EQUIPO C

ESTRATEGIA JURIDICA

AllianceTech S.A.S

Estimados DataHealth, de conformidad con la convocatoria, a continuación, encontrarán nuestra opinión profesional, con referencia a la estrategia jurídica que debe irradiar la negociación entre AllianceTech y DataHealth. Para tales efectos, hemos estructurado el presente documento de la siguiente manera:

INDICE:

1. INTRODUCCIÓN:

Datahealth, empresa en tecnología, desea desarrollar una IA que utilice algoritmos de aprendizaje automático para interpretar grandes conjuntos de datos médicos que le permitan ofrecer diagnósticos precisos y planes de tratamiento personalizado que apoyen los diagnósticos de los especialistas en salud. Además, dicho producto, pretende ser ofrecido por DataHealth a hospitales y clínicas en Colombia, y tener la potencialidad de expansión a países como Brasil, Estados Unidos y países europeos.

Ya que no existe en el mercado un producto que cumpla con estas características, AllianceTech S.A.S, empresa especialista en el desarrollo de sistemas complejos de IA que apoyan al sector salud, propone a DataHealth la adopción de una estrategia jurídica que tenga en cuenta los siguientes puntos:

2. PROBLEMAS TÉCNICOS:

2.1 ¿Es posible desarrollar un sistema que cumpla con las características que requiere DataHealth?

Sí, es posible desarrollar un sistema de software con las características de interoperabilidad hospitalaria, algoritmos de procesamiento de datos complejos con técnicas de aprendizaje profundo y supervisado, que además cuente con una capacidad de adaptación y aprendizaje, con un sistema de encriptación de datos y mecanismos de autenticación. Asimismo, que cuente con un sistema de soporte técnico 24/7 y que sea capaz de operar en distintos idiomas y de interactuar con tecnologías emergentes, tal y como lo exige DataHealth en la convocatoria.

Lo anterior lo lograremos implementando sistemas de información que se comunican entre sí, como HL7, DICOM y FHIR, para obtener mayor nivel de detalle al momento de utilizar VitalAI y para lograr intercambiar información médica en los distintos centros hospitalarios que instalen el sistema.

El tipo de IA que se utilizará para el desarrollo del sistema de VitalAI es el de superinteligencia artificial (ASI), el cual es un modelo que permite analizar datos de forma rápida, consciente y automática, lo que favorecerá el análisis para el diagnóstico de patologías y formulación de tratamientos. Por otra parte, el modelo de entrenamiento de este sistema será el de redes neuronales artificiales, ya que es apto para aprender a partir de la información de entrada, lo que permite optimizar su aprendizaje a medida que se utiliza y se ingresa más información.

Se garantizará el cumplimiento de estándares de seguridad por medio de: i) la encriptación de datos en reposo, es decir aquellos que están almacenados en discos duros y bases de datos, mediante VeraCrypt[1]; y ii) la encriptación de datos en tránsito, que son aquellos que protegen la información mientras se mueven a través de redes interna o externas - como, por ejemplo, entre dispositivos médicos o sistemas de información hospitalaria – Mediante Transport, Layer, Security (TLS)[2].

En materia de autenticación, se logrará por medio de dos herramientas que son: i) Single Sign-On (SSO), que sirve para que un usuario pueda acceder a distintos sistemas con una única credencial de inicio de sesión; y ii) Multifactor Authentification (MFA), que sirve para configurar métodos de autenticación robustos como contraseñas, autenticación biométrica y tokens de Hardware.

Por último, el requisito de soporte técnico se hará efectivo dependiendo de la elección que realice el cliente en materia de servidores, ya que se ofrece la posibilidad de utilizar servidores de Amazon

[1] Para una revisión más detallada sobre las funciones del sistema, véase el “anexo técnico”.

[2] Para una revisión más detallada sobre las funciones del sistema, véase el “anexo técnico”.

Web Services (AWS) o servidores propios, caso en el cual se utilizará Splunk[3]. Las implicaciones económicas de estas alternativas se abordarán más adelante en este documento.

2.2 ¿Qué tipos de datos se requerirán?

Para que VitalAI funcione tal como indica en la convocatoria, se debe ingresar una extensa base de datos médicos que abarca desde ciencias básicas como anatomía, fisiología y genética, a conocimientos clínicos y especialidades médicas como cardiología, neurología, oncología, gastroenterología, endocrinología, oftalmología, ortopedia, otorrinolaringología, fonoaudiología y hematología. Durante la ejecución del contrato solo entrenará la IA en el conocimiento de las especialidades anteriormente descritas, sin perjuicio de que DataHealth pueda ingresar más información médica de otras áreas de la medicina. Esto es así debido a que no es posible perfeccionar el entrenamiento de VitalAI en todos los campos del conocimiento médico en el transcurso de 1 año como lo propone DataHealth.

Por otro lado, será necesario que el sistema procese datos personales como altura, peso, sexo, género, grupo sanguíneo, viajes frecuentes, domicilio, estilo de vida, alimentación, frecuencia con la que hace deporte, si tiene enfermedades hereditarias, o enfermedades preexistentes, si se ha operado, si ha estado hospitalizado, si dona sangre, la frecuencia con la que asiste al médico, su información sexual y reproductiva. Lo anterior con la finalidad de que el sistema pueda proponer diagnósticos más precisos y tratamientos completos teniendo en cuenta condiciones particulares de los pacientes que puedan incidir en la valoración de enfermedades.

2.3 ¿AllianceTech cuenta con la experiencia, desde el punto de vista técnico, para desarrollar un sistema de inteligencia Artificial de estas características?

Sí, AllianceTech S.A.S es una empresa de desarrollo de software con una amplia trayectoria en el mercado de creación y comercialización de sistemas tecnológicos que apoyan las áreas de salud.

Uno de sus proyectos más importantes fue la creación de un sistema de inteligencia artificial capaz de procesar datos de diagnósticos de pacientes y bases de datos de inventario farmacéutico, con la finalidad de identificar sectores poblacionales con déficit de acceso a ciertos medicamentos para que fundaciones como el “Banco de medicamentos”, “farmamundi” y “fundación cottolengo” pudieran coordinar planes de donación de equipo médico y medicinas.

3. PROBLEMAS ÉTICOS:

Si bien ya determinamos que es posible desarrollar el sistema de VitalAI desde el punto de vista técnico, nos compete ahora analizar la viabilidad ética del sistema de IA requerido por DataHealth, para ello analizaremos los siguientes puntos:

3.1 ¿Es posible desarrollar un sistema con estos requerimientos desde el punto de vista ético?

Ahora bien, nos ocupa preguntarnos si es posible desarrollar un sistema de IA, que cumpla con las exigencias técnicas requeridas por DataHealth, desde el punto de vista técnico. Una respuesta rápida es que sí es posible.

Lo anterior, teniendo en cuenta los lineamientos y principios que se han expuesto en normas relativas a IA, como la AI act promulgada por la Unión Europea, la Guía de la casa blanca para la regulación de la IA, y próximamente el CONPES sobre IA en Colombia.

[3] La descripción de los beneficios y condiciones técnicas de cada opción de servidor se encuentra en el anexo técnico.

En estas normas se han desarrollado marcos éticos, para la implementación de sistemas de IA, que se basan en los principios de[4]:

- **Transparencia.** Que implica proporcionar información significativa y comprensible sobre el diseño, funcionamiento e impacto de los sistemas, de forma clara y accesible, a desarrolladores, usuarios e individuos que puedan ser afectados por las decisiones de la IA.
- **Privacidad.** Que supone respetar la intimidad y la esfera privada de las personas y que no pueda usarse la información que no se haya autorizado.
- **Control humano de las decisiones propias**. Que implica que las IA con autonomía en la toma de decisiones deben pasar por control humano para evitar resultados no deseados.
- **Seguridad**. Que hace referencia a que los sistemas de IA deben diseñarse y desarrollarse de manera que sean robustos, seguros y fiables. Deben ser capaces de resistir ataques cibernéticos y evitar resultados perjudiciales.
- **Responsabilidad.** Que implica que debe existir una responsabilidad solidaria por los resultados y/o afectaciones que produzca la IA. Lo anterior salvo que se demuestre que el resultado fue producto de la negligencia o intencionalidad de un individuo en particular.

3.2 ¿Qué debemos hacer para implementar los principios del marco ético a VitalAI?

Para dar respuesta a este punto nos vamos a remitir a las disposiciones de la ley de Inteligencia Artificial de la Unión Europea (AI Act), por medio de la se exige el cumplimiento de una serie de requisitos para la implementación de la IA según el nivel de riesgo en donde se encuentre[5].

En el caso que nos compete, el sistema de VitalAI se encuadra en el grado de riesgo alto ya que la funcionalidad de este requiere el procesamiento datos sensibles que requieren de protección especial y además porque puede influenciar la toma de decisiones en el campo médico – Ya que será utilizada como un apoyo para el diagnóstico médico-.

Para las inteligencias encuadradas en el grado de alto riesgo se exigen requisitos como: i) la implementación de planes de gestión de riesgos, ii) llevar documentación con información detallada sobre el desarrollo, funcionamiento y el rendimiento del sistema, iii) aviso de información a los usuarios, en este caso los titulares de los datos sensibles, sobre las capacidades del sistema, su nivel de precisión y riesgos que puede acarrear, iv) adopción de medidas técnicas que aseguren precisión y robustez en temas de ciberseguridad, v) el sometimiento previo de la IA a una evaluación de conformidad para garantizar que cumpla con los requisitos legales.

Todas estas medidas serán incluidas como obligaciones a cargo del desarrollador dentro del clausulado del contrato de desarrollo de software, instalación y servicios Post, que expondremos en un momento. Lo anterior, con la intención de garantizar que el sistema de VitalAI cumpla con los marcos éticos de las regulaciones del sistema europeo, Estadounidense y próximamente el colombiano, ya que estas medidas se ajustan al CONPES sobre IA que pretende ser implementado en agosto del presente año en el Estado colombiano[6].

4. PROBLEMAS JURÍDICOS:

[4] Para una revisión más detallada de la regulación sobre de la inteligencia artificial, véase (Ley de Inteligencia Artificial, 2023)

[5] La ley reconoce 4 clasificaciones de IA según el riego: riesgo inaceptable, riego Alto, Riesgo limitado y Riesgo Mínimo. Para una revisión más detallada de la regulación sobre de la inteligencia artificial, véase (Ley de Inteligencia Artificial, 2023).

[6] Para una revisión más detallada del CONPES sobre inteligencia artificial, véase (("CONPES sobre Inteligencia Artificial estará listo en agosto de 2024": Alexander López, director de Planeación Nacional, 2024)

4.1 ¿Es jurídicamente posible implementar un sistema de IA con las características que se exigen en la convocatoria?

Sí, es posible crear una inteligencia artificial con estas características, ya que en los ordenamientos en donde pretende implementarse el sistema no existe prohibición expresa y por el contrario, como en el caso de la Unión Europea, existen leyes que permiten que sistemas de IA traten información sensible siempre que adopten las medidas de seguridad necesarias para su protección.

En materia de la regulación colombiana, si bien no existe una norma expresa que regule el uso de la IA en el manejo de datos médicos sensibles, según algunas circulares expedidas por el ministerio de salud es posible hacer uso de tecnologías de punta [7]para el tratamiento de datos médicos, siempre que se cumpla con ciertos criterios y principios generales, como los son los contenidos en la ley 1581 de 2012.

Incluso, por si aun existe duda, es posible desarrollar un sistema como el de VitalAI en Colombia, pese a no existir normativa expresa, por la aplicación del principio de legalidad el cual expone que a los individuos les es permitido hacer aquello que no esté expresamente prohibido por la ley[8].

4.2 ¿Qué tipo negocial permite desarrollar software? ¿Qué tipo negocial regulará el desarrollo del sistema de VitalAI?

El contrato que se celebrará será un contrato al que AllianceTech S.A.S ha denominado “Contrato de desarrollo de software, instalación y servicios post”. Este contrato atípico es una figura desarrollada por AllianceTech en la búsqueda de una solución que supla todas necesidades de la convocatoria.
En primer lugar, es importante destacar que esta figura recoge dos contratos atípicos frecuentes en materia de software, uno es el contrato de desarrollo de software y el otro es el contrato de soporte y mantenimiento de software. La intención de integrar ambos modelos contractuales en uno fue abarcar todas las etapas del proyecto en un solo contrato y desarrollar de forma completa la regulación que regirá toda la relación contractual entre AllianceTech y DataHealth.

4.2.1 ¿por qué elegimos este tipo contractual?

Como ya se anticipó, esta figura une dos tipos de contrato: i) el contrato de desarrollo de software y ii) el contrato de soporte y mantenimiento de software. El primero de estos contratos, el de desarrollo, es un contrato atípico que tiene por objeto obligar a una de las partes a la creación de un sistema de software a cambio, de que su contraparte, pague una contraprestación monetaria.

El contrato de desarrollo de software es un contrato que por su naturaleza implica una especie de la confección de un bien, en este caso la creación del sistema de VitalAI (obligación de resultado), mientras a su vez se arrienda un servicio inmaterial, que en este caso es el “arrendamiento del conocimiento” del equipo desarrollador para llevar a cabo la actividad de desarrollo y creación del sistema (obligación de medio)[9].

En materia doctrinal, existe discusión respecto de la contraposición de unir figuras que incluyan obligaciones de medio y de resultado, ya que, a la luz de la responsabilidad es necesario identificar si el responsable tiene a su una obligación de medio, es decir la de poner todos sus esfuerzos y

[7] La **tecnología de punta** hace referencia a toda tecnología que fue desarrollada muy recientemente y que es **de avanzada** (es decir, que supone un adelanto o algo innovador respecto a los **productos** ya existentes).
[8] Para una revisión más detallada del principio de legalidad en Colombia, véase (Corte constitucional, 2007)

diligencia en el desarrollo de una actividad sin importar el resultado, o una obligación de resultado, en donde se busca la obtención de un resultado en particular con independencia de los medios empleados[10].

En razón de lo anterior, será importante identificar, para efectos de determinar la responsabilidad del desarrollador en el marco del contrato, si estamos frente a un contrato con obligaciones de medio o de resultado. Ahora, bien, en materia de la regulación civil colombiana (art 2063 CC) se ha expuesto que el contrato que tiene por objeto la elaboración de una obra intelectual es un contrato de arrendamiento de servicios inmateriales, sin embargo, en este articulo también se hace una mención al art 2059 del código civil en donde se encuentra contenida la obligación de resultado por confección de obras (Monroy, 2012)**.**

Es decir, y replicando la idea de Juan Carlos Monroy, el contrato de desarrollo de software, que se celebrará en el marco de esta estrategia jurídica, es un contrato de obra inmaterial es un contrato de arrendamiento de servicios inmateriales que genera una obligación de resultado, por consiguiente, el desarrollador prestará un servicio inmaterial que debe garantizar un resultado. (Monroy, 2012)**.**

Ahora bien, teniendo una vez clara la naturaleza obligacional de este contrato, es importante hacer mención al momento en donde se entiende perfeccionado, ya que por la naturaleza de la actividad de desarrollo es necesario que se ejecute en distintos momentos en el tiempo, no obstante, el contrato se entiende perfeccionado una vez se culmine con la confección del sistema de software y se haga entrega de este al cliente. Es decir, el cumplimiento del contrato se profesa con respecto al último momento de desarrollo del sistema, el cual es la entrega.

Por otro lado, teniendo en cuenta la segunda figura contractual que compone el “contrato de desarrollo de software, instalación y mantenimiento”, debemos hablar del objeto y naturaleza jurídica del contrato de soporte y mantenimiento de software.

El contrato de mantenimiento y soporte de software es un contrato atípico que tiene por objeto la prestación de servicios por parte del desarrollador de software o una persona con autorización para realizar labores tendientes a garantizar el buen funcionamiento de programas informáticos de software a cambio de un precio.

Si bien, este contrato atípico y no requiere del cumplimiento de ninguna formalidad para su celebración, si es importante destacar que para el cumplimiento de la obligación que contiene es necesario que el encargado del mantenimiento cuente con la autorización para acceder al código fuente del software y poder realizar el mantenimiento. Sobre este punto retomaremos la discusión en el punto (4.5) cuando se establezca la titularidad del código (Contrato de soporte y mantenimiento de software, 2024).

Por lo anterior, la idea de integrar esta figura contractual en la estrategia jurídica es responder a la necesidad del cliente de contar con un servicio de mantenimiento periódico del sistema para garantizar en todo momento que cuente con estándares de calidad técnica y administrativa para el buen funcionamiento del software, y que además este servicio sea prestado por el mismo desarrollador del código.

[10] Desarrollo de software a medida: arrendamiento de servicios o contrato de obra. 10 de agosto de 2015. Metricson. https://metricson.com/desarrollo-de-software-a-medida-arrendamiento-de-servicios-o-contrato-de-obra/

En conclusión, con respecto a las razones por las que proponemos la celebración del contrato de desarrollo de software, instalación y mantenimiento, desea abarcarse toda la relación jurídica entre DataHealth y AllianceTech en un solo contrato que pueda contener dentro de su objeto ambos requerimientos hechos por el cliente (desarrollo y mantenimiento). Es por ello que, el objeto del contrato es el desarrollo, por parte de AllianceTech SA, del programa de software, la instalación y prestación de servicios de mantenimiento y actualización según las especificaciones técnicas del anexo técnico.

4.2.2 ¿qué figuras contractuales se descartaron para la regulación del desarrollo del sistema de VitalAI?

Durante el estudio de exigencias de la convocatoria, se analizaron otras figuras contractuales que podrían ser aplicadas al caso, y las cuales fueron descartadas por los motivos que expondremos a continuación:

- **Contrato de compraventa de licencia de Software:** Este tipo contractual tiene por objeto el otorgamiento del derecho de uso del sistema de software a cambio de una contraprestación monetaria única. En este contrato no se transfiere como tal el software sino el derecho de uso, razón por la cual no se satisface la pretensión del cliente de convertirse en titular del sistema y gozar de los derechos patrimoniales del código para su explotación (Velandia Rocha, 2018).
  Por otro lado, este tipo contractual solo tiene por objeto la transferencia del derecho de uso de un sistema de software ya existente, más no prevé la creación y desarrollo de un sistema que cumpla con los requerimientos que realice el cliente.
- **Contrato de compraventa efectiva de software (cesión de derechos del software):** Este es un negocio jurídico por medio del cual se transfieren los derechos patrimoniales de un sistema software a cambio de una contraprestación única de carácter económico. En principio, esta figura supone que el desarrollador (Titular original) ya no tendría obligación de mantenimiento del sistema para con el cesionario, por lo que si se desea adquirir esta obligación deberá celebrarse un contrato de prestación de servicios de mantenimiento. (Velandia Rocha, 2018).
  Si bien este contrato satisface en principio la pretensión de DataHealth de convertirse en titular del sistema, este contrato no contempla el desarrollo ni creación del software, sino que parte de la idea de la cesión de derechos de un sistema preexistente, razón por la cual resulta insuficiente para comprender las necesidades de la convocatoria.

4.2.3 Estructura del contrato.

El contrato se estructurará en 5 etapas de acuerdo con las etapas técnicas en las cuales se ejecutará todo el desarrollo del sistema. Las etapas son las siguientes: predesarrollo, desarrollo, entrega, práctica y seguimiento y por último servicios post.

La primera etapa comprende el alistamiento de servidores con el fin de garantizar el adecuado funcionamiento del proyecto, la arquitectura del código de software e Inteligencia Artificial, la indicación de la data necesaria para entrenar el sistema de VitalAI y la recolección de la información médica general. Esta etapa tiene una duración de tres (3) meses que se contarán a partir de la celebración del contrato.

Luego, está la fase de desarrollo. En esta etapa se obtendrán las autorizaciones para el tratamiento de datos sensibles y se hará la recolección de estos, con el fin de iniciar el entrenamiento del sistema cos los datos personales. La duración de esta etapa es de cinco (5) meses a partir de la finalización de la etapa de predesarrollo.

La tercera etapa comprende la de entrega de los derechos del software y de código fuente. Asimismo, en esta etapa se realizará lo correspondiente a realizar la instalación del sistema en los equipos de cómputo del cliente y se capacitará al personal encargado de utilizar dichos equipos y de manejar el sistema. Esta fase contará con una duración de (2) meses contados a parite de la aprobación de la etapa de desarrollo.

La penúltima etapa es la etapa de práctica y seguimiento. En esta etapa se llevará a cabo la verificación del funcionamiento del sistema. Esto se hará a través de pruebas exhaustivas y la supervisión a la implementación del sistema en los equipos de los licenciatarios. Tendrá un tiempo de dos (2) meses contados a partir de la entrega e instalación del código.

La quinta etapa comprende los servicios post. Estos son una multiplicidad de funciones que incluye el mantenimiento, la actualización y el soporte del sistema. Se realizará luego de la finalizar la etapa de práctica y seguimiento y se suspenderá cuando el encargante así lo decida por escrito.

4.3 ¿cómo obtendremos los datos sensibles?

Sobre este punto es necesario precisar que para poder tratar datos sensibles es necesario ser responsable o encargado del tratamiento de datos. Según la ley 1581 de 2012, será responsable del tratamiento aquella entidad que por sí misma decida sobre el tratamiento datos, y encargado de tratamiento será aquel sujeto que realiza tratamiento de datos personales por cuenta del responsable.

Teniendo en cuenta lo anterior, hay que poner de presente que DataHealth ni AllianceTech son responsables del tratamiento de datos, por lo que deberán suscribir un acuerdo de colaboración comercial con los hospitales y clínicas, responsables del tratamiento, para permitir que AllianceTech pueda usar los datos durante la etapa de desarrollo de VitalAI a titulo de encargado del tratamiento.

4.3.1 ¿Qué interés podrían llegar tener los responsables del tratamiento para suscribir el acuerdo de colaboración comercial con AllianceTech?

La respuesta a esto debe necesariamente referirse a una estrategia jurídica que se plantea, y es la suscripción de una carta de intención entre AllianceTech, DataHealth y los responsables de tratamiento, en donde conste un acuerdo para el otorgamiento futuro de una licencia del sistema de VitalAI para aquellos centros de salud que hayan permitido que el desarrollador del sistema tratara los datos sensibles durante la etapa de desarrollo de la IA.

Es decir, en esta carta de intención DataHealth acuerda otorgar una licencia del sistema de VitalAI, bajo la modalidad de no cobro de los servicios de mantenimiento durante 6 meses, a los responsables de tratamiento que hayan prestado el insumo de datos necesario para el entrenamiento de VitalAI. Con respecto a las implicaciones económicas que supone la implementación de esta carta de intención, se discutirán más adelante al tratar los problemas de carácter económico de la convocatoria.

En virtud de lo anterior, ya existe un sustento jurídico que justifique la celebración de un acuerdo de colaboración comercial entre AllianceTech y los responsables de datos, para que se permita el tratamiento de datos médicos durante la etapa de entrenamiento de VitalAI.

4.3.2 ¿qué deben hacerse para obtener la autorización de los titulares de la información sobre el tratamiento de sus datos?

Los datos personales están estrechamente relacionados con derechos fundamentales, por tal motivo, la celebración de un acuerdo de colaboración comercial no es suficiente para tener autorización legal para el tratamiento de esta información.

Para poder estar legitimado para el tratamiento de datos es necesario obtener la autorización de los titulares de la información sensible, en este caso, autorización de los pacientes. Dicho consentimiento pretende ser obtenido por medio de un aviso de privacidad en donde se informe al titular que AllianceTech estará encargado para el tratamiento de datos para el desarrollo de una inteligencia artificial llamada VitalAI, informar las funcionalidades que tendrá VitalAI, exponer los derechos que tienen como titulares de la información, exponer con qué mecanismos cuentan por si desean retirar su consentimiento[11].

Una vez hecho este aviso de privacidad, solo podrán recolectarse y tratarse los datos de los titulares que hayan dado su consentimiento de forma expresa para el tratamiento de su información en la etapa de desarrollo de VitalAI.

4.3.2.1 Consentimiento informado para el tratamiento de datos sensibles de menores:

Si es posible tratar datos personales de menores, siempre y cuando se cumplan con ciertos requerimientos normativos del GDPR y los pronunciamientos de la Corte Constitucional.

En primer lugar, respecto de lo que se expone en el GDPR se menciona que el tratamiento de datos personales de menores requiere de la existencia de un consentimiento emitido por el representante legal del menor, es decir, es válido el tratamiento en tanto el consentimiento lo emita un adulto que sea responsable legalmente por el menor[12].

Por otro lado, en materia de lo dicho por la Corte Constitucional en la sentencia C 748 de 2011, en donde la corte analiza un proyecto de ley estatutaria (No. 184 de 2010), por la cual se dictan disposiciones generales para la protección de datos personales, se expone que es posible realizar tratamiento de datos de menores de edad siempre que sea por razones de interés superior del menor o interés público.

Lo anterior, implica que es posible tratar datos personales de menores de edad, siempre que se propenda en la protección de su interés superior y se obtenga consentimiento expreso de su representante legal.

Sin embargo, aunque jurídicamente es posible tratar datos sensibles, durante la etapa de entrenamiento de VitalAI no se tratarán datos de menores, es decir, durante la etapa de desarrollo del sistema, el desarrollador no requiere tratar de forma obligatoria datos de menores para que el sistema pueda aprender y desarrollar las funciones que se exigen en la convocatoria.

Lo anterior no quiere decir que el sistema no vaya a poder tratar datos de menores o que los hospitales y clínicas no puedan usar el sistema en favor de proponer diagnósticos o tratamientos médicos a pacientes que sean menores de edad; lo que en realidad quiere decir es que, durante la etapa de creación de VitalAI, no existe un argumento que sustente el tratamiento de menores de edad por lo que no se utilizarán para fines técnicos de creación del proyecto, pero si podrán ser tratados para el disfrute de los beneficios que otorgue esta tecnología.

---

[11] Para una revisión más detallada sobre el aviso de seguridad en materia de tratamiento de datos sensibles, véase (Health Insurance Portabily and Accountability, 1996).

[12] Para una revisión más detallada sobre el tratamiento de datos personales de menores en el marco de la UE, véase (Reglamento general de protección de datos, 2016).

4.4 ¿cómo garantizaremos la protección de los datos sensibles?

Esta pregunta adquiere relevancia bajo el entendido de que se usaran datos sensibles durante el entrenamiento de la IA, ya que, para el tratamiento de datos personales, en los distintos ordenamientos jurídicos en los que pretende implementar el sistema de VitalAI, es necesario que se cumplan requisitos en materia de seguridad para garantizar la protección de la información medica sensible, los cuales expondremos a continuación:

A. **LEY HIPAA (Estados Unidos):** La ley HIPAA, o Ley de portabilidad y responsabilidad del seguro médico, es una ley federal estadounidense que tiene por objeto proteger la privacidad de la información médica de los pacientes y garantizar el acceso a dicha información solo a personal autorizado.
   Esta ley deben cumplirla los responsables de tratamiento de datos– a los que se les denomina "entidades cubiertas" – y demás agentes, que, en virtud de una relación jurídica con una entidad cubierta, tengan acceso a información de salud protegida – Los encargados de tratamiento, o colaboradores comerciales según la denominación de esta ley- (Health Insurance Portabily and Accountability, 1996).
   Además, es importante mencionar que esta norma se descompone en tres importantes componentes: i) reglas de privacidad, por las cuales se establecen límites en el uso y divulgación de la información al "mínimo necesario", y restringen el acceso a personal autorizado. ii) reglas de seguridad, por medio de las cuales se describen las medidas de protección técnicas, administrativas y físicas que se deben implementar para proteger la confidencialidad, integridad y disponibilidad de los datos que consten en medios electrónicos. y iii) reglas de incumplimiento, que regulan la definición del concepto de infracción e imponen obligaciones de información a los usuarios titulares de la información que haya sido vulnerada. (Cigna).

B. **REGLAMENTO GDPR (Unión Europea):** Este reglamento de la Unión Europea regula la protección de datos en general. En principio, se aplica a cualquier empresa que recolecte o trate datos personales de ciudadanos de la Unión Europea, a estos sujetos la norma los reconoce como responsables del tratamiento. Por otro lado, esta norma también es aplicable a los denominados "encargados" que son aquellos sujetos que tratan datos por cuenta de un responsable de tratamiento, y a los cuales se les exige que adopten las mismas medidas de seguridad y privacidad que se le exigen al responsable de tratamiento (Reglamento general de protección de datos, 2016).
   En los términos del presente reglamento se prohíbe, por regla general el tratamiento de datos sensibles, como es el caso de los datos médicos, salvo una serie de supuestos dentro de los cuales se resalta el consentimiento a fin de realizar el estudio de esta convocatoria.
   El objetivo que pretende satisfacer esta norma es fortalecer el derecho a la privacidad, transparencia, seguridad de los datos y exigir que se obtenga el consentimiento informado del usuario para el tratamiento de la información. Es decir, para el GDPR, al haber una predominancia del consentimiento del titular de la información para el manejo de sus datos personales, impone un deber de información al interesado sobre el tratamiento que se realiza sobre sus datos, indicando responsables y encargados, plazos, objetivos del tratamiento y derechos que lo cobijan.
   Ahora bien, en materia de seguridad esta disposición impone el cumplimiento de estándares técnicos y organizativos para la protección de los datos, algunos ejemplos son la seudonimización y cifrado de los datos, verificación y evaluación de medidas técnicas de protección que permitan el acceso y conservación de la integridad de la información,

implementación de planes de control de incidentes e informar a los usuarios sobre las infracciones de seguridad.

