Asesoría Jurídica

Mat.: Aprueba *"Procedimiento de seguridad control de cambios en los medios y sistemas de procesamiento de información"*

Santiago.

VISTOS, Lo dispuesto en:

1. El Decreto con Fuerza de Ley N° 1, de 2005, del Ministerio de Salud, que fija texto refundido, coordinado y sistematizado del Decreto Ley N°2.763, de 1979, y de las leyes N^{os}. 18.933 y 18.469;

2. El Decreto con Fuerza de Ley N° 1/19.653, de 2001, que fija el texto refundido, coordinado y sistematizado de la ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado;

3. La Ley N°19.880, sobre Bases de los Procedimientos Administrativos de los Órganos del Estado;

4. Los Decretos Supremos N° 140/2004 y N° 38/2005, ambos del Ministerio de Salud, que aprueban los reglamentos orgánicos de los Servicios de Salud y de los Establecimientos de Autogestión en Red;

5. La Resolución N° 36/2024, de la Contraloría General de la República, que establece los actos administrativos exentos del trámite de toma de razón.

6. La Resolución Exenta RA N°116675/92/2024, de 30 de enero de 2024, que modifica la Resolución Exenta RA N°116675/419/2023, del Servicio de Salud Metropolitano Central, que nombra en calidad de titular el cargo de Director del Hospital de Urgencia Asistencia Pública.

7. Resolución Exenta N°3.195, de 2024, del Hospital de Urgencia Asistencia Pública, que establece jefaturas, determina subrogancia para los cargos de Director, Subdirector, Jefes y Encargados de Unidades, del Hospital de Urgencia Asistencia Pública.

XASV

CONSIDERANDO

a) Que, el Hospital de Urgencia Asistencia Pública, como establecimiento de alta complejidad y referencia nacional, depende de sistemas y servicios tecnológicos críticos para la continuidad operativa, la atención clínica segura y la gestión administrativa eficiente.

b) Que, la creciente complejidad de los entornos digitales hospitalarios, sumada al riesgo de fallas técnicas, errores humanos o ciberataques, exige la existencia de protocolos específicos que regulen los procesos de modificación de infraestructura, software y servicios TIC en el establecimiento.

c) Que, el presente Procedimiento de Seguridad para el Control de Cambios en los Medios y Sistemas de Procesamiento de Información establece un marco técnico-formal para la solicitud, evaluación, aprobación, implementación y cierre de cambios tecnológicos en el HUAP, con el fin de asegurar trazabilidad, control de riesgos y resguardo de la información crítica institucional.

d) Que, este instrumento incorpora estándares internacionales (como ISO/IEC 27001 y 27002), lineamientos del Ministerio de Salud y buenas prácticas en gestión de cambios, definiendo responsabilidades claras para el personal técnico, los usuarios claves y el Comité de Cambios TIC, así como criterios de documentación, validación, excepciones y actualización del inventario de activos.

e) Que, de conformidad con lo anterior, en el ejercicio de lo dispuesto en el artículo 23 letra c) del Decreto Supremo N°38. De 2005, del Ministerio de Salud, que contiene el Reglamento Orgánico de los Establecimientos de Salud de Menor Complejidad y de los Establecimientos de Autogestión en Red, según el cual le corresponde al Director organizar internamente el Establecimiento Autogestionado y;

f) asignar las tareas correspondientes, con el fin de atender las necesidades públicas o colectivas de una manera regular, continua y permanente, como lo ordenan los artículos 3° y 28 de la Ley N°18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado, y con la finalidad de establecer la ***primera versión*** del *"Procedimiento de seguridad control de cambios en los medios y sistemas de procesamiento de información"*, dicto la siguiente:

RESOLUCIÓN

I. APRUÉBANSE la ***primera versión*** del *"Procedimiento de seguridad control de cambios en los medios y sistemas de procesamiento de información "*, que es del siguiente tenor:

	PROCEDIMIENTO DE SEGURIDAD CONTROL DE CAMBIOS EN LOS MEDIOS Y SISTEMAS DE PROCESAMIENTO DE INFORMACIÓN				
	CÓDIGO UTIC	VERSIÓN 01	FECHA 09/2025	VIGENCIA 5 años	N° PÁGINAS 17

