Aplicación de la tecnología blockchain para la gestión de certificados de vacunación COVID-19 con resguardo de la identidad personal

Martín Zavala - Tutor: Gabriel Barrera

Licenciatura en Tecnologías de Información, Universidad de Palermo

***Resumen*—Este trabajo investiga la factibilidad de utilizar la plataforma *blockchain* para el almacenamiento y registro de las dosis de vacunas aplicadas en el marco de la pandemia de COVID-19. La investigación comienza con una introducción de alto nivel a la tecnología. Luego, se toman como referencia los marcos legales HIPPA y GDPR, se realiza un estudio de algunas soluciones que implementan esquemas similares y se realiza una comparación de sus características. Se propone un prototipo de aplicación móvil para implementar la funcionalidad mínima que permita evaluar la factibilidad de la solución. Se utilizará un *smart contract* para la gestión de los datos de los certificados. Finalmente se establecen los riesgos identificados y se proponen pasos para escalar la solución.**

I. Introducción

En los últimos años ha cobrado especial relevancia la toma de conciencia sobre la privacidad de los datos personales que se almacenan en línea y, particularmente, del uso que se le pueden dar a éstos y de la falta de control sobre los mismos de sus propietarios. La aparición de la pandemia de COVID-19 suma un ingrediente particular a este escenario al obligar a la población a tener que compartir sus datos médicos y personales[1] relativos a las vacunas que le fueron aplicadas usándose esta información a modo de *pasaporte sanitario*, no pudiendo negarse a compartir los mismos a riesgo de ser excluida de la vida social por el mismo Estado[2].

Este trabajo explora una alternativa para subsanar esta situación, aprovechando tecnologías existentes[3] que aseguran la inviolabilidad y anonimidad de los datos que almacena, así como también un almacenamiento descentralizado que no depende de ningún organismo de control[4]. Se trata de la tecnología *blockchain*[5].

Para ello, en la sección II se realiza una descripción de la tecnología *blockchain*[5] y cómo sus características pueden adecuarse a la solución buscada[6].

En la sección III se realiza un análisis de soluciones similares ya investigadas para tenerlas como punto de partida.

En la sección IV se investiga sobre la legislación referente al tratamiento de datos médicos. Se toman como referencia la ley HIPPA de Estados Unidos[7] y la ley GDPR de la Unión Europea[8].

En la sección V se discute la solución propuesta que incluye un *smart contract* ejecutándose sobre la *blockchain* para el almacenamiento y gestión de los datos de los certificados vacunatorios. Además, se analiza una posible aplicación móvil que contemple los casos de uso mínimos para la solución.

Finalmente, en los apéndices A, B y C se agregan diagramas de actividades UML que reflejan el análisis de la solución planteada, un conjunto de pantallas de la aplicación móvil que la implementan y un ejemplo de implementación de *smart contract* en lenguaje *Solidity*.

II. Tecnología blockchain

II-A. Conceptos básicos

Según Belotti et al., se entiende como *blockchain* a «un libro mayor compartido que lee, valida y almacena transacciones en una cadena de bloques»[6]. Los sistemas basados en esta tecnología funcionan de manera distribuida, involucrando diversos participantes que son independientes entre sí y que se comunican entre ellos formando una red entre pares: el resultado de esto es la generación de un ecosistema distribuido que no tiene una autoridad central.

Los autores identifican estos dos pilares fundamentales para la constitución de una *blockchain*: las comunicaciones entre nodos deben estar encriptadas punta a punta y debe existir un protocolo de consenso para decidir sobre la validez de las nuevas transacciones antes de sumarlas a la cadena.

En este contexto se entiende por «transacción» a una operación única e indivisible que altera el estado del sistema.

Por otro lado, se entiende «consenso» al proceso de llegar a un acuerdo entre los participantes de la red para asegurar que los datos del sistema se encuentren en un estado correcto, de manera que todos los nodos vean exactamente los mismos datos almacenados. Al tratarse de un esquema distribuido, no existe una figura que cumpla la función de árbitro, debiendo la propia red resolver estas situaciones.

Vujičić et al. presenta en la figura 1 un esquema de cómo se almacena la información en la *blockchain*: cada bloque se encuentra firmado con un par de claves pública/privada y tiene un enlace al bloque siguiente de la cadena[5]. De aquí se desprende que la cadena de bloques sólo permite agregar información, característica fundamental del esquema de libro mayor referido más arriba por Belotti et al..

También Vujičić et al. destacan otra característica fundamental: todos los nodos de la red tienen una copia de todas las transacciones dentro de la cadena, por ello es importante la existencia de un algoritmo de consenso que asegure que esos datos sean los mismos para todos los nodos.

II-B. *Privacidad*

«Los datos en la cadena de bloques son públicos para todos los nodos», remarcan Peng et al., por tanto no solamente se debe prestar especial atención en qué información del usuario queda registrada en las transacciones sino también a la manera de conocer la identidad real de dichos usuarios[9].

Para ello, los autores proponen anonimizar las identidades reales de los usuarios a través de un mecanismo de *hashing*[1]. De esta manera, no es necesario contar con un identificador de usuario fácilmente reconocible sino que basta con trabajar con estos códigos *hash* para preservar la identidad de la persona.

Los datos almacenados en los bloques, en caso de ser sensibles, pueden ser encriptados con algún otro esquema, teniendo siempre en cuenta el impacto en la performance que estas técnicas suelen tener.

II-C. *Smart contracts y Dapps*

Yano et al. definen un *smart contract* como «un protocolo computarizado de transacciones que lleva a cabo las acciones de un contrato»[10]. Se denomina *contrato* ya que constituye un acuerdo entre partes y, por otro lado, se denomina *inteligente* ya que se puede ejecutar de manera autónoma sin necesidad de intervención humana. En términos técnicos, se trata un tipo especial de programa que se ejecuta en el entorno de una *blockchain*. Los autores destacan que a pesar de utilizar el término «contrato» no necesariamente esto tiene una implicancia legal.

Estos programas se pueden utilizar como punto de acceso para las transacciones almacenadas en la *blockchain* de manera de añadir una capa de reglas de negocio para implementar controles sobre los datos gestionados.

Una manera de interactuar con un *smart contract* es a través de *Dapps* o *aplicaciones descentralizadas*, definidas por los autores como aplicaciones que «no tienen un servidor central o una entidad controlante como en el esquema cliente-servidor». Las aplicaciones convencionales, ya sean móviles o de escritorio o incluso las aplicaciones web, requieren datos para su funcionamiento. Estos datos suelen estar almacenados en servidores o bien se suelen descargar de otras fuentes u organismos. La diferencia fundamental con una *Dapp* es que ésta utiliza la *blockchain* como almacén de datos; por ende, adquiere la misma naturaleza descentralizada sobre la que se basa la *blockchain*.

