PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

FACULTAD DE CIENCIAS E INGENIERÍA

ANEXOS

Tesis para optar por el Título de Ingeniero Informático, que presenta el bachiller:

Vasco Rodrigo Talavera Álvarez

ASESOR: Mg. Moisés Villena Aguilar

Lima, Mayo del 2015

Tabla de contenido

ANEXO 1: CARTA DE PRESENTACIÓN DEL PROYECTO A LA INSTITUCIÓN___ 3

ANEXO 2: AVAL DE LA INSTITUCIÓN EN EL DESARROLLO DEL PROYECTO__ 4

ANEXO 3: VALIDACIÓN DEL MODELADO DE PROCESOS DE NEGOCIO DESARROLLADO _____ 5

ANEXO 4: SUBPROCESOS DEL PROCESO DE ADMISIÓN DE PACIENTES ____ 6

ANEXO 5: SUBPROCESOS DEL PROCESO EMISIÓN DE COPIA DE HISTORIA CLÍNICA_____ 9

ANEXO 6: INVENTARIO DE ACTIVOS DE INFORMACIÓN _____ 10

ANEXO 7: MATRIZ DE RIESGOS_____ 13

ANEXO 8: DECLARACIÓN DE APLICABILIDAD _____ 67

Anexo 1: Carta de presentación del proyecto a la institución

FACULTAD DE
CIENCIAS E
INGENIERÍA
ESPECIALIDAD DE
INGENIERÍA INFORMÁTICA

PONTIFICIA
UNIVERSIDAD
CATÓLICA
DEL PERÚ

Lima, 14 de octubre de 2014

Ingeniera
NANCY ALVARADO LEGUA
Jefe – Oficina de Estadística e Informática
Instituto Nacional Materno Perinatal
Presente.-

De mi consideración,

Tengo el agrado de dirigirme a usted para poner en su conocimiento que la Facultad de Ciencias e Ingeniería de la Pontificia Universidad Católica del Perú, ofrece la carrera de Ingeniería Informática, la cual en su currícula cuenta con los cursos de Proyecto de Tesis I y II.

El objetivo del curso es llevar a cabo el desarrollo de un proyecto en el área de informática donde se demuestre la aplicación de habilidades y conocimientos adquiridos durante los años de estudio en la especialidad, por lo cual deseo solicitar a usted se brinde las facilidades al alumno *Vasco Rodrigo TALAVERA ALVAREZ código, 20064627* para la realización de su proyecto en el mencionado curso.

Se adjunta a la presente el resumen de actividades programadas para el proyecto, asimismo cabe señalar que no se mencionará en ningún caso el nombre de la empresa. De ser necesaria alguna coordinación adicional, le agradecería comunicarse con el Ing. Moises Villena Aguilar, asesor de la tesis del mencionado alumno al correo Villena.ma@pucp.edu.pe .

Agradeciendo por anticipado su valiosa colaboración, se despide

Muy atentamente,

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ
Departamento de Ingeniería
Mag. JORAN VALDEZON M.
Coordinador de Especialidad
Ingeniería Informática

MINISTERIO DE SALUD
Instituto Nacional Materno Perinatal
Nancy Betty Alvarado Legua
Jefe de la Oficina de Estadística e Informática
C.I.P. 141221

Anexo 2: Aval de la institución en el desarrollo del proyecto

PERÚ | Ministerio de Salud | INSTITUTO NACIONAL MATERNO PERINATAL | Oficina de Estadística e Informática

"Año de la Promoción de la Industria Responsable y del Compromiso Climático"

Señor,
Mg. Johan Baldeón Medrano
Coordinador de la especialidad de Ingeniería Informática
Pontificia Universidad Católica del Perú
Presente.-

De mi consideración.

Por medio de la presente carta se informa que la institución tiene conocimiento y avala los documentos que ha desarrollado el alumno Vasco Rodrigo Talavera Álvarez con código 20064627, como parte de su proyecto denominado "Diseño de un Sistema de Gestión de Seguridad de la Información para una entidad estatal de salud de acuerdo a la ISO/IEC 27001:2013", para la obtención del Título de Ingeniería Informática, y reconoce la idoneidad y pertinencia de los mismos en relación a la realidad del Instituto Nacional Materno Perinatal.

A continuación se presenta el detalle de los documentos presentados de acuerdo a los respectivos resultados esperados:

Actividades	Resultados esperados
1. Elaborar de la documentación exigida por la norma ISO 27001.	Documentación exigida por la norma ISO 27001 como paso inicial al proceso de Diseño del SGSI.
2. Realizar el modelado de los procesos correspondientes al alcance del Sistema de Gestión de Seguridad de la Información.	Mapa de procesos del alcance del proyecto.
3. Elaborar una metodología de análisis de riesgos y valoración de activos.	Metodología de análisis de riesgos Metodología de valoración de activos
4. Elaborar el mapa de riesgos de los procesos del alcance.	Mapa de Riesgos
5. Elaborar la declaración de aplicabilidad.	Declaración de aplicabilidad

Se expide la presente carta para los fines que el tesista requiera dentro de las actividades correspondientes al curso "Proyecto de Tesis 2".

Atentamente,

MINISTERIO DE SALUD
Instituto Nacional Materno Perinatal
Nancy Betty Alvarado Legua
Jefe de la Oficina de Estadística e Informática
C.I.P. 141621

ING. NANCY ALVARADO LEGUA
Jefe de la Oficina de Estadística e Informática
Instituto Nacional Materno Perinatal

Anexo 3: Validación del modelado de procesos de negocio desarrollado

Validación de Modelado de Procesos de Negocio

Procesos del Área: Admisión y Consultorios Externos

Mediante la presente el firmante, colaborador del Instituto Nacional Materno Perinatal, valida los procesos de negocio modelados como parte del desarrollo del Proyecto de Fin de Carrera titulado " Diseño de un Sistema de Gestión de Seguridad de la Información para una entidad estatal de salud de acuerdo a la ISO/IEC 27001:2013" estableciendo su correspondencia con los procesos tal y como se llevan a cabo en la institución.

Lima 27 de OCTUBRE de 2014

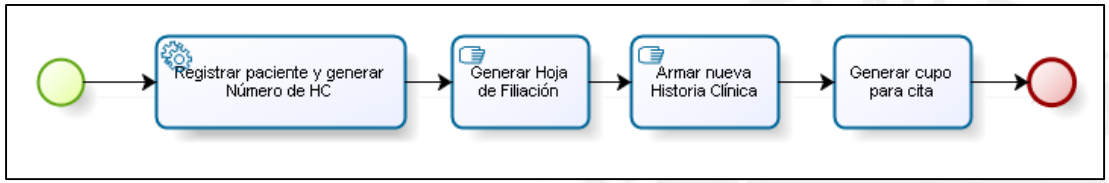
Nombre: NANCY BETTY ALVARADO LEGUA

Cargo: JEFE DE LA OFICINA DE ESTADISTICA E INFORMATICA

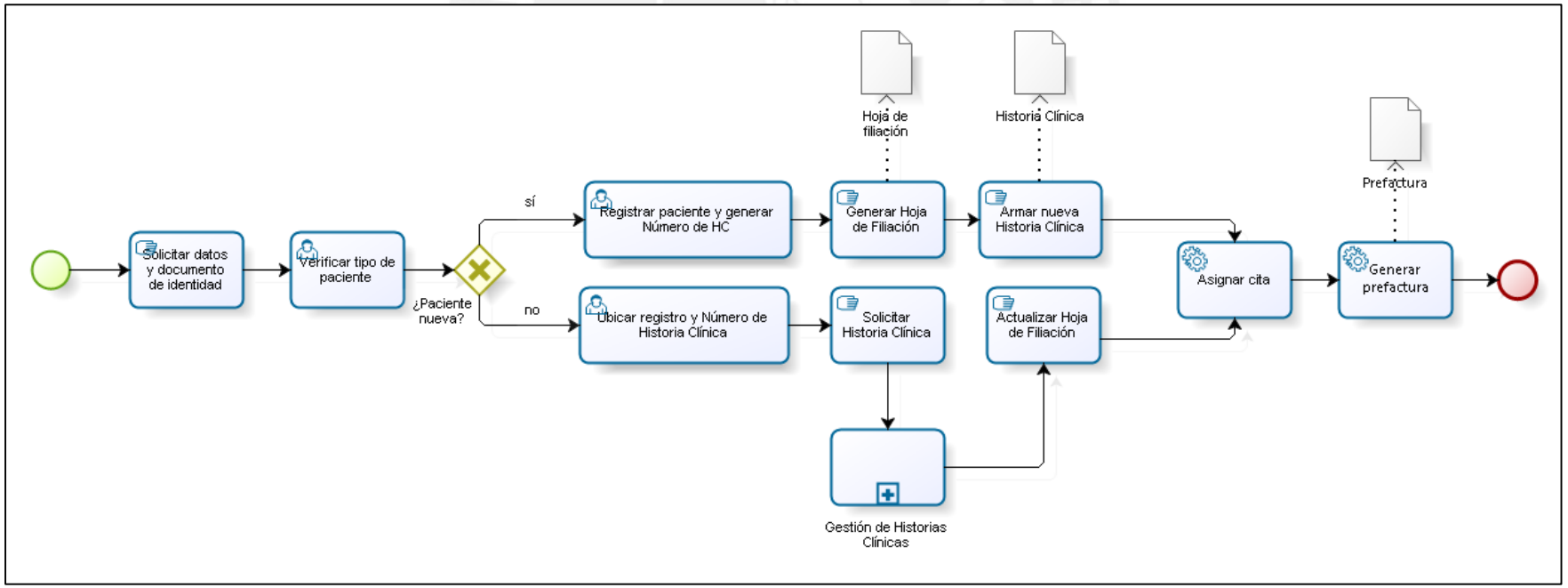
Firma: MINISTERIO DE SALUD Instituto Nacional Materno Perinatal Nancy Betty Alvarado Legua Jefe de la Oficina de Estadística e Informática C.I.P. 141621

Anexo 4: Subprocesos del Proceso de Admisión de Pacientes

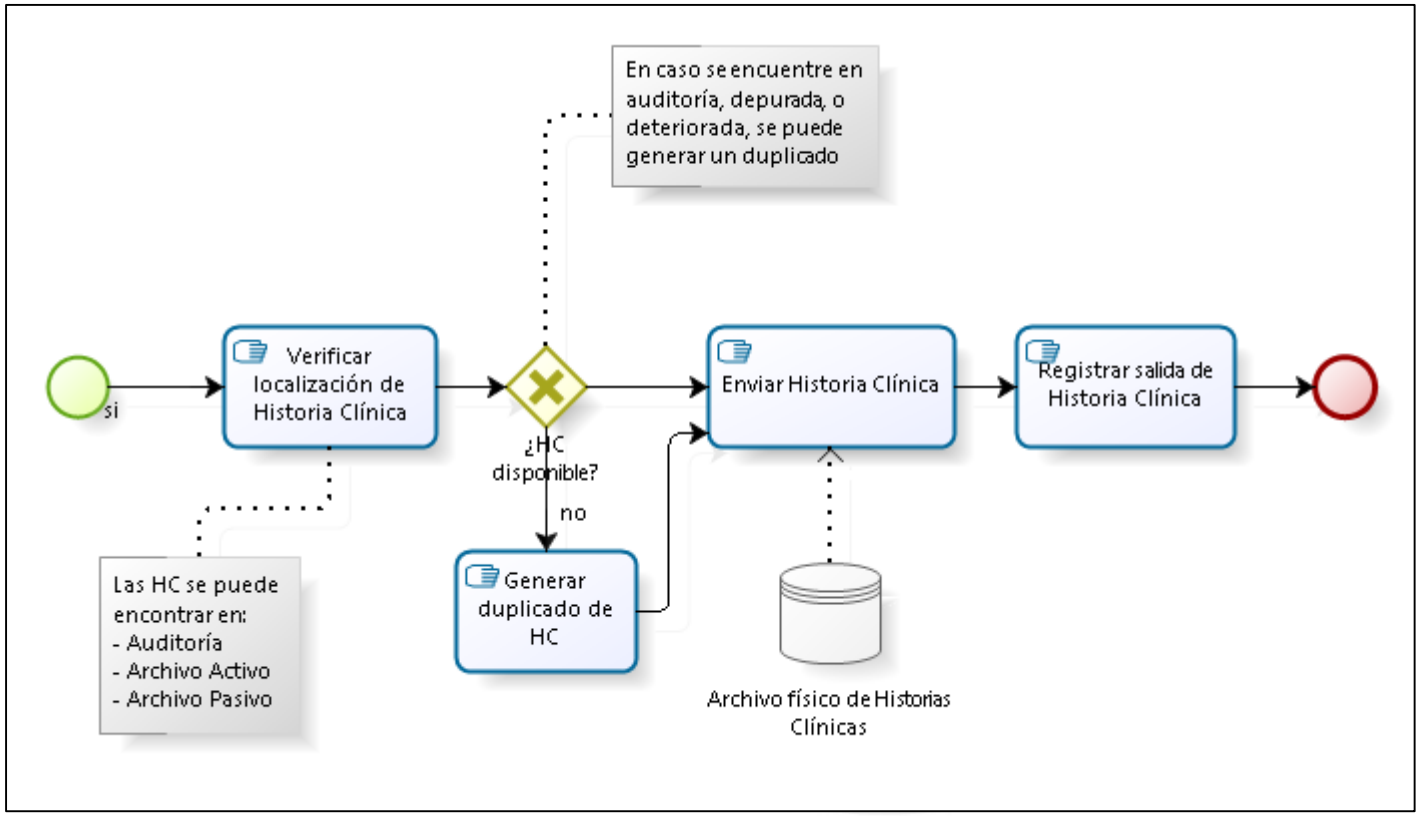
Sub Proceso “Generar Historia Clínica”