C. **LEY 1581 de 2012 (Colombia):** La ley 1581 de 2012 es la ley por medio de la cual se dictan disposiciones relativas a la protección de datos personales registrados en cualquier base de datos susceptible de tratamiento por parte de una entidad pública o privada en Colombia. La regulación colombiana, al igual que las regulaciones anteriormente expuestas, diferencia distintos roles que pueden desempeñar los sujetos en materia de tratamiento de datos; según esta disposición, será responsable del tratamiento aquella entidad que por sí misma decida sobre la base o tratamiento datos, y encargado de tratamiento será aquel sujeto que realiza tratamiento de datos personales por cuenta del responsable. (Ley 1281, 2012)
   Los principios que rigen a esta ley son principalmente la persecución de un fin legitimo en el tratamiento de datos, el tratamiento por consentimiento previo y expreso del titular, la protección de la integridad, veracidad y exactitud de la información, la limitación del acceso a la información solo a personal autorizado y la implementación de estándares técnicos, humanos y administrativos para asegurar las bases de datos y sus tratamientos.

Teniendo en cuenta estos tres grupos normativos, durante el proyecto pretende implementarse medidas de seguridad de carácter técnico que expone la ley, como el uso de contraseñas para que solo personal autorizado tenga acceso a la información, uso de sistemas de seguridad robustos que prevengan vulneración cibernética y encriptación de datos sensibles para evitar su infracción.

Asimismo, durante la etapa de desarrollo se pretende cumplir con requisitos de carácter administrativo como la capacitación del personal desarrollador sobre el acceso y uso de la información médica protegida que se usará para el entrenamiento de VitalAI, verificación de la existencia del consentimiento informado de los titulares de la información para el tratamiento de datos, implementación de planes de mitigación de riesgos e incidentes que puedan presentarse durante la etapa de desarrollo y nombramiento de auditores que revisen y lleven control sobre los usos de la información en la etapa de entrenamiento.

Y, por último, la utilización de estrategias de seguridad físicas como lo es asegurar las instalaciones en donde se encuentren los equipos de cómputo que contienen la información sensible con candados, contraseñas, etc.

4.5 ¿Quién tendrá titularidad de los derechos patrimoniales sobre el software y el código fuente?

Sobre este punto, en el análisis de las necesidades del cliente y las estrategias jurídicas aplicables, debemos tener en consideración tres puntos: i) derecho aplicable en materia de derechos sobre el sistema de software, ii) cesión de derechos patrimoniales del software y el código fuente y iii) el impacto de la cesión en materia de cumplimiento de otras obligaciones contractuales.

En cuanto al primer punto a considerar, es importante mencionar que, en el marco del desarrollo o creación de software, la regulación aplicable es la relativa a la protección de derechos de autor y el derecho de patente, para determinar la titularidad de los derechos que se deriven de él.

No obstante, en el análisis del caso en particular, debemos anticipar que no es posible aplicar la protección del software por vía de la patente, ya que distintos ordenamientos como el estadounidense, de la unión europea y de la comunidad andina han limitado la patentabilidad del

software para los casos en donde se demuestre que la invención es innovadora o nueva, es decir, que no se haya producido una tecnología como esta antes (OMC, 1994) (Sarmiento, 2016).

Por lo anterior, y según el tipo de estrategia técnica que pretende adoptarse para dar cumplimiento a la convocatoria, el tipo de tecnología que se implementará para la codificación, el procesamiento de datos y entrenamiento de la inteligencia artificial no constituyen nuevas invenciones, ni son propias de la empresa desarrolladora, por lo que no sería admisible aplicar la protección del software por vía de la patente.

Ahora bien, lo que sí es posible aplicar en el caso concreto es la regulación sobre derechos de autor, ya que autores como Ricardo Antequera, consideran que "*el lenguaje de programación debe ser considerado una obra literaria por tener una semántica y unas sintaxis preestablecidas".* Por otro lado, es necesario aplicar la protección del software por vía de derecho de autor ya que, por las limitaciones y restricciones que han impuesto los distintos ordenamientos para patentar el software, esta es la única vía que protege las invenciones de software que no son susceptibles de ser patentables, lo anterior, sin perjuicio de las discusiones doctrinales sobre la insuficiencia de la regulación en materia de protección del software. (Antequera & Gómez, 1999)

Dicho esto, y teniendo claro que la regulación aplicable es la relativa al derecho de autor, debe mencionarse que por vía de este se protegen dos clases de derechos, los morales y los patrimoniales. Los primeros de ellos, son los que "pretenden proteger un derecho personal referido esencialmente a la autoría de dicha producción." y son inalienables e intransferibles, y los segundos, los patrimoniales, son los buscan concretar "la explotación económica de la producción intelectual" y sobre los cuales si puede haber libre disposición. (Bernal & Conde, 2017)

Sobre los derechos patrimoniales, es donde se centra la discusión en materia del contrato que se pretenda celebrar entre DataHealth y AllianceTech, ya que, si bien es DataHealth encarga el desarrollo y creación del software, es AllianceTech quien efectivamente lo creará y quedará protegido por el derecho de autor, ya que en cabeza de DataHealth solo hay una idea (qué se quiere del sistema) y estas no son protegidas por el derecho.

Si bien, en un inicio el sistema de software está en cabeza de AllianceTech, por el derecho de autor, no hay ninguna intención por parte de la empresa en conservar alguno de los derechos patrimoniales que se derivan de la representación creada en virtud del contrato (el software). Por el contrario, AllianceTech pretende ceder la totalidad de los derechos patrimoniales a DataHealth, con la intención de satisfacer la intención de las partes – encomendar la creación de una obra a un agente especializado (el desarrollador), para posteriormente otorgar el uso y beneficio de la invención al encargante -.

Por lo anterior, como solución a esta problemática que nos pone de presente las regulaciones sobre derechos de autor, el desarrollador se compromete a incluir, dentro del "contrato de desarrollo de software, instalación y servicios post", una cláusula en donde se expone que una vez desarrollado el software (VitalAI), AllianceTech (desarrollador) se obliga a ceder la totalidad de los derechos patrimoniales, incluyendo en ellos los derechos sobre el código fuente.

No obstante, es importante mencionar que, si bien el desarrollador no pretende reservarse ningún derecho sobre el software o código fuente, si plantea la posibilidad de conservar la tenencia de una copia del código fuente, con la intención de poder prestar los servicios de mantenimiento,

actualización y soporte al sistema de VitalAI, que se pretende sean cubiertos por el desarrollador según lo expuesto en la convocatoria.

Lo anterior es así ya que, sin el acceso al código fuente original, o la copia de este, no sería posible, desde el punto de vista técnico, que el desarrollador pueda obligarse y dar cumplimiento a los servicios de mantenimiento, actualización y soporte del sistema de software de VitalAI. Aún con lo anterior, es importante resaltar que el titulo que ostentará AllianceTech sobre el código fuente es el de mero tenedor, por lo que DataHealth podrá en cualquier momento de la etapa de ejecución de servicios post pedir que le sea entregado el código fuente original o su copia.

4.6 ¿Qué mecanismos se incluirán dentro del contrato para proteger a DataHealth frente a riesgos?

En materia de este contrato son distintos los mecanismos que se implementarán para proteger a las partes de posibles riesgos durante la ejecución del contrato.

Primero, para proteger a ambas partes de posibles incumplimientos durante la ejecución de este contrato, se establecerá una cláusula que obligará a cada una a contratar un seguro de cumplimiento. De esta manera, en caso de incumplimiento, cualquier parte podrá solicitar a la aseguradora la indemnización correspondiente.

En segundo lugar, AllianceTech se compromete a suscribir una póliza de seguro de responsabilidad civil que cubra los daños y perjuicios que puedan sufrir terceros como consecuencia de una brecha de seguridad en los datos personales causada por el sistema de inteligencia artificial durante la etapa de desarrollo.

En tercer lugar, dentro del contrato de desarrollo, se implementará una cláusula de indemnidad en donde DataHealth tendrá derecho a ser indemnizada por AllianceTech durante un año por cualquier gasto generado debido a responsabilidades administrativas derivadas del uso del sistema VitalAI, en caso de que este presente defectos o no funcione correctamente.

4.7 ¿cómo aplicará la ley de protección al consumidor en el marco del contrato de desarrollo de software, instalación y servicios post?

Durante el desarrollo del contrato desarrollo de software, instalación y servicios post, se implementarán dos cláusulas en donde se expongan las garantías de buen funcionamiento y garantía por producto defectuoso.

Con respecto a la primera, AllianceTech se compromete a garantizar el correcto funcionamiento del sistema VitalAI durante un año a partir de su instalación en los equipos de cómputo de DataHealth. Esta garantía protege directamente a DataHealth de cualquier falla del sistema. En caso de que los hospitales o clínicas que adquieran el sistema a través de DataHealth experimenten problemas, AllianceTech será responsable de indemnizar a DataHealth por cualquier gasto o pérdida que esta última deba afrontar debido a dichos problemas. Es importante destacar que la garantía se inicia al momento de la instalación en DataHealth y no se ve afectada por las adquisiciones posteriores de otros centros de salud.

AllianceTech garantiza que el sistema VitalAI instalado en las instalaciones de DataHealth se encuentra libre de defectos de fabricación. Esta garantía, válida por un año a partir de la instalación, protege a DataHealth de cualquier problema originado por defectos congénitos del sistema. En caso de detectarse un defecto de este tipo, AllianceTech se compromete a indemnizar a DataHealth por cualquier gasto o pérdida resultante, además de obligarse a corregir dichos defectos del sistema de forma gratuita.

4.8 Ley aplicable y Jurisdicción aplicable al contrato de desarrollo de software.

El presente contrato estará sujeto a la legislación colombiana, pero incorporará los rigurosos estándares de seguridad del GDPR y la AI Act. Esta elección nos permitirá cumplir con las regulaciones más exigentes a nivel mundial y facilitar la implementación del sistema en otros países. La jurisdicción para resolver cualquier controversia será la de los tribunales de Bogotá, Colombia.

Mecanismos de resolución de controversias en el marco del contrato de desarrollo de software, instalación y servicios post.

En materia de este contrato cualquier controversia, disputa o reclamación que surja del presente contrato, o en relación con el mismo, incluyendo su formación, validez, interpretación, cumplimiento o terminación, será sometida a arbitraje técnico, en el centro de Arbitraje y Conciliación de la ciudad de Bogotá, de acuerdo con las siguientes reglas:

i) El Tribunal estará integrado por 3 árbitros.
ii) Cada una de las partes designará un árbitro, que se encuentre dentro de la lista de árbitros, y los dos árbitros así designados nombrarán un tercer árbitro que actuará como presidente del tribunal. En caso de desacuerdo con la designación, será designado por el Centro de Arbitraje y Conciliación de la Cámara de Comercio de Bogotá.
iii) El procedimiento se sujetará a los reglamentos que para tal fin disponga el mencionado Centro de Arbitraje y se aplicarán de conformidad con los criterios que en ellos se establezcan.
iv) El Tribunal decidirá en derecho.
v) Todos los árbitros deberán poseer conocimientos y experiencia en desarrollo de software, ingeniería de software y protección de datos personales.

4.9 ¿Qué modelo de licencia sería el más adecuado para DataHealth, considerando que se trata de un software médico destinado a ser utilizado por hospitales y clínicas?

Recomendamos a DataHealth Solutions S.A la implementación de este modelo de licenciamiento de tipo cerrado o de propietario, ya que este permite al licenciante (DataHealth Solutions S.A.) distribuir el sistema sin necesidad de dar acceso al código fuente, lo cual resulta útil en materia de protección de la información sensible.

Por otro lado, se recomienda al licenciante este modelo de contrato de licencia por cuanto puede restringir el acceso y numero de distribuciones que se realizan del sistema, permitiendo así que DataHealth lleve un control sobre los usos del sistema y pueda garantizar el cumplimiento de los estándares de seguridad que imponen las regulaciones.

Asimismo, por medio de este tipo de licencia se genera la obligación, en cabeza de DataHealth, de capacitar al licenciatario sobre el uso y funcionamiento del sistema, lo que permite que haya mayor cumplimiento de los estándares de protección de las regulaciones aplicables.

4.9.1 ¿Qué otros modelos de licencia se evaluaron y posteriormente se descartaron?

En el presente caso se estudiaron únicamente tres grupos de licencias de uso de software, las de código abierto, las de código cerrado y las mixtas, sobre las cuáles elegimos la licencia de código cerrado o propietarias que se diferencian entre sí por la manera en que se usan, modifican y distribuyen.

Licencia de código abierto: en este tipo de software el licenciante le da al licenciatario el código fuente, de manera que el licenciatario puede enajenar el software como lo crea conveniente, además que no requiere el pago de derechos de autor o tasas por su venta. Por lo anterior, consideramos que no es adecuado implementar este modelo de licencia ya que lo que se pretende es proteger los derechos patrimoniales de DataHealth Solutions S.A. como propietario de VitalAI.

Y no solo eso, sino que se debe tener en cuenta que, al estarse tratando datos sensibles, la protección y rigurosidad en materia de control del código es mayor, ya que cualquier vulneración a este puede implicar que haya una infracción o vulneración de datos sensibles, exponiendo la seguridad de la información médica de pacientes, y exponiendo a DataHealth a responsabilidad civil extracontractual y administrativa por el incumplimiento de los estándares de protección y seguridad de los datos de los cuales es responsable (Brocca & Casamiquela, 2005).

Licencia mixta: esta modalidad de licenciamiento tiene elementos propios de las licencias de código abierto y las licencias de código cerrado o propietarias. En estas se permite el acceso al código fuente, pero establecen condiciones o restricciones para su uso y distribución. Sobre estas licencias seguimos la misma línea de argumentación que nos llevó a descartar las licencias de código abierto, ya que no resulta prudente la distribución del código fuente a los centros hospitalarios, sino únicamente su uso. (Brocca & Casamiquela, 2005).

4.10 ¿Qué mecanismos se incluirán dentro del contrato de licencia para proteger a los licenciatarios?

En cumplimiento con la normativa de protección al consumidor, este contrato establecerá garantías específicas para clínicas y hospitales, asegurando la calidad y el buen funcionamiento del sistema VitalAI. Ambas garantías tendrán la vigencia de un año contado a partir de la instalación del sistema. No obstante, durante el primer año posterior a la entrega del sistema por parte de AllianceTech, se establecerá una cláusula de indemnidad mediante la cual AllianceTech asumirá la responsabilidad por cualquier defecto o mal funcionamiento del sistema.

Asimismo, con el propósito de reforzar las garantías contractuales, se sugiere a DataHealth la contratación de una póliza de seguro que cubra los riesgos asociados a la filtración de datos médicos confidenciales.

5. PROBLEMAS ECÓNOMICOS:

5.1 variación en los precios del contrato según la elección del tipo de servidores que se utilizarán.

AllianceTech ofrece a DataHealth dos alternativas para gestionar sus servidores: servidores físicos propios o servidores en la nube de Amazon Web Services AWS. La opción de servidores físicos, con un costo inicial de $234.977 (IVA incluido), brinda un mayor control sobre el hardware. Sin embargo, la solución de servidores en la nube de AWS, aunque con un costo inicial más elevado de $765.027 (IVA incluido), ofrece mayor escalabilidad y flexibilidad.

El almacenamiento local destaca por su velocidad en el acceso a archivos grandes, especialmente en aplicaciones tradicionales, y ofrece un mayor control sobre los datos. Sin embargo, requiere una inversión inicial y mantenimiento continuo. Por su parte, la nube proporciona escalabilidad, alta disponibilidad y seguridad, gracias a la gestión especializada de proveedores. Aunque su costo inicial puede ser superior, elimina la necesidad de una infraestructura física y permite el acceso a los datos desde cualquier lugar con conexión a internet, reduciendo así el consumo energético y la huella de carbono.

5.2 ¿Cuál será el cronograma de pago según el contrato de desarrollo?:

En relación con esta cuestión, la estrategia jurídica planteada propone establecer una estructura de precios por etapas, donde la cuantificación de cada monto se basará en factores como los recursos necesarios para cada fase del proyecto, los costos operativos asociados y el margen de beneficio de la empresa desarrolladora. Por lo anterior, y teniendo en cuenta que los costos de los insumos en cada etapa del proyecto son variables según la elección de la alternativa anterior, el cronograma de pago para el contrato de desarrollo de software, instalación y servicios post será el siguiente:

- **Pre-desarrollo:**
  - ALTERNATIVA A: (valor: $149.855 USD) el pago debe hacerse en la fecha de celebración del contrato.
  - ALTERNATIVA B: (valor: $ 559,577 USD) el pago debe hacerse en la fecha de celebración del contrato.

- Desarrollo:
  - ALTERNATIVA A: (Valor: $ 249,872 USD) el pago debe realizar dentro de los 10 días siguientes a la finalización de la etapa de pre-desarrollo.
  - ALTERNATIVA B: (Valor: $370.200 USD) el pago debe realizar dentro de los 10 días siguientes a la finalización de la etapa de pre-desarrollo.

- Entrega:
  - ALTERNATIVA A; (Valor: $175,273 USD) el pago debe realizar dentro de los 10 días siguientes a la finalización de la etapa de desarrollo.
  - ALTERNATIVA B: (Valor: $390.223 USD) el pago debe realizar dentro de los 10 días siguientes a la finalización de la etapa de desarrollo.

- Práctica y seguimiento: (No tiene costo).

- Servicios Post:
  - Instalación del sistema a los licenciatarios de DataHealth: 1950 USD por cada sistema instalado (este será un único pago que se hará al momento de celebrar el contrato de licencia al desarrollador).
  - Mantenimiento, actualización y soporte: 1322 USD por sistema que se instale. (este precio deberá ser pagado de forma mensual por DataHealth a AllianceTech, por lo que se recomienda que se incluya este valor al valor de la licencia).

5.3 Licencia de fundadores.

Como se mencionó previamente, los centros hospitalarios que formalicen la carta de intención y posteriormente suscriban el acuerdo de colaboración comercial para el procesamiento de datos durante el entrenamiento del sistema, se beneficiarán de las siguientes exenciones:

Instalación gratuita del sistema: No se cobrará el costo de instalación del sistema.

Mantenimiento gratuito por 6 meses: Durante los primeros seis meses posteriores a la instalación, no se aplicará ningún cargo por los servicios de mantenimiento.

Ahorro total: Este beneficio representa un ahorro total de USD 9.885. Pasado este período de seis meses, los centros hospitalarios deberán asumir los costos habituales de los servicios postventa."

Bibliografía

"CONPES sobre Inteligencia Artificial estará listo en agosto de 2024": Alexander López, director de Planeación Nacional. (18 de abril de 2024). *Departamento Nacional de Desarrollo*, págs. https://www.dnp.gov.co/Prensa_/Noticias/Paginas/conpes-sobre-IA-estara-listo-en-agosto-de-2024.aspx.

Antequera, R., & Gómez, G. (1999). *Legislación sobre derecho de Autor y Derechos Conexos.* Caracas: editorial juridica venezolana.

Bernal, D., & Conde, C. (2017). *Los derechos morales de autor como derechos fundamentales en Colombia.* Bogotá: Externado.

Brocca, J. C., & Casamiquela, R. (2005). *LAS LICENCIAS DE SOFTWARE DESDE LA PERSPECTIVA DEL USUARIO FINAL.* Revista Pilquen.

Cigna, H. (s.f.). *HIPAA Compliance and Transaction Standards.* Estados Unidos.

Contrato de soporte y mantenimiento de software. (2024). España.

Corte constitucional, C. (2007). *Sentencia C-782 de 2007.*

Health Insurance Portabily and Accountability. (1996). estados unidos: ley federal.

LCIA Arbitration. (2020). Londrés: https://www.lcia.org/Dispute_Resolution_Services/LCIA_Arbitration.aspx.

Ley 1281. (2012). No. 48587.

Ley de Inteligencia Artificial. (2023). Unión Europea: Parlamento Europeo.

Monroy, J. C. (2012). *Cuestiones Jurídica en torno a los contratos de desarrollo y licencia de software.* Externado.

OMC. (1994). *Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio.*

Reglamento general de protección de datos. (2016). Unión Europea.

Sarmiento, C. (2016). *La protección del software desde la Propiedad Intelectual en Colombia: Conveniencia de la creación de una normativa especial que garantice los derechos de los desarrolladores.* Bogotá: Departamento de Propiedad Intelectual, Externado. .

Velandia Rocha, C. (2018). *Anotaciones a la compraventa de software.* colombia: Asuntos Legales.

TÉRMINOS DE REFERENCIA

CONVOCATORIA PARA LA SELECCIÓN Y CONTRATACIÓN DE PROVEEDOR

Versión 1.0

1. INTRODUCCIÓN

1.1. Antecedentes

DataHealth Solutions S.A., en adelante “la Empresa”, es una sociedad colombiana que se ha destacado en el sector de la tecnología de la salud. Fundada hace una década, la empresa ha crecido significativamente, enfocándose en el desarrollo de soluciones tecnológicas innovadoras para los desafíos del sector salud. La misión de DataHealth es mejorar la calidad de vida de las personas a través del uso de la tecnología, especialmente en áreas donde el diagnóstico y tratamiento de enfermedades pueden beneficiarse significativamente del análisis de datos y la inteligencia artificial.

En ejercicio de sus funciones y para el desarrollo de estas, la Empresa se encuentra interesada en contratar el servicio a adquirir un sistema avanzado basado en inteligencia artificial (IA) para el análisis y tratamiento en el sector salud. Dicho servicio se denominará “VitalAI” y deberá utilizar algoritmos de aprendizaje automático para interpretar grandes conjuntos de datos médicos, incluyendo pruebas genéticas, imágenes diagnósticas y registros electrónicos de salud. Su propósito deberá ser ofrecer diagnósticos precisos y planes de tratamiento personalizados, mejorando así la eficacia de los tratamientos médicos. Además, debe estar diseñado para integrarse con infraestructuras de salud existentes y adaptarse a diferentes regulaciones y estándares de privacidad en distintos países. Su implementación incluye varias fases, desde el licenciamiento del software hasta la prestación de servicios profesionales para la implementación y mantenimiento del sistema.

Para lo anterior, es necesario adelantar el presente proceso mediante el cual se seleccionará el proveedor que prestará el servicio y/o suministrará el(los) bien(es) anteriormente descrito(s).

1.2. Justificación de la convocatoria

La justificación para la convocatoria realizada por DataHealth para contratar una empresa especializada se basa en varios factores:

1. **Complejidad técnica y especialización.** El desarrollo e implementación de VitalAI requieren un alto grado de especialización en IA, análisis de datos y tecnologías de salud. DataHealth busca una empresa con la experiencia y el conocimiento técnico necesarios para manejar estas complejidades.

2. **Integración y cumplimiento regulatorio.** Dada la naturaleza del servicio, es crucial que la implementación de VitalAI cumpla con diversos estándares o regulaciones internacionales de salud, consentimiento informado, protección de datos, protección al consumidor, entre otras. Una empresa especializada podría ofrecer la experiencia necesaria para navegar estos aspectos legales y regulatorios.

3. **Eficiencia y eficacia.** Al externalizar estos servicios, DataHealth busca garantizar la eficiencia y eficacia en la implementación de VitalAI, aprovechando la experiencia y los recursos de una empresa dedicada a estos tipos de proyectos.

4. **Enfoque en el núcleo del negocio.** Esta contratación permitirá a DataHealth concentrarse en su núcleo de negocio y estrategia de expansión, mientras delega los aspectos técnicos y operativos a un proveedor especializado.

Este enfoque estratégico busca asegurar el éxito en la implementación y operación de VitalAI, maximizando su potencial para transformar el sector salud.

1.3. Definiciones

Para efectos de los presentes términos de referencia, se adoptan las siguientes definiciones:

a) VitalAI: sistema de inteligencia artificial desarrollado por DataHealth Solutions, destinado al análisis y tratamiento en el sector salud, utilizando algoritmos de aprendizaje automático para interpretar datos médicos.

b) Implementación: proceso de integración y puesta en funcionamiento de VitalAI en infraestructuras de salud, incluyendo instalación, configuración y personalización del sistema.
c) Licenciamiento de software: acuerdo legal mediante el cual DataHealth otorga derechos de uso de VitalAI a hospitales y clínicas bajo términos específicos.
d) Servicios profesionales: asistencia técnica y consultoría proporcionada por la empresa contratada, incluyendo capacitación, mantenimiento y soporte de VitalAI.
e) Cumplimiento regulatorio: alineación y adhesión de VitalAI a las normativas de salud, protección de datos, entre otras aplicables en cada jurisdicción donde se implementará.

2. OBJETO DE LA CONVOCATORIA

2.1. Objeto de la convocatoria

La presente convocatoria tiene como objeto la selección y contratación de un proveedor para el desarrollo, implementación, mantenimiento y soporte del sistema de inteligencia artificial 'VitalAI', diseñado para el análisis y tratamiento en el sector salud. Esto incluye la adaptación y personalización del sistema a diferentes entornos y normativas de salud, la integración eficiente con infraestructuras tecnológicas de hospitales y clínicas, y la capacitación del personal en su uso. Además, el proveedor deberá asegurar el cumplimiento de todas las regulaciones relevantes, así como proporcionar un soporte técnico continuo y eficiente para el sistema.

2.2. Descripción del bien o servicio a contratar

El objeto del contrato que eventualmente resulte de la presente convocatoria será:

1. **Desarrollo y Personalización de VitalAI:**

   • Adaptar y personalizar VitalAI a las necesidades específicas de cada institución de salud, incluyendo hospitales y clínicas en Colombia y potencialmente en mercados internacionales.

2. **Integración con Infraestructuras de Salud:**

   • Asegurar la integración eficiente de VitalAI con las infraestructuras tecnológicas existentes en los entornos de salud, incluyendo sistemas de registro médico electrónico y bases de datos de pacientes.

3. **Cumplimiento de Normativas de Salud y Protección de Datos:**

- Garantizar que VitalAI cumpla con todas las regulaciones de salud y protección de datos aplicables, tanto a nivel nacional como internacional.

4. **Capacitación y Soporte Técnico:**
   - Proporcionar capacitación exhaustiva al personal de salud en el uso de VitalAI y ofrecer soporte técnico continuo y eficiente.
5. **Mantenimiento y actualizaciones:**
   - Realizar el mantenimiento regular del sistema y proporcionar actualizaciones necesarias para asegurar su funcionamiento óptimo y la incorporación de avances tecnológicos.
6. **Evaluación de impacto y mejora continua:**
   - Realizar evaluaciones periódicas del impacto de VitalAI en los procesos de atención médica y proponer mejoras basadas en los resultados y feedback de los usuarios.
7. **Gestión de riesgos y responsabilidades:**
   - Identificar y mitigar posibles riesgos asociados con la implementación y uso de VitalAI, incluyendo responsabilidades legales y técnicas.

Este contrato busca establecer una colaboración efectiva y de largo plazo que permita la implementación exitosa de una solución tecnológica innovadora en el campo de la salud, con el objetivo de mejorar la calidad y eficiencia de la atención médica.

2.3. Especificaciones técnicas generales

2.3.1 Especificaciones Técnicas y Operativas de VitalAI:

a) Arquitectura de Inteligencia Artificial y Aprendizaje Automático:

- Uso de algoritmos de IA de última generación capaces de procesar y analizar datos médicos complejos.
- Implementación de técnicas de aprendizaje profundo y aprendizaje supervisado para mejorar continuamente la precisión y eficacia del diagnóstico.
- Capacidad de adaptarse y aprender de nuevos conjuntos de datos y últimas investigaciones médicas.

b) Integración con Sistemas de Información Hospitalaria:

- Capacidad para integrarse sin problemas con una variedad de sistemas de información hospitalaria (HIS) y registros médicos electrónicos (EMR).
- Adaptabilidad para trabajar con diferentes formatos de datos y estándares de interoperabilidad como HL7, FHIR, y DICOM.
- Herramientas de migración de datos y mapeo para garantizar una transición fluida y precisa de los sistemas existentes a VitalAI.

c) Seguridad de Datos y Conformidad Regulatoria:

- Uso de encriptación de datos de nivel empresarial para proteger la información de los pacientes.
- Mecanismos de autenticación robustos para controlar el acceso a datos sensibles.
- Protocolos de cumplimiento para adherirse a leyes de privacidad de datos como HIPAA en EE. UU., GDPR en Europa, y normativas locales relevantes.

2.3.2 Especificaciones de Interfaz de Usuario y Experiencia del Usuario

a) Diseño Intuitivo:

- Interfaz gráfica diseñada para ser intuitiva y fácil de usar para personal médico con diversos grados de competencia tecnológica.
- Visualización de datos clínicos y herramientas analíticas para una interpretación clara y efectiva.
- Opciones de personalización para ajustar la interfaz según las preferencias del usuario y necesidades específicas.

b) Soporte y Mantenimiento:

- Servicio de soporte técnico disponible 24/7 para resolver cualquier problema operativo o técnico.
- Plan de mantenimiento regular para asegurar la actualización constante del sistema y su adaptación a las últimas tecnologías y descubrimientos médicos.

- Estrategia proactiva para la gestión de incidencias, minimizando el tiempo de inactividad y garantizando una operación eficiente.