Revisado Por:	Aprobado Por:
Firmado por: Ilse Dora del Carmen Silva Robles Jefatura Calidad y Seguridad del Paciente (s) Fecha: 01-10-2025 16:34 CLT Hospital de Urgencia Asistencia Pública Dr. Alejandro del Río	Firmado por: Jorge Arturo Ibáñez Parga Director Huap (s) Fecha: 03-10-2025 17:10 CLT Hospital de Urgencia Asistencia Pública Dr. Alejandro del Río

ÍNDICE

I.INTRODUCCIÓN:

El Hospital de Urgencia Asistencia Pública (HUAP) depende de diversos sistemas y medios tecnológicos que resultan esenciales para la continuidad de la atención clínica, la gestión administrativa y la seguridad de la información. La evidencia internacional demuestra que las fallas en la gestión de cambios tecnológicos constituyen una de las principales causas de interrupciones en la operación hospitalaria, incidentes de ciberseguridad y pérdidas de datos sensibles (ISO/IEC 27001:2013; ISO/IEC 27002:2022; MINSAL, 2025).

En el ámbito sanitario, la magnitud del problema se refleja en que los hospitales son uno de los principales blancos de ataques informáticos a nivel mundial, generando riesgos críticos para la disponibilidad de los servicios, la confidencialidad de los registros clínicos y la integridad de los procesos asistenciales. Por esta razón, organismos internacionales como la Organización Mundial de la Salud (OMS) y el Ministerio de Salud de Chile han enfatizado la necesidad de contar con protocolos de seguridad informática y continuidad operativa.

El presente protocolo establece la forma en que se deben solicitar, evaluar, aprobar, implementar y cerrar los cambios tecnológicos en el Hospital de Urgencia Asistencia Pública (HUAP), garantizando la trazabilidad de los procesos, la mitigación de riesgos y la protección de los sistemas de información hospitalarios.

Este protocolo está dirigido a las y los funcionarios de la Unidad de Tecnologías de la Información, responsables de infraestructura, desarrollo de sistemas, ciberseguridad y soporte; al Comité de Cambios TIC; y a las y los usuarios clave de las áreas clínicas y administrativas, quienes participan en la validación y pruebas posteriores a la implementación de los cambios.

II.OBJETIVOS:

General

Establecer un procedimiento formal y sistemático para la gestión de cambios en los sistemas y medios tecnológicos del Hospital de Urgencia Asistencia Pública (HUAP), con el fin de asegurar la continuidad de los servicios y la protección de la información institucional.

Específicos

- Estandarizar la solicitud, evaluación, aprobación, implementación y registro de los cambios tecnológicos, garantizando trazabilidad y control.
- Minimizar los riesgos operativos y de ciberseguridad asociados a los cambios, favoreciendo la continuidad de la atención clínica y administrativa.

III.ALCANCE:

Este protocolo está dirigido a las y los funcionarios de la Unidad de Tecnologías de la Información del Hospital de Urgencia Asistencia Pública (HUAP), así como a las y los propietarios de sistemas y aplicaciones, integrantes del Comité de Cambios TIC (CAB) y usuarios/as clave designados/as en las distintas áreas clínicas y administrativas que participan en la validación y seguimiento de cambios tecnológicos.

IV.DEFINICIONES:

- **Cambio:** Toda modificación, adición, eliminación o actualización en los sistemas, aplicaciones, infraestructura o servicios tecnológicos del Hospital de Urgencia Asistencia Pública (HUAP).

- **Cambio estándar:** Modificación rutinaria, de bajo riesgo y bien documentada, que puede ejecutarse siguiendo un procedimiento previamente aprobado.

● **Cambio normal:** Modificación planificada que requiere evaluación, aprobación y coordinación antes de su implementación.

● **Cambio urgente:** Modificación necesaria para resolver una falla crítica, aplicar un parche de seguridad o restaurar un servicio esencial.

● **Solicitud de cambio (RFC, por sus siglas en inglés Request for Change):** Documento o registro formal donde se describe el cambio propuesto, su justificación, impacto, responsables y plan de implementación.

● **Plan de rollback:** Conjunto de pasos definidos para revertir un cambio en caso de problemas, restaurando la configuración previa.

● **Pruebas post-implementación:** Acciones que validan que el cambio fue realizado correctamente y que el sistema funciona como se esperaba.