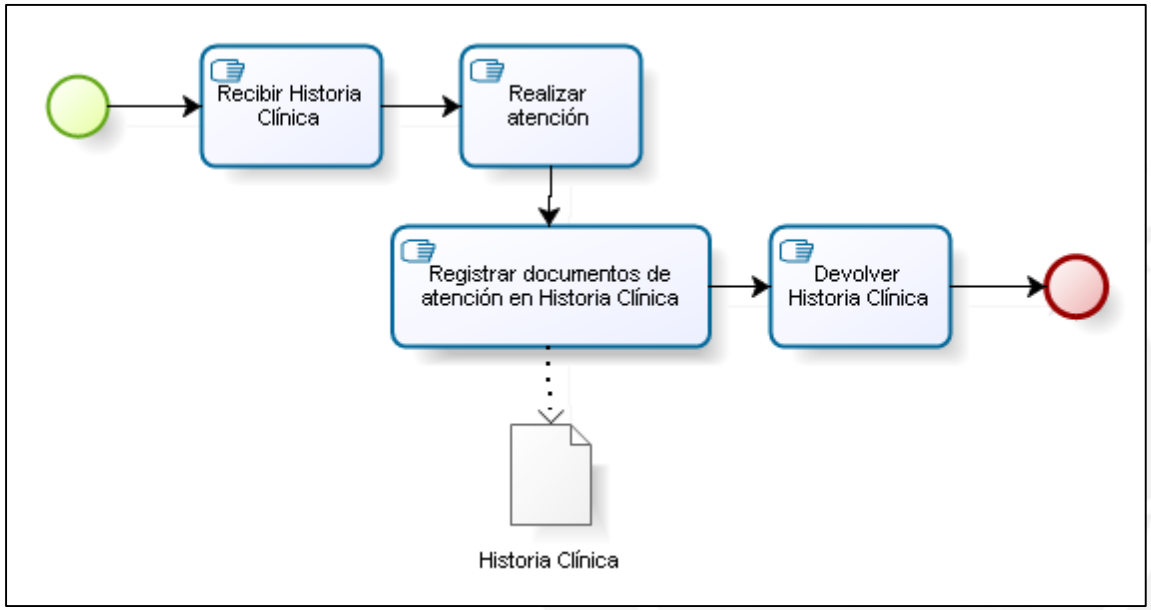
Sub Proceso “Atender paciente no SIS”



Sub Proceso “Gestión de Historias Clínicas”



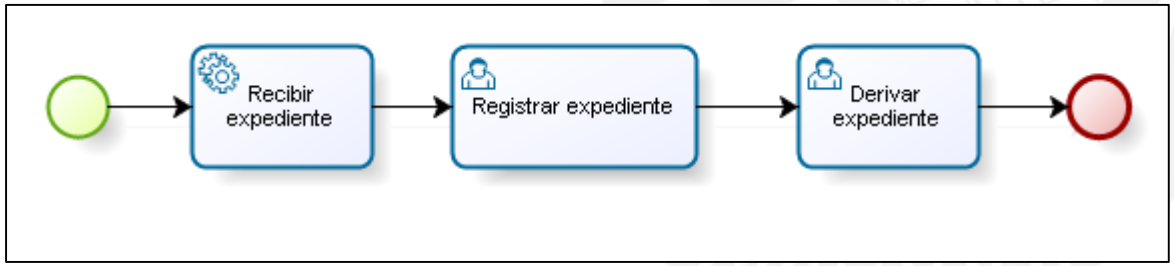
Sub Proceso “Atender paciente”



Anexo 5: Subprocesos del Proceso Emisión de copia de Historia Clínica

Sub Proceso “Recepción y derivación de solicitud”

Sub Proceso “Recepción y derivación de expediente”



Anexo 6: Inventario de activos de información

Nro. Activo	Proceso de Negocio Asociado	Nombre del Activo	Descripción del Activo	Clasificación del Activo	Propietario del Activo	Valoración parcial			Val. Final
						C	I	D	
ACT001	Admisión de pacientes	Sistema de Gestión Hospitalario	Utilizado para la gestión de citas y generación de número de Historia Clínica.	Activo Primordial	Admisión	4	3	4	4
ACT002	Admisión de pacientes	Archivo físico de Historias Clínicas	Archivo activo de Historias Clínicas, que contiene aquellas que pueden ser requeridas más frecuentemente.	Activo Primordial	Archivo	4	4	4	4
ACT003	Admisión de pacientes	Boleta de atención	Documento que detalla la información para realizar el pago de la cita por parte de la paciente.	Activo no Primordial	Paciente	1	1	1	1
ACT004	Admisión de pacientes	Cita médica	Documento exclusivo que presenta el paciente como comprobante de su atención programada consultorios externos.	Activo no Primordial	Paciente	1	2	2	2
ACT005	Admisión de pacientes	Tarjeta de citas	Tarjeta de seguimiento de la programación de las citas de la paciente en las diferentes especialidades cuando no se encuentra embarazada.	Activo Primordial	Paciente	2	2	1	2
ACT006	Admisión de pacientes	Carné de atención materno perinatal	Documento de seguimiento de los controles realizados a lo largo de las citas del embarazo.	Activo Primordial	Paciente	3	2	1	2
ACT007	Admisión de pacientes	Carta poder de paciente	Documento en el que la paciente autoriza a un tercero a solicitar una copia de su Historia Clínica.	Activo Primordial	Mesa de Partes	2	2	2	2

Nro. Activo	Proceso de Negocio Asociado	Nombre del Activo	Descripción del Activo	Clasificación del Activo	Propietario del Activo	Valoración parcial			Val. Final
						C	I	D	
ACT008	Admisión de pacientes	Informe diario de atenciones en consultorios externos	Informe en que se detalla las citas que se han atendido por doctor y por consultorio durante el día.	Activo no Primordial	Admisión, Oficina de Estadística e Informática	3	2	1	2
ACT009	Admisión de pacientes	Cuaderno de registro de entradas y salidas de Historias Clínicas hacia Consultorios Externos	Contiene el detalle de ingresos y salidas de Historias Clínicas desde el Admisión hacia los Consultorios Externos para la atención de las pacientes.	Activo Primordial	Admisión	2	3	4	3
ACT010	Emisión de Copia de Historia Clínica	Solicitud de copia	Documento requerido para iniciar el proceso de Copia de una Historia Clínica.	Activo Primordial	Mesa de Partes	2	2	3	2
ACT011	Emisión de Copia de Historia Clínica	Oficio de solicitud de copia por parte de la PNP	Documento emitido por la PNP para solicitar una copia de historia clínica.	Activo Primordial	Mesa de Partes	4	3	3	3
ACT012	Emisión de Copia de Historia Clínica	Cuaderno de registro de control de atención de casos	Se lleva el registro de los cargos de la entrega de las copias a Mesa de Partes.	Activo Primordial	Admisión	2	3	3	3
ACT013	Emisión de Copia de Historia Clínica	Máquina fotocopiadora	Utilizada para generar el duplicado de la Historia Clínica.	Activo no Primordial	Admisión	-	-	2	2

Nro. Activo	Proceso de Negocio Asociado	Nombre del Activo	Descripción del Activo	Clasificación del Activo	Propietario del Activo	Valoración parcial			Val. Final
						C	I	D	
ACT014	Emisión de Copia de Historia Clínica	Carta de entrega de copia a PNP	Documento anexado al inicio de la copia de Historia Clínica solicitada por PNP.	Activo no Primordial	Oficina de Estadística e Informática	1	2	1	1
ACT015	Todos	Computadora de escritorio	Equipo de cómputo utilizado por el área ara el acceso a los sistemas de información, impresión de facturas, etc.	Activo no Primordial	Áreas del servicio de Consultorios Externos	3	-	2	3
ACT016	Todos	Historia Clínica	Documento legal que contiene la información sobre las atenciones diagnósticos recibidos por la paciente.	Activo Primordial	Archivo	4	4	4	4
ACT017	Todos	Cuaderno de registro de entradas y salidas de Historias Clínicas	Contiene el detalle de ingresos y salidas de Historias Clínicas desde el Archivo para diferentes usos y áreas que lo requieran.	Activo Primordial	Archivo	3	3	3	3
ACT018	Todos	Sistema de Trámite Documentario	Registra la información de los trámites solicitados, generando un código para cada uno además de la información de seguimiento del mismo a través de las diferentes áreas que realicen las atenciones relacionadas. Además permite derivar el trámite de un área a otra.	Activo no Primordial	Todos	2	3	1	2
ACT019	Todos	Servidor de aplicaciones	Equipo de cómputo que centraliza y almacena la información utilizada en los sistemas de información de la institución.	Activo Primordial	Todos	4	4	4	4

Anexo 7: Matriz de Riesgos

Proceso: Admisión de Pacientes

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.
Acreditar paciente con SIS	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
Acreditar paciente con SIS	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 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
Acreditar paciente con SIS	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

