

Registro Seguro de Evidencias Digitales con Tecnología Blockchain

Herminia Beatriz Parra ¹[0000-0002-3230-3108], Gustavo Rivadera ¹[0000-0002-5468-7077], Enzo Notario ¹[0000-0002-0069-3623], Diego Petrus ², Graciela Feijoo ², Eduardo Servin, ², Facundo Arredondo ³

¹ Universidad Católica de Salta, Salta, Argentina {bgallo, grivadera, ernetario}@ucasal.edu.ar

² Empresa JusTech SRL, CABA, Argentina {dpetrus, gfeijoo, eservin}@justech.com.ar

³ Fundación Sadosky, Argentina, farredondo@fundacionsadosky.org.ar

Resumen. Este trabajo describe las características y punto de ejecución a la fecha de un proyecto de desarrollo de software, para el registro seguro de la cadena de custodia de la evidencia judicial. A partir de la vinculación interinstitucional entre la Fundación Sadosky, la empresa JusTech SRL y el Grupo de I+D+i de Forensia Digital y Ciberseguridad de la Facultad de Ingeniería de la UCASAL, se conformó un equipo de trabajo especializado que responde a una necesidad real de un sector demandante de nuestra sociedad como es la Justicia, con el objetivo de resolver la problemática sobre la trazabilidad de la evidencia judicial, a partir de los registros que indican quienes acceden a la misma y que deben garantizar la inalterabilidad de la evidencia en todo momento. Se incluyen en este trabajo los objetivos, metodología y resultados alcanzados en este proyecto, incluyendo el estado del arte y el marco de referencia sobre las tecnologías aplicadas, destacando las características propias de Blockchain para establecer la trazabilidad de los eventos relacionados a un objeto.

Palabras clave: Evidencia Judicial, Cadena de Custodia, Blockchain.

1 Introducción

Se señala en [1] que "*...la prueba (judicial) sirve, y con tal finalidad es empleada, como instrumento de conocimiento sobre el cual el juez se apoya para descubrir y establecer la verdad de los enunciados de hecho que son objeto de su decisión. En otras palabras, la prueba provee al juez los datos cognoscitivos, la información de la cual debe servirse para formular tal decisión...*". En todo momento del acto judicial, la evidencia debe estar protegida de manera segura y garantizando la inalterabilidad, pues de ella depende luego que el juez la considere una prueba y en ella fundamente su sentencia. Por lo tanto, es necesario recurrir a procedimientos seguros para el correcto manejo de las evidencias. La tecnología Blockchain es útil y adecuada para crear un registro cuidadoso y meticuloso de las personas que manejan las evidencias y contribuyen a su admisibilidad en un proceso judicial.

Para responder a esta problemática, se conforma un equipo de trabajo entre la empresa JusTech SRL y la Facultad de Ingeniería de la UCASAL a través de del Grupo

de I+D+i de Forensia Digital y Ciberseguridad. JusTech aporta lo necesario para el desarrollo de la arquitectura de software basada en Tecnologías Blockchain en tanto que el Grupo de I+D+i de Forensia Digital y Ciberseguridad aporta la base de conocimiento experto en el tratamiento de la evidencia digital y el modelo de negocio de la Cadena de Custodia, teniendo en consideración el marco de calidad y seguridad informática que exige el proyecto. El proyecto que inició en octubre del 2023 y cuenta con una duración de doce meses, prevé como resultado el diseño y desarrollo de una aplicación informática para el registro seguro de la Cadena de Custodia de resguardo de una evidencia, restringido para casos judiciales del ámbito Penal inicialmente. Con un desarrollo cercano al 48%, se muestran los resultados parciales obtenidos a la fecha.

Este trabajo está organizado de la siguiente manera: En la Sección 2 se describe el marco de referencia utilizado respecto de la Cadena de Custodia y la tecnología Blockchain. En la Sección 3 se analiza el estado del arte sobre la conexión entre Blockchain y los procesos judiciales y, más específicamente, la Cadena de Custodia. En la Sección 4 se describe el proyecto en sí mismo con mención de los apartados más destacados (objetivos, metodología de trabajo, arquitectura de la solución propuesta). Finalmente, en la Sección 5 se describen las conclusiones de este trabajo.

2 Marco de Referencia

A continuación, se aborda una descripción detallada del procedimiento judicial conocido como Cadena de Custodia, destacando sus características, problemática y otros elementos relevantes. Luego, se describe la tecnología Blockchain y sus características que la hacen apropiada para brindar una solución a la problemática de estudio.

