UNIVERSIDAD NACIONAL DE CÓRDOBA
FACULTAD DE CIENCIAS ECONÓMICAS
ESCUELA DE GRADUADOS

ESPECIALIZACIÓN EN GESTIÓN DE TECNOLOGÍAS INNOVADORAS

TRABAJO FINAL DE INTEGRACIÓN

"Uso de smart contracts para validación de certificados en una red blockchain"

Autor: Ing. Romina Carla Racca

Tutor: Cra. Marta E. Plasencia

2021

Uso de smart contracts para validación de certificados en una red blockchain

Tesis presentada por:
Romina Carla Racca

Aprobada en estilo y contenido por:

_____
Miembro del tribunal evaluador

_____
Miembro del tribunal evaluador

_____
Miembro del tribunal evaluador

Calificación: _____

Fecha: Córdoba, de de 2021

Agradecimientos

Los agradecimientos están dirigidos a mi tutora Marta Plasencia por compartir conmigo su conocimiento, su paciencia y por mantener siempre el contacto acompañando constantemente.

A mis compañeros y amigos de especialización Diego y Cecilia por la motivación y estar presentes.

Principalmente a mi pareja y familia por el apoyo constante en cada paso que llevo adelante.

Índice general

Índice de figuras

Índice de tablas

1

Introducción

Las universidades, como instituciones de educación superior, otorgan títulos y expiden certificaciones que avalan las actividades realizadas y los niveles alcanzados por sus estudiantes. Si bien es habitual que la información contenida en estos certificados provenga de sistemas de registro informatizados, también es frecuente que por cuestiones legales exista un respaldo en papel del resultado de ciertos actos académicos. Este esquema de doble registro genera la necesidad de validar los certificados contrastándolos con la información en papel, lo cual representa una carga de trabajo considerable.

Para despapelizar y confiar en la información que se registra unicamente en los sistemas es posible implementar soluciones basadas en firma digital, pero estas soluciones no resuelven del todo la situación. El presente trabajo presenta una propuesta de solución mediante el uso de blockchain.

La incorporación de blockchain en distintos procesos también puede colaborar en la búsqueda de transparencia en la administración pública. Es una buena herramienta en el avance hacia el gobierno abierto.

Es posible incorporar la tecnología blockchain a distintos procesos administrativos. El proyecto surge de la necesidad de mejorar el registro de la verificación de actas y certificados que corroboran la realización de distintas actividades.

Para brindar respuesta a la necesidad se busca realizar innovación en el proceso, utilizando el conocimiento y transformando una idea en un resultado nuevo.

Se propone el desarrollo de un esquema de registro de actas utilizando contratos inteligentes (smart contracts) desplegados en una red blockchain, más precisamente en la Blockchain Federal Argentina, una red permisionada que utiliza el modelo de consenso de prueba de autoridad.

Este trabajo describe los detalles del proceso actual, las características de una red blockchain, en qué consiste la Blockchain Federal Argentina, la propuesta para mejorar los procesos actuales y cuenta la necesidad de vinculación con otras instituciones para llevar al exito el proyecto.

Se utilizan conocimientos adquiridos en los diferentes módulos de la especialización. Lo aprendido en *Gerenciamiento de Proyectos Tecnológicos* para la gestión y planificación del proyecto, desglosando el proyectos en etapas; *Gestión del Conocimiento* ya que todo conocimiento que se genera en el transcurso del proyecto se hace con la intención de ser compartido y participado con otras instituciones. El proyecto requiere tanto de un proceso de *vinculación* interna entre las dependencias de la universidad, como externa para que pueda ser implementado en otras universidades, para ello se aplicaron conocimientos de *Gestión de Redes y Vinculación Tecnológica*.

La gestión del proyecto y las definiciones técnicas se llevan a cabo en la Prosecretaría de Informática (PSI) de la UNC. Actualmente desempeño como responsable de la coordinación y gestión de los proyectos de desarrollo informático que se realizan en la PSI para brindar soluciones a las diferentes dependencias, como asi también para automatizar, innovar y mejorar procesos en la Universidad.

Palabras clave: Blockchain, smart contracts, innovación, validación de certificados, vinculación, transparencia.

1.1 Objetivos

1.1.1 Objetivo general

El objetivo general consiste en gerenciar un proyecto para brindar transparencia en la administración haciendo uso de tecnología blockchain para la validación de certificados emitidos por el sistema académico.

1.1.2 Objetivos específicos

- Definir las tecnologías informáticas apropiadas.
- Promover la vinculación de la universidad con la red Blockchain Federal Argentina.
- Adecuar la propuesta a los estándares del Ministerio de Educación Nacional.
- Analizar la problemática de la despapelización en el ámbito administrativo.
- Garantizar la veracidad de los datos de los certificados analíticos.
- Avanzar en la automatización de procedimientos.
- Brindar seguridad y transparencia en los procesos de acreditación de antecedentes.

1.2 Organización del trabajo final

El trabajo se ha dividido en los siguientes capítulos:

- **Marco teórico:** explica conceptos teóricos aplicados al proyecto, contexto en el que se desarrolla y el vocabulario utilizado.
- **Desarrollo técnico:** desarrolla la descripción técnica del proyecto y describe la propuesta brindada.
- **Conclusiones:** analiza los resultados obtenidos y se brinda una conclusión.

2

Marco teórico

Este capitulo profundiza el contexto en el que se desarrolla el proyecto, las normativas y mecanismos de gestión académica establecidos en la Universidad Nacional de Córdoba. Luego se abordan conceptos fundamentales para comprender el vocabulario y características de una red blockchain y los tipos de problemas que permite resolver.

Se comenzará explicando el contexto de la universidad y su estatuto.

La Universidad Nacional de Córdoba (UNC) es una universidad pública argentina. Es un organismo autónomo, que dicta sus propios estatutos y normas de gobierno. Su autonomía tiene rango constitucional, consagrada por la reforma de la Constitución Nacional del año 1994 [1]. Fundada en 1613, es la universidad más antigua del país, y con más de 120.000 estudiantes, una de las más grandes [2]. Si bien su máxima autoridad es la Asamblea Universitaria, esta sólo se reúne por convocatoria expresa, por lo que el gobierno es ejercido por el Honorable Consejo Superior y el Rector. El Honorable Consejo Superior está conformado por el Rector, los Decanos, y representantes de todos los claustros: docentes, nodocentes, egresados y estudiantes. Todas las autoridades, tanto unipersonales como colegiadas, son elegidas por los miembros de la comunidad universitaria mediante elección

directa. La universidad está conformada por quince facultades, cada una de ellas gobernada por un Honorable Consejo Directivo y un Decano [3]. A nivel central, el equipo de gestión del rectorado está organizado en Secretarías y Prosecretarías.

2.1 Gestión académica en la Universidad Nacional de Córdoba

La organización interna del área de enseñanza de cada unidad o dependencia académica contempla tres sectores especializados:

- Despacho de Alumnos.
- Oficialía.
- Área de informática.

En el proceso de gestión académica estos sectores trabajan conjunta y coordinadamente bajo la responsabilidad de distintos funcionarios. Es responsabilidad de la autoridad de la respectiva dependencia académica la determinación y dotación de los recursos necesarios para el logro de un funcionamiento eficiente del área de enseñanza.

2.1.1 Sectores involucrados y responsabilidades

Despacho de Alumnos

El sector de Despacho de Alumnos depende funcional y jerárquicamente de la respectiva unidad académica. Este sector posee la responsabilidad primaria de la atención de los

trámites que afectan la actuación académica de los alumnos. Es el único punto de contacto del alumno de grado con los registros de su situación académica.

En cuanto a los procedimientos relacionados con el registro y mantenimiento de actas de exámenes, el sector de Despacho de Alumnos posee responsabilidad sobre los siguientes trámites, entre otros:

- Inscripción de alumnos para cursado.
- Inscripción de alumnos para exámenes finales.
- Emisión, por el sistema informático, de listas de exámenes (actas en blanco).
- Registro de entrega de actas en blanco a los profesores, debiendo comunicarse diariamente cualquier novedad a la respectiva Oficialía.
- Recepción de reclamos de alumnos por rectificaciones de actas de exámenes.
- Emisión de certificados provisorios.
- Inicio de trámites para otorgamiento de diplomas.

Oficialía

El sector de Oficialía posee dependencia jerárquica de la unidad académica respectiva. Ajusta sus operaciones a la normativa y recomendaciones funcionales de la Oficialía Mayor de la Universidad.

El sector de Oficialía posee como responsabilidad primaria la recepción, registro, almacenamiento y custodia de las *actas de exámenes finales* de la dependencia académica.

Oficialía también es responsable de mantener el archivo de los graduados de la dependencia (datos personales, desempeño académico, etc.) y procesar todos los trámites rela-

cionados con: otorgamiento de diplomas, informes a asociaciones profesionales, certificaciones, etc.

El sector de Oficialía tiene bajo su responsabilidad los siguientes trámites:

- Recepción y control de las actas manuscritas, completadas por el/los docente/s con las calificaciones y datos estadísticos, trámites que certificarán con la entrega del recibo correspondiente.
- Emisión, por el sistema informático, del acta final y acta copia (esta última, para el docente), con las calificaciones correspondientes. Recepción del acta final firmada por el/los docente/s responsable/s, con certificación del personal actuante.
- Cancelación de la condición de pendiente en el libro de actas entregadas en devolución por los docentes.
- Emisión de certificados definitivos o verificados contra actas de exámenes, tanto para alumnos activos como para graduados.
- Emisión de actas por trámites de equivalencia (actas de equivalencias).
- Emisión de actas por trámites de rectificaciones. (actas rectificativa).
- Completado del legajo para otorgamiento de diplomas.
- Mantenimiento del archivo de graduados.

Área de informática

El sector de informática posee dependencia jerárquica de la unidad académica respectiva. Ajusta sus funciones a las directivas y recomendaciones técnicas u operativas emitidas por la Prosecretaría de Informática de la Universidad.

El sector de informática es un sector opcional dentro de la respectiva dependencia académica.

Hoy en día el sistema de gestión académica se encuentra centralizado en la Prosecretaría de Informática (PSI). Más adelante, en el título *Sistema informático de gestión académica en la Universidad Nacional de Córdoba*, se cuenta con mayor detalle sobre el sistema de gestión académica.

2.1.2 Tipos de actas

A lo largo del proceso de gestión académica existen diferentes tipos de actas involucradas.

Actas en blanco: designadas también *listas de examen*; se refieren a las actas producidas por el sistema informático una vez finalizado el procedimiento de inscripción previa a los turnos de exámenes, y que son remitidas a los tribunales examinadores para asentar en las mismas las notas de desempeño académico. Una vez completadas por los docentes pasan a designarse como *actas manuscritas*.

Acta manuscrita: hace referencia a las listas de exámenes o actas en blanco después que han sido asentadas las notas obtenidas por los alumnos por puño y letra del docente interviniente, y con las estadísticas correspondientes, una vez finalizados los respectivos exámenes.

Actas de exámenes: hace referencia a los diferentes tipos de actas producidas como resultado de los exámenes finales, y en las cuales queda asentado o registrado el desempeño académico de los alumnos de grado una vez finalizados los exámenes. Actas de examen, actas de exámenes y actas de exámenes finales se entenderán como expresiones sinónimas.

Acta final: hace referencia al tipo de acta de examen producido por el sistema informá-

tico, y que se obtiene como resultado de volcar en tal sistema el contenido de las actas manuscritas y de imprimirlas por los medios adecuados. Expresión sinónima de acta final informática o acta definitiva.

Acta Copia: ejemplar que es *copia del acta final*, que se produce por impresión mediante el sistema informático de modo análogo al acta final, a fin de ser entregada al docente una vez que ha suscripto el acta definitiva correspondiente.

2.1.3 Procedimiento actual

A continuación se enumeran los pasos, controles y responsabilidades en cada uno de los procedimientos de la gestión académica, desde que se genera un acta de examen hasta que el alumnos obtiene el diploma.

Generación de acta de examen final

Las actas de examen final son los documentos que sustentan el sistema de desempeño académico del alumno. Dentro de las particularidades de cada unidad académica, los requisitos mínimos de las actas de exámenes finales son los siguientes:

- Identificación de unidad académica, carrera y materia.
- Identificación del alumno (apellido y nombre, matrícula, DNI o CUIL).
- Condición del alumno de acuerdo a la normativa de la unidad académica (por ejemplo, regular, promocional, libre, etc.).
- Nota final (en números y letras).
- Firma del alumno.

- Estadística en cada acta/folio (total alumnos, aprobados, aplazados, etc,).
- Cada folio de acta posee un número correlativo en base a un sistema de codificación única para la Oficialía de cada unidad académica. Este sistema incluye la numeración por acta (la que puede incluir varios folios). Por ejemplo, "Libro 143 Acta 395, 1/3" indica el primero de los tres folios perteneciente al acta número 395 del libro número 143.
- Firma del o de los docente/s.

Toda rectificación para corregir errores cometidos en el proceso del acta debe ir nuevamente firmada por el/los mismo/s docente/s firmante/s del acta.

La generación de las actas de examen final requiere los siguientes pasos:

Paso 1: Inscripción para examen final La inscripción para el examen final es responsabilidad del Despacho de Alumnos. Esto lo realiza el alumno por medio del sistema de auto-gestión, para lo cual existen controles que son determinados por la autoridad de la dependencia académica (régimen de correlatividades, regularidades, pago de contribuciones, etc).

Paso 2: Emisión de listas de exámenes La emisión de *listas de exámenes* o *actas en blanco* es responsabilidad del Despacho de Alumnos. Esto se realiza por medio del sistema informático; se produce un ejemplar y los folios se numeran. En este paso se mantiene un registro de actas en blanco entregadas a los tribunales de exámenes (se registra fecha, identidad y firma del docente que las retira); se informa diariamente a la Oficialía sobre las actas en blanco emitidas.

Paso 3: Confección de actas manuscritas En este paso el docente confecciona las actas de examen (actas manuscritas) y las devuelve a Oficialía.

El tribunal docente es el responsable de hacer firmar al alumno en el acta manuscrita donde figure la nota del examen, a los efectos de notificación de la calificación obtenida y no como control de asistencia.

En el caso de exámenes orales, el acta manuscrita debe ir firmada por todos los integrantes del tribunal; en el caso de exámenes escritos, debe ir firmada como mínimo por el profesor titular o el profesor encargado de la cátedra o asignatura.

Por último el docente entrega a Oficialía el acta manuscrita completa, dentro del plazo establecido por las normas propias de cada dependencia académica, el que no podrá superar los 20 días hábiles a partir de la fecha fijada para el comienzo del examen.

Paso 4: Generación del acta final Normalmente apenas Oficialía de la facultad o escuela recibe el acta manuscrita carga de forma inmediata el contenido del acta. En caso de imposibilidad, se efectúa una fotocopia de la misma, entregando al docente el acta manuscrita o bien una fotocopia de la misma. Se cargan a las notas a partir del ejemplar que quede en poder de Oficialía. Hoy en día se permite que el docente puede cargar por si mismo el acta en el sistema Guaraní.

Una vez producida el acta final, es decir, una vez emitida por el sistema informático, como resultado terminal del proceso de carga de notas y de impresión a través del sistema, se fijará cita al docente para que proceda a firmar el acta final, entregar el acta manuscrita para el libro de copias o fotocopia en su poder y reciba el acta copia emitida por el sistema informatizado.

El acta final, en la cual se debe cargar de manera fiel y completa las notas o calificaciones contenidas en el acta manuscrita con todos sus datos, emitida por el sistema informático, debe ser cuidadosamente controlada y firmada como mínimo por el profesor titular o el profesor encargado de la cátedra o asignatura. A partir de su emisión, control y firma, el acta final es el documento de trabajo para toda referencia o procedimiento de control en

cuanto al desempeño académico del alumno. El acta copia, que debe ser idéntica al acta final, es el documento que queda en poder del docente una vez que haya suscripto el acta final.

Oficialía se encarga de verificar el correcto llenado de las actas; certificar firma del docente y verificar que no se hayan realizado agregados manuales de alumnos a las actas manuscritas.

Luego Oficialía encuaderna y archiva las actas, tanto las actas finales como las actas manuscritas.

Oficialía también es el responsable de archivar el acta final dentro de muebles provistos de medidas de seguridad adecuadas (armario metálico con llave, caja fuerte ignífuga, etc.). Se archivan en el orden que resulte más indicado a los efectos de su uso, en lo posible en orden correlativo, a efectos de facilitar los procesos de control.

La responsabilidad por la guarda y custodia de las actas manuscritas corresponde al decano o director de la unidad o dependencia académica. Desde su emisión, las actas manuscritas deben estar siempre separadas y almacenadas en lugares distantes con respecto a las actas finales, y deben archivarse ordenadas por su número correlativo.

Paso 5: Copia digital de actas en soporte informático Oficialía Mayor cuenta con una copia digital de las actas de exámenes finales, por medio de la cual pueda realizar los controles para el muestreo a la hora del trámite de solicitud de diplomas.

Esta copia se encuentra actualizada y su integridad asegurada por las medidas de seguridad que establezca la Prosecretaría de Informática.

Generación de actas especiales

Se consideran actas especiales a las actas de rectificaciones y las actas de equivalencias. La emisión de actas especiales de rectificaciones y de equivalencias también posee un procedimiento sugerido.

Paso 1: Solicitud de rectificación o equivalencia Una vez producida la resolución decanal correspondiente, Oficialía emite el acta correspondiente al trámite(rectificativa o de equivalencia), en dos copias, y requiere las firmas de las autoridades y/o profesores involucrados.

Paso 2: Archivado de actas especiales Oficialía archiva las actas especiales siguiendo él mismo procedimiento que las actas de exámenes.

Emisión de certificados analíticos

Los certificados analíticos son emitidos por el sistema informático, incluyendo una marca con la leyenda “No verificados en actas”, “Provisorio”, etc. según el caso que corresponda.

Trámite de egreso

De acuerdo a las definiciones del Ministerio de Educación de la Nación, un egresado es quien ha cumplimentado los requerimientos del plan de estudios, no exigiéndose para ello la tramitación del diploma correspondiente, por lo cual es conveniente distinguir el trámite de egreso del trámite de graduación.

El trámite de egreso se inicia de oficio o a solicitud del alumno en el Despacho de Alum-

nos una vez que haya cumplido todos los requisitos exigidos por el plan de estudios. Este trámite deberá completarse como máximo dentro de los dos meses posteriores a la finalización del año académico.

Paso 1: Inicio del legajo de egresado Despacho de Alumnos emite un certificado de materias rendidas del alumno, el cual contiene al menos los siguientes datos: nombre y apellido, número de legajo, denominación de la carrera y título, listado de materias rendidas u otorgadas por equivalencia, calificaciones, fecha y número de acta.

Se inicia un legajo especial, "legajo de egresado", el que incluirá como mínimo el certificado de materias rendidas del alumno.

En esta instancia se debe verificar que estén aprobadas todas las materias correspondientes al plan de estudios y que se haya respetado el régimen de correlatividades y demás requisitos académicos y reglamentarios. En caso de no coincidir, se cita al alumno para aclarar e incorporar la documentación aportada por el mismo al respectivo legajo. Cada unidad o dependencia académica realiza los controles adicionales que considere necesarios (por ejemplo: comprobantes de pagos de contribución, constancia de baja de biblioteca, etc.). Se deja registro que permitan identificar fecha y personal interviniente.

Despacho de Alumnos transfiere el legajo del egresado verificado a Oficialía de la unidad académica o dependencia académica.

Paso 2: Pase de legajo a Oficialía de la unidad o dependencia académica Oficialía de la unidad o dependencia académica verifica que los registros de exámenes declarados en el certificado de materias rendidas se correspondan con los que constan en las actas finales, recurriendo a las actas manuscritas en caso de dudas.

Una vez verificado, emite por el sistema informático de gestión de alumnos el proyecto de resolución decanal de egresados con la lista de los alumnos en tal condición. Éste

es elevado al decanato o dirección para su firma adjuntando el certificado de materias rendidas con control en actas y firma de Oficialía. Registrándose en el sistema el número de la resolución y el hecho que se encuentra firmada. La resolución es publicada en el Digesto electrónico de la UNC.

Se archivan los legajos verificados en archivos de egresados y devuelve a Despacho de Alumnos los legajos incompletos o rechazados para que se complete el trámite.

Sólo una vez cumplidos estos pasos se emite en Oficialía, y a solicitud del egresado, el certificado analítico final. El solicitante debe confirmar, en carácter de declaración jurada, los datos y leyenda que aparecen en el certificado analítico final. Previo a su emisión, la unidad académica o dependencia puede solicitar el cumplimiento de requisitos adicionales que considere pertinentes.

El trámite de egreso también debe ser realizado para el caso de los alumnos que hayan cumplido los requerimientos académicos para obtener un título intermedio.

Trámite de graduación

Se denomina graduado a la persona que ha cumplido los requisitos académicos y reglamentarios para la obtención de un título y ha obtenido el diploma correspondiente.

El trámite de solicitud del diploma es el evento final producido por el sistema informático de gestión de alumnos, y es posterior al trámite de egreso.

La confección del diploma conlleva los siguientes pasos:

Paso 1: Solicitud de diploma El aspirante a graduado completa la solicitud del diploma en el sistema informático de gestión de alumnos. Luego presenta la solicitud firmada a

Oficialía.

Debe confirmar, en carácter de declaración jurada, los datos y leyenda que aparecerán en el diploma.

Será requisito para la obtención del diploma, que el aspirante haya completado la encuesta del recién graduado (SIU-Kolla).

Al momento de la solicitud del certificado analítico y/o diploma, las unidades académicas deben comunicar al interesado, que sus datos como graduados serán publicados en el Registro Público de Graduados Universitarios perteneciente a la Dirección Nacional de Gestión y Fiscalización Universitaria del Ministerio de Educación de la Nación.

Paso 2: Confección de la resolución de graduados La Oficialía de la unidad o dependencia académica incorpora la solicitud de diploma al legajo de egresado. Agrega además, como mínimo, una copia del DNI.

Eleva el proyecto de resolución de graduados emitido por el sistema informático de gestión de alumnos con la lista de los solicitantes en condiciones de recibir el diploma. Luego se eleva al decanato o dirección para su firma adjuntando copia del certificado analítico final firmado por Oficialía. Posteriormente se registra en el sistema el número de la resolución y el hecho que se encuentra firmada. La resolución deberá ser publicada en el Digesto electrónico de la UNC.

Se archivan los legajos verificados en archivos de egresados.

Por último se envía a Oficialía Mayor por sistema informático de gestión de graduados, la resolución decanal de graduados firmada.

Paso 3: Emisión de diplomas Oficialía Mayor verifica que la resolución decanal de graduados firmada coincida con la cargada en el sistema informático de gestión de graduados e imprime los correspondiente diplomas a través del sistema informático.

Oficialía Mayor verifica uno por uno los diplomas con el listado de la Resolución. Luego registra los diplomas en el sistema informático del Ministerio de Educación de la Nación.

Se firman los diplomas por las autoridades correspondientes. Una vez firmados se envían los diplomas al Ministerio de Educación de la Nación u organismo que corresponda, para su legalización.

Hoy en día la Dirección Nacional de Gestión y Fiscalización Universitaria (DNGyFU) es la repartición dentro del Ministerio de Educación, Cultura, Ciencia y Tecnología de la Nación responsable de la intervención de diplomas y certificados analíticos de egresados de instituciones universitarias argentinas.

Para iniciar el trámite de legalización, la universidad debe completar datos personales del egresado, los académicos de la carrera y los administrativos referidos al trámite del diploma. Hoy en día estos datos son importados del sistema informático de gestión académica, lo que permite la reducción de tiempos y limitación de errores de carga.