2.3.3 Otros

a) Capacitación y Recursos Educativos:

- Programas detallados de formación para usuarios, incluyendo médicos y personal administrativo, con módulos adaptados a distintos niveles de habilidad.
- Recursos educativos variados, como manuales de usuario, tutoriales en video, y sesiones de capacitación en línea y presenciales.
- Soporte continuo para la educación y el desarrollo de habilidades relacionadas con el uso de VitalAI.

b) Escalabilidad y Adaptabilidad del Sistema:

- Diseño modular y escalable para acomodar el crecimiento en la cantidad de usuarios y el volumen de datos.
- Flexibilidad para integrar nuevas funcionalidades y adaptaciones específicas para diferentes instituciones de salud y requisitos regionales.

c) Personalización y Configuración:

- Opciones de personalización extensas para adaptar VitalAI a los requisitos específicos de cada entorno de salud.
- Herramientas y configuraciones para ajustar algoritmos y funcionalidades según las necesidades y preferencias de los usuarios.

d) Soporte Multilingüe y Localización:

- Capacidad para operar en múltiples idiomas, ofreciendo una localización completa para usuarios en diferentes regiones geográficas.
- Soporte técnico y de usuario en los idiomas locales de los principales mercados de operación.

e) Interoperabilidad y Actualizaciones Tecnológicas:

- Capacidad para interactuar con sistemas y tecnologías emergentes en el campo de la salud digital.
- Actualizaciones continuas para mantener el sistema al día con los últimos avances en IA y medicina.

2.4. Componentes del trabajo a contratar

N	Servicios requeridos	Descripción
2.1	Viabilidad jurídica y técnica.	Viabilidad técnica y legal de la implementación de VitalAI, incluyendo análisis de cumplimiento normativo y recomendaciones de estructuras contractuales.
2.2	Integración y personalización	Descripción la integración de VitalAI con sistemas existentes y las personalizaciones realizadas para cada entorno de salud.
2.4	Seguridad y privacidad de datos	Medidas de seguridad y privacidad de datos implementadas, incluyendo pruebas de cumplimiento con los estándares internacionales relevantes.
2.5	Estrategia de mantenimiento y soporte	Estrategia de mantenimiento y soporte, incluyendo cronogramas de actualizaciones y detalles de soporte técnico.
2.6	Desarrollo de VitalAI	Desarrollo de VitalAI para pruebas y revisiones iterativas.
2.7	Implementación y Puesta en Marcha	Expectativa de implementación completa, los resultados de la puesta en marcha y las recomendaciones para operaciones futuras.

Nota: DataHealth está abierta a cualquier tipo contractual o de estrucutración jurídica y tecnológica, siempre y cuando sea eficiente para alcanzar sus logros.

3. CONDICIONES COMERCIALES

3.1. Presentación de la propuesta

La propuesta siempre debe estar precedida del ANEXO No. 1 de los presentes términos de referencia, denominado “Carta de Presentación de Propuesta”.

El formulario de precios y cantidades o ítems no podrá ser modificado, por lo tanto, no se podrá variar de ninguna forma la descripción, actividad, especificación técnica, cantidad, unidad de medida, etc., o suprimir, adicionar, complementar o incluir descripciones, actividades, especificaciones técnicas, cantidades, unidades de medida, etc., diferentes a las indicadas en el anexo correspondiente. Cualquier variación del formulario de precios y cantidades o ítems dará lugar al rechazo de la propuesta, siempre que sea susceptible de aclarar o recibida la aclaración la misma no sea de recibo para el Comité Evaluador. En todo caso, posterior a la entrega, la oferta económica no podrá modificarse en el sentido de complementarse o mejorarse frente a lo presentado inicialmente.

Cualquier nota, condición o criterio adicional incluido en la oferta económica o formulario de precios y cantidades o ítems se tendrá por no escrita.

Si el proponente al elaborar su propuesta encuentra discrepancias, inconsistencias u omisiones en los presentes términos de referencia y sus anexos, o tiene dudas sobre ellos, deberá solicitar por escrito al correo señalado en los términos de referencia, las aclaraciones necesarias, dentro del plazo establecido en el mismo cronograma.

La propuesta estará conformada por la oferta técnica y económica, así como por todos los documentos que soporten la acreditación de los requisitos exigidos en el presente proceso de selección, incluidos catálogos, fichas técnicas, muestras (si aplica), entre otros. La totalidad de la propuesta y sus anexos deberá presentarse por medio electrónico, acompañada de la carta de presentación de la oferta, debidamente suscrita por el representante legal o apoderado del proponente.

3.2. Información y documentos para incluir en la propuesta

- **Descripción de la compañía:** Este ítem hace referencia a la descripción del objeto social de la compañía y una descripción detallada de los productos, servicios y mercados atendidos por la misma.

- **Experiencia específica en el objeto de la futura contratación:** Descripción de la trayectoria de la compañía, años de experiencia y sectores o industrias en donde ha prestado los servicios de desarrollo e implementación de sistemas de inteligencia artificial y aprendizaje automático en el sector de la salud. Esto debe incluir una descripción detallada de proyectos previos relacionados con la integración de tecnología de IA en entornos de salud, incluyendo, pero no limitándose a, sistemas de registro

médico electrónico, diagnóstico asistido por IA, análisis de datos de salud y personalización de tratamientos médicos. Se valorará especialmente la experiencia en proyectos que involucren la manipulación y análisis de datos médicos sensibles, cumplimiento de normativas de protección de datos y experiencia en la implementación de soluciones en entornos de *cloud computing* y seguridad cibernética en el ámbito de la salud.

- **Definición de compradores y usuarios:** Esta subsección debe clarificar quiénes son los compradores (hospitales, clínicas) y los usuarios finales (personal médico, pacientes), destacando las implicaciones legales para cada uno.

- **Funcionalidades de VitalAI y tipología de servicio:** Debe describirse en detalle las funcionalidades de la plataforma, permitiendo entender cómo se utiliza en diferentes contextos y cuáles son las regulaciones aplicables en cada jurisdicción.

- ***Proof of work*:** Con el fin de analizar la calidad del trabajo del Proponente, la Empresa le solicita que realice lo descrito a continuación como una *Proof of work* (la "Prueba de Trabajo"), es decir, que realice las actividades sin costo para la Empresa y como parte de su propuesta de honorarios. En consecuencia, solicitamos a los Proponentes cumplir con las siguientes actividades en las fechas establecidas en el cronograma adjunto a este documento (el Cronograma):

    I. **Memorando de viabilidad técnica y legal:** desarrollo de un informe exhaustivo que evalúe la factibilidad técnica y legal de la implementación de VitalAI. Este memorando debe incluir análisis detallados sobre:
        Conformidad con regulaciones de salud, protección de datos, entre otras relevantes.
        Evaluación de riesgos técnicos y legales.
        Recomendaciones preliminares para la mitigación de riesgos.
        El memorando debe ser presentado en un formato claro y estructurado, facilitando su revisión por parte de los directivos de DataHealth.

    II. **Plan de implementación detallado:** elaboración de un documento completo que describa el plan de implementación de VitalAI, incluyendo:
        Fases del proyecto con cronogramas detallados e hitos clave.
        Estrategias para la integración con sistemas existentes en entornos de salud.
        Recursos necesarios, incluyendo personal, tecnología y logística.
        Este plan debe demostrar la capacidad del proveedor para gestionar proyectos complejos y garantizar una transición fluida y efectiva.

    III. Informe de seguridad y privacidad de datos:

Elaboración de un informe que detalle:
Medidas de seguridad implementadas para la protección de datos.
Procesos de cumplimiento con las normativas de privacidad y protección de datos.
Planes de respuesta ante incidentes de seguridad

IV. **Licenciamiento de Software:** los proponentes deben presentar un plan detallado sobre el tipo de licenciamiento propuesto para VitalAI. Deben considerar si es más adecuado un modelo de licencia perpetua, una suscripción o un enfoque híbrido. Este plan debe basarse en:
Las necesidades y expectativas de los hospitales y clínicas.
Los beneficios y limitaciones de cada modelo de licenciamiento.
Cómo cada opción afectaría la escalabilidad y la actualización del sistema.

V. **Suscripción y Mantenimiento:** es necesario un análisis exhaustivo de cómo se manejarán la suscripción y el mantenimiento de VitalAI. Esto incluye:
Detalles sobre cómo se realizarán y gestionarán las actualizaciones del sistema.
Planes para el soporte técnico y la asistencia continua.
Estrategias para garantizar la eficiencia operativa y la resolución rápida de problemas.

- **Recursos físicos y logísticos a utilizar:** descripción de los recursos físicos y logísticos utilizados para soportar el desarrollo del objeto del futuro contrato.

- **Valor agregado:** indicar el valor agregado que brinda el oferente que supera el alcance del proceso de selección y en general las necesidades de la Empresa. Este se refiere a otros servicios que ofrece dentro de su propuesta, sin costo adicional (esto es opcional para el proponente).

- **Oferta económica:** Descripción económica del servicio o bien objeto de esta convocatoria, conforme a lo exigido en los presentes términos de referencia y anexos o formatos, estos últimos, en el evento en que se haya dispuesto de los mismos para la presente contratación.

3.3. Declaraciones

Con la presentación de la oferta, el proponente declara que:

a) No se encuentra en proceso de liquidación.

b) No figura reportada la empresa ni sus representantes legales en ninguna lista restrictiva.
c) No esta incurso en ninguno conflicto de interés con la Empresa.
d) Es propietario o tiene las autorizaciones requeridas sobre los bienes de propiedad intelectual contenidos en la propuesta.
e) Autoriza expresamente a la Empresa para consultar la información, los anexos y soportes que haya suministrado con ocasión de esta convocatoria para constatar la transparencia y licitud de sus actividades
f) Toda la información que ha entregado o suministrado a la Empresa es verdadera, y posee todos los comprobantes y documentos necesarios para demostrar su veracidad g) Cuenta con la autorización de todos los participantes del equipo de la empresa para el tratamiento de sus datos personales por parte de la Empresa.

3.4. Validez de la propuesta

La propuesta deberá tener una validez como mínimo de noventa (90) días contados a partir del momento de su recepción por parte de la Empresa.

3.5 Oferta económica

Las ofertas deberán presentarse sin errores que afecten cantidades, valores, entre otros. Antes de preparar la propuesta, lea los términos de referencia. Esto evitará errores que impidan tener en cuenta su propuesta en el estudio, evaluación y adjudicación.

Los valores consignados en la propuesta se mantendrán vigentes durante el proceso de convocatoria y selección, y durante todo el término de ejecución del contrato.

Serán de exclusiva responsabilidad del proponente los errores u omisiones en que incurra al indicar los valores totales en la propuesta, debiendo asumir los mayores costos y/o perdidas que se deriven de dichos errores u omisiones.

Para preparar su oferta económica, tenga en cuenta los siguientes aspectos:

- Todos los aspectos deben presentarse discriminados y por cada una de las alternativas propuestas. El IVA debe indicarse por separado, aclarando la tarifa de IVA y en caso de que el ítem no sea sujeto de IVA, hacer dicha observación.
- Cada concepto incluido en la oferta económica debe presentarse en dólares estadounidenses (USD).
- Los precios ofrecidos en esta propuesta deberán incluir todos los descuentos que el proveedor esté en capacidad de ofrecer.

- El proponente será responsable de los errores u omisiones en que incurra en la presentación de los precios relacionados en la oferta económica.
- Todos los costos, gastos, honorarios y demás egresos que sean necesarios para el cumplimiento de las obligaciones por parte del proponente, deberán quedar incluidos en la propuesta económica, previo análisis que efectúe el mismo por su cuenta y riesgo, de manera que aquellos costos, gastos, honorarios y demás egresos no previstos en la oferta, no serán asumidos por la Empresa, ni cargados a ésta de forma alguna.
- Todos los gastos, impuestos, tasas, contribuciones o participaciones tanto en al ámbito nacional, departamental y municipal que se causen en razón de la suscripción, legalización, desarrollo y ejecución del contrato, estarán a cargo del proponente. En materia de impuestos no se aceptarán salvedades de ninguna naturaleza.
- Cualquier costo asociado a la elaboración de la presente propuesta es total responsabilidad del proponente.

Se deberán sostener los precios y tarifas ofertadas durante toda la vigencia del contrato. Los precios pactados por las partes no estarán sujetos a ningún tipo de reajuste durante su vigencia. Los valores convenidos comprenderán todos los costos y gastos en que incurra el oferente, incluyendo los gastos de administración, impuestos, imprevistos, utilidades y todos los componentes que puedan afectar el costo.

ANEXO No. 1
CARTA DE PRESENTACIÓN DE LA PROPUESTA

Ciudad, Fecha

Señores
DataHealth Solutions S.A
Bogotá

Asunto. Proceso de selección para la contratación de _____Alliancetech_____

Una vez analizados los términos de referencia del presente proceso con todos sus anexos, especificaciones y en general todos los documentos que forman parte del mismo, los cuales manifestamos conocer y aceptar en su totalidad, presentamos la propuesta al proceso de contratación del asunto.

De resultar seleccionada nuestra propuesta, nos comprometemos a suscribir y ejecutar el contrato, de acuerdo con lo especificado en los términos de referencia y sus anexos.

La propuesta tiene una validez de noventa (90) días calendario, contados desde la fecha de presentación de la misma la cual consta de (5) folios numerados.

La información contenida en nuestra propuesta es exacta y veraz.

Que como proponente SI_X_ NO__ presento con la propuesta, documentos de carácter confidencial o reservado.

Que en caso de presentar documentos con carácter confidencial o reservado los mismos son _____Anexo 1: Estrategia Jurídica. Anexo 2: Viabilidad técnica. Anexo 3: Contrato de Desarrollo. Anexo 4: Contrato de Licencia. Anexo 5: Propuesta Económica _____, y las normas que determinan su confidencialidad son ___1581___ de 2012 _____.

Que en caso de no determinar si se presentan documentos de carácter confidencial o no identificar la norma que les da ese carácter, como interesado aceptamos y se entendemos que son documentos de público conocimiento.

Adicionalmente y bajo la gravedad del juramento que se entiende prestado con la suscripción del presente documento, como interesado manifiesto que conozco y acepto en su integridad el documento Anexo a la carta de presentación de la propuesta e indico que presento oferta sin condicionamiento alguno.

NOMBRE O DENOMINACIÓN SOCIAL COMPLETA DEL PROPONENTE: Alliancetech
CÉDULA DE CIUDADANÍA O NIT: 3468889
REPRESENTANTE LEGAL: Sofia Castro Cortés
EMAIL: AreaDeContrataciónAlliancetech@advice.com (obligatorio para comunicar el desarrollo del proceso de contratación)
DIRECCIÓN FÍSICA: Carrera 7ma n# 72 A
TELÉFONO: +573227483859
CIUDAD: Bogotá
Nota: Este documento debe presentarse con nombre y firma del proponente en caso de ser persona natural, o del representante legal de la persona jurídica.

ANEXO A LA CARTA DE PRESENTACIÓN DE LA PROPUESTA
(Este anexo no debe modificarse)

1. Que no estamos incursos en ninguna de las causales de inhabilidad e incompatibilidad que se encuentran en la Constitución Política o la Ley.

2. Que no estamos incursos en algún conflicto de interés.

3. Que la propuesta y el contrato que llegare a celebrarse solo compromete a quienes suscriben la propuesta.

4. Que ninguna entidad o persona distinta de quienes suscriben la propuesta tienen interés comercial en dicha propuesta ni en el contrato que de ella se derive.

5. Que quien suscribe la propuesta conoce la información general y específica y demás documentos de los términos de referencia con sus anexos y acepta los requisitos en ellos contenidos.

6. Que quien suscribe la propuesta ha recibido y entendido las adendas al proceso de contratación, comunicadas con antelación a la fecha de entrega de la propuesta (si las hubo) y, acepta su contenido.

7. Que hemos recibido toda la información sobre aclaraciones, preguntas (si las hubo) y respuestas. Que conocida esta información de ser seleccionado como contratista cumplirá con los términos de referencia, su oferta y las estipulaciones del respectivo contrato.

8. Que en caso de ser contratista, nos someteremos al cumplimiento oportuno de toda la normatividad que la legislación laboral, de seguridad social y libre asociación en Colombia que le sea aplicable, en especial de aquellas que le surjan hacia sus empleados y el personal que tenga a su cargo; así como también seguridad y salud en el trabajo aplicable según su contratación, con el propósito de generar un alto grado de bienestar en sus trabajadores y prevenir los daños a la salud, a la dignidad, economía y subsistencia que puedan ser provocados por condiciones laborales.

9. Que en caso de ser contratista, nos comprometemos a implementar las medidas de protección y preservación del entorno, medio ambiente y el desarrollo sostenible cuidando que sus actividades sean sustentables mediante la satisfacción de las necesidades presentes sin comprometer las posibilidades futuras.

10. Que la propuesta que se presenta fue elaborada con base en los términos de referencia correspondientes al proceso objeto de esta propuesta. En consecuencia, conocimos y tuvimos las oportunidades para solicitar aclaraciones, y presentar observaciones, formular preguntas y obtener respuestas.

11. Que aceptamos las condiciones contenidas en los términos de referencia y en general, en todos los documentos del proceso de contratación.

12. Estamos en disposición de aportar la información que resulte necesaria para dar transparencia al proceso.

13. Nos comprometemos a no realizar acuerdos o pactos que puedan derivar en posibles actos de colusión.

14. Conocemos en general toda la normatividad correspondiente a la prevención y Control de Lavado de Activos y Financiamiento del Terrorismo, y que cuenta con los mecanismos e idóneos para el cumplimiento de las obligaciones que la normatividad aplicable le señale.

15. Conocemos la política colombiana de protección de la competencia y por lo tanto, nos comprometemos formalmente a no efectuar acuerdos o realizar actos o conductas que tengan por objeto o como efecto la colusión en el presente proceso de contratación.

16. Que no hemos sido investigados, ni nos encontramos en investigación, ni hemos sancionados por incumplimiento a la normatividad de prevención y Control de Lavado de Activos y Financiamiento del Terrorismo.

17. Conocemos y cumplimos el Decreto 1072 de 2015 y la Resolución 111 del 2017 en relación con las normas del sistema de Gestión de Seguridad y Salud en el Trabajo.

18. Que bajo la gravedad del juramento declaro que los documentos e información que hacen parte de la propuesta o de la documentación requerida en el proceso, es veraz, cierta, corresponde a la realidad de lo afirmado por el proponente, interesado o participante y que es susceptible de comprobación.

CONTRATO DE DESARROLLO DE SOFTWARE, INSTALACIÓN Y SERVICIOS POST

Propuesta creada por AllianceTech S.A.S

Definiciones

Servicios post:	Conjunto de acciones realizadas después de la cesión de derechos patrimoniales del programa, incluyendo la instalación, actualización y mantenimiento del software para asegurar su correcto funcionamiento.
Actualización:	Proceso de mejorar o añadir nuevas características a un software existente para optimizar su rendimiento o agregar funcionalidades.
Mantenimiento:	Conjunto de actividades realizadas para corregir errores, mejorar el rendimiento y asegurar la estabilidad del software a lo largo del tiempo.
Errores	Fallos o problemas en el software que afectan su correcto funcionamiento, los cuales pueden ser de lógica, de ejecución, de sintaxis, entre otros.
Instalación	Proceso de colocar y configurar el software en el entorno del usuario final para que esté listo para su uso.
Bases de datos	Sistemas organizados de almacenamiento de datos que permiten su acceso, gestión y actualización de manera eficiente.
Servidores	Equipos o sistemas informáticos que proporcionan servicios, recursos y datos a otros ordenadores, conocidos como clientes, en una red.
Autorización	Consentimiento previo, expreso e informado del titular de la información para llevar a cabo el tratamiento de datos personales.
Dato Personal	Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
Información médica general.	se refiere a información relacionada con anatomía, fisiología y genética y conocimientos clínicos y especialidades médicas como cardiología, neurología, oncología, gastroenterología, endocrinología, oftalmología, ortopedia, otorrinolaringología, fonoaudiología y hematología.

Servicios post	Comprende una multiplicidad de funciones incluyendo mantenimiento, actualización y soporte del sistema. No incluye la ampliación de la capacidad de almacenamiento de datos, ampliación de la Capacidad de Instalación de Licencias de Software e Instalación de otras funciones de software.
Superinteligencia Artificial (Así)	Es un tipo de inteligencia artificial capaz de superar la inteligencia humana en muchas áreas.
Redes neuronales con súper parámetros	Es un modelo de aprendizaje de inteligencia artificial que enseña a las computadoras a procesar datos de una manera que está inspirada en la forma en que lo hace el cerebro humano.
Aprendizaje continuo y generativo (Deeplearning)	Es un subconjunto del machine learning que utiliza redes neuronales multicapa, llamadas redes neuronales profundas, para simular el complejo poder de toma de decisiones del cerebro humano
Servidores.	Es un sistema que proporciona recursos, datos, servicios o programas a otros ordenadores, conocidos como clientes, a través de una red.
Enlistamiento de data.	Recomendaciones de información que se le solicita a los hospitales para recolectar información médica de paciente.
Interoperabilidad	Se refiere a los estándares, los protocolos, las tecnologías y los mecanismos que permiten que los datos fluyan entre diversos sistemas con una mínima intervención humana. Permite que diversos sistemas se comuniquen entre sí y compartan información en tiempo real.
Enlistamiento de data	Recomendaciones de información que se le solicita a los hospitales para recolectar información médica de paciente.
Dato Sensible	Dato que afecta la intimidad del titular o cuyo uso indebido puede generar su discriminación.

Encargado del Tratamiento	Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realiza el tratamiento de datos personales por cuenta del responsable del tratamiento.
Responsable del Tratamiento	Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realiza el tratamiento de datos personales.
Transferencia de datos	Situación en la que el responsable y/o encargado del tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es responsable del tratamiento y se encuentra dentro o fuera del país.
Transmisión de Datos	Tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia, con el objeto de que un encargado realice tratamiento por cuenta del responsable.
Tratamiento	Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

preámbulo

PARTES DEL CONTRATO 

LAS PARTES que se indican a continuación, han convenido celebrar el presente contrato de Desarrollo de software, instalación y servicios post:

NIT: 1023261206-7	**NIT: _____**
AllianceTech SA en adelante, Desarrollador	DataHealth Solutions S.A.S., en adelante, Cliente/encargante
representante legal: _____	representante legal: _____

OBJETO DEL CONTRATO

El presente contrato tiene por objeto el desarrollo, por parte de AllianceTech SA, del programa de software, la instalación y prestación de servicios de Post, según lo descrito en el Anexo “propuesta técnica” del contrato a cambio de una remuneración económica por parte de DataHealth.

DECLARACIONES

I. El Desarrollador es una empresa que desarrolla software y programas informáticos a medida.
II. El Cliente desea disponer de un software o programa informático para gestionar o realizar parte de las tareas de su empresa o negocio, en este caso, diagnósticos y tratamientos completos y precisos de pacientes médicos.
III. Ninguno se encuentra en proceso de liquidación.
IV. Ninguna empresa figura reportada ni sus representantes legales en ninguna lista restrictiva.
V. El desarrollador está incurso en ningún conflicto de interés con la Empresa encargante.
VI. El desarrollador autoriza expresamente a la Empresa para consultar la información, los anexos y soportes que haya suministrado con ocasión de esta convocatoria para constatar la transparencia y licitud de sus actividades.
VII. Toda la información que el desarrollador ha entregado o suministrado a la Empresa es verdadera y posee todos los comprobantes y documentos necesarios para demostrar su veracidad.
VIII. Cuenta con la autorización de todos los participantes del equipo de la empresa para el tratamiento de sus datos personales por parte de la Empresa.
IX. En virtud de las consideraciones precedentes, las Partes, de sus libres y espontáneas voluntades, han acordado celebrar el presente Contrato de desarrollo de Software, instalación y servicios post, (en adelante “el Contrato”) con sujeción a las siguientes cláusulas:

Ley aplicable y jurisdicción aplicable

Este contrato se regirá por las leyes de la República de Colombia, sin perjuicio de las normas de derecho internacional privado como lo es el HIPAA, RGPD y el AI ACT, en lo que concierte a protección de datos, protección al consumidor y reglamento para el uso de IA. Para la resolución de cualquier controversia derivada del presente contrato, las partes se someten a la jurisdicción de los tribunales de Bogotá, Colombia.

Pacto arbitral

En materia de este contrato cualquier controversia, disputa o reclamación que surja del presente contrato, o en relación con el mismo, incluyendo su formación, validez, interpretación, cumplimiento o terminación, será sometida a arbitraje técnico, en el centro de Arbitraje y Conciliación de la ciudad de Bogotá, de acuerdo con las siguientes reglas:

1. El Tribunal estará integrado por 3 árbitros.
2. Cada una de las partes designará un árbitro, que se encuentre dentro de la lista de árbitros, y los dos árbitros así designados nombrarán un tercer árbitro que actuará como presidente del tribunal. En caso de desacuerdo con la designación, será designado por el Centro de Arbitraje y Conciliación de la Cámara de Comercio de Bogotá.
3. El procedimiento se sujetará a los reglamentos que para tal fin disponga el mencionado Centro de Arbitraje y se aplicarán de conformidad con los criterios que en ellos se establezcan.
4. El Tribunal decidirá en derecho.
5. Todos los árbitros deberán poseer conocimientos y experiencia en desarrollo de software, ingeniería de software y protección de datos personales.

Cláusula de confidencialidad

Las Partes reconocen que durante la ejecución del presente contrato se intercambiará información confidencial, incluyendo, pero sin limitarse a, información técnica, comercial, financiera y de negocios relacionada con el desarrollo del software. Ambas Partes se comprometen a mantener dicha información en estricta confidencialidad y a no revelarla a terceros sin el consentimiento previo y por escrito de la otra Parte.

La obligación de confidencialidad subsistirá durante la vigencia del presente contrato y por un período de 2 años posteriores a su terminación. La información confidencial no podrá ser utilizada para ningún fin distinto al cumplimiento de este contrato.

Se considerará información confidencial toda aquella información que sea designada como tal por escrito por una de las Partes, así como toda aquella información que, por su naturaleza, sea considerada confidencial, incluyendo, pero sin limitarse a, secretos comerciales, know-how, diseños, listas de clientes, información financiera y planes de negocios.
Las Partes se comprometen a tomar todas las medidas razonables para proteger la confidencialidad de la información, utilizando al menos el mismo grado de cuidado que emplean para proteger su propia información confidencial.

Póliza de cumplimiento

Ambas partes (DataHealth y AllianceTech) acuerdan contratar una póliza de seguro que garantice el cumplimiento de todas las obligaciones estipuladas en este contrato, así como la cobertura de cualquier daño o perjuicio que pudiera surgir como consecuencia del incumplimiento de las mismas.

Etapas del contrato

1 AÑO

3 MESES

PRE-DESARROLLO

Esta etapa comprende el alistamiento de servidores para permitir el adecuado funcionamiento del proyecto, la arquitectura del código de software e Inteligencia Artificial, la indicación de la data necesaria para entrenar el sistema de VitalAI y la recolección de la información médica general. La duración de esta etapa comprende un periodo de 3 meses que se contarán a partir de la celebración del contrato.

5 MESES

DESARROLLO

En esta etapa se comprenden las actuaciones tendientes a obtener las autorizaciones para el tratamiento de datos sensibles y la recolección de estos. Esta etapa tendrá una duración de 5 meses contados a partir de la aprobación de la finalización de la etapa de pre-desarrollo.

2 MESES

ENTREGA

En esta etapa, se llevarán a cabo las siguientes acciones: entrega de los derechos del software y código fuente, instalación del sistema en los equipos del cliente y capacitación del personal. Esta fase tendrá una duración de 2 meses a partir de la aprobación de la etapa de desarrollo.

2 MESES

PRÁCTICA Y PRUEBA

La etapa de practica y seguimiento comprende un periodo de dos (2) meses durante el cual se llevará a cabo la verificación del funcionamiento del sistema desarrollado, la realización de pruebas exhaustivas, y la implementación de prácticas por parte de los licenciatarios sobre los usuarios finales.
EL objetivo es asegurar que el sistema funcione correctamente en un entorno real, identificar y corregir posibles fallos, y proporcionar el entrenamiento necesario a los usuarios del sistema.

PERMANENTE

SERVICIOS POST

La presente etapa comprende la prestación continua de servicios de mantenimiento, actualización y soporte del sistema de IA, tanto para DataHealth Solutions S.A. como para otros centros de salud que adquieran el sistema desarrollado en virtud de este contrato. Estos servicios se iniciarán a partir de la instalación del sistema en DataHealth Solutions S.A. y se extenderán hasta un mes después de que DataHealth Solutions S.A. notifique por escrito su intención de dar por terminada la prestación de estos servicios.

CLÁUSULADO

TITULO I: ETAPA PRE-DESARROLLO

PRIMERA. - DEFINICIÓN DE LA ETAPA DE DESARROLLO

Esta etapa comprende el alistamiento de servidores para permitir el adecuado funcionamiento del proyecto, la arquitectura del código de software e Inteligencia Artificial, la indicación de la data necesaria para entrenar el sistema de VitalAI y la recolección de la información médica general. La duración de esta etapa comprende un periodo de 3 meses que se contarán a partir de la celebración del contrato.

SEGUNDA.- PRECIO

El valor económico de esta etapa estará determinado por el valor de los insumos necesarios para la ejecución de esta etapa con su respectivo IVA y los gastos operacionales en los que deba incurrirse.

