TABLA DE CONTENIDO

1. DEFINICIÓN. 3
2. OBJETIVO. 3
3. ALCANCE 3
4. ENFOQUE DIFERENCIAL. 3
5. MARCO LEGAL. 3
6. RECURSO HUMANO. 3
7. MATERIALES INSUMOS, EQUIPOS Y/O DISPOSITIVOS MÉDICOS. 4
8. CONCEPTUALIZACIÓN IMEDICALCLOUD. 4
9. COMPONENTES DE LA APLICACIÓN IMEDICALCLOUD. 5
   9.1 APLICACIÓN WEB 5
   9.2 ACCESO A LA APLICACIÓN 6
   9.3 AMBIENTE DE DESARROLLO 6
   9.4 SEGURIDAD PARA EL ENTORNO DEL HOSPEDAJE DE LA INFORMACION 6
10. PUNTOS DE DISEÑO CLAVE DE LA ARQUITECTURA 7
   10.1 ENRUTADORES DE FILTRADO 8
   10.2 FIREWALLS 8
   10.3 PROTECCIÓN CRIPTOGRÁFICA DE MENSAJES 8
   10.4 ADMINISTRACIÓN DE REVISIONES DE SEGURIDAD DE SOFTWARE 8
   10.5 SUPERVISIÓN. 8
   10.6 SEGMENTACIÓN DE LA RED 9
   10.7 SEGURIDAD FÍSICA 9
11. REDUNDACIÓN DEL CENTRO DE DATOS 9
12. ITEMS DE SEGURIDAD DEL SOFTWARE 10
   12.1 ACCESO 10
   12.2 REGISTRO 10
   12.3 CAPACITACIÓN 11
   12.4 DESHABILITACIÓN 11
   12.5 IMPRESIÓN 11
   12.6 MODIFICACIONES 11

COPIA CONTROLADA

12.7 ADMINISTRACIÓN DE BASE DE DATOS.....11
13. PRIVACIDAD 12
14. BACK UPS.....12
15. CONTROL DE CAMBIOS 13
16. MATRIZ DE RESPONSABILIDAD.....13

COPIA CONTROLADA

SEGURIDAD Y CONFIDENCIALIDAD DE LA HISTORIA CLÍNICA IMEDICALCLOUD

1. DEFINICIÓN.

El sistema de información IMEDICALCLOUD es una aplicación Web Enabled que permite la gestión de información integral en instituciones prestadoras de servicios de salud. Debido al diseño modular y funcional del sistema la aplicación puede funcionar en entidades de salud de baja complejidad (como consultorios clínicos, centros de salud o clínicas odontológicas) así como entidades de alta complejidad (hospitales nivel III-IV).

2. OBJETIVO.

Garantizar la seguridad y la confidencialidad en el manejo de la historia clínica electrónica por medio del software Imedical cloud.

3. ALCANCE.

Aplica para todas las historias clínicas electrónica gestionadas por el software Imedical cloud.

4. ENFOQUE DIFERENCIAL.

Ver PT07 DA.

5. MARCO LEGAL.

Resolución 3100 de 2019, define los procedimientos y condiciones que deben cumplir los Prestadores de Servicios de Salud para habilitar los servicios.

6. RECURSO HUMANO.

- Ingenieros de informática de la institución.
- Tecnólogos de informática.

COPIA CONTROLADA

7. MATERIALES INSUMOS, EQUIPOS Y/O DISPOSITIVOS MÉDICOS.

- Equipos de hardware utilizados en el proceso (Computadores, enrutadores, servidores, etc.)
- Software utilizado en el proceso.

8. CONCEPTUALIZACIÓN IMEDICALCLOUD.

El modelo de servicios de ImedicalServices SAS está basado en el concepto de Servicios Cloud (SaaS), lo cual nos permite ofrecer aplicaciones de software de alta calidad soportadas en infraestructura con modelo de nube, para acceder a las aplicaciones lo único que se necesita es un navegador de Internet. SaaS es una manera de entregar soluciones de tecnología que cumplan la visión de arquitectura de SOA.



Al estar implementado IMEDICALCLOUD sobre el modelo de Nube, a nuestros clientes les podemos ofrecer altos estándares en calidad del servicio:

Escalabilidad
Disponibilidad
Capacidad de cómputo: procesamiento almacenamiento
Tiempos de respuesta Seguridad

9. COMPONENTES DE LA APLICACIÓN IMEDICALCLOUD.

El sistema de información IMEDICALCLOUD está desarrollado bajo tecnologías que nos permitirán garantizar buenos tiempos de respuesta, un alto grado de seguridad de la información, soportar la operación en línea las 24 hora del día 7 días a la semana, la escalabilidad, modularidad y un fácil mantenimiento de la aplicación.

