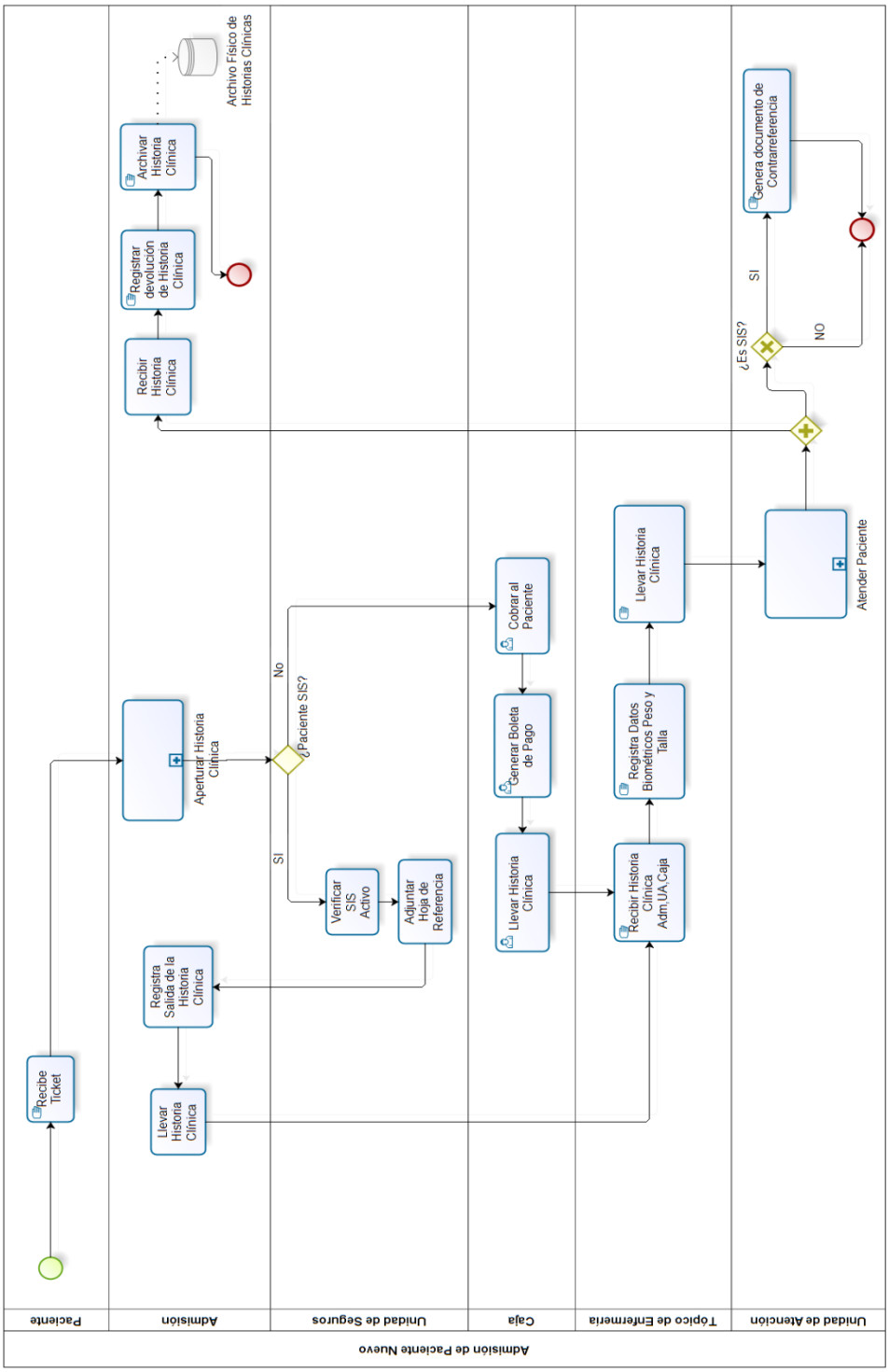
Ahora presentaremos el modelamiento utilizando la notación BPMN 2.0 mediante el apoyo de la herramienta Bizagi Modeler del proceso de admisión establecido en el alcance del proyecto. Este modelado es importante para mejorar el análisis durante el plan de seguridad de la Información, basado en la NTP ISO/IEC 27001:2014 la cual está orientado a procesos. (CNB - INDECOPI, 2014) (Chávez Paz & Nepo López , 2015).

Los subprocesos se encontraran en las secciones “Anexo 10: Subproceso del proceso de Admisión de Paciente Nuevo” y “Anexo 11: Subproceso del proceso de Admisión de Paciente Continuador”.

Modelado de Proceso de Admisión

a) Paciente Nuevo

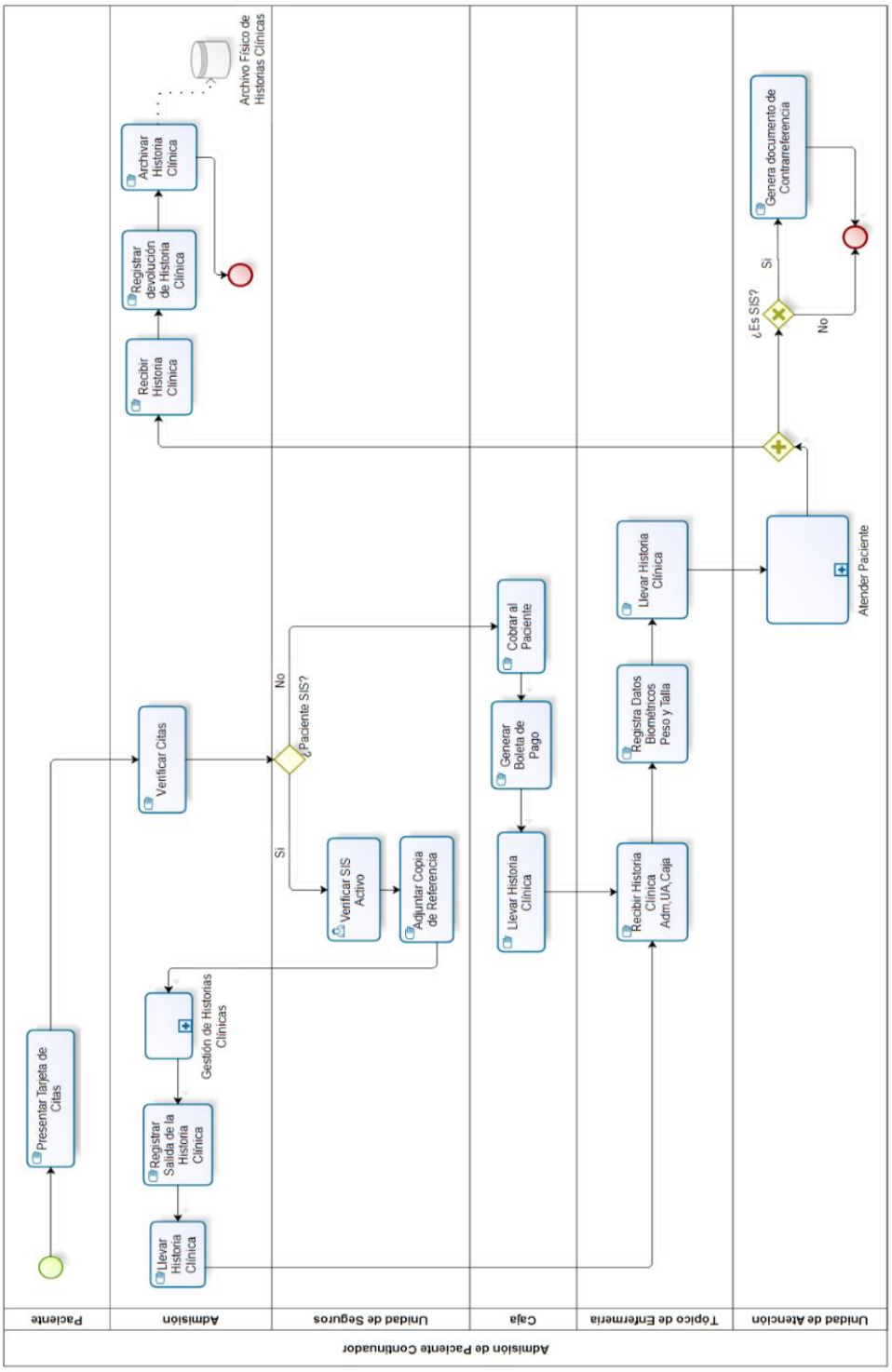
Figura 1: Proceso de negocio de Admisión de paciente nuevo



Fuente: Elaboración propia.

b) Paciente Continuador

Figura 2: Proceso de negocio de Admisión de paciente continuador



Fuente: Elaboración propia.

3.2 Análisis de Riesgos

Una vez identificados los procesos y las actividades en el área de admisión, realizaremos el análisis de riesgos de seguridad de la información, donde se identifican, valoran y estiman los diversos elementos de riesgo (Justino Salinas, 2015). Al definir criterios de aceptación y valoración de los riesgos en seguridad de la información, servirá como preámbulo al proceso de selección de controles en el área de admisión.

En el Centro de Salud Mental Comunitario es necesario establecer un control del flujo de la información que se transmite día a día a través de los procesos de negocio, la responsabilidad de salvaguardar la información es una obligación legal (PRESIDENCIA DEL CONSEJO DE MINISTROS, 2016) y es el establecimiento quien debe realizar seguimiento de los riesgos y los controles establecidos como parte del sistema de cambios (Creación de nuevas unidades de atención, cambio de personal en las diferentes jefaturas).

En el análisis de riesgos se definen las herramientas y técnicas para el análisis en seguridad de la información, se analizan los controles existentes y se define el enfoque de análisis a realizar que puede ser cuantitativo o cualitativo. (Chang Ampuero, 2011)

Según la norma ISO/IEC 27005: 2011 se definen dos enfoques:

a) Evaluación Cualitativa: La evaluación cualitativa utiliza una escala de atributos de clasificación para describir la magnitud de las posibles consecuencias por ejemplo baja, media, alta y la probabilidad de que estas consecuencias se produzcan. (ISO 27005, 2011) (ISO 31000, 2013) (Chang Ampuero, 2011).

b) Evaluación cuantitativa: La evaluación cuantitativa utiliza una escala con valores numéricos en lugar de las escalas descriptivas utilizadas en la estimación cualitativa, tanto para las consecuencias como para la probabilidad, utilizando datos de una variedad de fuentes (ISO 27005, 2011) (ISO 31000, 2013) (Chang Ampuero, 2011).

Clasificación y valoración de riesgos

Se ha considerado necesario la elaboración de una matriz de calor que considere la probabilidad de que una amenaza explote una vulnerabilidad y el impacto de dicho evento o sus consecuencias sobre el negocio. Existen dos criterios:

a) **Criterio de Probabilidad**: Posibilidad de ocurrencia de riesgo, se puede medir con criterios de frecuencia basado en intervalos de tiempo.

Tabla 1: Calificación de Probabilidad

Calificación	Descripción
1	Rara
2	Poco probable
3	Posible
4	Muy probable
5	Casi certeza

Fuente: (ISO 27005, 2011)

a.1) Tipificación

Tabla 2: Tipificación de la Calificación de probabilidad

Criterio de Probabilidad				
Rara	Poco Probable	Posible	Muy Probable	Casi certeza
Frecuencia de ocurrencia muy baja, ocurrencia muy remota.	Frecuencia de ocurrencia baja (un evento 2 a 5 años).	Frecuencia de ocurrencia media (un evento cada 1 a 2 años).	Frecuencia de ocurrencia bimensual.	Frecuencia de ocurrencia mensual, alta certeza que ocurra dicho evento.

Fuente: (ISO 27005, 2011)

b) Criterio de Impacto: Consecuencias que puedan ocasionar la materialización del riesgo en la organización.

Tabla 3: Calificación de Impacto

Calificación	Descripción
1	Muy Bajo
2	Bajo
3	Medio
4	Alto
5	Muy Alto

Fuente: (ISO 27005, 2011)

b.1) Tipificación

Tabla 4: Tipificación de la Calificación de Impacto

Criterio de Impacto				
Muy Bajo	Bajo	Medio	Alto	Muy Alto
La información afectada es de dominio público (citas generadas, recetas médicas).	La información afectada tiene un bajo impacto en la atención del paciente. Retarda su atención.	La Información afectada paraliza el servicio 1 día.	La información afectada paraliza el servicio por una semana, se filtra o se pierde información personal.	La información afectada inhabilita al servicio por más de una semana, se filtra o se pierde información personal.

Fuente: Elaboración propia

c) Matriz de calor

Es una matriz que muestra la relación entre la probabilidad e impacto, con ello se medirá el riesgo.

Tabla 5: Matriz de calor utilizado para la valoración de riesgos identificados en el proyecto

Probabilidad de Materialización		Nivel de Impacto				
		Muy Bajo	Bajo	Medio	Alto	Muy Alto
		1	2	3	4	5
Casi certeza	5					
Muy probable	4					
Posible	3					
Poco probable	2					
Rara	1					

Fuente: Elaboración propia

d) Matriz cualitativa

Permite identificar y evaluar los riesgos, los cuales son calculados por una combinación de valores y niveles de requerimiento de seguridad, con esta comparación se trataran los riesgos y se tomaran decisiones de acuerdo a la normativa legal vigente, reglamento del establecimiento de salud, etc.

Tabla 6: Matriz Cualitativa para la evaluación de riesgos

Probabilidad de Materialización		Nivel de Impacto				
		Muy Bajo	Bajo	Medio	Alto	Muy Alto
		1	2	3	4	5
Casi certeza	5	Moderado	Alto	Alto	Extremo	Extremo
Muy probable	4	Bajo	Moderado	Alto	Alto	Extremo
Posible	3	Bajo	Moderado	Moderado	Alto	Alto
Poco probable	2	Bajo	Bajo	Moderado	Moderado	Moderado
Rara	1	Bajo	Bajo	Bajo	Bajo	Moderado

Fuente: (ISO 27005, 2011)

e) Apetito por el riesgo

Es el nivel del riesgo que una organización está dispuesta a aceptar sin necesidad de establecer controles especiales que los mitiguen dado que su impacto es bajo en relación a los procesos de negocio. En nuestro caso de estudio, el centro de salud mental es una organización joven, por ello el apetito por el riesgo será de un nivel bajo.

f) Riesgo residual

Es el riesgo que no podrá ser mitigado con el uso de controles, este se mantiene a pesar de los controles implementados. En organizaciones nuevas, se suele comparar con el apetito por el riesgo, siendo de nivel bajo.

3.3 Valoración de Activos

Una vez establecido la gestión de riesgos identificados con los procesos de negocios en el área de admisión, es necesario establecer un estudio sobre los activos de la información que participan en estos procesos con la finalidad de contar con un inventario de activos y una medida de valor para el negocio como entes de soporte y transmisión de información.

a. Identificación de activos.

Con la identificación de los procesos, y el apoyo del personal “dueño del negocio”, se identificó los activos de la información utilizados y su respectiva clasificación en las siguientes categorías:

1. **Activos Primordiales:** Aquellos que participan directamente en el flujo de información de los procesos identificados en el alcance de nuestro proyecto.

2. **Activos no Primordiales:** Aquellos activos que brindan un soporte al flujo de la información y a los activos primordiales.