Los datos son cotejados por la DNGyFU que, con el uso de tecnología de cruzamiento de datos, coteja la carga con las reglamentaciones vigentes, lo que permite detectar inconsistencias. De esta evaluación puede surgir la aprobación o la necesidad de subsanar o rectificar alguna información suministrada. En este último caso, se avisa a la universidad para que subsane el error y vuelva a iniciar el trámite.

Una vez que la DNGyFU aprueba la solicitud, la universidad debe remitir la imagen del diploma o certificado, se coteja con los datos suministrados y las firmas de los funcionarios actuantes. Una vez aprobado el diploma o certificado, se incorpora al *Registro Público de*

Graduados Universitarios[1]. En ese momento la universidad puede proceder a la entrega del diploma o certificado.

Se envían a la unidad académica los diplomas legalizados. Los diplomas rechazados se devuelven al área correspondiente para la rectificación del trámite.

Finalmente se registra en el libro de grados los graduados con la fecha de la colación de grados.

2.1.4 Marco normativo

Los procedimientos de registro y archivo de la actividad académica han sido establecidos en distintas ordenanzas y resoluciones del Honorable Consejo Superior. En el contexto de la enseñanza de grado, tiene especial relevancia la Ordenanza del HCS N°7/2004 [4]. En esta ordenanza se establecen:

- La organización funcional de las áreas de enseñanza de las distintas unidades académicas.
- Los procedimientos básicos relacionados con el registro del desempeño de los alumnos de grado.
- Las normas de archivo de la documentación de desempeño académico.
- Las normas mínimas de administración y seguridad del sistema informático de desempeño académico.

En su artículo 6°, ordena:

[1] https://registrograduados.siu.edu.ar/

> “Establecer que las actas de examen, firmadas por los docentes responsables integrantes del tribunal examinador, sobre soporte de papel, tienen el carácter de documentos públicos y son las únicas fuentes originales de información para certificar el desempeño académico de los estudiantes de grado de la Universidad Nacional de Córdoba. Los profesores firmantes son los únicos responsables de la nota del alumno escrita en las actas de examen.”

Como puede apreciarse, si bien se reglamenta el uso del sistema informático, también se establece que la fuente última de verdad son las actas en papel.

La Ordenanza del HCS N°6/14 establece el contenido, características y formato de los certificados analíticos que emiten las distintas unidades académicas de la universidad.

La Ordenanza del HCS N°17/14 dispone el modo de confeccionar los diplomas y certificados analíticos cuando una carrera se dicta bajo la modalidad a distancia.

La Ordenanza del HCS N°7/15 aprueba el sistema informático de gestión de graduados, en la que se hace referencia al certificado de materias rendidas que deben emitir los despacho de alumnos de cada unidad académica.

La Resolución Ministerial 231-E/2018 de fecha 7 de febrero del 2018 en su ANEXO IF-2017-30740979-APN-DNGU#ME, se aprueba el "Procedimiento simplificado para la intervención de diplomas, certificados analíticos y demás certificaciones universitarias". Lo que implica que el diploma y el certificado analítico deben confeccionarse conforme a la resolución ministerial de reconocimiento oficial y validez del título.

2.2 Sistema informático de gestión académica en la Universidad Nacional de Córdoba

La Universidad Nacional de Córdoba utiliza SIU-Guaraní como sistema informático de gestión académica. SIU-Guaraní es un sistema desarrollado por Sistema de Información Universitaria (SIU), un organismo que desarrolla distintos sistemas de gestión dirigidos a las universidades nacionales, y que depende del Consejo Interuniversitario Nacional (CIN).

SIU-Guaraní registra las actividades de la gestión académica dentro de la universidad desde que un alumno se inscribe hasta que egresa.

El objetivo de SIU-Guaraní es la administración de las tareas académicas, con la finalidad de obtener información consistente para los niveles operativos y directivos.

Entre sus principales funcionalidades se destacan las siguientes [5]:

Para los docentes:

- Consulta de agenda de clases: comisiones asignadas y alumnos inscriptos.
- Consulta de agenda de mesas de exámenes, calidad de alumnos inscriptos (libre, regular, etc.).
- Alta y baja de evaluaciones parciales.
- Ingreso y consulta de notas de evaluaciones parciales.
- Carga de notas en actas de examen, cursado y promoción.
- Recepción y envío de mensajes.
- Creación de cursos en Moodle.
- Asistencia de alumnos.

Para los alumnos:

- Inscripción a exámenes y cursadas.
- Reinscripción a carrera.
- Consulta de créditos.
- Consulta de inscripciones, plan de estudios e historia académica.
- Consulta de cronograma de evaluaciones parciales.
- Notas de evaluaciones parciales.
- Materias regulares.
- Agenda de clases.
- Solicitud de certificados.
- Actualización de datos censales.
- Recepción de mensajes.

Para autoridades:

- Consulta de ficha del alumno: carreras, regularidades, historia académica, títulos, promedios, sanciones, certificados solicitados, pérdidas de regularidad, readmisiones, etc.
- Consulta de actas de examen, actas de regulares y promociones.
- Consulta de planes de estudio.

Si bien inicialmente cada facultad administraba su propio sistema de gestión académica, con el correr de los años esa administración se fue centralizando en la Prosecretaría

de Informática, mediante el proceso de delegación establecido en la ordenanza. Es decir, cada facultad es dueña de los datos, y determina los usuarios y roles necesarios, pero la administración de las bases de datos, actualizaciones, personalizaciones del sistema y resolución de problemas técnicos son responsabilidad del personal de la Prosecretaría. Esta unificación en la administración ha tenido también su correlato en la unificación de las bases de datos. Hasta el año 2017, por motivos en parte técnicos y en parte organizacionales, cada unidad académica tenía su propia instancia de base de datos. En el año 2017 se comenzó la migración a la versión 3 de Guaraní, y en este proceso se han unificando todas las bases de datos en una base única gestionada a nivel central. Esa migración culminó en el primer semestre de 2019 para las carreras de grado, y en septiembre de 2019 la migración de las carreras de posgrado.

Una pregunta que nos hacemos en esta instancia es **¿De qué forma se puede garantizar que el resultado registrado en sistema informático no ha sido alterado?** Aquí es donde podemos pensar en firma digital y blockchain. Por ahora solo se realizará una introducción teórica de ambos conceptos y en el desarrollo del proyecto se responderá a esta pregunta.

2.3 Firma digital

La firma digital [6][7] es un mecanismo de protección de la integridad de un documento u objeto digital.

Los documentos digitales son, por ejemplo, texto escrito en un procesador de textos, un email, un sitio web, una planilla de cálculo, un PDF y toda información contenida en un soporte electrónico.

La firma digital, a diferencia de una firma tradicional, no es un nombre sino que consta de dos *claves*. Consiste en aplicar mecanismos criptográficos al contenido de un documento digital con el objetivo de demostrar al receptor del documento lo siguiente:

1. **autenticación:** el emisor del documento digital es real, ha sido producido (o al menos procesado) por el firmante.
2. **no repudio:** el firmante no puede negar la validez de su firma.
3. **integridad:** el documento no ha sido alterado desde su firma.

La firma digital es legal, pero su objetivo no es dar fe de un acto de voluntad por parte del firmante, sino encriptar los datos de un documento para conferirle mayor seguridad [8].

Las firmas digitales se basan en la criptografía de clave pública, también conocida como criptografía asimétrica. Normalmente hay tres algoritmos involucrados con el proceso de firma digital:

1. Generación de dos claves que están matemáticamente vinculadas: un algoritmo proporciona una clave privada junto con su clave pública correspondiente.
2. Firma: algoritmo que produce una firma al recibir una clave privada y el documento digital que se está firmando.
3. Verificación: algoritmo que comprueba la autenticidad del documento digital al verificarlo junto con la firma y la clave pública.

Un concepto muy relacionado a firma digital es el término **hash**. La función resumen o hash es el resultado de algoritmos que consiguen crear a partir de una entrada (ya sea un texto, una contraseña o un archivo, por ejemplo) una salida alfanumérica de longitud normalmente fija, que representa un resumen de toda la información que se le ha dado. Es decir, a partir de los datos de la entrada crea una cadena que solo puede volverse a crear con esos mismos datos.

Para crear una firma digital, el software de firma crea un hash unidireccional de los datos electrónicos que se deben firmar. La clave privada se usa para encriptar el hash. El hash cifrado junto con otra información es la firma digital.

Cualquier cambio en los datos, incluso un mínimo cambio en la foto como pasarla a blanco y negro o eliminando un solo carácter, da como resultado un valor diferente. Este atributo permite a otros validar la integridad de los datos mediante el uso de la clave pública del firmante para descifrar el hash.

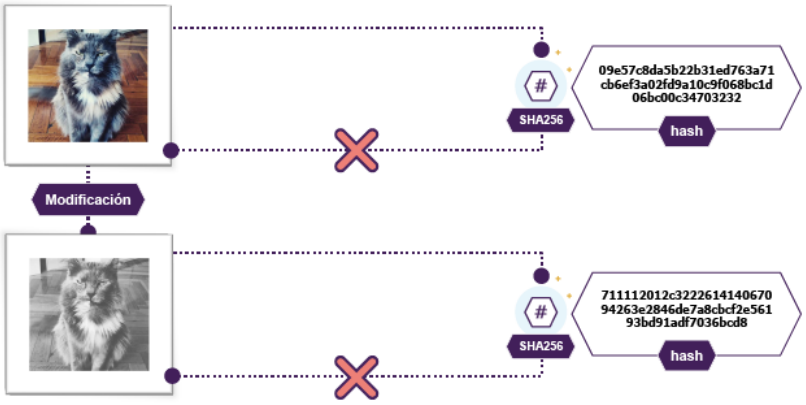


FIGURA 2.1 – Resultado de aplicar la función hash. [Internet] [acceso el 05 de marzo de 2021] *Blockchain Federal Argentina*. Disponible en: https://bfa.ar/blockchain/criptografia

Si el hash descifrado coincide con un segundo hash calculado de los mismos datos, prueba que los datos no han cambiado desde que se firmó. Si los dos hash no coinciden, los datos se han alterado de algún modo (*integridad*) o la firma se ha creado con una clave privada que no corresponde a la clave pública presentada por el firmante (*autenticación*).

Las firmas digitales dificultan que el firmante niegue haber firmado algo (*no repudio*), suponiendo que su clave privada no se haya visto comprometida, ya que la firma digital es única tanto para el documento como para el firmante, y los une.

Un **certificado digital**, un documento electrónico que contiene la firma digital de la autoridad emisora del certificado, vincula una clave pública con una identidad y se puede usar para verificar que una clave pública pertenece a una persona o institución en particular.

A la hora de implementar firma digital las preocupaciones más comunes que enfrentan las personas e instituciones cuando se trata de documentos en papel son: ¿Es la persona que

firmó el documento quien dicen ser? ¿Cómo puedo verificar si la firma es válida y no ha sido falsificada? ¿Cómo compruebo si el documento ha sido alterado?

Además de facilitar los procesos y prevenir la falsificación de documentos, el uso de la firma digital proporciona beneficios adicionales de validación. En el caso donde se necesita una garantía de que un documento no ha sido alterado durante la transmisión, una firma digital evitará que las alteraciones desconocidas pasen desapercibidas.

Si el contenido firmado digitalmente se altera, la firma se invalidará, lo que alertará al remitente y al receptor de una infracción. Esto se debe a que las funciones criptográficas aplicadas evitarán que se produzca una firma nueva y válida para ese documento.

La mayoría de los métodos de no repudio proporcionan un **sello de tiempo** que no se puede alterar y proporcionan evidencia de la firma digital en caso de que la clave privada se haya visto comprometida o revocada. El sello de tiempo garantiza la no alteración de una serie de datos asociados con la firma como la fecha y hora de realización de la firma.

Las firmas digitales se usan ampliamente para proporcionar pruebas de autenticidad, integridad de los datos y no repudio de las comunicaciones y transacciones realizadas a través de Internet.

2.3.1 Firma digital en Argentina

En la República Argentina se sancionó el 14 de noviembre de 2001 la Ley 25.206 [9] referente a firma digital. Fue publicada en el Boletín Nacional el 14 de diciembre de 2001 donde se establece que la firma digital posee el mismo valor probatorio que la firma autógrafa.

La ley define firma digital como al resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante,

encontrándose bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma.

Los procedimientos de firma y verificación a ser utilizados para tales fines serán los determinados por la Autoridad de Aplicación en consonancia con estándares tecnológicos internacionales vigentes.

La Ley 25.506 establece en su artículo 12:

> "La exigencia legal de conservar documentos, registros o datos, también queda satisfecha con la conservación de los correspondientes documentos digitales firmados digitalmente."

En el ámbito de la Universidad Nacional de Córdoba a partir de la Resolución Rectoral RR-2019-570-E-UNC-REC se crea el Área de Firma Digital, dependiente de la Secretaría General del Rectorado.

La firma digital en la UNC permite mejorar la eficiencia para todo tipo de actuaciones administrativas. Numerosos actos administrativos sólo se firman digitalmente, como por ejemplo, las resoluciones rectorales.

2.4 Blockchain

Blockchain o "cadena de bloques descentralizada", como se podría traducir al castellano, ha pasado de ser desconocido a que no pase un día sin que aparezca una noticia sobre esta tecnología.

Más allá del Bitcoin, que fue la primera aplicación de blockchain, ha surgido otra aplica-

ción basada en blockchain que es particularmente relevante para este proyecto: los contratos inteligentes o smart contracts.

En esta sección se comenzará definiendo blockchain y sus características para luego profundizar los conceptos de smart contracts.

A grandes rasgos, blockchain se puede pensar como un libro contable, una bitácora o una base de datos donde solo se puede ingresar entradas nuevas y donde todas las existentes no se pueden modificar ni eliminar. Esas entradas, llamadas *transacciones*, se agrupan en bloques que se van agregando, sucesivamente, al registro en forma de cadena secuencial, cada uno de ellos relacionado necesariamente con el anterior.

En ese esquema, si se quisiera corregir información ya registrada, solo se puede realizar mediante el agregado de nueva información. Los datos originales siempre van a permanecer y pueden ser fiscalizados en cualquier momento.

En lugar de tener información centralizada en una sola computadora y con unos pocos usuarios con capacidad de modificarla, una cadena de bloques está replicada a lo largo de toda una serie de computadoras bajo un modelo de *red de pares*, que agregan datos solo a partir del *consenso* (acuerdo) de las partes.

Blockchain tiene una particularidad que hasta el momento no se daba en el mundo digital: *es imposible que alguna persona, ni siquiera quienes almacenan una copia de la información puedan alterar datos en la cadena de bloques.*[10]

Red de pares

Considere que el registro de la información en lugar de estar almacenado en un solo servidor, se replica permanentemente en un conjunto de computadoras, conocidos como *nodos*, que forman una red de pares. Cada vez que alguien agrega una entrada al registro, esa transacción se suma a otras para componer un bloque. Este se agrega a la cadena y de

forma casi automática se replica en todas esas computadoras conectadas. Así, se garantiza la seguridad de esa información ya que, por ejemplo, habría que "hackear" gran parte de la red y no solamente un servidor central para poder modificarla, borrarla o robarla.

Pero también se tiene que tener en cuenta que la blockchain no solo está protegida por este modelo de red descentralizada, sino que también está atravesada por métodos criptográficos que garantizan que nada pueda ser borrado o alterado sin que todos los usuarios puedan darse cuenta de ello.

En redes centralizadas, el ataque a un nodo crítico pondría en riesgo a toda la estructura.

En una red de blockchain, todos los nodos que sellan transacciones, llamados *selladores o mineros* acuerdan contribuir con el mantenimiento y el procesamiento del registro. Y lo hacen bajo una plataforma distribuida: una estructura confiable y que puede sobrevivir tranquilamente si una de las partes de la red se ve comprometida.

Función hash

Gran parte de la seguridad de la información en blockchain se debe al uso de métodos criptográficos para encriptar la misma, y una de las principales herramientas para hacerlo son los llamados *hash*.

Como se explicó anteriormente un *hash* es un código que se obtiene al procesar información a través de una función. Si se modifica aunque sea algo muy pequeño de esa información, como el color de una foto, o simplemente agregar un acento en un documento de texto, el hash va a cambiar completamente. Los hash suelen llamarse digestos o resúmenes, porque normalmente tienen un tamaño fijo y de pocos dígitos.

Así, al registrar hashes de documentos en blockchain, se puede tener la certeza de detectar si alguien cambia su contenido, ya que esas modificaciones harían que el hash de la nueva versión sea completamente diferente.

Esta técnica permite dejar de lado la necesidad de almacenar, por ejemplo, fotos en blockchain. Con solo almacenar el hash, y dejar esa foto en nuestra computadora, servidor o nube, se tiene la certeza de que será posible detectar si alguien la modifica. O mejor aún, se tendrá la certeza de que ni uno mismo, responsables de esa foto, lo podremos modificar sin que nadie se entere.

Al mismo tiempo, no se puede reconstruir la información original a partir de un hash, por lo cual se asegura que no se esta brindando acceso a alguna persona no deseada, por más que ese hash esté registrado públicamente en la blockchain.

Cadena de bloques

Los hash también juegan un papel elemental en la arquitectura de blockchain. Cada bloque de información que se suma al registro posee necesariamente el hash del bloque de información anterior.

De nuevo, al procesar el hash de un bloque y almacenarlo en el siguiente, podemos tener la certeza de que el bloque anterior no puede ser modificado. Si alguien intentara cambiar algo, el hash de ese bloque sería completamente diferente al que ya tenemos registrado y toda esa red de pares que almacena el registro distribuido se percataría de ello.

Transacciones

Las operaciones que se realizan para agregar información a una blockchain son denominadas *transacciones*.

Su contenido puede ser muy variado y generalmente depende del tipo de red que se esté operando: hay redes blockchain que por medio de transacciones permiten subir archivos digitales al registro. Otras, orientadas estrictamente al intercambio de criptomonedas, toman forma de operaciones de compra-venta de activos. Una transacción puede ser simplemente una línea de texto, o incluso un hash de un documento almacenado fuera de la

cadena de bloques.

Cada transacción es enviada a la red a través de un nodo, y se combina con otras transacciones para conformar un bloque. Cuando ese bloque se agrega a la cadena, la transacción queda incorporada definitivamente y se considera como “completada”.

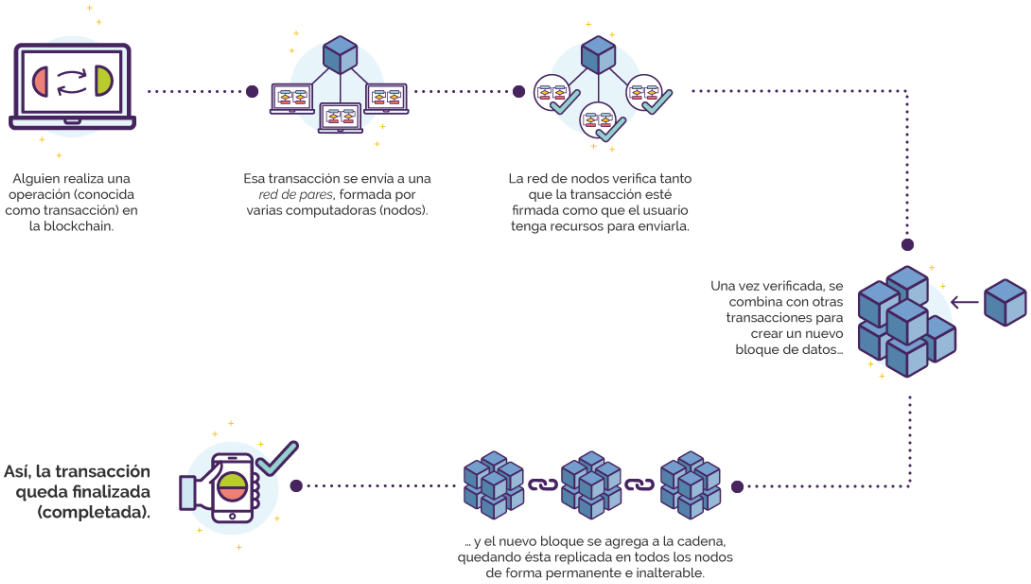


FIGURA 2.2 – Transacciones en blockchain. [Internet] [acceso el 05 de marzo de 2021] *Blockchain Federal Argentina*. Disponible en: https://bfa.ar/blockchain/bloques-y-transacciones

Protocolos de consenso

En blockchain, el proceso de armar un bloque de transacciones y sumarlo definitivamente en la cadena se llama *sellado o minado*. Cuando un bloque queda sellado, la información que contiene pasa a formar parte de la cadena de forma permanente, inmutable e inalterable. El protocolo de consenso es el mecanismo que regula la forma en que los nodos que sellan bloques llegan a un acuerdo entre sí para poder hacerlo e incorporar ese bloque a la cadena.

Hay varias formas de implementar ese protocolo. La más común de todas se denomina

proof of work o prueba de trabajo. En este modelo todos los nodos son pares iguales en la red, y todos compiten para sellar un bloque antes que el resto y poder conseguir criptomoneda a cambio. Para realizar esto, deben resolver un algoritmo complejo. El que primero logre hacerlo y pueda agregar un bloque a la cadena es el obtendrá esa recompensa (criptomoneda). Pero para realizar ese trabajo se necesita un alto nivel de procesamiento, lo que se termina traduciendo en un mayor costo energético.

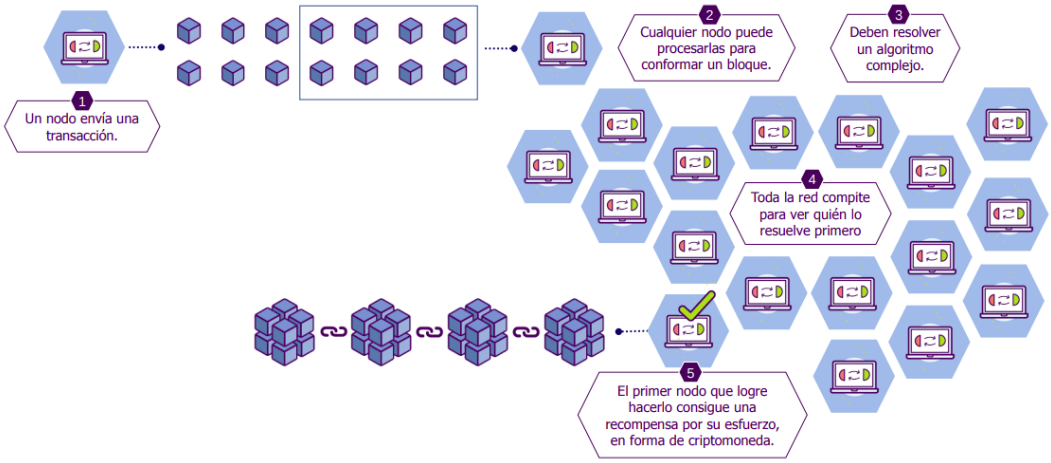


FIGURA 2.3 – Protocolo de consenso: prueba de trabajo o proof of work. [Internet] [acceso el 05 de marzo de 2021] *Blockchain Federal Argentina*. Disponible en: https://bfa.ar/blockchain/protocolos-de-consenso

En el modelo de *proof of authority o prueba de autoridad*, solo hay una cantidad determinada de nodos que están autorizados a resolver el sellado de bloques.