Asimismo, el precio de esta primera etapa variará de acuerdo con la elección que realice el encargante de la cláusula (TERCERA) expuesta en este contrato. De no realizarse la elección se aplicarán las disposiciones del parágrafo 1 de la cláusula (TERCERO).

Precio alternativa A **$ 149.855 USD**

Etapa de Pre-Desarrollo				
insumos	iva	precio con IVA	costos operacionales	total
61.265	19%	72.905	76.950	149.855

$ 559,577 USD **Precio alternativa B**

Etapa de Pre-Desarrollo				
insumos	iva	precio con IVA	costos operacionales	total
405.569	19%	482.627	76.950	559.577

OBLIGACIONES DEL DESARROLLADOR

TERCERA. Alistamiento de servidores

Realizar el alistamiento del servidor que cosiste en configurar y preparar el servidor para su uso y producción. Implica una serie de tareas que aseguren que el servidor esté listo para ejecutar servicios y aplicaciones. Lo anterior, según la elección que realice el encargante sobre las siguientes prestaciones:

Alternativa A. Servidores de AllianceTech

El desarrollador se obliga a la preparación de la infraestructura necesaria para el efectivo desarrollo y despliegue de la inteligencia artificial (IA) con la página web asociada. Para lograrlo, el desarrollador se obliga a adoptar correctos parámetros de hardware y software para la adecuada configuración de la arquitectura de la Inteligencia artificial generativa, adopción de sistemas de seguridad para el almacenamiento y tratamiento de datos sensibles y la adopción de políticas internas para el debido tratamiento de estos. El alistamiento de los servidores tendrá una duración de 2 meses contados a partir de la celebración del contrato.

Alliancetech se obliga a implementar un plan de acción respecto a la seguridad que se necesitará para la gestión de datos para que se integre y funcione correctamente en cumplimiento a las normativas colombiana, europea y estadounidense.

Alliancetech se obliga a evaluar una arquitectura viable y personalizada para la realización de VitalA. Lo anterior, para que el sistema cumpla con todos los requisitos exigidos en la convocatoria.

Alternativa B. Servidores de Amazón Web Services (AWS)

El desarrollador se obliga a realizar la correcta preparación de la infraestructura necesaria para el efectivo desarrollo y despliegue de la inteligencia artificial (IA) con la página web asociada. Alliancetech asegurará la correcta adopción de parámetros de hardware y software en la nube de Amazon Web Services (AWS) para la adecuada configuración de la arquitectura de la Inteligencia artificial generativa, adopción de sistemas de seguridad para el almacenamiento y tratamiento de datos sensibles, junto a la adopción de políticas internas para el debido tratamiento de estos.

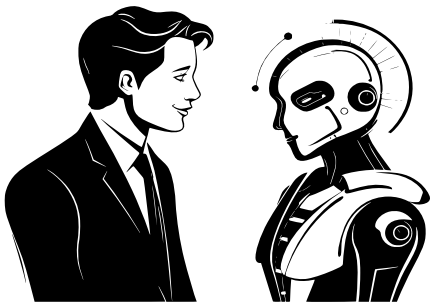
El alistamiento de los servidores tendrá una duración de 2 meses contados a partir de la celebración del contrato.

Parágrafo 1: El cliente deberá realizar la elección al momento de la celebración del contrato, so pena de que se entienda que la elección es la ALTERNATIVA B (“Servidores de Amazon Web Services”.)

CUARTA-. Verificación Técnica y Configuración Inicial

El desarrollador se obliga a realizar una verificación técnica detallada y validación por parte del equipo técnico para asegurar la correcta configuración de los servicios AWS para el desarrollo del proyecto.

AllianceTech se obliga a implementar un plan de acción con respecto a la seguridad necesaria para la gestión de datos con el fin de asegurar que todas las medidas de seguridad se integren y funcionen correctamente desde el inicio.



QUINTA-. Evaluación y Diseño de Arquitectura

AllianceTech se obliga a evaluar una arquitectura viable y personalizada para la realización de Vital IA, utilizando servicios de AWS. Lo anterior para que el sistema tenga interoperabilidad y los requisitos exigidos en la convocatoria.

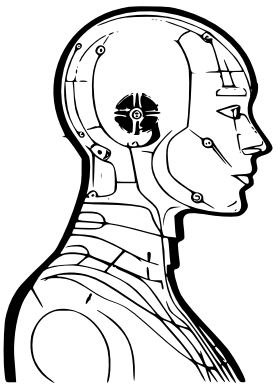
SEXTA-. Entrenamiento de la inteligencia artificial

El desarrollador se obliga a entrar la inteligencia artificial con bases de datos que contengan información de carácter general. En ninguna circunstancia durante esta etapa puede iniciarse el entrenamiento de la Inteligencia Artificial con información médica sensible

Valiéndonos de información captada por el equipo en bases de datos públicas y datos relacionados de bibliotecas digitales, Aliancetech ajustará los hiperparámetros necesarios para dirigir el diseño de la Inteligencia Artificial teniendo en cuenta los requisitos dispuestos por el encargante. Para esto, se utilizará la información que se encuentra en bases de datos públicas y datos de biblotecas digitales.

SÉPTIMA. Políticas Internas

AllianceTech se oblilga al desarrollo y adopción de políticas internas para el debido tratamiento de datos sensibles, asegurando el cumplimiento de todas las normativas vigentes en cuanto a seguridad y privacidad de la información.



OCTAVA-. Presentación del Informe

AllianceTech se obliga a presentar el informe de finalización de la etapa de predesarrollo al encargante en un plazo que no sobrepase los 3 meses a partir de la celebración del contrato de desarrollo.

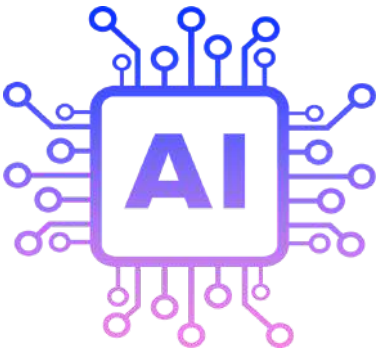
NOVENA-. Corrección del informe

AllianceTech dispondrá de un plazo de 15 días hábiles para realizar las correcciones necesarias y presentar un nuevo informe al encargante.

OBLIGACIONES DEL ENCARGANTE

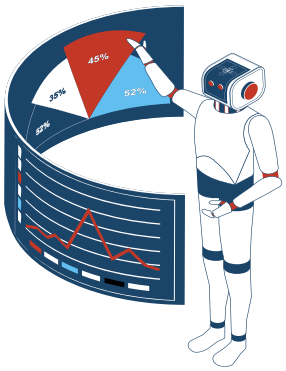
DÉCIMA. Pago del precio de la etapa de predesarrollo

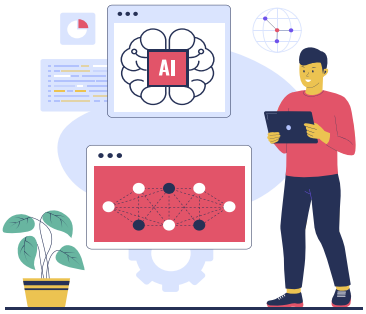
El Encargante se obliga a realizar el pago correspondiente a la etapa de predesarrollo según lo acordado en el contrato deacuerdo al tiempo y forma establecidos.



UNDÉCIMA-. Evaluación del Informe

El encargante evaluará el informe presentado por AllianceTech. Este proceso de evaluación deberá completarse en un plazo no mayor a 15 días hábiles a partir de su recepción





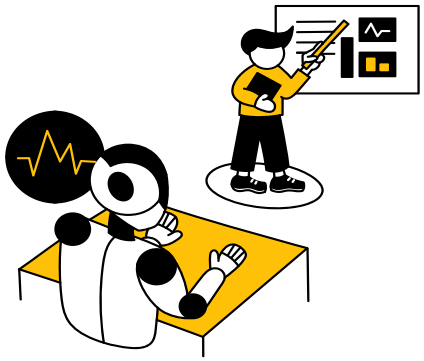
DUODÉCIMA-. Feedback y Revisión

En caso de identificar cualquier modificación, el encargante proporcionará a Alliancetech un feedback detallado indicando las áreas que requieren corrección o mejora

DÉCIMOTERCERA-. Aceptación del informe de finalización de la etapa de predesarrollo

El Encargante se obliga a revisar y aceptar el informe de finalización de la etapa de predesarrollo. Esta aceptación implica una revisión detallada del informe presetado por Alliancetech, asegurando que todas las actividades y entregables establecidadas para esta etapa se hayan cumplido.

En caso de existir observaciones o requerimientos adicionales, el encargante deberá comunicarlo de manera oportuna para proceder a las correcciones necesarias antes de avanzar a la siguiente fase del proyecto.



DÉCIMOCUARTA-. Aceptación Final

Una vez que el encargante haya evaluado todas las modificaciones y el informe revisado cumpla con todos los requisitos técnicos y jurídicos, el encargante se obliga a emitir un documento de aceptación formal de la etapa de predesarrollo. Este documento certificará que la etapa ha sido completada satisfactoriamente y permitirá el avance a la siguiente fase del proyecto

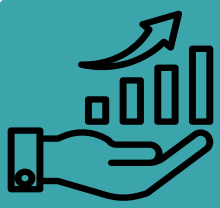
DÉCIMOQUINTA-. DERECHOS DE LAS PARTES

01. DERECHO A SOLICITAR INFORMES PERIÓDICOS

Las partes tendrán el derecho de solicitar informes periódicos sobre el avance de la etapa de pre-desarrollo. Se podrá solicitar un máximo de cuatro (4) informes trimestrales durante el período de pre-desarrollo.

Estos informes se solicitarán por escrito por correo electrónico formal. AllianceTech tendrá un plazo máximo de cinco (5) días hábiles para presentar el informe requerido, a partir de la recepción de la solicitud

02. DERECHO A SOLICITAR ASAMBLEAS DE VERIFICACIÓN



Las partes tendrán el derecho de solicitar un máximo de tres asambleas para verificar el cumplimiento de los avances de la etapa de pre-desarrollo. Las solicitudes de asambleas deberán hacerse por escrito a través de correo electrónico formal.

Alliancetech tendrá un plazo máximo de siete (7) días hábiles para coordinar y realizar la asamblea solicitada, contados desde la recepción de la solicitud.

03. DERECHO A SOLICITAR ACLARACIONES TÉCNICAS

Las partes tendrán el derecho de solicitar aclaraciones sobre aspectos técnicos que se adelanten en esta etapa, con un máximo de cinco solicitudes de aclaración durante el período de pre-desarrollo.

Las solicitudes se presentarán por escrito por correo electrónico formal. AllianceTech tendrá un plazo máximo de tres (3) días hábiles para responder a cada solicitud de aclaración, contados desde la recepción de la solicitud.

Título II: Etapa de desarrollo

DÉCIMOSEXTA.- definición de la etapa de desarrollo

En esta etapa se comprenden las actuaciones tendientes a obtener las autorizaciones para el tratamiento de datos sensibles y la recolección de estos. Esta etapa tendrá una duración de 5 meses contados a partir de la aprobación de la finalización de la etapa de pre-desarrollo.

DÉCIMOSEPTIMA-. Valor de la etapa de desarrollo.

El valor económico de esta etapa estará determinado por el valor de los insumos necesarios para la ejecución de esta etapa, más su respectivo IVA y los gastos operacionales en los que deba incurrirse para la ejecución de esta etapa.

Asimismo, el precio de esta variará de acuerdo con la elección que realice el encargante de la cláusula (TERCERA) expuesta en este contrato. De no realizarse la elección se aplicarán las disposiciones del parágrafo 1 de la cláusula (TERCERA).

ALTERNATIVA A
$249.872 USD

Etapa de Desarrollo				
insumos	iva	precio con IVA	costos operacionales	total
136.195	19%	162.072	87.800	249.872

ALTERNATIVA B
$370.200 USD

Etapa de Desarrollo				
insumos	iva	precio con IVA	costos operacionales	total
237.311	19%	282.400	87.800	370.200

Obligaciones de las partes

DÉCIMOCTAVA. Carta de Intención.

Datahealth y AllianceTech se obligan a suscribir una carta de intención con los centros de salud que sean potenciales adquirentes de una licencia del sistema, en donde se acuerde el otorgamiento una licencia especial para el uso de VitalAI a aquellos responsables de tratamiento que permitan el tratamiento datos personales a AllianceTech durante la etapa de desarrollo, con fines de entrenar el sistema de IA.

Dicho acuerdo debe proponer el otorgamiento de una licencia especial de uso de VitalAI a los centros de salud que haya prestado apoyo con la etapa de desarrollo del sistema, bajo esta modalidad el responsable de tratamiento no deberá asumir los costos de instalación, mantenimiento ni soporte durante los primeros 6 meses de uso del sistema.

Dicha carta de intención deberá ser suscrita por ambos contratantes en un término no mayor a 3 meses, contados a partir de fecha de aprobación del informe de finallización de la etapa de desarrollo. Asimismo, es obligación del encargante identificar y proponer los centros de salud con los que se entablaran los acuerdos de la carta de intención.

Obligaciones del Desarrollador

DÉCIMONOVENA. Acuerdo de Colaborador comercial

El desarrollador se obliga a celebrar acuerdo de colaboración comercial con los centros de salud con los que se haya suscrito la carta de intención, de que trata la Cláusula (DÉCIMOCTAVA), con el fin de adquirir la calidad de encargado para el tratamiento de datos, en un término no mayor a 15 días constados a partir de la suscripción de la carta de intención.

En dicho acuerdo de colaboración comercial debe constar el uso que se realizará sobre los datos personales y los medios de protección de datos que se utilizarán durante la etapa de entrenamiento de la IA.

VIGÉSIMA. Remisión del modelo de aviso de seguridad

el desarrollador se obliga a proporcionar a cada centro de salud una plantilla estándar para informar a los pacientes. Este documento, se denominará aviso de privacidad, y explicará de manera clara y sencilla cómo se utilizarán los datos personales de los pacientes y solicitará su autorización expresa para dicho uso. El modelo debe remitirse en un plazo no mayor a 5 días contados desde la celebración del acuerdo de colaboración.

Parágrafo 1: Adicionalmente a este acuerdo, se incluirá un modelo llamado 'Enlistamiento de Data'. Este modelo servirá como guía para que los centros médicos recolecten la información necesaria para el desarrollo del sistema.

NOTA:

anexo a este contrato habrá un modelo de aviso de seguridad que podrá se difundida para la recolección de consentimiento informado de los pacientes.

VIGÉSIMAPRIMERA-. Recepción de la información.

El desarrollador está obligado a recopilar la información proporcionada por los responsables de datos, siempre y cuando se cuente con el consentimiento informado del titular de los datos. Asimismo, el desarrollador deberá garantizar la seguridad de esta información mediante la implementación de medidas técnicas y organizativas adecuadas, como el uso de contraseñas fuertes, el control de acceso a los sistemas, la vigilancia y protección de los sistemas en donde se almacene la información. Dichas medidas deben ser adoptadas en menos de 5 días desde la recepción de la información.

VIGÉSIMOSEGUNDA-. Demostración de las medidas de aseguramiento.

El desarrollador tiene la obligación de enviar un informe a los responsables de tratamiento sobre las medidas de seguridad adoptadas para la protección de la información médica protegida y a la SIC. Lo anterior para cumplir con las exigencias legales sobre tratamiento de datos. Este informe debe ser enviado en un término no mayor a tres días contados a partir de la implementación de las medidas de seguridad de la que trata la cláusula anterior.

VIGÉSIMOTERCERA-. Inicio del entrenamiento del sistema con los datos personales.

El desarrollador se obliga a entrar la inteligencia artificial con la información personal que haya sido recolectada y que cuente con su debido consentimiento informado.

La información que servirá para el entrenamiento será altura, peso, sexo, género, grupo sanguíneo, viajes frecuentes, domicilio, estilo de vida, alimentación, frecuencia con la que hace deporte, enfermedades hereditarias, o enfermedades preexistentes, operaciones quirúrgicas, donaciones de sangre, frecuencia con la que asiste al médico, información sexual y reproductiva del paciente.

VIGÉSIMOCUARTA. Informe de finalización de la etapa de desarrollo.

El desarrollador se obliga a entregar un informe de finalización de la etapa de desarrollo al encargante para su aprobación. Dicho informe debe ser entregado antes del vencimiento del plazo de la etapa de desarrollo.

Parágrafo 1: si el encargante realiza objeciones o pide aclaraciones, estas deben ser resueltas en un término de 3 días.

VIGÉSIMOQUINTA-. Llevar registro de seguimiento

AllianceTech se obliga a levar documentación con información detallada sobre el desarrollo, funcionamiento y el rendimiento del sistema durante toda la etapa de desarrollo

VÍGESIMOSEXTA-. Plan de gestión de incidencias.

En caso de que se presenten errores, fallos o deficiencias en el funcionamiento del sistema de Software, que generen un incumplimiento de las medidas de seguridad, el desarrollador se obliga a llevar a cabo un plan de incidentes de seguridad, en donde se detalle:

- Identificación de los ataques y amenazas.
- Análisis y Priorización de los incidentes.
- Identificación del agente responsable.
- Comunicación al titular de la información.
- Contención y erradicación de las amenazas.
- Restauración del estado de seguridad.
- Revisión.

Obligaciones del Encargante

VIGÉSIMOSEPTIMA-. Pago del precio de la etapa de desarrollo.

DataHealth deberá realizar el pago por la etapa de desarrollo, según lo expuesto en la cláusula (DÉCIMOSEPTIMA), dentro de los 10 días siguientes a la finalización de la etapa de pre-desarrollo. Este pago no podrá dividirse en partes menores, y se efectuará mediante transferencia bancaria a las cuentas bancarias del desarrollador indicadas en este contrato.

VIGÉSIMOCTAVA-. Aprobación del informe de finalización de la etapa de desarrollo.

El encargante deberá revisar el informe de finalización de la etapa de desarrollo, proporcionado por AllianceTech, y emitir su aprobación, objeciones o comentarios dentro de los 5 días siguientes a su recepción

Parágrafo 1: En caso de no recibir ninguna comunicación por parte del encargante dentro de este plazo, se entenderá que el informe ha sido aprobado y se procederá a la siguiente etapa del proyecto.

Garantías de la etapa de desarrollo

VIGÉSIMONOVENA-. seguro contra vulneración de la información

AllianceTech se compromete a suscribir una póliza de seguro de responsabilidad civil que cubra los daños y perjuicios que puedan sufrir terceros como consecuencia de una brecha de seguridad en los datos personales causada por el sistema de inteligencia artificial durante la etapa de desarrollo. Esta póliza solo cubrirá los daños que se presenten durante la etapa de desarrollo y no etapas posteriores del contrato, ya que AllianceTech solo tendrá acceso a información sensible en dicha etapa,

Derechos de las partes durante la etapa de desarrollo

Las partes tendrán derecho a solicitar información sobre el avance de la etapa de desarrollo y a recibirla en un lapso no mayor a 5 días

Las partes tendrán derecho a solicitar reuniones para constatar la adopción de medidas de aseguramiento.

Las partes tendrán derecho a pedir que se adopten medidas adicionales para el aseguramiento de datos personale

Las partes podrán solicitar aclaraciones sobre aspectos técnicos del desarrollo del contrato y obtenerla en 5 días.

TÍTULO III: ETAPA DE ENTREGA

TRIGÉSIMA - Definición de la etapa de entrega.

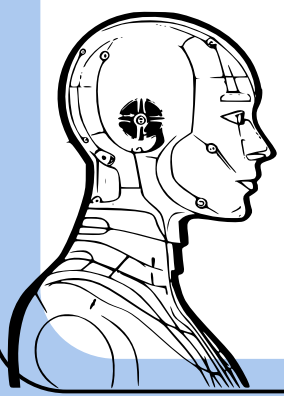
En esta etapa, se llevarán a cabo las siguientes acciones: entrega de los derechos del software y código fuente, instalación del sistema en los equipos del cliente y capacitación del personal. Esta fase tendrá una duración de 2 meses a partir de la aprobación de la etapa de desarrollo.

TRIGÉSIMOPRIMERA - Precio.

El valor económico de esta etapa estará determinado por el porcentaje de utilidad (30%) que percibirá AllianceTech por el desarrollo del sistema de software.
Asimismo, el precio de esta variará de acuerdo con la elección que realice el encargante de la cláusula (TERCERA) expuesta en este contrato. En caso de que el encargante no realice la elección se aplicarán las disposiciones del parágrafo 1 de la cláusula (TERCERA).

Alternativa A
$175273 USD

Etapa de Entrega				
insumos etapa de pre-desarrollo	insumos etapa de desarrollo	ingreso total x insumos	costos operacionales	total a pagar
72.905	162.072	234.977	164.750	**175.273**



Alternativa B
$390223 USD

Etapa de Entrega				
insumos etapa de pre-desarrollo	insumos etapa de desarrollo	ingreso total x insumos	costos operacionales	total a pagar
482.627	282.400	765.027	164.750	**390.223**

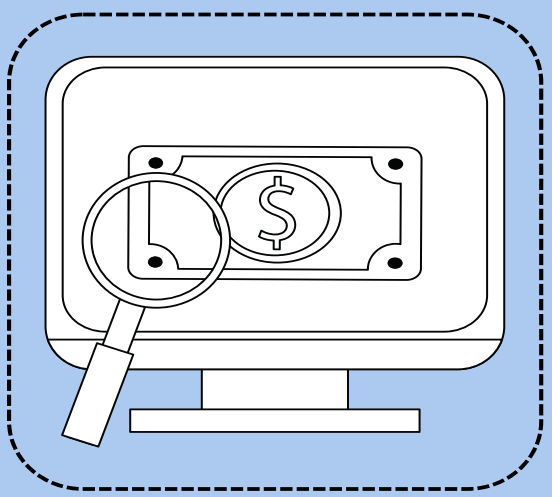
TRIGÉSIMOSEGUNDA-. Descripción de Producto final.

El desarrollador entregará a DataHealth el sistema VitalAI, una herramienta que permitirá procesar una gran cantidad de datos de salud, incluyendo información sobre antecedentes familiares, hábitos de vida, resultados de exámenes y tratamientos médicos. VitalAI estará capacitado para analizar estos datos y generar informes personalizados que podrán ser utilizados en diversas especialidades médicas, como cardiología, oncología, neurología, gastroenterología, endocrinología, oftalmología, ortopedia, otorrinolaringología, fonoaudiología y hematología para mejorar la atención al paciente y optimizar los recursos sanitarios.

Obligaciones del desarrollador

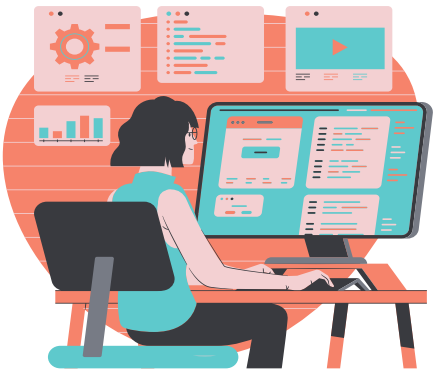
TRIGÉSIMOTERCERA-. Cesión de derechos patrimoniales

Una vez efectuado el pago total del precio convenido, el desarrollador se obliga a transferir al cliente, de forma irrevocable y exclusiva, todos los derechos patrimoniales sobre el software desarrollado, incluyendo el código fuente completo. Esta transferencia implica que el cliente será el único propietario del software y tendrá la libertad de utilizarlo, modificarlo y distribuirlo a su discreción. Esta cesión deberá hacerse durante los tres días siguientes al pago total del precio.



TRIGÉSIMOCUARTA-. Uso de la copia del código fuente

El Desarrollador reconoce que el Programa informático y su código fuente son propiedad exclusiva del Encargante. La única finalidad de la copia del código fuente proporcionada al Desarrollador es permitir la prestación de los servicios de mantenimiento del sistema. En consecuencia, el Desarrollador se compromete a No revelar, No reproducir, No modificar y No utilizar el código fuente con fines distintos a los anteriormente descritos.



TRIGÉSIMOQUINTA-. Instalación del sistema de VitalAI

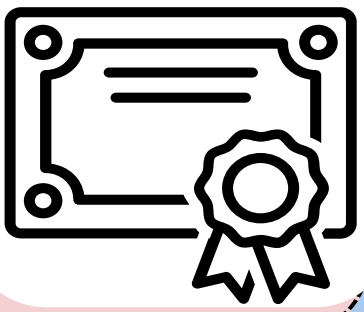
El desarrollador se obliga a realizar la instalación del sistema VitalAI en los equipos de cómputo de los licenciatarios. Para esto, primero se abre la terminal o la línea de comandos en el computador o sistema que se vaya a instalar, seguidamente se dirige al directorio del código y se ejecuta el comando para instalarlo. El encargo de realizar dicho procedimiento será un ingeniero de software.

El desarrollador se obliga a realizar dicha instalación dentro de los 15 días siguientes a la cesión del código fuente.

TRIGÉSIMOSEXTA-. Capacitación sobre el uso del sistema

El Desarrollador se compromete a brindar capacitación al personal designado por DataHealth sobre el uso, funcionamiento y gestión del VitalAI. Esta capacitación incluirá aspectos técnicos y normativos, y se llevará a cabo mediante sesiones presenciales o virtuales, así como la entrega de material de apoyo. Esta obligación deberá ejecutarse de forma périodica en un plazo de 2 meses contados a partir de la fecha de instalación del sistema a DataHealth.

TRIGÉSIMOSEPTIMA-. Emitir Certificación de la capacitación



Al finalizar la capacitación, el Desarrollador está obligado a emitir un certificado por cada participante, el cual acreditará su asistencia y aptitud para operar el sistema VitalAI de acuerdo con los estándares establecidos. Estos certificados serán enviados por medios electrónicos a DataHealth y a al personal que haya obtenido su certificación. Esto deberá hacerse en un plazo que no exceda los 3 días contado a partir de la finalización de la capacitación según el cronograma propuesto.

Obligaciones del encargante

TRIGÉSIMOCTAVA-. Pagar el precio

DataHealth deberá realizar el pago por la etapa de desarrollo, según lo expuesto en la cláusula (TRIGÉSIMOPRIMERA), dentro de los 10 días siguientes a la finalización de la etapa de desarrollo. Este pago no podrá dividirse en partes menores, y se efectuará mediante transferencia bancaria a las cuentas bancarias del desarrollador indicadas en este contrato.

TRIGÉSIMONOVENA-. Permitir mantener la tenencia de una copia del código fuente

El Encargante autoriza al Desarrollador a conservar una copia del código fuente del sistema con el fin de garantizar la prestación de los servicios de mantenimiento por parte de AllianceTech.

Parágrafo 1: en ninguna circunstancia autoriza al desarrollador para revender o utilizar el Programa informático o su código fuente para realizar otras aplicaciones informáticas.

CUADRIGÉSIMA - Brindar indicaciones para la instalación.

El Encargante se obliga a informar al Desarrollador, dentro de los tres (3) días hábiles siguientes a la cesión de derechos, el lugar físico exacto donde se instalará el sistema VitalAI, así como las especificaciones técnicas de los equipos de cómputo en los que se ejecutará.

CUADRIGÉSIMAPRIMERA-. Aptitud para la instalación

Indicar el personal que recibirá la capacitación. Dentro de un plazo máximo de tres (3) días hábiles posteriores a la formalización de la cesión total de los derechos, el Encargante se obliga a entregar al Desarrollador un listado detallado que incluya: i) Nombres completos: De cada uno de los empleados que participarán en la capacitación indicada en la cláusula (TRIGÉSIMOSEXTA). Ii) Cargos: Los cargos que desempeñan dentro de la organización del Encargante. Y iii) Departamentos: Los departamentos a los que pertenecen.

Esta información es esencial para que el Desarrollador pueda planificar y organizar la capacitación de manera adecuada.

CUADRIGÉSIMASEGUNDA- Recibir la capacitación

El Encargante se obliga a garantizar que su personal asista y participe activamente en la capacitación indicada en la cláusula (TRIGÉSIMOSEXTA), cumpliendo al menos el 80% de los cronogramas y actividades propuestas por el Desarrollador.

Garantías de la etapa de entrega

CUADRIGÉSIMATERCERA-. Garantía de buen funcionamiento

AllianceTech otorgará al Encargante una garantía de buen funcionamiento del sistema VitalAI por un período de un (1) año a partir de la fecha de instalación. Esta garantía cubre cualquier daño, error o falla del sistema que no sea atribuible a actos u omisiones de DataHealth o su personal.

Si se hace efectiva la garantía, AllianceTech se obliga a realizar las respetivas reparaciones del sistema y a pagar los perjuicios directos que se hayan causado a DataHealth por el mal funcionamiento del sistema.

CUADRIGÉSIMACUARTA-. Cláusula de exclusividad

Durante la vigencia del presente contrato y por un período de un (1) año posterior a su terminación, el Desarrollador se compromete a no desarrollar, comercializar o licenciar a terceros ningún software, aplicación o sistema que sea sustancialmente similar al desarrollado en virtud del presente contrato, ni prestar servicios de desarrollo a terceros que compitan directa o indirectamente con el Encargante en relación con el objeto del presente contrato.

CUADRIGÉSIMAQUINTA- Garantía de protección por producto defectuoso

AllianceTech garantiza que el producto objeto de este contrato se encuentra libre de defectos de fabricación y materiales por un período de 1 año a partir de la fecha de entrega.