Como ya se indicó anteriormente, el establecimiento de salud tiene un año de iniciadas sus actividades, por ello, se realizó esta identificación con el personal que se encuentra en el área de admisión desde su fundación, logrando establecer una escala

cuantitativa que medirá el nivel en que una pérdida o falla en el activo afecte alguno de los pilares de la seguridad de la información –Confidencialidad, Disponibilidad, Integridad-

En el desarrollo de los procesos identificados, la información personal que manejan los establecimientos de salud es de vital importancia en nuestro plan de seguridad de la información, por ello, es necesaria la identificación de los activos vinculados a esos procesos, asegurando que estas entidades deben cumplir los siguientes requisitos:

1. Reglas de carácter legal para el óptimo manejo de la información en salud. Se determinan varias directivas en la Norma Técnica de Historias Clínicas (MINSA, 2005) y en la ley de protección de datos personales (CONGRESO DE LA REPUBLICA, 2011) (PODER EJECUTIVO, 2013)

2. Responsabilidad legal y ética sobre los activos de la información (PODER EJECUTIVO, 2015)**.**

3. Personal dedicado a la custodia de la información en los procesos identificados.

Tabla 7: Inventario de activos de información

Nro. Activo	Proceso de negocio identificado	Nombre del activo	Descripción del Activo	Clasificación del activo	Propietario del Activo	Valoración Parcial			Valoración Final
						C	I	D	
A01	Admisión de pacientes	Archivo físico de Historias Clínicas	Archivo de Historias Clínicas del tipo Activo, las cuales son requeridas frecuentemente.	Activo Primordial	Admisión	4	4	4	4
A02	Admisión de pacientes	Boleta de atención	Documento que detalla la información para realizar el pago de la cita por el paciente.	Activo no Primordial	Paciente	1	1	1	1
A03	Admisión de pacientes	Tarjeta de citas	Documento que permite seguir la programación de citas del paciente en las unidades de atención	Activo Primordial	Paciente	2	2	1	2
A04	Admisión de pacientes	Cuaderno que registra entradas y salidas de las Historias Clínicas hacia las unidades de atención	Cuaderno que contiene en detalle el ingreso y salida de las historias clínicas desde la unidad de Admisión hacia el consultorio para la atención de pacientes	Activo Primordial	Admisión	2	3	4	3
A05	Admisión de pacientes	Computadora de escritorio	Equipo de cómputo instalado utilizado por el área de admisión para la verificación de afiliación de pacientes SS y registro y conteo de Historias Clínicas.	Activo no Primordial	Área de Unidades de Atención	3	_	2	3
A06	Admisión de pacientes	Historia Clínica	Documento legal -NTP Historia Clínica- que contiene las atenciones, diagnósticos y exámenes recibidas por el paciente	Activo Primordial	Archivo	4	4	4	4

b. Valorización de activos.

Una vez identificado los activos, el siguiente paso a realizar es la escala de valoración, determinando cuantitativamente el valor que tienen para la organización y cuál es su importancia dentro de ella, por lo tanto deben ser protegidos.

Se valorará una escala cuantitativa de cuerdo a los criterios de disponibilidad (D), integridad (I) y confidencialidad (C), siendo el número 1 el de menor relevancia “muy poco” y el numero 4 el más relevante “muy alto”.

El valor promedio de las tres medidas realizadas para cada activo de información determinará el valor del impacto general del activo. Con un valor promedio de impacto mayor o igual a 3 son sobre los que se debe realizar el análisis de riesgos asociados. Buscando establecer controles que los protejan de las amenazas persistentes asegurando así la información.

Tabla 8: Escala de valoración de activos de información

Valor en escala Likert	Pilares de Seguridad de la Información		
	Confidencialidad	Integridad	Disponibilidad
1	La publicación o filtración de la información no presenta un riesgo para la organización. Se puede considerar como información de dominio público	Si la información presentada en el activo no es correcta o tiene un porcentaje de error del 25% no presenta un riesgo para la organización dado que no afecta de manera critica las actividades de la misma	En caso se requiera el activo de información debe poder ser accesible un 25% de las ocasiones en que se haga necesario, sin embargo su no disponibilidad por distintos factores no se considera un riesgo
2	El activo de información debería ser solo de uso interno a la organización, sin embargo su filtración no supone un riesgo o un daño para la misma	Se requiere que el activo tenga un porcentaje de error como máximo del 50%, dado que un porcentaje mayor podría perjudicar a la organización.	El activo de información debe ser accesible el 50% de las veces en que se requiera, caso contrario podría perjudicar de manera leve a la organización.
3	El activo de información contiene información de índole privada, debiendo establecer controles para el acceso al mismo. Su filtración supone un riesgo moderado para la organización	El activo de información debe contener información correcta en un 75%, caso contrario se podría generar un daño moderado a la organización o incluso iniciar acciones legales contra la misma	Se requiere que sea accesible el 75% de las ocasiones en que se necesite, de lo contrario perjudica moderadamente los procesos de negocio asociados al mismo pudiendo llevar a consecuencias legales.
4	La información contenida por el activo es altamente sensible y debe ser protegida contra cualquier posible filtración, caso contrario los dueños de la información contenida pueden ser afectados y la organización ser demandada o multada.	La información no debe contener errores, de otro modo se afecta seriamente los procesos de negocio asociados, siendo susceptible la organización a ser demandada o multada.	La información contenida en el activo de información no puede ser inaccesible dada su criticidad. Su no disponibilidad se traduce en una paralización de las actividades asociadas ocasionando pérdidas serias o acciones legales en contra de la organización.

3.4 Mapa de Riesgos

Con la documentación obtenida de la metodología de Análisis de Riesgos y valoración de activos, ambos documentos serán puestos en práctica en el Mapa de Riesgos Identificados.

Para empezar el análisis de riesgos mediante una metodología de análisis de riesgos, realizaremos una valoración basada en la probabilidad de ocurrencia y el impacto que pueda tener un incidente que afecte dicho activo. Por último, se podrá establecer la estrategia a utilizar según el apetito de la empresa y de las posibilidades de la misma.

3.4.1 Identificación de Activos

Haciendo uso del mapa de procesos, se realiza un análisis de los activos de información asociados a lo largo de las actividades en los procesos del área de admisión.

Identificados los activos, se procede a clasificarlos, determinando el propietario del activo, la valoración del impacto respecto a la disponibilidad, integridad y confidencialidad y su valoración según el impacto que genere la pérdida o daño de este al proceso de negocio siguiendo la metodología de valoración de activos.

3.4.2 Identificación y Análisis de Riesgos

Luego de haber realizado la identificación de los activos, así como su valoración para determinar su criticidad, se procede a realizar el análisis de riesgos sobre las actividades que se identificaron en el modelado de procesos del alcance del proyecto.

Hacemos uso de la metodología de Análisis de Riesgos, con el cual haremos una revisión de los riesgos a los que dichas actividades están expuestas, determinando los factores que lo originan, sus consecuencias y la evaluación del mismo que nos permitirá definir el tratamiento o aceptación del apetito del riesgo de la institución.

La matriz de riesgos desarrollada puede encontrarse en el “Anexo 13: Matriz de Riesgos. Proceso de admisión de paciente nuevo” y en el “Anexo 14: Matriz de Riesgos. Proceso de admisión de paciente continuador”.

3.5 Declaración de Aplicabilidad

La declaración de aplicabilidad o SOA (Statement of Applicability) (ISO 27001, 2013) hace referencia a la cláusula 6.1.3d de la Norma Técnica Peruana ISO/IEC 27001:2014 y describe los objetivos de control, controles

relevantes y aplicables al Plan de Seguridad de la Información del Centro de Salud Mental Comunitario y en función de la política y conclusiones del proceso de evaluación y tratamiento del riesgo.

La declaración de aplicabilidad puede encontrarse en el “Anexo 15: Matriz de aplicabilidad”.

CONCLUSIONES

Habiendo finalizado el plan de seguridad de la información, se ha podido llegar a las siguientes conclusiones:

El Centro de Salud Mental comunitario es un centro de atención que pertenece a la Red de Salud SJM – VMT, durante mis continuas visitas para recabar la información (acceso a documentos, recojo de evidencias) siempre se tuvo la disposición de la Jefa del Establecimiento, ella mostro todo su interés y conocimiento en el manejo de las nuevas normas y la necesidad imperiosa de regular las estrategias como institución hacia una política de seguridad de la información.

El Ministerio de Salud como miembro del Sistema Nacional de Informática, debió nombrar un comité de seguridad de la información en los establecimientos desde los de menor a mayor complejidad apenas publicada la Norma Técnica Peruana ISO/IEC 27001:2014. (PRESIDENCIA DEL CONSEJO DE MINISTROS, 2016). La importancia de nombrar este comité radica en que recaerá sobre su responsabilidad la implementación del Sistema de Gestión de Seguridad de la Información.

Los colaboradores no mostraron ninguna resistencia al cambio, por el contrario, durante el proceso de levantamiento de información, se conversó con la encargada de admisión, enfermería y triaje y todos mostraron la disponibilidad de concurrir a futuras capacitaciones sobre

aspectos legales vigentes respecto al manejo de los principales activos de la información en el proceso crítico de admisión de pacientes.

La gestión de Historias Clínicas son procedimientos que se encuentran normados y presentan un marco regulatorio en el cual toda entidad que brinda servicios de salud debe seguir, dentro de estas exigencias, indica que la información recolectada de los pacientes debe ser almacenada en formato físico (MINSA, 2005). En la actualidad, el establecimiento no cuenta con controles implementados para mantener los documentos físicos (activos críticos) bajo los tres pilares de la seguridad de la información (Integridad, disponibilidad y confidencialidad).

Se verificó que las medidas actuales para asegurar estos documentos no cumplen los requisitos mínimos para el acceso físico al área de admisión (ingresa personal de otras unidades de atención) además, no se cuenta con la señalización de seguridad ante desastres y lo más crítico aún, no se cuenta con extintores, ambos requerimientos se evidencian mediante el OFICIO No 022 – 2016 “Solicito extintores y señalización de seguridad” (Ver Anexo 1).

RECOMENDACIONES

Se recomienda como medida temporal que se establezca un comité de seguridad de la información liderado por la Jefatura de la Oficina de Estadística e Informática en conjunto con la Red de Salud San Juan de Miraflores – Villa María del Triunfo. Este comité debe contar con profesionales capacitados y certificados en seguridad de la información para el control y mantenimiento del SGSI, ejecutando lo desarrollado en este proyecto.

Se recomienda capacitar al personal integrante del comité de modo que puedan conocer los conceptos fundamentales del SGSI, asi como la implementación y sus distintas fases, haciendo extensiva la importancia del mismo en sus respectivas áreas de atención

Se recomienda que los demás centros de salud conectados a la Red de Salud San Juan de Miraflores – Villa María del triunfo adopten está el presente plan de seguridad de la información como una herramienta que les permita salvaguardar sus activos críticos (historias clínicas).

Se recomienda utilizar un proceso de digitalización de los archivos y documentos importantes dentro del establecimiento de salud para fines asistenciales. Por normativa vigente, la información almacenada de los pacientes debe realizarse de manera física (MINSA, 2005), esto pone en

peligro la información que allí se guarda ante siniestros que pueden ocurrir (incendios).

Se recomienda brindar asesoría a los profesionales de la salud en cuanto a las medidas de seguridad de la información a implementar para proteger la historia clínica de daños diversos a los que está expuesta durante el proceso de alcance identificado.

Se recomienda a todos los establecimientos de salud contar con el modelado de sus procesos de negocio, revisando sus riesgos y actualizando sus controles, ello garantizará el apropiado manejo de los activos de información evitando incidentes que afecten, disponibilidad, integridad y confidencialidad.

Se recomienda que la Unidad de Estadística e Informática de la Red de Salud SJM - VMT, entidad macro a la cual el Centro de Salud pertenece, este a cargo de un profesional con perfil en seguridad de la información y necesariamente un ingeniero en sistemas de información. A la fecha, esta unidad está a cargo de un médico que no cuenta con el perfil para ser un agente activo en el proceso de planificación e implementación de un Plan de Seguridad de la Información, como prueba de ello; la unidad de informática se encuentra acéfala hace más de 5 meses, dejando las funciones al personal técnico que desarrolla las actividades diarias de soporte la cual está distribuida en dos profesionales técnicos no universitarios.

BIBLIOGRAFÍA

Barros, Oscar. (1994). Reingeniería de Procesos de Negocio, 56. Chile: Editorial Dolmen.

Briceño Ortega, D. (Abril de 2009). Mejora del proceso software de una pequeña empresa desarrolladora de software: Caso competisoft-Perú-Omega. Tesis para optar por el Título de Ingeniero Informático. Lima.

Camarena Gil, M. C., Pedreschi Núñez , J. M., & Rondón Suasnabar, S. S. (2008). Análisis, Diseño y Construcción de una Herramienta para Modelado de Procesos: MJS Process Designer. Tesis para optar el Título de Ingeniero Informático. Lima.

Chang Ampuero, C. (2011). Diseño de un Sistema de Gestión de Seguridad de la Informacion para una compañia de seguros. Tesis para optar el titulo de Ingeniero Informático. Lima: PUCP.

Chávez Paz , J. H., & Nepo López , G. A. (Julio de 2015). Sistema de Gestión de Seguridad de Información basado en la Norma ISO/IEC 27001 para la Superintendencia de Transporte Terrestre de Personas, Carga y Mercancías (SUTRAN) – Región Lambayeque. Tesis para optar por el Título de Ingeniero en Computación e Informática. Lambayeque.

CNB - INDECOPI. (16 de Enero de 2007). NTP-ISO/IEC 17799: 2007. Tecnología de la información. Código de buenas prácticas para la gestión de la seguridad de la información. Lima.

CNB - INDECOPI. (20 de Noviembre de 2014). NTP-ISO/IEC 27001: 2014. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos. Lima

.

CONGRESO DE LA REPUBLICA. (2011). Ley 29733. Ley de proteccion de datos personales. Lima

.

Delgado, M. F. (2014). Oficina Nacional de Gobierno Electrónico e Informática. Taller de Gestión de Riesgos. Lima.

Freund , J., Rucker, B., & Hitpass, B. (2014). BPMN 2.0 Manual de referencia y guía práctica. Santiago , Chile.

Gonzáles Aguado, F., & Castejón Bellmunt, M. A. (2016). Proyecto para el desarrollo del Centro de Salud Mental Comunitario "San Gabriel Alto" Un modelo para el trabajo comunitario de los CSMC en las Redes de Salud. Villa Maria del Triunfo.

Henarejos, A. S., Fernández Alemán, J. L., & Toval, Á. A. (2013). Recomendaciones sobre Seguridad y Privacidad Informática en el Tratamiento de Datos de Salud. Murcia.

ISACA. (2012). CISM - Certified Information Security Manager - Review Manual 2013. ISACA
.
ISO 27000. (2016). ISO/IEC 27000 Information technology - Security techniques - Information security management systems - Overview and vocabulary.

ISO 27001. (2013). ISO 27001:2013. Information technology – Security techniques - Information security management systems - Requirements.

ISO 27001. (2013). ISO 27001. (2013). ISO 27001:2013. Information technology – Security techniques -- Information security management systems -- Requirements.

ISO 27002. (2013). ISO 27002:2013. Information technology - Security techniques - Code of practice for information security control.

ISO 27005. (2011). Information technology - Security techniques - Information security risk management.