2.1 La Cadena de Custodia de la Evidencia Judicial

Se puede considerar la definición de Cadena de Custodia del Ministerio Público Fiscal de Argentina [2], que señala: *“La cadena de custodia es el conjunto de medidas que deben adoptarse a fin de preservar la identidad e integridad de objetos o muestras que pueden ser fuente de prueba de hechos criminales, para su total eficacia procesal... Debe garantizar que el elemento de prueba o evidencia que se presenta en juicio, con el objeto de probar una determinada afirmación, sea el que ha sido reclutado y que no haya sufrido adulteraciones o modificaciones de parte de quienes lo introducen o terceras personas... Se debe tener especial cuidado en evitar cuestionamientos respecto del levantamiento y la custodia de los elementos o rastros que se presentan en el plenario, aventando cualquier sospecha sobre su procedencia y dejando en claro que se corresponden con los efectivamente secuestrados en la escena del crimen...”*

La Cadena de Custodia es un procedimiento que incluye distintos momentos en la manipulación de la evidencia:

- a) Recolección de la evidencia: cuando se secuestra el elemento de prueba o se recibe si fuera entregada voluntariamente. Se da inicio al registro de la cadena de custodia, con el detalle de las características del acto de obtención (fecha, hora, lugar, etc.)

- b) **Análisis Forense de la evidencia:** según el tipo de evidencia se procede al análisis forense por parte del laboratorio adecuado (Genética, de Reconstrucción Criminal, de Informática Forense, entre otros). La evidencia es tomada por el personal actuante indicando en la cadena de custodia que es responsable de la misma.
- c) **Destino Final de la Evidencia:** cuando lo dispone la autoridad judicial, se ordena el destino final de la evidencia, que puede ser la destrucción (caso de armas o drogas incautadas) o devolución al propietario (bienes muebles de cierto valor).

Todas estas etapas deben ser registradas en la Cadena de Custodia, indicando al responsable de manejar las pruebas en cada etapa, las fechas y las condiciones de las pruebas entregadas. Cada institución judicial aplica un procedimiento válido para mantener la Cadena de Custodia y proporciona modelos de formularios para registrarlas. La Cadena de Custodia permite identificar dónde está la evidencia, por qué está en un lugar determinado y quién es el responsable de ella. Es común encontrar registros en papel de la Cadena de Custodia, pero hay algunos casos de sistemas informáticos para la registración digital de los eventos, aunque usualmente están orientados a la gestión judicial más que al cuidado y resguardo de la trazabilidad de la evidencia.

En este sentido, [3] y [4] señalan las ventajas de desarrollar una aplicación informática que incluya tecnologías ágiles para la identificación rápida de evidencias (códigos QR y códigos de barras), incorpore bases de datos relacionales que soporten los eventos sobre las evidencias y un software propio para su seguimiento. Por su parte, [3] se refiere al reto que representa la evidencia digital para la justicia, y propone Blockchain como herramienta para establecer la trazabilidad de la evidencia. La Unión Europea impulsa su propio proyecto sobre esta materia denominado Proyecto LOCARD [5], que proporciona una plataforma colaborativa y distribuida para automatizar la grabación, análisis y custodia de cualquier tipo de evidencia digital.

Uno de los factores clave en este proyecto es el uso de la tecnología Blockchain, que, gracias a la inmutabilidad de los datos, asegura que las evidencias registradas no han sido manipuladas ni falsificadas. Esto añade una nueva característica a la calidad probatoria de las pruebas en un proceso policial o judicial. Obviamente, este sistema de registro también se puede aplicar al seguimiento de las pruebas materiales.

2.2 Tecnología Blockchain

Una red Blockchain es un sistema descentralizado y distribuido, por lo tanto, disponible para todos los participantes que son actores de una transacción. Su integridad radica en un consenso total de la red de la historia del libro mayor de transacciones. Cada miembro es un nodo de la red y mantiene una copia de todo el libro mayor. Se utiliza un sistema de verificación seguro llamado protocolo de consenso. No requiere la participación de terceros de confianza. Tiene tres principios técnicos básicos: a) la replicación del libro mayor con el registro de todas las transacciones entre los miembros de la red; b) el uso de criptografía como garantía de la seguridad y privacidad de las transacciones y confirmación de la identidad de los miembros; y c) un protocolo consensuado para regular la incorporación de nuevos bloques o la modificación de los existentes.