● **Comité de Cambios TIC (CAB, por sus siglas en inglés Change Advisory Board):** Grupo conformado por representantes de la Unidad de Tecnologías de la Información (UTIC) que evalúa y aprueba cambios significativos o urgentes.

● **HUAP:** Hospital de Urgencia Asistencia Pública.

● **MINSAL:** Ministerio de Salud de Chile.

● **TIC:** Tecnologías de la Información y Comunicaciones.

● **Repositorio de versiones (GitLab):** Herramienta utilizada para gestionar, almacenar y controlar versiones de aplicaciones y código fuente de forma segura.

● **Bitácora técnica:** Documento o registro donde se anotan las acciones realizadas en la ejecución de un cambio tecnológico, incluyendo evidencias y observaciones.

● **Inventario de Activos TIC:** Registro oficial donde se mantiene actualizada la información sobre los equipos, sistemas y servicios tecnológicos del HUAP.

V.RESPONSABLES:

Responsables de Ejecución

- **Propietarios/as de sistemas o aplicaciones**
  - Solicitar formalmente los cambios.
  - Evaluar el impacto funcional respondiendo preguntas básicas como:
    - ¿Qué funciones o procesos dejarán de estar disponibles mientras se hace el cambio?
    - ¿Quiénes (personas o áreas) se verán afectados?
    - ¿Cuánto tiempo puede estar detenido el sistema sin causar problemas graves?
    - ¿Existen tareas alternativas (ej.: planillas, respaldo manual) en caso de falla?
  - Validar el funcionamiento tras la implementación.

- **Encargado/a de Infraestructura y Soporte TIC**
  - Planificar, coordinar y ejecutar cambios en redes, servidores y hardware.
  - Realizar respaldos previos y documentar la ejecución técnica.
  - Atender incidentes derivados de los cambios.

- **Equipo de Desarrollo TIC**
  - Planificar e implementar cambios en sistemas desarrollados internamente.
  - Mantener control de versiones y documentar actualizaciones.
  - Validar la funcionalidad de aplicaciones y bases de datos modificadas.

- **Responsable técnico del cambio**
  - Completar la RFC.
  - Evaluar riesgos y coordinar con otras áreas cuando sea necesario.
  - Ejecutar el cambio aprobado, validar resultados y actualizar registros.

- **Encargado/a de Ciberseguridad y Seguridad de la Información**
  - Evaluar los cambios con foco en seguridad.
  - Verificar que no se introduzcan vulnerabilidades.

- Mantener evidencias y reportes de impacto para auditorías.

- **Usuarios/as clave designados/as**
  - Realizar pruebas funcionales posteriores al cambio.
  - Reportar incidencias.
  - Confirmar el funcionamiento del sistema antes de su uso general.

Responsables de Supervisión

- **Comité de Cambios TIC (CAB)**
  - Evaluar y aprobar cambios significativos o urgentes.
  - Revisar planes de respaldo y rollback.
  - Registrar las decisiones tomadas y asegurar trazabilidad.
  - Está conformado por:
    - Jefe/a de la Unidad de TIC
    - Jefe/a de Desarrollo TIC
    - Encargado/a de Infraestructura
    - Encargado/a de Ciberseguridad y Seguridad de la Información

Responsables de Evaluación

- **Jefatura de la Unidad de Tecnología de la Información**
  - Evaluar el cumplimiento del protocolo de forma anual.
  - Proponer y realizar actualizaciones del documento conforme a normativa vigente.

VI. DESARROLLO DEL PROCESO

Inicio del Protocolo

El proceso comienza cada vez que un usuario, propietario de sistema o área requiera realizar un cambio en un sistema, aplicación, infraestructura o servicio tecnológico, ya sea por necesidades operativas, mejoras de funcionalidad, requerimientos normativos o resolución de incidentes.

En estos casos, el/la propietario/a del sistema o el/la persona responsable deberá ingresar una Solicitud de Cambio (RFC) elaborada en un documento o correo

electrónico y enviarla a la **Unidad de Tecnologías de la Información (UTIC)** a través del correo institucional oficial.

Para la elaboración de la solicitud, las y los usuarios deberán utilizar como referencia el **formato descrito en el Anexo N° 2** de este protocolo, el cual sirve únicamente como guía para asegurar que se incluyan los antecedentes mínimos requeridos.