ISO 27799. (2008). ISO 27799:2008. Health Informatics - Information security - management in health using ISO/IEC 27002
.
ISO 31000. (2013). ISO 31000:2009. Risk management - Principles and guidelines.

Justino Salinas, Z. (Febrero de 2015). Diseño de un Sistema de Gestión de Seguridad de la Información para una empresa inmobiliaria alineado a la Norma ISO/IEC 27001:2013. Lima.

María Fátima Cueva Murillo. (Marzo de 2015). Diseño de un sistema de gestion de continuidad de negocios para una entidad estatal de salud bajo la optica de la ISO/IEC 22301:2012. Lima.

MIDIS. (19 de Febrero de 2016). R.M. Nº 036-2016.Constitución del Comité de Gestión de Seguridad de la Información, 2. Lima.

MIDIS. (21 de Julio de 2016). Política Social es gestionada con Calidad: El MIDIS y sus programas sociales reciben Certificación Internacional ISO 9001:2008 e ISO 27001:2013. Obtenido de Oficina General de Información Estratégica: http://www.midis.gob.pe/index.php/es/centro-de-informacion/2049-politica-social-es-gestionada-con-calidad-el-midis-y-sus-programas-sociales-reciben-certificacion-internacional-iso-9001-2008-e-iso-27001-2013

MIDIS. (19 de Febrero de 2016). R.M. Nº 036-2016. Funciones del Comité de Gestión de Seguridad de la Información. Lima.

MINSA. (2005). N.T. Nº 022-MINSA/DGSP-V.02. Norma Técnica de la Historia Clinica de los Establecimientos de Salud. Lima.

MINSA. (30 de Junio de 2016). Anteproyecto norma técnica de salud de los centros de salud mental comunitarios V.08. Lima.

Pacheco Vargas, O. A., & Fernández Peñaloza, D. A. (2014). Mejora de Seguridad de la información en la comandancia de operaciones guardacostas basada en la Norma Técnica Peruana NTP-ISO/IEC 27001:2008. Tesis para optar el título profesional de Ingeniero de Computación y Sistemas. Lima, Perú.

Palacios Portilla, D. O. (2015). DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN. Tesis de grado para optar el título de:. San Juan de Pasto.

PODER EJECUTIVO. (2013). Reglamento de la ley Nº 29733, ley de proteccion de datos personales.

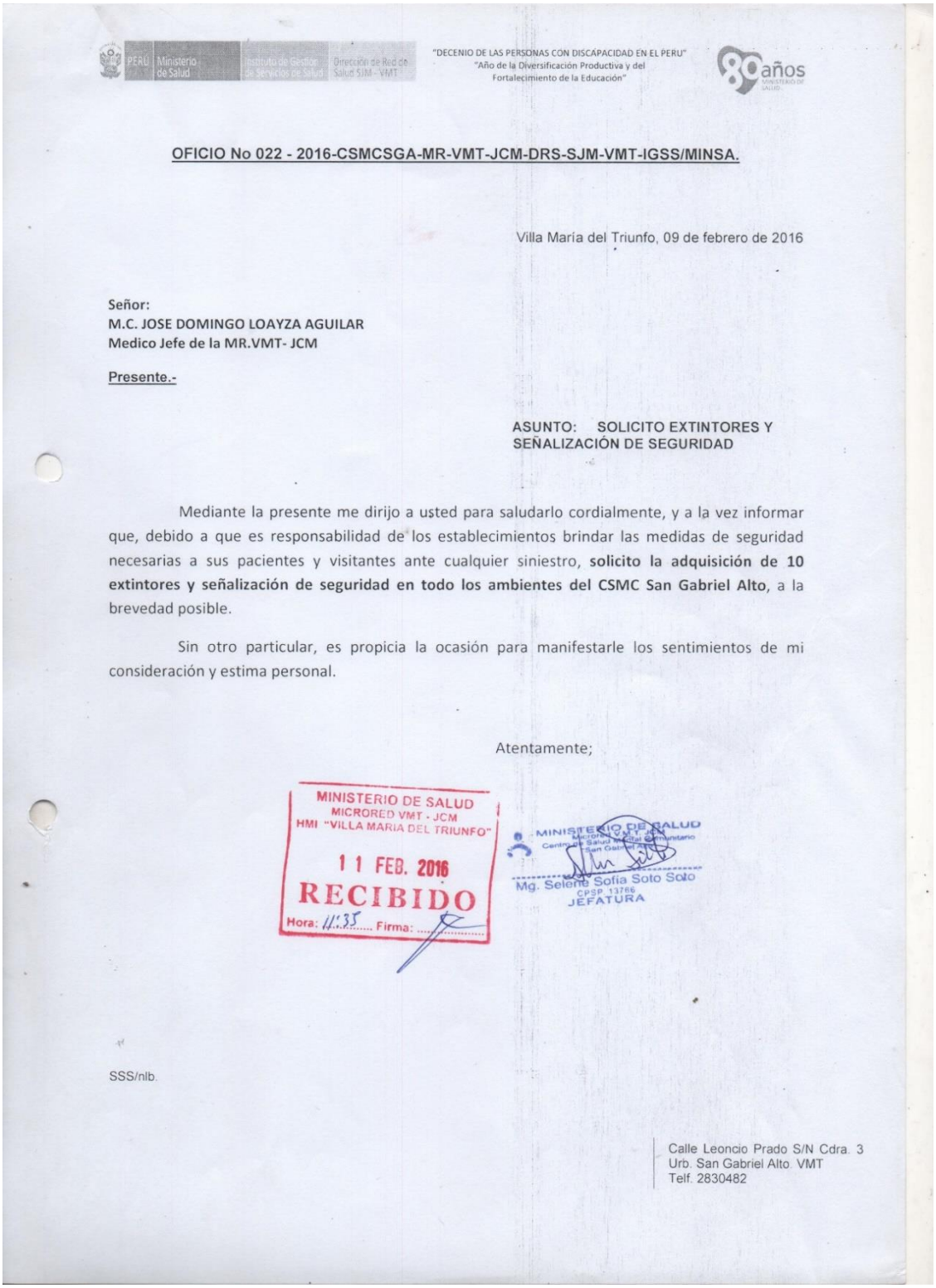
PODER EJECUTIVO. (13 de Agosto de 2015). Reglamento de ley Nª 29414, ley que establece los derechos de las personas usuarias de los servicios de salud, pág. 2.

PRESIDENCIA DEL CONSEJO DE MINISTROS. (10 de Julio de 2013). D.S Nº081-2013. Decreto Supremo mediante el cual se aprueba la Política Nacional de Gobierno Electrónico 2013- 2017.

PRESIDENCIA DEL CONSEJO DE MINISTROS. (14 de Enero de 2016). Aprueban el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Informacion. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos.2a. Edición" . Lima.

ANEXOS

Anexo 1: Oficio de solicitud de extintores y señalización de seguridad



PERÚ | Ministerio de Salud | Instituto de Gestión de Servicios de Salud | Dirección de Red de Salud SJM - VMT

"DECENIO DE LAS PERSONAS CON DISCAPACIDAD EN EL PERU"
"Año de la Diversificación Productiva y del Fortalecimiento de la Educación"

80 años MINISTERIO DE SALUD

OFICIO No 022 - 2016-CSMCSGA-MR-VMT-JCM-DRS-SJM-VMT-IGSS/MINSA.

Villa María del Triunfo, 09 de febrero de 2016

Señor:
M.C. JOSE DOMINGO LOAYZA AGUILAR
Medico Jefe de la MR.VMT- JCM

Presente.-

ASUNTO: SOLICITO EXTINTORES Y SEÑALIZACIÓN DE SEGURIDAD

Mediante la presente me dirijo a usted para saludarlo cordialmente, y a la vez informar que, debido a que es responsabilidad de los establecimientos brindar las medidas de seguridad necesarias a sus pacientes y visitantes ante cualquier siniestro, **solicito la adquisición de 10 extintores y señalización de seguridad en todo los ambientes del CSMC San Gabriel Alto**, a la brevedad posible.

Sin otro particular, es propicia la ocasión para manifestarle los sentimientos de mi consideración y estima personal.

Atentamente;

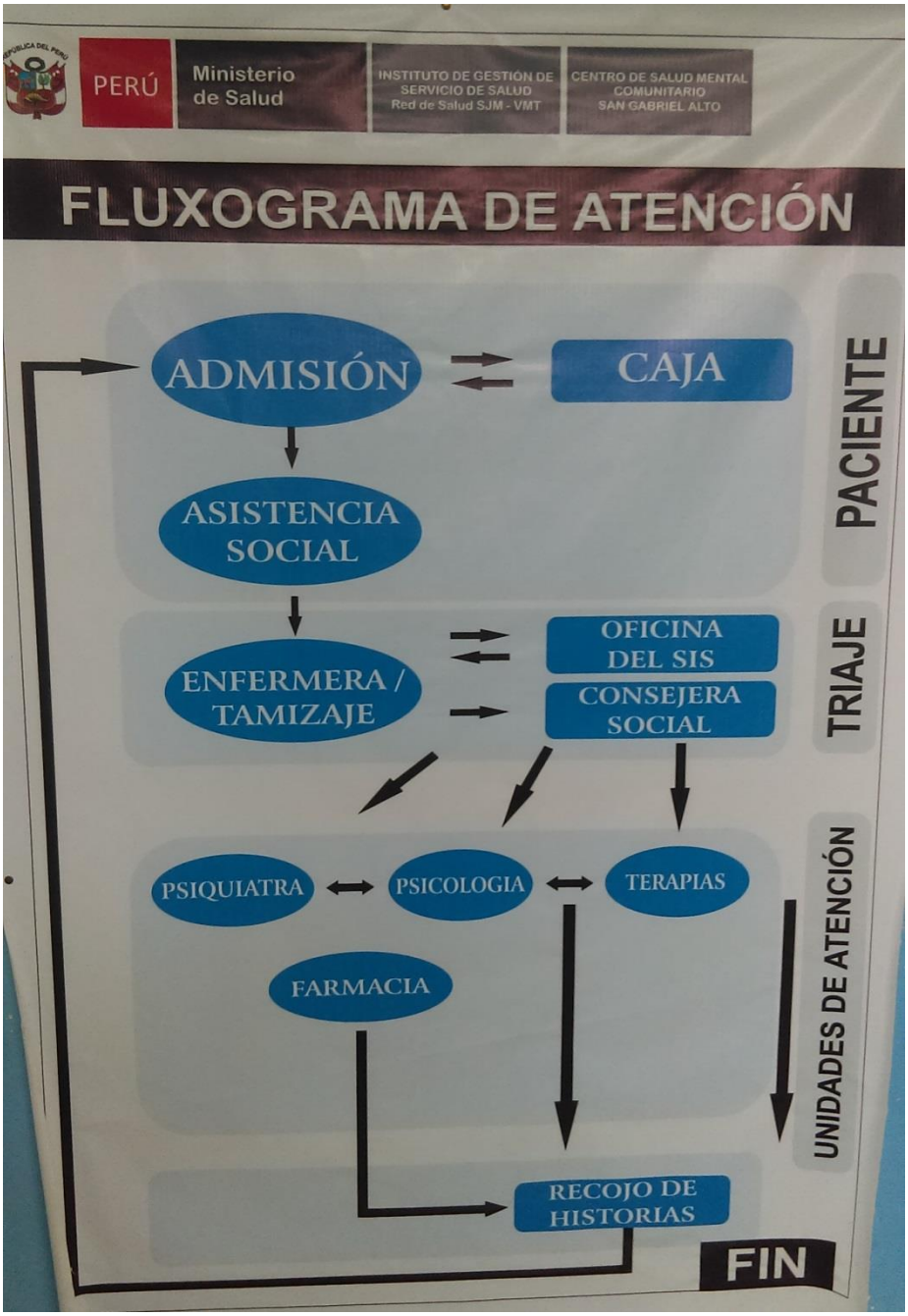
MINISTERIO DE SALUD
MICRORED VMT - JCM
HMI "VILLA MARIA DEL TRIUNFO"
11 FEB. 2016
RECIBIDO
Hora: 11:35 Firma:

MINISTERIO DE SALUD
Mg. Selene Sofía Soto Soto
CPSP 13766
JEFATURA

SSS/nlb.

Calle Leoncio Prado S/N Cdra. 3
Urb. San Gabriel Alto. VMT
Telf. 2830482

Anexo 2: Flujograma de Atención



Anexo 3: Costos del servicio por Unidades de Atención

PERÚ Ministerio de Salud | Instituto de Gestión de Servicios de Salud | Dirección de Red de Salud SJM - VMT

"DECENIO DE LAS PERSONAS CON DISCAPACIDAD EN EL PERU"
"Año de la Diversificación Productiva y del Fortalecimiento de la Educación"

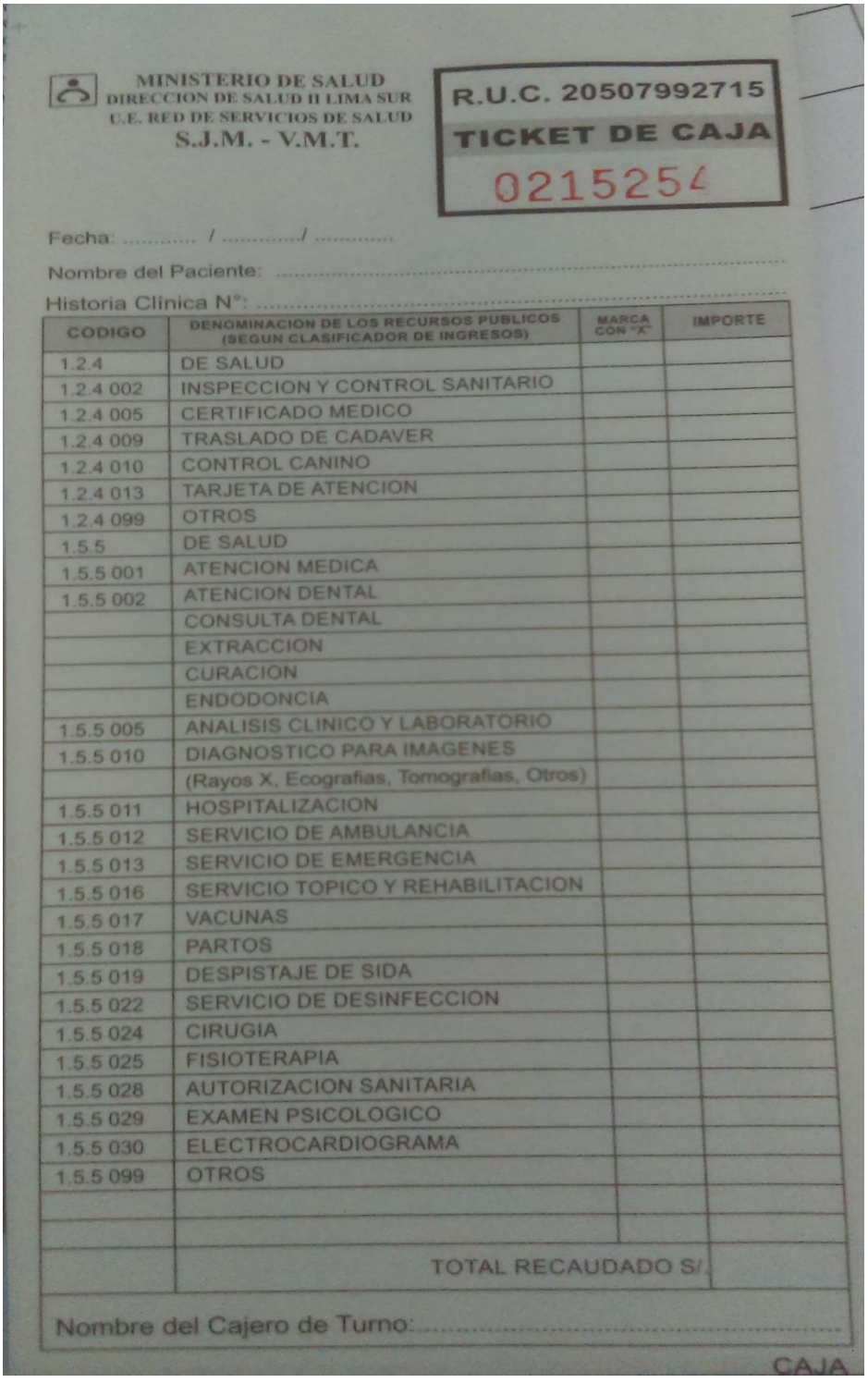
80 años MINISTERIO DE SALUD

TARIFARIO SOCIAL

CONCEPTO	TARIFA SOCIAL
CONSULTA PSIQUIATRICA	6.00
CERITIFICADO PSIQUIATRICO	25.00
TERAPIA PSIQUIATRICA	10.00
CONSULTA PSICOLÓGICA	5.00
EVALUACIÓN PSICOLOGICA	10.00
TERAPIA PSICOLÓGICA	10.00
TERAPIA PAREJA Y FAMILIA	15.00
TERAPIA GRUPAL	10.00
INFORME PSICOLÓGICO	15.00

Calle Leoncio Prado S/N Cdra. 3 Urb. San Gabriel Alto. VMT
Telf. 2830482

Anexo 4: Comprobante de pago



MINISTERIO DE SALUD
DIRECCION DE SALUD II LIMA SUR
U.E. RED DE SERVICIOS DE SALUD
S.J.M. - V.M.T.