Si bien el caso más conocido es la aplicación de Blockchain en las criptomonedas, existen diversas investigaciones y avances acerca de la implementación de Blockchain

en entornos no empresariales, como en el caso de la trazabilidad de cadenas de suministros de productos agropecuarios e industriales [6]. Aunque la aplicación de Blockchain constituye un reto inicial para las empresas en aspectos como infraestructura, ciberseguridad y costo computacional, los contratos inteligentes basados en Blockchain son muy útiles en campos no tradicionales como los servicios de seguros, la industria automotriz, las empresas de construcción y las instituciones educativas, entre otros.

Es importante considerar otros factores sobre la tecnología Blockchain, en [7] se analiza esta tecnología desde una perspectiva ética considerando las dimensiones morales (favorables y desfavorables) de su aplicación a los negocios. Lo interesante de esta investigación es la descripción de la naturaleza descentralizada, democrática y no mediada de Blockchain, gracias a ello, Blockchain no origina asimetrías de poder entre las partes. Esto genera un modelo de igualdad y objetividad que es muy útil en el ámbito de la justicia, promoviendo la equidad en la forma en que se manejan las pruebas.

Respecto del sector demandante de la aplicación resultante de este proyecto, se ha identificado como tal a los ámbitos de la Justicia que utilizan la Cadena de Custodia para la salvaguarda de la evidencia. Específicamente, se identificó a los Ministerios Públicos Fiscales, que tienen a su cargo la investigación de los delitos y la promoción de la acción penal pública contra los autores o partícipes a fin de, eventualmente, acreditar en un juicio oral y público los hechos que fundamenten su acusación. Diferentes estamentos de esta institución, que reciben el nombre de “Policía Judicial” o “Investigaciones Fiscales”, hacen uso de la Cadena de Custodia durante todo el proceso investigativo y judicial involucrado en la comisión de los supuestos delitos penales.

3 Estado del Arte

La propuesta de una aplicación informática para la Cadena de Custodia basada en tecnologías Blockchain no es nueva, existen investigaciones muy valiosas que se han considerado al momento de plantear la solución tecnológica más adecuada para esta problemática que -de por sí- exige aspectos cuidadosos en lo que hace a métricas de calidad del software y a requerimientos de seguridad que fortalezcan la reserva y privacidad de los datos que se procesan, relacionados a la evidencia judicial.

En [9] se realizó una primera revisión bibliográfica del estado del arte de uso de tecnologías Blockchain al ámbito de la Justicia. De este artículo se resumen aquellas de mayor interés: en el trabajo [10] se discute sobre el uso de Blockchain en los procesos de mediación judicial; la investigación [11] aborda la aplicación de Blockchain para la investigación criminal, enfatizando la importancia de conocer esta tecnología, por parte de la justicia y la fuerza policial; y el trabajo [12] plantea consignas para confirmar si Blockchain se puede aplicar a la Cadena de Custodia de la evidencia digital. Otros aportes de interés se encontraron en la investigación [13] que trata sobre el uso de la tecnología Blockchain para compartir datos de casos penales, especialmente cuando se recurre a correos electrónicos o documentos en papel que se exponen a la alteración ilegal de datos. El trabajo [14] analiza la convergencia de las tecnologías Blockchain y los procesos judiciales de foros civiles, considerando las relaciones sociales que surgen, al aplicar este tipo de tecnologías.

Este análisis bibliográfico se completa con otros artículos revisados una vez que se inició el proyecto, porque contienen investigaciones de interés para alguno de los aspectos que discutidos durante el diseño de la solución tecnológica propuesta. En la investigación [15] los autores establecen que el bienestar de un usuario de Blockchain depende críticamente de tres características de la Blockchain: a) Adopción (número de usuarios activos en la misma plataforma Blockchain); b) Escala (velocidad a la que se agregan transacciones a la cadena de bloques), y c) Seguridad (probabilidad de que una transacción pueda revertirse). Las características citadas se analizan en el contexto de este proyecto, considerando que la solución propuesta debe utilizarse en ambientes distribuidos de masiva participación de diferentes actores (funciones policiales; funcionarios judiciales, analistas forenses, laboratorios externos, entre otros). Este contexto supone que las instituciones que actúan sobre la evidencia digital, todas ellas con su propia cultura organizacional, deben acordar los criterios básicos para garantizar la inalterabilidad de la evidencia. El trabajo [16] aborda un modelo de arquitectura por niveles que expresa con claridad la vinculación entre las distintas capas de las tecnologías intervinientes, permitiendo plasmar las actividades o procesos en los que interviene la Blockchain, y a su vez cómo se vincula ésta (en cuanto a modelo de back-end) con la aplicación informática a la que accede el usuario para la gestión de la información (en cuanto a modelo de front-end) mediante los contratos inteligentes.