Este protocolo no está basado en la competencia, sino en el hecho de que ese grupo reducido que tiene permisos para agregar bloques a la cadena se turne para hacerlo. Como aquí no hay necesidad de resolver algoritmos complejos, la cantidad de procesamiento es mínima. Por eso se considera a estos modelos como livianos y más eficientes en relación a consumo energético.

La otra gran característica es que generalmente en modelos de prueba de autoridad no hay circulación de criptomonedas con valor económico, ya que en realidad no es necesaria una recompensa por esa participación.

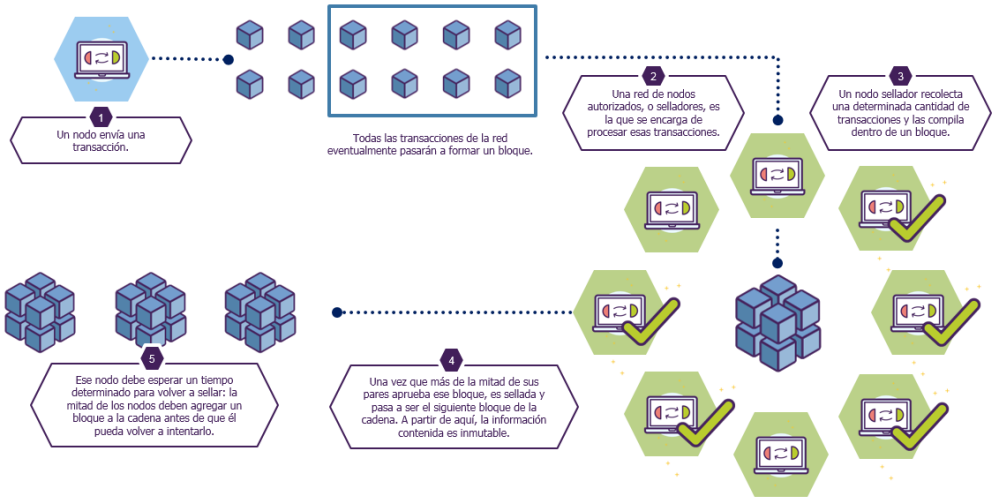


FIGURA 2.4 – Protocolo de consenso: prueba de autoridad o proof of authority. [Internet] [acceso el 05 de marzo de 2021] *Blockchain Federal Argentina*. Disponible en: https://bfa.ar/blockchain/criptografia

Características de blockchain

A continuación se listan las características esenciales de blockchain[16]:

Distribuida: Una de las características más diferenciales de blockchain es que no puede ser controlada por una sola entidad. Dado que la base de datos se replica en todos los nodos, nadie puede manipular los registros sin dejar evidencia.

Segura: Al no tener ningún punto o servidor central, blockchain es una red blindada ante cualquier ciberataque que pueda comprometer la seguridad de la red.

Blockchain funciona sin intermediarios, no hace falta una persona, empresa o institución que legitime la información guardada en la cadena, ya que es segura por naturaleza

Está garantizada por la matemática, por la criptografía.

Transparente: La información contenida en blockchain se puede consultar para compro-

bar que existe. Cualquier participante en una blockchain determinada puede hacerlo.

No solo todo agregado al registro se incorpora de forma pública y visible para todos los usuarios, sino que cualquiera de ellos, inclusive de forma anónima, puede validarlo. En definitiva, cualquier persona puede velar por la integridad de la información contenida en la cadena de bloques.

Anónima: El uso de cifrado y de criptografía asimétrica permite que blockchain tenga diferentes niveles de anonimato.

Auditable: Poder garantizar en cada transacción la identidad de las partes involucradas, ya que todas las transacciones son firmadas criptográficamente. Toda la información almacenada en la cadena es completamente auditable: se incorpora de forma pública y visible para todos los usuarios.

Inalterable: La información es inmutable e inalterable: no es posible modificarla ni borrarla. De la misma forma que en un libro contable, las entradas no se pueden borrar o modificar, solo agregar.

Se trata de un registro en constante crecimiento. Cada dato que se suma a la cadena lo hace integrando un nuevo bloque. Si esa información se quiere modificar, solo puede hacerse mediante datos nuevos que corrijan los anteriores, pero los originales nunca se borran, permanecen siempre en la cadena y pueden ser fiscalizados.

Así, de forma casi orgánica, una blockchain siempre suma nueva información a medida que se agregan nuevos bloques. Crece permanentemente.

2.4.1 Contratos inteligentes

Blockchain funciona como un registro de transacciones, pero también habilita la programación de aplicaciones a través de los llamados *contratos inteligentes o smart contracts*. Estos desarrollos pueden tanto ejecutarse como consecuencia de transacciones como generar, ellos mismos, transacciones nuevas.

El término contratos puede ser un poco confuso, porque no son justamente contratos. Son más bien flujos de tareas programables dentro de blockchain, que abren la posibilidad de desarrollar aplicaciones.

A diferencia de una aplicación tradicional, donde se tiene que confiar en las garantías que da su desarrollador, en un contrato inteligente es posible programar un flujo de tareas preestablecido entre partes interesadas, apoyado en todas las garantías de confianza y transparencia que nos da una red de cadena de bloques.

Gracias a los contratos inteligentes se pueden realizar tareas cada vez más complejas. Así, se puede dejar de pensar en blockchain como un mero registro y comenzar a pensar procesos como seguimiento de licitaciones, sistemas de trazabilidad de productos, plataformas de documentos vivos, y mucho más.

Características de los contratos inteligentes

A continuación se listan las características esenciales de los contratos inteligentes[16]:

Ahorro: Gracias a la automatización de procesos y a la no necesidad de intermediarios.

Agilidad: La automatización también permite agilizar procedimientos y facilitar así el cumplimiento de un contrato.

Seguridad: Al ser un sistema encriptado se mantiene la seguridad de los documentos. Se evita el riesgo de manipulación por parte de terceros, puesto que la ejecución es automática. Por el hecho de ser un sistema distribuido existen copias exactas e inmutables de todos los registros.

Autonomía: No se necesitan intermediarios para formalizar y ejecutar un contrato inteligente.

Transparencia: La característica esencial del contrato inteligente es la transparencia ya que la información que recoge es inamovible e inmutable y visible para todos.

De estas característica se desprende que los contratos inteligentes o Smart Contracts tienen ventajas únicas que pueden agilizar los procesos burocráticos actuales y fomentar la confianza y transparencia.

2.4.2 Blockchain Federal Argentina

El avance de blockchain ha demostrado que esta tecnología guarda una enorme capacidad para garantizar seguridad, resiliencia y transparencia en diferentes tipos de procesos. Estas características, sumadas a la posibilidad de programar flujos de transacciones y contratos inteligentes nos permiten dejar de pensar solamente en un mero registro y empezar a pensar en la posibilidad de desarrollar todo un ecosistema de aplicaciones confiables y efectivas, garantizadas por la cadena de bloques.

La Blockchain Federal Argentina (BFA) es plataforma multiservicios abierta y gratuita pensada para integrar servicios y aplicaciones que puedan heredar todas las características de blockchain. Una iniciativa confiable y completamente auditable que permita optimizar procesos y funcione como herramienta de empoderamiento para toda la comunidad.[10]

Blockchain Federal Argentina fue concebida dentro de un espacio de trabajo colaborativo,

y apunta a reproducir ese patrón como bases de la plataforma.

El modelo de gobierno es de *múltiples partes interesadas o multistakeholder* representa tanto una ventaja como una responsabilidad. Escuchar diferentes voces y construir un esquema a partir de distintas perspectivas es una obligación asumida como necesaria para desarrollar proyectos que atraviesan a todos los sectores de la sociedad. Pero al mismo tiempo es una estrategia que toma forma de ventaja diferencial para hacer frente a los diferentes desafíos que se presenten en nuestro camino. Participan organizaciones gubernamentales, de la academia, empresas y organizaciones de la sociedad civil. La Universidad Nacional de Córdoba ha participado en la BFA desde su comienzo, y es uno de los cuatro selladores que comenzaron a operar la red el 27 de septiembre de 2018.

Diseñada para potenciarse a través de los aportes de sectores públicos, privados, académicos y de la sociedad civil, BFA opta por una estrategia donde la participación de toda la comunidad es esencial, desde la ingeniería organizacional hasta el despliegue de la infraestructura.

Características en la BFA

A continuación se listan las características esenciales de la Blockchain Federal Argentina:

Sin criptomoneda: Blockchain Federal Argentina está diseñada específicamente para no poseer criptomoneda asociada.

El incentivo para participar en BFA es favorecer el desarrollo de servicios e iniciativas basadas en la innovación tecnológica y en un trabajo horizontal entre diversos actores.

No es necesaria la implementación de una moneda virtual para aprovechar las ventajas que blockchain nos proporciona. Se opta por un camino que no se alimenta de la competencia entre las partes: el objetivo para participar no es la acumulación de moneda virtual, no es

la ganancia.

Modelo liviano: Al no requerir la resolución del algoritmos complejos para el minado de criptomonedas, se habilita la implementación de mecanismos de consenso eficientes, tanto en lo relativo a cantidad de transacciones por unidad de tiempo como en el consumo eléctrico.

BFA está basada en un protocolo de *prueba de autoridad*, requiere de muchos menos recursos que una blockchain tradicional que utiliza prueba de trabajo.

Permisionada: BFA funciona bajo el modelo de una blockchain permisionada. Al utilizar un método de prueba de autoridad, se puede estructurar una red en base a un conjunto confiable, una determinada cantidad de nodos selladores autorizados, en lugar de basar el procesamiento en un conjunto de mineros anónimos compitiendo por la creación de un bloque.

Además, en Blockchain Federal Argentina la distribución de nodos selladores está garantizando la representatividad de los sectores en el procesamiento de la cadena.

Plataforma - Aplicaciones: La utilización de la BFA es pública. Las organizaciones que deseen desarrollar servicios y/o aplicaciones sobre la blockchain solo deberán aceptar un acuerdo de utilización y buenas prácticas, pero no estarán obligados a desplegar nodos selladores. BFA se encargará de la infraestructura mientras que los usuarios desarrollarán las aplicaciones.

Transacciones gratuitas: Las transacciones realizadas sobre Blockchain Federal Argentina no tienen costo.

Al no poseer una criptomoneda asociada, y estructurar la red bajo el modelo de prueba de autoridad con un costo de infraestructura marginal, las transacciones en BFA son gra-

tuitas. El *combustible*[2] necesario para realizarlas será provisto, sin ningún costo asociado, por Blockchain Federal Argentina. Esta asegurará también las medidas para evitar abusos.

Software libre: El software de Blockchain Federal Argentina se basa en una implementación abierta y robusta. Todos los desarrollos y modificaciones que se realizan son abiertos, de modo que puedan ser públicamente auditados por cualquier interesado, más allá de los participantes de la organización.

La transparencia inherente en el modelo queda también garantizada desde el código.

Almacenamiento off-chain: En BFA no se almacenan documentos o archivos dentro de la blockchain, solo se guardan los hashes de esos documentos.

Los usuarios, los servicios, son responsables de resguardarlos de la manera que consideren más adecuada, pero al tener los digestos criptográficos sellados en la blockchain encuentran la forma de demostrar que esos documentos no fueron modificados luego de que ese hash se obtuvo.

Tecnología en la BFA

Ethereum: BFA está basada en la tecnología *Ethereum*[3], una de las redes blockchain públicas más difundidas a nivel internacional. Es una plataforma descentralizada que funciona con prueba de trabajo y permite a cualquier desarrollador crear y publicar aplicaciones distribuidas para ejecutar contratos inteligentes o smart contracts garantizados por la cadena de bloques. La red posee una infraestructura de nodos a nivel global.

Como el desarrollo está basado en código abierto, toda la comunidad puede participar en las pruebas de concepto existentes para mejorar la plataforma, o tomar todo ese trabajo y

[2] ver Destilería de gas

[3] https://ethereum.org

adaptarlo a otros contextos y necesidades.

Blockchain Federal Argentina toma el software de Ethereum, utilizando prueba de autoridad, sin criptomoneda asociada.

Nodos: La red está integrada por distintos tipos de nodos.

Los *nodos selladores* conforman la estructura central de la red confiable de BFA ya que son los únicos que pueden sellar (agregar) bloques a la cadena. Todos ellos están desplegados por miembros de la organización. BFA estará inicialmente estructurada a partir de 23 nodos selladores.

Los selladores están conectados solamente entre sí, y a los *nodos tipo gateway*, que actúan como buffer entre ellos y el resto de la red.

Los *nodos transaccionales o transaction nodes* son aquellos que pueden enviar transacciones para que luego sean agregadas a la cadena por los nodos selladores. Usualmente son ejecutados por operadores de servicios que utilizan la blockchain (los que implementan aplicaciones). Cualquier usuario puede ejecutar este tipo de nodos. Solo debe contar con una cuenta registrada en BFA y aceptar las políticas de uso.

Existen también *nodos solo lectura o read-only nodes*. Estos son parte de la red de pares, reciben todos los bloques y sus transacciones. Pueden funcionar como validadores o auditores, verificando que todos los bloques sean válidos. Cualquier usuario puede correr este tipo de nodos, sin necesidad de registrarse (anónimo) ni contar con autorización de BFA. También podrían servir para acceder a la información por parte de una aplicación o servicio.

Destilería de gas: Para enviar transacciones a la blockchain se necesita *combustible* llamado **Ether**, que BFA distribuye a aquellos operadores registrados de nodos transaccionales que desplieguen aplicaciones sobre la plataforma.

El Ether no tienen ningún tipo de valor económico y se envía periódicamente mediante un espacio operado por la organización. Así, se implementa un modelo donde se evita la especulación y/o el tráfico, además de posibilitar métodos para detectar el abuso.

Al mismo tiempo, para reafirmar la transparencia, cualquier nodo solo lectura que se integre a la red podrá verificar la fidelidad de la información, sin necesidad de poseer Ether para realizarlo.

Monitoreo: Cada entidad que administre un nodo de BFA es responsable de su mantenimiento y monitoreo. De hecho no existe en la red un sistema central de administración.

Como apoyo, Blockchain Federal Argentina implementa un esquema de monitoreo a través del NOC (Network Operation Center), permitiendo estar atento al funcionamiento de los nodos selladores y gateway. El mismo no posee una única ubicación centralizada sino que se encuentra distribuido geográficamente y entre varias partes de la organización.

Sello de tiempo: Existen modos de certificar contenidos a través de blockchain. Estos mecanismos permiten generar una *prueba de existencia*, algo así como un sello digital que demuestra que el contenido de un mensaje existía antes de una fecha y hora determinada y no fue modificado.

El servicio de *Time Stamping Authority o TSA*[4] desarrollado por BFA permite demostrar o evidenciar que un determinado archivo digital se ha mantenido inalterado en el tiempo a partir de una determinada fecha.

Hay varias formas de utilizar la TSA de Blockchain Federal Argentina, de acuerdo a las necesidades y posibilidades de cada usuario.

[4]https://bfa.ar/sello

Gobernanza en la BFA

Toda la comunidad tiene las puertas abiertas para participar en Blockchain Federal Argentina. Individuos, organismos, instituciones o empresas de cualquier sector interesados en desplegar aplicaciones y servicios aprovechando todas las características de la plataforma, o simplemente contribuir al primer desarrollo de esta índole en el país, pueden sumarse a la iniciativa y comenzar a participar.

Hay dos grandes formas de integrarse a la Blockchain Federal Argentina: como usuarios del servicio o como partes de la organización.

La Cámara Argentina de Internet (CABASE), la Asociación Red de Interconexión Universitaria (ARIU) y la Network Information Center Argentina (NIC Argentina) decidieron emprender esta iniciativa, que hereda años de experiencia en proyectos conjuntos. Antecedentes como la primer red Anycast de DNS autoritativo en el país se fueron gestando a partir de la multiplicidad de visiones y de un mismo compromiso: potenciar y democratizar el espacio tecnológico en nuestro país para que pueda transformarse en una economía de vanguardia de cara a los desafíos del siglo XXI.

Estos organismos traen la experiencia de un modelo de Gobernanza y Múltiples Partes Interesadas, regido por el trabajo colaborativo y la cooperación entre miembros de diferentes sectores del ecosistema de Internet.

Esta experiencia histórica, reforzada por el trabajo en espacios de colaboración regional e internacional como Corporación de Internet para la Asignación de Nombres y Números (ICANN), Internet Society (ISOC), Registro de Direcciones de Internet de América Latina y Caribe (LACNIC), LACTLD y el Foro de Gobernanza de Internet (IGF), deja su marca en el camino de Blockchain Federal Argentina.

La plataforma está diseñada pensando en una infraestructura que garantice la interopera-

bilidad y la sinergia entre emprendimientos similares en toda América Latina y el Caribe.

Imaginar una blockchain regional nos permite tomar todas sus ventajas y multiplicar exponencialmente sus beneficios y su solidez, transparencia y seguridad.

El diseño tanto técnico como de gestión de Blockchain Federal Argentina no solo es pensado para garantizar que la iniciativa sea escalable gracias a la incorporación de nuevos participantes, sino también a asegurar su continuidad en el tiempo: que perdure más allá de las personas e instituciones que lo gestaron gracias a un modelo de trabajo horizontal y colaborativo.

2.5 Antecedentes

Existen diferentes instituciones que haciendo uso de la tecnología blockchain buscan realizar propuestas innovadoras para evitar fraudes en instituciones educativas.

La Universidad de Nicosia, institución privada de educación superior más grande de Chipre, ha implementado blockchain para almacenar toda la información sus diplomas y certificados.[26]

Varias instituciones han estado desarrollando herramientas que utilizan blockchain para rastrear y certificar sus títulos. El Massachusetts Institute of Technology (MIT) desarrolló una plataforma llamada *Blockcerts*[5] en donde implementa blockchain en programas educativos.

Blockcerts es una plataforma de código abierto que se centra principalmente en la emisión y verificación de certificados usando blockchain. Utiliza principalmente la blockchain de Bitcoin, el soporte de Ethereum también se está implementando y se puede usar para

[5]https://www.blockcerts.org/

propósitos de prueba en este momento.

Muchas instituciones educativas de la India han realizado gran variedad de publicaciones en revistas u organizaciones científicas intentando buscar soluciones para detectar el fraude en la emisión de títulos.

La publicación científica *Education Degree Fraud Detection and Student Certificate Verification using Blockchain*[27] de julio de 2020 realizada por la Universidad Smt. Indira Gandhi College Of Engineering plantea que el fraude de certificados académicos (título universitario, doctorado o cualquier certificación de estudios) es un hecho y viene mediante la falsificación, así como mediante la participación de las autoridades y empleados de la institución. Demostrar de forma inequívoca que dispone de un certificado académico es un proceso que cambia en cada país o institución de educación. Consideran que el uso de blockchain descentralizado es una solución sencilla, simple y económica que permite la verificación fácil, confiable y barata de documentos oficiales, como títulos universitarios.

La School of Electrical Engineering and Computer Sciences (SEECS) - National University of Sciences and Technology (NUST) de Pakistán realizó un trabajo de investigación en diciembre de 2019 llamado *A Blockchain-Based Accreditation and Degree Verification System*[28] donde comenta que el fraude de certificados académicos es una práctica generalizada que socava la inversión y la confianza en los sistemas de educación y conlleva importantes costos económicos y sociales. Los sistemas de verificación de certificados suelen consumir mucho tiempo, son costosos y burocráticos, por lo que proponen una solución de verificación de certificados basada en blockchain llamada Cerberus.

Al día de hoy son muchas las propuestas y esfuerzos que se llevan adelante, pero no hay una solución a nivel global ni a nivel nacional que se adapte a las diversas instituciones educativas.

En el marco del Consejo Federal de Educación, las autoridades educativas del país aprobaron el 29 de mayo de 2008 la Resolución Nº 53/07, por la cual se encomienda al Ministerio

de Educación de la Nación la elaboración de un Proyecto de Resguardo Documental de los Títulos y Certificaciones de Estudios correspondientes a la finalización de la Educación Secundaria y de la Educación Superior. Este proyecto busca fortalecer la confiabilidad de la documentación educativa en tiempos donde muchos títulos y certificados analíticos son adulterados, falsificados y/o presentan carencias en el resguardo documental.[19]

Son numerosos los casos de adulteración de contenido, falsificación de firmas y ausencia de medidas de seguridad en la documentación educativa, lo que conlleva a la incertidumbre en relación a la autenticidad de la misma.

En 2005 se publica la noticia en donde la Universidad de Formosa (UNaF), en acuerdo con el World College de Ushuaia y el Instituto Cibernos de Madrid, otorgaron títulos irregulares. Un estudiante español, que nunca pisó Argentina logró obtener un certificado analítico de la carrera Licenciatura en Sistemas. El certificado analítico emitido por la Universidad Nacional de Formosa con la firma del decano de la Facultad de Economía indica que el estudiante completó su carrera en sólo 10 meses. El documento certifica que el alumno rindió y aprobó todas las materias del plan de estudios. El escándalo le costó el puesto al rector de la UNaF y al decano de Economía. Once empleados fueron procesados. *Fuente: UNCUYO Prensa*[20]

En 2008 se publica la noticia en donde la Universidad de Tucumán (UNT) había emitido 70 títulos falsos a estudiantes de Derecho en cuyos certificados analíticos figuraban materias que no rindieron. *Fuente: Clarin*[21]

Al poco tiempo, se confirmó que la Fundación Unión de Centros Educativos (FUCE) ofrecía carreras a distancia de la Universidad de La Matanza (UNLaM) a centros universitarios españoles sin haber firmado ningún convenio. La UNLaM negó toda vinculación con la FUCE.

En 2017 una docente adulteró su título de profesora, presentando un título falso de profesora de física en su legajo docente. El título apócrifo le permitió la designación de horas.

El título falso que estaba en su legajo supuestamente era de la Universidad Nacional de La Plata (UNLP) pero tenía un sello de la Universidad de Mar del Plata.

Tras la investigación quedó imputada por haber adulterado título de profesora de física expedido por la Universidad Nacional de La Plata, en fecha 30 de marzo de 2015; haber adulterado certificado analítico de finalización de estudios de la UNLP; haber adulterado certificado del Programa de Diplomatura Superior en Intervención Educativa en la Universidad expedido por la Universidad Nacional de San Martín en fecha 16 de junio de 2016; haber adulterado certificado de Diplomado Superior en Ciencias Sociales con Mención en Currículum y Prácticas Escolares expedido por la Facultad Latinoamericana. *Fuente: Diario de Misiones Primera Edición*[22]

Esta situación no solo se da a nivel nacional, a continuación se comentan algunos casos en otros países.

En 2015 se da a conocer que la universidad de Agra (India) otorgó miles de títulos falsos durante la última década. Detectaron que se habían otorgado más de 100 títulos a familiares de empleados universitarios que ni siquiera estudiaron en la universidad. La universidad tiene la distinción de tener como estudiantes a varias personalidades nacionales, políticas y sociales de la India. *Fuente: India Today*[23]

En 2015 un organismo gubernamental investigó un sitio web en China que vendía certificados de grado falsos de muchas universidades del Reino Unido. *Fuente: BBC*[24]

En 2015 el director ejecutivo de Axact, una compañía de software acusada de administrar una fábrica de diplomas, fue arrestado en Pakistán después de descubrir un almacén lleno de títulos falsos. *Fuente: New York Times*[25]

Como se puede notar el fraude académico es una realidad, no solo en Argentina, es una preocupación a nivel mundial. Los diplomas falsos son un desafío para las instituciones educativas.