R.U.C. 20507992715
TICKET DE CAJA
0215254

Fecha: ..... / ...../ .....

Nombre del Paciente: .....

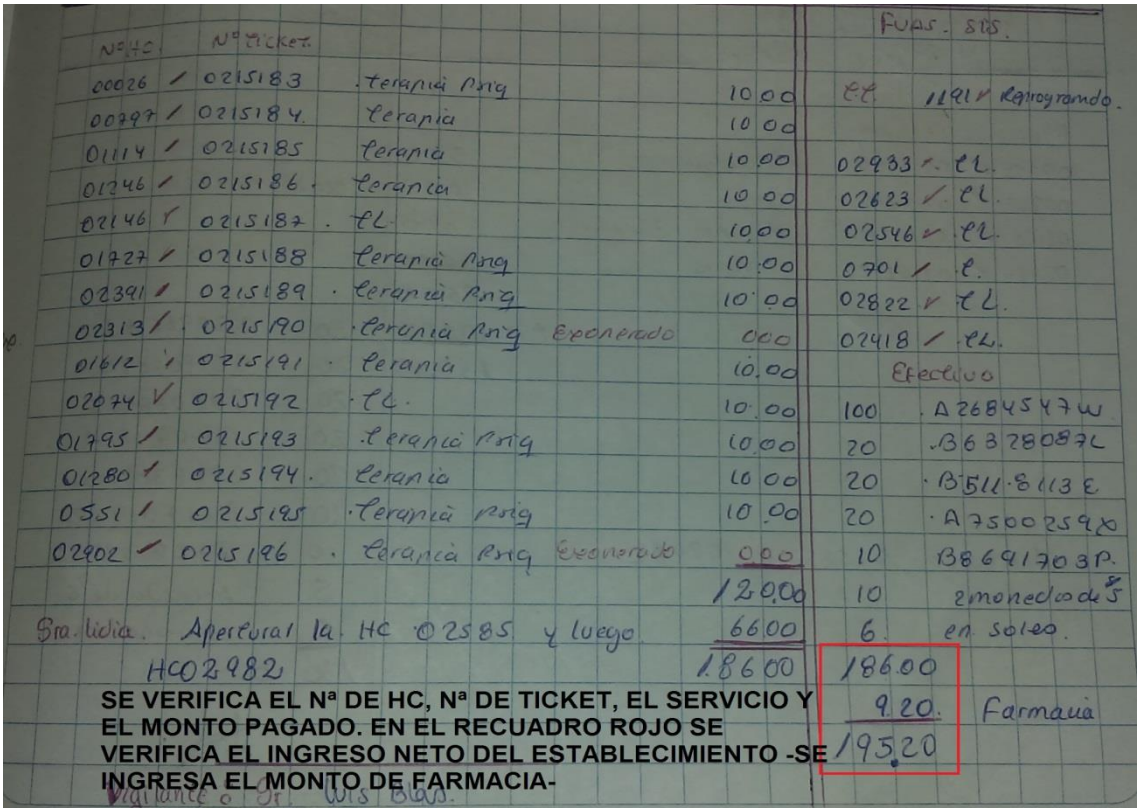
Historia Clínica N°: .....

CODIGO	DENOMINACION DE LOS RECURSOS PUBLICOS (SEGUN CLASIFICADOR DE INGRESOS)	MARCA CON "X"	IMPORTE
1.2.4	DE SALUD		
1.2.4 002	INSPECCION Y CONTROL SANITARIO		
1.2.4 005	CERTIFICADO MEDICO		
1.2.4 009	TRASLADO DE CADAVER		
1.2.4 010	CONTROL CANINO		
1.2.4 013	TARJETA DE ATENCION		
1.2.4 099	OTROS		
1.5.5	DE SALUD		
1.5.5 001	ATENCION MEDICA		
1.5.5 002	ATENCION DENTAL		
	CONSULTA DENTAL		
	EXTRACCION		
	CURACION		
	ENDODONCIA		
1.5.5 005	ANALISIS CLINICO Y LABORATORIO		
1.5.5 010	DIAGNOSTICO PARA IMAGENES		
	(Rayos X, Ecografias, Tomografias, Otros)		
1.5.5 011	HOSPITALIZACION		
1.5.5 012	SERVICIO DE AMBULANCIA		
1.5.5 013	SERVICIO DE EMERGENCIA		
1.5.5 016	SERVICIO TOPICO Y REHABILITACION		
1.5.5 017	VACUNAS		
1.5.5 018	PARTOS		
1.5.5 019	DESPISTAJE DE SIDA		
1.5.5 022	SERVICIO DE DESINFECCION		
1.5.5 024	CIRUGIA		
1.5.5 025	FISIOTERAPIA		
1.5.5 028	AUTORIZACION SANITARIA		
1.5.5 029	EXAMEN PSICOLOGICO		
1.5.5 030	ELECTROCARDIOGRAMA		
1.5.5 099	OTROS		
	TOTAL RECAUDADO S/.		

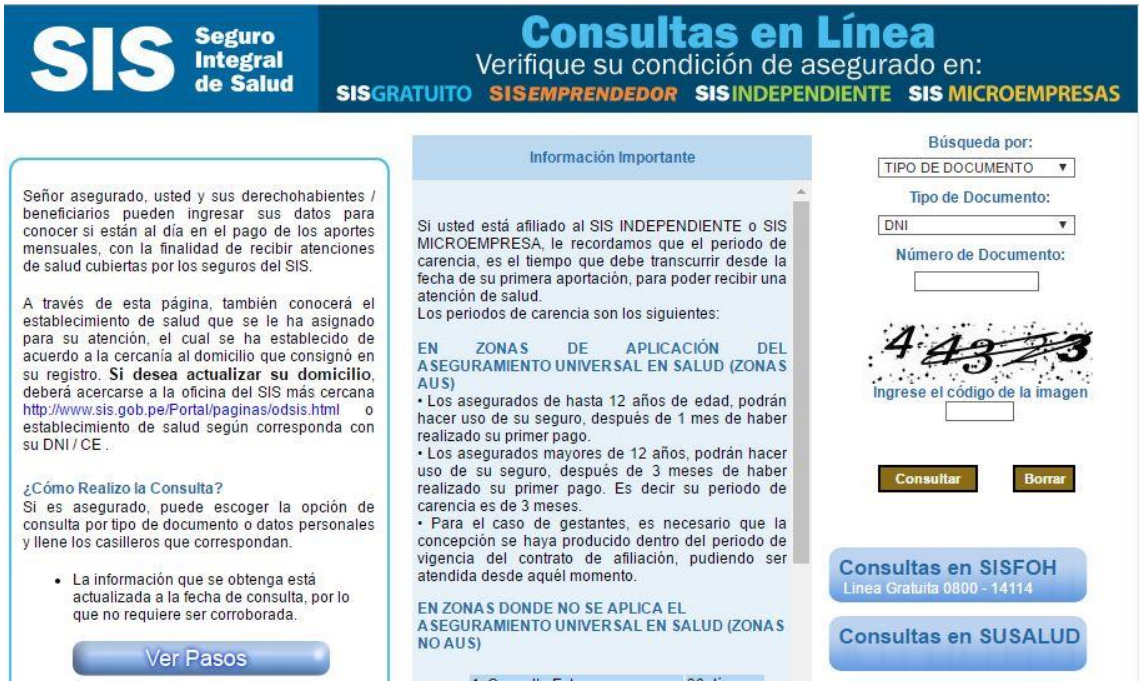
Nombre del Cajero de Turno:.....