4 Características del Proyecto de “Registro Seguro de Evidencias Digitales con Tecnología Blockchain”

4.1 Objetivos y Alcance

El proyecto plantea como objetivo “Impulsar el desarrollo y aplicación de las Tecnologías de la Información y la Comunicación (TICs), más precisamente, las asociadas a Blockchain y en particular en la nube, en el ámbito de la Justicia”. La consecución de este objetivo general se traduce en los siguientes objetivos específicos:

- Formular un proyecto tecnológico que integre los recursos que cada parte aporta desde el rol que le compete, para el desarrollo de una arquitectura basada en los fundamentos metodológicos, técnicos y científicos requeridos por la Forensia Digital, con la adición de la trazabilidad inmutable de Blockchain.
- Desarrollar una arquitectura de software de tipo Blockchain en la nube que incorpore los resultados y conclusiones de OE1 considerando las estrategias necesarias para la implementación gradual de la solución encontrada.
- Evaluar tres tipos de tecnologías Blockchain para el caso de uso de esta propuesta: i) redes públicas completamente descentralizadas, ii) redes privadas, iii) un enfoque centralizado usando bases de datos de tipo ledger encriptadas, inmutables y auditables.
- Desarrollar una infraestructura de bases de datos en la nube que soporte la arquitectura Blockchain antes mencionada, permitiendo experimentar y obtener conclusiones desde el punto de vista de las bases de datos cloud.

Estos objetivos permiten definir el alcance del proyecto, y las características de los resultados esperados, que se resumen en el desarrollo de una aplicación informática -a nivel prototipo- que contemple funcionalidades de back-end (basadas en las tecnologías Blockchain) y funcionalidades de front-end (basadas en tecnologías web 2.0), que brinden al usuario experto un registro de la creación y sucesivas transacciones realizadas sobre una evidencia o elemento de prueba.

4.2 Equipo de Trabajo

El proyecto se ha estructurado a partir de la participación de tres instituciones, cada una de las cuales tiene su rol identificado para la consecución exitosa del mismo: la Fundación Sadosky, la Empresa JUSTECH SRL y el Grupo de I+D+i de Forensia Digital y Ciberseguridad de la UCASAL. Lograda esta vinculación interinstitucional entre Fundación Sadosky, JusTech SRL y UCASAL, a partir de la presentación del proyecto en la convocatoria “Soluciones Innovadoras para Desafíos de Software 2023”, y que fuera seleccionado, fue posible generar un ámbito en el que se conjugan la ciencia, la tecnología y una demanda del medio productivo, con foco en la transferencia de conocimientos y tecnología como base para la formulación de una solución tecnológica basada en tecnologías novedosas como lo es Blockchain, para lo cual cada parte se integra en el proyecto conformando un equipo interdisciplinario con roles bien definidos.

4.3 Metodología de Trabajo

Del trabajo [17] es de interés la metodología seguida para el análisis del problema, desde el punto de vista de las consideraciones relativas a la funcionalidad de todo el sistema. Este autor propone:

- Identificar los requisitos funcionales y no funcionales del caso de uso
- Realizar el análisis de seguridad a partir de las probables vulnerabilidades del modelo tecnológico propuesto y también respecto de los criterios de la seguridad de los datos registrados (integridad, confidencialidad, disponibilidad y autenticación).
- Realizar el análisis de carga energética exigida y de eficiencia algorítmica
- Definir el marco legal y ético que servirá de base para la solución propuesta

A estas consideraciones se deben sumar las correspondientes a la modelización de un proyecto basado en tecnología Blockchain:

- Identificación de los partícipes del sistema
- Identificación del modelo de negocio según el caso de uso que se utilice
- Definición de las actividades y distintos estados que transitan las mismas
- Definición de los activos que se representarán en los contratos inteligentes

Con estos criterios, se trabajó en la definición del plan de trabajo que identificó las responsabilidades del equipo de trabajo interinstitucional, así como la definición de hitos trimestrales con presentación de informes de avance que deben correlacionarse con el plan general de trabajo acordado por las partes. A la fecha, el proyecto cuenta con un avance aproximado del 48% logrado en cinco meses de ejecución.