El desarrollo de la aplicación esta implementado en la plataforma de servicios PaaS Windows Azure, lo cual nos permite aprovechar las infraestructuras de nube (centros de datos) provistas por Microsoft.



El sistema de información IMEDICALCLOUD está conformado por los siguientes componentes tecnológicos:

9.1 APLICACIÓN WEB

IMEDICALCLOUD es una aplicación Web Enabled conformada por módulos que garantizan los procesos asistenciales y en particular la historia clínica electrónica otorgando protección, confidencialidad y seguridad de los datos clínicos y administrativos de una IPS. Los usuarios del sistema autorizados mediante direccionamiento IP podrán acceder desde cualquier punto de Internet o Intranet; La aplicación cuenta con una arquitectura de desarrollo de 3 capas: Presentación, Lógica del Negocio y Acceso a Datos.

COPIA CONTROLADA

Capa de Presentación se utilizarán Controles web que permitirán la reutilización de código, garantizando la modularidad y un fácil mantenimiento.

Capa de Lógica del Negocio se utilizará un modelo de componentes en N niveles.

Capa de acceso a datos y sobre este se construirán los subsiguientes niveles. Estos componentes serán transaccionales garantizando así la escalabilidad, la modularidad y la persistencia de la información.

9.2 ACCESO A LA APLICACIÓN

El acceso está controlado por roles definidos por el área de informática del Hospital Cardiovascular. Cada usuario debe autenticarse con su cuenta personal, creada a solicitud formal de las áreas responsables. Los perfiles determinan los permisos de lectura, escritura o impresión.

9.3 AMBIENTE DE DESARROLLO

El desarrollo de la aplicación IMEDICALCLOUD esta implementado en la plataforma de servicios PaaS Windows Azure, lo cual nos permite aprovechar las infraestructuras de nube (centros de datos) provistas por Microsoft. Esta plataforma de Servicios está conformada por:

Windows Azure: servicio de procesamiento (capacidad de cómputo), que permite alojar y desarrollar aplicaciones basadas en Cloud. Permite almacenar la información en servidores de datos.

SQL Azure: base de datos relacional habilitada para proyectos Cloud.

AppFabric: servicio de control de acceso (seguridad), servicio de almacenamiento en caché, servicio de bus de conexiones.

La Herramienta de desarrollo del sistema de información es MS Visual Studio 2010 (ASP.NET: WebForms) y MS Visio. Para el control de versiones se utiliza MS Team Foundation Server 2010.