CAJA

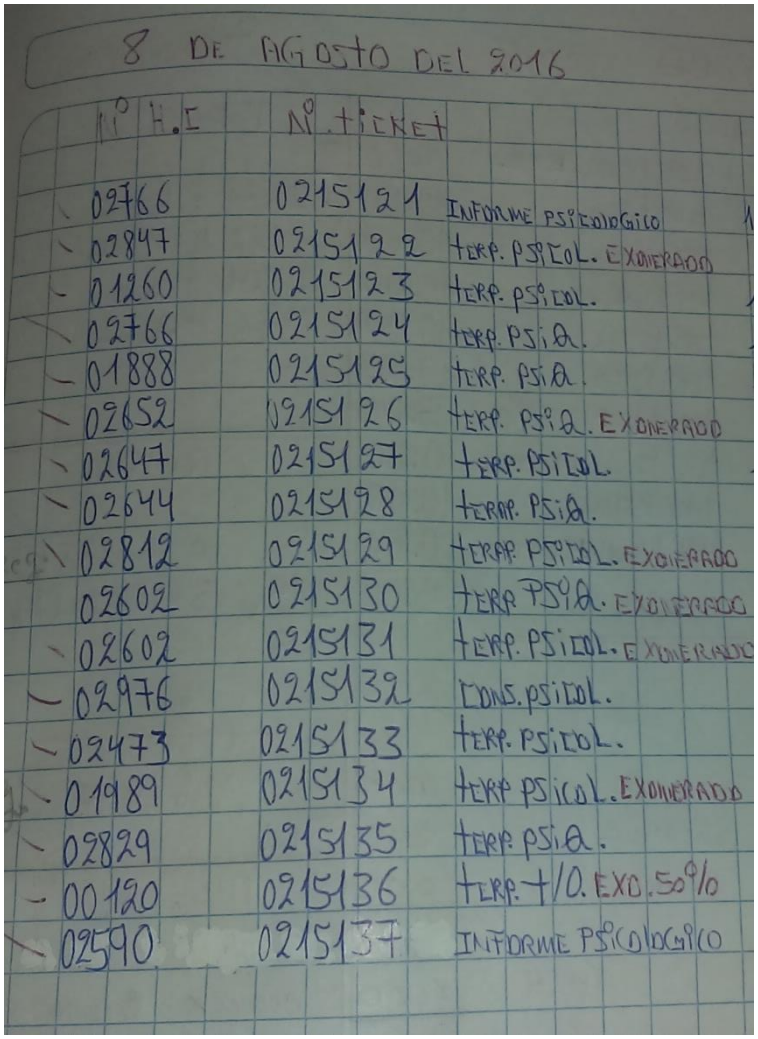
Anexo 5: Control de Ingresos y Egresos



Anexo 6: Acreditación de SIS activo



Anexo 7: Cuaderno de Registro de Salida y Entrada de Historia Clínica

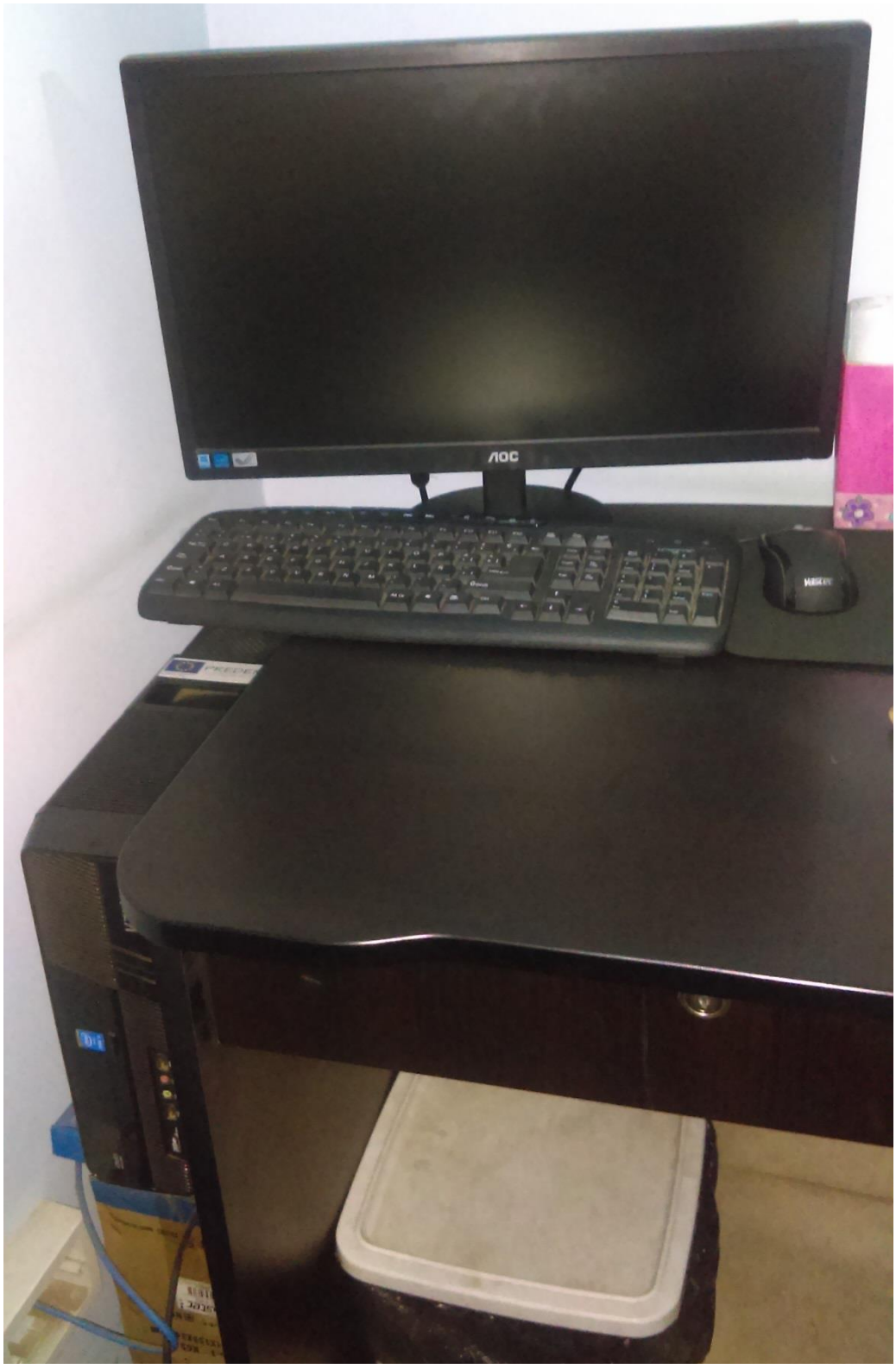


8 DE AGOSTO DEL 2016

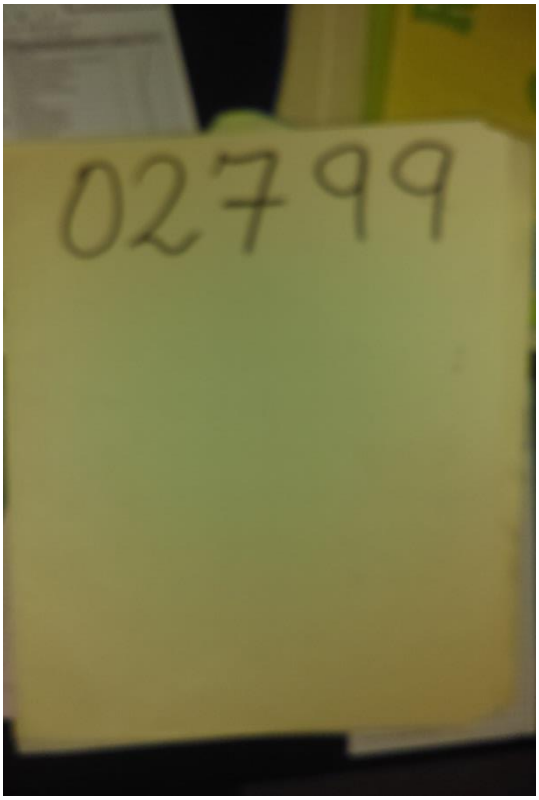
Nº H.C	Nº ticket	
02766	0215121	INFORME PSICOLOGICO
02847	0215122	TERAP. PSICOL. EXONERADO
01260	0215123	TERAP. PSICOL.
02766	0215124	TERAP. PSIQ.
01888	0215125	TERAP. PSIQ.
02652	0215126	TERAP. PSIQ. EXONERADO
02647	0215127	TERAP. PSICOL.
02644	0215128	TERAP. PSIQ.
02812	0215129	TERAP. PSICOL. EXONERADO
02602	0215130	TERAP PSIQ. EXONERADO
02602	0215131	TERAP. PSICOL. EXONERADO
02976	0215132	CONS. PSICOL.
02473	0215133	TERAP. PSICOL.
01989	0215134	TERAP PSICOL. EXONERADO
02829	0215135	TERAP. PSIQ.
00120	0215136	TERAP. T/O. EXO. 50%
02590	0215137	INFORME PSICOLOGICO

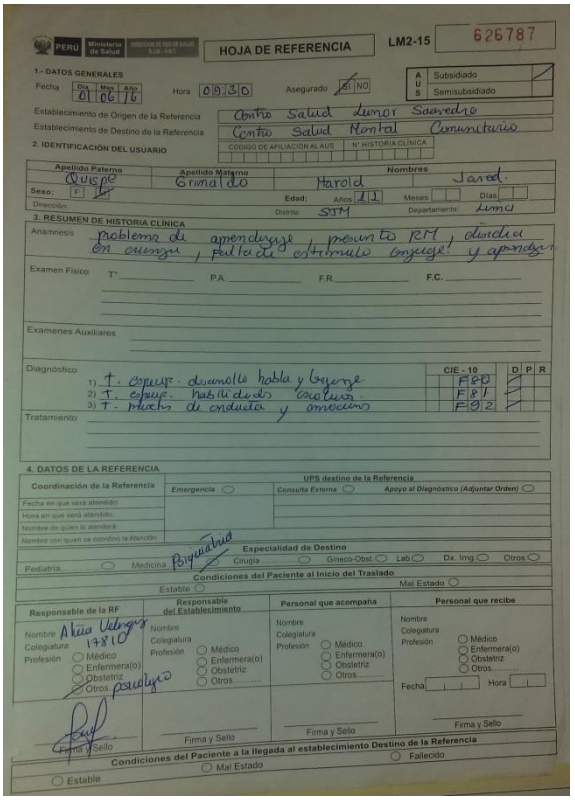
En la imagen, se registra el número de HC, el ticket asignado y se especifica el área de atención.

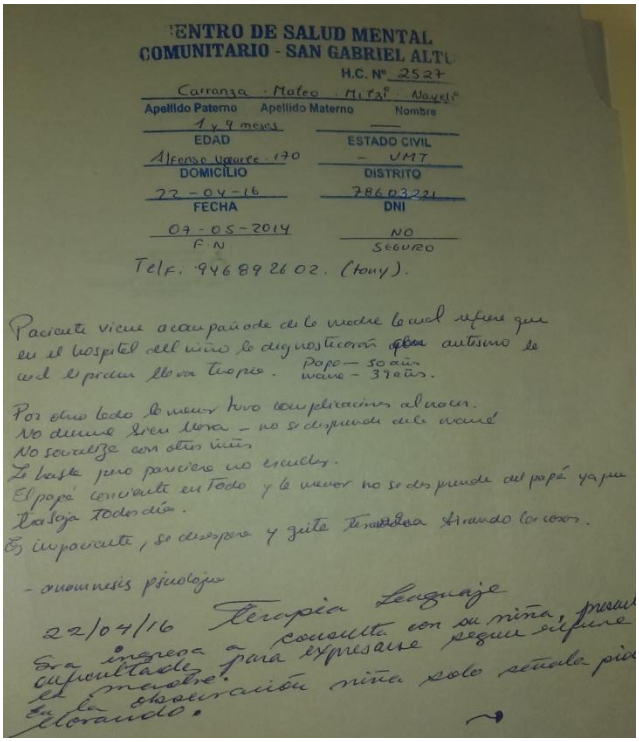
Anexo 8: Computadora de Escritorio



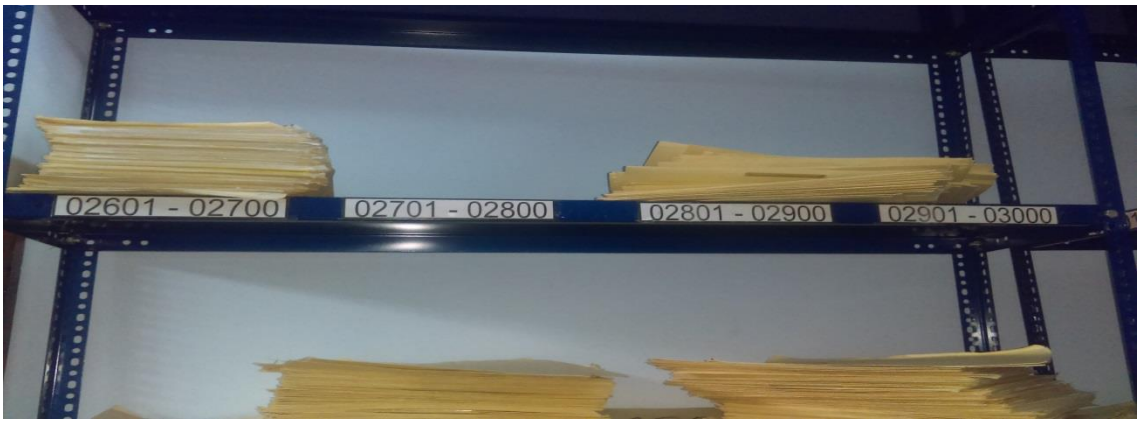
Anexo 9: Historia Clínica (contenido)





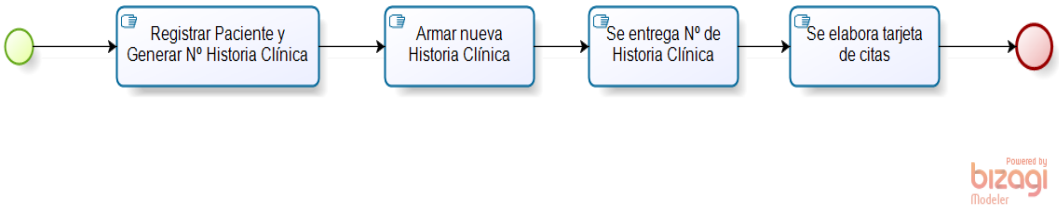


Anexo 10: Archivo de Historias Clínicas

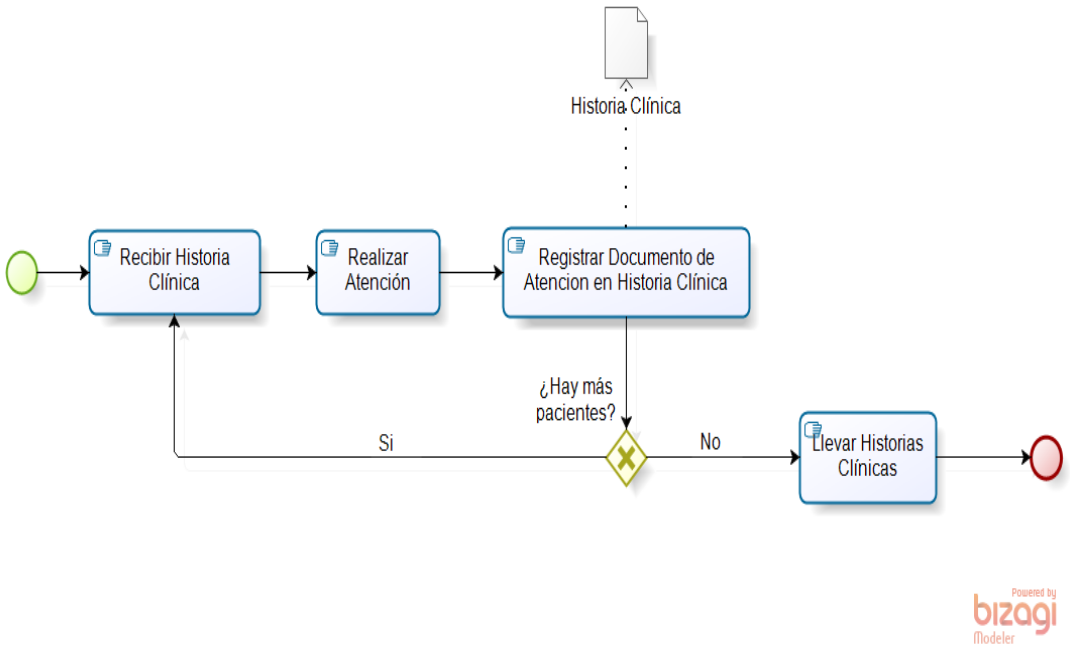


Anexo 11: Subprocesos del Proceso de Admisión de Paciente Nuevo

Sub Proceso: “Apertura Historia Clínica”.

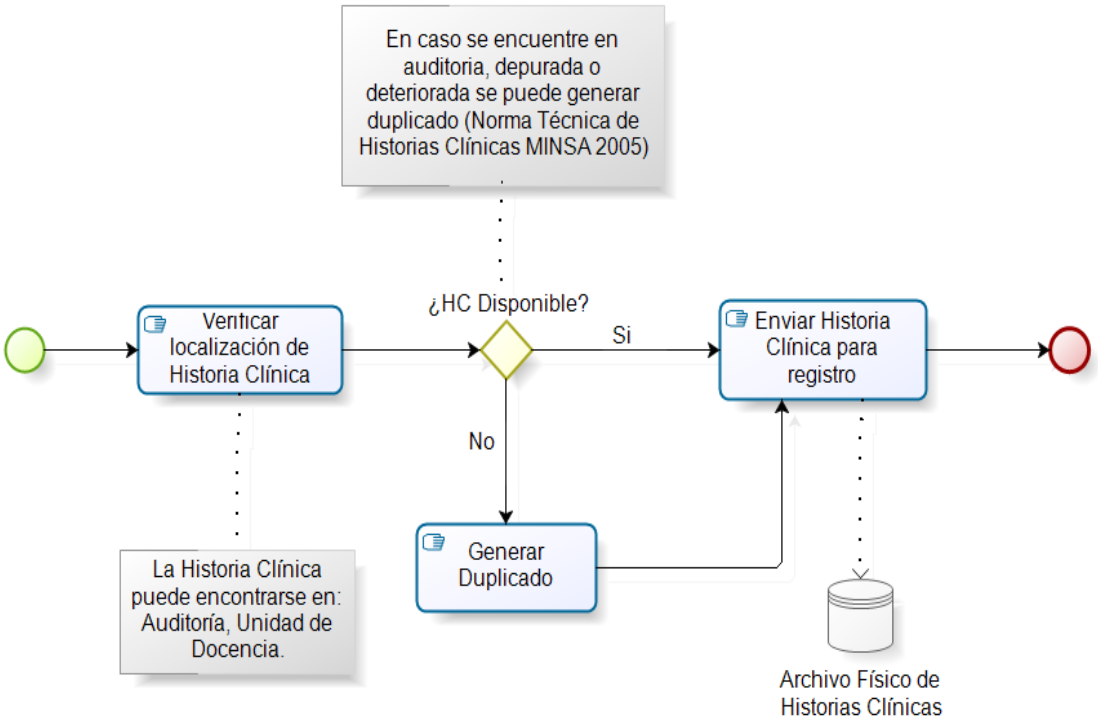


Sub Proceso: “Atender Paciente”.



Anexo 12: Subproceso del proceso de Admisión de Paciente Continuador

Sub Proceso: “Gestión de Historias Clínicas”.