4.4 Arquitectura de la Solución Propuesta

Como modelo de negocio se tomó el procedimiento establecido para la Cadena de Custodia por el Ministerio Público Fiscal de Argentina [18], aunque luego se fue ajustando mediante una instancia de prueba de concepto que se implementó entre usuarios expertos (fiscales, peritos, criminalísticos) para validar los procesos y atributos de datos relacionados a la Cadena de Custodia.

El gráfico de la Fig. 1 muestra el modelo de arquitectura por niveles, basado en la investigación [16] que muestra la vinculación entre los distintos componentes de la solución propuesta para este caso.

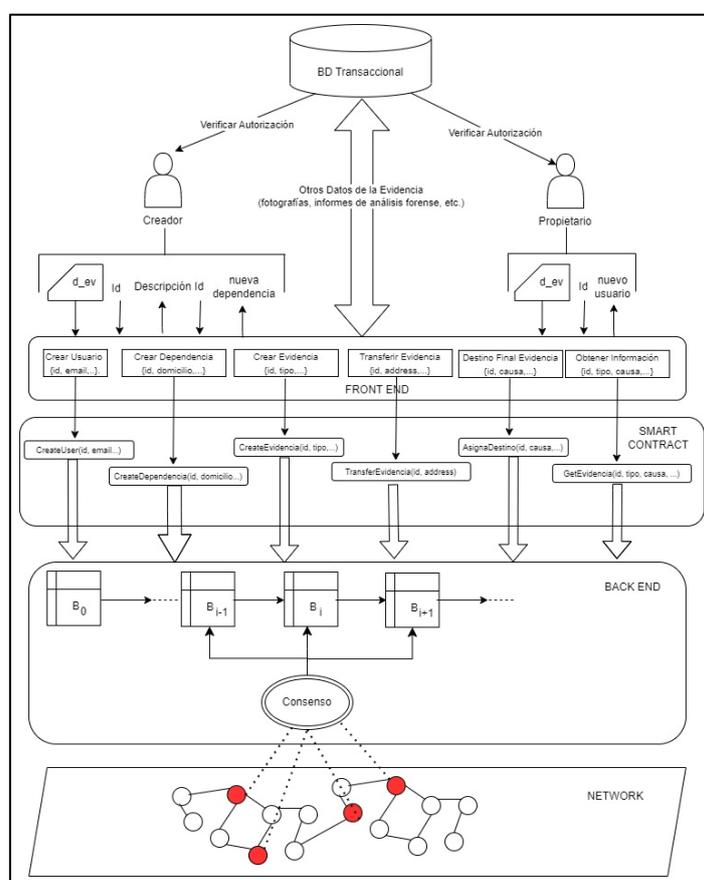


Figura 1: Modelo de la Arquitectura por Niveles

El proyecto se basa en las siguientes definiciones respecto de las características de la tecnología Blockchain que se utilizará:

- Se trabajará sobre un red permissionada privada, con acceso restringido y la identidad de los participantes será conocida. Esto es así por las propias características del objeto de la transacción: el registro de la evidencia judicial.

- b) El consenso se logrará mediante la aplicación del método PoA (Proof Of Authority) por ser este un protocolo de consenso especialmente dirigido a una Blockchain privada. PoA se aprovecha de las identidades reales para permitir la validación dentro de una Blockchain. Esto significa, que los validadores ponen su identidad real y reputación como garantía de transparencia.

La arquitectura propuesta incluye tanto una base de datos relacional como una Blockchain permissionada: en la primera se almacenan datos complementarios de las evidencias como ser fotografías y análisis forenses, y en la segunda lo que sería un registro de cada transacción de la evidencia, desde su creación, su transferencia entre distintos responsables y disposición final. Una de las diferencias entre ambas bases es que una almacena información inmutable y de mayor volumen mientras que la otra contiene registros más pequeños con la capacidad de ser actualizados con mayor frecuencia.

Por otra parte, la Tabla 1 resume los actividades de base a las que responderá la aplicación, así como las funciones y atributos de los datos de la solución propuesta:

Tabla 1: Actividades, Funciones y Atributos de la aplicación propuesta

Actividad	Funciones	Atributos de los datos
Administración del Sistema	Creación y Modificación de: <ul style="list-style-type: none"> • Roles • Usuarios • Dependencia • Subdependencias • Ubicaciones Geográfica 	Id_rol Id_Usuario Id_Dependencia Id_Subdependencia Id_UbicGeografica
Ingreso de una Evidencia	Creación del registro inicial de una Evidencia	Id_Evidencia Id_UsuarioResponsable Id_LugarHallazgo Id_tipoEvidencia Id_DependenciaQueLaCrea Id_Nro_Causa Id_Nro_Folio Id_EspacioFotografias Id_NroMuestraEnEvidencia CantidadElementosQueIntegranLaEvidencia FechaHora_IngresoEvidencia FechaHora_SecuestroEvidencia Id_Nro_Precinto DescripcionGralEvidencia Id_EstadoCadenaDeCustodiaEnPapel Observaciones
Eventos o Transferencia de una Evidencia	Registro de los sucesivos eventos o traspasos a otra persona/dependencia	Id_rol Id_Usuario Id_Dependencia Id_Subdependencia Id_UbicGeografica
Destino Final de la Evidencia	Registro del evento final de la evidencia	Id_Evidencia Id_UsuarioResponsable Id_FolioQueDisponeDestinoFinal FechaHora_DisposicionFinal Observaciones

Actividad	Funciones	Atributos de los datos
Consultas Varias	Visualización de consultas según distintos filtros	Por Id_Usuario Por FechaHora Por Dependencia/Subdependencia Por Subdependencia Por Id_Tipo_Muestra Por Trazabilidad

4.5 Requisitos de Calidad y Seguridad Informática

Desde el punto de vista de seguridad informática, la seguridad de la información y la ciberseguridad, la aplicación informática propuesta debe estar contenida en un contexto que contemple las condiciones esenciales de la seguridad de toda la infraestructura tecnológica en la que se implementará. Aspectos tales como:

- Las cuestiones referidas a la disponibilidad de los datos almacenados en la nube, respecto de las cuestiones legales y de jurisdicción que le son propias a una institución de la justicia deben estar claramente definidas.
- El control de acceso de los usuarios pertenecientes a distintas instituciones estatales, cada una de ellas con sus propias políticas de roles y privilegios, es importante, y deben ajustarse de manera sincronizada entre ellas mismas y con los criterios de seguridad de la Blockchain.
- Las transacciones de la cadena de custodia de una evidencia pueden llegar a conformar un volumen de datos considerables, que es necesario mantener en el tiempo debido a la duración de los procesos de la justicia. Esto implica que se deben instrumentar mecanismos apropiados para las tareas complementarias del procesamiento de los datos (resguardo y recuperación de datos, logs de todos los eventos que ocurren sobre la Blockchain, entre otros).
- Todas las instituciones que interactúen con la aplicación propuesta deberán ajustarse a las condiciones de seguridad organizacionales de estilo (políticas de seguridad, equipos específicos para análisis y prevención de incidentes) los que, por supuesto, deberán crear las respectivas instancias de colaboración para la prevención y contención de ataques y accesos indebidos.

Existen varios estándares y marcos de trabajo reconocidos internacionalmente para asegurar la calidad del proceso de un producto. En particular podemos mencionar la serie de normas ISO 9000 como estándares generales y en particular la ISO/IEC 17032:2019, que tiene por objetivo proporcionar directrices y ejemplos para la implementación de un esquema de certificación de procesos, y se aplica a la certificación de procesos de cualquier tipo, independientemente del tamaño o la complejidad de la organización.

Además de este estándar, podemos mencionar los siguientes estándares y normas particulares del desarrollo de software.

- De la serie ISO, se puede considerar la ISO/IEC 25002:2024, ISO/IEC 25010:2023 e ISO/IEC 25019:2023, todas referidas a los procesos de desarrollo de software.
- Los modelos de mejora de procesos de software como CMMI (Capability Maturity Model Integration), ITIL (Information Technology Infrastructure Library) y las metodologías de desarrollo ágil son también de interés para la calidad del software.

- Las normas IEEE 730 e IEEE 830 también proporcionan una guía para la especificación de requerimientos de software.
- En cuanto a los criterios de seguridad informática, los estándares OWAPS son pertinentes al proyecto, así como la familia de normas de la serie ISO 27000.

A partir de un análisis de los documentos indicados, se encuentra en elaboración un “Check-List de Control de Calidad y Ciberseguridad”, que permitirá chequear que la solución tecnológica elaborada, cumpla con los criterios mínimos y básicos referidos a calidad y seguridad. A modo de muestra, a continuación, se incluyen las consignas que comprenderá el Check-List indicado en la Tabla 2.