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.
Acreditar paciente con SIS	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
Acreditar paciente con SIS	Posible denegación de atención como paciente SIS falta de documentos del paciente	Clientes, servicios y prácticas 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
Armar expediente de paciente para atención	Posible error al crear el documento del paciente por error del operador al suscribir los datos	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 de lo indicado por el paciente o distracción	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.	Niv. de Riesgo	Estr. de Rpta.
Armar expediente de paciente para atención	Posible demora en la atención del paciente debido a 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 expediente de paciente para atención	Posible denegación de atención como paciente SIS falta de documentos del paciente	Clientes, servicios y prácticas institucionales	Eventos Externos	El usuario no cuenta con los documentos requeridos para su reconocimie nto como paciente SIS	Se deniega el acceso a los servicios del paciente a través del seguro SIS	Posible	Muy bajo	Bajo	Aceptar
Armar expediente de paciente para atención	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
Registrar paciente y generar Número de HC	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.	Niv. de Riesgo	Estr. de Rpta.
Registrar paciente y generar Número de HC	Posible imposibilidad de atender al paciente originada por daño en la información o el sistema debido a malware	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Débil control de acceso a la red Equipos con puertos usb desbloqueados	Pérdida o filtración de información sensible	Posible	Muy alto	Alto	Reducir
Registrar paciente y generar Número de HC	Posible imposibilidad de atender al paciente originada por daño en la información o el sistema debido a un ataque de hacker	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Débil control de acceso a la red Equipos con puertos usb desbloqueados	Pérdida o filtración de información sensible	Posible	Muy alto	Alto	Reducir
Registrar paciente y generar Número de HC	Posible demora en la atención del paciente originada por indisponibilidad del sistema	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
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 de lo indicado por el paciente o distracción	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.	Niv. de Riesgo	Estr. de Rpta.
Registrar paciente y generar Número de HC	Posible error en la generación del número de Historia Clínica del paciente originada por fallo en el sistema	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Se presenta un fallo en el sistema de registro que genera un número erróneo o ya asignado a otra paciente	Demora en la atención de la paciente	Posible	Bajo	Moderado	Reducir
Registrar paciente y generar Número de HC	Posible pérdida de información originada por un fallo de hardware	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Se presenta un fallo en el hardware del equipo del operador que produce su apagado o mal funcionamie nto	Pérdida de información y demora en la atención de la paciente	Posible	Bajo	Moderado	Reducir
Registrar paciente y generar Número de HC	Posible pérdida de información originada por un fallo de software	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Se presenta un fallo en el software del equipo del operador produciendo un mal funcionamie nto del mismo	Pérdida de información y demora en la atención de la paciente	Posible	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.	Niv. de Riesgo	Estr. de Rpta.
Registrar paciente y generar Número de HC	Posible pérdida de información originada por un fallo de comunicación con el servidor de la aplicación	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Se presenta un fallo en la comunicación con el servidor	Pérdida de información y demora en la atención de la paciente	Posible	Bajo	Moderado	Reducir
Registrar paciente y generar Número de HC	Posible pérdida de conexión con el sistema originada por falla eléctrica	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Se presenta una falla en el suministro eléctrico que ocasiona el apagado de los equipos	Pérdida de información y demora en la atención de la paciente	Posible	Bajo	Moderado	Reducir
Generar Hoja de Filiación	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	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.	Niv. de Riesgo	Estr. de Rpta.
Generar Hoja de Filiación	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 en el sistema	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 Hoja de Filiación	Posible demora en la atención del paciente debido a 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
Generar Hoja de Filiación	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.	Niv. de Riesgo	Estr. de Rpta.
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 o distracción	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 en el sistema	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
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

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.
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 en su lugar para realizar la atención del paciente	Demora en el tiempo de atención del paciente	Posible	Muy bajo	Bajo	Aceptar
Generar cupo para 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 concurrencia entre dos usuarios queriendo registrar un mismo campo	Generación de doble cita en un mismo horario	Poco probable	Bajo	Bajo	Aceptar
Generar cupo para cita	Posible imposibilidad de atender al paciente originada por daño en la información o el sistema debido a malware	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Débil control de acceso a la red Equipos con puertos usb desbloqueados	Pérdida o filtración de información sensible	Posible	Muy alto	Alto	Reducir
Generar cupo para cita	Posible imposibilidad de atender al paciente originada por daño en la información o el sistema debido a un ataque de hacker	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Débil control de acceso a la red Equipos con puertos usb desbloqueados	Pérdida o filtración de información sensible	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.	Niv. de Riesgo	Estr. de Rpta.
Generar cupo para cita	Posible pérdida de información originada por un fallo de hardware	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Se presenta un fallo en el hardware del equipo del operador que produce su apagado o mal funcionamiento	Pérdida de información y demora en la atención de la paciente	Posible	Bajo	Moderado	Reducir
Generar cupo para cita	Posible pérdida de información originada por un fallo de software	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Se presenta un fallo en el software del equipo del operador produciendo un mal funcionamiento del mismo	Pérdida de información y demora en la atención de la paciente	Posible	Bajo	Moderado	Reducir
Generar cupo para cita	Posible demora en la atención del paciente originada por indisponibilidad del sistema	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

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.
Generar cupo para cita	Posible pérdida de conexión con el sistema originada por falla eléctrica	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Se presenta una falla en el suministro eléctrico que ocasiona el apagado de los equipos	Pérdida de información y demora en la atención de la paciente	Posible	Bajo	Moderado	Reducir
Generar cita para paciente SIS	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
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 en el sistema	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
Cobrar cita a paciente	Posible demora en la atención del paciente originada por indisponibilidad del sistema	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

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.
Cobrar cita a paciente	Posible pérdida de información originada por un fallo de hardware	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Se presenta un fallo en el hardware del equipo del operador que produce su apagado o mal funcionamiento	Pérdida de información y demora en la atención de la paciente	Posible	Bajo	Moderado	Reducir
Cobrar cita a paciente	Posible pérdida de información originada por un fallo de software	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Se presenta un fallo en el software del equipo del operador produciendo un mal funcionamiento del mismo	Pérdida de información y demora en la atención de la paciente	Posible	Bajo	Moderado	Reducir
Cobrar cita a paciente	Posible pérdida de conexión con el sistema originada por falla eléctrica	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Se presenta una falla en el suministro eléctrico que ocasiona el apagado de los equipos	Pérdida de información y demora en la atención de la paciente	Posible	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.	Niv. de Riesgo	Estr. de Rpta.
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
Generar boleta de pago	Posible demora en la atención del paciente originada por indisponibilidad del sistema	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
Generar boleta de pago	Posible imposibilidad de atender al paciente originada por daño en la información o el sistema debido a malware	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Débil control de acceso a la red Equipos con puertos usb desbloqueados	Pérdida o filtración de información sensible	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.	Niv. de Riesgo	Estr. de Rpta.
Generar boleta de pago	Posible imposibilidad de atender al paciente originada por daño en la información o el sistema debido a un ataque de hacker	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Débil control de acceso a la red Equipos con puertos usb desbloqueados	Pérdida o filtración de información sensible	Posible	Muy alto	Alto	Reducir
Generar boleta de pago	Posible pérdida de información originada por un fallo de hardware	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Se presenta un fallo en el hardware del equipo del operador que produce su apagado o mal funcionamiento	Pérdida de información y demora en la atención de la paciente	Posible	Bajo	Moderado	Reducir
Generar boleta de pago	Posible pérdida de información originada por un fallo de software	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Se presenta un fallo en el software del equipo del operador produciendo un mal funcionamiento del mismo	Pérdida de información y demora en la atención de la paciente	Posible	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.	Niv. de Riesgo	Estr. de Rpta.
Generar boleta de pago	Posible pérdida de conexión con el sistema originada por falla eléctrica	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Se presenta una falla en el suministro eléctrico que ocasiona el apagado de los equipos	Pérdida de información y demora en la atención de la paciente	Posible	Bajo	Moderado	Reducir
Generar cita para paciente SIS	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 concurrencia entre dos usuarios queriendo registrar un mismo campo	Generación de doble cita en un mismo horario	Poco probable	Bajo	Bajo	Aceptar
Generar cita para paciente SIS	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.	Niv. de Riesgo	Estr. de Rpta.
Generar cita para paciente SIS	Posible pérdida de información originada por un fallo de hardware	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Se presenta un fallo en el hardware del equipo del operador que produce su apagado o mal funcionamiento	Pérdida de información y demora en la atención de la paciente	Posible	Bajo	Moderado	Reducir
Generar cita para paciente SIS	Posible pérdida de información originada por un fallo de software	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Se presenta un fallo en el software del equipo del operador produciendo un mal funcionamiento del mismo	Pérdida de información y demora en la atención de la paciente	Posible	Bajo	Moderado	Reducir
Generar cita para paciente SIS	Posible imposibilidad de atender al paciente originada por daño en la información o el sistema debido a malware	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Débil control de acceso a la red Equipos con puertos usb desbloqueados	Pérdida o filtración de información sensible	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.	Niv. de Riesgo	Estr. de Rpta.
Generar cita para paciente SIS	Posible imposibilidad de atender al paciente originada por daño en la información o el sistema debido a un ataque de hacker	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Débil control de acceso a la red Equipos con puertos usb desbloqueados	Pérdida o filtración de información sensible	Posible	Muy alto	Alto	Reducir
Generar cita para paciente SIS	Posible demora en la atención del paciente originado por indisponibilidad del sistema	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
Generar cita para paciente SIS	Posible pérdida de conexión con el sistema originada por falla eléctrica	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Se presenta una falla en el suministro eléctrico que ocasiona el apagado de los equipos	Pérdida de información y demora en la atención de la paciente	Posible	Bajo	Moderado	Reducir
Registrar 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.	Niv. de Riesgo	Estr. de Rpta.
Registrar 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
Registrar paciente y generar Número de HC	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
Registrar paciente y generar Número de HC	Posible demora en la atención del paciente originado por indisponibilidad del sistema	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
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 de lo indicado por el paciente o distracción	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.	Niv. de Riesgo	Estr. de Rpta.
Registrar paciente y generar Número de HC	Posible error en la generación del número de Historia Clínica del paciente originada por fallo en el sistema	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Se presenta un fallo en el sistema de registro que genera un número erróneo o ya asignado a otra paciente	Demora en la atención de la paciente	Posible	Bajo	Moderado	Reducir
Registrar paciente y generar Número de HC	Posible imposibilidad de atender al paciente originada por daño en la información o el sistema debido a malware	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Débil control de acceso a la red Equipos con puertos usb desbloqueados	Pérdida o filtración de información sensible	Posible	Muy alto	Alto	Reducir
Registrar paciente y generar Número de HC	Posible imposibilidad de atender al paciente originada por daño en la información o el sistema debido a un ataque de hacker	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Débil control de acceso a la red Equipos con puertos usb desbloqueados	Pérdida o filtración de información sensible	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.	Niv. de Riesgo	Estr. de Rpta.
Registrar paciente y generar Número de HC	Posible pérdida de información originada por un fallo de hardware	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Se presenta un fallo en el hardware del equipo del operador que produce su apagado o mal funcionamiento	Pérdida de información y demora en la atención de la paciente	Posible	Bajo	Moderado	Reducir
Registrar paciente y generar Número de HC	Posible pérdida de información originada por un fallo de software	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Se presenta un fallo en el software del equipo del operador produciendo un mal funcionamiento del mismo	Pérdida de información y demora en la atención de la paciente	Posible	Bajo	Moderado	Reducir
Registrar paciente y generar Número de HC	Posible pérdida de información originada por un fallo de comunicación con el servidor de la aplicación	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Se presenta un fallo en la comunicación con el servidor	Pérdida de información y demora en la atención de la paciente	Posible	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.	Niv. de Riesgo	Estr. de Rpta.
Registrar paciente y generar Número de HC	Posible pérdida de conexión con el sistema originada por falla eléctrica	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Se presenta una falla en el suministro eléctrico que ocasiona el apagado de los equipos	Pérdida de información y demora en la atención de la paciente	Posible	Bajo	Moderado	Reducir
Ubicar registro y Número de 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
Ubicar registro y Número de Historia Clínica	Posible demora en la atención del paciente originado por indisponibilidad del sistema	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
Ubicar registro y Número de Historia Clínica	Posible pérdida de conexión con el sistema originada por falla eléctrica	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Se presenta una falla en el suministro eléctrico que ocasiona el apagado de los equipos	Pérdida de información y demora en la atención de la paciente	Posible	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.	Niv. de Riesgo	Estr. de Rpta.
Generar Hoja de Filiación	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
Generar Hoja de Filiación	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 Hoja de Filiación	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 en el sistema	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

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.
Generar Hoja de Filiación	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
Actualizar Hoja de Filiación	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
Actualizar Hoja de Filiación	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 en el sistema	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

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.
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 o distracción	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 en el sistema	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
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

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.
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 en su lugar para realizar la atención del paciente	Demora en el tiempo de atención del paciente	Posible	Muy bajo	Bajo	Aceptar
Asignar 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 concurrencia entre dos usuarios queriendo registrar un mismo campo	Generación de doble cita en un mismo horario	Poco probable	Bajo	Bajo	Aceptar
Asignar 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