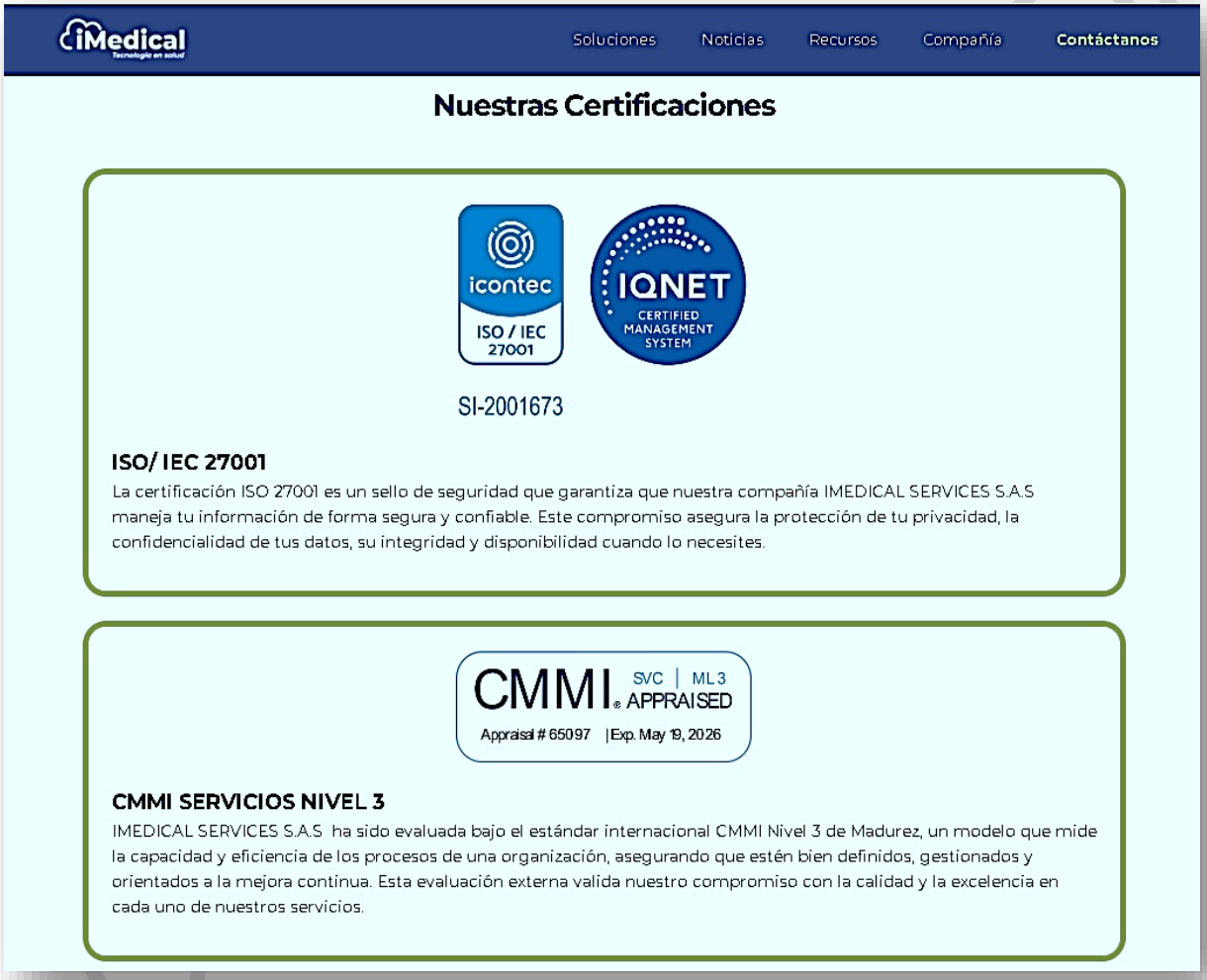
9.4 SEGURIDAD PARA EL ENTORNO DEL HOSPEDAJE DE LA INFORMACION

La nube utilizada por ImedicalServices SAS es Microsoft Azure, plataforma que cuenta con los más altos estándares internacionales de seguridad de la información, incluyendo la

COPIA CONTROLADA

certificación ISO/IEC 27001. Esta certificación es válida para todos los clientes cuyos servicios están alojados en Azure.

Adicionalmente ImedicalServices SAS también cuenta con la certificación ISO/IEC 27001, lo que ratifica su compromiso con la gestión segura de la información. Así mismo, ha obtenido la certificación en CMMI para Servicios Nivel 3, que garantiza la implementación de buenas prácticas en la gestión y prestación de servicios tecnológicos.



10. PUNTOS DE DISEÑO CLAVE DE LA ARQUITECTURA

La plataforma Windows Azure está diseñada para proporcionar “defensa en profundidad”, lo que reduce el riesgo de que un error de un mecanismo de seguridad ponga en peligro la seguridad de todo el entorno. Las capas de defensa en profundidad incluyen:

10.1 ENRUTADORES DE FILTRADO

Los enrutadores de filtrado rechazan los intentos de comunicación entre direcciones y puertos no configurados como permitidos. De este modo, se previenen ataques comunes que usan “drones” o “zombies” en busca de servidores vulnerables. Aunque su bloqueo es relativamente sencillo, estos tipos de ataques siguen siendo el método preferido de los atacantes malintencionados que buscan puntos vulnerables. Los enrutadores de filtrado también permiten la configuración de servicios back-end de modo que solo estén accesibles desde sus correspondientes front-ends.

10.2 FIREWALLS

Los firewalls restringen la comunicación de datos entre puertos, protocolos y direcciones IP de origen y destino autorizados y conocidos.

10.3 PROTECCIÓN CRIPTOGRÁFICA DE MENSAJES

Para proteger los mensajes de control que se envían entre los centros de datos de Windows Azure y entre los clústeres de un centro de datos dado, se utiliza TLS con claves criptográficas de al menos 128 bits. Asimismo, el tráfico entre los usuarios finales y las máquinas virtuales se encuentra cifrado mediante TLS, garantizando la confidencialidad e integridad de la información transmitida.

10.4 ADMINISTRACIÓN DE REVISIONES DE SEGURIDAD DE SOFTWARE

La administración de revisiones de seguridad es una parte de las operaciones que ayudan a proteger los sistemas de puntos vulnerables conocidos. La plataforma Windows Azure utiliza sistemas de implementación integrados para administrar la distribución e instalación de revisiones de seguridad de software de Microsoft.