CUADRIGÉSIMASEXTA-. Indemnidad administrativa

"AllianceTech se obliga a indemnizar a DataHealth por cualquier gasto generado debido a responsabilidades administrativas que surjan como consecuencia de defectos o mal funcionamiento del sistema VitalAI durante un período de un año a partir de la fecha de entrega del sistema.

Título IV: Etapa de Práctica y seguimiento

CUADRIGÉSIMASEPTIMA-. Definición de la etapa de práctica y seguimiento.

La etapa de practica y seguimiento comprende un periodo de dos (2) meses durante el cual se llevará a cabo la verificación del funcionamiento del sistema desarrollado, la realización de pruebas exhaustivas, y la implementación de prácticas por parte de los licenciatarios sobre los usuarios finales.

EL objetivo es asegurar que el sistema funcione correctamente en un entorno real, identificar y corregir posibles fallos, y proporcionar el entrenamiento necesario a los usuarios del sistema.

Obligaciones del Desarrollador

CUADRIGÉSIMAOCTAVA-. Verificación

Alliancetech se obliga a verificar el funcionamiento integral del sistema desarrollado, asegurando que todos los componentes de hardware y software operen de acuerdo con las especificaciones y requerimiento establecidos en el contrato

Alliancetech tendrá acceso completo a las instalaciones del licenciatario, previa coordinación y aprobación por escrito en un término de cinco (5) días hábiles a partir de su notificación al correo empresarial, para realizar las verificaciones necesarias.

CUADRIGÉSIMANOVENA. Prueba

Alliancetech se obliga a realizar pruebas exhaustivas dentro de las primeras cuatro (4) semanas de ejecución de esta etapa, realizando simulaciones de cargas máximas, intentos de penetración por terceros a los datos, monitoreos de tiempo de respuesta y rendimiento general del sistema.

QUINCUAGÉSIMA.
Capacitaciones de Seguimiento.

Alliancetech se obliaga a ofrecer, como mínimo, cuatro sesiones de capacitación y entrenamiento a los licenciatarios de DataHealth durante dos meses. Cada sesión tendrá una duración no inferior a tres horas..
Alliancetech se obliga a proporcionar guías de uso, manuales operativos y otros materiales de capacitación necesarios para asegurar que los usuarios puedan operar el sistema de manera eficiente.

QUINCUAGÉSIMAPRIMERA.
Identificación de fallos

Alliancetech se obliga a

1. La identificación de Fallos: Cualquier fallo identificado durante las pruebas o el uso del sistema será documentado y reportado al cliente inmediatamente.
2. La corrección de Fallos: Alliancetech se obliga a realizar las correcciones necesarias dentro de un plazo máximo de setenta y dos (72) horas hábiles a partir de la identificación del fallo.
3. La validación de Correcciones: Una vez realizadas las correcciones, se llevarán a cabo pruebas adicionales para validar que los fallos hayan sido subsanados correctamente. Se generarán informes de validación que serán entregados al cliente.

Obligaciones del Encargante

QUINCUAGÉSIMASEGUNDA. Cooperación.

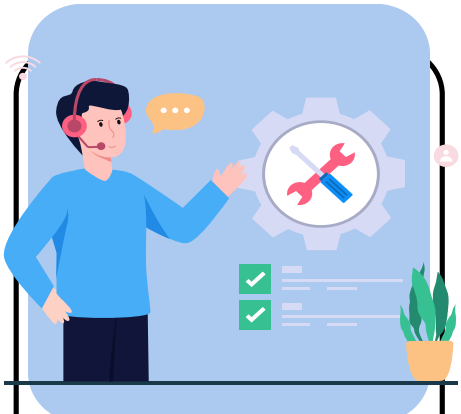
Se obliga a cooperar plenamente con Alliancetech durante la realización de pruebas y ajustes, proporcionando el personal necesario y facilitando los recursos requeridos.

QUINCUAGÉSIMATERCERA. Notificación

DataHealth se obliga a notificar a Alliancetech sobre cualquier incidencia o fallo detectado durante el uso del sistema de manera oportuna para que se puedan tomar las acciones correctivas necesarias.

QUINCUAGÉSIMACUARTA. Colaboración.

Se obliga a asegurar la participación de todos los licenciatarios designados en las sesiones de práctica y entrenamiento organizadas por Alliancetech.



QUINCUAGÉSIMAQUINTA. Auxilio técnico.

DataHealth se obliga a proporcionar un espacio adecuado y los recursos necesarios para llevar a cabo las sesiones de capacitación de manera efectiva.

Título V: Etapa de servicios Post

QUINCUAGÉSIMASEXTA.- definición de la etapa de desarrollo

La presente etapa comprende la prestación continua de servicios de mantenimiento, actualización y soporte del sistema de IA, tanto para DataHealth Solutions S.A. como para otros centros de salud que adquieran el sistema desarrollado en virtud de este contrato. Estos servicios se iniciarán a partir de la instalación del sistema en DataHealth Solutions S.A. y se extenderán hasta un mes después de que DataHealth Solutions S.A. notifique por escrito su intención de dar por terminada la prestación de estos servicios.

esta etapa NO incluye los servicios de ampliación de la capacidad de almacenamiento del sistema, la ampliación de la capacidad de instalación de licencias de software e instalación de otras funciones en el sistema de VitalAI.

QUINCUAGÉSIMASEPTIMA. Valor de la etapa de servicios Post.

el valor de esta etapa tiene en cuenta los costos operacionales de los servicios de mantenimiento, actualización y soporte del sistema de VitaAI por cada centro de salud que instale el sistema y una utilidad del 15% para AllianceTech por la prestación de los mismos.

gastos operacionales X centro de salud en USD	%utilidad	total a pagar en USD
1150	15%	1322,5

Obligaciones del Desarrollador

QUINCUAGÉSIMOCTAVA-. servicio de mantenimiento

El Desarrollador se obliga a prestar el servicio de mantenimiento periódico de la IA, de forma indefinida al Cliente y a todos los centros médicos que instalen el sistema, en virtud de relaciones contractuales que mantengan con el cliente.

QUINCUAGÉSIMONOVENA-. mantenimiento bajo auditoria

El Desarrollador solo podrá realizar tareas de soporte, actualización y mantenimiento sobre el sistema bajo la estricta supervisión de un auditor independiente, designado por DataHealth, quien verificará el cumplimiento de todas las regulaciones aplicables en materia de privacidad y seguridad de la información (HIPAA, GDPR, Ley 1581 de 2012 y demás normas concordantes). Esta supervisión se exceptúa únicamente en casos de mantenimiento correctivo urgente derivado de una infracción de seguridad.

SEXAGÉSIMA-. mantenimiento periódico

El desarrollador se obliga a prestar el servicio de mantenimiento, según lo expuesto en la cláusula (33) del presente contrato, de forma periódica para dar cumplimiento a la regulación sobre tratamiento de datos.
La determinación de los periodos está a cargo del cliente.

SEXAGÉSIMAPRIMERA-. entrega de la copia del código fuente

El Desarrollador se compromete a entregar a DataHealth, en un plazo máximo de 10 (diez) días hábiles a partir de la recepción de la notificación escrita de terminación unilateral del contrato por parte de DataHealth, todo el código fuente del Sistema, incluyendo las bases de datos, documentación técnica, manuales de usuario y cualquier otro material necesario para la operación y mantenimiento del Sistema. El código fuente será entregado en formato repositorio Git, debidamente documentado y listo para ser desplegado en un entorno de producción.

Obligaciones del Encargante

SEXAGÉSIMASEGUNDA-. información sobre fallas del sistema.

El cliente tiene a su cargo la obligación de informar sobre fallas, errores o deficiencias del sistema al desarrollador que se presenten durante el uso de la IA.

Esta información puede darse por cualquier medio que sea adecuado para informar de manera rápida y suficiente la condición del sistema y se evite la agravación del daño, falla o error.

SEXAGÉSIMATERCERA-. Facilitar el Mantenimiento.

l Cliente se obliga a brindar los medios administrativos, físicos o técnicos necesarios para permitir que el desarrollador cumpla con su obligación de mantenimiento.
El cliente debe nombrar a un auditor que supervise las actividades que realice el desarrollador y las apruebe una vez finaliza la visita de mantenimiento.

SEXAGÉSIMACUARTA-. pago mensual del servicio

El cliente se obliga a pagar de forma periódica el servicio de mantenimiento según los criterios expuestos en la cláusula SÉPTIMA del presente contrato.
Dicho pago debe realizarse en los últimos 5 días de cada mes (pago a mes vencido).

SEXAGÉSIMAQUINTA-. información al titular sobre infracciones

El cliente está obligado a informar a los titulares de la información médica protegida (Pacientes) sobre la vulneración o infracción de la seguridad en la protección de sus datos. Dicha información debe contener al menos: I. La naturaleza del incidente. II. Los datos personales comprometidos. III. Las recomendaciones al titular acerca de las medidas que este pueda adoptar para proteger sus intereses. IV. Las acciones correctivas realizadas de forma inmediata. V. Los medios donde puede obtener más información al respecto.

SEXAGÉSIMASEXTA-. información de la decisión de terminación unilateral del servicio

El Encargante deberá notificar al Desarrollador por escrito, con una antelación mínima de un mes, su decisión de dar por terminada la prestación de los servicios Post.

SEXAGÉSIMASEPTIMA-. recepción de la copia del código fuente

El cliente se obliga a recibir la copia del código fuente que proporcione el desarrollador a causa de la terminación de los servicios Post.
asimismo, el cliente se obliga a recibir toda la documentación que el desarrollador le proporcione con relación al mantenimiento y condiciones del sistema y a revisarla en su totalidad para verificar su autenticidad y utilidad.

Título VI: Causales de terminación unilateral

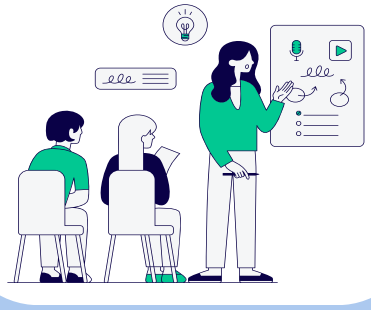
SEXAGÉSIMAOCTAVA - Causales de terminación unilateral del contrato por parte del encargante.

El encargante podrá terminar unilateralmente el contrato teniendo presente los requisitos jurisprudenciales establecidos por la CSJ para su validez y eficacia, en los siguientes casos:

1. Si el desarrollador no cumple con las especificaciones técnicas acordadas en el contrato.

2. Si el software no opera de acuerdo con los requerimientos funcionales definidos, impidiendo su uso para el propósito previsto.

3. Si el desarrollador no entrega la propuesta técnica para la respectiva aprobación en el plazo acordado.



4. Si el desarrollador no cumple con su obligación de proporcionar la capacitación necesaria al personal del cliente según lo establecido en el contrato.

5. Si el desarrollador no proporciona el mantenimiento y soporte acordado conforme a las condiciones y periodo establecido en el presente contrato.

6. Si el desarrollador de forma reiterada no entrega los informes o no cumple con la entrega del producto o servicio en los plazos establecidos en el cronograma del proyecto. De forma reiterada hace referencia a una tardanza en 3 o más ocasiones.

7. En caso de producirse cualquier violación o vulneración de la seguridad que comprometa la información sensible de las personas.

8. Si el desarrollador realiza declaraciones falsas o engañosas que hayan inducido a la otra a celebrar el contrato.

9. Si el desarrollador utiliza el código fuente o su copia con otros fines distintos a los estipulados en este contrato.

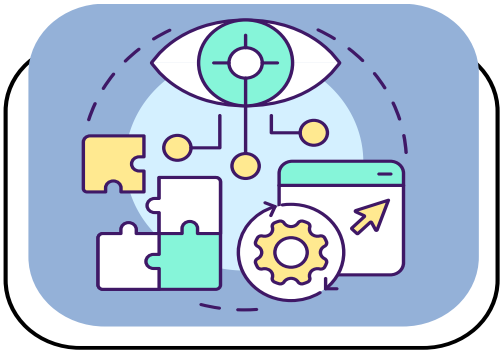
SEXAGÉSIMONOVENA.- Causales de terminación unilateral del contrato por parte del desarrollador.

Asimismo, el desarrollador podrá terminar unilateralmente el contrato teniendo presente los requisitos jurisprudenciales establecidos por la CSJ para su validez y eficacia, en los siguientes casos:

1. Si el cliente no realiza los pagos acordados en las fechas establecidas en el cronograma de pagos del contrato.

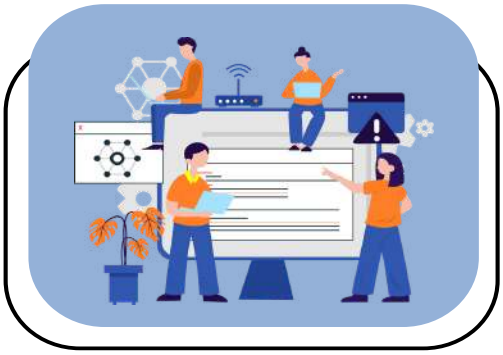
2. Si el cliente no proporciona los recursos, información o acceso necesarios para la realización del proyecto por parte del desarrollador según lo acordado.

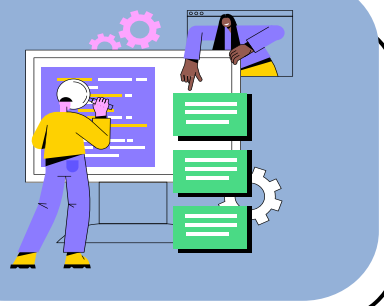
3. Si el cliente realiza modificaciones al software que afecten negativamente su desempeño o funcionalidad, durante la instalación y la realización de los mantenimientos, que genere retrasos o mayores costos para el desarrollador en el cumplimiento de sus obligaciones.



4. Si el cliente de forma reiterada no cumple con los plazos establecidos para la revisión y aprobación de entregables, afectando el cronograma del proyecto. De forma reiterada hace referencia a una tardanza en 3 o más ocasiones.

5. Si el cliente no coopera con el desarrollador en la realización de pruebas, capacitación, o cualquier otra actividad necesaria para la correcta implementación del software de forma reiterada y sin justa causa.





6. Si el cliente utiliza el software fuera de los términos y condiciones establecidos en las licencias otorgadas por el desarrollador.

7. Si el cliente no implementa las medidas de seguridad recomendadas por el desarrollador, comprometiendo la integridad y seguridad del software y los datos.

8. Si el encargante ha realizado declaraciones falsas o engañosas que han inducido a la otra a celebrar el contrato.

SEPTUAGÉSIMA- Notificación

La parte que desee terminar el contrato deberá notificar por escrito a la otra parte, mediante correo certificado, en un término no menor a 10 días, detallando los motivos de la terminación.

SEPTUAGÉSIMAPRIMERA- Plazo de enmienda del Incumplimiento.

En caso de incumplimiento, la parte incumplida tendrá un plazo de 15 días desde la recepción de la notificación para subsanar el incumplimiento. Si el incumplimiento no es subsanado en el plazo estipulado, la parte afectada podrá declarar resuelto el contrato mediante una segunda notificación por escrito en un término no mayor a 10 días.

NI HRTHT E THTI H: I QE ARI

N

El tratamiento de datos es un conjunto de operaciones de recolección, registro, organización y uso de los datos personales de una persona con un fin específico. En nuestro caso, necesitamos tratar datos para entrenar el sistema VitalAI y que esta pueda dar diagnósticos precisos en menor tiempo, lo que ayudaría a la eficiencia del sistema de salud y mejora en el nivel de vida de las personas.

N

R

El titular de los datos personales tiene varios derechos con respecto al tratamiento de datos:

1. Derecho a la información. El encargado del tratamiento de datos debe facilitar al interesado la información sobre el tratamiento. plazo durante el cual se conservarán los datos, los derechos del usuario para rectificar y eliminar los datos o retira el consentimiento al tratamiento
2. Derecho al acceso de datos. Tiene derecho a acceder a los datos personales recogidos para conocer y verificar la licitud del tratamiento, tendrá acceso a datos de salud como historias clínicas con diagnósticos, etc.

N

Es lícito el tratamiento de datos de los mayores de 18 años, cuando se trate de menores de 18 años el tratamiento únicamente se considera lícito si lo autorizó el titular de la patria potestad del menor.

Cuando hablamos de datos sensibles hablamos de un conjunto de datos que por su naturaleza podrían poner en riesgo derechos fundamentales del titular, caso por el cual se necesita cumplir con unos requisitos para poder utilizar tales datos. Un requisito indispensable para tratar datos sensibles es tener el consentimiento, que es la autorización que da el titular de los datos para que se puedan tratar.

R

3. Eliminación de los datos. Se podrá pedir la supresión de los datos personales cuando haya tratamiento indebido o ilícito de los datos, cuando ya no sean necesarios los datos para el fin del tratamiento o cuando se retire el consentimiento.
4. Derecho de retirar el consentimiento. Tiene derecho a retirarlo cuando desee, no obstante el tratamiento de datos dado antes del retiro es lícito.

NI HR THTI TH TC TQATAE THTI RT E R RATI R NTQRI HACTR HNCA THR I CI R RTHR MCTR

SÍ NO

Para dejar constancia de todo ello, firmo a continuación:

Firma del titular (representante): _____

Nombre Completo: _____

Fecha: _____

2024

CONTRATO

LICENCIA DE SOFTWARE

Propuesta contractual

REALIZADO POR:

AllianceTech

CONTRATO DE LICENCIA DE USO DE SOFTWARE

IDENTIFICACIÓN DE LAS PARTES

Las partes que se indican a continuación, han convenido celebrar el presente contrato de licencia de uso de software:

NIT: 1011092012-6	**NIT: _____**
DataHealth Solutions S.A., en adelante, el licenciante	Centros hospitalarios, en adelante, el licenciatario: _____
Representante legal: _____	Representante legal: _____

LAS PARTES MANIFIESTAN

1. La parte licenciante declara ser el propietario exclusivo de todos los derechos de propiedad intelectual sobre el Software VitalAI, incluyendo: los derechos de autor, patentes, marcas comerciales y secretos comerciales.
2. El Software VitalAI ha sido desarrollado de forma independiente y no infringe ningún derecho de propiedad intelectual de terceros.
3. Se permitirá el uso del Software VitalAI bajo los términos de esta licencia propietaria de tipo cerrado y está sujeto a las condiciones establecidas en este presente documento.
4. Las partes reconocen que el Software VitalAI puede recopilar y procesar datos personales y sensibles, y se compromete a cumplir con todas las leyes y regulaciones aplicables en materia de protección de datos personales según la legislación aplicable.
5. No se está ante ningún conflicto de intereses.
6. Ninguna de las partes se encuentra en proceso de liquidación.
7. El Licenciatario reconoce que el Software es una herramienta de apoyo a la práctica médica y que los diagnósticos y tratamientos sugeridos por el mismo no sustituyen la evaluación y el juicio clínico del profesional de la salud.

PREÁMBULO

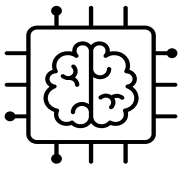
Con la celebración del contrato de desarrollo de software y servicios post entre DataHealth Solutions S.A. y AllianceTech S.A.S., que tenía como objeto el desarrollo de un sistema de Inteligencia Artificial que analizara distintos datos personales de naturaleza sensible para la formulación de diagnósticos y tratamientos médicos que apoyen la labor hospitalaria, se creó el software *VitalAI*, el cual se ajusta a las necesidades propuestas y el cumplimiento de requerimientos nacionales e internacionales de protección de datos, protección al consumidor y regulación de la IA.

Por tanto, en virtud del presente contrato de licencia propietaria de uso de software de tipo cerrado, el licenciante DataHealth Solutions S.A. como propietario del software, otorga al licenciatario la potestad de utilizar el software denominado *VitalAI*, sin generar entrega del código fuente, con las características y funciones detalladas en el manual de usuario, en los términos y condiciones que a continuación se establecen:

PRIMERA.- OBJETO

El presente contrato tiene por objeto otorgar al Licenciatario una licencia temporal, intransferible y limitada para utilizar el software denominado *VitalAI*, de propiedad del Licenciante, con la finalidad exclusiva de generar diagnósticos médicos preliminares y proponer posibles tratamientos. El Software está diseñado para asistir a profesionales de la salud en la toma de decisiones clínicas, proporcionando información y herramientas de análisis basadas en los datos ingresados.

SEGUNDA.- Definiciones



Software
Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora. En el presente contrato se trata de la IA denominada VitalAI cuyo uso se concede en virtud del presente contrato.

Licenciante
Es la persona natural o jurídica que da permiso para usar el software, en el presente contrato es DataHealth Solutions S.A. como propietario de los derechos patrimoniales del software VitalAI.

Licenciatario
Es la persona natural o jurídica sobre quien recae el permiso de usar el software.

Base de datos
Es el repositorio de todos los datos del software para un ambiente especifico independiente, que se aloja sobre el motor de bases de datos que se seleccione y cuya función es almacenar y leer la información necesaria para el funcionamiento del software.

Hardware
Son todas las partes físicas de un ordenador, como el teclado, el monitor, el disco duro, etc. Todo lo que puedes tocar.

Propiedad intelectual
Son creaciones de la mente, como inventos, obras literarias, artísticas o científicas, etc., que están protegidos por la ley.

Diagnóstico
Son pruebas o análisis que se realizan para identificar problemas.

Licencia de uso
Es el presente contrato en virtud del cual se autoriza y regula el uso permitido del software al licenciatario que constituye el límite y alcance del uso que puede hacer el licenciatario del software

Derechos patrimoniales
Son los derechos que permiten al creador de una obra explotarla económicamente, como venderla o licenciar su uso.

Licencia temporal
Es aquella que se adquiere mediante pago por instalamentos que da derecho al uso del software por tiempo limitado conforme a lo regulado en este contrato

Capacitación

Proceso continuo de aprendizaje y desarrollo que busca mejorar las habilidades, conocimientos y actitudes de los empleados de una organización

Copia de seguridad completa

Es una copia exacta y completa de todos los datos de un sistema en un momento determinado.

Copia de seguridad diferencial

Es una copia solo de los datos que han cambiado desde la última copia de seguridad completa

Auditoría

Es una revisión detallada de un sistema o proceso para evaluar su cumplimiento con normas o estándares

Cesión de derechos

Es el acto por el cual una parte contractual transfiere a otra sus derechos y obligaciones sobre un contrato, obra o invención.

Datos sensibles

Son datos personales que pueden revelar información privada sobre una persona, como su salud, origen racial o creencias religiosas

Rescisión

Es la terminación anticipada de un contrato.

Equipo computacional

Son todos los dispositivos electrónicos utilizados para procesar información, como ordenadores, tablets y smartphones.

Ingeniería inversa

Es el proceso de analizar un producto para descubrir cómo funciona y poder crear uno similar.

IPC

Índice de Precios al Consumo, un indicador que mide la variación de los precios de una cesta de bienes y servicios.

IVA

Impuesto sobre el Valor Añadido, un impuesto que se aplica a la venta de bienes y servicios.

IBC

índice Bancario Corriente. Se trata de un indicador financiero utilizado en el sector bancario para determinar la tasa de interés.

Riesgos

Son eventos futuros inciertos que pueden causar pérdidas.

Póliza de seguro

Es un contrato por el cual una aseguradora se compromete a indemnizar al asegurado por los daños materiales que sufra.

Medidas de mitigación de riesgos

Son acciones que se toman para reducir la probabilidad o el impacto de un riesgo.

Código fuente

Es el texto escrito en un lenguaje de programación que se utiliza para crear un programa.

Arbitraje

Es un método alternativo de resolución de conflictos en el que una tercera parte imparcial toma una decisión vinculante para las partes en disputa.

Amigable composición

La amigable composición es un mecanismo alternativo de resolución de conflictos que ofrece una vía más ágil y flexible para solucionar disputas, en comparación con los procesos judiciales tradicionales

RGPD

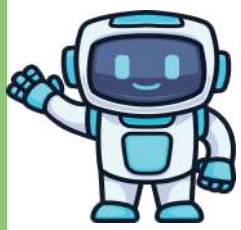
Reglamento General de Protección de Datos de la Unión Europea, que establece las normas sobre la recopilación y el procesamiento de datos personales.

HIPAA

La amigable composición es un mecanismo alternativo de resolución de conflictos que ofrece una vía más ágil y flexible para solucionar disputas, en comparación con los procesos judiciales tradicionales

AI ACT

Ley de IA. Es una propuesta de ley de la Unión Europea que busca regular el desarrollo y uso de la inteligencia artificial.



Jurisdicción

Es la autoridad legal de un tribunal o entidad para conocer de un asunto legal.

TERCERA.- INSTALACIÓN DEL SOFTWARE

DataHealth SA se compromete a llevar a cabo la instalación del software en los equipos de cómputo de los hospitales contratantes, de acuerdo con las obligaciones establecidas en este contrato. La instalación se realizará en las instalaciones físicas de los hospitales contratantes, para lo cual DataHealth enviará personal técnico especializado.

El personal de DataHealth se encargará de realizar la instalación del software en los equipos designados por el hospital y se asegurará de que el software funcione correctamente y cumpla con los requerimientos técnicos previamente establecidos. Además, se proporcionará una capacitación básica sobre el uso del software al personal designado por el hospital.

La instalación del software se llevará a cabo en un plazo de 20 días hábiles contados a partir de la firma del presente contrato.

Toda la información a la que DataHealth tenga acceso durante el proceso de instalación será tratada con estricta confidencialidad, y se tomarán todas las medidas necesarias para asegurar la integridad y seguridad de los datos del hospital contratante.

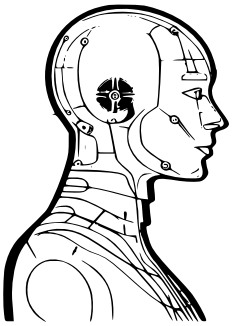
El costo de la instalación del software será de 1950 USD, y deberá ser pagado de acuerdo con los términos establecidos en este contrato. Cualquier costo adicional seguirá la suerte de lo que reza el contrato.

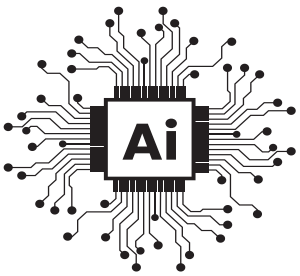
(Los precios señalados se pueden cambiar según como DataHealth considere, no obstante son un precio que AllianceTech recomienda como monto mínimo)

CUARTA.- DERECHOS OTORGADOS AL LICENCIATARIO

a. Uso del software

El licenciatario tiene derecho a utilizar el software para el propósito específico para el cual fue diseñado, es decir, generar diagnósticos médicos preliminares y proponer posibles tratamientos.





b. Acceso a actualizaciones

El licenciatario puede tener derecho a recibir actualizaciones del software siempre que pague la suma especificada en la cláusula décima cuarta, precio que integra a su vez el valor del mantenimiento.

c. Soporte técnico

El licenciante ofrece un nivel de soporte técnico avanzado para ayudar al licenciatario a utilizar el software de manera efectiva, siempre que pague el precio del mantenimiento precisado en la clausula décima cuarta.

d. Garantía de buen funcionamiento

Lo que implica un software libre de defectos, corrección de problemas y demás especificados en la cláusula quinta.

e. Copias de seguridad

El Licenciatario podrá realizar una (1) copia de seguridad por cada cambio que se realice al código fuente, exclusivamente para fines de restauración en caso de pérdida o daño accidental. Dicha copia de seguridad deberá ser almacenada en un lugar seguro y no podrá ser distribuida a terceros.

f. Documentación técnica

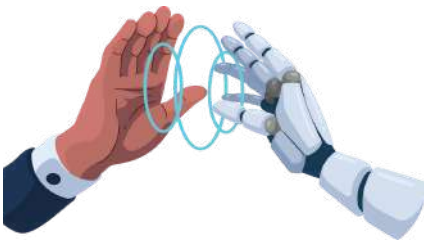
El licenciatario tiene derecho a recibir la documentación técnica necesaria para utilizar el software de manera adecuada.

g. Actualizaciones de la documentación

El licenciante se compromete a proporcionar actualizaciones de la documentación cuando se realicen cambios en el software.

h. Auditoria

El licenciatario tiene derecho a realizar auditorías para verificar que el uso del software se ajusta a las condiciones del contrato.

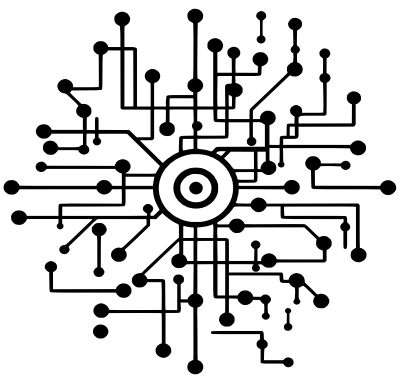


PARÁGRAFO 1

El soporte técnico es de nivel avanzado por la experiencia especializada, resolución de problemas complejos y acceso a herramientas especializadas. Para saber más sobre lo que conlleva el soporte técnico, ir al anexo técnico entregado con el contrato de licencia.

PARÁGRAFO 2

El licenciatario es el encargado de realizar las copias de seguridad. La primera copia de seguridad tendrá que ser completa, mientras que las demás que se hagan podrán ser completas o diferenciales dependiendo de lo que elija el licenciatario.