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.
Asignar cita	Posible pérdida de información originada por un fallo de hardware	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Se presenta un fallo en el hardware del equipo del operador que produce su apagado o mal funcionamiento	Pérdida de información y demora en la atención de la paciente	Posible	Bajo	Moderado	Reducir
Asignar cita	Posible pérdida de información originada por un fallo de software	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Se presenta un fallo en el software del equipo del operador produciendo un mal funcionamiento del mismo	Pérdida de información y demora en la atención de la paciente	Posible	Bajo	Moderado	Reducir
Asignar cita	Posible demora en la atención del paciente originado por indisponibilidad del sistema	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

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.
Asignar cita	Posible pérdida de conexión con el sistema originada por falla eléctrica	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Se presenta una falla en el suministro eléctrico que ocasiona el apagado de los equipos	Pérdida de información y demora en la atención de la paciente	Posible	Bajo	Moderado	Reducir
Generar prefactura	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 prefactura	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
Generar prefactura	Posible demora en la atención del paciente originada por indisponibilidad del sistema	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

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.
Generar prefactura	Posible pérdida de información originada por un fallo de hardware	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Se presenta un fallo en el hardware del equipo del operador que produce su apagado o mal funcionamiento	Pérdida de información y demora en la atención de la paciente	Posible	Bajo	Moderado	Reducir
Generar prefactura	Posible pérdida de información originada por un fallo de software	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Se presenta un fallo en el software del equipo del operador produciendo un mal funcionamiento del mismo	Pérdida de información y demora en la atención de la paciente	Posible	Bajo	Moderado	Reducir
Generar prefactura	Posible pérdida de conexión con el sistema originada por falla eléctrica	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Se presenta una falla en el suministro eléctrico que ocasiona el apagado de los equipos	Pérdida de información y demora en la atención de la paciente	Posible	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.	Niv. de Riesgo	Estr. de Rpta.
Verificar localización de 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
Verificar localización de Historia Clínica	Posible demora en la atención del paciente originado por desconocimiento de localización de la Historia Clínica	Ejecución, entrega y gestión de procesos	Personal	No se encuentra la Historia Clínica en el Archivo o en los grupos de documentos enviados a otras áreas	Pérdida de información crítica para los procesos asistenciales	Posible	Muy alto	Alto	Reducir
Verificar localización de Historia Clínica	Posible demora en la atención del paciente originado por daño físico de la Historia Clínica	Daños a activos materiales	Procesos Internos	Condiciones de almacenaje y tratamiento poco adecuadas y seguras	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.
Verificar localización de Historia Clínica	Posible demora en la atención del paciente originado por extravío de la Historia Clínica	Daños a activos materiales	Procesos Internos	Condiciones de almacenaje y tratamiento poco adecuadas y seguras	Pérdida de información crítica para los procesos asistenciales Filtración de información	Muy probable	Muy alto	Extremo	Reducir
Verificar localización de Historia Clínica	Posible demora en la atención del paciente originado por robo de la Historia Clínica	Daños a activos materiales	Procesos Internos	Condiciones de almacenaje y tratamiento poco adecuadas y seguras	Pérdida de información crítica para los procesos asistenciales Filtración de información	Muy probable	Muy alto	Extremo	Reducir
Generar duplicado de 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 o distracción	Muy probable	Alto	Alto	Reducir
Generar duplicado de Historia Clínica	Posible error en la creación del documento debido a no contar con la información del paciente	Ejecución, entrega y gestión de procesos	Personal	No se cuenta con una copia de seguridad del documento extraviado	Pérdida de información crítica para los procesos asistenciales	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.	Niv. de Riesgo	Estr. de Rpta.
Generar duplicado de 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 en el sistema	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 duplicado de 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
Generar duplicado de 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
Enviar 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.	Niv. de Riesgo	Estr. de Rpta.
Enviar 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
Enviar 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
Enviar 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.	Niv. de Riesgo	Estr. de Rpta.
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
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
Registrar documentos de atención en Historia Clínica	Posible pérdida de información debido a la 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
Devolver 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.	Niv. de Riesgo	Estr. de Rpta.
Devolver 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 pacienteDemora en el tiempo de atención a la paciente	Poco probable	Medio	Moderado	Reducir
Devolver 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
Verificar monto a pagar	Posible error en el monto a cobrar debido a error en el ingreso de la información por parte 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 de lo indicado por el paciente o distracción	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.	Niv. de Riesgo	Estr. de Rpta.
Verificar monto a pagar	Posible error en el monto a cobrar originada por información errónea ingresada en el sistema	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Se realizó un mal ingreso de la información sobre el cobro por la atención	Pérdida de información y demora en la atención de la paciente	Posible	Bajo	Moderado	Reducir
Verificar monto a pagar	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 monto a pagar	Posible pérdida de información originada por un fallo de hardware	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Se presenta un fallo en el hardware del equipo del operador que produce su apagado o mal funcionamiento	Pérdida de información y demora en la atención de la paciente	Posible	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.	Niv. de Riesgo	Estr. de Rpta.
Verificar monto a pagar	Posible pérdida de información originada por un fallo de software	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Se presenta un fallo en el software del equipo del operador produciendo un mal funcionamiento del mismo	Pérdida de información y demora en la atención de la paciente	Posible	Bajo	Moderado	Reducir
Verificar monto a pagar	Posible demora en la atención del paciente originado por indisponibilidad del sistema	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 monto a pagar	Posible pérdida de conexión con el sistema originada por falla eléctrica	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Se presenta una falla en el suministro eléctrico que ocasiona el apagado de los equipos	Pérdida de información y demora en la atención de la paciente	Posible	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.	Niv. de Riesgo	Estr. de Rpta.
Cobrar prefactura	Posible error en el ingreso de datos 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 de lo indicado por el paciente o distracción	Muy probable	Bajo	Moderado	Reducir
Cobrar prefactura	Posible demora en la atención del paciente originada por indisponibilidad del sistema	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
Cobrar prefactura	Posible demora en la atención del paciente debido a 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.	Niv. de Riesgo	Estr. de Rpta.
Cobrar prefactura	Posible pérdida de información originada por un fallo de hardware	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Se presenta un fallo en el hardware del equipo del operador que produce su apagado o mal funcionamiento	Pérdida de información y demora en la atención de la paciente	Posible	Bajo	Moderado	Reducir
Cobrar prefactura	Posible pérdida de información originada por un fallo de software	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Se presenta un fallo en el software del equipo del operador produciendo un mal funcionamiento del mismo	Pérdida de información y demora en la atención de la paciente	Posible	Bajo	Moderado	Reducir
Cobrar prefactura	Posible pérdida de conexión con el sistema originada por falla eléctrica	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Se presenta una falla en el suministro eléctrico que ocasiona el apagado de los equipos	Pérdida de información y demora en la atención de la paciente	Posible	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.	Niv. de Riesgo	Estr. de Rpta.
Registrar devolución de Historia Clínica	Posible pérdida de información originado por 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 Historias Clínicas	La Historia Clínica no se encuentra disponible en caso se requiera en otra atención	Posible	Medio	Moderado	Reducir
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 su lugar para realizar la atención de la devolución	La Historia Clínica no se encuentra disponible en caso se requiera en otra atención	Posible	Medio	Moderado	Reducir
Archivar Historia Clínica	Posible extravío 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 correspondía	Pérdida de información crítica para los procesos asistenciales	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 gestión de procesos	Personal	Se extravió parte de la Historia Clínica durante su manipulación	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 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 información crítica para los procesos asistenciales Filtración de información	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

Proceso: Emisión de copia de Historia Clínica

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.
Registrar y generar número de expediente	Posible demora en la atención de la solicitud 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 de la solicitud	Demora en el tiempo de atención de la solicitud	Posible	Muy bajo	Bajo	Aceptar
Registrar y generar número de expediente	Posible demora en la atención de la solicitud originado por indisponibilidad del sistema	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Se presenta una caída de los sistemas	Pérdida de información o demora en la atención de la solicitud	Posible	Bajo	Moderado	Reducir
Registrar y generar número de expediente	Posible error al ingresar los datos de la solicitud 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 de lo indicado por el paciente o distracción	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.	Niv. de Riesgo	Estr. de Rpta.
Registrar y generar número de expediente	Posible error en la generación del número de expediente originada por fallo en el sistema	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Se presenta un fallo en el sistema de registro que genera un número erróneo o ya asignado a otra paciente	Demora en la atención de la paciente	Posible	Bajo	Moderado	Reducir
Registrar y generar número de expediente	Posible pérdida de información originada por un fallo de hardware	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Se presenta un fallo en el hardware del equipo del operador que produce su apagado o mal funcionamie nto	Pérdida de información o demora en la atención de la solicitud	Posible	Bajo	Moderado	Reducir
Registrar y generar número de expediente	Posible pérdida de información originada por un fallo de software	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Se presenta un fallo en el software del equipo del operador produciendo un mal funcionamie nto del mismo	Pérdida de información o demora en la atención de la solicitud	Posible	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.	Niv. de Riesgo	Estr. de Rpta.
Registrar y generar número de expediente	Posible pérdida de información originada por un fallo de comunicación con el servidor de la aplicación	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Se presenta un fallo en la comunicación con el servidor	Pérdida de información o demora en la atención de la solicitud	Posible	Bajo	Moderado	Reducir
Registrar y generar número de expediente	Posible pérdida de conexión con el sistema originada por falla eléctrica	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Se presenta una falla en el suministro eléctrico que ocasiona el apagado de los equipos	Pérdida de información o demora en la atención de la solicitud	Posible	Bajo	Moderado	Reducir
Derivar expediente	Posible demora en la atención del expediente debido a que fue derivado a otra área	Ejecución, entrega y gestión de procesos	Personal	Se derivó el expediente a otra área a la cual no correspondía	Demora en el tiempo de atención de la solicitud	Rara	Medio	Bajo	Aceptar
Derivar expediente	Posible error en el proceso de derivación del expediente originada por un fallo por hardware	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Se presenta un fallo en el hardware del equipo del operador	Pérdida de información y demora en la atención de la paciente	Posible	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.	Niv. de Riesgo	Estr. de Rpta.
Derivar expediente	Posible error en el proceso de derivación del expediente originada por un fallo por software	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Se presenta un fallo en el software del equipo del operador	Pérdida de información o demora en la atención de la solicitud	Posible	Bajo	Moderado	Reducir
Derivar expediente	Posible error en el proceso de derivación del expediente originada por un fallo de comunicación con el servidor de la aplicación	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 o demora en la atención de la solicitud	Posible	Bajo	Moderado	Reducir
Derivar expediente	Posible demora en la atención del expediente debido a que fue derivado a otra área	Ejecución, entrega y gestión de procesos	Personal	Se derivó el expediente a otra área a la cual no correspondía	Demora en el tiempo de atención de la solicitud	Rara	Medio	Bajo	Aceptar
Derivar expediente	Posible error en el proceso de derivación del expediente originada por un fallo por hardware	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Se presenta un fallo en el hardware del equipo del operador	Pérdida de información y demora en la atención de la paciente	Posible	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.	Niv. de Riesgo	Estr. de Rpta.
Derivar expediente	Posible error en el proceso de derivación del expediente originada por un fallo por software	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Se presenta un fallo en el software del equipo del operador	Pérdida de información o demora en la atención de la solicitud	Posible	Bajo	Moderado	Reducir
Derivar expediente	Posible error en el proceso de derivación del expediente originada por un fallo de comunicación con el servidor de la aplicación	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 o demora en la atención de la solicitud	Posible	Bajo	Moderado	Reducir
Verificar localización de 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.	Niv. de Riesgo	Estr. de Rpta.
Verificar localización de Historia Clínica	Posible demora en la atención del paciente originado por desconocimiento de localización de la Historia Clínica	Ejecución, entrega y gestión de procesos	Personal	No se encuentra la Historia Clínica en el Archivo o en los grupos de documentos enviados a otras áreas	Pérdida de información crítica para los procesos asistenciales	Posible	Muy alto	Alto	Reducir
Verificar localización de Historia Clínica	Posible demora en la atención del paciente originado por daño físico de la Historia Clínica	Daños a activos materiales	Procesos Internos	Condiciones de almacenaje y tratamiento poco adecuadas y seguras	Pérdida de información crítica para los procesos asistenciales	Muy probable	Muy alto	Extremo	Reducir
Verificar localización de Historia Clínica	Posible demora en la atención del paciente originado por extravío de la Historia Clínica	Daños a activos materiales	Procesos Internos	Condiciones de almacenaje y tratamiento poco adecuadas y seguras	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.	Niv. de Riesgo	Estr. de Rpta.
Verificar localización de Historia Clínica	Posible demora en la atención del paciente originado por robo de la Historia Clínica	Daños a activos materiales	Procesos Internos	Condiciones de almacenaje y tratamiento poco adecuadas y seguras	Pérdida de información crítica para los procesos asistenciales Filtración de información	Muy probable	Muy alto	Extremo	Reducir
Registrar salida de Historia Clínica	Posible pérdida de información originado por 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 Historias Clínicas	Se pierde la trazabilidad en cuanto a la localización de la Historia Clínica	Posible	Medio	Moderado	Reducir
Registrar salida de Historia Clínica	Posible desfase de información originado por indisponibilidad de personal que realice el registro de la salida	Ejecución, entrega y gestión de procesos	Personal	El personal no se encuentra en su lugar para realizar la atención de la salida	La Historia Clínica no se encuentra disponible en caso se requiera en otra atención	Posible	Medio	Moderado	Reducir
Enviar 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.	Niv. de Riesgo	Estr. de Rpta.
Enviar 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
Enviar 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
Enviar 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 asistencialesFiltración 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.	Niv. de Riesgo	Estr. de Rpta.
Foliar 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 información crítica para los procesos asistenciales Filtración de información	Muy probable	Muy alto	Extremo	Reducir
Foliar Historia Clínica	Posible pérdida de información debido a extravío de parte del contenido de la Historia Clínica	Ejecución, entrega y gestión de procesos	Personal	Se extravió parte de la Historia Clínica durante su manipulación	Pérdida de información crítica para los procesos asistenciales	Muy probable	Muy alto	Extremo	Reducir
Fotocopiar contenido de 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 información crítica para los procesos asistenciales Filtración de información	Muy probable	Muy alto	Extremo	Reducir
Fotocopiar contenido de Historia Clínica	Posible pérdida de información debido a extravío de parte del contenido de la Historia Clínica	Ejecución, entrega y gestión de procesos	Personal	Se extravió parte de la Historia Clínica durante su manipulación	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.
Devolver 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
Derivar a OEI	Posible demora en la atención del expediente debido a que fue derivado a otra área	Ejecución, entrega y gestión de procesos	Personal	Se derivó el expediente a otra área a la cual no correspondía	Demora en el tiempo de atención de la solicitud	Rara	Medio	Bajo	Aceptar
Derivar a OEI	Posible pérdida de información debido a extravío de copia	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	Muy probable	Muy alto	Extremo	Reducir
Derivar a OEI	Posible pérdida de información debido a robo de copia	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