Anexo 13: Matriz de Riesgos: Admisión de Paciente Nuevo

Actividad	Descripción del Riesgo				Consecuencia del Riesgo	Evaluación del Riesgo			
	Formulación del Riesgo	Tipo de evento	Factor que origina el Riesgo	Descripción de la Causa del Riesgo		Prob.	Impac.	Nivel de Riesgo	Est. de Rpta.
Registrar paciente y generar Número de HC	Posible demora en la atención del paciente por falta de disponibilidad del personal.	Ejecución, entrega y gestión de procesos	Personal	El personal no se encuentra para realizar la atención.	Demora en el tiempo de atención del paciente.	Posible	Muy bajo	Bajo	Aceptar
Registrar paciente y generar Número de HC	Posible error al ingresar los datos del paciente en el sistema debido a error del operador.	Ejecución, entrega y gestión de procesos	Personal	Los operadores ingresan información errónea en el sistema.	Se pierde la integridad de la información, no contando con la correcta por mal entendimiento.	Muy probable	Bajo	Moderado	Reducir
Armar nueva Historia Clínica	Posible error en la creación del documento debido a información errónea brindada por el paciente.	Clientes, servicios y prácticas institucionales	Eventos Externos	El usuario brinda información poco clara o errónea.	Se pierde la integridad de la información, no contando con la correcta por mal entendimiento de lo indicado por el paciente.	Muy probable	Alto	Alto	Reducir
Armar nueva Historia Clínica	Posible error al crear el documento del paciente debido a error del operador al suscribir los datos.	Ejecución, entrega y gestión de procesos	Personal	Los operadores ingresan información errónea.	Se pierde la integridad de la información, no contando con la correcta por mal entendimiento de lo indicado por el paciente.	Muy probable	Bajo	Moderado	Reducir

Actividad	Descripción del Riesgo				Consecuencia del Riesgo	Evaluación del Riesgo			
	Formulación del Riesgo	Tipo de evento	Factor que origina el Riesgo	Descripción de la Causa del Riesgo		Prob.	Impac.	Nivel de Riesgo	Est. de Rpta.
Armar nueva Historia Clínica	Posible demora en la atención del paciente originado por falta de materiales para crear el documento.	Ejecución, entrega y gestión de procesos	Personal	No se cuenta con los insumos o equipos necesarios para realizar la atención.	Demora en el tiempo de atención del paciente.	Poco probable	Bajo	Bajo	Aceptar
Armar nueva Historia Clínica	Posible demora en la atención del paciente originado por falta de disponibilidad del personal.	Ejecución, entrega y gestión de procesos	Personal	El personal no se encuentra para realizar la atención del paciente.	Demora en el tiempo de atención del paciente.	Posible	Muy bajo	Bajo	Aceptar
Elaborar tarjeta de citas	Posible error al crear el documento del paciente por error del operador al suscribir los datos.	Ejecución, entrega y gestión de procesos	Personal	El personal ingresa información errónea de los datos del paciente.	Se pierde la integridad de la información, no contando con la correcta por mal entendimiento de lo indicado por el paciente.	Probable	Posible	Moderado	Reducir

Actividad	Descripción del Riesgo				Consecuencia del Riesgo	Evaluación del Riesgo			
	Formulación del Riesgo	Tipo de evento	Factor que origina el Riesgo	Descripción de la Causa del Riesgo		Prob.	Impac.	Nivel de Riesgo	Est.de Rpta.
Verificar SIS activo	Posible denegación de atención como paciente SIS originada por error en la consulta de los datos del paciente por error del operador.	Interrupción de las operaciones y fallos en los sistemas.	Personal	Los operadores ingresan información errónea en el sistema.	Se afecta el tiempo de atención del paciente.	Muy probable	Muy bajo	Bajo	Aceptar
Verificar SIS activo	Posible denegación de atención como paciente SIS originada por falla en la consulta de los datos del paciente por problemas de conexión con el servicio.	Interrupción de las operaciones y fallos en los sistemas.	Tecnología de Información	Se presenta falla en la comunicación con el servidor de la aplicación.	Pérdida de información y demora en la atención de la paciente.	Posible	Bajo	Moderado	Reducir
Verificar SIS activo	Posible denegación de atención como paciente SIS, originado por falla en la consulta de los datos del paciente por indisponibilidad del sistema respectivo.	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Se presenta una caída de los sistemas.	Pérdida de información y demora en la atención del paciente.	Posible	Bajo	Moderado	Reducir
Verificar SIS activo	Posible denegación de atención como paciente SIS originado por no contar con datos actualizados en el sistema.	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	El sistema cuenta con información antigua no actualizada.	Se niega la atención a un paciente asegurado.	Posible	Alto	Alto	Reducir

Actividad	Descripción del Riesgo				Consecuencia del Riesgo	Evaluación del Riesgo			
	Formulación del Riesgo	Tipo de evento	Factor que origina el Riesgo	Descripción de la Causa del Riesgo		Prob.	Impac.	Nivel de Riesgo	Est. de Rpta.
Verificar SIS activo	Posible denegación de atención como paciente SIS falta de documentos del paciente.	Clientes servicios y practicas institucionales	Eventos Externos	El usuario no cuenta con los documentos requeridos para su reconocimiento como paciente SIS.	Se deniega el acceso a los servicios del paciente a través del seguro SIS	Posible	Muy bajo	Bajo	Aceptar
Adjuntar hoja de referencia	Posible imposibilidad de atender al paciente originada por falta de daño en la información o el sistema debido a malware.	Clientes servicios y practicas institucionales	Eventos externos	El usuario no cuenta con la hoja de referencia como paciente	Se deniega el acceso a los servicios del paciente, se le deriva a su centro de origen	Posible	Muy alto	Alto	Reducir
Registrar salida de historia clínica	Posible pérdida de información originada por indisponibilidad del soporte de registro de entradas y salidas de HC.	Ejecución, entrega y gestión de procesos	Personal	No se encuentra o no está disponible el registro de entrada y salida de Hist. Clínicas.	La Historia Clínica no se encuentra disponible en caso se requiera en otra atención.	Posible	Medio	Moderado	Reducir
Llevar Historia Clínica	Posible demora en la atención del paciente originado por falta de personal.	Ejecución, entrega y gestión de procesos	Personal	El personal no se encuentra en su lugar para realizar la atención	Demora en el tiempo de atención del paciente	Posible	Muy bajo	Bajo	Aceptar

Actividad	Descripción del Riesgo				Consecuencia del Riesgo	Evaluación del Riesgo			
	Formulación del Riesgo	Tipo de evento	Factor que origina el Riesgo	Descripción de la Causa del Riesgo		Prob.	Impac.	Nivel de Riesgo	Est. de Rpta.
Llevar Historia Clínica	Posible envío de una Historia Clínica que no corresponde a la paciente debido a información errónea brindada por el paciente.	Ejecución, entrega y gestión de procesos	Personal	Se indicó mal el número de Historia Clínica, o se asignó un número de Historia ya asignado a la paciente.	Exposición de información sensible perteneciente a otra paciente Demora en el tiempo de atención a la paciente.	Poco probable	Medio	Moderado	Reducir
Llevar Historia Clínica	Posible pérdida de información debido a robo de la Historia Clínica durante su envío	Ejecución, entrega y gestión de procesos	Personal	No se cuenta con un control que establezca el personal a manipular las copias de Historias Clínicas.	Pérdida de información crítica para los procesos asistenciales Filtración de información.	Muy probable	Muy alto	Extremo	Reducir
Llevar Historia Clínica	Posible pérdida de información debido a extravío de la Historia Clínica durante su envío	Ejecución, entrega y gestión de procesos	Personal	Se extravió la copia de Historia Clínica generada durante su envío	Pérdida de información crítica para los procesos asistenciales	Muy probable	Muy alto	Extremo	Reducir

Actividad	Descripción del Riesgo				Consecuencia del Riesgo	Evaluación del Riesgo			
	Formulación del Riesgo	Tipo de evento	Factor que origina el Riesgo	Descripción de la Causa del Riesgo		Prob.	Impac.	Nivel de Riesgo	Est. de Rpta.
Cobrar cita a paciente	Posible error en el ingreso de datos debido a error del operador.	Ejecución, entrega y gestión de procesos	Personal	Los operadores ingresan información errónea.	Se pierde la integridad de la información, no contando con la correcta por mal entendimiento de lo indicado por el paciente o distracción.	Muy probable	Bajo	Moderado	Reducir
Generar boleta de pago	Posible demora en la atención del paciente originado por falta de disponibilidad del personal.	Ejecución, entrega y gestión de procesos	Personal	El personal no se encuentra en su lugar para realizar la atención del paciente.	Demora en el tiempo de atención del paciente.	Posible	Muy bajo	Bajo	Aceptar
Generar boleta de pago	Posible demora en la atención del paciente originado por falta de materiales para crear el documento.	Ejecución, entrega y gestión de procesos	Personal	No se cuenta con los insumos o equipos necesarios para realizar la atención.	Demora en el tiempo de atención del paciente.	Poco probable	Bajo	Bajo	Aceptar

Actividad	Descripción del Riesgo				Consecuencia del Riesgo	Evaluación del Riesgo			
	Formulación del Riesgo	Tipo de evento	Factor que origina el Riesgo	Descripción de la Causa del Riesgo		Prob.	Impac.	Nivel de Riesgo	Est. de Rpta.
Llevar Historia Clínica	Posible demora en la atención del paciente originado por falta de disponibilidad del personal	Ejecución, entrega y gestión de procesos	Personal	El personal no se encuentra en su lugar para realizar la atención del paciente	Demora en el tiempo de atención del paciente	Posible	Muy bajo	Bajo	Aceptar
Llevar Historia Clínica	Posible envío de una Historia Clínica que no corresponde a la paciente debido a información errónea brindada por el paciente.	Ejecución, entrega y gestión de procesos	Personal	Se indicó mal el número de Historia Clínica, o se asignó un número de Historia ya asignado a la paciente.	Exposición de información sensible perteneciente a otra paciente Demora en el tiempo de atención al paciente.	Poco probable	Medio	Moderado	Reducir
Llevar Historia Clínica	Posible pérdida de información debido a robo de la Historia Clínica durante su envío.	Ejecución, entrega y gestión de procesos	Personal	No se cuenta con un control que establezca el personal a manipular las copias de Hist. Clínicas	Pérdida de información crítica para los procesos asistenciales Filtración de información	Muy probable	Muy alto	Extremo	Reducir

Actividad	Descripción del Riesgo				Consecuencia del Riesgo	Evaluación del Riesgo			
	Formulación del Riesgo	Tipo de evento	Factor que origina el Riesgo	Descripción de la Causa del Riesgo		Prob.	Impac.	Nivel de Riesgo	Est.de Rpta.
Llevar Historia Clínica	Posible pérdida de información debido a extravío de la Historia Clínica durante su envío.	Ejecución, entrega y gestión de procesos	Personal	Se extravió la copia de Historia Clínica generada durante su envío.	Pérdida de información crítica para los procesos asistenciales	Muy probable	Muy alto	Extremo	Reducir
Recibir historia clínica	Posible demora en la atención del paciente debido a falta de disponibilidad del personal. .asignado	Ejecución, entrega y gestión de procesos	Personal	El personal no se encuentra en su lugar para realizar la recepción de la historia clínica	Demora en el tiempo de atención del paciente	Posible	Muy bajo	Bajo	Aceptar
Registrar datos biométricos Peso y Talla	Posible error en el registro de información debido a inexperiencia del personal.	Ejecución, entrega y gestión de procesos	Personal	El personal no cuenta con la experiencia necesaria para realizar la recolección de la información requerida.	Registro de información errónea	Posible	Medio	Moderado	Reducir

Actividad	Descripción del Riesgo				Consecuencia del Riesgo	Evaluación del Riesgo			
	Formulación del Riesgo	Tipo de evento	Factor que origina el Riesgo	Descripción de la Causa del Riesgo		Prob.	Impac.	Nivel de Riesgo	Est. de Rpta.
Registrar datos biométricos Peso y Talla	Posible demora en la atención del paciente originado por falta de equipos.	Ejecución, entrega y gestión de procesos	Personal	No se cuenta con los insumos o equipos necesarios para realizar la atención.	Demora en el tiempo de atención del paciente	Poco probable	Bajo	Bajo	Aceptar
Llevar Historia Clínica	Posible demora en la atención del paciente originado por falta de disponibilidad del personal.	Ejecución, entrega y gestión de procesos	Personal	El personal no se encuentra en su lugar para realizar la atención del paciente.	Demora en el tiempo de atención del paciente	Posible	Muy bajo	Bajo	Aceptar
Llevar Historia Clínica	Posible envío de una Historia Clínica que no corresponde a la paciente debido a información errónea brindada por el paciente.	Ejecución, entrega y gestión de procesos	Personal	Se indicó mal el número de Historia Clínica, o se asignó un número de Historia ya asignado al paciente.	Exposición de información sensible perteneciente a otra paciente Demora en el tiempo de atención a la paciente.	Poco probable	Medio	Moderado	Reducir

Actividad	Descripción del Riesgo				Consecuencia del Riesgo	Evaluación del Riesgo			
	Formulación del Riesgo	Tipo de evento	Factor que origina el Riesgo	Descripción de la Causa del Riesgo		Prob.	Impac.	Nivel de Riesgo	Est. de Rpta.
Llevar Historia Clínica	Posible pérdida de información debido a robo de la Historia Clínica durante su envío.	Ejecución, entrega y gestión de procesos	Personal	No se cuenta con un control que establezca el personal a manipular las copias de Historias Clínicas.	Pérdida de información crítica para los procesos asistenciales Filtración de información	Muy probable	Muy alto	Extremo	Reducir
Llevar Historia Clínica	Posible pérdida de información debido a extravío de la Historia Clínica durante su envío.	Ejecución, entrega y gestión de procesos	Personal	Se extravió la copia de Historia Clínica generada durante su envío.	Pérdida de información crítica para los procesos asistenciales	Muy probable	Muy alto	Extremo	Reducir
Recibir historia clínica	Posible demora en la atención del paciente debido a falta de disponibilidad del personal asignado.	Ejecución, entrega y gestión de procesos	Personal	El personal no se encuentra en su lugar para realizar la recepción de la HC.	Demora en el tiempo de atención del paciente	Posible	Muy bajo	Bajo	Aceptar
Registrar documentos de atención en Historia Clínica	Posible pérdida de información debido a olvido por parte del doctor del llenado de la Historia Clínica	Ejecución, entrega y gestión de procesos	Personal	Se obvió información importante que debía formar parte de la Historia Clínica	No se cuenta con información completa en el registro de la Historia Clínica	Poco probable	Alto	Moderado	Reducir

Actividad	Descripción del Riesgo				Consecuencia del Riesgo	Evaluación del Riesgo			
	Formulación del Riesgo	Tipo de evento	Factor que origina el Riesgo	Descripción de la Causa del Riesgo		Prob.	Impac.	Nivel de Riesgo	Est. de Rpta.
Registrar documentos de atención en Historia Clínica	Posible demora en la atención del paciente debido a falta de materiales para realizar el	Ejecución, entrega y gestión de procesos	Personal	No se cuenta con los insumos o equipos necesarios para realizar la atención.	Demora en el tiempo de atención del paciente.	Poco probable	Bajo	Bajo	Aceptar
Llevar Historia Clínica	Posible demora en la atención del paciente originado por falta de disponibilidad del	Ejecución, entrega y gestión de procesos	Personal	El personal no se encuentra en su lugar para realizar la atención del paciente.	Demora en el tiempo de atención del paciente	Posible	Muy bajo	Bajo	Aceptar
Llevar Historia Clínica	Posible envío de una Historia Clínica que no corresponde a la paciente debido a información errónea brindada por el paciente.	Ejecución, entrega y gestión de procesos	Personal	Se indicó mal el número de Historia Clínica, o se asignó un número de Historia ya asignado a la paciente.	Exposición de información sensible perteneciente a otra paciente Demora en el tiempo de atención a la paciente.	Poco probable	Medio	Moderado	Reducir