2.6 Vinculación tecnológica

Argentina el 4 de junio conmemora el día de la *Vinculación Tecnológica* por el nacimiento de Jorge Alberto Sábato, físico y tecnólogo argentino, famoso por el desarrollo del *Triángulo de Sábato* como modelo de política científico-tecnológica. En Argentina, desde 1990 se dispone de la *ley 23.877 de Promoción y Fomento de la Innovación Tecnológica*, que tiene por objeto mejorar la actividad productiva a través de la promoción y fomento de la investigación y desarrollo, la transferencia de tecnología, jerarquizando la tarea del científico, del tecnólogo y del empresario innovador.

En la propuesta que se cuenta más adelante en este trabajo se podrá notar que se requiere de dos instancias de vinculación. Por un lado la vinculación y participación de la Universidad Nacional de Córdoba en la Blockchain Federal Argentina (BFA), y por otro lado la vinculación con la comunidad del Sistema de Información Universitaria (SIU) perteneciente al Consejo Interuniversitario Nacional (CIN).

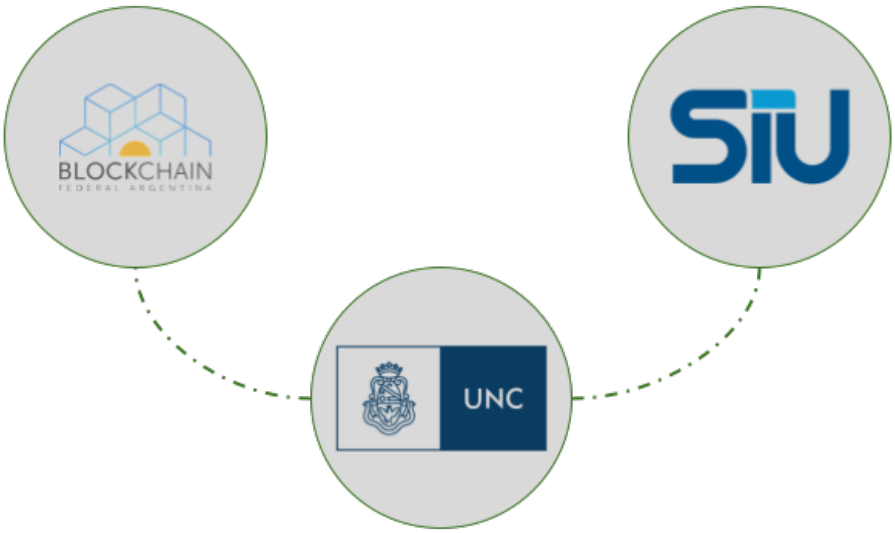


FIGURA 2.5 – Vinculación. *Elaboración propia.*

Para la existencia de la BFA se necesita de la colaboración del estado y sector privado para contar con la infraestructura, y del conocimiento científico para que se encuentre en

funcionamiento.

Dada la necesidad de llevar adelante este proyecto la Universidad Nacional de Córdoba es un actor maś que forma parte de aportar conocimiento técnico-científico a BFA. Éste proyecto será un caso de uso más que formará parte de la BFA.

Como se comentó anteriormente el sistema de gestión académico que se utiliza en la universidad es Guarani, sistema desarrollado por la comunidad SIU. Este trabajo final integrador implicará un trabajo en conjunto entre la UNC y el SIU para poder generar el nuevo proceso.

En el desarrollo técnico de este trabajo se darán a conocer en detalle los diferentes interesados o stakeholders que requieren vincularse para poder llevar adelante el proyecto.

2.7 Gestión de proyecto

Para poder llevar adelante el proyecto es necesario gestionarlo. La gestión de proyecto es la aplicación de conocimientos, habilidades, herramientas y técnicas a las actividades del proyecto para cumplir con los requisitos del mismo.

En un proyecto existen muchas restricciones, pero hay tres que se consideran especialmente importantes, que son comunes a todos los proyectos: alcance, coste y tiempo (plazo). Para referirse a estas tres restricciones y su interacción a lo largo del proyecto se utiliza el término *triple restricción* y se representa como un triángulo equilátero.

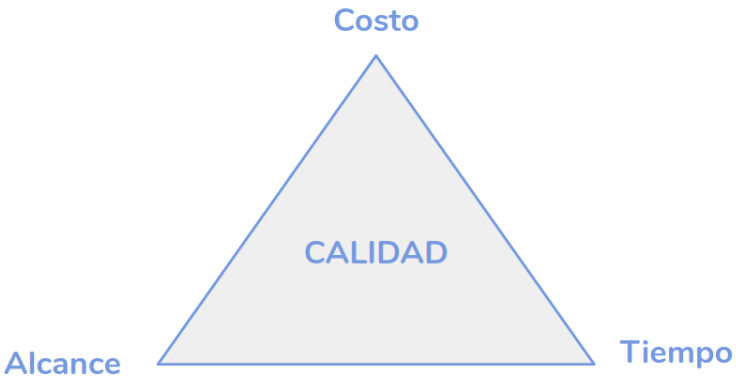


FIGURA 2.6 – Triple restricción. *Elaboración propia.*

- **Alcance:** cada proyecto produce un único producto (bien o servicio), el alcance del proyecto describe y limita el trabajo requerido para conseguir el producto.
- **Coste:** esta variable no solo incluye el dinero, incluye todos los recursos que se necesitan para llevar a cabo el proyecto, el coste incluye personas, equipamientos, materiales, etc.
- **Tiempo:** todos los proyectos vienen delimitados por el tiempo, siempre hay una fecha que cumplir.

La teoría dice que este triángulo hipotético siempre mantiene su forma equilátera. En otras palabras, si movemos una de las restricciones, entonces se moverá o ajustará por lo menos otra, para que el triángulo recupere su forma de equilátero.

En la gestión de los proyectos se debe realizar siempre un balance de las delimitaciones del alcance, costo y tiempo. En la imagen se muestra un triángulo en el que cada lado representa cada variable. Si una de las variables se modifica, el resto de las variables también cambiará.

La calidad es otra dimensión que está relacionada con la triple restricción y hay quienes piensan que el producto de la triple restricción es la calidad o consideran a la calidad

como una cuarta restricción, pero en realidad los requisitos de calidad están definidos como parte de las características del producto.

La gestión de proyectos se logra mediante la aplicación e integración adecuadas de procesos de la dirección de proyectos, agrupados de manera lógica, categorizados en cinco grupos de procesos.

Un *proceso* es un conjunto de acciones y actividades, relacionadas entre sí, que se realizan para crear un producto, resultado o servicio predefinido. Cada proceso se caracteriza por sus entradas, por las herramientas y técnicas que se pueden aplicar y por las salidas que se obtienen.

Project Management Body of Knowledge (PMBOK) [18] diferencia los siguientes cinco grupos de procesos de la dirección de proyectos:

- **Grupo de procesos de inicio:** aquellos procesos realizados para definir un nuevo proyecto o nueva fase de un proyecto existente al obtener la autorización para iniciar el proyecto o fase.
- **Grupo de procesos de planificación:** aquellos procesos requeridos para establecer el alcance del proyecto, refinar los objetivos y definir el curso de acción requerido para alcanzar los objetivos propuestos del proyecto.
- **Grupo de procesos de ejecución:** aquellos procesos realizados para completar el trabajo definido en el plan para la dirección del proyecto a fin de satisfacer las especificaciones del mismo.
- **Grupo de procesos de monitoreo y control:** aquellos procesos requeridos para rastrear, revisar y regular el progreso y el desempeño del proyecto, para identificar áreas en las que el plan requiera cambios y para iniciar los cambios correspondientes.
- **Grupo de procesos de cierre:** aquellos procesos realizados para finalizar todas las

actividades a través de todos los Grupos de Procesos, a fin de cerrar formalmente el proyecto o una fase del mismo.

Los grupos de procesos de la dirección de proyectos se vinculan entre sí a través de las salidas que producen.

Los procesos de la dirección de proyectos están vinculados por entradas y salidas específicas, de modo que el resultado de un proceso se convierte en la entrada de otro proceso.

Los grupos de procesos no son fases del ciclo de vida del proyecto. De hecho, es posible que todos los grupos de procesos se lleven a cabo dentro de una fase. Dado que los proyectos están separados en fases diferenciadas o subcomponentes, por lo general todos los grupos de procesos se repiten en cada fase.

Los grupos de procesos rara vez son eventos discretos o únicos; son actividades superpuestas que tienen lugar a lo largo del proyecto. La salida de un proceso normalmente se convierte en la entrada para otro proceso o constituye un entregable del proyecto, subproyecto o fase del proyecto. Los entregables a nivel del subproyecto o del proyecto pueden llamarse *entregables incrementales*.

Un *entregable* es cualquier producto, resultado o capacidad de prestar un servicio, único y verificable, que debe producirse para terminar un proceso, una fase o un proyecto. Los entregables son componentes tangibles completados para alcanzar los objetivos del proyecto y pueden incluir elementos del plan para la dirección del proyecto.

La naturaleza integradora de la gestión de proyectos requiere que el grupo de procesos de monitoreo y control y el resto de grupos de procesos ejerzan acciones uno sobre los otros de manera recíproca. Los procesos de monitoreo y control transcurren al mismo tiempo que los procesos pertenecientes a otros grupos de procesos. Por lo tanto, el grupo de procesos de monitoreo y control se considera como un grupo de procesos *de fondo* para los otros cuatro grupos de procesos.

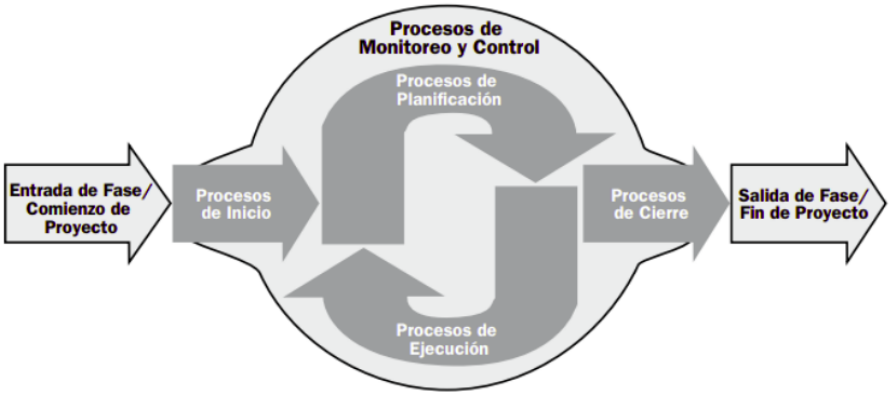


FIGURA 2.7 – Grupo de procesos de la gestión de proyectos. *Fundamentos para la dirección de proyectos.* [Guía del PMBOK - Quinda edición] [2013]

Un proyecto posee un ciclo de vida. El ciclo de vida de un proyecto es la serie de fases por las que atraviesa un proyecto desde su inicio hasta su cierre. Las fases son generalmente secuenciales y sus nombres y números se determinan en función de las necesidades de gestión y control de la organización u organizaciones que participan en el proyecto, la naturaleza propia del proyecto y su área de aplicación.

Las fases se pueden dividir por objetivos funcionales o parciales, resultados o entregables intermedios, hitos específicos dentro del alcance global del trabajo o disponibilidad financiera.

Las fases son generalmente acotadas en el tiempo, con un inicio y un final o punto de control.

Las fases del proyecto se utilizan cuando la naturaleza del trabajo a realizar en una parte del proyecto es única y suelen estar vinculadas al desarrollo de un entregable específico importante.

Las fases del proyecto suelen completarse en forma secuencial, pero pueden superponerse en determinadas circunstancias de los proyectos. Normalmente las diferentes fases implican una duración o esfuerzo diferentes. Por su naturaleza de alto nivel, las fases del

proyecto constituyen un elemento del ciclo de vida del proyecto.

La estructuración en fases permite la división del proyecto en subconjuntos lógicos para facilitar su dirección, planificación y control. El número de fases, la necesidad de establecer fases y el grado de control aplicado dependen del tamaño, la complejidad y el impacto potencial del proyecto.

Mientras que cada proyecto tiene un inicio y un final definidos, los entregables específicos y las actividades que se llevan a cabo variarán ampliamente dependiendo del proyecto.

El ciclo de vida de un proyecto define:

- Qué trabajo técnico se debe realizar en cada fase.
- Cuándo se deben generar los productos entregables en cada fase y cómo se revisa, verifica y valida cada producto entregable.
- Quién está involucrado en cada fase.
- Cómo controlar y aprobar cada fase.

El ciclo de vida proporciona el marco de referencia básico para dirigir el proyecto, independientemente del trabajo específico involucrado. Los enfoques de los ciclos de vida de los proyectos pueden variar continuamente desde enfoques predictivos u orientados a plan hasta enfoques adaptativos u orientados al cambio. En un *ciclo de vida predictivo* el producto y los entregables se definen al comienzo del proyecto y cualquier cambio en el alcance es cuidadosamente gestionado. En un *ciclo de vida adaptativo* el producto se desarrolla tras múltiples iteraciones y el alcance detallado para cada iteración se define solamente en el comienzo de la misma. En el caso de este trabajo final integrador se toma un enfoque adaptativo u orientado al cambio.

En el desarrollo técnico de este trabajo se realiza un analisis detallado de las diferentes

fases que conforman el proyecto. Analizando alcance, tiempo y costo y riesgos.

3

Desarrollo técnico

En el capítulo anterior se ha realizado un análisis del proceso actual desde que se emite un acta de examen hasta que un estudiante obtiene el diploma que lo habilita a desempeñarse profesionalmente. Ha quedado de manifiesto lo engorroso que resulta la verificación de cada certificado.

El certificado de cada estudiante debe ser verificado renglón por renglón contra las actas de cada examen que ha rendido a lo largo de la carrera para poder emitirse el diploma. La automatización de este proceso es parte de la propuesta que se plantea en este trabajo.

Cuando se verifica un certificado y emite diploma, la universidad habilita a esa persona a ejercer profesionalmente por eso es importante entender la implicancia e importancia de la verificación de un certificado.

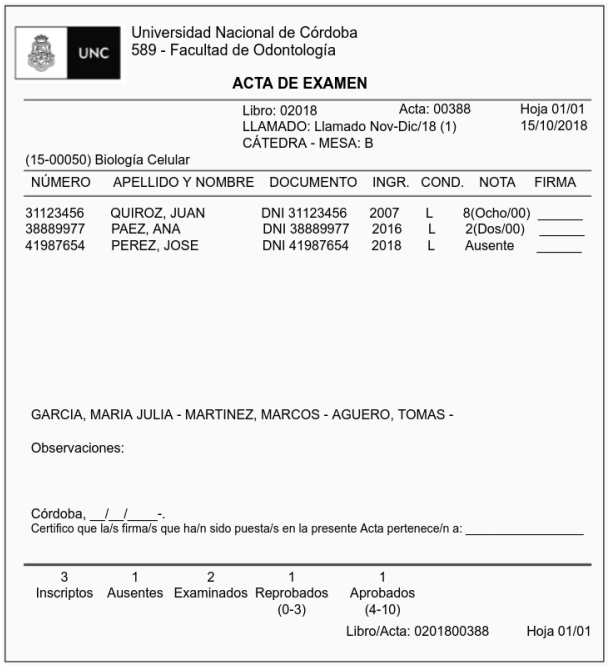
En esta sección se cuentan los detalles de la propuesta que permitiría confiar en la información que se registra en los sistemas informáticos y de este modo no acumular actas en papel generando un primer paso a la despapelización.

La transparencia es la base para poder llevar adelante esta propuesta. Se propone un sistema de registro de datos, abierto a la comunidad, con múltiples instancias de control y seguridad, tantas como actores intervengan en el proceso, en el que nadie puede eliminar datos.

A continuación se explicará como llevar adelante el proyecto.

3.1 Propuesta

Retomando el proceso de gestión académica se sabe que los resultados de los exámenes se plasman en *actas*, como la que se muestra en la figura 3.1.



Universidad Nacional de Córdoba
589 - Facultad de Odontología

ACTA DE EXAMEN

Libro: 02018 Acta: 00388 Hoja 01/01
LLAMADO: Llamado Nov-Dic/18 (1) 15/10/2018
CÁTEDRA - MESA: B

(15-00050) Biología Celular

NÚMERO	APELLIDO Y NOMBRE	DOCUMENTO	INGR.	COND.	NOTA	FIRMA
31123456	QUIROZ, JUAN	DNI 31123456	2007	L	8(Ocho/00)	_____
38889977	PAEZ, ANA	DNI 38889977	2016	L	2(Dos/00)	_____
41987654	PEREZ, JOSE	DNI 41987654	2018	L	Ausente	_____

GARCIA, MARIA JULIA - MARTINEZ, MARCOS - AGUERO, TOMAS -

Observaciones:

Córdoba, __/__/____-.
Certifico que la/s firma/s que ha/n sido puesta/s en la presente Acta pertenece/n a: _____

3	1	2	1	1
Inscriptos	Ausentes	Examinados	Reprobados (0-3)	Aprobados (4-10)

Libro/Acta: 0201800388 Hoja 01/01

FIGURA 3.1 – Modelo de acta de examen. *Elaboración propia.*

El acta contiene una serie de datos propios del acta en sí (fecha, asignatura, tribunal, etc.) y una serie de *renglones* cada uno de los cuales corresponde a un estudiante y contiene información acerca de él (nombre, número de documento, calificación, etc). Se denominará

al conjunto de datos comunes *cabecera*, independientemente de si en la versión impresa figuran en el encabezado o en el pie del acta.

Las actas son cargadas en el sistema Guaraní, impresas, firmadas de manera ológrafa por los docentes integrantes del tribunal examinador, y archivadas por el área de Oficialía de cada unidad académica en libros de actas. Cuando se imprime la versión final del acta para ser firmada se considera que el acta ha sido *cerrada*, y ya no puede ser modificada. Cualquier error que se detecte a partir de ese momento sólo puede ser corregido mediante un *acta rectificativa*.

A requerimiento del estudiante, el sistema Guaraní también emite *certificados*. Un ejemplo de certificado se muestra en la figura 3.2. Al igual que un acta, también está compuesto por una cabecera y renglones, aunque en este caso los renglones corresponden a asignaturas o actividades realizadas.

UNC

Universidad Nacional de Córdoba
589 - Facultad de Odontología

CERTIFICADO ANALÍTICO FINAL

Carrera: Odontología - Plan 2008

Título: 5254 Odontólogo

Apellido: QUIROZ
Nombres: JUAN
Documento: DNI 31123456

Materia	Cred	Fecha Examen	Cd	Nota aplazo	Nota aprobado	Libro	Acta	Pg
15-00019 Química General I		20/06/2004	L		7.00 (Siete)	00001	13180	1
15-00050 Biología Celular		15/10/2018	L		8.00 (Ocho)	02018	00338	1
15-00027 Física I		20/06/2005	R		6.50 (Seis c/50)	00015	14517	1
15-00035 Matemática I		20/06/2006	R		5.50 (Cinco c/50)	00016	00062	2
15-02302 Laboratorio I		26/07/2005	R		3.00 (Tres)	00015	15789	1
15-02302 Laboratorio I		16/12/2006	R		8.00 (Ocho)	00016	13578	3

Total de materias rendidas: 5
Total de materias aprobadas: 5
Total de aplazos: 1
Promedio con aplazos:
Promedio sin aplazos:
Total de Créditos: 0

El promedio sólo incluye a las materias que son consideradas promediables.

Fecha de ingreso: 02/12/2007

Fecha de egreso: 23/02/2019

CÓRDOBA, Rep. Argentina, VEINTIDÓS DE FEBRERO DE DOS MIL DIECINUEVE

FIGURA 3.2 – Modelo de certificado analítico. *Elaboración propia.*

Un certificado puede ser *provisorio o definitivo*. En el caso del certificado analítico definitivo, la unidad académica debe poseer un procedimiento de verificación de que su

contenido se corresponda con lo que está registrado en las actas.

Este requerimiento de verificar en actas forma parte de un conjunto de procedimientos destinados a garantizar la integridad de las calificaciones obtenidas por los estudiantes. Estos procedimientos implican una serie de controles cruzados en las que ninguna persona tiene de por sí la capacidad de alterar las calificaciones sin que esa alteración sea detectada por otros funcionarios que intervienen en el trámite. La comisión de un acto fraudulento requiere pues la colusión de varias personas pertenecientes a distintos departamentos.

Si no existiera la verificación en actas cabría la posibilidad de que los administradores del sistema informático modifiquen las notas almacenadas en la base de datos, y que esas modificaciones resulten en certificados fraudulentos, o que podría llevar a la Universidad a brindar títulos a estudiantes, habilitando futuros profesionales a ejercer.

La contrastación de los certificados con las respectivas actas conlleva un trabajo considerable. Para cada renglón del certificado es necesario buscar en papel el acta correspondiente, y verificar que los datos de dicho renglón coincidan con los registrados en el acta, como se aprecia en la figura 3.3.

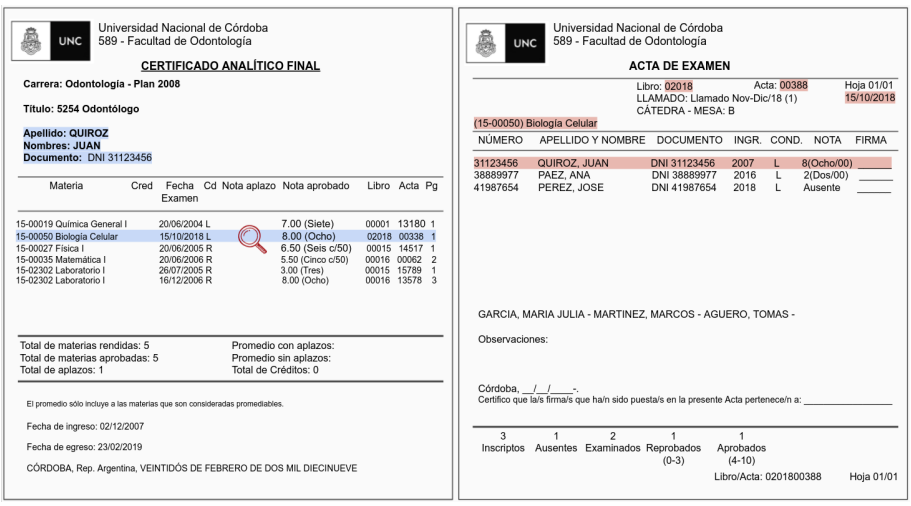


FIGURA 3.3 – Contrastación de certificados contra actas. *Elaboración propia.*

Si bien es posible disminuir el trabajo utilizando técnicas de muestreo, el problema sub-

siste: ¿De qué forma se puede garantizar que el resultado registrado en la base de datos del sistema informático no ha sido alterado?

El sistema informático de gestión académica Guaraní posee una serie de características destinadas a minimizar el riesgo, en la forma de controles de acceso y registros de auditoría. Pero esto no es suficiente, los controles de acceso no protegen contra abusos por parte del administrador de bases de datos (DBA), o incluso de usuarios con perfiles de datos privilegiados; y los registros de auditoría permiten detectar cambios a posteriori, pero tampoco protegen contra abusos del DBA, que puede modificar estos registros.

Una buena solución a este problema debe garantizar a los responsables legales de las calificaciones que estas no han sido alteradas. Claramente se trata de un problema de integridad de los datos. Esta identificación del tipo de problema permite esbozar una primera solución razonable: el uso de *firma digital*.

Firma digital

Existe el respaldo legal para reemplazar las actas en papel por actas digitales. Sin embargo, el mero reemplazo del acta en papel por un acta digital no resuelve la situación, ya que ahora se debería contrastar los certificados contra las actas digitales.

Se necesita un mecanismo que garantice la integridad de la información que posee la base de datos del sistema informático. Por lo tanto se necesitaría que se firme la información de la base de datos.