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.
Derivar a Mesa de Partes	Posible demora en la atención del expediente debido a que fue derivado a otra área	Ejecución, entrega y gestión de procesos	Personal	Se derivó el expediente a otra área a la cual no correspondía	Demora en el tiempo de atención de la solicitud	Rara	Medio	Bajo	Aceptar
Derivar a Mesa de Partes	Posible pérdida de información debido a extravío de copia	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	Muy probable	Muy alto	Extremo	Reducir
Derivar a Mesa de Partes	Posible pérdida de información debido a robo de copia	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
Derivar a Trámite Documentario	Posible demora en la atención del expediente debido a que fue derivado a otra área	Ejecución, entrega y gestión de procesos	Personal	Se derivó el expediente a otra área a la cual no correspondía	Demora en el tiempo de atención de la solicitud	Rara	Medio	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.	Niv. de Riesgo	Estr. de Rpta.
Derivar a Trámite Documentario	Posible pérdida de información debido a extravío de copia	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	Muy probable	Muy alto	Extremo	Reducir
Derivar a Trámite Documentario	Posible pérdida de información debido a robo de copia	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
Realizar el cobro según cantidad de hojas de la copia	Posible error en el ingreso de datos 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 de lo indicado por el paciente o distracción	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.	Niv. de Riesgo	Estr. de Rpta.
Realizar el cobro según cantidad de hojas de la copia	Posible demora en la atención del paciente originada por indisponibilidad del sistema	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Se presenta una caída de los sistemas	Pérdida de información o demora en la atención de la solicitud	Posible	Bajo	Moderado	Reducir
Realizar el cobro según cantidad de hojas de la copia	Posible demora en la atención del paciente debido a 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
Realizar el cobro según cantidad de hojas de la copia	Posible pérdida de información originada por un fallo de hardware	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Se presenta un fallo en el hardware del equipo del operador que produce su apagado o mal funcionamie nto	Pérdida de información o demora en la atención de la solicitud	Posible	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.	Niv. de Riesgo	Estr. de Rpta.
Realizar el cobro según cantidad de hojas de la copia	Posible pérdida de información originada por un fallo de software	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Se presenta un fallo en el software del equipo del operador produciendo un mal funcionamiento del mismo	Pérdida de información o demora en la atención de la solicitud	Posible	Bajo	Moderado	Reducir
Realizar el cobro según cantidad de hojas de la copia	Posible pérdida de conexión con el sistema originada por falla eléctrica	Interrupción de las operaciones y fallos en los sistemas	Tecnología de Información	Se presenta una falla en el suministro eléctrico que ocasiona el apagado de los equipos	Pérdida de información o demora en la atención de la solicitud	Posible	Bajo	Moderado	Reducir

Anexo 8: Declaración de Aplicabilidad

Declaración de Aplicabilidad
Leyenda (para la selección de controles y razón por la que se seleccionaron)
RL: requerimientos legales, **RN**: requerimientos del negocio, **RVR**: resultado de la valoración de riesgos

ISO 27001:2013 Controles de Seguridad			Controles Actuales	Comentarios (Justificación de Exclusión)	Controles seleccionados y razones de selección			Comentarios (Visión general de la implementación)
					RL	RN	RVR	
Cláusula	Sección	Objetivo de Control / Control						
5 Políticas de Seguridad	5.1	Dirección de la Alta Gerencia para la Seguridad de la Información						
	5.1.1	Políticas de Seguridad de la Información		Se requiere establecer las políticas necesarias que definan los lineamientos internos para asegurar los activos de información críticos que contienen información confidencial o son vitales para la continuidad de las operaciones de la institución.	x	x		Se debe establecer la política general de seguridad de la información y, en caso sea pertinente, políticas específicas para cada uno de los casos que así lo requieran como por ejemplo: Política de buen uso de recursos tecnológicos Política de uso de correo institucional Política de buen uso de internet Cabe destacar que todas las políticas que se definan como parte de este control u otros controles incluidos en el presente documento deberán ser comunicados a todos los colaboradores de la institución.
	5.1.2	Revisión de las Políticas de Seguridad de la Información		Las políticas de seguridad deben ser revisadas periódicamente (idealmente cada año) para asegurar el cumplimiento de las modificaciones o nuevas normas legales que involucren a la institución, así como los cambios internos que pueda sufrir la institución. Adicionalmente la política debe ser revisada luego de la ocurrencia de un incidente grave de seguridad.		x		

ISO 27001:2013 Controles de Seguridad			Controles Actuales	Comentarios (Justificación de Exclusión)	Controles seleccionados y razones de selección			Comentarios (Visión general de la implementación)
					RL	RN	RVR	
Cláusula	Sección	Objetivo de Control / Control						
6 Organización de la Seguridad de la Información	6.1	Organización Interna						
	6.1.1	Roles y Responsabilidad de Seguridad de la Información		Se debe establecer las responsabilidades y roles requeridos tanto en el equipo de seguridad así como para los trabajadores internos. Como mínimo se debe establecer un comité de seguridad de la información que lleve a cabo la implementación y mantenimiento del SGSI.	x	x		El comité de seguridad de la información deberá estar precedido por un oficial de seguridad - el cual idealmente debería ser el Jefe del Área de Estadística e Informática - el cual deberá recibir el apoyo y compromiso de parte de la Dirección de la institución - ente desde el cual debe nacer la iniciativa de implementación del proyecto. Adicionalmente se deberá integrar a las diferentes direcciones como parte de dicho comité.
	6.1.2	Segregación de deberes	Flujogramas no unificados ni actualizados de las funciones de las distintas áreas de la institución	Las actividades de cada área son conocidas, sin embargo la documentación de las mismas es casi nula, además de no existir gráficos unificados que muestren el flujo de información a través de los distintos procesos operativos.		x		Es importante establecer las limitaciones de acceso en cuanto a la información crítica que tiene cada área durante el flujo que sigue la misma como parte de la atención de los pacientes.
	6.1.3	Contacto con autoridades		El establecimiento del flujo a seguir para la notificación de un incidente de seguridad de la información, así como la identificación de las autoridades pertinentes - policía, entes reguladores, etc. - permitirá que dichos eventos no pasen desapercibidos, recibiendo el tratamiento adecuado por parte de las autoridades correspondientes.		x		

ISO 27001:2013 Controles de Seguridad			Controles Actuales	Comentarios (Justificación de Exclusión)	Controles seleccionados y razones de selección			Comentarios (Visión general de la implementación)
					RL	RN	RVR	
Cláusula	Sección	Objetivo de Control / Control						
6 Organización de la Seguridad de la Información	6.1.4	Contacto con grupos de interés especial	Se cuenta con un área de relaciones públicas encargada de brindar información hacia externos	La institución debe establecer flujos de comunicación con los grupos de interés a los que pertenece (en este caso el Ministerio de Salud, EsSalud y otras instituciones prestadoras de salud) con la finalidad de mantener un canal en el que se comparta información respecto a las buenas prácticas utilizadas en instituciones similares, alertas sobre nuevas vulnerabilidades que puedan afectar la seguridad de la información, etc.		x	x	De acuerdo a la magnitud del incidente, se debería realizar una comunicación formal por parte de la institución al Ministerio de Salud, detallando lo ocurrido, así como las consecuencias encontradas y el impacto que el mismo pueda haber tenido en sus operaciones. Es importante también establecer relaciones con las áreas implementadoras de SGSI de instituciones similares, de modo que se pueda compartir experiencias que permitan realizar un mejor proceso.
	6.1.5	Seguridad de la Información en la gestión de proyectos		Los proyectos que se realicen dentro del alcance del presente proyecto deberán ser gestionado debidamente mediante una metodología que tenga en cuenta la gestión de riesgos y que además pueda seguir lineamientos de seguridad de la información como parte de su desarrollo con la finalidad de garantizar el cumplimiento de los requisitos de seguridad de la institución una vez finalizados los proyectos.		x		Utilizar una metodología de gestión de proyectos especializada que pueda ser alineada a una adecuada de riesgos en cuanto a seguridad de la información tal como PMI o Prince 2.
	6.2	Dispositivos móviles y teletrabajo						
	6.2.1	Política de dispositivos móviles		No se considera dado que no se utilizan dispositivos móviles en los procesos del alcance del presente proyecto.				
	6.2.2	Teletrabajo		No se considera dado que no se tiene el servicio de teletrabajo en los procesos del alcance del presente proyecto.				