Tabla 2: Consignas del Check-List de Control de Calidad y Ciberseguridad

Nro	Consigna
1	¿El proceso de desarrollo de software de su organización se describe claramente?
2	¿Se utilizan técnicas de estimación para planificar el proyecto en tiempo y costos?
3	¿Se utilizan herramientas para la gestión del proyecto de software?
4	¿Existe documentación de diseño preliminar o de alto nivel en el proceso software?
5	¿Existe documentación de diseño detallado en el proceso software?
6	¿Existe documentación de especificación de requerimientos de software (ERS) en el proceso de desarrollo de software?
7	¿Se realiza alguna planificación para las pruebas dentro del proceso?
8	¿Qué tipos de prueba realiza su organización durante la etapa de pruebas del software?
9	¿Se utilizan métricas del Software para el control del proyecto?
10	¿Se utilizan herramientas para la gestión de la Configuración del producto software?
11	¿Se identificaron atributos/valores que contienen Información Personalmente Identificable (PII) que se estén almacenando en la cadena de bloques?
12	¿Existe un mecanismo por el cual el Usuario brinde su acuerdo para el uso de datos?
13	¿Se ha contemplado la opción de modificar (y mantener un historial) del Contrato Inteligente debido a modificaciones de legislación/jurisdicción?
14	¿Se contempla la posibilidad de modificar algún dato ya escrito en la Blockchain?
15	¿Se almacenan valores encriptados en la Blockchain y con cual algoritmo son encriptados? ¿Se utilizan algoritmos para el Salt Hashing?
16	¿El sistema requiere un mecanismo de Autenticación para ser utilizado?
17	¿Registra fallas de control de acceso y alerta a los administradores cuando sea adecuado?
18	¿Invalida los tokens de sesión en el servidor después de cerrar la misma?
19	¿Aplica el principio de privilegios mínimos?
20	¿Cuenta con un control de acceso adecuado y mecanismos de autorización?
21	¿Implementa la autenticación multifactor para evitar ataques automatizados, de diccionario, de fuerza bruta y de reutilización de credenciales robadas?
22	¿Implementa un tiempo de espera de sesión inactiva?
23	¿Cuenta con un límite razonable de cantidad de sesiones activas e informa el detalle de cada una?
24	¿Cuenta con un botón de cierre de sesión en cada página?

Nro	Consigna
25	¿Establece el tiempo de caducidad de las cookies de autenticación?
26	¿Se toman acciones ante un número de intentos de autenticación fallidos?
27	¿Cuenta con un sistema seguro de restablecimiento de contraseña?

5 Conclusiones

Los principales resultados alcanzados a la fecha son los siguientes:

- Se logró el primer nivel de la arquitectura de la solución tecnológica y un avance de nivel 1 del prototipo de la aplicación informática.
- Se realizó una extensa revisión bibliográfica para identificar las tendencias tecnológicas sobre la solución tecnológica del caso.
- Se desarrolló una Prueba de Concepto que permitió validar los datos y procesos identificados para la Cadena de Custodia, por parte de usuarios expertos (fiscales, personal policial, abogados penalistas, entre otros).
- Se relevaron y establecieron los principales requisitos de calidad y seguridad que debe cumplir la aplicación a desarrollar de acuerdo a los estándares establecidos en protocolos de estilo (Normas ISO, recomendaciones OWASP, entre otras).

La sistematización de los registros de la Cadena de Custodia trae aparejada una gestión inteligente de los datos para la elaboración de estadísticas y para la generación de nuevos conocimientos que pueden obtenerse mediante la analítica de datos, lo que permitirá contar con información que fundamente las políticas procesales y de seguridad que involucran al proceso penal, entregando a los actores de nivel superior información derivada de casos concretos, para que puedan tomar mejores decisiones sobre la organización y administración de justicia.

La vinculación entre las tres instituciones UCASAL, JusTech y Fundación Sadosky permitió generar un espacio de interacción colaborativa para dar respuesta a una demanda requerida desde ámbitos con dificultades propias para lograr el uso eficiente de las TICS, como lo es la Justicia. Por parte de cada una de las instituciones partícipes del proyecto, también se observan ventajas de esta alianza estratégica, en términos del fortalecimiento continuo de sus recursos humanos y técnicos abocados al proyecto.

Divulgación de intereses.

Los autores no tienen intereses contrapuestos que declarar que sean relevantes para el contenido de este artículo.