La figura 2 muestra un diagrama que resume todos los componentes mencionados anteriormente.

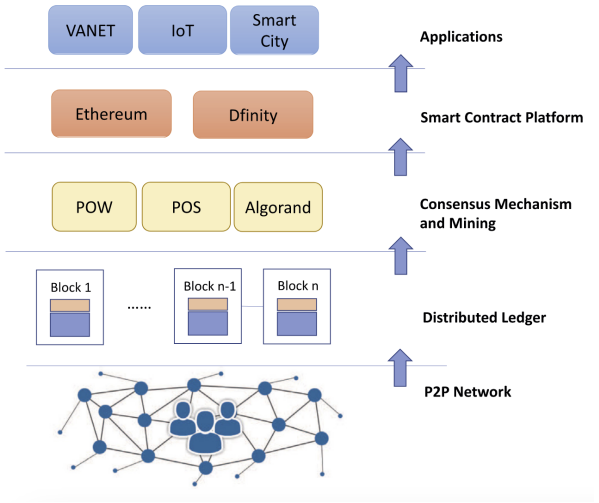


Figura 2: Arquitectura blockchain

II-D. *Implementaciones más utilizadas*

De acuerdo a Kuo et al. los elementos fundamentales de la tecnología *blockchain* que la hacen propicia para soluciones relacionadas con la salud son[11]:

- la tecnología está disponible *off the shelf*[2] lo que disminuye los tiempos de despliegue y por consiguiente los costos iniciales asociados
- la arquitectura descentralizada favorece la organización de información que proviene de diferentes organismos
- la trazabilidad de los cambios en los datos ayuda a los procesos de auditoría y verificación

Los mismos autores recopilan las plataformas más populares y realizan un estudio de sus diferentes características que se resumen en el cuadro I. También se toma en cuenta el análisis realizado por Lawton[12].

Los protocolos de consenso son:

- *Proof of work*: tiene como objetivo dificultar ataques o polución de la *blockchain*; requiere que se realice algún proceso muy costoso en términos computacionales para ser validado por la red.
- *Proof of stake*: su objetivo es validar los bloques mediante la posesión de una cantidad alta de tokens nativos de la plataforma; asume que a mayor inversión en la plataforma, mayor confianza se puede tener en ese nodo.
- *RPDCA*: basado en la confianza, cada nodo de la red elige un conjunto de validaciones diferente y son validados por otros nodos que compartan las mismas validaciones.
- *Kafka*: basado en un esquema de colas de mensajes, cada nodo puede agregar nodos a la cadena al haber sido aprobado en una cantidad mínima de mensajes de la cola.

[1]Hashing: algoritmo matemático que transforma el conjunto de datos de entrada en una expresión alfanumérica que tiene una longitud predeterminada

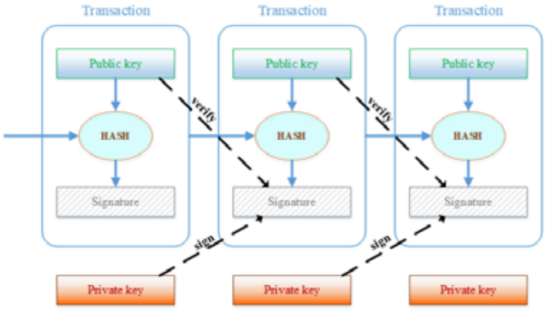


Figura 1: Estructura de una transacción

[2]Off the shelf: Disponible inmediatamente para su uso, no requiere licencias ni implementaciones

Plataforma	**Característica principal**	**Protocolo de consenso**	**Soporta *smart contracts***
Bitcoin	Primera implementación. Transacciones lentas. Alto costo energético.	PoW	No
Ethereum	Gestión automática de activos digitales. Transacciones lentas. Alto costo energético.	PoW (migrando a PoS)	Solidity
Zcash	Privacidad y anonimato	PoW (Equihash)	No
Litecoin	Tolerancia ASIC	PoW (Scrypthash)	No
Dash	Privacidad y anonimato	Proof of Service	No
Peercoin	Eficiencia energética	PoW/PoS	No
Ripple	Transacciones con baja latencia	RPDCA	No
Monero	Privacidad y anonimato	PoW (Ring CT)	No
MultiChain	Red privada	PoW (Mining Diversity)	No
Hyperledger	Red orientada a empresas. Ecosistema modular que permite el agregado de componentes. Alta privacidad en los canales de comunicación.	Kafka	Chaincode

Cuadro I: Comparativa de plataformas más utilizadas

III. Estado del arte: soluciones existentes

Karopoulos et al. [3] presentan el resultado de una investigación realizada sobre la base de aquellos países que han implementado algún mecanismo on line de gestión de certificados de COVID-19. Los resultados de esta investigación se reflejan en el cuadro II.

Iniciativa	**Entidad**	**Tecnología**
WHO Smart Vaccination Certificate	WHO	Public key based
IATA Travel Pass Iniciative	IATA	Verifiable Credentials
COVID-19 Credentials Initiative	CCI	Verifiable Credentials
EU Digital COVID Certificate	EU	Public key based
CommonPass	CPF	Public key based
AOKpass	ICC	Blockchain
Certify.health Initiative	Consortium	Blockchain
i-Covid19 certificates	BlockTack	Blockchain
IBM Digital Health Pass	IBM	Verifiable Credentials and blockchain

Cuadro II: Iniciativas de soluciones on line.

Del total de iniciativas relevadas, sólo cuatro contemplan soluciones implementadas sobre *blockchain*, ya que el esquema más habitual es utilizar combinaciones de usuario/contraseña o bien certificados de clave pública.

Un ecosistema de información médica basado en *blockchain* puede resolver la problemática del almacenamiento a largo plazo de los datos de los pacientes, según indica Magyar [13], al mismo tiempo que los protege de un uso no apropiado por parte de las empresas de explotación de datos debido a la naturaleza descentralizada y con la fuerte criptografía soportada por este tipo de soluciones.

Por otro lado, y en el contexto de tener que compartir el estado vacunatorio de las personas entre profesionales, Wang and Li [4] proponen una solución para evitar riesgos a la hora de que estos datos deban ser accedidos por distintos participantes. En la figura 3 se identifican los componentes que se deben tener en cuenta para una solución robusta.