ISO 27001:2013 Controles de Seguridad			Controles Actuales	Comentarios (Justificación de Exclusión)	Controles seleccionados y razones de selección			Comentarios (Visión general de la implementación)
					RL	RN	RVR	
Cláusula	Sección	Objetivo de Control / Control						
7 Seguridad en los Recursos Humanos	7.1	Previo al Empleo						
	7.1.1	Verificación de antecedentes		La verificación de los antecedentes del personal permitirá filtrar a aquellas personas que puedan constituir un riesgo para la institución o la información que manejen ya sea por conflicto ético o intereses personales.	x	x		Como parte del proceso de reclutamiento se deberá solicitar un informe de antecedentes policiales/penales a los postulantes, de modo que se pueda filtrar personas que puedan constituir un riesgo para la institución en caso se incorporen a las actividades de la misma.
	7.1.2	Términos y condiciones del empleo		Establecer las condiciones de empleo, las cuales deben comunicadas a los seleccionados previo a la firma del contrato en el cual se detalle las responsabilidades en cuanto a seguridad de la información que el suscriptor acepta al momento de iniciar sus labores en la institución.	x		x	Luego de establecer las condiciones de empleo, lo recomendable sería realizar reuniones con el personal que pertenece a la institución - específicamente aquellos que trabajan haciendo uso de información sensible - explicando las nuevas condiciones de trabajo así como la necesidad de establecerlas de acuerdo al marco normativo actual. El personal debería firmar el nuevo acuerdo de modo que sea anexado a su expediente interno de Recursos Humanos.
	7.2	Durante el Empleo						
	7.2.1	Responsabilidades de la Alta Gerencia		Se debe especificar la responsabilidad de la alta gerencia en cuanto a la implementación y mantenimiento del SGSI puesto que responde al plan estratégico de la misma y a los intereses de sus pacientes, motivo por el cual debe ser parte activa en los requerimientos del mismo.		x		La alta gerencia - en este caso la Dirección institucional - debe reconocer la importancia y necesidad de contar con un SGSI como parte del cumplimiento normativo al cual se encuentra sujeta la institución. Es también responsabilidad de este ente interno dirigir los esfuerzos de los colaboradores de modo que se facilite el cumplimiento de las políticas de seguridad establecidas.

ISO 27001:2013 Controles de Seguridad			Controles Actuales	Comentarios (Justificación de Exclusión)	Controles seleccionados y razones de selección			Comentarios (Visión general de la implementación)
					RL	RN	RVR	
Cláusula	Sección	Objetivo de Control / Control						
7 Seguridad en los Recursos Humanos	7.2.2	Conciencia, educación y entrenamiento de Seguridad de la Información		Establecer un plan de capacitación de los colaboradores sobre la política de seguridad de la información, así como su evaluación permitirá medir el nivel de conocimiento de los mismos en este tema.	x	x		Es recomendable realizar anualmente cursos - incluso en modalidad virtual - que refuercen los conocimientos relacionados a seguridad de la información en el personal, siendo necesaria una evaluación de los mismos de modo que se pueda identificar la necesidad de realizar un refuerzo en determinadas áreas de dichos conocimientos.
	7.2.3	Proceso disciplinario		Se debe establecer las penalizaciones disciplinarias a aplicar a los colaboradores en caso de infringir las condiciones de empleo en cuanto a seguridad de la información con la que se trabaje.		x	x	
	7.3	Término y Cambio de Empleo						
	7.3.1	Termino de responsabilidades o cambio de empleo		El establecimiento del periodo en que el colaborador se encuentra sujeto a los términos y condiciones establecidos en el momento de su incorporación permitirá a la institución protegerse legalmente frente a filtraciones realizadas por trabajadores cesados		x		Como parte de los términos y condiciones de empleo se debe detallar al futuro empleado el período sobre el cual se encontrará sujeto al cumplimiento de dichos términos luego de la finalización de su relación con la institución.

ISO 27001:2013 Controles de Seguridad			Controles Actuales	Comentarios (Justificación de Exclusión)	Controles seleccionados y razones de selección			Comentarios (Visión general de la implementación)
					RL	RN	RVR	
Cláusula	Sección	Objetivo de Control / Control						
8 Gestión de Activos	8.1	Responsabilidad de los Activos						
	8.1.1	Inventario de activos		Dado el uso de información sensible utilizada para fines médicos, la institución debe manejar un inventario de activos en el que se identifique los activos de los diferentes tipos además de su ubicación, de esta forma se podrá relacionar este inventario con las políticas de uso según la categorización de los activos.	x	x		Se deberá trabajar en conjunto con los dueños de los procesos para poder identificar los diferentes activos de información así como la criticidad de los mismos.
	8.1.2	Propiedad de activos	Se establece como dueño de la información a las áreas custodias de la misma. En el caso de las Historias Clínicas es el área de Archivo	Los activos de información deben ser asignados a un custodio encargado del inventario, clasificación y protección de los activos, así como de la destrucción en caso sea necesario y la revisión de las restricciones en cuanto a accesos.	x	x		
	8.1.3	Uso aceptable de los activos		Especificar y documentar a qué se define como uso aceptable en cuanto a manejo de información personal y sensible mediante una política o procedimiento que debe ser de conocimiento obligatorio para el personal del área.	x	x		
	8.2	Clasificación de la Información						
	8.2.1	Clasificación de la información		Según la normativa vigente se deberá realizar una clasificación de los activos identificados según su criticidad para el negocio o el nivel de confidencialidad que se les debe otorgar. La clasificación de la información puede ser subjetiva dependiendo del contexto o de la época en que se utiliza la misma, por este motivo se debe revisar la clasificación periódicamente.	x	x		Tener en cuenta tanto la clasificación indicada en la Ley de Protección de Datos Personales así como en la Norma Técnica de la Historia Clínica de los establecimientos del sector salud.
	8.2.2	Etiquetado de la información		Con la finalidad de mantener un correcto uso de la información, se debe realizar el etiquetado que identifique la información según la clasificación previamente definida. En el caso de los sistemas de información, los usuarios deberán ver un mensaje visible que indique la clasificación de la información a la cual están accediendo.		x	x	No toda la información relacionada a salud es confidencial, se debe tener en cuenta que la confidencialidad de la información es subjetiva, dependiente del contexto y cambiante a lo largo del tiempo. Por este motivo la clasificación de la información debe ser revisada periódicamente.

ISO 27001:2013 Controles de Seguridad			Controles Actuales	Comentarios (Justificación de Exclusión)	Controles seleccionados y razones de selección			Comentarios (Visión general de la implementación)
					RL	RN	RVR	
Cláusula	Sección	Objetivo de Control / Control						
8 Gestión de Activos	8.2.3	Manejo de activos		Establecer procedimientos de manejo de activos de información permitirá que se sigan protocolos que garanticen la seguridad de los mismos, por ejemplo, en el traslado de Historias Clínicas entre áreas para algunas funciones.		x	x	
	8.2.4	Devolución de activos	Cuaderno de control de Historias Clínicas salientes del Archivo.	Dado que la información más crítica para la institución se almacena en un medio físico, se necesita garantizar su devolución en caso de extracción del archivo por diferentes motivos. Este control incluye la devolución de activos de información entregados a los colaboradores una vez finalizada su relación con la institución.		x	x	
	8.3	Manejo de Medios						
	8.3.1	Gestión de medios removibles		No se considera dado que no se utilizan medios digitales removibles en los procesos del alcance del presente proyecto.				
	8.3.2	Eliminación de medios		La eliminación de medios que contienen información confidencial deben seguir un protocolo que asegure su correcto desecho, de manera que no puedan ser reutilizados por otras personas no autorizadas.	x	x		En el caso de las Historias Clínicas, al momento de pasar al archivo pasivo, la información que no vaya a ser archivada debería ser triturada con la finalidad que la información contenida no pueda ser reconstruida.
	8.3.3	Transporte de medios físicos	Cuaderno de control de Historias Clínicas salientes del Archivo.	Se debe establecer protocolos que aseguren la información en su transferencia física de manera que entre la salida de su archivo y la recepción en el área destino - y viceversa - se garantice que no fue manipulada por personas no autorizadas.		x	x	Establecer una cadena de custodia en el envío de las Historias Clínicas hacia las áreas que lo requieran, indicando quiénes son el personal autorizado en llevar y en recibir estos documentos.

ISO 27001:2013 Controles de Seguridad			Controles Actuales	Comentarios (Justificación de Exclusión)	Controles seleccionados y razones de selección			Comentarios (Visión general de la implementación)
					RL	RN	RVR	
Cláusula	Sección	Objetivo de Control / Control						
9 Control de Acceso	9.1	Requerimientos de Negocio para el Control de Acceso						
	9.1.1	Política de control de acceso	Acceso medianamente vigilado al archivo activo por el personal del área.	El control de acceso a la información médica crítica debe estar documentado y ser de conocimiento del personal. Se debe definir también los niveles de escalamiento para la autorización del uso de información en caso se requiera.		x	x	Se debe tener en cuenta que la política deberá considerar que existen casos en los que se deba romper el procedimiento establecido en caso de un requerimiento que corresponda a un caso de emergencia, en el cual se necesita la información cuanto antes.
	9.1.2	Política en el uso de servicios de red		Establecer una política de accesos a nivel de red que establezca los lineamientos en cuanto a segmentación de redes, acceso de externos a la red interna, monitoreo, etc.		x		
	9.2	Gestión de Accesos de Usuario						
	9.2.1	Registro y baja del usuario	Se cuenta con procedimientos de alta y baja de usuarios en la institución.	Para mitigar el riesgo de acceso no autorizado, se debe mantener un procedimiento de alta y sobretodo bajas de usuarios de los sistemas de la institución.		x	x	Las revisiones periódicas de usuarios activos en los sistemas permitirán tener un mejor control que elimine el riesgo que constituyen las cuentas huérfanas - aquellas que se han quedado activas en los sistemas luego de que el dueño de la misma ya ha terminado sus relaciones laborales con la institución.
	9.2.2	Gestión de privilegios	Actualmente sólo cierto tipo de personal puede contar con acceso a las Historias Clínicas, de igual manera se valida que persona solicita acceso a un duplicado y si cuenta con el visto bueno del usuario dueño de la información.	Contar con una correcta gestión de privilegios permitirá limitar el acceso según las funciones o áreas a las cuales cada colaborador perteneces.		x	x	Establecer la segregación de funciones en base a los cargos, de modo que se pueda diseñar un control de privilegios de acceso en base a los cargos que tienen los colaboradores.

ISO 27001:2013 Controles de Seguridad			Controles Actuales	Comentarios (Justificación de Exclusión)	Controles seleccionados y razones de selección			Comentarios (Visión general de la implementación)
					RL	RN	RVR	
Cláusula	Sección	Objetivo de Control / Control						
9 Control de Acceso	9.2.3	Gestión de información de autenticación secreta de usuarios	Todos los usuarios de los sistemas cuentan con autenticación mediante password según las buenas prácticas que la institución sigue.	Se debe mantener un método de identificación para poder acceder a los sistemas de la institución que permitan una trazabilidad de las acciones realizadas por los usuarios.		x		La configuración de los sistemas de información deben tener en cuenta los siguientes aspectos relacionados a las credenciales de los usuarios: Complejidad de contraseñas. Cambio de contraseña en el primer inicio de sesión. Bloqueo de cuentas luego de varios intentos fallidos de inicio de sesión. Deshabilitación de cuentas luego de un número determinado de días de inactividad.
	9.2.4	Revisión de derechos de acceso de usuarios		Los dueños de los activos de información son quienes deben revisar los usuarios que cuentan con accesos a sus activos de información periódicamente de manera que se identifiquen usuarios que no deberían contar con acceso, vencimiento de accesos temporales o usuarios que ya no requieren del acceso por cambio de área.		x		
	9.2.5	Eliminación o ajuste de derechos de acceso		Los privilegios con los que cuentan los usuarios deberán ser eliminados en el caso en que el colaborador haya cesado su relación con la institución, o ajustados a lo largo del tiempo en caso el usuario requiera mayores privilegios o ya no los necesite.		x		
	9.3	Responsabilidades del Usuario						
	9.3.1	Uso de información de autenticación secreta		Se debe establecer las directivas de uso de los métodos de autenticación, así como los requisitos para asegurar la confidencialidad de estos datos siendo indispensable que estas directivas se hagan públicas a todos los colaboradores de la compañía.		x	x	