Una posible forma de resolver esto consistiría en:

1. Representar el acta en un formato procesable por una computadora (por ejemplo JSON o XML).
2. Presentar este documento digital para que se pueda validar que sus datos se corres-

ponden con la realidad.

3. Permitir la firma digital de dicho documento y almacenar el resultado.

4. Representar los certificados en un formato similar procesables por una computadora.

5. Validar los certificados contra estas actas digitales, aceptando el resultado solo si la firma del documento sigue siendo válida.

Este mecanismo resuelve algunos ítems planteados. Por ejemplo, ya no es posible para el DBA modificar un acta sin que esa modificación sea detectada, dado que el DBA no posee la clave privada necesaria para generar una firma válida.

Sin embargo, tiene varios inconvenientes:

Es complejo. La firma digital no es fácil de implementar en escala. Para mantener la seguridad de la clave privada es necesario utilizar tokens criptográficos, es decir, dispositivos de hardware que almacenan la clave en forma segura, y estos dispositivos suelen tener problemas de compatibilidad con determinados sistemas operativos y browsers. El manejo de claves no es trivial. La pérdida del PIN o contraseña implica la generación de un nuevo par de claves y la revocación del anterior.

No protege contra la eliminación de actas. Si bien puede alegarse que esto no es un problema de integridad sino de disponibilidad, esto no es cierto en todos los casos. La ausencia de una calificación desfavorable puede afectar un promedio y eso ya es un problema de integridad si esa situación no es detectada.

Cuando se detecta un error en un acta que ya está cerrada, la solución no consiste en corregir el acta, sino en elaborar una nueva acta, denominada *acta rectificativa*, que salva el error. Pero si el acta original está firmada digitalmente, esa firma sigue siendo válida. No importa que se genere una nueva acta firma, si alguien intenta validar un certificado

contra el acta original y la firma original, el certificado parecerá válido aunque ya no lo sea, debido a que el acta rectificativa ha reemplazado la nota.

La validación debería ser hecha fuera del sistema. Si es el mismo sistema de gestión académica el que valida su propia salida, podría dudarse de su integridad. El sistema debe por lo tanto brindar a algún sistema externo las actas necesarias para validar. Pero esto a su vez es otro problema: se esta dando demasiada información. Para validar un certificado de un estudiante se estaría brindando información sobre todos los estudiantes que rindieron con él.

Ninguna de estas dificultades es insuperable, sin embargo obligan a recurrir a herramientas adicionales. Por ejemplo se debería prever un mecanismo encadenado de firmas para que no se puedan borrar actas.

Cuando se analizan las características que debe tener la solución se nota que muchas de ellas coinciden con las provistas por una red *blockchain*.

Blockchain

Como se mencionó anteriormente, la firma digital es una solución parcial, ya que no resuelve problemas tales como la eliminación de actas o los asociados con las actas rectificativas. Lo que se requiere es un mecanismo que no permita modificar los datos una vez que se han registrado, y blockchain parece brindar una herramienta adecuada para implementar ese mecanismo.

Blockchain es una herramienta, y como toda herramienta debe aplicarse sólo a los problemas para los cuales es adecuada. Muchos problemas que pretenden resolverse con una red blockchain se pueden resolver de manera mucho más eficiente con una solución centralizada.

La clave aquí es la descentralización. ¿Requiere el problema una solución descentraliza-

da? Si es así, tal vez vale la pena analizar una solución basada en blockchain.

En ese sentido es útil un documento elaborado por NIST (National Institute of Standards and Technology)[17], que incluye un diagrama de flujo destinado a ayudar en la decisión sobre si es adecuado usar blockchain para un determinado problema. Este diagrama fue elaborado originalmente por The United States Department of Homeland Security (DHS) Science & Technology Directorate, y reconoce como válidos los casos de uso en los que:

1. Se requiere un almacén de datos compartido y consistente.
2. Existe más de una entidad que aporta datos o se trata de un caso de auditoría.
3. Los registros escritos no serán nunca borrados ni modificados.
4. No se almacenarán datos sensibles.
5. Es difícil determinar quién debe controlar el almacén de datos.
6. Se requiere una bitácora (log) de todo lo registrado.

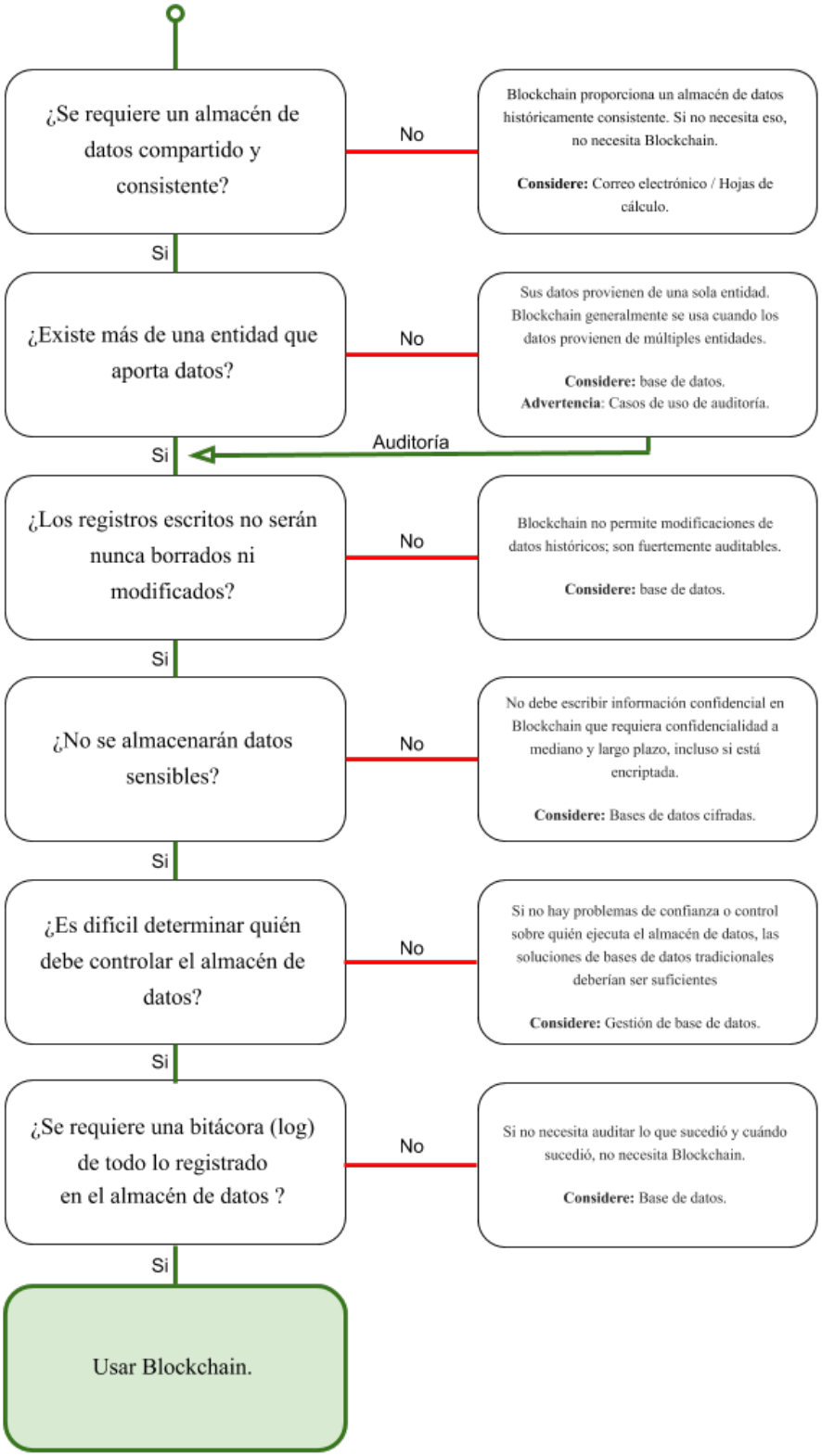


FIGURA 3.4 – Diagrama de flujo para evaluar la pertinencia de una solución blockchain. Basado en Dylan Yaga, Peter Mell, Nik Roby y Karen Scarfone. [Internet] [acceso el 13 de octubre de 2019] *Blockchain Technology Overview* NISTIR 8202. Disponible en: https://doi.org/10.6028/NIST.IR.8202

A continuación se realiza un análisis de la situación con la secuencia de preguntas propuestas por NIST:

¿Se necesita un almacén de datos compartido y consistente? Sí, se quiere tener un registro de las actas que sea verificable por múltiples partes interesadas.

¿Existe más de una entidad que aporta datos o se trata de un caso de auditoría? Los datos provienen de una fuente principal, que es el sistema de gestión informático Guaraní. Sin embargo, se quiere que estos datos puedan ser auditados por múltiples partes.

¿Los registros escritos nunca serán borrados ni modificados? Ese es justamente el objetivo que se busca.

¿No se almacenarán datos sensibles? El diseño que se realice deberá tener en cuenta que así sea.

¿Es difícil determinar quién debe controlar el almacén de datos? Precisamente se desea que nadie tenga control absoluto del almacén de datos.

¿Se requiere una bitácora de todo lo registrado? Sí, se quiere que exista un registro de todas las acciones realizadas.

Dado el análisis anterior se sabe que blockchain es una buena respuesta tecnológica para la incorporación en un nuevo proceso que garantice transparencia.

Blockchain permite mejorar la transparencia de los procesos a partir de su exposición en un entorno público, así como la trazabilidad de los datos allí colocados.

En general todos los mecanismos que implican aprobación de actividades académicas realizadas por estudiantes quedan registrados en un acta. Se pretende dejar una prueba de la existencia del acta y del contenido del acta en el momento del cierre, de esa forma

se puede garantizar a futuro tanto para los estudiantes como para las autoridades de las facultades y los profesores que firmaron las actas que esas actas no han sido modificadas, y que las notas en las cuales están basados los certificados son las que se pusieron en el momento en que se cerro el acta.

Básicamente se coloca cierta información fuera del control del área de informática, en una red pública y transparente. De este modo se puede garantizar que no cambiará una vez que se ha declarado que cierta información es tal. Todo lo que se coloca en la BFA está disponible, tanto para los que son miembros como para los que no lo son. Se busca mecanismos que maximicen la transparencia. Cualquiera puede conectarse a la BFA y ver la información que se encuentra alli. No es un mecanismo que se utilice para acceder a datos primarios, sino de auditoría.

El proceso consiste en registrar en blockchain los datos en el momento en que el acta se cierra, un mecanismo de certificación o firma por parte de las autoridades que esos datos cargados en la blockchain son reales mediante firma en blockchain por medio de claves públicas y privadas.

Para firmar cada usuario de una blockchain tiene una clave pública y una privada. La clave pública es la dirección del usuario en blockchain y todo el mundo puede conocerla; mientras que la clave privada sólo la conoce el usuario propietario de esas claves, y es la llave de acceso a los activos digitales que también permite firmar las transacciones, en este caso las actas.

El proyecto brinda un mecanismo de validación de certificados, es decir los certificados digitales emitidos por la universidad pueden ser validados comparándolos con lo almacenado en blockchain, sin necesidad de recurrir al sistema de gestión académica. De tal forma cualquiera que posea un certificado emitido por la universidad pueda validar que esté respaldado en ciertas actas emitidas en cierto momento.

Dado el análisis anterior para facilitar la gestión del proyecto se dividirá en tres fases:

- **Registro de actas:** Responsable de registrar en la red de blockchain las actas.
- **Conformidad de actas:** Permite verificar y firmar la información del acta que se encuentra en blockchain.
- **Validación de certificados:** Valida los certificados contra las actas que se encuentran en blockchain.

3.1.1 Registro de actas

En esta fase se busca registrar en la blockchain *evidencia* de las actas emitidas por el sistema de gestión académica Guaraní. El término evidencia se usa en el sentido de que lo que se guarda no es el acta misma, ya que no se debe guardar datos sensitivos en blockchain, sino una prueba de que cierta acta existía en un determinado momento.

Para ello se debe realizar el modelado del acta como un *smart contract*, en el cual se guarda un resumen o digesto criptográfico de la cabecera y de cada uno de los renglones. Ese resumen se obtiene aplicando una función de hash criptográfica, y tiene la propiedad de que es computacionalmente imposible encontrar otro mensaje o documento que produzca el mismo resumen.

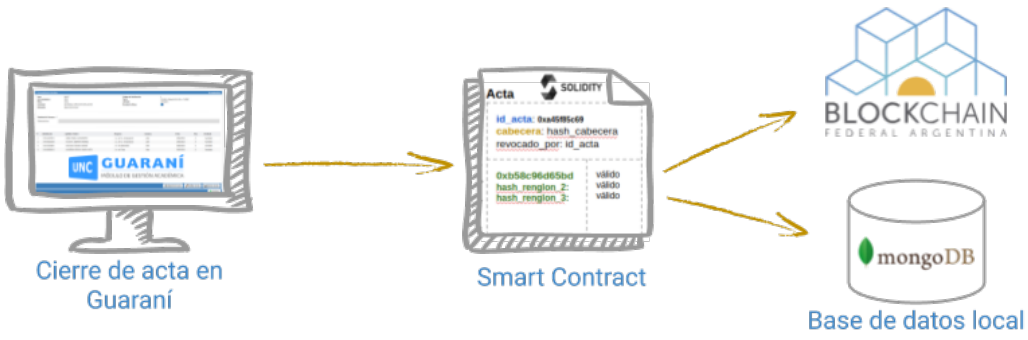


FIGURA 3.5 – Registro de actas. *Elaboración propia.*

En el sistema de gestión académica Guaraní al momento de cierre del acta, es decir cuan-

do el acta no será modificada a futuro, se transmite el contenido del acta cerrada a la blockchain de la BFA. Al mismo tiempo cuando esto sucede se preserva la información del acta en una base de datos local.

La razón para preservar el acta en una base de datos local es que cuando se emite un certificado es necesario poder reconstruir la realidad existente al momento del cierre de las actas. El acta contiene muchos datos que pueden cambiar con el paso del tiempo en el sistema de gestión académica Guaraní. Por ejemplo, el alumno puede cambiar de nombre o de número de documento. Ambas son realidades que no están modeladas adecuadamente en el sistema de gestión académica. Es decir, el sistema registra el nombre y el número de documento actual, pero no es capaz de determinar qué nombre y número de documentos estaban registrados en el momento de un determinado examen. Esta necesidad de preservar el acta en una base de datos local separada puede desaparecer si, en alguna versión futura del sistema de gestión académica Guaraní, eso comienza a ser provisto por él mismo.

3.1.2 Conformidad de actas

El sistema que permite certificar la validez del acta por medio de firma en la Blockchain Federal Argentina. Al firmar el acta se esta generando evidencia de conformidad con el contenido del acta.

Brindar conformidad significa que los funcionarios certifiquen la validez del acta por medio de su firma en blockchain. Una vez que las actas están registradas en la blockchain, los funcionarios responsables de su validez pueden firmarla. Esa firma queda registrada en el contrato.

El proceso de firma implica tener el documento PDF del acta que se desea firmar, adjuntarlo al sistema de conformidad de actas. El sistema de conformidad de actas calcula un hash, si el hash coincide con el que se encuentra en la BFA, por lo tanto lo registra como

firmador válido.

FIGURA 3.6 – Conformidad de actas. *Elaboración propia.*

Los archivos PDF poseen información no visible como la fecha de creación, el tamaño, el número de paginas entre otros. Para el caso de los archivos PDF de actas se incrusta información que se visualiza en el acta en formato JSON para que luego esto permita la firma del acta. No cualquier PDF es valido para firmar, sino solo aquel que es obtenido del sistema Guarani dado que es el que posee el JSON incrustado con toda la información del acta. Si el formato visual del PDF de acta se modifica no impactaría en el sistema de firma dado que el JSON que se incrusta en el PDF continuaría siendo el mismo.

3.1.3 Validación de certificados

Una vez que las actas se encuentran en la blockchain firmadas se está en condiciones de realizar la validación de los certificados.

La persona que desea validar un certificado debe subir al sistema validador el PDF del certificado y el sistema se encarga de recorrer renglón por renglón, identificar el acta que corresponde a cada renglón, y verificar que el resumen construido a partir del certificado coincide con el resumen registrado del acta en el contrato de blockchain.

El certificado debe tener toda la información necesaria para validarse tal y como se guar-

daron en el momento de crearse las actas.

El sistema validador busca no tener falsos positivos, pero puede tener falsos negativos. Es decir, si el sistema dice que un renglón del certificado ha sido verificado, es porque se corresponde con las actas. Por el contrario, si dice que no ha podido verificarlo simplemente dice que con la evidencia existente en blockchain no puede certificar que es válido, y debe validarse por otro medio (por ejemplo, contrastando contra las actas originales).

Para poder brindar la mayor transparencia posible en la validación de los certificados es necesario que ni la firma de las actas ni la validación de certificados requieran utilizar herramientas desarrolladas por la Universidad. Ambas operaciones se realizan interactuando directamente con blockchain. El código de los contratos desplegados en la BFA es público, por lo que cualquiera puede desarrollar su propia versión del firmador o del validador.

FIGURA 3.7 – Validación de certificados. *Elaboración propia.*

El objetivo de este diseño es maximizar la transparencia. Se registran en blockchain las actas en el momento del cierre, y a partir de ese momento la universidad no tiene posibilidades de modificar lo que ha declarado. Existe un registro auditable de todas las acciones realizadas. Y al mismo tiempo, dado que no se guardan datos primarios en blockchain, no se compromete ningún tipo de información sensible. No es posible obtener nombres de alumnos, números de documento ni calificaciones.

Como se mencionó anteriormente los archivos PDF poseen información no visible como

la fecha de creación. Para el caso de los archivos PDF de certificados también se incrusta la información que se visualiza en el certificado en formato JSON para que luego esto permita la validación del certificado. No cualquier certificado PDF puede ser validado. Sino solo aquel que es emitido por el sistema Guarani. Si el formato visual del PDF del certificado se modifica no impactaría en el sistema de validación dado que el JSON que se incrusta en el PDF continuaría siendo el mismo.

La propuesta de diseño de la interfaz gráfica se encuentra en el Anexo A.

3.1.4 Desafíos

El desarrollo de esta aplicación brinda una serie de desafíos en cuanto que existen diferencias fundamentales con el desarrollo de aplicaciones tradicionales.

El código desplegado en la blockchain no puede ser modificado. Es necesario pensar detenidamente lo que esto implica. En una aplicación tradicional, si se detecta un *bug* o error, se corrige y se despliega la versión corregida. Los contratos inteligentes o smart contracts desplegados, por el contrario, viven por siempre. Entre las medidas que es necesario aplicar se pueden mencionar:

- Existencia desde un comienzo de un mecanismo de versionado, que permita incorporar funcionalidades mediante nuevas versiones de un contrato inteligente.
- Máxima simplicidad de los contratos. Los contratos deben ser lo más sencillos posibles, y delegar funcionalidades no esenciales en programas externos.

No se puede modelar la solución basándose en los modelos tradicionales existentes. Existe la tentación de basarse en modelos existentes, en este caso el sistema de gestión académico Guaraní. Pero las diferencias de enfoque son tan grandes que eso no es posible. Hay que analizar el problema que se desea resolver y modelarlo con una nueva visión.

Los contratos deben ser simples. Se ha mencionado anteriormente, pero esta necesidad va más allá de la imposibilidad de modificación. Los contratos deben ser fáciles de comprender, y su semántica debe ser clara simplemente leyendo el código.

El sistemas de gestión académica registra insuficiente información histórica. El sistema de gestión académica carece de la capacidad de obtener de manera sencilla el estado en un cierto momento del pasado. Si bien todos los cambios se registran, esto se hace con fines de auditoría. Durante mucho tiempo se consideraron ciertos atributos de una persona como inamovibles (por ejemplo el nombre o género), cuando la realidad nos ha probado que no lo son. Esto dificulta el desarrollo de sistemas como este, en los cuales se necesita poder reconstruir el estado en un cierto momento (como por ejemplo un examen).

Usabilidad para la firma de actas en la blockchain. La firma de actas requiere que el funcionario responsable de garantizar la validez del acta firme la misma en la blockchain, para eso es necesario contar con software externo llamado MetaMask que permite al funcionario conectarse con su cuenta de blockchain y con su clave a la BFA. Esta parte del proceso requiere de un fuerte trabajo para su usabilidad.

3.1.5 Análisis FODA

El análisis FODA (Fortalezas, Oportunidades, Debilidades y Amenazas) ayuda a evaluar lo mejor y lo peor de una situación para luego confeccionar una estrategia. Permite tomar las mejores decisiones basadas en un análisis de la situación considerando tanto los factores internos (Fortalezas y Debilidades) como los factores externos (Oportunidades y Amenazas).

Esta técnica examina el proyecto desde cada uno de los aspectos FODA para aumentar el espectro de riesgos identificados, incluidos los riesgos generados internamente. La técnica comienza con la identificación de las fortalezas y debilidades de la organización, centrándose ya sea en el proyecto, en la organización o en el negocio en general. El análisis

FODA identifica luego cualquier oportunidad para el proyecto con origen en las fortalezas de la organización y cualquier amenaza con origen en las debilidades de la organización. El análisis también examina el grado en el que las fortalezas de la organización contrarrestan las amenazas, e identifica las oportunidades que pueden servir para superar las debilidades.

La forma visual de un análisis FODA es una matriz de cuatro cuadrantes en el que en cada cuadrante se listan las principales Fortalezas, Oportunidades, Debilidades y Amenazas.

- **Fortalezas:** Reúnen el conjunto de recursos internos y cualquier tipo de ventaja competitiva propia de la organización.
- **Oportunidades:** Factores ajenos a la organización que favorecen su desarrollo o brindan la posibilidad de implantar mejoras.
- **Debilidades:** Constituyen los aspectos limitadores de la capacidad de desarrollo de la organización, debido a sus características internas.
- **Amenazas:** Todos aquellos factores externos que pueden llegar a impedir la ejecución o poner en peligro la viabilidad.

A continuación se expone el análisis FODA del proyecto.

FIGURA 3.8 – Análisis FODA. *Elaboración propia.*

3.1.6 Interesados

Al llevarse adelante el desarrollo del proyecto se ve afectado por los diferentes *interesados o stakeholders*. Un interesado es un individuo, grupo u organización que puede afectar, verse afectado, o percibirse a sí mismo como afectado por una decisión, actividad o resultado de un proyecto. Los interesados pueden participar activamente en el proyecto o tener

intereses a los que puede afectar positiva o negativamente la ejecución o la terminación del proyecto.

Los diferentes interesados pueden tener expectativas contrapuestas susceptibles de generar conflictos dentro del proyecto.

Los interesados también pueden ejercer influencia sobre el proyecto, los entregables y el equipo del proyecto a fin de lograr un conjunto de resultados que satisfagan los objetivos estratégicos del negocio u otras necesidades.

Los interesados tienen diferentes niveles de responsabilidad y autoridad cuando participan en un proyecto. Estos niveles pueden cambiar durante el ciclo de vida del proyecto. Su participación puede variar desde una participación ocasional hasta el patrocinio total del proyecto, lo cual incluye proporcionar apoyo financiero, político o de otro tipo. Algunos interesados también pueden impedir el éxito del proyecto, ya sea de forma pasiva o activa. La identificación de los interesados es un proceso continuo a lo largo de todo el ciclo de vida del proyecto. Es crítico para el éxito de un proyecto la identificación de los interesados, la comprensión de su grado relativo de influencia en el proyecto y el equilibrio de sus demandas, necesidades y expectativas. Si esto no se consiguiera, puede conducir a retrasos, aumento de los costos, incidentes inesperados y otras consecuencias negativas, incluyendo la cancelación del proyecto.