Ejemplo: solicitar la actualización de un servidor o la instalación de una nueva versión de una aplicación

Desarrollo del Proceso

El procedimiento de gestión de cambios TIC se desarrolla en las siguientes etapas, según el **Flujograma de gestión de cambios** (Anexo N° 1):

1. Solicitud de cambio (RFC)

- Todo cambio debe **ser solicitado mediante un RFC**, siguiendo el formato mostrado en el **Anexo N° 2** de este protocolo.
- Cambios de bajo impacto (estándar) se registran directamente en la bitácora técnica y en el **Historial de Cambios** (Anexo N° 3).

2. Evaluación y coordinación

- El/la responsable técnico analiza riesgos y coordina con las áreas afectadas en un plazo máximo de **2 días hábiles** desde la recepción de la solicitud.
- Se priorizan horarios de baja carga (ej.: fuera de horario laboral).

3. Aprobación del cambio

- Estándar: aprobado por responsable técnico en un plazo máximo de **1 día hábil**.
- Normal: aprobado por Jefatura TIC o Comité de Cambios (CAB) en un plazo máximo de **5 días hábiles**.
- Urgente: aprobado por Jefatura TIC y Ciberseguridad de forma inmediata, con documentación posterior en el formato RFC.

4. Planificación

- El plan de implementación, rollback y pruebas debe definirse y comunicarse a las áreas involucradas en un plazo máximo de **3 días hábiles** tras la aprobación.

5. Implementación

- El cambio debe ejecutarse dentro de la ventana autorizada y en un plazo no superior a 10 días hábiles desde su aprobación, salvo casos justificados, como, por ejemplo:
  - Dependencia de proveedores externos.
  - Requerimientos de coordinación con unidades clínicas o administrativas críticas.
  - Restricciones derivadas de mantenciones programadas en infraestructura ministerial o de terceros.
  - Situaciones de fuerza mayor (ej.: emergencia hospitalaria, contingencia sanitaria, indisponibilidad de recursos).
- Supervisión del responsable técnico.
- Registro en el Historial de Cambios (Anexo N° 3).
- Ejemplo: reemplazar un switch de red en horario nocturno.

6. Pruebas post-implementación

- Validación de funcionamiento según lo planificado, dentro de las **24 horas siguientes** a la ejecución.
- Confirmación de usuarios/as clave.
- Registro en el formulario RFC y/o Historial de Cambios.

7. Cierre y registros

- Cierre formal del RFC dentro de los **3 días hábiles siguientes** a la validación.
- Actualización del inventario TIC en un máximo de **5 días hábiles**.
- Almacenamiento seguro de documentación y evidencias.

Tipos de cambios según su alcance

- **Infraestructura y hardware**
  - A cargo del Encargado/a de Infraestructura o Soporte TIC.
  - Proveedores externos pueden participar, siempre supervisados.
  - Documentación en el Historial de Cambios.
  - Ejemplo: reemplazo de discos en un servidor.

- **Software básico (sistemas operativos, parches, utilitarios)**
  - Se realizan en horarios de baja carga.
  - Sólo se aceptan actualizaciones desde fuentes oficiales.
  - Registro en el Historial de Cambios y pruebas posteriores.

- **Aplicaciones**
  - **Generales**: registro en historial, control de versiones, pruebas en ambiente de desarrollo, aprobación del propietario/a.
  - **Mayores**: se planifican como mini-proyectos, se documentan diferencias con la versión anterior, incluyen capacitación al personal afectado y salida a producción coordinada por TIC.

- **Cambios de emergencia**
  - Se ejecutan de inmediato priorizando la continuidad operativa.
  - Documentación retroactiva en RFC.
  - Validación posterior por Ciberseguridad.
  - Revisión por el CAB en la siguiente sesión o vía remota.

Término del Protocolo

El proceso finaliza con el cierre formal de la RFC y la distribución de los registros a la **Unidad de Tecnología de la Información**, a los/as propietarios/as de sistemas y al **Comité de Cambios TIC (CAB)**, asegurando trazabilidad y disponibilidad de la información.

VII.CONTINGENCIAS

En el marco de la gestión de cambios TIC, se consideran contingencias aquellas situaciones de emergencia que puedan interrumpir la correcta implementación del protocolo.