ISO 27001:2013 Controles de Seguridad			Controles Actuales	Comentarios (Justificación de Exclusión)	Controles seleccionados y razones de selección			Comentarios (Visión general de la implementación)
					RL	RN	RVR	
Cláusula	Sección	Objetivo de Control / Control						
9 Control de Acceso	9.4	Control de Acceso de Sistemas y Aplicaciones						
	9.4.1	Restricción de acceso a la información	Todos los sistemas de información cuentan con acceso a través de usuario y contraseña.	Si bien se cuenta con el control básico, sería recomendable establecer un doble factor de autenticación en aquellos sistemas en los que se encuentra información sensible.	x	x		
	9.4.2	Procedimientos de inicio de sesión segura	La configuración de cuentas es adecuada en cuanto a la seguridad con la que se realiza el procedimiento de inicio de sesión.	Control enfocado a proteger la información de inicio de sesión del usuario en los sistemas, de forma que no pueda ser sustraída por un agente externo.		x	x	
	9.4.3	Sistema de gestión de contraseñas	La configuración en cuanto a contraseñas es adecuada, permitiendo a los usuarios realizar cambios de contraseña y cumplir con la complejidad mínima solicitada.	Establecer requisitos mínimos en cuanto a complejidad de contraseñas, los procedimientos de cambios de contraseñas y el almacenamiento de las mismas entre otros.		x	x	
	9.4.4	Uso de programas y utilidades privilegiadas		Identificar los lineamientos de uso de utilidades ya sean internas o externas, traídas por los usuarios a la institución.		x	x	
	9.4.5	Control de acceso al código fuente del programa		No se considera dado que no se cuenta con el código fuente de los aplicativos utilizados en los procesos del alcance del presente proyecto, al ser software empaquetado.				

ISO 27001:2013 Controles de Seguridad			Controles Actuales	Comentarios (Justificación de Exclusión)	Controles seleccionados y razones de selección			Comentarios (Visión general de la implementación)
					RL	RN	RVR	
Cláusula	Sección	Objetivo de Control / Control						
10 Criptografía	10.1	Controles Criptográficos						
	10.1.1	Política en el uso de controles criptográficos		No se considera dado que no se cuenta con información digitalizada sensible que requiera este tipo de control en los procesos del alcance del presente proyecto.				
	10.1.2	Gestión de llaves		No se considera dado que no se cuenta con información digitalizada sensible que requiera este tipo de control en los procesos del alcance del presente proyecto.				
11 Seguridad Física y del Entorno	11.1	Áreas Seguras						
	11.1.1	Perímetro de seguridad físico	El archivo Activo de Historias Clínicas se encuentra custodiado dentro del área de Admisión. El archivo pasivo se encuentra en otro ambiente externo al hospital y no se encuentra resguardado.	El perímetro de seguridad físico tiene por objetivo establecer un límite de accesos entre los pacientes y los trabajadores y entre estos últimos aquellos que tienen acceso autorizado a las locaciones en las que se almacena información sensible.		x		La protección de los ambientes dentro del perímetro que almacena las Historias Clínicas deberá ser gestionado en conjunto con el personal de seguridad de la institución.
	11.1.2	Controles físicos de entrada		Utilizar controles de registro de acceso para el personal y las visitas que puedan requerir accesos a los ambientes en los que se almacena la información crítica. El personal debe estar debidamente identificado en todo momento.		x		Crear un registro de acceso a los archivos. Implementar el uso obligatorio del fotocheck en un lugar visible.
	11.1.3	Seguridad de oficinas, habitaciones y facilidades		Se debe evitar el acceso de personal no autorizado o al público que hace uso de los servicios de la institución a los ambientes en los que se almacena información sensible.		x		La información referente en cuanto al personal y su locación no debe ser accesible a personas externas.
	11.1.4	Protección contra amenazas externas y del ambiente		Implementar medidas para proteger la información crítica frente a incidentes que puedan afectarla, tanto naturales como provocados (incendios).		x		Implementar un sistema contra incendios en el archivo. Realizar el aseguramiento de los archivadores al piso y/o techo del ambiente.

ISO 27001:2013 Controles de Seguridad			Controles Actuales	Comentarios (Justificación de Exclusión)	Controles seleccionados y razones de selección			Comentarios (Visión general de la implementación)
					RL	RN	RVR	
Cláusula	Sección	Objetivo de Control / Control						
11 Seguridad Física y del Entorno	11.1.5	Trabajo en áreas seguras		No se considera dado que no afecta directamente los activos de información del inventario.				
	11.1.6	Áreas de entrega y carga		No se considera dado que el envío de los activos de información se realizan directamente al área correspondiente.				
	11.2	Equipo						
	11.2.1	Instalación y protección de equipo		Los equipos utilizados en el alcance del presente proyecto deben instalarse de manera que se evite el acceso no autorizado a los mismos por parte de personas ajenas al servicio.		x		
	11.2.2	Servicios de soporte		Los equipos críticos relacionados al mantenimiento de información sensible deben contar con medidas que aseguren su funcionamiento en el caso de caída de algún servicio sobre el que se soporten (fluido eléctrico por ejemplo)		x		Los servidores de los sistemas deben contar con equipos UPS que mantengan el suministro eléctrico de manera temporal con la finalidad de que se puedan terminar las transacciones evitando la pérdida de información.
	11.2.3	Seguridad en el cableado		No se considera dado que no se cuenta con información digitalizada sensible que requiera este tipo de control en los procesos del alcance del presente proyecto.				
	11.2.4	Mantenimiento de equipos		Los equipos que cuenten con acceso a información crítica deberán seguir un procedimiento de mantenimiento adecuado, de manera que la información que contienen no sea comprometida.		x		

ISO 27001:2013 Controles de Seguridad			Controles Actuales	Comentarios (Justificación de Exclusión)	Controles seleccionados y razones de selección			Comentarios (Visión general de la implementación)
					RL	RN	RVR	
Cláusula	Sección	Objetivo de Control / Control						
11 Seguridad Física y del Entorno	11.2.5	Retiro de activos	Cuaderno de control de Historias Clínicas salientes del Archivo.	La institución debe establecer políticas que limiten el retiro de la información sensible de las instalaciones a excepción de ser para cumplir con alguno de los servicios que brinda.		x	x	Se debe tener especial cuidado en el caso en que se solicita información médica con fines académicos.
	11.2.6	Seguridad del equipo y activos fuera de la instalación		La institución debe asegurar que cualquier uso externo de la información médica que maneja haya sido previamente autorizado por las personas correspondientes.		x		Establecer una matriz de autorizaciones que especifique qué usuarios brindan este tipo de autorizaciones para los diferentes activos de información.
	11.2.7	Eliminación segura o reúso del equipo		Los equipos que se den de baja o se cambien de ambiente deben haber pasado por un proceso de limpieza que elimine de manera adecuada la información sensible que puedan contener		x		
	11.2.8	Equipo de usuario desatendido		Los usuarios deberán mantener la seguridad de sus equipos incluso cuando no estén trabajando con los mismos.		x		Establecer políticas de tiempo de bloqueo automático de los equipos. Establecer una política que especifique el requisito de mantener el equipo bloqueado en caso se requiera ausentarse del mismo, cambio de contraseña, etc.
	11.2.9	Política de escritorio limpio y pantalla limpia		Los usuarios deberán mantener sus escritorios libre de cualquier información sensible que pueda usar un agente externo como consecuencia de su exposición como parte de un olvido o mala gestión.		x		Establecer una política que indique a los colaboradores los cuidados que deben tener frente a la posible exposición de la información sensible en su centro de trabajo.

ISO 27001:2013 Controles de Seguridad			Controles Actuales	Comentarios (Justificación de Exclusión)	Controles seleccionados y razones de selección			Comentarios (Visión general de la implementación)
					RL	RN	RVR	
Cláusula	Sección	Objetivo de Control / Control						
12 Seguridad en las Operaciones	12.1	Procedimientos Operacionales y Responsabilidades						
	12.1.1	Documentación de procedimientos operacionales	Se cuenta con flujogramas que definen procesos desactualizados	Se requiere la documentación de los procesos que se tienen con la finalidad de que se entienda los flujos de información crítica que existen y se pueda realizar una evaluación continua sobre el nivel de riesgo existente y establecer nuevos controles necesarios.		x		
	12.1.2	Gestión de cambios		No se considera puesto que en el alcance del presente proyecto no se toma en cuenta este tipo de actividades.				
	12.1.3	Gestión de la capacidad		No se considera puesto que en el alcance del presente proyecto no se toma en cuenta este tipo de actividades.				
	12.1.4	Separación de los ambientes de desarrollo, pruebas y operación		No se considera puesto que en el alcance del presente proyecto no se toma en cuenta este tipo de actividades.				
	12.2	Protección de Software Malicioso						
	12.2.1	Controles contra software malicioso	La institución cuenta con un antivirus licenciado para todos sus equipos.	Dado el gran avance en cuanto a amenazas informáticas, la institución deberá preocuparse por asegurar que las estaciones de trabajo se encuentren debidamente protegidos frente a programas malware que podrían causar daños a la información utilizada en la institución.		x		
	12.3	Respaldo						
	12.3.1	Respaldo de información	Actualmente se cuenta con respaldo únicamente en los servidores más críticos de los sistemas de información utilizados.	Establecer una política de respaldo que garantice la continuidad de la atención y mitigue la pérdida de datos en caso de incidente.		x		
	12.4	Registro y Monitoreo						
	12.4.1	Registro de eventos		Los sistemas que acceden a información crítica deben contar con un log de auditoría que almacene los eventos de manera que sea factible verificar el acceso de los usuarios y las tareas que éstos han realizado en el sistema.		x		
	12.4.2	Protección de registros de información						
	12.4.3	Registros de Administrador y Operador						
	12.4.4	Sincronización de relojes		No se considera puesto que no afecta la atención de los servicios.				

ISO 27001:2013 Controles de Seguridad			Controles Actuales	Comentarios (Justificación de Exclusión)	Controles seleccionados y razones de selección			Comentarios (Visión general de la implementación)
					RL	RN	RVR	
Cláusula	Sección	Objetivo de Control / Control						
12 Seguridad en las Operaciones	12.5	Control de Software Operacional						
	12.5.1	Instalación de software en sistemas operacionales		Establecer procedimientos que garanticen la correcta instalación del software utilizado, incluyendo los parches de seguridad y las actualizaciones requeridas		x		
	12.6	Gestión de Vulnerabilidades Técnicas						
	12.6.1	Gestión de vulnerabilidades técnicas		El equipo de seguridad deberá monitorear las vulnerabilidades que puedan aparecer a lo largo del tiempo con la finalidad de que se apliquen las remediaciones correspondientes. Se debe desarrollar un procedimiento de análisis de vulnerabilidades o ethical hacking en los sistemas críticos de manera periódica.		x		Se debe centralizar la actualización de parches del sistema operativo así como de la suite antimalware de modo que puedan ser desplegadas para todos los equipos de la institución.
	12.6.2	Restricciones en la instalación de software		Establecer una política que evite que el personal pueda instalar aplicaciones no licenciadas o no permitidas.		x		La instalación de software en los equipos de la institución debería estar bloqueada para todos los usuarios de modo que sólo pueda realizarse mediante un usuario Administrador con mayores privilegios.
	12.7	Consideraciones de Auditoria de Sistemas de información						
	12.7.1	Controles de Auditoría de Sistemas de Información		Se debe mantener una auditoría periódica de modo que se verifique el buen funcionamiento y uso de los sistemas de información, además de asegurar que solo los usuarios debidamente autorizados cuentan con acceso a información sensible .		x		