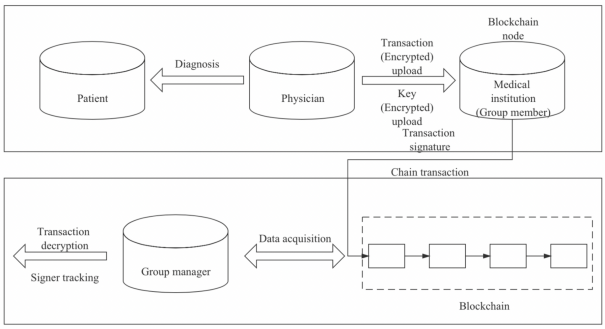


Figura 3: Modelo de solución para compartir información médica entre profesionales

El esquema propuesto por Wang and Li sugiere que todas las plataformas de las instituciones médicas participantes funcionen como nodos de consenso (ver capítulo II) a la hora de agregar nueva información en la blockchain de manera que los datos de los pacientes sólo abandonen los sistemas locales una vez encriptados.

IV. Regulaciones sobre información médica

Para analizar las implicancias legales del manejo de datos que podrían ser considerados sensibles, se toman como referencia los dos marcos legales más conocidos en la actualidad: la regulación HIPPA en Estados Unidos y la reglamentación GDPR en la Unión Europea.

IV-A. HIPPA en Estados Unidos

En los Estados Unidos de América está en vigencia desde 1996 el Acta para la Responsabilidad y Portabilidad del Seguro de Salud, también conocida como HIPPA (*Health Insurance Portability and Accountability Act*)[14], que regula el flujo de la información médica y protege la confidencialidad de los datos médicos de los ciudadanos estadounidenses. Los derechos reconocidos por esta ley son:

- ver y solicitar una copia de los registros médicos
- agregar correcciones a la información de salud
- conocer cómo la información de salud fue usada y con quién fue compartida
- elegir el uso que se le dará a la información de salud
- restringir el uso de la información para determinados propósitos
- hacer reclamos judiciales si se sospecha que algún derecho fue vulnerado

En el trabajo de Shuaib et al. se identifican como *Electronic Health Records* (EHR) a los registros médicos que se almacenan en los sistemas informáticos como información sensible[7]. Por tanto los autores concluyen que todo sistema que se ocupe del almacenamiento, procesamiento y distribución de estos registros está sujeto a la aplicación de la legislación HIPPA y deben aplicar para aprobar el proceso de certificación.

Por su parte, Antón et al. sostienen que las vulnerabilidades más comunes que se deben considerar a la hora de aplicar al proceso de certificación HIPPA son[15]:

- Contacto: cómo y por qué razón una entidad se contacta con el usuario
- Recolección de información: qué información se recoge del usuario, con o sin su consentimiento
- Monitoreo de información: cómo una entidad rastrea el comportamiento del usuario en el uso de su sistema
- Personalización de información: de qué manera un sitio web ajusta el contenido mostrado al usuario en base a la manera en que interactúa con él
- Almacenamiento de información: qué información del usuario queda registrada en las bases de datos de la aplicación
- Transferencia de información: de qué manera la información viaja de una entidad a otra
- Agregación de información: cómo se combina la información obtenida por la entidad con aquélla que provenga de otras fuentes

En la figura 4 se encuentra un análisis comparativo que cuantifica las vulnerabilidades que más se han reportado, de manera de tenerlas en cuenta a la hora de diseñar una solución que pueda ser certificada por las normas HIPPA.

IV-B. GDPR en Europa

En la Unión Europea, todos los ciudadanos tienen derecho a la protección de sus datos personales. Para ello, en el año 2018 entró en vigor el reglamento 2016/679, también conocido como GDPR (*General Data Protection Regulation*)[16]. Este reglamento establece los siguientes derechos para las personas físicas dentro de la UE:

- derecho a estar informado
- derecho de acceso
- derecho a la rectificación
- derecho a la eliminación
- derecho a la restricción del procesamiento
- derecho a la portabilidad de los datos
- derechos vinculados al perfilado de datos

Estos derechos requieren que todas las entidades que manipulen datos de ciudadanos de UE deban cumplir con la legislación establecida, dando lugar su incumplimiento a sanciones.

De acuerdo a lo indicado por Gstrein, esta reglamentación obliga a cada entidad que maneje datos sensibles de salud a realizar un diagnóstico de impacto de protección de datos (en inglés *Data Protection Impact Assessment*, DPIA) que debe ser validado por el comisario europeo de protección de datos. Si bien la reglamentación no especifica cómo debe ser ese diagnóstico, es un requisito que debe llevarse a cabo para asegurar el cumplimiento de los derechos arriba mencionados[8].

En la conclusión del análisis sobre la aplicación de este diagnóstico realizado por Hasselgren et al., los autores destacan las siguientes obligaciones que deben cumplir las entidades que quieran aprobar un DPIA[17]:

- están obligadas a asegurar que la recolección de datos sólo se realizará con un fin específico
- los propietarios de los datos siempre serán los ciudadanos
- están obligadas a informar a los ciudadanos cómo han sido utilizados sus datos dentro de un límite de tiempo prestablecido
- en caso de brechas de seguridad deben informar a los ciudadanos dentro de las 72hs de producido el incidente

Por tanto, y atendiendo a las restricciones de la propia tecnología *blockchain*, Tatar et al. encuentran los siguientes problemas a la hora de compatibilizar la tecnología con los requisitos legales[18]:

- el derecho a la eliminación de los datos (también llamado «derecho al olvido») colisiona con la inmutabilidad de los registros almacenados en la *blockchain*
- la responsabilidad del aseguramiento de la protección de los datos recae en un tercero, en este caso la red sobre la que se implementa la *blockchain*, con lo que se dificulta garantizar la transparencia del uso de los mismos

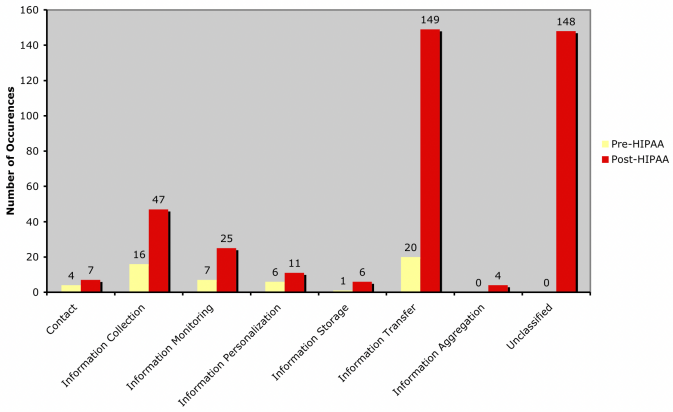


Figura 4: Clasificación de vulnerabilidades pre y post-HIPPA

- la implementación sobre nodos descentralizados dificulta procedimientos de auditoría que serían más sencillos sobre controladores de datos centralizados

Wirth and Kolain investigan sobre qué tipo de datos se consideran como datos personales y por ende sujetos al derecho al olvido en el contexto de la GDPR. Los autores sugieren que, a priori, dado que en la *blockchain* no se almacena ni el nombre ni la dirección de correo ni ningún número de identificación, no cabe dentro de la definición de datos personales[1]. Sin embargo, debe tenerse especial precaución en no realizar una correlación entre una persona concreta y su *hash* en las aplicaciones que consuman los datos almacenados en la *blockchain*.