Actividad	Descripción del Riesgo				Consecuencia del Riesgo	Evaluación del Riesgo			
	Formulación del Riesgo	Tipo de evento	Factor que origina el Riesgo	Descripción de la Causa del Riesgo		Prob.	Impac.	Nivel de Riesgo	Estr. de Rpta.
Llevar Historia Clínica	Posible pérdida de información debido a robo de la Historia Clínica durante su envío.	Ejecución, entrega y gestión de procesos	Personal	No se cuenta con un control que establezca el personal a manipular las copias de HC.	Pérdida de información crítica para los procesos asistenciales Filtración de información.	Muy probable	Muy alto	Extremo	Reducir
Llevar Historia Clínica	Posible pérdida de información debido a extravío de la Historia Clínica durante su envío.	Ejecución, entrega y gestión de procesos	Personal	Se extravió la copia de Historia Clínica generada durante su envío.	Pérdida de información crítica para los procesos asistenciales	Muy probable	Muy alto	Extremo	Reducir
Recibir historia clínica	Posible demora en la atención del paciente debido a falta de disponibilidad del personal asignado.	Ejecución, entrega y gestión de procesos	Personal	El personal no se encuentra en su lugar para realizar la recepción de la historia	Demora en el tiempo de atención del paciente	Posible	Muy bajo	Bajo	Aceptar
Registrar devolución de historia clínica	Posible pérdida de información debido a la indisponibilidad del soporte de registro de entrada y salida de historia clínicas.	Ejecución, entrega y gestión de procesos	Personal	No se encuentra o no está disponible el registro de entradas y salidas de la hist. Clínica.	La historia clínica no se encuentra disponible en caso requiera otra atención.	Posible	Medio	Moderado	Reducir

Actividad	Descripción del Riesgo				Consecuencia del Riesgo	Evaluación del Riesgo			
	Formulación del Riesgo	Tipo de evento	Factor que origina el Riesgo	Descripción de la Causa del Riesgo		Prob.	Impac.	Nivel de Riesgo	Est. de Rpta.
Registrar devolución de historia clínica	Posible desfase de información originado por indisponibilidad de personal que realice el registro de la devolución.	Ejecución, entrega y gestión de procesos	Personal	El personal no se encuentra en el lugar para realizar la atención de la devolución.	La historia clínica no se encuentra disponible en caso se requiera otra atención.	Posible	Medio	Moderado	Reducir
Archivar historia clínica	Posible pérdida de información por daño físico a la historia clínica.	Ejecución, entrega y gestión de procesos	Personal	Condiciones de almacenaje y tratamiento poco adecuadas y seguras.	Pérdida de la información para los procesos asistenciales de filtración de información.	Muy probable	Muy alto	Extremo	Reducir
Archivar historia clínica	Posible pérdida de información debido a extravío de parte del contenido de la historia clínica.	Ejecución, entrega y ejecución de procesos	Personal	Se extravió parte de la historia clínica durante su traslado.	Pérdida de información crítica para los procesos asistenciales.	Muy probable	Muy alto	Extremo	Reducir

Actividad	Descripción del Riesgo				Consecuencia del Riesgo	Evaluación del Riesgo			
	Formulación del Riesgo	Tipo de evento	Factor que origina el Riesgo	Descripción de la Causa del Riesgo		Prob.	Impac.	Nivel de Riesgo	Est.de Rpta
Archivar historia clínica	Posible extravió de historia clínica debido a error en la localización del archivo.	Ejecución, entrega y gestión de procesos	Personal	Se archivó la historia clínica en un lugar donde no corresponde.	Pérdida de información crítica para los procesos asistenciales.	Muy probable	Muy alto	Extremo	Reducir
Generar documento de contrarreferen-cia	Posible error en la creación del documento debido a información errónea brindada por el paciente.	Clientes, servicios y prácticas institucionales	Eventos externos	El usuario brinda información poco clara o errónea.	Se pierde la integridad de la información, no contando con la correcta por mal entendimiento de lo indicado por el paciente o distracción.	Muy probable	Alto	Alto	Reducir

Anexo 14: Matriz de Riesgos: Admisión de Paciente Continuador

Actividad	Descripción del Riesgo				Consecuencia del Riesgo	Evaluación del Riesgo			
	Formulación del Riesgo	Tipo de evento	Factor que origina el Riesgo	Descripción de la Causa del Riesgo		Prob.	Impac.	Nivel de Riesgo	Est. de Rpta.
Verificar cita	Posible error en la generación del cupo originada por error de concurrencia.	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Se presenta un error de entre dos usuarios queriendo registrar un mismo campo.	Generación de doble cita en un mismo horario	Poco probable	Bajo	Bajo	Aceptar
Verificar cita	Posible demora en la atención del paciente originado por falta de disponibilidad del personal.	Ejecución, entrega y gestión de procesos	Personal	El personal no se encuentra en su lugar para realizar la atención del paciente.	Demora en el tiempo de atención del paciente	Posible	Muy bajo	Bajo	Aceptar
Verificar SIS activo	Posible denegación de atención como paciente SIS originada por error en la consulta de los datos del paciente por error del operador.	Interrupción de las operaciones y fallos en los sistemas	Personal	Los operadores ingresan información errónea en el sistema	Se afecta el tiempo de atención del paciente	Muy probable	Muy bajo	Bajo	Aceptar
Verificar SIS activo	Posible denegación de atención como paciente SIS originada por falla en la consulta de los datos del paciente por problemas de conexión con el	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Se presenta una falla en la comunicación con el servidor de la aplicación	Pérdida de información y demora en la atención de la paciente	Posible	Bajo	Moderado	Reducir

Actividad	Descripción del Riesgo Riesgo				Consecuencia del Riesgo	Evaluación del Riesgo			
	Formulación del Riesgo	Tipo de evento	Factor que origina el Riesgo	Descripción de la Causa del Riesgo		Prob.	Impac.	Nivel de RiGesgo	Est.de Rpta.
Verificar SIS activo	Posible denegación de atención como paciente SIS originada por falla en la consulta de los datos del paciente por indisponibilidad del sistema respectivo.	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Se presenta una caída de los sistemas	Pérdida de información y demora en la atención de la paciente	Posible	Bajo	Moderado	Reducir
Verificar SIS activo	Posible denegación de atención como paciente SIS originado por no contar con datos actualizados en el sistema.	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	El sistema cuenta con información antigua no actualizada	Se niega la atención a un paciente asegurado	Posible	Alto	Alto	Reducir
Adjuntar copia de referencia	Posible imposibilidad de atender al paciente originada por falta de daño en la información o el sistema debido a malware.	Clientes servicios y prácticas institucionales	Eventos externos	El usuario no cuenta con la hoja de referencia como paciente	Se deniega el acceso a los servicios del paciente, se le deriva a su centro de origen	Posible	Muy alto	Alto	Reducir

Actividad	Descripción del Riesgo				Consecuencia del Riesgo	Evaluación del Riesgo			
	Formulación del Riesgo	Tipo de evento	Factor que origina el Riesgo	Descripción de la Causa del Riesgo		Prob.	Impac.	Nivel de Riesgo	Est. de Rpta.
Cobrar cita a paciente	Posible error en el ingreso de datos debido a error del operador.	Ejecución, entrega y gestión de procesos	Personal	Los operadores ingresan información errónea.	Se pierde la integridad de la información, no contando con la correcta por mal entendimiento de lo indicado por el paciente o distracción.	Muy probable	Bajo	Moderado	Reducir
Generar boleta de pago	Posible demora en la atención del paciente originado por falta de disponibilidad del personal.	Ejecución, entrega y gestión de procesos	Personal	El personal no se encuentra en su lugar para realizar la atención del paciente	Demora en el tiempo de atención del paciente	Posible	Muy bajo	Bajo	Aceptar
Generar boleta de pago	Posible demora en la atención del paciente originado por falta de materiales para crear el documento	Ejecución, entrega y gestión de procesos	Personal	No se cuenta con los insumos o equipos necesarios para realizar la atención	Demora en el tiempo de atención del paciente	Poco probable	Bajo	Bajo	Aceptar
Llevar Historia Clínica	Posible demora en la atención del paciente originado por falta de disponibilidad del personal.	Ejecución, entrega y gestión de procesos	Personal	El personal no se encuentra en su lugar para realizar la atención del paciente	Demora en el tiempo de atención del paciente	Posible	Muy bajo	Bajo	Aceptar

Actividad	Descripción del Riesgo				Consecuencia del Riesgo	Evaluación del Riesgo			
	Formulación del Riesgo	Tipo de evento	Factor que origina el Riesgo	Descripción de la Causa del Riesgo		Prob.	Impac.	Nivel de Riesgo	Estr. de Rpta.
Llevar Historia Clínica	Posible envío de una Historia Clínica que no corresponde a la paciente debido a información errónea brindada por el paciente	Ejecución, entrega y gestión de procesos	Personal	Se indicó mal el número de Historia Clínica, o se asignó un número de Historia ya asignado a la paciente	Exposición de información sensible perteneciente a otra paciente Demora en el tiempo de atención a la paciente	Poco probable	Medio	Moderado	Reducir
Llevar Historia Clínica	Posible pérdida de información debido a robo de la Historia Clínica durante su envío.	Ejecución, entrega y gestión de procesos	Personal	No se cuenta con un control que establezca el personal a manipular las copias de HC	Pérdida de información crítica para los procesos asistenciales Filtración de información	Muy probable	Muy alto	Extremo	Reducir
Llevar Historia Clínica	Posible pérdida de información debido a extravío de la Historia Clínica durante su envío.	Ejecución, entrega y gestión de procesos	Personal	Se extravió la copia de H.C generada durante su envío.	Pérdida de información crítica para los procesos asistenciales	Muy probable	Muy alto	Extremo	Reducir
Recibir historia clínica	Posible demora en la atención del paciente debido a falta de disponibilidad del personal asignado.	Ejecución, entrega y gestión de procesos	Personal	El personal no se encuentra en su lugar para realizar la recepción de la historia clínica.	Demora en el tiempo de atención del paciente	Posible	Muy bajo	Bajo	Aceptar

Actividad	Descripción del Riesgo				Consecuencia del Riesgo	Evaluación del Riesgo			
	Formulación del Riesgo	Tipo de evento	Factor que origina el Riesgo	Descripción de la Causa del Riesgo		Prob.	Impac.	Nivel de Riesgo	Estr. de Rpta.
Registrar datos biométricos Peso y Talla	Posible demora en la atención del paciente originado por falta de equipos	Ejecución, entrega y gestión de procesos	Personal	No se cuenta con los insumos o equipos necesarios para realizar la atención	Demora en el tiempo de atención del paciente	Poco probable	Bajo	Bajo	Aceptar
Llevar Historia Clínica	Posible demora en la atención del paciente originado por falta de disponibilidad del personal.	Ejecución, entrega y gestión de procesos	Personal	El personal no se encuentra en su lugar para realizar la atención del paciente.	Demora en el tiempo de atención del paciente.	Posible	Muy bajo	Bajo	Aceptar
Llevar Historia Clínica	Posible envío de una Historia Clínica que no corresponde a la paciente debido a información errónea brindada por el paciente.	Ejecución, entrega y gestión de procesos	Personal	Se indicó mal el número de Historia Clínica, o se asignó un número de Historia ya asignado a la paciente.	Exposición de información sensible perteneciente a otra paciente Demora en el tiempo de atención a la paciente.	Poco probable	Medio	Moderado	Reducir

Actividad	Descripción del Riesgo				Consecuencia del Riesgo	Evaluación del Riesgo			
	Formulación del Riesgo	Tipo de evento	Factor que origina el Riesgo	Descripción de la Causa del Riesgo		Prob.	Impac.	Nivel de Riesgo	Estr. de Rpta.
Llevar Historia Clínica	Posible pérdida de información debido a robo de la Historia Clínica durante su envío	Ejecución, entrega y gestión de procesos	Personal	No se cuenta con un control que establezca el personal a manipular las copias de Historias Clínicas	Pérdida de información crítica para los procesos asistenciales Filtración de información	Muy probable	Muy alto	Extremo	Reducir
Llevar Historia Clínica	Posible pérdida de información debido a extravío de la Historia Clínica durante su envío	Ejecución, entrega y gestión de procesos	Personal	Se extravió la copia de Historia Clínica generada durante su envío	Pérdida de información crítica para los procesos asistenciales	Muy probable	Muy alto	Extremo	Reducir
Recibir Historia Clínica	Posible demora en la atención del paciente debido a falta de disponibilidad del personal asignado	Ejecución, entrega y gestión de procesos	Personal	El personal no se encuentra en su lugar para realizar la recepción de la historia clínica	Demora en el tiempo de atención del paciente	Posible	Muy bajo	Bajo	Aceptar
Registrar documentos de atención en Historia Clínica	Posible pérdida de información debido a olvido por parte del doctor del llenado de la Historia Clínica	Ejecución, entrega y gestión de procesos	Personal	Se obvió información importante que debía formar parte de la Historia Clínica	No se cuenta con información completa en el registro de la Historia Clínica	Poco probable	Alto	Moderado	Reducir

Actividad	Descripción del Riesgo				Consecuencia del Riesgo	Evaluación del Riesgo			
	Formulación del Riesgo	Tipo de evento	Factor que origina el Riesgo	Descripción de la Causa del Riesgo		Prob.	Impac.	Nivel de Riesgo	Estr. de Rpta.
Registrar documentos de atención en Historia Clínica	Posible demora en la atención del paciente debido a falta de materiales para realizar el registro	Ejecución, entrega y gestión de procesos	Personal	No se cuenta con los insumos o equipos necesarios para realizar la atención	Demora en el tiempo de atención del paciente	Poco probable	Bajo	Bajo	Aceptar
Llevar Historia Clínica	Posible demora en la atención del paciente originado por falta de disponibilidad del personal	Ejecución, entrega y gestión de procesos	Personal	El personal no se encuentra en su lugar para realizar la atención del paciente	Demora en el tiempo de atención del paciente	Posible	Muy bajo	Bajo	Aceptar
Llevar Historia Clínica	Posible envío de una Historia Clínica que no corresponde a la paciente debido a información errónea brindada por el paciente	Ejecución, entrega y gestión de procesos	Personal	Se indicó mal el número de Historia Clínica, o se asignó un número de Historia ya asignado al paciente	Exposición de información sensible perteneciente a otra paciente Demora en el tiempo de atención a la	Poco probable	Medio	Moderado	Reducir

Actividad	Descripción del Riesgo				Consecuencia del Riesgo	Evaluación del Riesgo			
	Formulación del Riesgo	Tipo de evento	Factor que origina el Riesgo	Descripción de la Causa del Riesgo		Prob.	Impac.	Nivel de Riesgo	Estr. de Rpta.
Llevar Historia Clínica	Posible pérdida de información debido a robo de la Historia Clínica durante su envío	Ejecución, entrega y gestión de procesos	Personal	No se cuenta con un control que establezca el personal a manipular las copias de Historias Clínicas	Pérdida de información crítica para los procesos asistenciales Filtración de información	Muy probable	Muy alto	Extremo	Reducir
Llevar Historia Clínica	Posible pérdida de información debido a extravío de la Historia Clínica durante su envío	Ejecución, entrega y gestión de procesos	Personal	Se extravió la copia de H.C generada durante su envío	Pérdida de información crítica para los procesos asistenciales	Muy probable	Muy alto	Extremo	Reducir
Recibir historia clínica	Posible demora en la atención del paciente debido a falta de disponibilidad del personal asignado	Ejecución, entrega y gestión de procesos	Personal	El personal no se encuentra en su lugar para realizar la recepción de la historia clínica	Demora en el tiempo de atención del paciente	Posible	Muy bajo	Bajo	Aceptar
Registrar devolución de historia clínica	Posible pérdida de información debido a la indisponibilidad del soporte de registro de entradas y salidas de historias clínicas	Ejecución, entrega y gestión de procesos	Personal	No se encuentra o no está disponible el registro de entradas y salidas de las HC	La historia clínica no se encuentra disponible en caso requiera otra atención	Posible	Medio	Moderado	Reducir