10.5 SUPERVISIÓN.

La seguridad se supervisa con ayuda de sistemas de supervisión, correlación y análisis centralizados que administran la gran cantidad de información generada por los dispositivos del entorno, proporcionando supervisión y alertas pertinentes y puntuales.

COPIA CONTROLADA

10.6 SEGMENTACIÓN DE LA RED

Microsoft usa varias tecnologías para crear barreras para el tráfico no autorizado en las conexiones hacia y en los centros de datos, incluidos firewalls, cuadros de traducción de direcciones de red (equilibradores de carga) y enrutadores de filtrado. La red back-end se compone de redes de área local con particiones para servidores web y de aplicaciones, almacenamiento de datos y administración centralizada. Estos servidores se agrupan en segmentos de direcciones privadas protegidos por enrutadores de filtrado.

10.7 SEGURIDAD FÍSICA

La seguridad física corre paralela a las medidas de seguridad basadas en software, y ambas tienen procedimientos de evaluación y mitigación de riesgos similares.

Los servicios de la plataforma Windows Azure se entregan a los clientes a través de una red de centros de datos globales, cada uno de los cuales está diseñado para ejecutarse las 24 horas del día, los 7 días de la semana, y emplea varias medidas para ayudar a proteger las operaciones de errores de alimentación, intrusiones físicas e interrupciones de red. Estos centros de datos, dispersos geográficamente, dirigidos, administrados y supervisados por personal de operaciones de Microsoft, cumplen los estándares del sector en cuanto a seguridad física y confiabilidad.

Microsoft utiliza mecanismos de acceso de alta seguridad, limitados a personal de operaciones reducido, que debe cambiar con regularidad sus contraseñas de acceso de administrador. El director de operaciones de red controla el acceso a los centros de datos y los permisos para abrir vales de acceso a los centros de datos, en combinación con las prácticas de seguridad de los centros de datos locales.

Redundancia del servicio

Cada capa de la infraestructura de la plataforma Windows Azure está diseñada para que continúen las operaciones en caso de que se produzca un error, incluidos los dispositivos de red redundantes de cada capa y los proveedores de acceso a Internet duales de cada centro de datos. La conmutación por error es automática en la mayoría de los casos y no requiere la intervención del usuario. El Centro de operaciones de red supervisa la red las 24 horas del día, los 7 días de la semana, a fin de detectar cualquier anomalía o posibles problemas en la red.

11. REDUNDACIÓN DEL CENTRO DE DATOS

La plataforma Windows Azure se ejecuta en varios centros de datos de todo el mundo. Si se

COPIA CONTROLADA

produjese una catástrofe que afectase a un centro de datos completo, un cliente podría implementar su aplicación en una ubicación de copia de seguridad.

12. ITEMS DE SEGURIDAD DEL SOFTWARE

12.1 ACCESO

Para el ingreso y acceso al sistema de Historia Clínica del Hospital Cardiovascular a través del software iMedical Cloud, es requisito contar con un usuario y contraseña.

El proceso de creación de usuarios inicia cuando el área de Talento Humano entrega el formato de solicitud de creación de usuario al colaborador. Este debe diligenciarlo completamente, recolectar las firmas correspondientes de las áreas responsables (Coordinador Inmediato y Talento Humano), y entregarlo al área de Informática para su validación y creación del acceso.

El usuario es creado con base en el tipo y número de documento de identidad del colaborador, permitiendo una identificación unívoca en el sistema.

Una vez creado, el sistema envía automáticamente un correo electrónico al nuevo usuario con un enlace para que este mismo defina su contraseña de acceso.
La contraseña debe cumplir los siguientes requisitos de seguridad:

Tener mínimo 8 y máximo 16 caracteres.

Incluir al menos un número.

Incluir letras (mayúsculas o minúsculas).

Incluir al menos un carácter especial válido: - +., $ _! % / =

Las credenciales son personales, intransferibles y su custodia es responsabilidad exclusiva del usuario.

En el caso de personas externas a la institución, como los auditores médicos, el acceso se limita a los pacientes correspondientes a su entidad. Para estos casos se habilita un código general por entidad auditora, sin cuentas individuales.

12.2 REGISTRO

El software hospitalario está diseñado para registrar toda la información de cada uno de los procedimientos que se le realicen al paciente durante su estancia, quedando como soporte la fecha, hora y responsable de la persona que realiza el registro de acuerdo al cargo que desempeña.