Entre ellas se incluyen:

- **Alertas sanitarias o eventos hospitalarios críticos**, que obliguen a priorizar la continuidad asistencial sobre la aplicación formal del proceso.

- **Fallas de infraestructura externa** (cortes de energía, caída de enlaces de internet o servicios ministeriales), que impidan ejecutar cambios en el tiempo programado.
- **Emergencias tecnológicas** (incidentes de ciberseguridad, ataques informáticos, fallas masivas de sistemas) que requieran activar cambios urgentes fuera de lo planificado.

En estos casos, se dará prioridad a mantener la continuidad operativa y la seguridad de la información, documentando posteriormente las acciones realizadas en la **Solicitud de Cambio (Anexo N° 2)** y en el **Historial de Cambios (Anexo N° 3)**.

VIII. REGISTROS

Los registros generados durante la gestión de cambios TIC deben almacenarse de forma segura y trazable, garantizando su integridad, confidencialidad y disponibilidad, y quedando accesibles para auditorías internas y externas.

- **Repositorio de versiones (GitLab)**
  - Registro: control de cambios en aplicaciones desarrolladas internamente (código fuente, scripts).
  - Herramienta: GitLab.
  - Responsable: Equipo de Desarrollo TIC y Encargado/a de Infraestructura TIC.
  - Frecuencia: cada cambio aprobado y liberado a producción debe registrarse en el repositorio.

- **Historial de Cambios (RFC)**
  - Registro: solicitudes de cambio, aprobación/rechazo, ejecución y cierre.
  - Formato: Formulario RFC (Anexo N° 2), Planilla de Historial de Cambios (Anexo N° 3) o correo institucional en casos excepcionales.
  - Responsable: Encargado/a de Ciberseguridad y Comité de Cambios TIC.
  - Almacenamiento: carpeta compartida con control de acceso.

- **Inventario de Activos TIC**
  - Registro: actualización del inventario de activos TIC cuando corresponda al cambio aplicado.
  - Responsable: Encargado/a de Ciberseguridad.
  - Plazo: dentro de los 5 días hábiles posteriores al cierre del cambio.
- **Bitácoras técnicas de ejecución y validación**
  - Registro: documentación técnica básica (logs, capturas de pantalla, evidencias de validación de usuarios/as).
  - Responsable: responsable Técnico del Cambio.

IX.DIFUSIÓN

El protocolo se difundirá de manera accesible y comprensible para las áreas involucradas, mediante:

- Envío de correo electrónico informativo a todas las unidades del hospital.

X.REVISIÓN

El presente protocolo deberá ser revisado al menos una vez al año, o antes si ocurre alguna de las siguientes situaciones:

- Cambios relevantes en los sistemas TIC o en procesos críticos.
- Actualización de normativa aplicable.
- Incidentes que evidencien deficiencias en su aplicación.

Responsables de la revisión: Jefatura de la Unidad de Tecnologías de la Información en coordinación con el Comité de Cambios TIC.

El resultado de la revisión deberá documentarse en el apartado “Modificaciones del Documento” de la presente versión.
.

XI.EXCEPCIONES AL CUMPLIMIENTO

Podrán solicitarse excepciones a este protocolo en casos debidamente justificados, mediante correo electrónico formal dirigido a la Jefatura TIC, con copia al Comité de Cambios TIC.

Toda solicitud de excepción deberá incluir:

- Descripción del cambio o requisito al que se solicita excepción.
- Justificación técnica o clínica.
- Medidas de control compensatorio propuestas (si corresponde).
- Plazo solicitado para la excepción (máximo 6 meses).

La aprobación corresponde a la Jefatura TIC, con visto bueno del Comité de Cambios TIC.

Las excepciones deberán registrarse en el repositorio oficial definido por la UTIC (carpeta de gestión documental), y serán revisadas antes de su vencimiento. En caso de persistir la causa, podrán renovarse formalmente o cerrarse mediante la regularización definitiva.

El/la Encargado/a de Ciberseguridad será responsable de mantener actualizado el registro de excepciones y su estado.

XII. DISTRIBUCIÓN

- Dirección
- Subdirección de Gestión Clínica
- Subdirección Administrativa y Financiera
- Subdirección de Gestión del Cuidado
- Subdirección de Gestión y Desarrollo de las Personas
- Unidad de Calidad y Seguridad del Paciente.
- Unidad de Tecnologías de la Información.