V. Aplicación de blockchain para gestionar certificados

Como plantea Greely, la principal preocupación a la hora de instalar el requerimiento masivo de certificados de vacunación COVID es la pregunta: ¿quién y para qué lo utilizará? ¿qué organismo tendrá la responsabilidad de velar por el correcto cuidado de la información médica de los ciudadanos?[2].

Esta tesis se suma a las restricciones expuestas en la sección IV donde se observa que dentro de los derechos protegidos, tanto por la legislación HIPPA como la GDPR, se encuentra justamente la propiedad de los datos médicos personales por parte justamente del ciudadano, debiendo cada organismo interviniente velar por el correcto cuidado de dichos datos.

Es por ello que la tecnología *blockchain* se adecúa correctamente a este uso, ya que tal como se detalla en las secciones II y III, al utilizar códigos de *hash* para anonimizar a los usuarios y criptografía para almacenar la información, se enmarca en las legislaciones arriba mencionadas. Esto lo describe también Bansal et al.: «Este sistema no puede ser utilizado para extraer ninguna información de la persona sino solamente para validar la veracidad de su declaración»[19]; esto es, se utiliza la plataforma solamente para determinar la correlación entre el estado de vacunación declarado por el individuo y la información registrada en la *blockchain*.

Partiendo entonces de todas estas necesidades, se presenta a continuación el análisis de una aplicación *mobile*[3] que sirve para la gestión de los certificados digitales de vacunación y el registro y validación de los mismos.

V-A. Descripción

Se trata de una aplicación *mobile* que utiliza un código QR para presentar los datos almacenados en el certificado de vacunación. Este código podrá ser escaneado por la misma *app* para validar sus datos.

Cada usuario se identifica con un *hash* que no se encuentra vinculado con ninguna información personal; esto es, no se requiere ingresar ni un correo electrónico, ni número de DNI ni ningún otro dato que pueda ser asociado directamente con la persona.

Los diagramas de actividades correspondientes a los casos de uso se pueden consultar en el apéndice A.

[3]Aplicación *mobile*: programa informático que se ejecuta en dispositivos móviles como teléfonos inteligentes, tabletas, etc.

En la figura 5 se detallan los actores identificados y los casos de uso que conforman la solución.

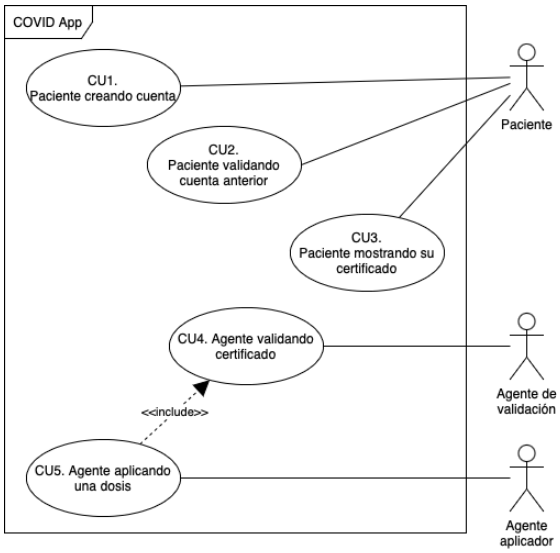


Figura 5: Diagrama de casos de uso

A los efectos de simplificar el análisis, se dejan fuera del modelado el rol y las funciones de gestión de los datos internos del sistema (alta de nuevas marcas de vacuna, alta de centro de vacunación, asignación de roles, etc).

Se identifican los siguientes roles:

- Paciente: la persona poseedora del certificado de vacunación. Todos los usuarios del sistema tienen por defecto este rol.
- Agente de validación: la persona que valida el estado de vacunación de un paciente. Se les asigna un rol específico para acceder a esta función.
- Agente aplicador: la persona que se ocupa de aplicar las dosis de la vacuna a los pacientes y de registrar en el sistema dicha aplicación. Se les asigna un rol específico para acceder a esta función.

V-B. Gestión de cuenta de usuario

Al crear una cuenta la app le mostrará al usuario un conjunto de 20 palabras aleatorias que en su conjunto forman la «frase de recuperación». Esta frase es una representación mnenotécnica del *hash* del usuario y es generado por la misma *blockchain* al solicitar el alta. En la figura 6 se observa de qué manera está conformada esta frase.

Si el usuario ya estaba registrado, en caso por ejemplo que haya tenido que reinstalar la *app* o que haya cambiado de dispositivo móvil, podrá acceder a su cuenta reingresando la frase de recuperación que le fue dada al crearla.

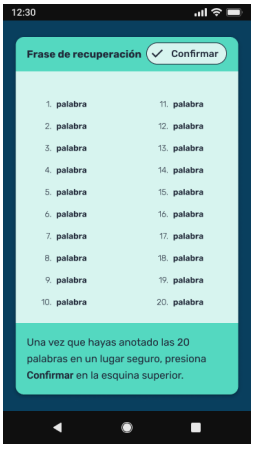


Figura 6: Frase de recuperación

V-C. *Validación de un certificado*

Para validar el certificado, el paciente debe ingresar a la *app* y automáticamente se mostrará un código QR que contiene toda la información de las dosis aplicadas (fig. 7). Este código se escanea por el agente de validación que, utilizando la misma *app* pero corriendo en otro dispositivo, lo lee a través de la cámara del dispositivo, accediendo de esta forma a los datos guardados en la *blockchain* y mostrándolos en su pantalla (fig. 8 y 9).

En caso que el código QR no sea correcto se indica con un mensaje de error.



Figura 7: Código QR



Figura 8: Escaneo del código QR



Figura 9: Validación del código QR

V-D. *Aplicación de una dosis*

Esta función la realiza el agente aplicador. Primero se debe realizar la verificación del código QR tal como se detalla en la sección anterior. Una vez validado el certificado, el agente procede a elegir los datos de la dosis aplicada y, tras confirmar la operación, los mismos se envían a la *blockchain* para ser almacenados. La *app* almacenará por defecto la fecha y la hora actuales para el registro de la dosis.

Esta pantalla de selección se observa en la figura 10.