Para llevar adelante el proyecto es necesario que el conjunto de personas, dependencias e instituciones colaboren entre si. A continuación se muestra una gráfica con los grupos de interesados detectados en este proyecto.

En el gráfico se han agrupado los interesados en diferentes grupos: UNC, BFA y CIN. En el grupo UNC se encuentran todas aquellas áreas involucradas en el proyecto de forma directa o indirecta, es decir, involucradas en la realización del proyecto o bien porque el nuevo proceso planteado en la propuesta afecta en su trabajo diario.

En el grupo de interesados de la Blockchain Federal Argentina (BFA) se encuentran todos los miembros que forman parte de la BFA, lo cual incluye a individuos, organismos, instituciones o empresas de cualquier sector que interactúan o contribuyen con la plataforma.

En el grupo de interesados del Consejo Interuniversitario Nacional (CIN) se encuentra el Sistema de Información Universitaria (SIU), área en donde se encuentra el equipo de desarrollo del sistema académico Guaraní y el Sistema Informático de Diplomas y Certificaciones (SIDCer). Ambos sistemas con los que se interactúa en el proceso de solicitud de diploma.

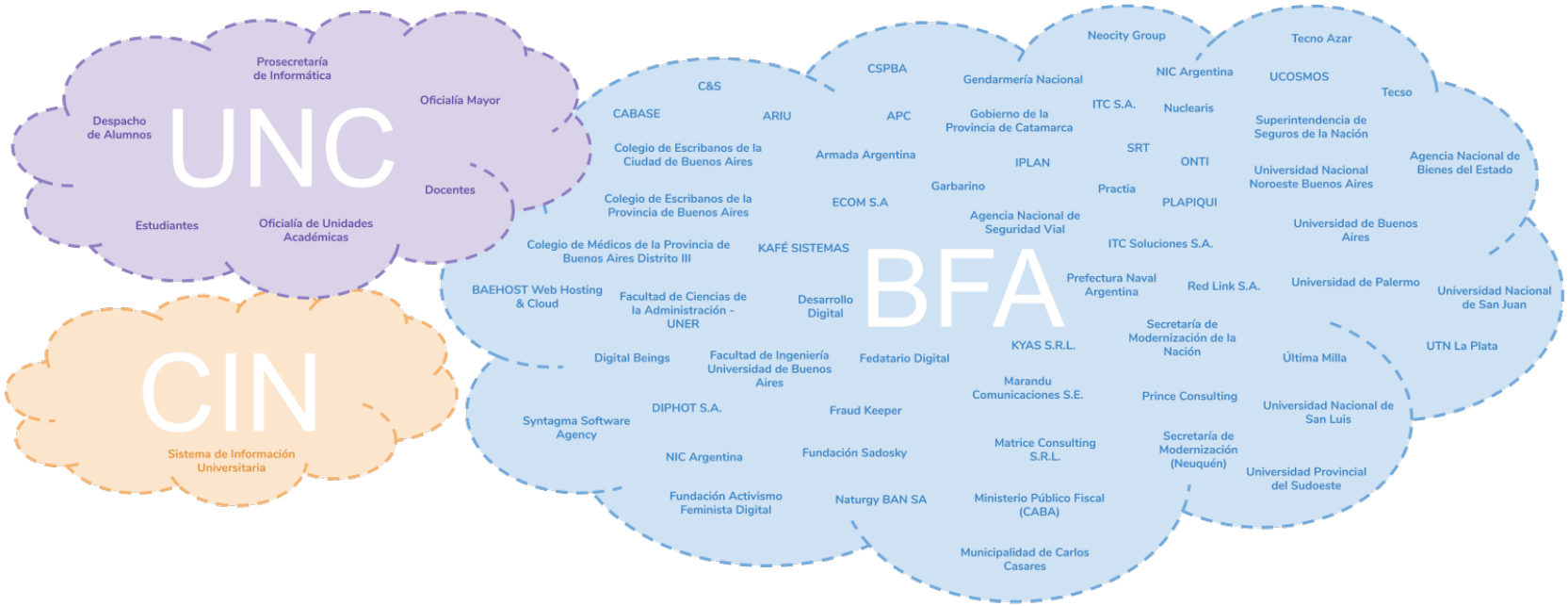


FIGURA 3.9 – Stakeholders del proyecto. *Elaboración propia.*

3.2 Gestión de proyecto

Como se explicó anteriormente para poder llevar adelante el proyecto es necesario gestionarlo.

Se comienza con la recopilación de los requerimientos permitiendo determinar y gestionar las necesidades y los requisitos de los interesados para cumplir con los objetivos del proyecto. El beneficio clave de este proceso es que proporciona la base para definir y gestionar el alcance del proyecto.

Se continua con la definición del alcance, lo cual consiste en desarrollar una descripción detallada del proyecto. Se genera una base común de entendimiento entre los interesados (stakeholders) del alcance del proyecto.

El alcance se dividirá en actividades. Las actividades tienen duraciones, a lo largo de las cuales se lleva a cabo el trabajo, y pueden tener asimismo recursos y costos asociados a dicho trabajo.

3.2.1 Requerimientos

El éxito del proyecto depende directamente de la participación activa de los interesados en el descubrimiento y la descomposición de las necesidades en requisitos, y del cuidado que se tenga al determinar y gestionar los requisitos del proyecto. Los requisitos incluyen condiciones o capacidades que el proyecto debe cumplir o que deben estar presentes en el producto, servicio o resultado para satisfacer un acuerdo u otra especificación formalmente impuesta. También incluyen las necesidades y expectativas.

A continuación se listan los requisitos del proyecto:

- Registrar en la red de blockchain BFA los diferentes tipos de actas.
- Verificar y mediante la firma en la cadena de blockchain brindar conformidad del acta.
- Validar certificados directamente contra blockchain BFA.
- Un acta cerrada no puede ser revocada.
- El libro y número de acta de un acta, en caso de tener, debe ser único por facultad.
- La fecha del acta debe ser un campo editable.
- Cada acta puede ser rectificada más de una vez.
- En un acta rectificativa no permitir agregar estudiantes.
- En un acta rectificativa solo permitir modificar datos que se encuentran en el acta original.
- Registrar histórico de actas.
- Contar con la infraestructura necesaria que permita el acceso al sistema.

3.2.2 Alcance

Como se comento anteriormente los proyectos se pueden dividir en fases. Una fase del proyecto es un conjunto de actividades del proyecto, relacionadas de manera lógica. Un proyecto se puede dividir en cualquier número de fases.

No existe una única estructura ideal que se pueda aplicar a todos los proyectos. Algunos proyectos tendrán una sola fase. Otros, en cambio, pueden constar de dos o más fases.

Para facilitar la gestión de este proyecto se dividirá en tres fases

- Registro de actas: Responsable de registrar en la red de blockchain las actas.
- Conformidad de actas: Permite verificar y firmar la información del acta que se encuentra en blockchain.
- Validación de certificados: Valida los certificados contra las actas que se encuentran en blockchain.

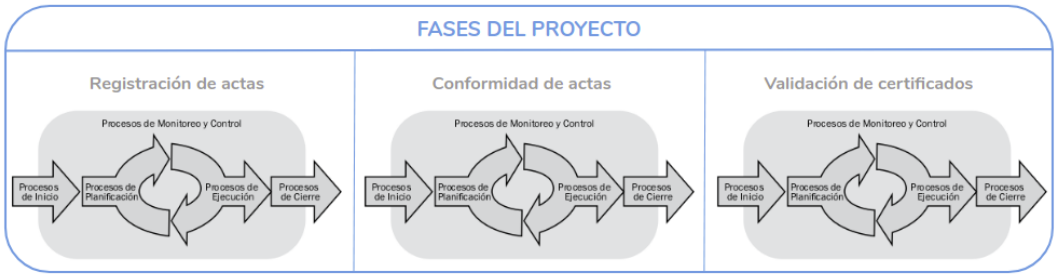


FIGURA 3.10 – Fases del proyecto. *Elaboración propia.*

Los procesos que se utilizan para gestionar el alcance del proyecto, así como las herramientas y técnicas de apoyo, pueden variar según el proyecto. En este caso se hará uso de la *Estructura de Desglose del Trabajo o Work Breakdown Structure (EDT/WBS)*

La Estructura de Desglose del Trabajo o Work Breakdown Structure (EDT/WBS) es un agrupamiento de los elementos del proyecto, orientado a entregables, que organiza y define el alcance total del proyecto.

Crear la WBS consiste en subdividir los entregables del proyecto y el trabajo del proyecto en componentes más pequeños y más fáciles de manejar. El beneficio clave de este proceso es que proporciona una visión estructurada de lo que se debe entregar.[18]

La WBS es una descomposición jerárquica del alcance total del trabajo a realizar por el equipo del proyecto para cumplir con los objetivos del proyecto y crear los entregables requeridos. La WBS organiza y define el alcance total del proyecto.

El trabajo planificado está contenido en el nivel más bajo de los componentes de la WBS,

denominados *paquetes de trabajo o work packages*. Un paquete de trabajo se puede utilizar para agrupar las actividades donde el trabajo es programado y estimado, seguido y controlado. En el contexto de la WBS, la palabra trabajo se refiere a los productos o entregables del trabajo que son el resultado de la actividad realizada, y no a la actividad en sí misma.

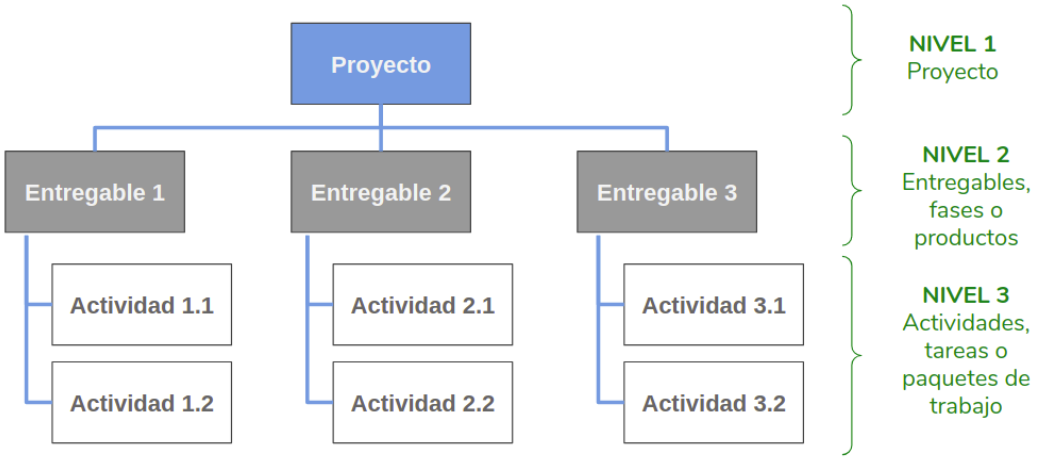


FIGURA 3.11 – Ejemplo de estructura de desglose del trabajo. *Elaboración propia.*

Resumen de las características de la estructura de desglose del trabajo o work breakdown structure (EDT/WBS):

- El trabajo que no está en la WBS está fuera del alcance del proyecto. Llamada *regla del 100 por ciento*.
- Cada nivel descendente representa un detalle mayor en la descripción de los elementos del proyecto.
- Incluye las descripciones de todos los paquetes de trabajo (work packages).
- Incluye tiempos, presupuestos, y asignaciones de responsabilidades.

La estructura de WBS se puede crear a través de varios enfoques. Entre los métodos más habituales se cuentan el enfoque descendente, el uso de guías específicos y el uso

de plantillas. La estructura de la WBS se puede representar de diferentes maneras, tales como:

- utilizando las fases del ciclo de vida del proyecto como segundo nivel de descomposición, con los entregables del producto y del proyecto insertados en el tercer nivel.
- utilizando los entregables principales como segundo nivel de descomposición.
- incorporando componentes de nivel inferior que pueden desarrollar organizaciones externas al equipo del proyecto.

La WBS se puede estructurar como un esquema, como un organigrama, o mediante otro método que represente un desglose jerárquico.

A continuación se definen por cada fase los entregables y paquetes de actividades.

Registración de actas	
Código	Actividades
1	Reunión de definiciones
1.1	Coordinar reuniones
1.2	Definir temas de reuniones
1.3	Definir cronograma de reuniones
1.4	Definir nuevos procesos
1.5	Detectar las habilidades necesarias para llevar adelante el proyecto
1.6	Realizar minuta de reuniones
2	Especificación técnica finalizada
2.1	Generar definiciones técnicas
2.2	Definir base de datos
2.3	Modelar base de datos
2.4	Realizar pruebas técnicas
2.5	Documentar decisiones tomadas
3	Desarrollo de sistema de registración de actas finalizado
3.1	Definir repositorio de código
3.2	Definir estructura de APIs
3.3	Definir estructura de smart contract
3.4	Desarrollar APIs
3.5	Desplegar nodos de blockchain para desarrollo
3.6	Integrar con sistema Guaraní
3.7	Realizar pruebas de funcionalidad
3.8	Desplegar sistema desarrollado en producción
4	Infraestructura preparada
4.1	Configurar servidor donde se despliega el código
4.2	Definir y crear URLs de las APIs
4.3	Desplegar nodo en BFA
4.4	Desplegar smart contract en BFA
5	Comunicación institucional realizada
5.1	Comunicar a las autoridades nuevos procesos
5.2	Comunicar a las facultades nuevos procesos

TABLA 3.1 – WBS - Registro de actas. *Elaboración propia.*

Conformidad de actas	
Código	Actividades
1	Reunión de definiciones
1.1	Coordinar reuniones
1.2	Definir temas de reuniones
1.3	Definir cronograma de reuniones
1.4	Definir nuevos procesos
1.5	Realizar minuta de reuniones
2	Especificación técnica finalizada
2.1	Generar definiciones técnicas
2.2	Realizar pruebas tecnicas (MetaMask)
2.3	Documentar decisiones tomadas
2.4	Mostrar avances
3	Desarrollo de sistema de conformidad de actas finalizado
3.1	Definir repositorio de código
3.2	Definir estructura de APIs
3.3	Definir estructura de smart contract
3.4	Desarrollar APIs
3.5	Desplegar nodo firmador de blockchain para desarrollo
3.6	Integrar con sistema externo para firmar en BFA
3.7	Definir interfaz gráfica de firma de actas
3.8	Realizar pruebas de funcionalidad
3.9	Desplegar sistema desarrollado en producción
4	Infraestructura preparada
4.1	Configurar servidor donde se despliega el código
4.2	Desplegar nodo firmado en BFA
4.3	Desplegar smart contract en BFA
5	Comunicación institucional realizada
5.1	Comunicar a las autoridades nuevos procesos
5.2	Comunicar a las facultades nuevos procesos
5.3	Brindar documentación de nuevo proceso

TABLA 3.2 – WBS - Conformidad de actas. *Elaboración propia.*

Validación de certificados	
Código	Actividades
1	Reunión de definiciones
1.1	Coordinar reuniones
1.2	Definir temas de reuniones
1.3	Definir cronograma de reuniones
1.4	Definir nuevos procesos
1.5	Realizar minuta de reuniones
2	Especificación técnica finalizada
2.1	Generar definiciones técnicas
2.2	Realizar pruebas técnicas
2.3	Documentar decisiones tomadas
3	Desarrollo de sistema de validación de certificados finalizado
3.1	Definir repositorio de código
3.2	Definir interfaz gráfica del sistema validador
3.3	Conectar con BFA para validar
3.4	Realizar pruebas de funcionalidad
3.5	Realizar pruebas de usabilidad
3.6	Desplegar sistema desarrollado en producción
4	Infraestructura preparada
4.1	Configurar servidor donde se despliega el código
4.2	Definir y crear URLs para la validación
5	Comunicación institucional realizada
5.1	Comunicar la posibilidad de validar certificados
5.2	Brindar documentación

TABLA 3.3 – WBS - Validación de certificados. *Elaboración propia.*

3.2.3 Tiempo

Estimar la duración de las actividades es el proceso de realizar una estimación de la cantidad de períodos de trabajo necesarios para finalizar las actividades individuales con los recursos estimados. El beneficio clave de este proceso es que establece la cantidad de tiempo necesario para finalizar cada una de las actividades, lo cual constituye una entrada fundamental para el proceso que permite desarrollar el cronograma.

La estimación de la duración de las actividades utiliza información sobre el alcance del

trabajo que conlleva la actividad, los tipos de recursos necesarios y las cantidades estimadas de los mismos. Las entradas para las estimaciones de la duración de las actividades provienen de la persona o grupo del equipo del proyecto que esté más familiarizado con la naturaleza del trabajo a desarrollar en cada actividad específica.

Estimar la duración de las actividades se torna un poco complejo debido a factores internos o externos que cambian constantemente. Influye significativamente la complejidad, el tamaño del proyecto, el grado de incertidumbre y la disponibilidad de información.

Para poder realizar predicciones sobre características del proyecto actual es necesario disponer de información obtenida en proyectos pasados sobre las variables a estimar y factores que les afectan o datos recolectados de cada uno de los expertos en cada tema, debido a la gran cantidad de factores que influyen.

Existen diferentes técnicas para estimar la duración de las actividades:

- Juicio de expertos: Toma información histórica, se proporciona información sobre la estimación de la duración o duraciones máximas recomendadas, procedente de proyectos similares anteriores.
- Estimación análoga: Es una técnica para estimar la duración o el costo de una actividad o de un proyecto mediante la utilización de datos históricos de una actividad o proyecto similar. Se utilizan parámetros de un proyecto anterior similar, tales como duración, presupuesto, tamaño, carga y complejidad, como base para estimar los mismos parámetros o medidas para un proyecto futuro.
- Técnicas grupales de toma de decisiones: Los enfoques grupales son útiles para involucrar a los miembros del equipo en la mejora de la exactitud de la estimación y del compromiso con las resultados de las estimaciones que se produzcan. Mediante la participación en el proceso de estimación de un grupo estructurado de personas cercano a la ejecución técnica del trabajo, se obtiene información adicional y se obtienen estimaciones más precisas.

Estimar el tiempo de las actividades es una parte principal del proyecto y su gestión, ya que visibiliza los recursos necesarios para llevar con precisión el tiempo, costo y alcance. Al ser impreciso o mal estimado el tiempo alguno de los vértices, vistos en el triangulo de la triple restricción, afectará directamente a los dos restantes impactando en la calidad del proyecto.

Una estimación errada puede dar dos resultados: *subestimar*; generando proyectos que exceden sus presupuestos e incumplen las fechas programadas, comprometiendo la calidad, o *sobrestimar*, generando proyectos excesivos en costos y recursos.

El tiempo de cada una de las actividades se ha estimado para cada una de las fases

Código	Actividades	Fecha inicio	Fecha fin	Duración (dias)	Días desde el comienzo
1	Reunión de definiciones				
1.1	Coordinar reuniones	01/01/2020	11/01/2020	10	0
1.2	Definir temas de reuniones	03/01/2020	15/01/2020	12	2
1.3	Definir cronograma de reuniones	01/01/2020	15/01/2020	14	0
1.4	Definir nuevos procesos	10/01/2020	15/02/2020	36	9
1.5	Detectar las habilidades necesarias para llevar adelante el proyecto	10/01/2020	01/02/2020	22	9
1.6	Realizar minuta de reuniones	03/01/2020	15/02/2020	43	2
2	Especificación técnica finalizada				
2.1	Generar definiciones técnicas	02/02/2020	30/03/2020	57	32
2.2	Definir base de datos	15/03/2020	18/03/2020	3	74
2.3	Modelar base de datos	18/03/2020	05/04/2020	18	77
2.4	Realizar pruebas técnicas	03/04/2020	01/06/2020	59	93
2.5	Documentar decisiones tomadas	20/03/2020	02/06/2020	74	79
3	Desarrollo de sistema de registración de actas finalizado				
3.1	Definir repositorio de código	01/06/2020	03/06/2020	2	152
3.2	Definir estructura de APIs	02/06/2020	15/07/2020	43	153
3.3	Definir estructura de smart contract	05/06/2020	15/07/2020	40	156
3.4	Desarrollar APIs	16/06/2020	15/08/2020	60	167
3.5	Desplegar nodos de blockchain para desarrollo	10/06/2020	15/06/2020	5	161
3.6	Integrar con sistema Guaraní	20/06/2020	15/07/2020	25	171
3.7	Realizar pruebas de funcionalidad	10/07/2020	30/08/2020	51	191
3.8	Desplegar sistema desarrollado en producción	30/07/2020	05/08/2020	6	211
4	Infraestructura preparada				
4.1	Configurar servidor donde se despliega el código	30/07/2020	05/08/2020	6	211
4.2	Definir y crear URLs de las APIs	30/07/2020	03/08/2020	4	211
4.3	Desplegar nodo en BFA	28/07/2020	01/08/2020	4	209
4.4	Desplegar smart contract en BFA	01/08/2020	03/08/2020	2	213
5	Comunicación institucional realizada				
5.1	Comunicar a las autoridades nuevos procesos	01/09/2020	05/09/2020	4	244
5.2	Comunicar a las facultades nuevos procesos	01/09/2020	10/09/2020	9	244

TABLA 3.4 – Estimación de tiempo de actividades - Registro de actas. *Elaboración propia.*

Código	Actividades	Fecha inicio	Fecha fin	Duración (días)	Días desde el comienzo
1	Reunión de definiciones				
1.1	Coordinar reuniones	01/09/2020	11/09/2020	10	0
1.2	Definir temas de reuniones	03/09/2020	15/09/2020	12	2
1.3	Definir cronograma de reuniones	01/09/2020	15/09/2020	14	0
1.4	Definir nuevos procesos	10/09/2020	15/10/2020	35	9
1.5	Realizar minuta de reuniones	03/09/2020	15/10/2020	42	2
2	Especificación técnica finalizada				
2.1	Generar definiciones técnicas	15/10/2020	30/11/2020	46	44
2.2	Realizar pruebas tecnicas (MetaMask)	28/10/2020	15/11/2020	18	57
2.3	Documentar decisiones tomadas	01/11/2020	16/11/2020	15	61
2.4	Mostrar avances	15/11/2020	20/11/2020	5	75
3	Desarrollo de sistema de conformidad de actas finalizado				
3.1	Definir repositorio de código	15/11/2020	16/11/2020	1	75
3.2	Definir estructura de APIs	16/11/2020	25/11/2020	9	76
3.3	Definir estructura de smart contract	20/11/2020	30/11/2020	10	80
3.4	Desarrollar APIs	25/11/2020	01/01/2021	37	85
3.5	Desplegar nodo firmador de blockchain para desarrollo	15/12/2020	20/12/2020	5	105
3.6	Integrar con sistema externo para firmar en BFA	15/12/2020	01/01/2021	17	105
3.7	Definir interfaz gráfica de firma de actas	20/12/2020	30/12/2020	10	110
3.8	Realizar pruebas de funcionalidad	01/01/2021	25/01/2021	24	122
3.9	Desplegar sistema desarrollado en producción	25/01/2021	30/01/2021	5	146
4	Infraestructura preparada				
4.1	Configurar servidor donde se despliega el código	20/01/2021	25/01/2021	5	141
4.2	Desplegar nodo firmado en BFA	30/01/2021	05/02/2021	6	151
4.3	Desplegar smart contract en BFA	01/02/2021	05/02/2021	4	153
5	Comunicación institucional realizada				
5.1	Comunicar a las autoridades nuevos procesos	01/02/2021	05/02/2021	4	153
5.2	Comunicar a las facultades nuevos procesos	03/02/2021	10/02/2021	7	155
5.3	Brindar documentación de nuevo proceso	01/02/2021	10/02/2021	9	153

TABLA 3.5 – Estimación de tiempo de actividades - Conformidad de actas. *Elaboración propia.*

Código	Actividades	Fecha inicio	Fecha fin	Duración (días)	Días desde el comienzo
1	Reunión de definiciones				
1.1	Coordinar reuniones	01/01/2021	11/01/2021	10	0
1.2	Definir temas de reuniones	03/01/2021	15/01/2021	12	2
1.3	Definir cronograma de reuniones	01/01/2021	15/01/2021	14	0
1.4	Definir nuevos procesos	10/01/2021	15/02/2021	36	9
1.5	Realizar minuta de reuniones	03/01/2021	15/02/2021	43	2
2	Especificación técnica finalizada				
2.1	Generar definiciones técnicas	15/02/2021	30/03/2021	43	45
2.2	Realizar pruebas técnicas	28/02/2021	20/04/2021	51	58
2.3	Documentar decisiones tomadas	01/03/2021	25/04/2021	55	59
3	Desarrollo de sistema de validación de certificados finalizado				
3.1	Definir repositorio de código	15/03/2021	16/03/2021	1	73
3.2	Definir interfaz gráfica del sistema validador	15/03/2021	15/04/2021	31	73
3.3	Conectar con BFA para validar	16/03/2021	25/03/2021	9	74
3.4	Realizar pruebas de funcionalidad	18/03/2021	30/04/2021	43	76
3.5	Realizar pruebas de usabilidad	20/04/2021	30/04/2021	10	109
3.6	Desplegar sistema desarrollado en producción	01/05/2021	05/05/2021	4	120
4	Infraestructura preparada				
4.1	Configurar servidor donde se despliega el código	01/05/2021	03/05/2021	2	120
4.2	Definir y crear URLs para la validación	01/05/2021	03/05/2021	2	120
5	Comunicación institucional realizada				
5.1	Comunicar la posibilidad de validar certificados	05/05/2021	20/05/2021	15	124
5.2	Brindar documentación	05/05/2021	15/05/2021	10	124

TABLA 3.6 – Estimación de tiempo de actividades - Validación de certificados. *Elaboración propia.*

Los recursos requeridos para las actividades que se han estimado tendrán un efecto sobre la duración de las actividades, puesto que el grado con el que los recursos asignados a cada actividad cumplen con los requisitos tendrá una influencia significativa sobre la duración de la mayoría de las actividades. Por ejemplo, si se asignan recursos adicionales o con menos habilidades a una actividad, puede producirse una disminución del desempeño o de la productividad debido a que se incrementarán las necesidades de comunicación, de formación y de coordinación, lo que redundará en una duración estimada mayor.