XIII.REFERENCIAS BIBLIOGRÁFICAS

- Instituto Nacional de Normalización. (2013). *NCh-ISO 27001.Of2013: Sistemas de gestión de la seguridad de la información*. Santiago, Chile: INN.
- International Organization for Standardization & International Electrotechnical Commission. (2022). *ISO/IEC 27002:2022 – Information security, cybersecurity and privacy protection — Information security controls*. Ginebra, Suiza: ISO/IEC.
- Ministerio de Salud de Chile. (2025). *Orientaciones técnicas sobre ciberseguridad y continuidad operativa (COMGES 2025)*. Santiago, Chile: MINSAL.

XIV.MODIFICACIONES DEL DOCUMENTO

SÍNTESIS DE MODIFICACIONES			RESPONSABLE MODIFICACIÓN	APROBADO POR DIRECTOR
VERSIÓN	**FECHA**	**CAUSA DE MODIFICACIÓN**		
01	09/2025	Creación del Documento	Enzo Mayo G. Encargado Ciberseguridad	Dr. Patricio Barría

XV.ANEXOS

Anexo N° 1: Flujograma de gestión de cambios TIC

Anexo N° 2: Formato de Solicitud de Cambio (RFC)

N° de RFC	
Título del cambio	
Fecha	
Solicitante	
Descripción del cambio	
Justificación	
Sistemas afectados	
Impacto esperado	
Riesgos identificados	
Plan de implementación	
Plan de rollback	
Responsable(s) de ejecución	
Aprobación (Jefatura TIC / CAB)	

Anexo N° 3: Planilla de historial de cambios

N° RFC	Fecha	Tipo de cambio (Estándar / Normal / Urgente)	Descripción breve	Responsable	Estado (Abierto / Cerrado)	Observaciones

Elaborado por:

1. Enzo Mayo G., Encargado de Ciberseguridad y Seguridad de la Información

Revisado por:

1. Susana Avendaño D., Jefa Unidad de Tecnologías de la Información
2. TM. Camila Andrea Benítez Ugarte, Profesional Unidad de Calidad y Seguridad del Paciente
3. Christian Echeverría A., Subdirector Administrativo y Financiero

FIRMA ELECTRÓNICA AVANZADA · GOBIERNO DE CHILE

Firmado por:
Camila Andrea Benítez Ugarte
Profesional Unidad Calidad y Seguridad del Paciente
Fecha: 26-09-2025 13:53 CLT
Hospital de Urgencia Asistencia Pública Dr. Alejandro del Río

Firmado por:
Christian Irving Echeverría Aburto
Subdirector Gestión Administrativa y Financiera
Fecha: 26-09-2025 15:11 CLT
Hospital de Urgencia Asistencia Pública Dr. Alejandro del Río

Firmado por:
Susana Ximena Avendaño Durán
Jefatura Tic
Fecha: 30-09-2025 17:08 CLT
Hospital de Urgencia Asistencia Pública Dr. Alejandro del Río

II. TÉNGASE PRESENTE la vigencia de este procedimiento a contar de la fecha de la total tramitación de la presente Resolución.

III. ESTABLÉCESE que el señalado *"Procedimiento de seguridad control de cambios en los medios y sistemas de procesamiento de información"*, debe ser el que se tenga en consideración a contar de la fecha de su entrada en vigencia.

IV. DÉJESE SIN EFECTO toda normativa interna que diga relación con la materia de este procedimiento.

ANÓTESE, COMUNÍQUESE Y ARCHÍVESE

FIRMA ELECTRÓNICA AVANZADA · GOBIERNO DE CHILE

Firmado por:
Patricio Raúl Barría Ailef
Director Huap
Fecha: 06-11-2025 16:44 CLT
Hospital de Urgencia Asistencia Pública Dr. Alejandro del Río

CEWSP
Distribución:

1. Dirección.
2. Subdirección de Gestión Clínica.
3. Subdirección de Gestión del Cuidado.
4. Subdirección de Gestión y Desarrollo de las Personas.
5. Departamento de Planificación y Desarrollo.
6. Unidad de Calidad y Seguridad del Paciente.
7. Unidad de Auditoría.
8. Asesoría Jurídica.
9. Oficina de Partes.

XASV