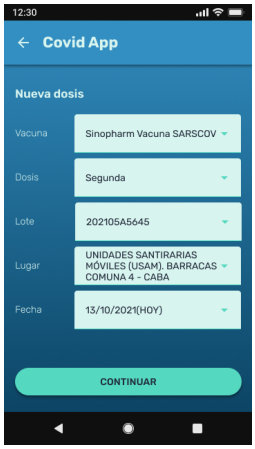


Figura 10: Registro de aplicación de dosis

V-E. *Implementación de un smart contract*

Se presenta una primera aproximación a un *smart contract* que implemente la funcionalidad mínima necesaria para el prototipo.

En éste, se implementa un mapa que asocia a cada *hash* una lista de dosis aplicadas. De esta manera queda anonimizado el paciente al que se refiere cada conjunto de dosis.

En el *smart contract* se exponen los siguientes métodos:

- constructor: se encarga de inicializar los datos del contrato y de asignarle el rol de administración al usuario que lo está instalando en la *blockchain*.

- agregarAplicador: asigna el rol de aplicar dosis al usuario indicado. Sólo lo puede ejecutar un administrador.
- eliminarAplicador: elimina el rol de aplicador del usuario indicado. Sólo lo puede ejecutar un administrador.
- obtenerAplicaciones: devuelve el listado de dosis aplicadas del usuario indicado.
- obtenerAplicacionDosis: devuelve una dosis particular del conjunto de dosis del usuario indicado.
- aplicarDosis: registra los datos de una nueva dosis aplicada al usuario indicado. Sólo lo puede ejecutar un aplicador de dosis. Emite un evento para notificar a la aplicación que la dosis fue registrada exitosamente.

El código fuente de este contrato se encuentra en el apéndice C.

VI. Conclusiones

Si bien a través de la plataforma *blockchain* se cumplen las condiciones requeridas por los marcos regulatorios relacionadas a la privacidad de los datos personales, persisten algunos riesgos que es necesario evaluar a la hora de escalar una solución como la propuesta.

En primer lugar, al haber anonimizado la identidad del usuario y asociado la misma a la frase de recuperación, existe la posibilidad que el mismo la pierda o la olvide. Esto implica necesariamente la pérdida del acesso a su información vacunatoria ya que aunque los datos siguen persistiendo en la *blockchain* no hay manera de saber a qué usuario pertenecen.

Por otro lado, al estar la plataforma descentralizada y basarse en una red entre pares, en caso que se pierdan muchos nodos se podría degradar de manera sustancial la *performance* de las consultas, haciendo que la operación de registrar nuevas dosis sea un proceso lento y se afecte la usabilidad.

También se debe considerar el tratamiento de los datos de las dosis ya aplicadas por fuera de este esquema. En ese caso se debería ejecutar un proceso global que vuelque esos datos a la *blockchain*, siendo probable que ese proceso sí deba conocer los datos personales de los usuarios, lo que cancelaría el cumplimiento de las legislaciones mencionadas.

Finalmente, si llegara a cambiar el marco regulatorio y se necesitase eliminar la información de los usuarios, esto sería imposible por la misma naturaleza de la plataforma. En este caso existen maneras de simular esta operación pero se debería contemplar desde el inicio del desarrollo.

En resumen, se debería continuar realizando una investigación de mercado para definir estos aspectos y analizar la factibilidad de la solución propuesta.

Referencias

[1] C. Wirth and M. Kolain, "Privacy by BlockChain design: A BlockChain-enabled GDPR-compliant approach for handling personal data," accepted: 2018-06-07T13:42:39Z Publisher: European Society for Socially Embedded Technologies (EUSSET). [Online]. Available: https://dl.eusset.eu/handle/20.500.12015/3159

[2] H. T. Greely, "COVID-19 immunity certificates: science, ethics, policy, and law," vol. 7, no. 1, p. lsaa035. [Online]. Available: https://doi.org/10.1093/jlb/lsaa035

[3] G. Karopoulos, J. L. Hernandez-Ramos, V. Kouliaridis, and G. Kambourakis, "A survey on digital certificates approaches for the COVID-19 pandemic," vol. 9, pp. 138 003–138 025, conference Name: IEEE Access.

[4] B. Wang and Z. Li, "Healthchain: A privacy protection system for medical data based on blockchain," vol. 13, no. 10, p. 247, number: 10 Publisher: Multidisciplinary Digital Publishing Institute. [Online]. Available: https://www.mdpi.com/1999-5903/13/10/247

[5] D. Vujičić, D. Jagodić, and S. Ranđić, "Blockchain technology, bitcoin, and ethereum: A brief overview," in *2018 17th International Symposium INFOTEH-JAHORINA (INFOTEH)*, pp. 1–6.

[6] M. Belotti, N. Božić, G. Pujolle, and S. Secci, "A vademecum on blockchain technologies: When, which, and how," vol. 21, no. 4, pp. 3796–3838, conference Name: IEEE Communications Surveys & Tutorials.

[7] M. Shuaib, S. Alam, M. Shabbir Alam, and M. Shahnawaz Nasir, "Compliance with HIPAA and GDPR in blockchain-based electronic health record."

[8] O. J. Gstrein, "The EU digital COVID certificate: A preliminary data protection impact assessment," vol. 12, no. 2, pp. 370–381, publisher: Cambridge University Press. [Online]. Available: https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/eu-digital-covid-certificate-a-preliminary-data-protection-impact-assessment/F51BABA3959C62E1EE9EFDB26D21EBB9

[9] L. Peng, W. Feng, Z. Yan, Y. Li, X. Zhou, and S. Shimizu, "Privacy preservation in permissionless blockchain: A survey," vol. 7, no. 3, pp. 295–307. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2352864819303827

[10] M. Yano, C. Dai, K. Masuda, and Y. Kishimoto, "Blockchain and crypto currency: Building a high quality marketplace for crypto data." [Online]. Available: http://link.springer.com/10.1007/978-981-15-3376-1

[11] T.-T. Kuo, H. Zavaleta Rojas, and L. Ohno-Machado, "Comparison of blockchain platforms: a systematic review and healthcare examples," vol. 26, no. 5, pp. 462–478. [Online]. Available: https://doi.org/10.1093/jamia/ocy185

[12] G. Lawton. Top 9 blockchain platforms to consider in 2022. [Online]. Available: https://www.techtarget.com/searchcio/feature/Top-9-blockchain-platforms-to-consider

[13] G. Magyar, "Blockchain: Solving the privacy and research availability tradeoff for EHR data: A new disruptive technology in health data management," in *2017 IEEE 30th Neumann Colloquium (NC)*, pp. 000 135–000 140.