La duración del tiempo de las actividades se realiza en base a los siguientes recursos para cada fase

Recursos para la fase de registro de actas:

- Prosecretaría de Informática UNC: 2 programadores, 1 programador Guaraní, 1 líder técnico, 1 gestor de proyecto, 1 DevOps
- Equipo SIU Guaraní: 1 programador
- Equipo BFA: 2 especialistas

Recursos para la fase de conformidad de actas:

- Prosecretaría de Informática UNC: 2 programadores, 1 líder técnico, 1 gestor de proyecto, 1 DevOps

Recursos para la fase de validación de certificados:

- Prosecretaría de Informática UNC: 2 programadores, 1 programador Guaraní, 1 líder técnico, 1 gestor de proyecto, 1 DevOps
- Equipo SIU Guaraní: 1 programador

Cronograma

Desarrollar el cronograma del proyecto es el proceso de analizar las secuencias de actividades, las duraciones y los recursos disponibles para cada actividad.

El cronograma se puede representar en forma de tabla, aunque es más frecuente representarlo en forma gráfica. En este caso lo representaremos por cada fase en un diagrama de barras o *diagrama de Gantt*, en donde se presenta la información del cronograma con la lista de actividades en el eje vertical, las fechas en el eje horizontal y las duraciones de las actividades se representan en forma de barras colocadas en función de las fechas de inicio y de finalización.

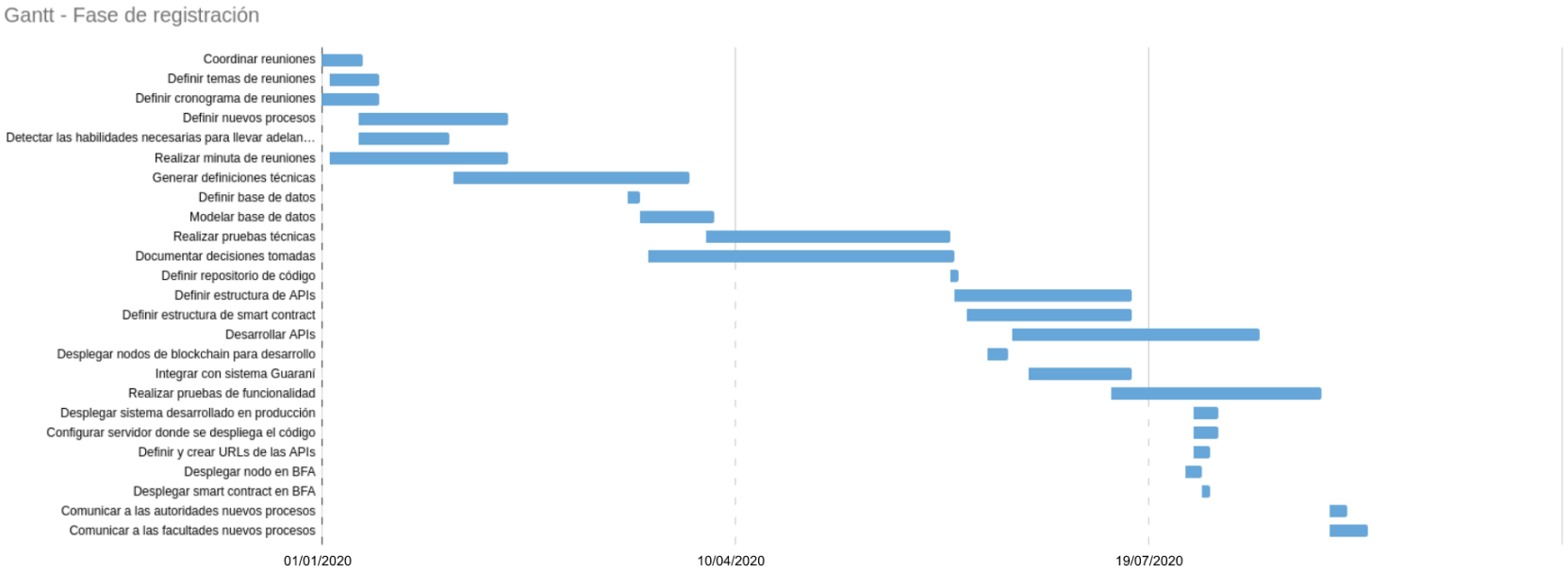


FIGURA 3.12 – Diagrama de Gantt - Registro de actas. *Elaboración propia.*

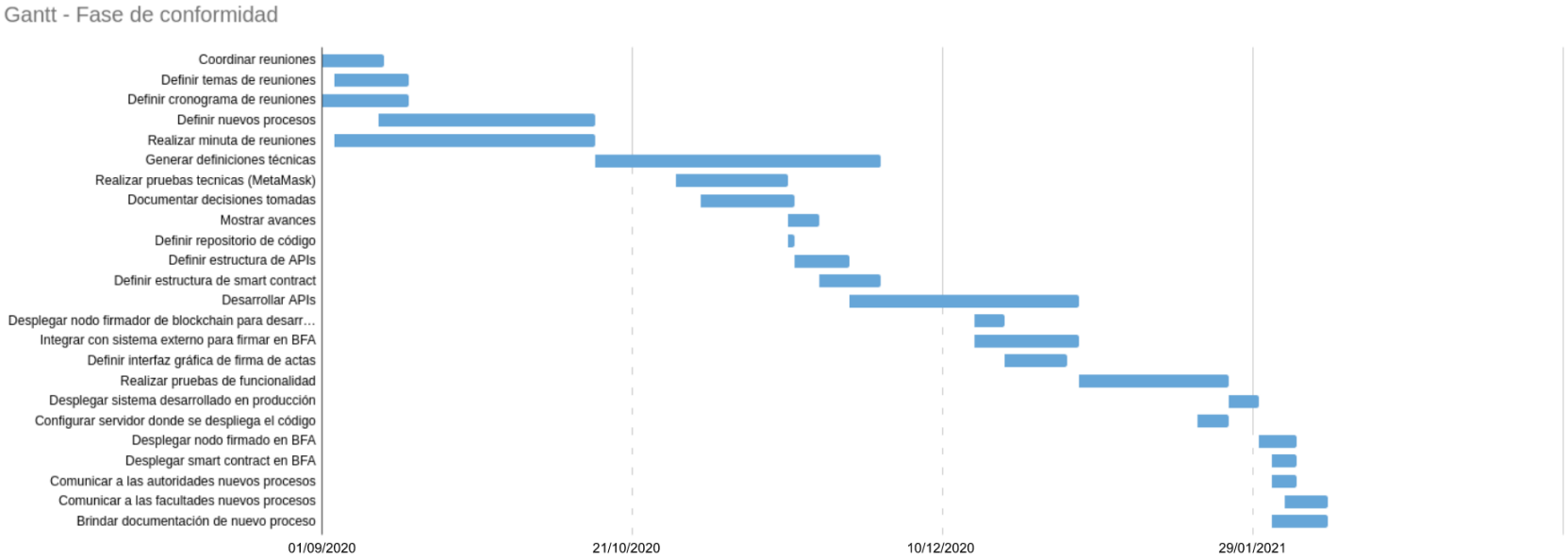


FIGURA 3.13 – Diagrama de Gantt - Conformidad de actas. *Elaboración propia.*

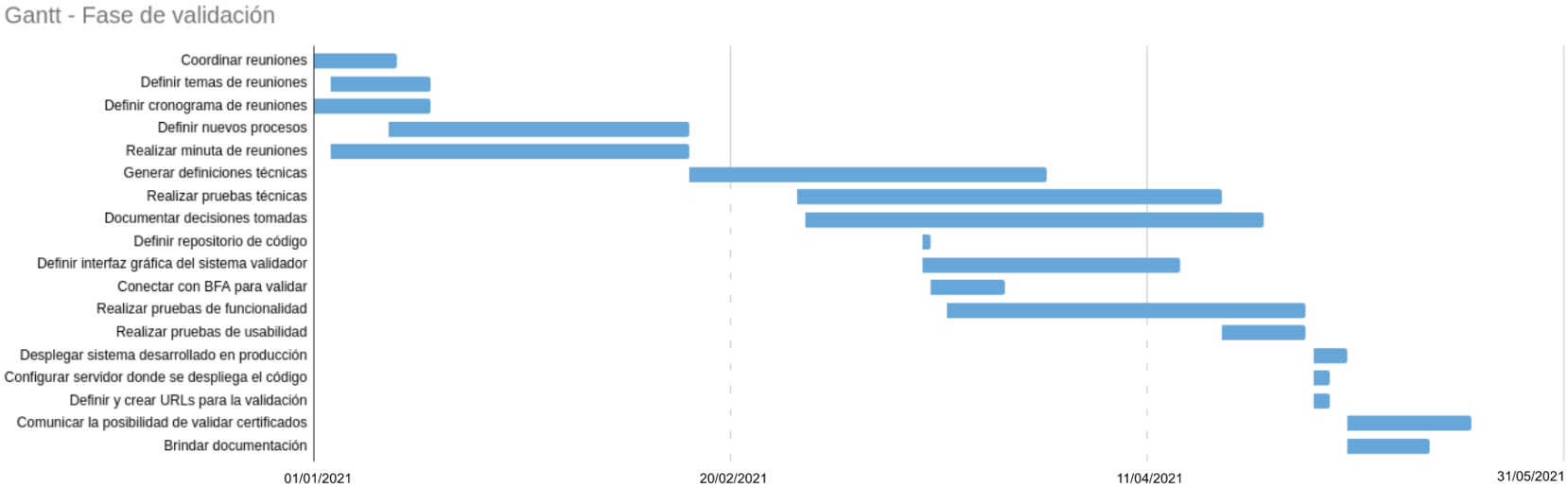


FIGURA 3.14 – Diagrama de Gantt - Validación de certificados. *Elaboración propia.*

3.2.4 Costo

En este punto es importantes descatacar que la decisión de llevar adelante un proyecto en la universidad no suele estar atado al costo del mismo, sino a los beneficios que ofrece el proyecto. A pesar de no ser el factor fundamental a la hora de decidir realizar un proyecto en la universidad, es importante tener un estimativo del costo el proyecto, por ejemplo si se desea considerar una posible tercerización en su implementación.

En esta instancia se estimarán los costos del proyecto para luego determinar un presupuesto.

Estimar los costos consiste en desarrollar una aproximación de los recursos financieros necesarios para completar las actividades del proyecto.

Se estiman los costos para todos los recursos que se van a asignar al proyecto. Estos incluyen, entre otros, el personal, los materiales, el equipamiento, los servicios y las instalaciones. La estimación de costos consiste en una evaluación cuantitativa de los costos probables de los recursos necesarios para completar la actividad. Las estimaciones de costos se pueden presentar a nivel de actividad o en formato resumido.

Las estimaciones de costos se expresan normalmente en unidades de alguna moneda (ej. dólares, euros, yenes, etc.), aunque en algunos casos pueden emplearse otras unidades de medida, como las horas o los días de trabajo del personal para facilitar las comparaciones, al eliminar el efecto de las fluctuaciones de las divisas.

La estimación de costos se revisa y refina a lo largo del proyecto para ir reflejando los detalles adicionales a medida que éstos se van conociendo y que se van probando los supuestos de partida. La exactitud de la estimación del costo de un proyecto aumenta conforme el proyecto avanza a través de su ciclo de vida.

Anteriormente definimos el personal necesario por cada fase para realizar el proyecto. Para estimar los costos de los sueldos de cada profesional se hará uso de la información brindada por la plataforma Openqube[1] en base a una encuesta realizada en el periodo julio 2020 a agosto 2020.

Profesional	Sueldo promedio mensual (en peso argentinos)
Lider tecnico (senior)	$156.682,00
Gestor de proyecto (senior)	$140.000,00
Programador (senior)	$120.000,00
Programador (junior)	$62.000,00
DevOps (semi-senior)	$85.000,00

TABLA 3.7 – Sueldo promedio mensual. *Elaboración propia.*
Datos: Openqube, encuesta julio 2020 a agosto 2020.

Para cada fase del proyecto se necesita un conjunto diferentes de profesionales, por lo que se estimará el costo por fase.

En cada una de las filas que poseen un asterisco, se ha realizado el cálculo del sueldo dividido cuatro dado que son roles sin dedicación completa únicamente a este proyecto.

Registración de actas			
Cantidad	Profesional	Sueldo promedio mensual (en peso argentinos)	
1	Lider tecnico (senior)	$39.170,50	*
1	Gestor de proyecto (senior)	$35.000,00	*
2	Programador (senior)	$240.000,00	
3	Programador (junior)	$46.500,00	*
1	DevOps (semi-senior)	$21.250,00	*
TOTAL		**$381.920,50**	

TABLA 3.8 – Costos fase de registro de actas. *Elaboración propia.*

[1] https://sueldos.openqube.io/

Conformidad de actas			
Cantidad	Profesional	Sueldo promedio mensual (en peso argentinos)	
1	Lider tecnico (senior)	$39.170,50	*
1	Gestor de proyecto (senior)	$35.000,00	*
2	Programador (senior)	$240.000,00	
0	Programador (junior)	$0,00	*
1	DevOps (semi-senior)	$21.250,00	*
TOTAL		**$335.420,50**	

TABLA 3.9 – Costos fase de conformidad de actas. *Elaboración propia.*

Validación de certificados			
Cantidad	Profesional	Sueldo promedio mensual (en peso argentinos)	
1	Lider tecnico (senior)	$39.170,50	*
1	Gestor de proyecto (senior)	$35.000,00	*
2	Programador (senior)	$240.000,00	
3	Programador (junior)	$46.500,00	*
1	DevOps (semi-senior)	$21.250,00	*
TOTAL		**$381.920,50**	

TABLA 3.10 – Costos fase de validación de certificados. *Elaboración propia.*

Para determinar el presupuesto se sumarán los costos estimados.

Fases	Cantidad de meses (aprox)	Sueldos prom profesional mensual	Costo total
Registración de actas	9	$366.420,50	$3.297.784,50
Conformidad de actas	5	$335.420,50	$1.677.102,50
Validación de certificados	5	$366.420,50	$1.832.102,50
TOTAL	**19**	**$1.068.261,50**	**$6.806.989,50**

TABLA 3.11 – Costos del proyecto. *Elaboración propia.*

En esta estimación de costos se multiplica cada fase por el tiempo en meses estimado basándose en la información brindada por el diagrama de Gantt.

El proyecto no requiere de materiales, equipamiento o servicios adicionales para llevarse

adelante, ya que se cuenta con todo ello y el acceso a la red de la BFA es gratuito.

3.2.5 Riesgos

El riesgo de un proyecto es un evento o condición incierta que, de producirse, tiene un efecto positivo o negativo en uno o más de los objetivos del proyecto, tales como el alcance, el cronograma, el costo y la calidad.

Un riesgo puede tener una o más causas y, de materializarse, uno o más impactos. Una causa puede ser un requisito especificado o potencial, un supuesto, una restricción o una condición que crea la posibilidad de consecuencias tanto negativas como positivas. Los riesgos del proyecto tienen su origen en la incertidumbre que está presente en todos los proyectos.

Dada la existencia de riesgos en el proyecto estos se deben registrar para tener en cuenta los costos de mitigación de los mismos. Los riesgos, que pueden representar amenazas u oportunidades, en general ejercen un impacto tanto en los costos de las actividades como en los del proyecto global. Por regla general, cuando el proyecto experimenta un evento de riesgo negativo, normalmente se incrementa el costo a corto plazo del proyecto y en ocasiones se produce un retraso en el cronograma del proyecto.

Los riesgos identificados para este proyectos son:

- Dificultades en la aceptación del cambio del proceso para cierre de actas.
- Inconvenientes del personal de la universidad en la aceptación del cambio de proceso para firmar actas.
- Problemas en la BFA que afecten al sistema.
- Demoras de gran cantidad de horas en el proceso de enviar un acta a la red de la

BFA.

- La cuenta de la BFA quedar sin ether al momento de enviar un acta a la red de la BFA.
- La cuenta de la BFA quedar sin ether al momento de firmar un acta en la red de la BFA.
- El sistema no funciona al momento de realizar un cierre de acta.
- El sistema no funciona al momento de realizar la firma del acta.
- Inconvenientes en la verificación de certificados.
- Falta de conexión a internet.
- No disponer de profesionales externos en el tiempo previsto para llevar adelante el proyecto.

La identificación de riesgos es un proceso iterativo debido a que pueden evolucionar o se pueden descubrir nuevos riesgos conforme el proyecto avanza a lo largo de su ciclo de vida.

Una vez identificados los riesgos que pueden afectar al proyecto se lleva a cabo el análisis de los mismos. Para ello se combina la probabilidad de ocurrencia e impacto de dichos riesgos.

Probabilidad de ocurrencia	
Muy baja	< 10%
Bajo	> 10 – 25%
Moderado (medio)	25 – 50%
Alto	50 – 75%
Muy alto	> 75%

TABLA 3.12 – Riesgos - Probabilidad de ocurrencia. *Elaboración propia.*

Impacto
Insignificante
Tolerable
Serio
Catastrófico

TABLA 3.13 – Riesgos - Impacto. *Elaboración propia.*

Identificador	Riesgo	Ocurrencia	Impacto
1	Dificultades en la aceptación del cambio del proceso para cierre de actas.	Moderado	Serio
2	Inconvenientes del personal de la universidad en la aceptación del cambio de proceso para firmar actas.	Alto	Serio
3	Problemas en la BFA que afenten al sistema.	Bajo	Catastrófico
4	Demoras de gran cantidad de horas en el proceso de enviar un acta a la red de la BFA.	Muy alto	Tolerable
5	La cuenta de la BFA quedar sin ether al momento de enviar un acta a la red de la BFA.	Bajo	Tolerable
6	La cuenta de la BFA quedar sin ether al momento de firmar un acta en la red de la BFA.	Bajo	Tolerable
7	El sistema no funciona al momento de realizar un cierre de acta.	Bajo	Serio
8	El sistema no funciona al momento de realizar la firma del acta.	Bajo	Tolerable
9	Inconvenientes en la verificación de certificados.	Moderado	Serio
10	Falta de conexión a internet.	Muy bajo	Serio
11	No disponer de profesionales externos en el tiempo previsto para llevar adelante el proyecto.	Bajo	Tolerable

TABLA 3.14 – Análisis de riesgos. *Elaboración propia.*

La evaluación de la importancia de cada riesgo y de su prioridad de atención se efectúa utilizando una tabla de búsqueda o una *matriz de probabilidad e impacto*. Dicha matriz especifica las combinaciones de probabilidad e impacto que llevan a calificar los riesgos con una prioridad baja, moderada o alta.

La matriz de probabilidad e impacto es una cuadrícula que permite vincular la probabilidad de ocurrencia de cada riesgo con su impacto sobre los objetivos del proyecto en caso de que ocurra dicho riesgo. Los riesgos se priorizan de acuerdo con sus implicaciones potenciales sobre los objetivos del proyecto.

Para este caso se ha generado una matriz en donde cada celda se encuentra coloreada representando la importancia con la cual ese riesgo debe ser atendido. El área de color rojo representa un riesgo crítico, el área de color naranja representa un riesgo de apreciable importancia, el área de color amarillo representa un riesgo moderado y el área de color verde representa un riesgo menor. Los números que se encuentran en las celdas de la ma-

triz representan el número de identificación de cada riesgo de la tabla anterior de análisis de riesgos.

Matriz de probabilidad e impacto				
	Insignificante	Tolerable	Serio	Catastrófico
Muy alto		4		
Alto			2	
Moderado			1 , 9	
Bajo		5, 6, 8, 11	7	3
Muy bajo			10	

FIGURA 3.15 – Riesgos - Matriz de probabilidad e impacto. *Elaboración propia.*

Ahora que se tiene identificada la importancia de cada uno de los riesgos detectados es posible planificar *respuesta a los riesgos* para desarrollar opciones y acciones para mejorar las oportunidades y reducir las amenazas de los objetivos del proyecto.

Para este caso se realizará respuesta a los riesgos críticos y de apreciable importancia detectados por medio de la matriz de probabilidad e impacto.

Riesgo	Situación	Acción
2. Inconvenientes del personal de la universidad en la aceptación del cambio de proceso para firmar actas.	El personal administrativo de la universidad se siente molesto o incomodo por el cambio de proceso, lo que generaría demoras en los procesos adminitrativos o se rechaza el nuevo proceso quedando obsoleto.	Generar capacitación y apoyo al cambio de proceso. Acompañar al personal adminitrativo en el cambio de proceso. Se gradual con el cambio. Brindar documentación de antemano. Comunicar con tiempo el nuevo proceso. Hacer participar al personal adminitrativo en la etapa de pruebas para mitigar la resistencia al cambio.
4. Demoras de gran cantidad de horas en el proceso de enviar un acta a la red de la BFA.	Una vez que las actas se han cerrado son guardadas en la red de la BFA. El proceso por el cual se guardan puede demorar varias horas si el número de actas cerradas es alto en el mismo día	Brindar información al personal docente y administrativo de las potenciales demoras en el cierre de actas. Brindar un grafico o información del estado de cada acta. Generar notificación al momento que un acta se ha guardado totalmente en la red de la BFA

TABLA 3.15 – Respuestas a los riesgos. *Elaboración propia.*

3.3 Motivación

Hoy en día la Universidad Nacional de Córdoba cuenta con más de 100.000 (cien mil) estudiantes. A lo largo de los años la cantidad de egresados ha incrementado y el control de los certificados también. A continuación se muestra una tabla con el número de egresados de carreras de grado por año.