ISO 27001:2013 Controles de Seguridad			Controles Actuales	Comentarios (Justificación de Exclusión)	Controles seleccionados y razones de selección			Comentarios (Visión general de la implementación)
					RL	RN	RVR	
Cláusula	Sección	Objetivo de Control / Control						
13 Seguridad en las Comunicaciones	13.1	Gestión de Seguridad en Red						
	13.1.1	Controles de red	Los equipos deben estar en el dominio institucional para poder acceder a la red.	La red interna de la institución debe contar con los controles necesarios que aseguren la información que viaja a través de la misma, de modo que no pueda ser capturada por un agente externo al flujo de información.		x		Establecer limitaciones de modo que sólo los equipos debidamente autorizados puedan conectarse a la red de la institución y puedan ver los recursos que se comparten en la misma. Se debe realizar una segmentación adecuada de la red, de modo que los servidores con los que se cuenta no puedan ser accedidos por cualquier usuario.
	13.1.2	Seguridad de los servicios en red		Se debe contar con un inventario de servicios de red que establezca los niveles de servicio que deben cumplir, además de las características de seguridad con los que se cuenta (firewalls, ips, filtro web, restricciones de red)		x		
	13.1.3	Segregación en redes		Se debe contar con una correcta segregación tanto de redes, como de usuarios en el dominio de la institución que permita verificar los accesos brindados y puedan ser verificados.		x	x	

ISO 27001:2013 Controles de Seguridad			Controles Actuales	Comentarios (Justificación de Exclusión)	Controles seleccionados y razones de selección			Comentarios (Visión general de la implementación)
					RL	RN	RVR	
Cláusula	Sección	Objetivo de Control / Control						
13 Seguridad en las Comunicaciones	13.2	Transferencia de Información						
	13.2.1	Políticas y procedimientos para la transferencia de información		Se debe establecer la documentación necesaria que defina el flujo de transferencia de información a entes externos, tales como instituciones públicas, abogados o el mismo paciente, siempre y cuando haya sido adecuadamente autorizado. Se busca evitar que esta información pueda ser capturada por agentes externos durante la transferencia de la misma.		x	x	
	13.2.2	Acuerdos en la transferencia de información		Durante la transferencia de información se debe especificar a la entidad que la recibe la categoría de la información (confidencial, sensible o pública) e indicar mediante un acuerdo las condiciones de confidencialidad que deben tenerse en cuenta para la misma.		x	x	
	13.2.3	Mensajería electrónica		No se considera puesto que no se realiza envío de información mediante mensajería electrónica.				
	13.2.4	Acuerdos de confidencialidad o no-revelación		La institución debe establecer acuerdos de confidencialidad que detallen las limitaciones de divulgación de la información tanto por sus trabajadores como por sus proveedores en caso sea necesario.		x	x	

ISO 27001:2013 Controles de Seguridad			Controles Actuales	Comentarios (Justificación de Exclusión)	Controles seleccionados y razones de selección			Comentarios (Visión general de la implementación)
					RL	RN	RVR	
Cláusula	Sección	Objetivo de Control / Control						
14 Adquisición, Desarrollo y Mantenimiento de Sistemas	14.1	Requerimientos de Seguridad de Sistemas de Información						
	14.1.1	Análisis y especificación de requerimientos de seguridad		No se considera puesto que no se realiza adquisición de software por parte del área del alcance del proyecto.				
	14.1.2	Aseguramiento de servicios de aplicación en redes públicas						
	14.1.3	Protección de transacciones de servicios de aplicación						
	14.2	Seguridad en el Proceso de Desarrollo y Soporte						
	14.2.1	Política de desarrollo seguro		No se considera puesto que no se realiza desarrollo de software por parte del área del alcance del proyecto.				
	14.2.2	Procedimientos de control de cambios						
	14.2.3	Revisión técnica de aplicaciones después de cambios a la plataforma operativa						
	14.2.4	Restricción de cambios a paquetes de software						
	14.2.5	Procedimientos de desarrollo de sistemas						
	14.2.6	Entorno de desarrollo seguro						
	14.2.7	Desarrollo tercerizado						
	14.2.8	Pruebas de seguridad del sistema						
	14.2.9	Pruebas de aceptación del sistema						
	14.3	Datos de Prueba						
	14.3.1	Protección de datos de prueba		No se considera puesto que no se realiza adquisición de software por parte del área del alcance del proyecto.				

ISO 27001:2013 Controles de Seguridad			Controles Actuales	Comentarios (Justificación de Exclusión)	Controles seleccionados y razones de selección			Comentarios (Visión general de la implementación)
					RL	RN	RVR	
Cláusula	Sección	Objetivo de Control / Control						
15 Relaciones con Proveedores	15.1	Seguridad en Relaciones con el Proveedor						
	15.1.1	Política de Seguridad de la Información para relaciones con proveedores		No se considera puesto que no se comparte información con proveedores externos.				
	15.1.2	Atención de tópicos de seguridad dentro de los acuerdos con proveedores						
	15.1.3	Cadena de suministros de TIC						
	15.2	Gestión de Entrega de Servicios de Proveedor						
	15.2.1	Monitoreo y revisión de servicios de proveedor		No se considera puesto que no se comparte información con proveedores externos en los procesos del alcance del presente proyecto.				
	15.2.2	Gestión de cambios a servicios de proveedor						
16 Gestión de Incidentes de Seguridad de la Información	16.1	Gestión de Incidentes de Seguridad de la Información y Mejoras						
	16.1.1	Responsabilidades y Procedimientos		Se debe detallar las responsabilidades y procedimientos correspondientes a dicho equipo de manera que se encuentren debidamente identificadas las funciones del mismo.		x	x	Establecer un equipo debidamente capacitado que se encargue de la gestión de incidentes. Establecer las categorías de incidentes que deberán ser reportados al equipo correspondiente de manera que los colaboradores conozcan qué eventos de seguridad existen y ante quién deben ser reportadas.
	16.1.2	Reporte de eventos de Seguridad de la Información		Los eventos y vulnerabilidades identificados deberán ser reportados al equipo correspondiente.		x		
	16.1.3	Reporte de debilidades de Seguridad de la Información				x		
	16.1.4	Valoración y decisión de eventos de Seguridad de la Información		Los eventos de seguridad de la información que hayan sido reportados deberán ser analizados por el equipo determinando las acciones a tomar en respuesta de los incidentes.		x		

ISO 27001:2013 Controles de Seguridad			Controles Actuales	Comentarios (Justificación de Exclusión)	Controles seleccionados y razones de selección			Comentarios (Visión general de la implementación)
					RL	RN	RVR	
Cláusula	Sección	Objetivo de Control / Control						
	16.1.5	Respuesta a incidentes de Seguridad de la Información		Establecer el procedimiento que se deberá seguir como respuesta al incidente de seguridad de la información.		x		
	16.1.6	Aprendizaje de incidentes de Seguridad de la Información		Las conclusiones del análisis de los incidentes deberán ser debidamente documentados en una bitácora de manera que sirvan como base del conocimiento para disminuir la ocurrencia de los mismos.		x		
16 Gestión de Incidentes de Seguridad de la Información	16.1.7	Colección de evidencia		La recolección de evidencias en casos de incidentes que lo requieran deberá seguir un procedimiento que establezca los lineamientos en los cuales dicha evidencia debe ser obtenida, de manera que pueda ser utilizada, en caso se requiera, en procesos judiciales.	x	x		La recolección de evidencias debe hacerse garantizando una cadena de custodia que evite la manipulación de la misma que la invalidaría como tal. El procedimiento, en caso sea necesario, deberá detallar la comunicación con las autoridades públicas correspondientes (policía, fiscal, etc.) que puedan ser requeridos para la recolección de la evidencia.

ISO 27001:2013 Controles de Seguridad			Controles Actuales	Comentarios (Justificación de Exclusión)	Controles seleccionados y razones de selección			Comentarios (Visión general de la implementación)
					RL	RN	RVR	
Cláusula	Sección	Objetivo de Control / Control						
17 Aspectos de Seguridad de la Información para la Gestión de Continuidad del Negocio	17.1	Seguridad de la Información en la Continuidad						La implementación de un Sistema de Gestión de Continuidad de Negocios en la institución permitiría realizar un mejor análisis de los activos de información críticos para la continuidad operativa de la institución frente a un desastre, así como el análisis de riesgos a nivel macro que permita definir planes de acción (dentro de los planes de crisis) frente a escenarios que afecten la continuidad de negocios (tales como incendios, terremotos, apagones, entre otros). De este modo el trabajo conjunto con el equipo de continuidad permitirá verificar la correctitud de los planes en cuanto a las acciones a realizar para proteger la información, así como la recuperación de la misma como parte de los planes de contingencia.
	17.1.1	Planeación de Seguridad de la Información en la continuidad		Se debe identificar aquellos activos de información que son críticos para asegurar la continuidad de las operaciones de la institución, según el impacto en disponibilidad del servicio que tendría una pérdida de dicha información.		x	x	
	17.1.2	Implementación de Seguridad de la Información en la continuidad		Los planes de continuidad de negocios deben tener en cuenta la protección de los activos de información previamente identificados, de manera que se asegure la disponibilidad de los mismos haciendo más eficiente la recuperación de los servicios de la institución.		x	x	
	17.1.3	Verificación, revisión y evaluación de Seguridad de la Información en la continuidad		Como parte de las pruebas a realizar para verificar la adecuación de los planes de contingencia establecidos, así como el nivel de protección de la información frente a los distintos escenarios que se haya definido.		x	x	
	17.2	Redundancias						
	17.2.1	Disponibilidad de instalaciones de procesamiento de información		Los servidores que almacenen información sensible o crítica para las operaciones deberán contar con instalaciones alternas en las cuales se almacene la información de manera redundante. De este modo se facilita la recuperación de la información en un escenario en el que el centro de datos principal sea afectado o destruido.		x	x	

ISO 27001:2013 Controles de Seguridad			Controles Actuales	Comentarios (Justificación de Exclusión)	Controles seleccionados y razones de selección			Comentarios (Visión general de la implementación)
					RL	RN	RVR	
Cláusula	Sección	Objetivo de Control / Control						
18 Cumplimiento	18.1	Cumplimiento con Requerimientos Legales y Contractuales						
	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 que afecte a la institución.	x			
	18.1.2	Derechos de propiedad intelectual (IPR)		No se considera, dado que no se trabaja con activos con propiedad intelectual en los procesos del alcance del presente proyecto.				
	18.1.3	Protección de información documentada		La institución debe contar con procedimientos que determinen las condiciones de almacenamiento de información física, el periodo de tiempo por el cual dicha información debe ser almacenada y los procedimientos estándar de desecho de información.	x	x	x	Se debe tener especial cuidado en el caso de las Historias Clínicas, dado que se encuentran reguladas por el Ministerio de Salud y tienen un procedimiento específico para su almacén y desecho.
	18.1.4	Privacidad y protección de información personal identificable		La información personal deberá ser protegida de acuerdo a lo indicado por la Ley de Protección de Datos Personales.	x	x	x	
	18.1.5	Regulación de controles criptográficos		No se considera, dado que no se utiliza información digital o cifrada.				
	18.2	Revisiones de Seguridad de la Información						
	18.2.1	Revisión independiente de Seguridad de la Información		El Sistema de Gestión de Seguridad de la Información deberá ser revisado periódicamente teniendo en cuenta los cambios organizacionales o legislativos que se produzcan.		x		
	18.2.2	Cumplimiento con políticas y estándares de seguridad		Las políticas de Seguridad de la Información deberán ser evaluadas periódicamente en cuanto a su cumplimiento en la institución, así como ajustados de acuerdo a los cambios que se puedan haber producido en el marco legal u organizacional.		x		
	18.2.3	Inspección de cumplimiento técnico		Los sistemas de información utilizados deben ser evaluados periódicamente en cuanto al cumplimiento de los aspectos técnicos relacionados con las políticas de seguridad de modo que se puedan detectar fallas o vulnerabilidades nuevas.		x		Se aconseja realizar análisis de Ethical Hacking que permitan garantizar el cumplimiento de los requerimientos de seguridad en las redes y sistemas de la institución.