[14] O. f. C. Rights (OCR). Your rights under HIPAA. Last Modified: 2022-01-19T09:45:51-0500. [Online]. Available: https://www.hhs.gov/hipaa/for-individuals/guidance-materials-for-consumers/index.html

[15] A. I. Antón, J. B. Earp, M. W. Vail, N. Jain, C. Gheen, and J. M. Frink, "An analysis of web site privacy policy evolution in the presence of HIPAA," p. 11.

[16] La protección de datos en la UE. [Online].

Available: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en
[17] A. Hasselgren, P. K. Wan, M. Horn, K. Kralevska, D. Gligoroski, and A. Faxvaag, "GDPR compliance for blockchain applications in healthcare," type: article. [Online]. Available: http://arxiv.org/abs/2009.12913
[18] U. Tatar, Y. Gokce, and B. Nussbaum, "Law versus technology: Blockchain, GDPR, and tough tradeoffs," vol. 38, p. 105454.
[19] A. Bansal, C. Garg, and R. P. Padappayil, "Optimizing the implementation of COVID-19 "immunity certificates" using blockchain," vol. 44, no. 9, p. 140. [Online]. Available: https://doi.org/10.1007/s10916-020-01616-4

GLOSARIO

blockchain
: libro mayor compartido que lee, valida y almacena transacciones en una cadena de bloques. 1, 2, 3, 4, 5, 6, 7

código QR
: código que almacena información digital en una matriz bidimensional. 5, 6

consenso
: proceso de llegar a un acuerdo entre los participantes de la red para asegurar que los datos del sistema se encuentren en un estado correcto. 1, 2, 3

Dapp
: aplicación descentralizada; no tienen un servidor central o una entidad controlante como en el esquema cliente-servidor. 2

frase de recuperación
: representación mnenotécnica del *hash* del usuario. 5, 7

hash
: expresión alfanumérica que tiene una longitud predeterminada resultante de aplicar el algoritmo de *hashing*. 2, 5, 6

hashing
: algoritmo matemático que transforma el conjunto de datos de entrada en una expresión alfanumérica que tiene una longitud predeterminada. 2

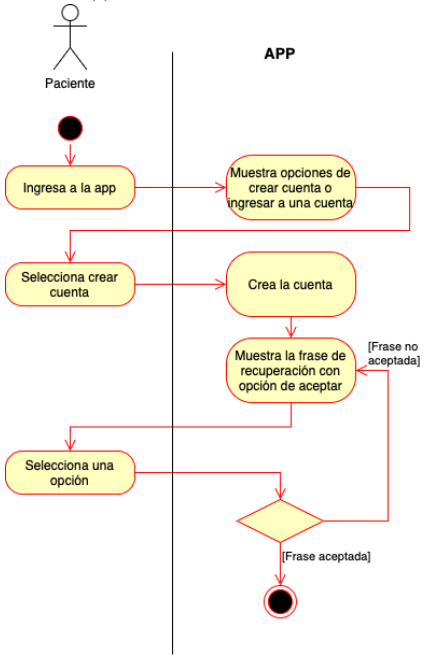
smart contract
: tipo especial de programa que se ejecuta en el entorno de una *blockchain*. 1, 2, 6

Solidity
: lenguage de programación soportado por la plataforma Ethereum, caracterizado por ser de tipado estático, orientado a contratos y de alto nivel. 1

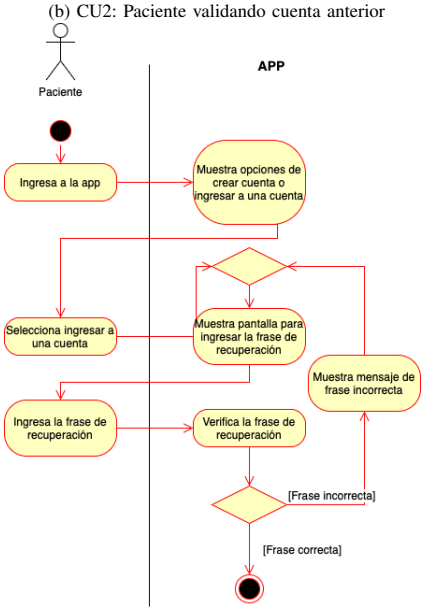
transacción
: operación única e indivisible que altera el estado del sistema. 1