QUINTA.- GARANTÍA DE BUEN FUNCIONAMIENTO

PERIODO DE GARANTÍA

El licenciante garantiza el correcto funcionamiento del sistema de IA instalado en los sistemas de cómputo del cliente por un período de un (1) año. Este período de garantía comenzará a contar a partir de la fecha de instalación del sistema de IA.

COBERTURA DE LA GARANTÍA

El Licenciante garantiza que el software, al momento de su entrega, funcionará sustancialmente de acuerdo con la propuesta técnica proporcionada por DataHealth. Esta garantía cubre defectos materiales en el software que afecten su funcionamiento y precisión en la realización de diagnósticos y consultas.

EXCLUSIÓN DE LA GARANTÍA

La garantía no cubrirá problemas causados por:

- Uso indebido o no autorizado del sistema de IA por parte del cliente.
- Modificaciones o alteraciones al sistema de IA realizadas por el cliente sin la aprobación del desarrollador.
- Fallos del hardware del cliente o problemas de red no relacionados con el sistema de IA.
- Causas de fuerza mayor, tales como desastres naturales, actos de terrorismo, o cualquier otro evento fuera del control del desarrollador.

PROCESO DE RECLAMACIÓN

En caso de detectar un defecto o fallo sin estar dentro de las causales de exclusión, el cliente deberá notificarlo por escrito al desarrollador, realizando una descripción detallada del problema. El licenciante se compromete a responder a dicha notificación en un plazo no mayor a 20 días hábiles y a resolver el problema en el menor tiempo posible.

CONSTANCIA DE RECIBO Y REPARACIÓN

El licenciante debe expedir una constancia de recibo que indique los motivos de la reclamación. Al reparar un producto bajo garantía legal o suplementaria, debe entregar al consumidor un comprobante de reparación que incluya una descripción de la reparación, las piezas reemplazadas o reparadas, la fecha en que se entregó el producto y la fecha de su devolución.

SEXTA.- POLÍTICA DE PRIVACIDAD

El licenciatario reconoce y acepta que el uso del Software está sujeto a la Política de Privacidad del Licenciante, la cual se encuentra disponible al final del documento. La Política de Privacidad describe las prácticas del Licenciante en relación con la recopilación, uso, divulgación y protección de los Datos Personales del Usuario. El licenciante se compromete a leer y aceptar la Política de Privacidad antes de utilizar el Software.

SÉPTIMA.- LICENCIA DE FUNDADORES

En adición a los derechos otorgados en la cláusula cuarta, los licenciatarios que hayan contribuido al desarrollo de *VitalAI* mediante el suministro de datos sensibles para su entrenamiento (en adelante, "Licenciatarios Fundadores"), adquirirán un beneficio especial: un período de mantenimiento gratuito de seis (6) meses a partir de la fecha de instalación del software. Transcurrido este plazo, se aplicarán las tarifas de mantenimiento establecidas en la cláusula décimo cuarta.

OCTAVA.-PROPIEDAD INTELECTUAL

Este contrato otorga una licencia de uso del software al Licenciatario. Los derechos patrimoniales sobre el software seguirán siendo propiedad exclusiva de DataHealth. El Licenciatario reconoce y acepta que no adquiere ningún derecho patrimonial sobre el software, más allá de la licencia de uso otorgada por este contrato.

NOVENA.-PROHIBICIÓN DE CEDER A 3EROS

Queda expresamente prohibida la cesión, total o parcial, de los derechos y obligaciones derivados de este contrato por parte del Licenciatario, a cualquier título y bajo cualquier forma, sin el consentimiento previo y por escrito del Licenciante.

En caso de cesión autorizada, el cesionario asumirá todas las obligaciones del cedente y responderá solidariamente por tres (3) meses con éste frente al Licenciante por el cumplimiento de todas y cada una de las estipulaciones del presente contrato.

DÉCIMA.- RESTRICCIONES DE USO

USO EXCLUSIVO DEL PERSONAL MÉDICO

El software únicamente podrá ser utilizado por el personal médico debidamente acreditado y autorizado para realizar consultas y diagnósticos. Esto incluye médicos y profesionales de la salud que están habilitados para manejar datos sensibles y tomar decisiones clínicas basadas en los resultados proporcionados por el software.

MANEJO DE DATOS SENSIBLES

El personal médico autorizado que utilice el software debe adherirse a todas las normativas y regulaciones aplicables en materia de protección de datos sensibles y privacidad del paciente. El software debe ser utilizado de manera que garantice la seguridad, confidencialidad e integridad de la información del paciente en todo momento.

CAPACITACIÓN OBLIGATORIA

El personal médico que utilice el software deberá recibir capacitación adecuada y continua sobre el manejo y uso del software, así como sobre la correcta gestión de datos sensibles y la protección de la privacidad del paciente. La capacitación debe será realizada por personal cualificado y aprobado de parte de DataHealth.

FINALIDAD DE USO

El software no podrá ser modificado, descompuesto, desensamblado, ni utilizado para fines distintos a los previstos en la licencia. Cualquier uso indebido, alteración o intento de modificación del software constituirá una violación de los términos de la licencia y podrá resultar en la rescisión de la misma.

El incumplimiento de las restricciones establecidas en esta cláusula puede resultar en la revocación inmediata de la licencia

DÉCIMA PRIMERA.- OBLIGACIONES DEL LICENCIANTE

Instalación del software

El Licenciante se obliga a proporcionar el software objeto de esta licencia, diseñado para realizar diagnósticos y consultas precisas mediante inteligencia artificial, entrenada con datos de diversas disciplinas médicas y métodos de diagnóstico.

Actualizaciones y mantenimiento

El Licenciante se obliga a proporcionar todas las actualizaciones y mejoras del software que se desarrollen durante el período de vigencia de la licencia. Estas actualizaciones incluirán mejoras en la funcionalidad, la seguridad y la precisión del software. Además, el Licenciante ofrecerá servicios de mantenimiento para asegurar el correcto funcionamiento del software.

Capacitación

El Licenciante se obliga a proporcionar capacitación inicial y continua al personal médico del Licenciatario sobre el uso adecuado del software, incluyendo la gestión de datos sensibles y la protección de la privacidad del paciente. La capacitación será impartida por personal cualificado y estará diseñada para asegurar un uso óptimo y seguro del software.

Protección de datos

El Licenciante se obliga a cumplir con todas las normativas aplicables en materia de protección de datos y confidencialidad. Cualquier información a la que el Licenciante tenga acceso durante la provisión del software y los servicios asociados será tratada con la máxima confidencialidad y se tomarán todas las medidas necesarias para protegerla.

DÉCIMA SEGUNDA.- OBLIGACIONES DEL LICENCIATARIO

Uso adecuado del software

El Licenciatario se compromete a utilizar el software únicamente para los fines previstos en este contrato, en estricto cumplimiento con las instrucciones y especificaciones proporcionadas por el Licenciante. El uso del software debe realizarse exclusivamente por el personal médico autorizado y capacitado para manejar datos sensibles y realizar diagnósticos médicos.

Protección de datos

El Licenciatario se obliga a proteger la confidencialidad e integridad de los datos sensibles compartidos por los usuarios. Ello implica un acceso limitado únicamente a las personas capacitadas para el propio manejo de ellos.

Equipos de computación

El Licenciatario deberá garantizar que los equipos de cómputo en los que se instalará y operará el software cumplan con los requerimientos técnicos mínimos especificados por el Licenciante. Además, el Licenciatario se compromete a mantener estos equipos en condiciones óptimas de funcionamiento para asegurar el correcto desempeño del software.

Capacitación

El Licenciatario se obliga a asegurar que todo el personal médico que utilice el software reciba la capacitación inicial y continua proporcionada por el Licenciante. Esta formación es esencial para garantizar un uso adecuado y seguro del software, así como para maximizar su eficiencia y precisión en los diagnósticos.

Uso adecuado del software

El Licenciatario se obliga a realizar el pago de las tarifas establecidas para la licencia del software, así como cualquier costo adicional acordado, en los plazos y términos especificados en el contrato. El incumplimiento de estas obligación puede resultar en la suspensión o revocación de la licencia.

DÉCIMA TERCERA.- DURACIÓN Y RENOVACIÓN DE LA LICENCIA

La presente licencia es temporal de manera que el licenciatario adquiere el derecho de usar el software durante un (1) año, no obstante el pago es por instalamentos es decir que deberá pagar un valor a partir de la fecha de aceptación de los términos y condiciones por parte del Licenciatario.

PARÁGRAFO: Al vencimiento de este plazo, la licencia se **renovará** automáticamente por un periodo igual, salvo que cualquiera de las partes notifique a la otra por escrito su intención de no renovarla con una antelación mínima de treinta (30) días calendario a la terminación del contrato.

DÉCIMA CUARTA.- PAGO DE LA LICENCIA

El licenciatario se obliga con el licenciante a pagarle mensualmente dentro de los tres primeros días hábiles de cada mes la suma (el precio lo decide DataHealth) por la licencia. Esta suma NO tiene incluido el IVA.

En el evento de incumplimiento de cualquiera de los pagos, la licencia se suspenderá inmediatamente hasta tanto se verifique el pago.

(Los precios señalados se pueden cambiar según como DataHealth considere, no obstante son un precio que AllianceTech recomienda como monto mínimo)

El precio mensual se aumentará el primer día del mes de enero de cada año y de manera automática de acuerdo al índice de precios del consumidor del año anterior.

El licenciante podrá modificar libremente el precio mensual de la licencia dando aviso por escrito al licenciatario con un (1) mes de anterioridad a la entrada en vigencia del nuevo precio

En ese mes el licenciatario podrá decidir si desea continuar la relación contractual en los nuevos términos.
De lo contrario se entenderá por terminado el contrato al finalizar el mes de preaviso sin penalidad alguna para el licenciatario.

PARÁGRAFO 1: El Licenciatario debe cancelar al Licenciante una tarifa mensual de mantenimiento 1322 USD por cada centro hospitalario al que se le tendrá que hacer mantenimiento. Esta tarifa comprende, entre otros, los servicios de actualización y mejora del Software, así como el soporte técnico necesario para garantizar su correcto funcionamiento y se prestará mensualmente.

PARÁGRAFO 2: Todas las sumas adeudadas en virtud del presente contrato serán pagadas en dólares estadounidenses (USD). El Licenciatario efectuará los pagos mediante transferencia bancaria a la cuenta bancaria designada por el Licenciante. Dicha cuenta bancaria será comunicada al Licenciatario por escrito posterior a la firma del presente contrato de licencia. Queda prohibido el pago en efectivo o mediante cheque.

PARÁGRAFO 3: La fecha de vencimiento para el pago de cada cuota será el día 3 de cada mes. El incumplimiento en el pago de cualquiera de las cuotas dará lugar a la constitución en mora automática del Licenciatario, sin necesidad de requerimiento judicial o extrajudicial.

Los intereses moratorios se calcularán sobre el monto adeudado a una tasa equivalente al 1.5 veces la tasa bancaria corriente (IBC) vigente a la fecha de vencimiento de cada cuota, y se devengarán desde la fecha de vencimiento hasta la fecha de pago.

DÉCIMA QUINTA.- PÓLIZA DE SEGURO ANTE DAÑOS

El licenciante durante la vigencia de este contrato se obliga a adquirir una póliza de seguro de responsabilidad civil profesional con una aseguradora solvente y de reconocida reputación, que cubra los daños y perjuicios que puedan sufrir el licenciatario, sus clientes o terceros por el uso del software. (**Esta cláusula constituye una recomendación para DataHealth de adquirir una póliza de seguro ante daños**).

DÉCIMA SEXTA.- RIESGOS

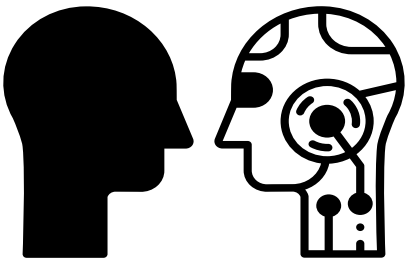
Riesgo	Descripción	Impacto	Medidas de mitigación
Fallos técnicos	Posibles fallos en el funcionamiento del software debido a errores de programación o problemas técnicos.	Interrupción del servicio o prestación de servicio deficiente	Soporte técnico y actualizaciones regulares proporcionadas por el Licenciante.
Uso indebido	Uso del software por personal no autorizado o para fines distintos a los establecidos en el contrato.	Vulneración a la integridad personal de los usuarios pacientes	Capacitación adecuada y restricciones de acceso implementadas por el Licenciatario.
Dependencia de proveedor	Imposibilidad que tiene el licenciatario de modificar el sistema por si solo	Interrupción del servicio	Implementación de sistemas de mantenimiento continúo 24/7 y de visitas periódicas para vitar daños y problemas de funcionamiento
Fallos del Hardware	Problemas en los equipos de cómputo donde se instala el software, afectando su funcionamiento.	No funcionamiento del software	Mantenimiento regular de los equipos y requisitos técnicos claros para la instalación del software.
Confidencialidad de datos	Riesgo de divulgación no autorizada de datos sensibles manejados por el software.	Vulneración de datos sensibles	Acuerdos de confidencialidad y políticas de manejo de datos estrictas implementadas por el Licenciatario.

DÉCIMA SÉPTIMA.- RESPONSABILIDAD DEL LICENCIANTE

a. No otorgar la licencia

Si el licenciante no otorga al licenciatario los derechos de uso acordados, este último puede rescindir el contrato y reclamar una indemnización por los daños y perjuicios sufridos.

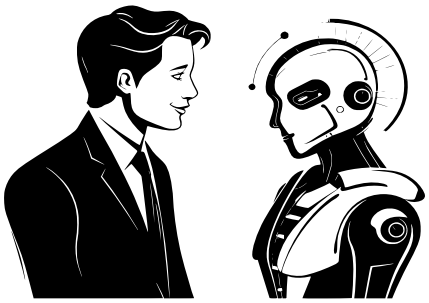
b. Entregar un software defectuoso

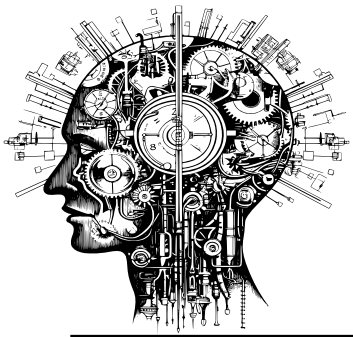


Si el software entregado no funciona correctamente o tiene errores, el licenciante se compromete a corregir cualquier defecto en el Software dentro de un plazo razonable a partir de la notificación por escrito del licenciatario. Si no se corrige en un plazo razonable, el licenciante será responsable de reparar los defectos o de indemnizar al licenciatario por los daños causados.

c. Incumplimiento de las obligaciones de soporte técnico:

Si el licenciante no proporciona el soporte técnico acordado, el licenciatario puede reclamar una indemnización por los daños causados por la falta de asistencia.



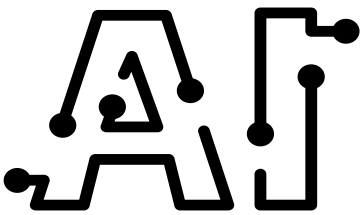


d. Violación de la confidencialidad

Si el licenciante revela información confidencial del licenciatario, puede ser responsable de los daños causados por dicha divulgación.

e. Violación a derechos de autor

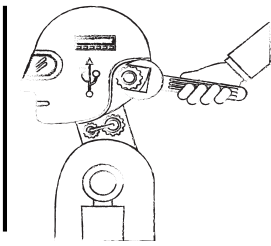
El Licenciante será responsable de cualquier reclamación, demanda, pérdida, daño o gasto que surja de cualquier reclamación de terceros alegando que el Licenciante no tiene el derecho a otorgar la licencia o que el Software infringe los derechos de propiedad intelectual de terceros.

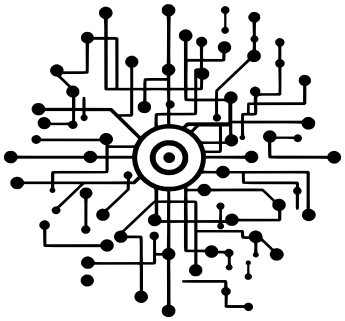


DÉCIMA OCTAVA.- RESPONSABILIDAD DEL LICENCIATARIO

a. Dar un uso incorrecto

El Licenciatario será el único responsable por el uso que haga del Software y por cualquier daño o perjuicio que pueda causar a terceros como consecuencia de dicho uso, e indemnizará y mantendrá indemne al Licenciante de cualquier reclamación, demanda, pérdida, daño o gasto que surja del uso indebido del Software por parte del Licenciatario.



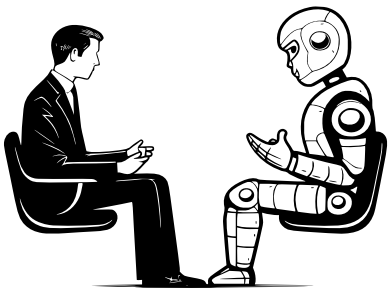


b. No hacer copias de seguridad

El Licenciatario será el único responsable de realizar copias de seguridad de todos los datos y cualquier otra información relacionada con el uso del Software. El Licenciante no será responsable por la pérdida o daño de dichos datos.

c. Manipulación del código fuente sin autorización

El Licenciatario será responsable en caso de que realice ingeniería inversa, modifique o manipule el código fuente sea directa o indirectamente sin autorización del licenciante.



d. Violación de la confidencialidad

Si el licenciatario revela información confidencial del licenciante o del software VitalAI, puede ser responsable de los daños causados por dicha divulgación.

DÉCIMA NOVENA.- LIMITE DE RESPONSABILIDAD

A. Se establece que el licenciante solo será responsable por los daños causados intencionalmente o por una negligencia grave.

B. El Licenciante no será responsable por ningún daño causado a terceros como consecuencia del uso del Software por parte del Licenciatario.

C. El Licenciatario deberá notificar por escrito al Licenciante cualquier defecto en el Software inmediatamente después de tener conocimiento del mismo, de lo contrario se liberará al licenciante de cualquier responsabilidad.

D. Se excluye la responsabilidad por daños indirectos o que no sean consecuencia inmediata del incumplimiento.

E. Se excluye la responsabilidad por la pérdida de ganancias futuras que el cliente hubiera obtenido de no haberse producido el incumplimiento.

PARÁGRAFO En ningún caso, la responsabilidad total del Licenciante excederá el monto de los pagos realizados por el Licenciatario durante los seis (6) meses anteriores al evento que dio lugar a la reclamación.

VIGÉSIMA.- TERMINACIÓN DEL CONTRATO

a. ***Por vencimiento del plazo***. Cuando la duración del contrato esté por cumplirse, el licenciatario deberá dar un preaviso de 30 días calendario para dar por terminado el contrato, de lo contrario se entenderá por renovado.
b. ***Incumplimiento de las obligaciones***: Si alguna de las partes incumple alguna de las obligaciones estipuladas en el contrato, la otra parte puede tener derecho a rescindirlo y si es el caso, pedir indemnización por daños y perjuicios causados.
c. ***Resolución judicial***: Un juez puede declarar la nulidad o rescisión del contrato si se demuestra que existe alguna causa legal para ello, como un vicio en el consentimiento o un incumplimiento grave de las obligaciones.
d. ***Preaviso:*** Cualquiera de las partes podrá dar por terminado el presente contrato dando un preaviso de treinta (30) días calendario de anticipación a la otra parte.
e. ***Defectos graves e irreparables***: Si el software presenta errores o defectos que impiden su uso de manera significativa y el licenciante no logra solucionarlos en un plazo razonable, el licenciatario podría tener derecho a rescindir el contrato.
g. ***Desacuerdo en el aumento del precio de la licencia***. Si el licenciante modifica el precio de la licencia y el licenciatario no está de acuerdo, puede darse la terminación del contrato sin penalidad alguna. No aplica en caso de aumentarse el precio automáticamente.
PARÁGRAFO 1: En caso de que el licenciatario dé el preaviso para poder terminar el contrato, estará obligado a pagar el precio mensual hasta la fecha de la efectiva terminación del contrato. En caso de que el licenciante sea quien dé el preaviso, estará obligado a pagar los daños y perjuicios que conlleve la terminación del contrato.
PARÁRAFO 2: La causal de terminación por preaviso se da en los casos en que no exista incumplimiento de alguna de las partes, de lo contrario se rige por la cláusula que comprende la terminación por incumplimiento.

VIGÉSIMA PRIMERA.- CONSENCUANCIAS DE LA TERMINACIÓN DEL CONTRATO

a. ***Cesación de los derechos***: Al finalizar el contrato, el licenciatario pierde el derecho a utilizar el software de acuerdo con las condiciones establecidas.
b. ***Obligación de devolución***: El licenciatario puede estar obligado a devolver al licenciante cualquier copia del software.
c. ***Pago de indemnizaciones***: Si la terminación del contrato se debe a un incumplimiento, la parte responsable debe pagar una indemnización a la parte perjudicada.

VIGÉSIMA SEGUNDA.- MECANISMOS DE SOLUCIÓN DE CONFLICTOS

Amigable Composición:

Toda controversia o diferencia relativa a este contrato se resolverá a través de un panel de amigable composición que funcionará en el Centro de Arbitraje y Conciliación de la Cámara de Comercio de Bogotá, de conformidad con el Reglamento de Amigable Composición de dicho Centro. Si no se llega a un acuerdo en un plazo de dos meses desde la solicitud, las partes podrán proceder al arbitraje según se describe a continuación.

VIGÉSIMA TERCERA- CLÁUSULA COMPROMISORIA.

Toda controversia o diferencia que se derive de este contrato se resolverá por un Tribunal Arbitral que sesionará en el Centro de Arbitraje y Conciliación de la Cámara de Comercio de Bogotá, de acuerdo con las siguientes reglas:

1. El Tribunal estará integrado por 1 árbitro.
2. El árbitro será designado por las partes de común acuerdo. En caso de que no sea posible, será designado por el Centro de Arbitraje y Conciliación de la Cámara de Comercio de Bogotá, a solicitud de cualquiera de las partes.
3. El procedimiento se sujetará a los reglamentos que para tal fin disponga el mencionado Centro de Arbitraje y se aplicarán de conformidad con los criterios que en ellos se establezcan.
4. El Tribunal decidirá en derecho.

VIGÉSIMA CUARTA.- LEY Y JURISDICCIÓN APLICABLE

Este contrato se regirá por las leyes de la República de Colombia, sin perjuicio de las normas de derecho internacional privado como lo es el HIPAA, RGPD y el AI ACT, en lo que concierte a protección de datos, protección al consumidor y reglamento para el uso de IA.

Para la resolución de cualquier controversia derivada del presente contrato, las partes se someten a la jurisdicción de los tribunales de Bogotá, Colombia. En caso de existir alguna discrepancia entre la versión en español y cualquier otra versión de este contrato, prevalecerá la versión en español.

POLÍTICA DE PRIVACIDAD

De: DataHealth Solutions S.A.

Podemos actualizar esta Política de Privacidad periódicamente. Le notificaremos cualquier cambio material

En DataHealth Solutions S.A., valoramos la privacidad de nuestros usuarios y nos comprometemos a proteger sus datos personales. Esta Política de Privacidad describe cómo recopilamos, utilizamos, divulgamos y protegemos la información personal que obtenemos a través de nuestro software VitalAI.

DATOS QUE RECOPILAMOS

- ***Información de identificación***: Nombre, dirección de correo electrónico, número de teléfono.
- ***Datos de salud***: Información médica relevante para el uso del software, como historial clínico, resultados de pruebas, etc. (Siempre con el consentimiento informado del paciente).
- ***Datos de uso***: Información sobre cómo se utiliza el software, como frecuencia de acceso, funciones utilizadas, etc.

CÓMO UTILIZAMOS LOS DATOS

- ***Proporcionar el servicio***: Para ofrecer el software VitalAI y sus funcionalidades.
- ***Personalización***: Para personalizar la experiencia del usuario y ofrecer recomendaciones relevantes.

Utilizamos los datos personales recopilados con los siguientes fines:

- ***Mejora del software***: Para analizar los datos de uso y mejorar el software.
- ***Cumplimiento legal***: Para cumplir con las obligaciones legales aplicables.

DIVULGACIÓN DE DATOS

Podemos compartir sus datos personales con:

- ***Proveedores de servicios***: Con empresas que nos ayudan a prestar nuestros servicios (por ejemplo AllianceTech S.A.S. o quien haga el mantenimiento).
- ***Autoridades competentes***: En caso de que sea requerido por ley o para proteger nuestros derechos.

SEGURIDAD DE LOS DATOS

Implementamos medidas de seguridad técnicas y organizativas adecuadas para proteger sus datos personales de pérdidas, accesos no autorizados, divulgación, copia, uso o modificación no autorizados.

SUS DERECHOS

- ***Acceder***: Solicitar una copia de sus datos personales.
- ***Rectificar***: Solicitar la corrección de datos inexactos.
- ***Suprimir***: Solicitar la eliminación de sus datos personales.
- ***Portabilidad***: Solicitar la transferencia de sus datos a otro responsable del tratamiento.

Anexo: Documento Técnico

Sofia Castro Cortes
Aura Yazmin Cristancho Gómez
Miguel Ángel Espinosa Rico
Danna Gabriela Quintana Suarez
Daniela Jaimes Cano

Mentores. Anabel Riaño Saad y Juan Felipe Navia Revollo

Universidad Externado de Colombia
Facultad de Derecho
Concurso.

Bogotá, Colombia.
29 de julio de 2024

1. Introducción

1.1 Contextualización

En el mundo actual, la inteligencia artificial (IA) ha demostrado ser una herramienta esencial para mejorar la eficiencia y precisión en diversos campos, incluido el sector salud. La implementación de IA en la medicina permite la optimización de diagnósticos, tratamientos personalizados y la gestión eficiente de grandes volúmenes de datos médicos. La adopción de estas tecnologías no solo mejora la calidad de los servicios de salud, sino que también facilita una atención más rápida y precisa a los pacientes.

El proyecto VitalAI surge como una solución innovadora para el análisis y gestión de datos médicos, ofreciendo un sistema de inteligencia artificial diseñado para integrarse con las infraestructuras de salud existentes. Este sistema tiene como objetivo principal mejorar los procesos de diagnóstico y tratamiento mediante el uso de tecnologías avanzadas de aprendizaje automático y procesamiento de datos.

1.2 Concurso

Los equipos deberán asumir el reto de presentar, de manera escrita y oral, el diseño de una estrategia tecnológica, de negocio y legal que dé solución efectiva al caso planteado.

1.3 Caso para resolver

El caso planteado en el concurso requiere desarrollar una solución de inteligencia artificial que pueda integrarse de manera eficiente con las infraestructuras de salud existentes, facilitando la gestión y análisis de grandes volúmenes de datos médicos. El sistema debe ser capaz de:

1. Recopilar y procesar datos médicos de diversas fuentes, garantizando la seguridad y privacidad de la información.

2. Utilizar algoritmos avanzados de aprendizaje automático para analizar los datos y proporcionar diagnósticos y recomendaciones de tratamiento precisos.

3. Integrarse con los sistemas de información de salud (HIS) existentes, permitiendo una interoperabilidad sin problemas.

4. Cumplir con todas las normativas y regulaciones vigentes en cuanto a la protección de datos personales y la seguridad de la información.

5. Proporcionar un sistema de soporte y mantenimiento continuo para asegurar su funcionamiento óptimo a lo largo del tiempo.

Alliancetech ha desarrollado el proyecto VitalAI para abordar estos desafíos. El sistema está diseñado para ser flexible y escalable, permitiendo su adaptación a diferentes entornos de salud y necesidades específicas. Además, se han implementado medidas de seguridad

robustas para garantizar la protección de los datos médicos y cumplir con todas las normativas legales pertinentes.

2. Objetivos del Proyecto

El proyecto VitalAI tiene como finalidad desarrollar una solución innovadora y eficiente que permita optimizar la gestión y análisis de datos médicos mediante el uso de inteligencia artificial. Esta solución busca no solo mejorar la precisión y rapidez en los diagnósticos y tratamientos, sino también garantizar la seguridad y privacidad de la información médica, cumpliendo con todas las normativas legales vigentes. Los objetivos específicos del proyecto son los siguientes:

2.1 Objetivo General

Desarrollar una plataforma de inteligencia artificial que integre la gestión y análisis de datos médicos, mejorando los procesos de diagnóstico y tratamiento en los centros de salud, y garantizando la seguridad y privacidad de la información conforme a las normativas vigentes.

2.2 Objetivos Específicos

2.2.1 Recopilación y Procesamiento de Datos

Diseñar e implementar mecanismos eficientes para la recopilación y procesamiento de datos médicos provenientes de diversas fuentes, asegurando la integridad y calidad de la información. Esto incluye la integración de tecnologías como HTML, CSS, JavaScript, Django, Talend Data Integration y Amazon RDS (MySQL) para la adecuada gestión de la información.

2.2.2 Análisis de Datos y Diagnóstico

Desarrollar algoritmos avanzados de aprendizaje automático y procesamiento de datos que permitan analizar grandes volúmenes de información médica y proporcionar diagnósticos y recomendaciones de tratamiento precisos. El uso de TensorFlow y otras herramientas de inteligencia artificial será crucial para el entrenamiento y optimización de estos algoritmos.