Año	Egresados
2001	2322
2002	2552
2003	2561
2004	3303
2005	4357
2006	5057
2007	5036
2008	5613
2009	5752
2010	5557
2011	6795
2012	6720
2013	6595
2014	6665
2015	7101
2016	7329
2017	7139
2018	7315
2019	7353

TABLA 3.16 – Cantidad de egresados por año de carrera de grado en la Universidad Nacional de Córdoba. *Elaboración propia.* Datos: Sistema de registro de egresados

En los últimos años han egresado cerca de 7.000 (siete mil) estudiantes. Suponiendo que el total de los egresados decidieran solicitar su diploma implicaría que cada uno de los certificados de los estudiantes debe verificarse renglón por renglón contra las actas de examen que ha rendido a lo largo de la carrera.

Según lo consultado a personas que realizan la tarea de verificación de certificado, una persona con experiencia demora aproximadamente 15 minutos en verificar todos los renglones de un certificado.

Continuando con el supuesto, tomaremos un caso de ejemplo. La Facultad de Ciencias Económicas realiza por año cuatro colaciones de 200 estudiantes, lo que le llevaría por cada colación a una única persona con experiencia dedicando su jornada completa a la tarea de verificación de certificados más de una semana poder constatar las notas de todos los renglones.

Si los 7.000 estudiantes solicitan su diploma implicaría 250 jornadas de trabajo exclusiva de una persona con experiencia para poder verificar los certificados. A continuación se muestra una tabla con los supuestos planteados anteriormente.

Certificados	Minutos para verificar certificado	Horas para verificar certificado	Jornada laboral (7 horas)
1	15	0,25	0
200	3000	50	7
800	12000	200	29
7000	105000	1750	250

TABLA 3.17 – Tiempo de verificación de certificados. *Elaboración propia.*

No hay que olvidar que cada diploma que emite la universidad esta habilitando a un profesional, por lo cual es de suma importancia la verificación del certificado de cada estudiante.

La propuesta planteada permite brindar transparencia en el proceso de verificación de certificados y reducir los 15 minutos de verificación de un certificado a segundos. Con solo contar con el documento PDF del certificado y subirlo al sistema de verificación se validaría en segundos el certificado.

La innovación mejora el proceso de verificación y control de la universidad, pero va más

allá de eso. La implementación de este proyecto permitiría que cualquier agente externo a la universidad, por ejemplo el Ministerio de Educación Nacional, pueda verificar que el certificado es emitido por el sistema académico y que ese profesional realmente ha cumplimentado con todas sus materias para contar con su titulo habilitante a realizar trabajos profesionales.

3.4 Resumen

En este cápitulo se ha planteado la propuesta de un sistema que permite mejorar el proceso y el tiempo de que lleva la verificación de certificados. Se explica la importancia de este proceso.

La tecnología elegida para llevar adelante el proyecto es blockchain. Se ha explicado por qué se utilizará blockchain para su implementación y los desafios que ello implica.

Finalmente se ha realizado un analisis de los riegos, alcance, costos y tiempos del proyectos.

4

Conclusión

Hoy en día la tecnología es un elemento clave para hacer que nuestro trabajo sea más productivo, pero la tecnología por si sola no beneficia a la organización, es necesario que se incorpore a las actividades cotidianas. Para extraer de la tecnología todo su potencial debe contemplarse en el contexto de una estrategia tecnológica sostenible en el tiempo.

La capacidad de una organización para innovar es una condición sin la que no puede darse una utilización eficaz de los recursos y las nuevas tecnologías.

Incorporar innovación en las organizaciones permite mejorar los procesos y en este caso la transparencia de los mismos.

Generar innovación exige los esfuerzos coordinados de muchas personas y la integración de actividades vinculadas a múltiples funciones especializadas, dominios de conocimiento y ámbitos de aplicación. La propuesta planteada en este trabajo no es escalable ni realizable sin un fuerte trabajo de vinculación y cooperación interna en la universidad como externa con otras instituciones.

El sistema propuesto en este proyecto ha sido pensado de la forma más genérica posible, y se ha previsto su uso por distintas instituciones educativas, pudiendo ser utilizado por cualquier institución que registre sus instancias de aprobación utilizando actas, y que emita certificados analíticos basados en ellas. En particular, este modelo es aplicable a todas las universidades argentinas porque refleja la normativa existente a nivel nacional.

La propuesta planteada permitirá reducir los tiempos en el proceso actual de verificación de certificados y mejorará el proceso de verificación y control de la universidad.

La implementación de este proyecto permitirá que cualquier institución externa a la universidad, por ejemplo el Ministerio de Educación Nacional, pueda verificar que el certificado es emitido por el sistema académico de la universidad y que el estudiante realmente ha cumplimentado con todas sus actividades a fin de contar con su titulo habilitante para realizar trabajos profesionales.

Al momento de terminar de escribir este trabajo se encuentra desplegado en la BFA un smart contract, en donde se está realizando una etapa de prueba de guardado de actas en la BFA. Hasta el momento es un prototipo básico de la primer fase del proyecto.

Este proyecto será considerado como un caso de uso más que valida la existencia de la Blockchain Federal Argentina, en conjunto con los demás casos ya implementados o en desarrollo.

Este sistema es un paso en la dirección correcta de asegurar la transparencia, y es un caso de uso adecuado para la herramienta seleccionada, blockchain. Como se ha mostrado a lo largo de este trabajo, las soluciones basadas en blockchain son adecuadas en un estricto conjunto de casos, las cuales el proyecto reúne todas las características necesarias. Es posible mejorar y brindar mayor transparencia en los procesos administrativos basándose en este tipo de tecnología.

4.1 Trabajo futuro

La propueta planteada en este trabajo no ha tenido en cuenta aspectos como la usabilidad ni tampoco recomienda una total desplapelización de actas. Ambos son temas que requieren mejoras y no han sido abarcados en la propueta actual.

Como trabajo a futuro se necesita trabajar fuertemente en los aspectos relacionado a la usabilidad. En la propueta actual se ha tratado de plantear un sistema en donde se simplifique al máximo la operación por parte de usuarios no técnicos, el manejo de claves para la firma de las actas sigue siendo un tema conflictivo que es necesario mejorar.

Basandose en la propuesta actual del proyecto no se espera la total eliminación de las actas en papel, por lo cual otra línea de trabajo futuro es avanzar en ese sentido. Una vez implementado y afianzado este mecanismo de registro, será necesario analizar los cambios en la normativa para el reemplazo de las actas en papel por algún otro sistema de resguardo.

A

Anexo

A.1 Interfaz gráfica del sistema

Se muestra a continuación un bosquejo de la interfaz gráfica del sistema de conformidad de actas y del sistema de validación de certificados. Debemos recordar que el sistema de registro de actas no cuenta con su propia interfaz ya que el registro de actas se realiza al momento de cierre de un acta desde el sistema de gestión académica Guaraní.

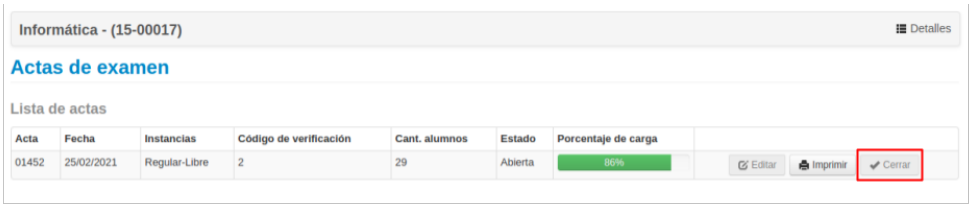


FIGURA A.1 – Interfaz gráfica del sistema Guaraní - Registro de acta. *Captura de pantalla del sistema Guaraní*

A.1.1 Conformidad de actas

El sistema que permite certificar la validez del acta por medio de firma en la Blockchain Federal Argentina. Al firmar el acta se esta generando evidencia de conformidad con el contenido del acta.

El proceso de firma implica tener el documento PDF del acta que se desea firmar, subirlo al sistema de conformidad de actas. Para poder firmar se debe generar un cuenta en la BFA, a la que luego se conectan por medio de MetaMask.

La interfaz gráfica del sistema permite visualizar en diferentes formatos el documento PDF del acta que se desea firmar. Se puede visualizar en forma de tabla o en formato JSON aparte de una previsualización del PDF.

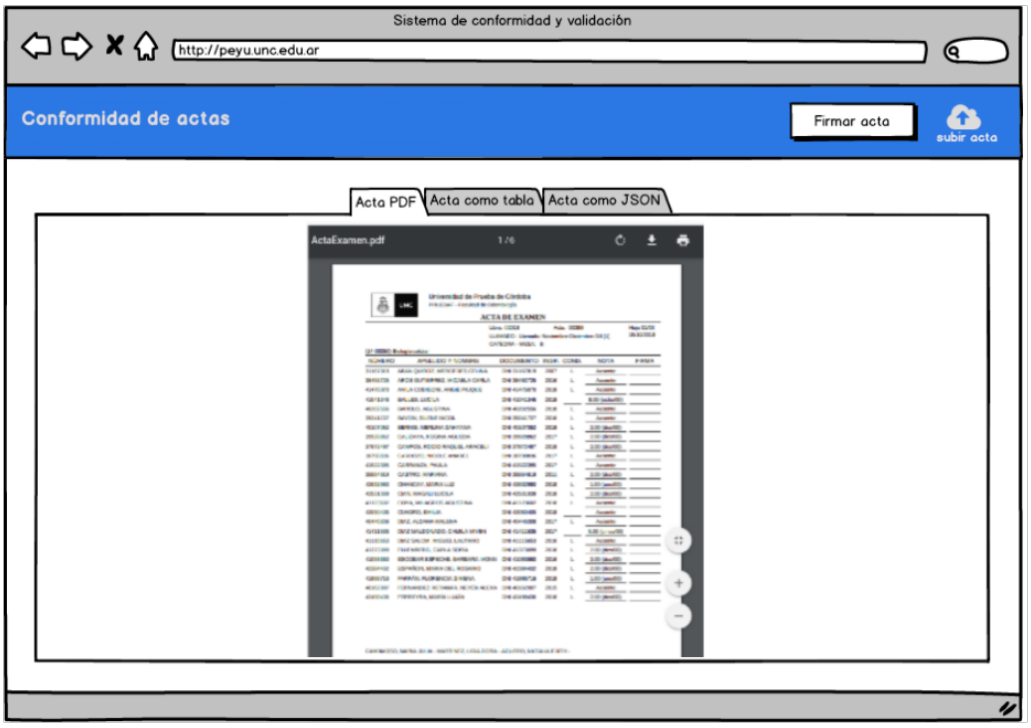


FIGURA A.2 – Interfaz gráfica - Conformidad de actas. *Elaboración propia.*

A.1.2 Validación de certificados

Una vez que las actas se encuentran en la blockchain firmadas se esta en condiciones de realizar la validación de los certificados.

La persona que desea validar un certificado debe subir al sistema validador el certificado y el sistema se encarga de recorrer renglón por renglón, identificar el acta que corresponde a cada renglón, y verificar que el resumen construido a partir del certificado coincide con el resumen registrado del acta en el contrato de blockchain.

El certificado debe tener toda la información necesaria para validarse tal cual como se guardaron en el momento de crearse las actas.

El sistema validador busca no tener falsos positivos, pero puede tener falsos negativos. Es decir, si el sistema dice que un renglón del certificado ha sido verificado, es porque se corresponde con las actas. Por el contrario, si dice que no ha podido verificarlo simplemente dice que con la evidencia existente en blockchain no puede certificar que es válido, y debe validarse por otro medio (por ejemplo, contrastando contra las actas originales).

Al igual que en la interfaz gráfica del sistema de conformidad aquí se permite visualizar en diferentes formatos el certificado. Se puede visualizar el PDF del certificado, en forma de tabla o en formato JSON.

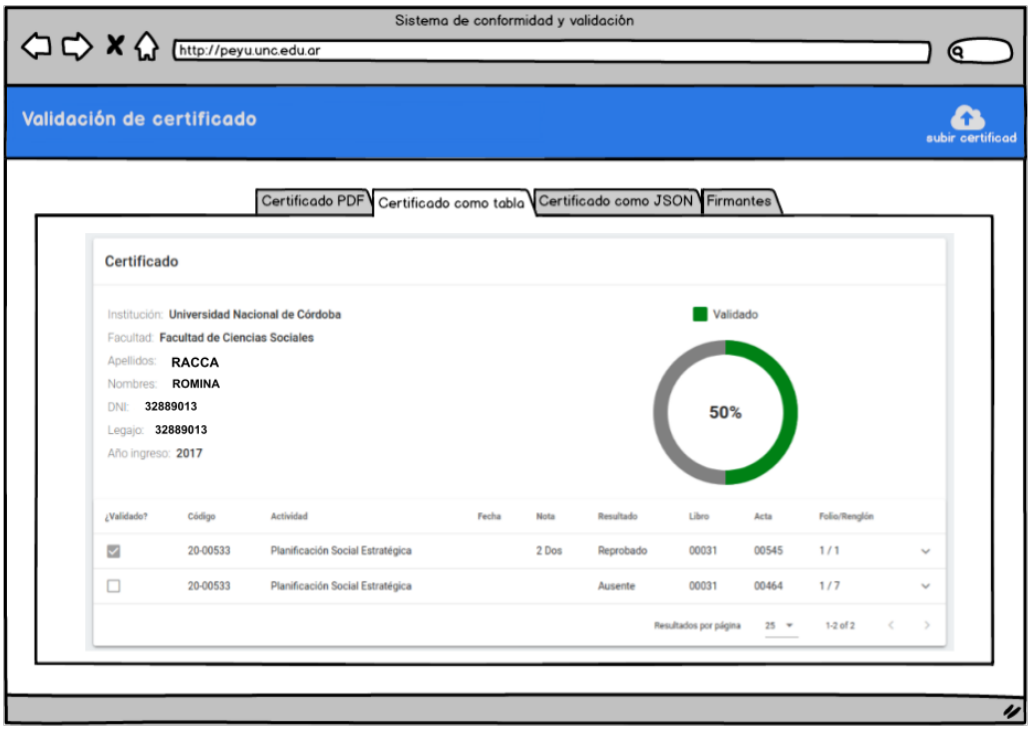


FIGURA A.3 – Interfaz gráfica - Validación de certificado. *Elaboración propia.*

La interfaz muestra el porcentaje de renglones que han podido ser validados contra las actas que se encuentran en la BFA. Los renglones que no se encuentran validados pueden ser porque las actas no se encuentren en la BFA o porque no coincida algún dato del renglón con el acta que se encuentra en la BFA.

Otra posibilidad que brinda la interfaz del sistemas es elegir los firmantes de confianza que han brindado conformidad del acta. Es decir la siguiente interfaz permite cargar de forma individual o importando de un archivo los firmantes en los que confía la persona que valida el certificado. De este modo cada renglón será considerado valido si por lo menos el acta la ha firmado uno de los firmantes de confianza de la persona que valida.

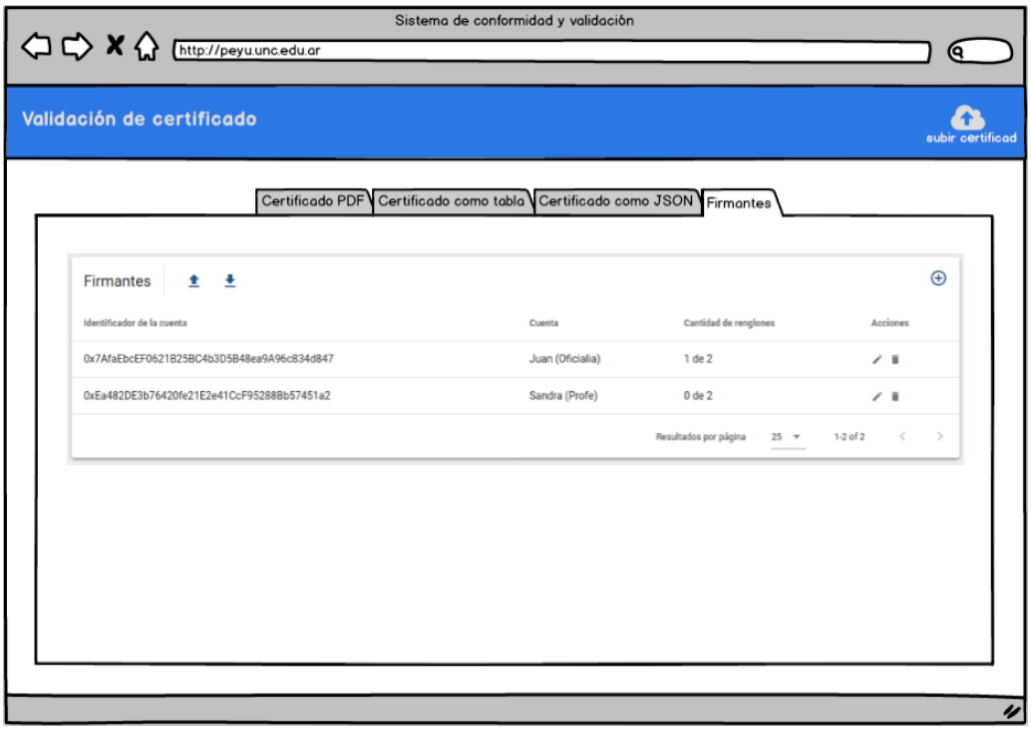


FIGURA A.4 – Interfaz gráfica - Conformidad de actas. *Elaboración propia.*

Bibliografía

[1] El Senado y Cámara de Diputados de la Nación Argentina reunidos en Congreso. Constitución de la Nación Argentina. Disponible en: http://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/804/norma.html [Internet] [acceso el 01 de octubre de 2019] 2

[2] Anuario Estadístico 2017. Universidad Nacional de Córdoba. ISBN 978-987-778-889-1. Disponible en: https://www.unc.edu.ar/sites/default/files/Anuario %20UNC %202017.pdf [Internet] [acceso el 01 de octubre de 2019] 2

[3] Estatuto de la Universidad Nacional de Córdoba. Disponible en: https://www.unc.edu.ar/sobre-la-unc/estatuto [Internet] [acceso el 01 de octubre de 2019] 2

[4] Honorable Consejo Superior. Ordenanza HCS 7/2004. Disponible en: http://www.digesto.unc.edu.ar/consejo-superior/honorable-consejo-superior/ordenanza/7_2004 [Internet] [acceso el 01 de octubre de 2019] 2.1.4

[5] SIU Guaraní. Disponible en: https://www.siu.edu.ar/siu-guarani/ [Internet] [acceso el 26 de abril de 2020] 2.2

[6] Alfred J. Menezes, Paul C. van Oorschot y Scott A. Vanstone. Handbook of Applied Cryptography. CRC Press (1997) 2.3

[7] Jean-Philippe Aumasson. Serious Cryptography. No Starch Press Inc. (2019) 2.3

[8] Signaturit. Qué es la firma digital. Disponible en: https://blog.signaturit.com/es/que-es-una-firma-digital [Internet] [acceso el 10 de mayo de 2020] 2.3

[9] Ley 25.506. Ley de Firma Digital (2001). Disponible en: http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70749/norma.html [Internet] [acceso el 01 de octubre de 2019] 2.3.1

[10] Blockchain Federal Argentina. Disponible en: https://bfa.ar/ [Internet] [acceso el 06 de marzo de 2021] 2.4, 2.4.2

[11] Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. (2006)

[12] Vitalik Buterin. Ethereum White Paper. A next generation smart contract & decentralized application platform. (2013)

[13] Gavin Wood. Ethereum: A Secure Decentralised Generalised Transaction Ledger. (2018)

[14] Solidity 0.5.12 documentation. Disponible en: https://solidity.readthedocs.io/en/v0.5.12/ [Internet] [acceso el 13 de octubre de 2019]

[15] web3.js - Ethereum Javascript API. Disponible en: https://web3js.readthedocs.io/en/v1.2.1/ [Internet] [acceso el 13 de octubre de 2019]

[16] Signaturit. Smart Contracts en el Sector Asegurador. 2.4, 2.4.1

[17] Dylan Yaga, Peter Mell, Nik Roby y Karen Scarfone. Blockchain Technology Overview NISTIR 8202. Disponible en: https://csrc.nist.gov/publications/detail/nistir/8202/final [Internet] [acceso el 13 de octubre de 2019] 3.1

[18] Project Managment Institute. Fundamentos para la dirección de proyectos (guía del PMBOK - Quinda edición). (2013) 2.7, 3.2.2

[19] Anexo Resolución Consejo Federal de Educación Nº 59/08. Sistema Federal de Títulos y Certificados Analíticos con Resguardo Documental. Disponible en: https://cfe.educacion.gob.ar/resoluciones/res08/59-08-anexo1.pdf [Internet] [acceso el 05 de marzo de 2021] 2.5

[20] Universidad Nacional de Cuyo - Prensa. Disponible en: http://www.uncuyo.edu.ar/prensa/clarin-domingo-11-formosa-mas-pruebas-sobre-titulos-truchos [Internet] [acceso el 05 de marzo de 2021] 2.5

[21] Clarin - Sociedad. Disponible en: https://www.clarin.com/sociedad/controles-evitar-titulos-truchos_0_S1Dgquj0aKx.html [Internet] [acceso el 05 de marzo de 2021] 2.5

[22] El Diario de Misiones Primera Edición. Disponible en: https://www.primeraedicion.com.ar/nota/100130904/tras-comprobar-que-el-titulo-de-tatiana-borgmann-es-falso-el-cge-la-dejo-cesante/ [Internet] [acceso el 05 de marzo de 2021] 2.5

[23] India Today. Disponible en: https://www.indiatoday.in/india/story/agra-university-awarded-thousands-of-fake-degrees-reveals-sit-287202-2015-08-08 [Internet] [acceso el 05 de marzo de 2021] 2.5

[24] BBC News. Disponible en: https://www.bbc.com/news/uk-england-32194976 [Internet] [acceso el 05 de marzo de 2021] 2.5

[25] The New York Times. Disponible en: https://www.nytimes.com/2015/05/28/world/asia/axact-chief-executive-arrested-in-pakistan-over-fake-diplomas-scandal.html [Internet] [acceso el 05 de marzo de 2021] 2.5

[26] University of Nicosia - Certificate Verification. Disponible en: https://www.unic.ac.cy/verify/ [Internet] [acceso el 05 de marzo de 2021] 2.5

[27] Jayesh G. Dongre, Sonali M. Tikam, Dr.Kishore.T.Patil y Vasudha B. Gharat. Education Degree Fraud Detection and Student Certificate Verification using Blockchain Vol. 9 Issue 07, July-2020. Disponible en: https://www.ijert.org/ [Internet] [acceso el 13 de marzo de 2021] 2.5

[28] Aamna Tariq, Hina Binte Haq y Syed Taha Ali. A Blockchain-Based Accreditation and Degree Verification System. Disponible en: https://arxiv.org/abs/1912.06812 [Internet] [acceso el 13 de marzo de 2021] 2.5