APÉNDICE A
DIAGRAMAS DE ACTIVIDADES

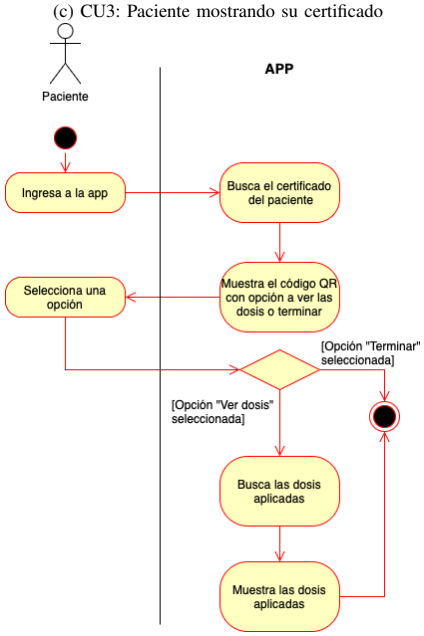
(a) CU1: Paciente creando cuenta



(b) CU2: Paciente validando cuenta anterior



(c) CU3: Paciente mostrando su certificado



(d) CU4: Agente validando certificado

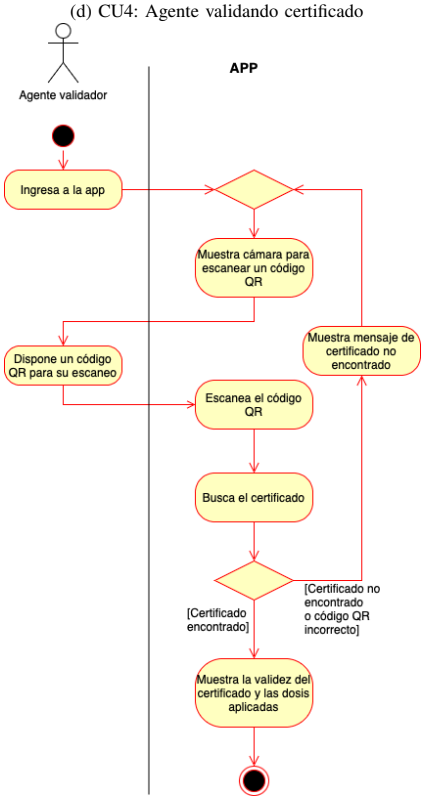
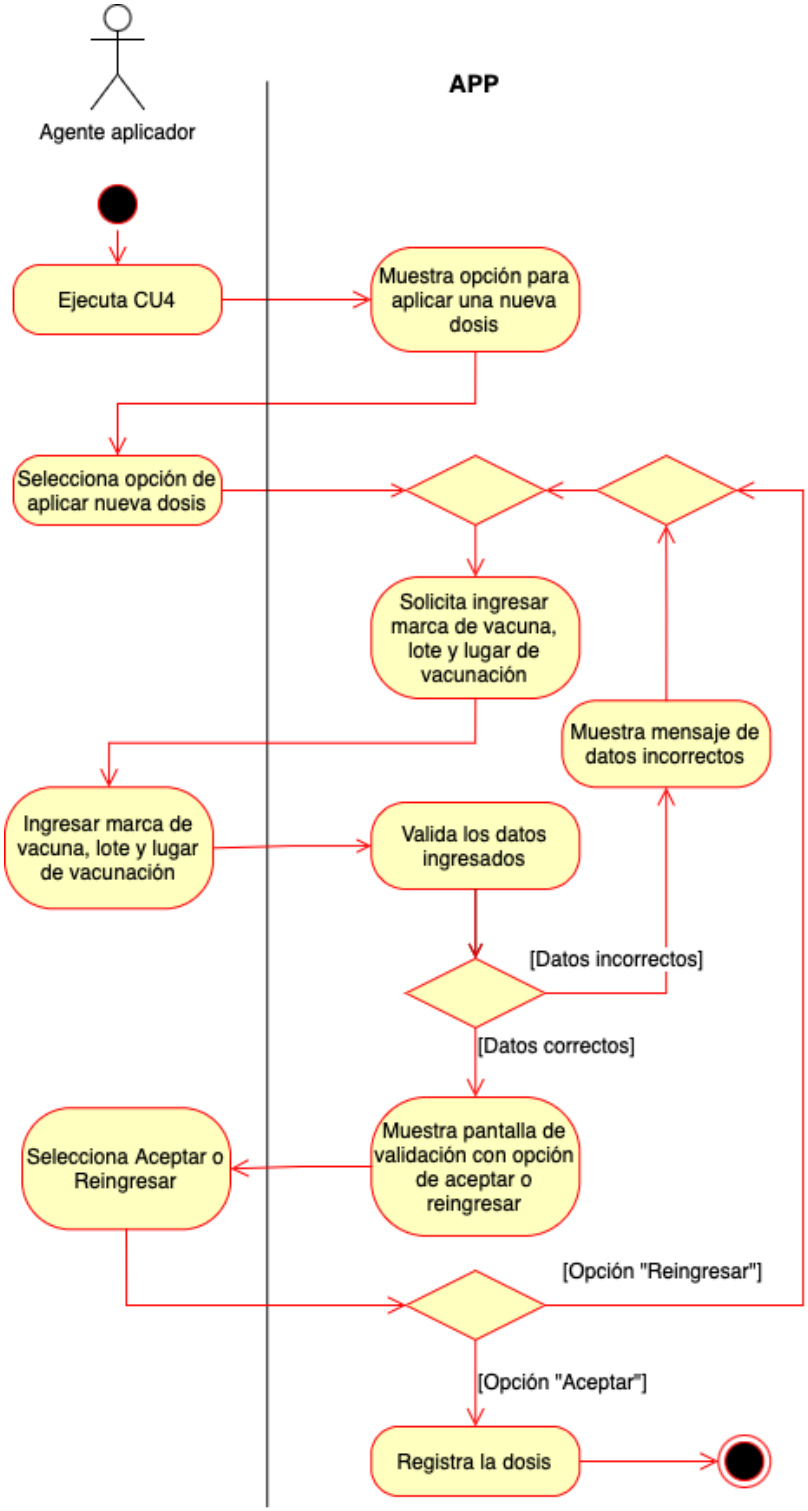


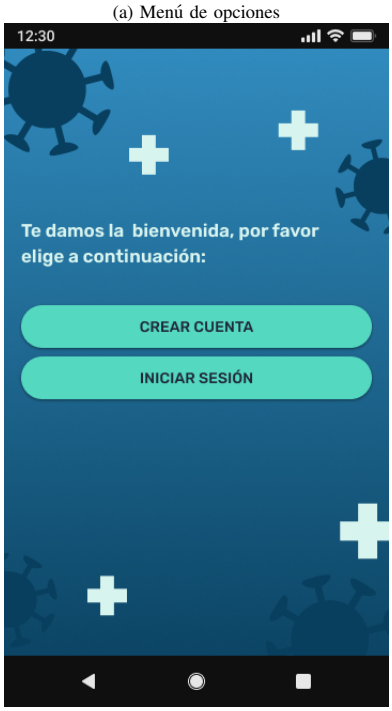
Figura 12: CU5: Agente aplicando una dosis