Actividad	Descripción del Riesgo				Consecuencia del Riesgo	Evaluación del Riesgo			
	Formulación del Riesgo	Tipo de evento	Factor que origina el Riesgo	Descripción de la Causa del Riesgo		Prob.	Impac.	Nivel de Riesgo	Estr. de Rpta.
Registrar devolución de historia clínica	Posible desfase de información originado por indisponibilidad de personal que realice el registro de la devolución	Ejecución, entrega y gestión de procesos	Personal	El personal no se encuentra en el lugar para realizar la atención de la devolución	La historia clínica no se encuentra disponible en caso se requiera otra atención	Posible	Medio	Moderado	Reducir
Archivar historia clínica	Posible pérdida de información por daño físico a la historia clínica	Ejecución, entrega y gestión de procesos	Personal	Condiciones de almacenaje y tratamiento poco adecuadas y seguras	Pérdida de la información para los procesos asistenciales de filtración de información	Muy probable	Muy alto	Extremo	Reducir
Archivar historia clínica	Posible pérdida de información debido a extravío de parte del contenido de la historia clínica	Ejecución, entrega y ejecución de procesos	Personal	Se extravió parte de la historia clínica durante su traslado	Pérdida de información crítica para los procesos asistenciales	Muy probable	Muy alto	Extremo	Reducir

Actividad	Descripción del Riesgo				Consecuencia del Riesgo	Evaluación del Riesgo			
	Formulación del Riesgo	Tipo de evento	Factor que origina el Riesgo	Descripción de la Causa del Riesgo		Prob.	Impac.	Niv. de Riesgo	Estr. de rpta.
Archivar historia clínica	Posible extravió de historia clínica debido a error en la localización del archivo	Ejecución, entrega y gestión de procesos	Personal	Se archivó la historia clínica en un lugar donde no corresponde	Pérdida de información crítica para los procesos asistenciales	Muy probable	Muy alto	Extremo	Reducir
Generar documento de contrarreferencia	Posible error en la creación del documento debido a información errónea brindada por el paciente	Clientes, servicios y prácticas institucionales	Eventos externos	El usuario brinda información poco clara o errónea	Se pierde la integridad de la información, no contando con la correcta por mal entendimiento de lo indicado por el paciente o distracción	Muy probable	Alto	Alto	Reducir

Anexo 15: Declaración de aplicabilidad (RL= Requerimientos Legales, RN = Requerimientos del Negocio, EVR = *Evaluación de Riesgo)*

NTP-ISO 27001:2014 Controles de Seguridad			Controles actuales	Justificación de inclusión -comentarios-	Controles seleccionados y razones de selección			Comentarios
					RL	RN	EVR	
Cláusula	Sección	Objetivo del Control						
A.5. Políticas de Seguridad	A.5.1	Dirección de gerencia para la seguridad de la información						
	A.5.1.1	Políticas de Seguridad de la Información		Es necesario establecer políticas para asegurar los activos de información críticos que contienen información confidencial	X	X		Se deben establecer políticas específicas comunicadas a toda la organización
A.6. Organización de la Seguridad de la Información	A.6.1	Organización Interna						
	A.6.1.1	Roles y Responsabilidad de Seguridad de la Información		Establecer responsabilidades y roles para los trabajadores.	X	X		Compromiso de la alta dirección
	A.6.1.2	Segregación de funciones	Si hay flujo gramas, pero no encontramos documentación de los procesos de negocio	Se encontró que no existen gráficos unificados que muestren el flujo de información en los procesos críticos		X		Establecer quienes tienen acceso al flujo de la información.
	A.6.1.3	Contacto con autoridades		El Establecimiento de salud debe notificar cualquier incidente de seguridad de la información y a la policía de ser necesario		X		

NTP-ISO 27001:2014 Controles de Seguridad		Controles actuales	Justificación de inclusión -comentarios-	Controles seleccionados y razones de selección			Comentarios
				RL	RN	EVR	
Sección	Objetivo del Control						
A.7.1	Previo al empleo						
A.7.1.1	Selección		Permite filtrar aquellas personas que constituyan un riesgo para la información en el EESS	X	X		Durante la fase de reclutamiento, solicitar antecedentes policiales y penales a los postulantes
A.7.1.2	Términos y condiciones de empleo		Previo a la firma de contrato, indicar la responsabilidad respecto a la seguridad de la información	X		X	Explicar el marco normativo actual
A.7.2	Durante el empleo						
A.7.2.1	Responsabilidades de la Gerencia		Velar por una atención de calidad de sus pacientes, desarrollando planes estratégicos que permitan el uso de la seguridad de la información		X		Dirigir el esfuerzo de los trabajadores para el cumplimiento de las políticas de seguridad establecidas.
A.7.2.2	Conciencia, educación y entrenamiento de Seguridad de la Información		Establecer planes de capacitación sobre la política de seguridad de la información	X	X		Se recomienda realizar anualmente cursos
A.7.2.3	Proceso disciplinario		Establecer sanciones para aquellos colaboradores que incumplan las condiciones de seguridad de la información.		X	X	

NTP-ISO 27001:2014 Controles de Seguridad			Controles actuales	Justificación de inclusión -comentarios-	Controles seleccionados y razones de selección			Comentarios
					RL	RN	EVR	
Cláusula	Sección	Objetivo del Control						
A.8 Gestión de Activos	A.8.1	Responsabilidad por los Activos						
	A.8.1.1	Inventario de Activos	Los dueños de la información de la historia clínica es el área de admisión	Al ser un establecimiento de salud, se debe tener una lista que permita la ubicación de los activos.	X	X		Se trabaja con los dueños del proceso
	A.8.1.2	Propiedad de Activos		Se deben encargar a un custodio encargado del inventario, clasificación y protección de los activos así como su destrucción	X	X		
	A.8.1.3	Uso aceptable de los Activos		Documentar la definición en cuanto al manejo aceptable de activos de información	X	X		
	A.8.2	Clasificación de la Información						
	A.8.2.1	Clasificación de la Información		Clasificar los activos debido a su criticidad para el negocio	X	X		Tener en cuenta la Ley de Protección de datos personales y la norma técnica de historias clínicas

NTP-ISO 27001:2014 Controles de Seguridad			Controles actuales	Justificación de inclusión - comentarios-	Controles seleccionados y razones de selección			Comentarios
					RL	RN	EVR	
Cláusula	Sección	Objetivo del Control						
A.8 Gestión de activos	A.8.2	Clasificación de la Información						
	A.8.2.2	Etiquetado de la información		Permite identificar la información de acuerdo a clasificaciones y especificaciones		X	X	
	A.8.2.3	Manejo de Activos		Establecer procedimientos permitirá que se sigan protocolos garantizando la seguridad de los activos		X	X	
	A.8.2.4	Devolución de Activos	Cuaderno de control de Historias Clínicas salientes de admisión	Debido a la criticidad de los activos físicos, es necesario aplicar este tipo de controles		X	X	
	A.8.3	Manejo de los medios						
	A.8.3.3	Transferencia de medios físicos	Cuaderno de control de historias salientes de admisión	Establecer protocolos que aseguren la información en su transferencia física tanto en la salida como su recepción en el área de destino, garantizando que no sea manipulada.		X	X	

NTP-ISO 27001:2014 Controles de Seguridad			Controles actuales	Justificación de inclusión - comentarios-	Controles seleccionados y razones de selección			Comentarios
					RL	RN	EVR	
Cláusula	**Sección**	**Objetivo del Control**						
A.9 Control de Acceso	A.9.1	Requisitos del negocio para el Control de acceso						
	A.9.1.1	Política de control de acceso	Acceso medianamente vigilado al área de admisión por el personal del área	El control de acceso debe estar documentado y ser de conocimiento del personal		X	X	En caso de emergencia, se rompe este procedimiento debido a la situación de urgencia
	A.9.2	Gestión de acceso de usuario						
	A.9.2.3	Gestión de derechos de accesos privilegiados	Actualmente cierto tipo de personal cuanta con acceso a las historias clínicas	Se debe contar con una correcta gestión de privilegios, impidiendo el acceso a colaboradores de otras áreas		X	X	

NTP-ISO 27001:2014 Controles de Seguridad			Controles actuales	Justificación de inclusión -comentarios-	Controles seleccionados y razones de selección			Comentarios
					RL	RN	EVR	
Cláusula	Sección	Objetivo del Control						
A.11 Seguridad Física y del Entorno	A.11.1	Áreas Seguras						
	A.11.1.1	Perímetro de Seguridad Física	El archivo se encuentra custodiado en el área de Admisión	Establecer un límite de acceso entre los pacientes y los trabajadores del establecimiento		X		
	A.11.1.2	Controles de ingreso físico		Personal debidamente identificado en todo momento		X		Implementar el uso obligatorio del fotocheck en un lugar visible
	A.11.1.3	Asegurar oficinas, áreas e instalaciones		No permitir el acceso al público a las instalaciones que almacenan información sensible		X		La información del personal y su lugar de trabajo no debe ser accesible a personas externas
	A.11.1.4	Protección contra amenazas externas y ambientales	En la actualidad, no se cuenta con extintores ni un plan de seguridad en casos de sismo	Implementar medidas para proteger información critica frente a incidentes naturales como provocados -incendios-		X		Implementar un sistema contra incendios en el archivo. Realizar el aseguramiento de los archivadores al piso y techo, alarmas contra incendios

NTP-ISO 27001:2014 Controles de Seguridad			Controles actuales	Justificación de inclusión - comentarios-	Controles seleccionados y razones de selección			Comentarios
					RL	RN	EVR	
Cláusula	Sección	Objetivo del Control						
A.11 Seguridad Física y del Entorno	A.11.2	Equipo						
	A.11.2.1	Emplazamiento y protección de los equipos		Evitar los accesos no autorizados		X		
	A.11.2.5	Remoción de activos	Cuaderno de control de historias clínicas salientes del área de admisión	El establecimiento deberá establecer políticas para que el retiro de la información sea solo para cumplir servicios de atención de pacientes		X	X	Cuidado con la información médica para fines académicos, ya que el establecimiento tiene unidad de docencia e investigación
	A.11.2.8	Equipo de usuario desatendido		Se debe mantener la seguridad de los equipos a pesar que no se utilicen por el personal a cargo		X		Establecer políticas de bloqueo automático de equipo, que sea necesario bloquear el equipo en caso de ausentismo por el personal del servicio
	A.11.2.9	Política de escritorio limpio y pantalla limpia		Evitar la exposición de información sensible sobe nuestros escritorios que pueda ser sustraído por un agente externo		X		Establecer políticas que indiquen a los colaboradores los cuidados frente una situación de amenaza

NTP-ISO 27001:2014 Controles de Seguridad			Controles actuales	Justificación de inclusión -comentarios-	Controles seleccionados y razones de selección			Comentarios
					RL	RN	EVR	
Cláusula	Sección	Objetivo del Control						
A.12 Seguridad de las Operaciones	A.12.1	Procedimientos y responsabilidades operativas						
	A.12.1.1	Documentos de procedimientos operacionales	Se cuenta con flujo grama que no describe el tipo de paciente, si es nuevo o continuador	Se requiere la información de los procesos con la finalidad que se entienda los flujos de información crítica y se realice una evaluación continua del nivel de riesgo existente		X		
	A.12.3	Respaldo						
	A.12.3.1	Respaldo de información	No se cuenta con ningún tipo de respaldo	Establecer una política de respaldo que garantice la continuidad de la atención y mitigue la perdida de datos ante cualquier incidente		X		
	A.12.5	Control de Software Operacional						
	A.12.5.1	Instalación de software en sistemas operacionales		Establecer procedimientos que garanticen la correcta instalación, incluyendo parches de seguridad y actualizaciones		X		
	A.12.6	Gestión de vulnerabilidades técnicas						
	A.12.6.1	Restricciones en la instalación de software		Establecer una política que evite que el personal pueda instalar aplicaciones no licenciadas o permitidas		X		La instalación de software debe estar bloqueada para todos los usuarios.

NTP-ISO 27001:2014 Controles de Seguridad			Controles actuales	Justificación de inclusión - comentarios-	Controles seleccionados y razones de selección			Comentarios
					RL	RN	EVR	
Cláusula	Sección	Objetivo del Control						
A.13 Seguridad de las comunicaciones	A.13.2	Transferencia de información						
	A.13.2.4	Acuerdos de confidencialidad o no-revelación		La institución deberá establecer acuerdos que detallen la confidencialidad de sus trabajadores y proveedores en caso sea necesario		X	X	
A.16 Gestión de incidentes de Seguridad de la Información	A.16.1	Gestión de incidentes de seguridad de la información y mejoras						
	A.16.1.5	Respuesta a incidentes de seguridad de la información		Establecer el procedimiento para la respuesta ante un incidente de seguridad de la información		X		
	A.16.1.6	Aprendizaje de incidentes de seguridad de la información		Almacenar estos documentos que sirvan como base para la disminución de incidentes		X		
	A.16.1.7	Control de evidencia		Ante un incidente, demos Recoger evidencias que pueden ser utilizados en procesos judiciales	X	X		Comunicarse con la policía, fiscal para recoger evidencia

NTP-ISO 27001:2014 Controles de Seguridad			Controles actuales	Justificación de inclusión -comentarios-	Controles seleccionados y razones de selección			Comentarios
					RL	RN	EVR	
Cláusula	Sección	Objetivo del Control						
A.17 Aspectos de Seguridad de la información para la gestión de continuidad del negocio	A.17.1	Seguridad de la Información en la Continuidad						
	A.17.1.1	Planeación de seguridad de la información en la continuidad		Es necesario identificar aquellos activos de información que son críticos para asegurar la continuidad de las operaciones de la institución.		X	X	
	A.17.1.2	Implementación de seguridad de la información en la continuidad		Los planes de continuidad deben proteger los activos previamente identificados, asegurando la disponibilidad y así hacer más fácil su recuperación		X	X	
	A.17.1.3	Verificación, revisión y evaluación de seguridad de la información en la continuidad		Ver el nivel de protección de la información frente a diversos escenarios		X	X	

NTP-ISO 27001:2014 Controles de Seguridad			Controles actuales	Justificación de inclusión - comentarios-	Controles seleccionados y razones de selección			Comentarios
					RL	RN	EVR	
Cláusula	Sección	Objetivo del Control						
A.18 Cumplimiento	A.18.1	Cumplimiento con requerimientos legales y contractuales						
	A.18.1.1	Identificación de legislación aplicable y requerimientos contractuales		Se debe contar con la documentación referida a la normativa relacionada a seguridad de la información	X			
	A.18.1.3	Protección de información documentada		El establecimiento debe contar con procedimientos que determinen las condiciones de almacenamiento de información física así como el desecho	X	X	X	Se debe tener especial cuidado en el caso de las historias clínicas, mediante Norma Técnica tienen procedimientos específicos para su almacén y desecho
	A.18.1.4	Privacidad y protección de información de información personal identificable		Se debe proteger la información de acuerdo a la ley de protección de datos personales	X	X	X	
	A.18.2	Revisiones de Seguridad de la Información						
	A.18.2.1	Revisión independiente de Seguridad de la Información		Se debe revisar periódicamente debido a los cambios organizacionales y legislativos		X		
	A.18.2.2	Cumplimiento con políticas y estándares de seguridad		Las políticas de seguridad de la información deben ser evaluadas periódicamente respecto a si cumplen con los objetivos de la organización		X		