2.2.3 Interoperabilidad con Sistemas de Salud

Garantizar que la plataforma de inteligencia artificial pueda integrarse de manera eficiente con los sistemas de información de salud (HIS) existentes, permitiendo una interoperabilidad sin problemas. Esto incluye la configuración y uso de instancias de Amazon EC2, Amazon S3 y Amazon EBS para asegurar la escalabilidad y flexibilidad del sistema.

2.2.4 Seguridad y Privacidad de la Información

Implementar medidas de seguridad robustas para garantizar la protección de los datos médicos recopilados y procesados, cumpliendo con todas las normativas y regulaciones vigentes en cuanto a la protección de datos personales y la seguridad de la información. El uso de herramientas como OpenSSL, KMS, IAM y MFA será esencial para asegurar la confidencialidad e integridad de la información.

2.2.5 Soporte y Mantenimiento Continuo

Establecer un sistema de soporte y mantenimiento continuo para asegurar el funcionamiento óptimo de la plataforma de inteligencia artificial a lo largo del tiempo. Esto incluye la implementación de servicios como CloudWatch Logs, planes de soporte empresarial de AWS y medidas de autoescalado para ajustar automáticamente la capacidad de computación según la demanda.

2.2.6 Formación y Capacitación

Desarrollar programas de formación y capacitación para los usuarios del sistema, asegurando que el personal médico y administrativo de los centros de salud pueda utilizar la plataforma de manera efectiva y segura. Esta formación incluirá tanto aspectos técnicos como normativos relacionados con el uso de la inteligencia artificial en la medicina.

2.2.7 Colaboración y Acuerdos Comerciales

Fomentar la colaboración con centros de salud y otras instituciones relevantes mediante la celebración de acuerdos comerciales y la suscripción de cartas de intención. Estos acuerdos permitirán a AllianceTech recopilar datos reales y entrenar el sistema de inteligencia artificial en un entorno controlado, ofreciendo a los centros de salud participantes una licencia especial para el uso de VitalAI sin costos adicionales durante los primeros seis meses.

3. Planificación del Proyecto

La planificación del proyecto VitalAI se desarrolla en varias fases cuidadosamente estructuradas, cada una con actividades específicas y objetivos claros para asegurar la entrega exitosa del sistema. Esta planificación abarca desde la preparación inicial de la infraestructura hasta la implementación y el seguimiento del sistema en producción. A continuación, se describe detalladamente cada fase del proyecto, considerando las dos opciones de infraestructura: servidores propios de Alliancetech y servicios de Amazon Web Services (AWS).

3.1 Fases del Proyecto

El proyecto VitalAI consta de cuatro fases principales:

1. Fase de Preparación
2. Fase de Desarrollo y Entrenamiento
3. Fase de Implementación
4. Fase de Práctica y Seguimiento

3.1.1 Fase de Preparación

Esta fase inicial se centra en la preparación de la infraestructura necesaria para el desarrollo y despliegue efectivo de la inteligencia artificial (IA) y la página web asociada. Los objetivos de esta fase incluyen la configuración de servidores, la adopción de sistemas de seguridad para el almacenamiento y tratamiento de datos sensibles, y el establecimiento de políticas internas para el manejo de estos datos. La infraestructura se puede implementar usando servidores propios de Alliancetech o los servicios en la nube de AWS.
Objetivos de la Fase de Preparación:

- Configuración de Servidores: Establecimiento de la infraestructura de servidores necesaria para soportar el desarrollo y la operación de VitalAI. Esto incluye la configuración de servidores físicos o virtuales con capacidades adecuadas para el procesamiento de datos y el entrenamiento de modelos de IA.

- Adopción de Sistemas de Seguridad: Implementación de medidas de seguridad iniciales para proteger los datos sensibles durante el almacenamiento y procesamiento. Esto incluye el uso de cifrado, autenticación multifactor (MFA), y sistemas de gestión de identidades y accesos (IAM).

- Políticas Internas: Desarrollo de políticas internas para el tratamiento adecuado de datos sensibles, asegurando el cumplimiento con normativas de protección de datos y privacidad.

Actividades Principales:

- Opción 1: Servidores Propios de Alliancetech
    - **Configuración de Servidores:**
        - Adquisición de hardware de servidores de alto rendimiento con procesadores Intel Xeon Gold y GPUs NVIDIA Tesla V100.
        - Instalación y configuración de sistemas operativos (Linux) y software base.
        - Configuración de redes y sistemas de almacenamiento, incluyendo almacenamiento SSD de alta velocidad.
    - **Implementación de Seguridad Inicial:**
        - Configuración de cifrado para datos en reposo y en tránsito.
        - Implementación de sistemas IAM y MFA para el control de acceso.
        - Configuración de sistemas de monitoreo y registro de eventos (CloudWatch Logs).
- Opción 2: Servicios en la Nube de AWS
    - **Configuración de Servidores:**
        - Selección y configuración de instancias de Amazon EC2, incluyendo instancias de alto rendimiento como EC2 r5.2xlarge y EC2 P3.2xlarge.
        - Configuración de servicios de almacenamiento como Amazon S3 y Amazon EBS.
        - Configuración de servicios de bases de datos como Amazon RDS (MySQL).
    - **Implementación de Seguridad Inicial:**
        - Configuración de cifrado utilizando AWS Key Management Service (KMS).
        - Implementación de sistemas IAM y MFA para el control de acceso.
        - Configuración de sistemas de monitoreo y registro de eventos (AWS CloudWatch).
- **Establecimiento de Políticas Internas:**

- Desarrollo de políticas de tratamiento de datos sensibles.
- Capacitación del personal en las políticas y procedimientos de seguridad.
- Implementación de medidas de cumplimiento con normativas de protección de datos.

Plazo:

- Duración: 2 meses a partir de la celebración del contrato.

Responsabilidades:

- Alliancetech: Responsable de la configuración técnica, implementación de seguridad, y desarrollo de políticas internas.

3.1.2 Fase de Desarrollo y Entrenamiento

Esta fase se centra en el desarrollo de la plataforma de inteligencia artificial y el entrenamiento de los algoritmos con los datos médicos recopilados. El objetivo es crear un sistema funcional y eficiente capaz de analizar grandes volúmenes de datos y proporcionar diagnósticos precisos.
Objetivos de la Fase de Desarrollo y Entrenamiento:

- **Desarrollo del Software**: Creación de la plataforma de IA utilizando lenguajes de programación y frameworks adecuados. Esto incluye el desarrollo de interfaces de usuario, algoritmos de IA, y componentes backend.

- **Entrenamiento de Modelos de IA:** Utilización de datos médicos reales para entrenar los modelos de IA. Esto incluye la selección de conjuntos de datos, preprocesamiento de datos, y ajuste de hiperparámetros para optimizar el rendimiento de los modelos.

- Validación y Optimización: Evaluación del rendimiento de los modelos de IA y realización de ajustes necesarios para mejorar la precisión y eficiencia del sistema.

Actividades Principales:

- **Desarrollo del Software:**

  - Programación de interfaces de usuario utilizando HTML, CSS, JavaScript, y frameworks como Django.
  - Desarrollo de algoritmos de IA utilizando plataformas como TensorFlow.
  - Implementación de componentes backend para la gestión de datos y procesamiento de IA.

- **Entrenamiento de Modelos de IA:**

  - Recolección y preprocesamiento de datos médicos.
  - Entrenamiento de modelos de IA utilizando infraestructura de AWS (Amazon EC2, Amazon S3) o servidores propios.
  - Ajuste de hiperparámetros y evaluación de modelos para optimizar el rendimiento.

- **Validación y Optimización:**

  - Pruebas de rendimiento y precisión de los modelos de IA.
  - Ajustes y optimizaciones basadas en los resultados de las pruebas.

- Documentación de los procesos y resultados del entrenamiento.

Plazo:

- Duración: 4 meses tras la fase de preparación.

Responsabilidades:

- Alliancetech: Desarrollo de algoritmos y entrenamiento de IA.
- DataHealth: Proporcionar datos necesarios para el entrenamiento y colaborar en la validación.

3.1.3 Fase de Implementación

La fase de implementación se enfoca en la integración de la plataforma de IA en los sistemas de información de salud (HIS) de los centros de salud participantes. Se asegurará que el sistema esté completamente operativo y accesible para los usuarios finales.
Objetivos de la Fase de Implementación:

- Integración con HIS: Conectar la plataforma de IA con los sistemas de información de salud existentes en los centros de salud.

- Implementación de Seguridad Adicional: Asegurar que todas las medidas de seguridad estén en su lugar para proteger los datos durante la operación del sistema.

- Configuración Final y Pruebas: Realizar configuraciones finales y pruebas exhaustivas para garantizar que el sistema funcione correctamente y cumpla con los requisitos.

Actividades Principales:

- **Integración con HIS:**
  - Desarrollo de interfaces de integración para conectar la plataforma de IA con los HIS.
  - Configuración de APIs y otros mecanismos de integración.
  - Pruebas de integración para asegurar la compatibilidad y funcionalidad.

- **Implementación de Seguridad Adicional:**
  - Revisión y fortalecimiento de las medidas de seguridad.
  - Configuración de firewalls, sistemas de detección y prevención de intrusiones (IDS/IPS).
  - Monitoreo continuo de seguridad y ajuste de configuraciones.

- **Configuración Final y Pruebas:**
  - Ajustes finales de configuración del sistema.
  - Pruebas de funcionamiento, rendimiento y usabilidad.
  - Documentación de configuraciones y resultados de pruebas.

Plazo:

- Duración: 2 meses tras la fase de desarrollo y entrenamiento.

Responsabilidades:

- Alliancetech: Integración técnica y pruebas de funcionamiento.
- DataHealth: Supervisión de la integración y retroalimentación para ajustes necesarios.

3.1.4 Fase de Práctica y Seguimiento

En esta fase, se llevará a cabo la formación de los usuarios del sistema, el monitoreo del funcionamiento del sistema en un entorno real y la realización de ajustes necesarios para asegurar su eficacia. Además, se establecerán mecanismos de soporte y mantenimiento continuo.

Objetivos de la Fase de Práctica y Seguimiento:

- Capacitación de Usuarios: Proveer formación completa a los usuarios finales para asegurar que puedan utilizar el sistema de manera efectiva.
- Monitoreo del Funcionamiento: Evaluar el rendimiento y la funcionalidad del sistema en un entorno real de operación.
- Ajustes y Mejoras: Realizar los ajustes necesarios para resolver cualquier problema y optimizar el sistema basado en el feedback de los usuarios y el monitoreo.

Actividades Principales:

- **Capacitación de Usuarios:**
  - Desarrollo de materiales de formación y manuales de usuario.
  - Realización de sesiones de formación para diferentes perfiles de usuario.
  - Evaluación de la comprensión y competencia de los usuarios en el uso del sistema.
- **Monitoreo del Funcionamiento:**
  - Configuración de herramientas de monitoreo para evaluar el rendimiento del sistema.
  - Análisis de logs y métricas para identificar problemas y áreas de mejora.
  - Reuniones periódicas con usuarios para obtener feedback sobre el funcionamiento del sistema.
- **Ajustes y Mejoras:**
  - Implementación de ajustes y correcciones basadas en el monitoreo y feedback.
  - Optimización continua del sistema para mejorar rendimiento y usabilidad.
  - Documentación de ajustes realizados y resultados obtenidos.

Plazo:

- Duración: 2 meses tras la fase de implementación.

Responsabilidades:

- Alliancetech: Provisión de formación, monitoreo y soporte técnico.
- DataHealth: Facilitar la implementación, proporcionar feedback y participar en la evaluación del sistema.

3.2 Recursos y Herramientas

Para la correcta ejecución de cada fase del proyecto, se utilizarán diversos recursos y herramientas tecnológicas. Estas incluyen servidores de alto rendimiento, software especializado para el desarrollo y entrenamiento de IA, y sistemas de seguridad avanzados para la protección de datos. Entre las herramientas clave se encuentran:

- **Hardware:**
    - **Opción 1:** Servidores Propios de Alliancetech
        - Servidores con procesadores Intel Xeon Gold y GPUs NVIDIA Tesla V100.
        - Almacenamiento SSD de alta velocidad.
        - Infraestructura de enfriamiento y energía adecuada.
    - **Opción 2:** Servicios en la Nube de AWS
        - Instancias de Amazon EC2 de alto rendimiento, como EC2 r5.2xlarge y EC2 P3.2xlarge.
        - Servicios de almacenamiento como Amazon S3 y Amazon EBS.
        - Servicios de bases de datos como Amazon RDS (MySQL).
- **Software:**
    - **Lenguajes y Frameworks de Desarrollo:**
        - HTML, CSS, JavaScript, Django para el desarrollo de interfaces de usuario.
        - TensorFlow para el desarrollo de algoritmos de IA.
        - Talend Data Integration para la integración y procesamiento de datos.
    - **Servicios de Seguridad y Monitoreo:**
        - AWS Key Management Service (KMS) para cifrado de datos.
        - AWS CloudWatch para monitoreo y registro de eventos.
        - Sistemas de gestión de identidades y accesos (IAM) y autenticación multifactor (MFA).

Responsabilidades en la Adquisición y Configuración:

- Alliancetech: Se encargará de la adquisición, instalación y configuración del hardware y software necesario para el proyecto, asegurando que todos los componentes estén optimizados para el desarrollo y operación de VitalAI.
- DataHealth: Proveerá los requisitos específicos y colaborará en la definición de políticas de seguridad y tratamiento de datos.

4. Estudio de Mercado

El estudio de mercado es una fase crucial para el proyecto VitalAI, ya que permite comprender las necesidades, expectativas y comportamientos del mercado objetivo. Este estudio proporciona datos esenciales que guiarán el desarrollo y la implementación del sistema, asegurando su relevancia y aceptación en el sector de la salud.

4.1 Análisis del Mercado Objetivo

El análisis del mercado objetivo se centra en identificar y comprender a los principales actores del sector de la salud que se beneficiarán del sistema VitalAI. Este análisis incluye:

4.1.1 Segmentación del Mercado

- **Segmentación Geográfica:**
    - Identificación de las regiones con mayor demanda de sistemas de inteligencia artificial en salud.
    - Análisis de la infraestructura tecnológica y capacidades de los centros de salud en estas regiones.
- **Segmentación Demográfica:**
    - Identificación de los principales usuarios del sistema (médicos, administradores de salud, pacientes).
    - Análisis de las características demográficas relevantes (edad, género, nivel educativo, especialización médica).

4.1.2 Análisis de la Competencia

- **Identificación de Competidores Directos e Indirectos:**
    - Evaluación de otros sistemas de inteligencia artificial y soluciones tecnológicas en el mercado de la salud.
    - Análisis de las características y funcionalidades de los productos competidores.

4.2 Necesidades y Expectativas del Cliente

La identificación de las necesidades y expectativas del cliente es fundamental para asegurar que VitalAI satisfaga las demandas del mercado y proporcione un valor significativo a sus usuarios.

4.2.1 Identificación de Necesidades

- **Requisitos Funcionales:**
    - Identificación de las funcionalidades esenciales que los usuarios esperan de un sistema de inteligencia artificial en salud.
    - Análisis de las características técnicas y operativas necesarias para cumplir con estos requisitos.
- **Requisitos de Usabilidad:**
    - Evaluación de la facilidad de uso y accesibilidad del sistema para los usuarios finales.

- Identificación de las preferencias de los usuarios en cuanto a la interfaz y experiencia de usuario.

- **Requisitos de Seguridad y Privacidad:**

  - Análisis de las expectativas de los usuarios respecto a la protección de datos personales y médicos.

  - Identificación de las normativas y estándares de seguridad aplicables al sistema.

5. Tratamiento de Datos

Para que la Inteligencia Artificial funcione, se debe ingresar una extensa base de datos médicos que abarca desde ciencias básicas como anatomía, fisiología y genética, a conocimientos clínicos y especialidades médicas como cardiología, neurología, oncología, dermatología, ginecología, entre otras. Aparte de esto, se ingresarán otro tipo de datos para complementar la información y que la Inteligencia Artificial de un diagnóstico más preciso. Datos que señalen si por vivir en cierto lugar, mantener un cierto estilo de vida las personas pueden ser más propensas a sufrir de algunos tipos de enfermedades.

Asimismo, la Inteligencia Artificial tendrá una trazabilidad de los datos de los pacientes. Lo anterior significa que se debe ingresar información detallada de la persona como, por ejemplo: altura, peso, sexo, género, grupo sanguíneo, viajes frecuentes, domicilio, estilo de vida, alimentación, frecuencia con la que hace deporte, si tiene enfermedades hereditarias, o enfermedades preexistentes, si se ha operado, si ha estado hospitalizado, si dona sangre, la frecuencia con la que asiste al médico, su información sexual y reproductiva, entre otras preguntas.

La anterior información será utilizada con el único fin de que la IA sea capaz de proponer diagnósticos precisos, tratamtientos completos, aconseje medicamentos y que también se pueda utilizar como una historia clínica de la persona.

Para asegurar la privacidad, seguridad se detalla a continuación las obligaciones, responsabilidades y procedimientos relacionados con el tratamiento de datos, asegurando el cumplimiento de todas las normativas legales y estándares técnicos.

5.1 Obligaciones y Responsabilidades

5.1.1 Obligaciones del Desarrollador

1. Recopilación de Datos:

Legalidad y Transparencia: Alliancetech debe garantizar que todos los datos personales sean recopilados de manera lícita, justa y transparente, cumpliendo con la normativa vigente en materia de protección de datos.
Consentimiento Informado: Obtener los consentimientos necesarios de los titulares de los datos, asegurando que comprendan el propósito y el uso de su información, mediante formularios de consentimiento claro y detallado.

2. Seguridad de los Datos:

Medidas Técnicas y Organizativas: Implementar medidas adecuadas para proteger los datos personales contra pérdida, robo, acceso no autorizado, divulgación, alteración y destrucción. Estas medidas incluyen el cifrado de datos en reposo y en tránsito, autenticación de múltiples factores (MFA), y control de acceso basado en roles (RBAC).

Cifrado de Datos: Utilizar algoritmos de cifrado robustos, como AES-256 para datos en reposo y TLS 1.2 o superior para datos en tránsito, asegurando que los datos sensibles estén protegidos en todo momento.

Auditorías de Seguridad: Realizar auditorías de seguridad periódicas, incluyendo pruebas de penetración y revisiones de código, para identificar y corregir vulnerabilidades en el sistema.

Copias de Seguridad: Mantener copias de seguridad regulares y seguras de todos los datos personales en infraestructuras separadas y protegidas contra accesos no autorizados.

3. Tratamiento de Datos:

Uso Exclusivo para el Proyecto: Asegurar que los datos personales sean utilizados únicamente para los fines especificados en el proyecto VitalAI. Cualquier otro uso debe ser aprobado explícitamente por los titulares de los datos.

Minimización de Datos: Recopilar y procesar únicamente los datos necesarios para el cumplimiento de los objetivos del proyecto, evitando el almacenamiento de información innecesaria.

Almacenamiento Seguro: Utilizar infraestructuras seguras para el almacenamiento de datos, garantizando que los servidores sean protegidos contra accesos no autorizados y ciberataques.

4. Documentación y Conformidad:

Políticas de Seguridad: Documentar todas las políticas de seguridad y procedimientos implementados, asegurando su conformidad con las normativas legales y estándares de la industria**.**

Registros de Consentimiento: Mantener registros detallados de todos los consentimientos informados obtenidos de los titulares de datos, asegurando la trazabilidad y auditoría de los procesos de consentimiento.

5.1.3 Medidas de Seguridad

1. Datos en Reposo:

Cifrado: Los datos almacenados en los servidores de Alliancetech o AWS deben estar cifrados utilizando algoritmos de cifrado robustos, como AES-256.
Seguridad Física: Asegurar que las instalaciones donde se almacenan los

servidores cumplan con altos estándares de seguridad física, incluyendo controles de acceso y vigilancia.

2. Datos en Tránsito:

Cifrado de Tráfico: Todo el tráfico de datos entre los centros de salud, Alliancetech y AWS debe estar cifrado utilizando protocolos seguros como TLS 1.2 o superior.
VPN: Utilización de redes privadas virtuales (VPN) para proteger las conexiones de red y garantizar la seguridad de los datos en tránsito.

3. Gestión de Identidades y Accesos (IAM):

Autenticación Multifactor (MFA): Implementar autenticación multifactor para todos los usuarios que accedan a los sistemas que contienen datos personales.
Roles y Permisos: Definir roles y permisos claros para asegurar que los usuarios tengan acceso únicamente a los datos necesarios para sus funciones.

4. Monitorización y Auditoría:

Monitoreo Continuo: Implementar sistemas de monitoreo continuo para detectar actividades sospechosas y potenciales amenazas en tiempo real.
Auditorías Regulares: Realizar auditorías de seguridad periódicas para revisar la eficacia de las medidas de protección y realizar mejoras continuas.

5. Respuesta a Incidentes:

Planes de Contingencia: Desarrollar y mantener planes de contingencia para responder a incidentes de seguridad, incluyendo brechas de datos y ciberataques.

Notificación de Incidentes: Notificar de manera inmediata a los responsables de tratamiento y a las autoridades competentes en caso de cualquier incidente que afecte la seguridad de los datos personales.

5.1.4 Responsabilidades de los Centros de Salud Licenciatario

1. **Recolección de Datos:**

Consentimiento Informado: Asegurar que los datos personales se recopilen con el consentimiento informado de los pacientes.

Seguridad de la Información: Implementar medidas de seguridad para proteger los datos recopilados antes de transferirlos a Alliancetech.

2. **Transferencia de Datos:**

Protocolos Seguros: Utilizar métodos seguros para la transferencia de datos a Alliancetech, asegurando que los datos en tránsito estén protegidos contra accesos no autorizados.

5.1.5 Monitoreo y Evaluación

1. Indicadores de Rendimiento:

Definición de KPI: Establecer indicadores clave de rendimiento (KPI) para monitorear el progreso y la eficacia de las medidas de tratamiento de datos.

Revisión Periódica: Realizar revisiones periódicas de los KPI para evaluar el desempeño y hacer ajustes necesarios.

2. Informes Periódicos:

Reportes de Seguridad: Generar y distribuir informes periódicos sobre el estado de seguridad de los datos y el cumplimiento de las políticas de tratamiento de datos.

Evaluaciones de Riesgo: Realizar evaluaciones de riesgo regulares para identificar y mitigar posibles amenazas a la seguridad de los datos.

6. Inteligencia Artificial

6.1 Selección de Instancias

La selección adecuada de instancias es crucial para el éxito del proyecto VitalAI. Las instancias deben ser capaces de manejar grandes volúmenes de datos y ejecutar modelos de aprendizaje automático de manera eficiente.

Tipos de Instancias:

GPU (Unidad de Procesamiento Gráfico): Se utilizarán instancias con GPUs para acelerar el entrenamiento de modelos de aprendizaje profundo. Ejemplos incluyen instancias P3 de Amazon Web Services (AWS) y A100 de Google Cloud Platform (GCP).

CPU (Unidad Central de Procesamiento): Se seleccionarán instancias de alto rendimiento con múltiples núcleos para el preprocesamiento de datos y la ejecución de algoritmos de aprendizaje automático que no requieran GPUs. Ejemplos incluyen instancias C5 de AWS y N1 de GCP**.**

Criterios de Selección:

Costo-Eficiencia: Evaluación del costo en relación con el rendimiento proporcionado.
Escalabilidad: Capacidad de ajustar los recursos según la demanda.

Compatibilidad: Soporte para herramientas y frameworks de IA como TensorFlow, PyTorch y Scikit-learn.

6.2 Almacenamiento

El almacenamiento seguro y eficiente de los datos médicos es esencial para el éxito de VitalAI.

Soluciones de Almacenamiento:

Almacenamiento en la Nube: Servicios como Amazon S3, Google Cloud Storage y Azure Blob Storage proporcionarán almacenamiento escalable y seguro.

Bases de Datos: Se emplearán bases de datos relacionales (PostgreSQL) para datos estructurados y bases de datos NoSQL (MongoDB) para datos no estructurados, asegurando flexibilidad y rendimiento.

Estrategias de Almacenamiento:

Replicación de Datos: Implementación de replicación de datos para asegurar alta disponibilidad y recuperación ante desastres.

6.3 Seguridad

La seguridad es una prioridad máxima en la gestión de datos médicos. Se implementarán medidas robustas para proteger la integridad y confidencialidad de la información.

6.3.1 Encriptación de Datos

En Reposo: Los datos serán encriptados utilizando AES-256.

En Tránsito: Se empleará TLS (Transport Layer Security) para proteger los datos durante su transmisión.

6.3.2 Autenticación y Autorización

Autenticación Multifactor (MFA): Añadirá una capa extra de seguridad para el acceso a sistemas críticos.

Autorización Basada en Roles (RBAC): Gestionará permisos según los roles de los usuarios dentro de la organización.

6.3.3 Monitoreo y Auditoría

Sistemas de Monitoreo: Herramientas como AWS CloudWatch, Google Stackdriver o Azure Monitor serán utilizadas para detectar actividades anómalas y generar alertas.

Auditoría de Acceso: Mantendremos registros detallados de accesos y actividades para asegurar la trazabilidad y cumplimiento normativo.

6.3.4 Garantía y Soporte

Soporte Técnico 24/7: Disponibilidad de un equipo de soporte para resolver incidencias.

Actualizaciones de Seguridad: Implementación de actualizaciones regulares para proteger contra nuevas vulnerabilidades.

6.4 Desglose Técnico y Presupuestal por Fases

El proyecto VitalAI se llevará a cabo en tres fases principales, cada una con sus propias necesidades técnicas y presupuestarias.

6.4.1 Fase 1: Preparación e Implementación Inicial

Actividades:

- Selección y configuración de instancias.
- Configuración inicial de almacenamiento y seguridad.
- Despliegue inicial de modelos de IA.

6.4.2 Fase 2: Ajustes y Optimización

Actividades:

- **Optimización de modelos de IA y configuraciones de instancias.**
  Mejora en la seguridad y monitoreo del sistema.
- **Capacitación del personal y pruebas de rendimiento.**

6.4.3 Fase 3: Mantenimiento y Soporte Continuo

Actividades:

- **Mantenimiento regular y actualizaciones de seguridad.**
- **Soporte técnico continuo y resolución de incidencias.**
- **Evaluación continua y mejora del sistema.**

6.5 Enseñanza de la IA

6.5.1Diseño de la Arquitectura de la IA

1. Arquitectura de Redes Neuronales.

El diseño de la arquitectura de la IA es el núcleo de este proyecto. Para obtener un sistema sólido, intuitivo y capaz de analizar datos complejos se realizará de la siguiente forma.

2. Red Neuronal Convolucional (CNN)

Para el análisis de imágenes diagnósticas como rayos X y resonancias magnéticas se cuenta con una red neuronal convolucional (CNN) con 50 capas convolucionales, que es donde se realizan la mayoría de los cálculos y aproximadamente 20 millones de parámetros. Las capas principales incluirán capas de activación ReLU, capas de agrupamiento (pooling) y capas totalmente conectadas (fully connected).

La razón detrás de la elección de una CNN para este propósito se debe a la capacidad de estas redes para captar características espaciales en las imágenes. Las capas convolucionales actúan como filtros que extraen características importantes de las imágenes, como bordes, texturas y patrones. Al aumentar el número de capas convolucionales, la red puede aprender características más complejas y abstractas a diferentes niveles de la imagen. La activación ReLU introduce no linealidades en la red, permitiendo que aprenda funciones más complejas mientras que las capas de agrupamiento reducen la dimensionalidad de los datos, lo que ayuda a disminuir la carga computacional y a controlar el sobreajuste. Las capas totalmente conectadas, al final de la red, son responsables de tomar las características extraídas y realizar la clasificación final.

3. Red Neuronal Recurrente (RNN)

Para el análisis de secuencias temporales en registros electrónicos de salud, desarrollamos una red neuronal recurrente (RNN) utilizando capas LSTM (Long Short-Term Memory). Esta red consta de 30 capas LSTM y alrededor de 10 millones de parámetros, lo que permitirá capturar dependencias a largo plazo en los datos secuenciales.

Las RNN son adecuadas para datos secuenciales porque pueden mantener una memoria de entradas anteriores, lo que es esencial para tareas donde el contexto a lo largo del tiempo es importante. Las LSTM, en particular, son un tipo avanzado de RNN que pueden aprender y recordar dependencias a largo plazo más eficazmente que las RNN estándar, gracias a su diseño especial de células que gestionan el flujo de información. La elección de 30 capas LSTM y 10 millones de parámetros permitió a la red capturar patrones temporales complejos y dependencias a largo plazo en los datos de salud, como la evolución de los signos vitales y las respuestas a tratamientos a lo largo del tiempo.

6.5.2 Monitoreo y Evaluación

Para asegurarnos de que el modelo de IA funciona correctamente y continuara mejorando, implementaremos un sistema de monitoreo y evaluación continuo de la siguiente forma.

1. **Ajustes iterativos.**

Esta segunda fase también puede demorarse entre tres (3) meses y cinco (5) meses. En este punto, se realizarán ajustes iterativos basados en las métricas de rendimiento obtenidas. Se evalúan

continuamente la precisión, recall y F1-score del modelo, ajustando hiperparámetros como la tasa de aprendizaje, el tamaño del lote y el número de épocas para optimizar el rendimiento.

2. Evaluación Continua del Rendimiento

El objeto principal de esta fase es evaluar continuamente el rendimiento del modelo utilizando métricas clave. Las métricas que utilizamos son: precisión, recall y F1-score.