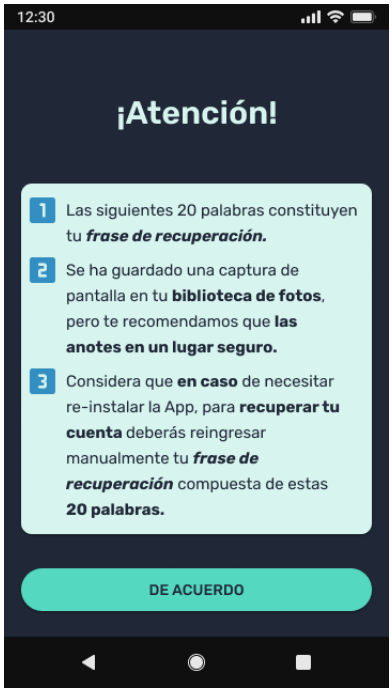
APÉNDICE B
PANTALLAS DE LA APLICACIÓN

B-A. CU1: Paciente creando cuenta

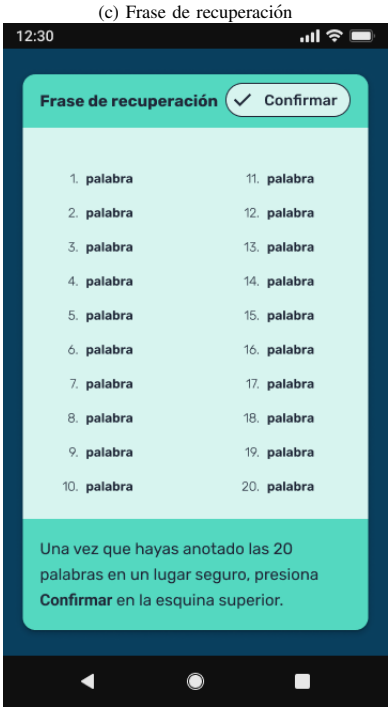
(a) Menú de opciones



(b) Indicaciones sobre el uso de la frase de recuperación

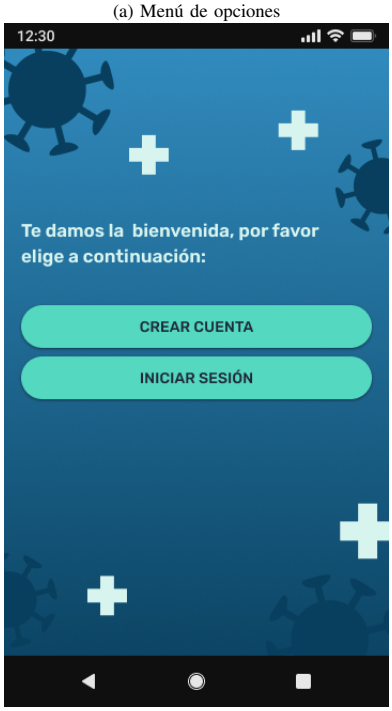


(c) Frase de recuperación



B-B. CU2: Paciente validando cuenta anterior

(a) Menú de opciones



(b) Solicitud de ingreso de la frase de recuperación



B-C. CU3: Paciente mostrando su certificado

(a) Código QR



(b) Detalle de dosis aplicadas



B-D. CU4: Agente validando un certificado

(a) Escaneo de código QR mediante la cámara



(b) Resultado de la validación

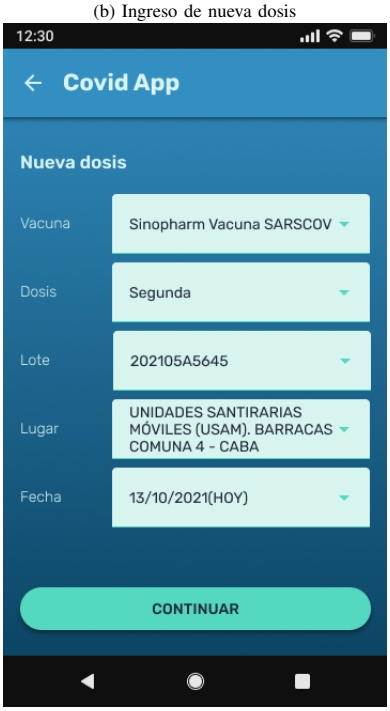


B-E. CU5: Agente aplicando una dosis

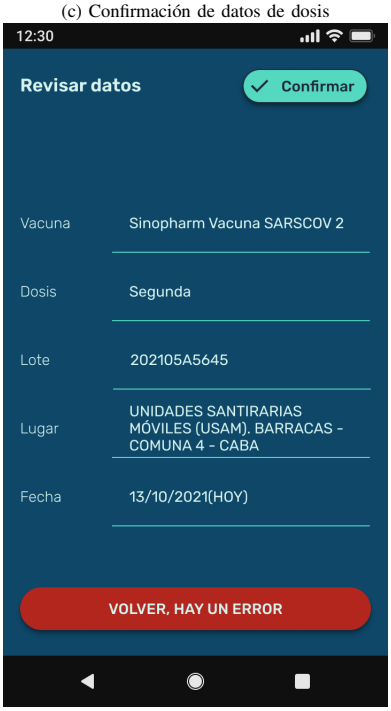
(a) Verificación de dosis previas



(b) Ingreso de nueva dosis



(c) Confirmación de datos de dosis



(d) Dosis registrada



Apéndice C
Implementación de contrato en Solidity

```
// SPDX-License-Identifier: MIT
pragma solidity >=0.4.22 <0.9.0;
import "@openzeppelin/contracts/access/AccessControl.sol";

contract CertificadoVacunacion is AccessControl {

    struct Dosis {
        string sede;
        uint256 fecha;
        string marcaVacuna;
    }
    bytes32 internal constant ROL_APLICADOR = keccak256("ROL_APLICADOR");
    bytes32 internal constant ROL_ADMIN = keccak256("ROL_ADMIN");
    mapping(address => Dosis[]) internal aplicacionesDosis;

    /// @notice Inicializa como administrador la direccion que hace deploy del contrato
    constructor() {
        _setRoleAdmin(ROL_ADMIN, ROL_ADMIN);
        _setRoleAdmin(ROL_APLICADOR, ROL_ADMIN);
        _setupRole(ROL_ADMIN, msg.sender);
    }

    /// @notice Agregar una direccion con el rol de aplicador (quien registra la aplicacion de una dosis)
    /// @param aplicador Direccion de la persona que puede registrar aplicaciones
    function agregarAplicador(address aplicador) public {
        grantRole(ROL_APLICADOR, aplicador);
    }

    /// @notice Elimina el rol de aplicador de una direccion
    /// @param aplicador Direccion de la persona quien se le quita el rol
    function eliminarAplicador(address aplicador) public {
        revokeRole(ROL_APLICADOR, aplicador);
    }

    /// @notice Registra la aplicacion de una dosis a una persona. Para aplicar hay que ser aplicador.
    /// @param persona Direccion del paciente que esta siendo vacunado
    /// @param _sede Nombre del lugar donde se aplica la dosis
    /// @param _fecha Timestamp del momento de aplicacion
    /// @param _marcaVacuna Nombre de la marca de la vacuna aplicada
    function aplicarDosis(address persona, string memory _sede, uint256 _fecha, string memory _marcaVacuna)
         public esAplicador {
        Dosis memory dosis = Dosis(_sede, _fecha, _marcaVacuna);
        (aplicacionesDosis[persona]).push(Dosis(_sede, _fecha, _marcaVacuna));
        emit dosisAplicada(msg.sender, persona, dosis);
    }

    /// @notice Consulta la informacion de una dosis aplicada. Solo lo puede hacer la misma persona
        vacunada.
    /// @return Sede de vacunacion, timestamp y marca de la vacuna aplicada.
    function obtenerAplicacionDosis(address persona, uint8 nroDosis) public view esPropietarioCertificado(
        persona) returns(Dosis memory)  {
        return((aplicacionesDosis[persona])[nroDosis]);
    }

    /// @notice Consulta todas las dosis aplicadas a una persona. Solo lo puede hacer la misma persona.
    /// @return Lista de: sede de vacunacion, timestamp y marca de la vacuna aplicada.
    function obtenerAplicaciones(address persona) public view esPropietarioCertificado(persona) returns(
        Dosis[] memory)  {
        return(aplicacionesDosis[persona]);
    }

    event dosisAplicada(address aplicador, address persona, Dosis dosis);

    modifier esAplicador {
        require(hasRole(ROL_APLICADOR, msg.sender), "solo aplicadores registrados");
        _;
    }

    modifier esPropietarioCertificado(address persona) {
        require(msg.sender == persona, "solo para el propietario del certificado");
        _;
    }
}
```