Referencias

1. Taruffo, M. (2018). La función epistémica de la prueba. MV Mosmann, & M. Panigadi, Problemática de la prueba (pág. 5). Buenos Aires: Astrea.
2. Ministerio de Seguridad de la Nación, (2021), IF-2021-114265868-APN-SSYPC#MSG, PROTOCOLO DE ACTUACIÓN PARA LA INVESTIGACIÓN CIENTÍFICA EN EL

- LUGAR DEL HECHO <http://servicios.infoleg.gob.ar/infolegInternet/anexos/355000-359999/357248/norma.htm>
3. C. Aguiar Miranda, A. Montoya Moreno y F. Rascón Figueroa, "Implementación de un software de registro de cadena de custodia. (Primera parte)," *Visión Criminológica-Criminalística*, vol. 24, pp. 54-65, 2018.
 4. T. M. Palmbach, *Investigación y Examen de la Escena del Crimen: Cadena de Evidencia*, vol. 1. Elsevier Ltd., 2015. doi: 10.1016/B978-0-12-800034-2.00100-2.
 5. López-Aguilar, P., & Solanas, A. (2021, September). An effective approach to the cross-border exchange of digital evidence using blockchain. In *International Conference on Applications in Electronics Pervading Industry, Environment and Society* (pp. 132-138). Cham: Springer International Publishing.
 6. I. Konstantinidis, G. Siaminos, C. Timplalexis, P. Zervas, V. Peristeras y S. Decker, *Blockchain para aplicaciones empresariales: una revisión sistemática de la literatura*, vol. 320. Springer International Publishing, 2018. doi: 10.1007/978-3-319-93931-5_28.
 7. C. Dierksmeier y P. Seele, "Blockchain y ética empresarial", *Ética Empresarial*, vol. 29, no. 2, pp. 348-359, 2020, doi: 10.1111/beer.12259
 8. Estevez, E. C., Linares, S., & Fillotrani, P. (2020). PROMETEA: Transformando la administración de justicia con herramientas de inteligencia artificial. https://ri.conicet.gov.ar/bitstream/handle/11336/183777/CONICET_Digital_Nro.5e6bc385-5734-46f5-ae12-5c433541d7fe_B.pdf?sequence=2&isAllowed=y
 9. de Gallo, H. B. P., Medina, O. C., Dorado, J. G., Fleming, J. A., Párraga, C., Notario, E. R., & Sanchez, E. (2023). The Application of Blockchain to the Chain Of Custody of Judicial Evidence. *Eureka 2023*, Universidad de Jaen (España).
 10. Y. Aouidef, F. Ast y B. Deffains, "Justicia descentralizada: un análisis comparativo de los proyectos de resolución de disputas en línea de blockchain", *Fronteras en Blockchain*, vol. 4, núm. Marzo, pp. 1-8, 2021, doi: 10.3389/fbloc.2021.564551.
 11. H. Al-Khateeb, G. Epiphaniou y H. Daly, "Blockchain for modern digital forensics: The chain-of-custody as a distributed ledger" (Cadena de bloques para el análisis forense digital moderno: la cadena de custodia como libro mayor distribuido), *Ciencias y Tecnologías Avanzadas para Aplicaciones de Seguridad*, pp. 149-168, 2019, doi: 10.1007/978-3-030-11289-9_7.
 12. A. H. Lone y R. N. Mir, "Cadena forense: cadena de custodia forense digital basada en blockchain con PoC en Hyperledger Composer", *Digit Investig*, vol. 28, pp. 44-55, 2019, doi: 10.1016/j.diin.2019.01.002.
 13. Ramazhamba, P., & Venter, H. (2023, January). A blockchain model for sharing information in criminal justice systems. In *IFIP International Conference on Digital Forensics* (pp. 249-266). Cham: Springer Nature Switzerland.
 14. Davydova, I., Nahnybida, V., Adamova, O., Zhurylo, S., & Tokareva, V. (2023). Blockchain and civil proceedings: points of convergence. *Dixi*, 25(1), 1-20.
 15. Irresberger, F., John, K., Mueller, P., & Saleh, F. (2021). The public blockchain ecosystem: An empirical analysis. NYU Stern School of Business.
 16. S. Bonomi, M. Casini y C. Ciccotelli, "B-CoC: Una cadena de custodia basada en blockchain para la gestión de evidencias en análisis forense digital", *Serie OpenAccess en Informática*, vol. 71, 2020, doi: 10.4230/OASICS.Tokenomics.2019.12.
 17. Montoliu Rico, P. (2022). Implementación de un sistema básico de Blockchain y su aplicación en la trazabilidad de datos médicos (Doctoral dissertation, Universitat Politècnica de València).
 18. "Manual de Procedimientos del Sistema de Cadena de Custodia", 2015. [En línea]. Disponible: <https://www.mpf.gob.ar/capacitacion/files/2015/07/Cadena-de-Custodia.pdf>