COPIA CONTROLADA

12.3 CAPACITACIÓN

Todo el personal es capacitado en el manejo de la Historia Clínica, según el cargo que vaya a desempeñar. Esta capacitación la realiza el personal de Informática o el jefe de área de cada servicio dependiendo del rol perfil asignado. Esta capacitación se hace siempre antes de la creación de usuarios

12.4 DESHABILITACIÓN

El proceso de inactivación de usuarios se realiza al momento de la desvinculación laboral. El colaborador debe gestionar el formato de paz y salvo y obtener las firmas de las diferentes áreas, incluyendo la del área de Informática. Una vez firmada esta sección, el usuario es inmediatamente inactivado del sistema.

12.5 IMPRESIÓN

La impresión de información de la Historia Clínica Electrónica está controlada mediante la asignación de permisos específicos en el sistema.

Esta opción se otorga únicamente a los perfiles de usuario cuya operación y funciones así lo requieran.

El objetivo de esta medida es garantizar que solo el personal autorizado pueda generar impresiones, reduciendo riesgos de divulgación no autorizada de información clínica.

12.6 MODIFICACIONES

Una vez registrada y guardada la información en la Historia Clínica Electrónica, no es posible realizar modificaciones sobre el contenido original, lo que garantiza la integridad y trazabilidad de los registros clínicos.

En caso de requerirse una corrección, aclaración o complemento, esta debe ser realizada a través de una nota aclaratoria, la cual quedará asociada al episodio clínico correspondiente.

12.7 ADMINISTRACIÓN DE BASE DE DATOS

COPIA CONTROLADA

La responsable de administrar el servidor de Bases de Datos y realizar los backups es la empresa ImedicalServices SAS dueños del software.

13. PRIVACIDAD

Microsoft trata la información personal como privada y tomará todas las medidas razonables y habituales para manipular correctamente los datos personales de los clientes.

Microsoft (incluidas, a tal fin, todas sus subsidiarias de EE. UU.) Cuenta con la certificación Safe Harbor del Departamento de Comercio de EE. UU. Esto permite la transferencia legal de datos a Microsoft para su procesamiento desde la Unión Europea y países con leyes de protección de datos similares. Microsoft actúa como procesador de datos y, en lo que afecta a la capacidad del servicio, las decisiones sobre el uso de los datos las toma el controlador de datos.

14. BACK UPS

iMedicalCloud realiza copias de seguridad automáticas de toda la información registrada, utilizando la infraestructura de Microsoft Azure.

Se efectúan:

-Backups completos de manera periódica.

-Backups diferenciales para registrar los cambios entre respaldos completos.

-Backups del registro de transacciones (log) que se ejecutan cada 2 a 10 minutos, según la carga de trabajo de la base de datos.

Las copias de seguridad se almacenan en múltiples ubicaciones mediante mecanismos de redundancia local (LRS) y redundancia geográfica (GRS), lo que garantiza la disponibilidad de la información incluso ante eventos catastróficos.

Además, se cuenta con opciones de retención a largo plazo, lo que permite restaurar versiones históricas de la base de datos si es requerido por normativas o por solicitud institucional. El acceso a estas copias está restringido y gestionado exclusivamente por iMedicalCloud, cumpliendo con los estándares internacionales de seguridad y confidencialidad.

COPIA CONTROLADA

15. CONTROL DE CAMBIOS

Versión	Ítem	Descripción del Cambio	Elaboró	Revisó	Aprobó	Fecha
01		No se realizan ajustes ni modificaciones	Malitson Torres	Lilibeth Escamilla R.	Dr. Leonidas Olaya	Abril 2024
02	9.2	Actualización de roles	Malitson Torres	Lilibeth Escamilla R.	Dr. Leonidas Olaya	Agosto 2025
02	12.1	Inclusión de requisitos de creación de contraseña de acceso.	Malitson Torres	Lilibeth Escamilla R.	Dr. Leonidas Olaya	Agosto 2025
03	10.3	Se anexa información sobre cifrado mediante TLS, el cual garantiza la confidencialidad e integridad de la información transmitida	Malitson Torres	Lilibeth Escamilla R.	Dr. Leonidas Olaya	Septiembre 2025

16. MATRIZ DE RESPONSABILIDAD

	NOMBRE	CARGO	FIRMA	FECHA ELABORACIÓN	FECHA VIGENCIA
ELABORÓ	ALEJANDRO VALERO	COORDINADOR INFORMÁTICA		ABRIL 2021	SEPTIEMBRE 2028
REVISÓ	LILIBETH ESCAMILLA RUBIO	DIRECCCIÓN ADMINISTRATIVA		ABRIL 2021	
APROBÓ	DR. RICARDO PERICO	DIRECCIÓN GENERAL		ABRIL 2021	

COPIA CONTROLADA