- **Precisión**: Esta métrica indica la proporción de verdaderos positivos entre el total de predicciones positivas realizadas por el modelo. En otras palabras, mide cuán precisa es la IA cuando identifica casos positivos en el sector de la salud. Un ejemplo de lo anterior puede ser cuando con la siguiente información: fiebre, dolor de cabeza, escalofríos, cansancio y saber que el paciente viajó en el último mes, la IA diagnostica malaria.

- **Recall**: El recall mide la capacidad del modelo para identificar correctamente todas las instancias relevantes. Es la proporción de verdaderos positivos entre el total de casos que son realmente positivos.

- **F1-score**: El F1-score es la media armónica entre la precisión y el recall. Esta métrica proporciona un balance entre ambas, especialmente útil cuando necesitamos un modelo que tenga un buen desempeño en ambas áreas y no solo en una.

Al evaluar estas métricas, podemos identificar las áreas donde el modelo necesita mejoras y enfocarnos en ajustarlas para lograr un mejor rendimiento general.

3. Ajuste de Hiperparámetros

Para optimizar el rendimiento del modelo, se realizarán ajustes iterativos en varios hiperparámetros clave, considerando la experiencia y especialidad de varios médicos en cada especialización de la medicina.

- **Tasa de Aprendizaje**: La tasa de aprendizaje determina la velocidad a la que el modelo ajusta sus parámetros en respuesta a los errores. Si la tasa de aprendizaje es demasiado alta, el modelo puede saltar por encima del mínimo óptimo, mientras que, si es demasiado baja, el proceso de entrenamiento puede ser excesivamente lento.

- **Tamaño del Lote**: El tamaño del lote se refiere al número de muestras de datos que el modelo procesa antes de actualizar sus parámetros. Un tamaño de lote mayor puede hacer que el modelo aprenda de manera más estable, pero puede requerir más memoria y tiempo de procesamiento. Por otro lado, un tamaño de lote más pequeño puede hacer que el modelo aprenda más rápido, pero con mayor variabilidad**.**

- **Número de Épocas**: Las épocas son el número de veces que el modelo pasa por todo el conjunto de datos durante el entrenamiento. Un mayor número de épocas permite que el modelo aprenda más de los datos, pero también aumenta el riesgo de sobreajuste. La experiencia con la configuración de IAs, ha sido muy buena con el número de épocas a la cual exponemos en esta fase.

7. Propuesta de Servicios mediante Amazon AWS

7.1 Favorabilidad

Amazon Web Services (AWS) ofrece una plataforma de servicios en la nube que es ideal para el proyecto VitalAI debido a sus características de escalabilidad, seguridad, redundancia y disponibilidad. A continuación se detallan estos aspectos y cómo contribuyen al éxito del proyecto.

7.1.1 Escalabilidad

La escalabilidad es una de las principales ventajas de utilizar AWS. Permite ajustar los recursos informáticos según la demanda, lo que es crucial para manejar grandes volúmenes de datos médicos y realizar análisis complejos.

- **Auto Scaling:** AWS Auto Scaling permite ajustar automáticamente la capacidad de las instancias de EC2 (Elastic Compute Cloud) para mantener un rendimiento predefinido a un costo mínimo. Esto es esencial para adaptarse a las variaciones en la carga de trabajo sin intervención manual.

- **Elastic Load Balancing (ELB):** ELB distribuye el tráfico de aplicación entrante automáticamente entre múltiples instancias, asegurando que cada instancia tenga una carga de trabajo manejable y equilibrada.

- **Amazon S3 y Amazon RDS:** Servicios como Amazon S3 (Simple Storage Service) y Amazon RDS (Relational Database Service) permiten escalar el almacenamiento y las bases de datos de manera eficiente según las necesidades del proyecto.

7.1.2 Seguridad

La seguridad es una prioridad en el manejo de datos médicos. AWS proporciona múltiples capas de seguridad para proteger la información y cumplir con las normativas de salud.

- **AWS Identity and Access Management (IAM):** IAM permite gestionar el acceso a los servicios y recursos de AWS de manera segura. Con IAM, se pueden definir y gestionar roles y políticas de acceso detalladas para asegurar que solo usuarios autorizados puedan acceder a los datos sensibles.

- **Encriptación:** AWS ofrece encriptación tanto en reposo como en tránsito. Amazon S3 y Amazon RDS permiten la encriptación de datos en reposo usando claves gestionadas por AWS Key Management Service (KMS). El tráfico de red puede ser protegido utilizando TLS (Transport Layer Security).
  AWS Shield y AWS WAF: AWS Shield ofrece protección contra ataques DDoS (Denial of Service) y AWS WAF (Web Application Firewall) protege las aplicaciones web de vulnerabilidades comunes como SQL injection y cross-site scripting.

7.1.3 Redundancia y Disponibilidad

AWS proporciona una infraestructura altamente redundante y disponible, lo que garantiza la continuidad del servicio incluso en caso de fallos.

- **Zonas de Disponibilidad y Regiones:** AWS opera en múltiples regiones y zonas de disponibilidad. Esto permite replicar y distribuir datos y aplicaciones en diferentes ubicaciones geográficas para asegurar alta disponibilidad y recuperación ante desastres.

- **Amazon Route 53:** Un servicio de DNS (Domain Name System) que permite enrutar el tráfico de usuario a las instancias de AWS más cercanas, mejorando la latencia y la disponibilidad.

- **Backups Automatizados:** Servicios como Amazon RDS y Amazon S3 ofrecen backups automatizados y recuperación a punto en el tiempo, asegurando que los datos estén siempre protegidos y disponibles.

7.2 Funcionamiento del Servicio de Servidores en AWS

El funcionamiento del servicio de servidores en AWS implica una implementación y configuración cuidadosa, seguida de una planificación estructurada por fases. Este enfoque asegura que el sistema se implemente de manera eficiente y pueda ser optimizado y mantenido adecuadamente.

7.2.1 Implementación y Configuración

La implementación y configuración inicial de los servidores en AWS implica varias etapas cruciales:

- **Selección de Instancias:** Basado en los requisitos de procesamiento y almacenamiento, se seleccionarán instancias adecuadas como EC2 para procesamiento intensivo y S3 para almacenamiento escalable.

- **Configuración de Redes:** Configuración de VPCs (Virtual Private Clouds), subredes, y grupos de seguridad para asegurar que el tráfico de red sea gestionado de manera segura y eficiente.

- **Despliegue de Aplicaciones:** Uso de servicios como AWS Elastic Beanstalk para desplegar y gestionar aplicaciones web automáticamente, ajustando la capacidad de la infraestructura según la demanda.

- **Integración de Servicios:** Configuración de servicios adicionales como AWS Lambda para ejecutar código en respuesta a eventos, y Amazon RDS para bases de datos gestionadas.

7.2.2 Planificación por Fases

La implementación del proyecto se divide en tres fases principales para asegurar una ejecución ordenada y eficiente.

7.2.2.1 Fase 1: Preparación e Implementación Inicial

Actividades:

- **Evaluación de Requisitos:** Identificación de las necesidades de procesamiento, almacenamiento y seguridad.
- **Configuración Inicial:** Selección y configuración de instancias EC2, S3, y RDS. Configuración de VPC, subredes y grupos de seguridad.
- **Despliegue de Modelos Iniciales:** Implementación de los primeros modelos de IA para pruebas iniciales.
- **Configuración de Seguridad:** Implementación de IAM, encriptación y configuraciones de seguridad básicas.

7.2.2.2 Fase 2: Ajustes y Optimización

Actividades:

- **Optimización de Recursos:** Ajuste de configuraciones de instancias y almacenamiento basados en el uso real y rendimiento.
- **Mejora de Modelos de IA:** Optimización y ajuste de los modelos de IA para mejorar su precisión y eficiencia.
- **Implementación de Herramientas de Monitoreo:** Configuración de AWS CloudWatch y otras herramientas de monitoreo para seguimiento continuo del rendimiento.
- **Capacitación del Personal**: Programas de formación para asegurar que el personal esté capacitado en el uso y gestión de AWS.

7.2.2.3 Fase 3: Mantenimiento y Soporte Continuo

Actividades:

- **Mantenimiento Regular:** Realización de mantenimientos periódicos y actualizaciones de seguridad.
- **Soporte Técnico:** Provisión de soporte técnico 24/7 para resolver incidencias y asegurar el funcionamiento continuo.
- **Evaluación y Mejora Continua:** Evaluación continua del rendimiento y la implementación de mejoras basadas en el feedback y nuevas necesidades.

8. Sistema de Detección y Prevención de Intrusiones (IDS/IPS)

8.1 Descripción y Beneficios

Un Sistema de Detección y Prevención de Intrusiones (IDS/IPS) es una tecnología de seguridad de red que monitorea el tráfico de red en busca de actividades maliciosas y puede tomar medidas para bloquear o prevenir esas actividades. Mientras que un IDS (Intrusion Detection System) solo detecta y alerta sobre actividades sospechosas, un IPS (Intrusion Prevention System) puede detectar y tomar medidas proactivas para detener dichas actividades.
Beneficios del IDS/IPS:

- **Detección Temprana de Amenazas**: IDS/IPS puede identificar y alertar sobre intentos de intrusión en tiempo real, permitiendo una respuesta rápida a posibles amenazas.

- **Prevención de Ataques:** Un IPS puede bloquear automáticamente el tráfico malicioso, protegiendo la red y los sistemas de ataques en curso.
- Visibilidad de la Red: Proporciona una visibilidad detallada del tráfico de red, ayudando a identificar patrones de ataque y comportamientos anómalos.

- **Cumplimiento Normativo:** Ayuda a cumplir con normativas de seguridad que requieren la implementación de medidas de detección y prevención de intrusiones.

- **Reducción de Riesgos:** Al identificar y mitigar amenazas de manera proactiva, reduce el riesgo de comprometer datos sensibles y sistemas críticos.

8.2 Implementación de IDS/IPS

La implementación de un sistema IDS/IPS efectivo implica una planificación cuidadosa, selección de herramientas adecuadas, y una configuración meticulosa para asegurar que el sistema funcione de manera óptima y eficaz.

8.2.1 Selección de Herramientas IDS/IPS

La selección de la herramienta IDS/IPS adecuada depende de varios factores, incluidos los requisitos de la red, el presupuesto, y las características específicas que se necesitan. Algunas de las herramientas IDS/IPS más utilizadas son:

- **Snort:** Una herramienta de código abierto ampliamente utilizada para la detección de intrusiones. Es altamente configurable y ofrece una gran flexibilidad.

- **Suricata:** Similar a Snort, es una herramienta de código abierto que proporciona capacidades avanzadas de IDS/IPS, incluyendo la inspección de paquetes a alta velocidad y análisis de tráfico.

- **Cisco Firepower:** Una solución comercial que combina IDS/IPS con características adicionales como firewall y protección avanzada contra malware.

- **Palo Alto Networks:** Ofrece un sistema de prevención de intrusiones integrado en sus firewalls de próxima generación, proporcionando una protección integral.

8.2.2 Configuración y Despliegue

La configuración y despliegue de un sistema IDS/IPS requiere una serie de pasos técnicos detallados para asegurar que el sistema esté optimizado para la red en la que se implementará.

Paso 1: Evaluación de la Red

Antes de implementar el IDS/IPS, se debe realizar una evaluación completa de la red para entender su arquitectura, tráfico típico, y puntos críticos de seguridad. Esto incluye:

- **Mapeo de la Red:** Crear un diagrama detallado de la red, identificando todos los dispositivos, segmentos de red y puntos de acceso.
- **Análisis de Tráfico**: Monitorear y analizar el tráfico de red para identificar patrones normales y anómalos.
- **Identificación de Activos Críticos:** Determinar qué activos son más críticos y vulnerables, y que requieren mayor protección**.**

Paso 2: Selección de Puntos de Implementación

Elegir los puntos estratégicos en la red donde se desplegarán los sensores IDS/IPS. Los puntos comunes incluyen:

- **Perímetro de la Red:** Monitoreo del tráfico que entra y sale de la red.
- **Segmentos de Red Internos:** Monitoreo del tráfico entre diferentes segmentos de red para detectar movimientos laterales.
- **Puntos Críticos:** Monitoreo de tráfico alrededor de servidores críticos y bases de datos.

Paso 3: Configuración de Sensores y Políticas

Configurar los sensores IDS/IPS y definir las políticas de detección y prevención:

- **Configuración de Sensores:** Instalar y configurar los sensores en los puntos seleccionados. Asegurarse de que los sensores estén optimizados para el tráfico y la arquitectura de la red.
- **Definición de Políticas:** Establecer políticas de detección que definan qué tipos de tráfico y comportamientos deben ser monitoreados y alertados. Esto puede incluir firmas de ataque conocidas, comportamientos anómalos, y patrones de tráfico sospechoso.
- **Tuning y Optimización:** Ajustar las configuraciones y políticas para minimizar falsos positivos y asegurar que el sistema responda de manera adecuada a las amenazas reales.

Paso 4: Integración con Sistemas de Gestión

Integrar el IDS/IPS con otros sistemas de gestión y respuesta a incidentes:

- **Sistemas SIEM (Security Information and Event Management):** Integrar con soluciones SIEM para correlacionar eventos de seguridad y obtener una visión completa de la seguridad de la red.

- **Herramientas de Respuesta a Incidentes:** Asegurar que el IDS/IPS esté integrado con las herramientas de respuesta a incidentes para una acción rápida y coordinada en caso de detectar una amenaza.

- **Automatización y Orquestación:** Implementar automatización para respuestas rápidas y orquestación para coordinar múltiples herramientas de seguridad.

Paso 5: Monitoreo y Mantenimiento

Establecer procesos continuos de monitoreo y mantenimiento para asegurar que el IDS/IPS funcione correctamente:

- **Monitoreo Continuo:** Supervisar el tráfico de red y las alertas generadas por el IDS/IPS en tiempo real.

- **Análisis de Alertas:** Revisar y analizar las alertas para identificar amenazas y responder de manera adecuada.

- **Actualizaciones de Firmas y Políticas:** Mantener las firmas de ataque y las políticas de detección actualizadas para proteger contra nuevas amenazas.

- **Revisión y Ajuste:** Revisar regularmente las configuraciones y políticas del IDS/IPS para mejorar su efectividad y adaptarse a los cambios en la red.

9. Implementación de Control de Acceso Basado en IP

El control de acceso basado en IP es una medida de seguridad esencial para proteger redes y sistemas de accesos no autorizados. Implementar un control de acceso efectivo implica definir políticas claras, configurar listas de acceso, y establecer procedimientos de monitoreo y respuesta. A continuación, se describe en detalle el proceso de implementación.

9.1 Definición de Políticas de Acceso

Las políticas de acceso definen las reglas que determinan qué direcciones IP pueden acceder a ciertos recursos de la red. Estas políticas deben ser claras, detalladas y adaptadas a las necesidades específicas de la organización.

- **Análisis de Necesidades:** Identificar los recursos críticos y los usuarios o sistemas que necesitan acceder a ellos. Este análisis incluye:

    - **Recursos Críticos:** Servidores de bases de datos, aplicaciones web, servicios internos.

    - **Usuarios Autorizados:** Direcciones IP de empleados, socios, proveedores de servicios externos.

    - **Segmentos de Red:** Diferentes segmentos de la red que requieren diferentes niveles de acceso.

- **Definición de Reglas de Acceso:** Establecer reglas que especifiquen qué direcciones IP pueden acceder a qué recursos. Estas reglas deben ser específicas y basadas en el principio de privilegio mínimo.
    - **Acceso Permitido:** Direcciones IP o rangos de IP que tienen permiso para acceder a ciertos recursos.
    - **Acceso Denegado:** Direcciones IP o rangos de IP que están explícitamente bloqueados.
    - **Condiciones de Acceso:** Horarios de acceso permitidos, requisitos de autenticación adicionales.
- **Documentación de Políticas:** Crear una documentación detallada de todas las políticas de acceso definidas, asegurando que estén disponibles para el equipo de seguridad y TI**.**

9.2 Configuración de Listas Blanca y Negra

Las listas blanca y negra son herramientas fundamentales para implementar el control de acceso basado en IP. La lista blanca contiene direcciones IP permitidas, mientras que la lista negra contiene direcciones IP bloqueadas.

- **Lista Blanca:**
    - **Identificación de IPs Permitidas:** Recopilar y verificar las direcciones IP que necesitan acceso a los recursos críticos. Esto incluye direcciones IP estáticas y rangos de IP.
    - **Configuración de Lista Blanca:** Utilizar firewalls, sistemas IDS/IPS y otros dispositivos de seguridad para configurar la lista blanca. Asegurarse de que solo las direcciones IP de la lista blanca puedan acceder a los recursos específicos.
    - **Revisión Periódica:** Revisar y actualizar la lista blanca regularmente para reflejar cambios en las necesidades de acceso y asegurar que solo las IP autorizadas permanezcan en la lista.
- **Lista Negra:**
    - **Identificación de IPs Maliciosas:** Recopilar direcciones IP conocidas por actividades maliciosas o no autorizadas, utilizando fuentes de inteligencia de amenazas y registros de seguridad.
    - **Configuración de Lista Negra:** Configurar la lista negra en firewalls, sistemas IDS/IPS y otros dispositivos de seguridad para bloquear el acceso desde estas direcciones IP.
    - **Actualización Dinámica:** Implementar mecanismos para actualizar la lista negra dinámicamente en respuesta a nuevas amenazas e incidentes de seguridad.

9.3 Monitoreo y Actualización

El monitoreo continuo y la actualización regular de las políticas y listas de acceso son esenciales para mantener la efectividad del control de acceso basado en IP.

- **Monitoreo en Tiempo Real:**
    - **Sistemas de Monitoreo:** Utilizar herramientas como AWS CloudWatch, Splunk, o sistemas SIEM (Security Information and Event Management) para monitorear el tráfico de red en tiempo real.
    - **Alertas y Notificaciones:** Configurar alertas para actividades sospechosas o intentos de acceso no autorizados desde direcciones IP no permitidas.
    - **Análisis de Tráfico:** Realizar análisis detallados del tráfico de red para identificar patrones y tendencias que puedan indicar intentos de intrusión.
- **Actualización de Políticas y Listas:**
    - **Revisión Regular:** Revisar las políticas de acceso y las listas blanca y negra en intervalos regulares para asegurar que reflejen las necesidades actuales y las amenazas emergentes.
    - **Automatización de Actualizaciones**: Implementar scripts y herramientas automatizadas para actualizar las listas de acceso en respuesta a nuevos datos de amenazas y cambios en la red.
    - **Feedback y Ajustes:** Recibir feedback del equipo de seguridad y TI sobre la efectividad de las políticas y hacer ajustes según sea necesario.

1.1.1. Single Sign-On (SSO) y Multifactor Authentication (MFA)

La administración de cuentas es una de las medidas más críticas para la seguridad de un sistema que maneja datos sensibles, como el sistema VitalAI. La implementación de Single Sign-On (SSO) y la autenticación multifactor (MFA) son pasos fundamentales para asegurar que solo los usuarios autorizados puedan acceder a la información confidencial.

SSO CON OKTA

Single Sign-On (SSO)

Single Sign-On (SSO) es una tecnología que permite a los usuarios acceder a múltiples aplicaciones y sistemas con una sola credencial de inicio de sesión. Esto simplifica la gestión de accesos, mejora la experiencia del usuario y reduce el número de contraseñas que los usuarios necesitan recordar. Además, disminuye la probabilidad de errores humanos y el riesgo de contraseñas débiles o reutilizadas.

Para este proyecto, se utilizará Okta, una plataforma líder en gestión de identidades y accesos. Okta proporciona una integración robusta con una amplia variedad de aplicaciones y sistemas, asegurando una experiencia de usuario fluida y segura. Okta se integrará con todas las aplicaciones

y sistemas utilizados por VitalAI. Esto incluye sistemas de información hospitalaria (HIS), registros médicos electrónicos (EMR), herramientas de análisis de datos y cualquier otro sistema relevante. Para ello, se utilizarán los conectores preconfigurados y las APIs de Okta para facilitar la integración.

La configuración de políticas de acceso estará basada en roles RBAC dentro de Okta. Esto asegura que los usuarios solo puedan acceder a las aplicaciones y datos que necesitan para realizar su trabajo. Además, se establecen políticas de tiempo de sesión y bloqueo automático después de múltiples intentos fallidos de inicio de sesión.

MFA

Implementación de MFA. Configurar Multifactor Authentication (MFA) para todos los usuarios que accedan a datos sensibles. Para ello puede utilizar métodos de autenticación robustos como aplicaciones de autenticación, tokens de hardware o biometría.

Integrar con IAM (Identity and Access Management). Usar sistemas de gestión de identidades y accesos (IAM) como Okta para asegurar la autenticación robusta y la gestión centralizada de accesos. Monitorear y auditar los intentos de acceso para detectar y responder rápidamente a posibles amenazas.
Selección de Factores de Autenticación. Utilizar una combinación de factores para la autenticación multifactor. Para VitalAI, los factores seleccionados incluirán:

- Contraseñas robustas.
- Tokens generados por aplicaciones de autenticación (como Google Authenticator o la propia aplicación de Okta).
- Autenticación biométrica (huellas dactilares, reconocimiento facial) donde sea posible.

Políticas de MFA: Definir políticas que especifiquen cuándo y cómo se requiere MFA. Por ejemplo:

- Requerir MFA en cada inicio de sesión.
- Requerir MFA después de períodos de inactividad.
- Requerir MFA para acceder a datos altamente sensibles o realizar acciones críticas.

Proceso de Autenticación.

- Cuando un usuario intenta acceder a una aplicación, primero ingresará su contraseña.
- Okta solicitará un segundo factor de autenticación, como un código temporal generado por una aplicación de autenticación o un mensaje push enviado a un dispositivo móvil.
- Una vez que se verifica el segundo factor, Okta concede el acceso al usuario.

Gestión de Incidentes y Soporte.
Establecer procedimientos claros para el manejo de incidentes relacionados con MFA, como la pérdida de un dispositivo de autenticación. Se debe proporcionar soporte técnico a los usuarios para resolver problemas relacionados con MFA, incluyendo la configuración inicial y la recuperación de acceso.

Capacitación del Personal.

- **Programas de Capacitación.**

Desarrollar programas de capacitación para educar al personal sobre la importancia de SSO y MFA, cómo utilizarlos correctamente y cómo manejar situaciones de acceso comprometido.

- **Simulacros y Ejercicios.**

Realizar simulacros de seguridad para entrenar al personal en la respuesta a incidentes relacionados con la autenticación, incluyendo la recuperación de acceso y la notificación de intentos de acceso no autorizados.

Monitoreo y Auditoría.

Monitoreo Continuo.
Configurar herramientas de monitoreo como Splunk para supervisar el uso de SSO y MFA y monitorear el acceso y actividades en los volúmenes encriptados. Okta proporciona capacidades de monitoreo integrado que permiten rastrear intentos de inicio de sesión, actividades sospechosas y el cumplimiento de políticas de seguridad. Es decir, establece alertas y notificaciones en caso de actividades sospechosas o intentos de acceso no autorizados.

Auditorías Periódicas.
Programar auditorías regulares para revisar la efectividad de los procesos de cifrado y gestión de claves. Documentar los resultados de las auditorías y realizar mejoras basadas en los hallazgos.
Plan de Recuperación de Datos.

Establecer procedimientos de recuperación.
Definir procedimientos detallados, claros y precisos para la recuperación de datos encriptados en caso de desastres o incidentes de seguridad. Documentar los pasos necesarios para restaurar los datos y validar su integridad y confidencialidad tras la recuperación. Se debe designar un equipo responsable de la recuperación de datos y proporcionarles la capacitación necesaria.

Pruebas Regulares de recuperación.
Realizar simulaciones periódicas de recuperación de datos para asegurar que los procedimientos definidos son efectivos y que el equipo está preparado. Documentar los resultados de cada simulación, identificar posibles mejoras y ajustar los procedimientos según sea necesario. Asimismo, es importante asegurar que las pruebas cubren diversos escenarios, incluyendo fallos de hardware, ataques cibernéticos y errores humanos.

Uso de Soluciones de Backup y Recuperación.
AllianceTech implementará soluciones de backup y recuperación, como Veeam Backup & Replication, para gestionar las copias de seguridad de datos encriptados. También, configurará políticas de backup que aseguren la creación regular de copias de seguridad y la retención segura de estas copias y realizará pruebas de restauración de datos a partir de las copias de seguridad para verificar su integridad y disponibilidad.

Sistema de Detección y prevención de intrusiones. (IDS/IPS)

Descripción y Beneficios.
Los sistemas de detección de intrusiones (IDS) y los sistemas de prevención de intrusiones (IPS) son herramientas críticas para monitorear, detectar y prevenir actividades maliciosas en la red. Un IDS monitorea el tráfico de la red en busca de comportamientos sospechosos y alerta a los administradores de sistemas sobre posibles intrusiones. Por su parte, un IPS no solo detecta actividades maliciosas, sino que también puede tomar medidas automatizadas para bloquearlas.

- **Gartner Magic Quadrant for Data Integration Tools* (2021). GartneR*
- *Krizhevsky, A., Sutskever, I., & Hinton, G. E. (2012). Imagenet classification with deep convolutional neural networks. *Advances in Neural Information Processing Systems*, 25, 1097-1105.*
- *Dean, J., Corrado, G., Monga, R., Chen, K., Devin, M., Mao, M., ... & Ng, A. (2012). Large scale distributed deep networks. *Advances in Neural Information Processing Systems*, 25, 1223-1231.*
- *Szegedy, C., Zaremba, W., Sutskever, I., Bruna, J., Erhan, D., Goodfellow, I., & Fergus, R. (2014). Intriguing properties of neural networks. *International Conference on Learning Representations*.*
- *Smith, M., & Jones, A. (2022). Reducing system downtime with proactive monitoring. *Gartner Research*.*
- *Simonyan, K., & Zisserman, A. (2014). Very deep convolutional networks for large-scale image recognition. *arXiv preprint arXiv:1409.1556*.*
- *Zaharia, M., Chowdhury, M., Franklin, M. J., Shenker, S., & Stoica, I. (2016). Spark: Cluster computing with working sets. *USENIX Conference on Hot Topics in Cloud Computing (HotCloud 16)*.*
- *Ng, A. (2008). Modern graphics processors far surpass the computational capabilities of multicore CPUs. Stanford University.*
- *OpenAI. (2023). AI and Compute. Retrieved from [OpenAI](https://openai.com)*
- *Agile Alliance. (2024). How AI Will Reshape Agile Development. Retrieved from [Agile Alliance](https://www.agilealliance.org)*
- *Moore, G. E. (1965). Cramming more components onto integrated circuits. *Electronics*, 38(8).*
- *Brown, T., Mann, B., Ryder, N., Subbiah, M., Kaplan, J., Dhariwal, P., ... & Amodei, D. (2020). Language models are few-shot learners. *Advances in Neural Information Processing Systems*, 33, 1877-1901.*
- *NVIDIA. (2023). Why GPUs Are Great for AI. Retrieved from [NVIDIA Blog](https://blogs.nvidia.com)*

- *RedHat. (2023). Benefits of Open Source for AI Development. Retrieved from [Redat](https://www.redhat.com)*
- *Abadi, M., et al. (2016). TensorFlow: A System for Large-Scale Machine Learning. Proceedings of the 12th USENIX Conference on Operating Systems Design and Implementation (OSDI 16), 265-283.*
- *European Commission. (2018). General Data Protection Regulation (GDPR).*
- *Kaplan, R. (2020). Evaluating the Performance and Scalability of Modern Data Centers. Journal of Data Center Management.*
- *Artículo de Revista de Derecho Informático de la Universidad de la República. (n.d.). Retrieved from https://www.sriuy.org.uy/ojs/index.php/Rdi/article/view/94*
- *Artículo de Revista de Ingeniería Biomédica de ScienceDirect. (n.d.). Retrieved from https://www.sciencedirect.com/science/article/pii/S0716864023000032*

- *Artículo de Revista de Procesamiento de Datos Médicos de ScienceDirect. (n.d.). Retrieved from https://www.sciencedirect.com/science/article/pii/S0212656720301463*
- *Artículo de Revista de Inteligencia Artificial Médica de ScienceDirect. (n.d.). Retrieved from https://www.sciencedirect.com/science/article/pii/S0716864023000032*
- *Kingma, D. P., & Ba, J. (2015). Adam: A Method for Stochastic Optimization. arXiv preprint arXiv:1412.6980.*
- *LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. Nature, 521(7553), 436-444. Hochreiter, S., & Schmidhuber, J. (1997). Long Short-Term Memory. Neural Computation, 9(8), 1735-1780.*
- *Mentz, C., et al. (2019). TensorBoard: Visualization Toolkit for Machine Learning. Journal of Machine Learning Research, 20(1), 245-251.*
- *Amazon Web Services. (2023). AWS Pricing. Retrieved from https://aws.amazon.com/pricing/*
  Mather, T., Kumaraswamy, S., & Latif, S. (2019). Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance. O'Reilly Media.
- *AWS Security Documentation. (2023). AWS Security Best Practices. Retrieved from https://docs.aws.amazon.com/security/*
- *Kaplan, R. S., & Norton, D. P. (1996). The Balanced Scorecard: Translating Strategy into Action. Harvard Business School Press*