MAESTRÍA EN CIBERSEGURIDAD

PROYECTO DE GRADUACIÓN

Sometido al Tribunal Examinador de Postgrados para optar por el grado de Maestría en Ciberseguridad

Propuesta para la implementación de un sistema de identidad digital basado en blockchain para los funcionarios del Instituto Nacional de Seguros, alineado con las mejores prácticas de seguridad de la norma ISO 27001

AUTOR
Ing. Raúl Barrantes Elizondo

TUTOR: Randall Artavia Delgado

LECTOR: Irvin Argenis Sáenz Córdoba

Perez Zeledón, Costa Rica
diciembre, 2025

UNIVERSIDAD SAN ISIDRO DEL LABRADOR

MAESTRÍA EN CIBERSEGURIDAD

TRIBUNAL EXAMINADOR

Ing. Ruddy Rodríguez Acuña

Director de Maestría

Msc. Randall Artavia Delgado

Tutor

Msc. Irvin Argenis Sáenz Córdoba

Lector

DECLARACIÓN JURADA

Yo, Raúl Armando Barrantes Elizondo, mayor, soltero(a), egresado(a) de la carrera de Maestría Profesional en Ciberseguridad de la Universidad San Isidro Labrador, domiciliado en la ciudad de Naranjo, portador(a) de la cédula de identidad número 1-1262-0997, en este acto, debidamente apercibido y entendido de las penas y consecuencias con las que se castiga, en el Código Penal, el delito del perjurio, ante quienes se constituyen en el Tribunal Examinador de mi Trabajo Final de Graduación para optar por el título de maestría, juro solemnemente que mi trabajo final de graduación titulado "**Propuesta para la implementación de un sistema de identidad digital basado en blockchain para los funcionarios del Instituto Nacional de Seguros, alineado con las mejores prácticas de seguridad de la norma ISO 27001**" es una obra original que ha respetado todo lo preceptuado por las Leyes Penales así con la Ley de Derechos de Autor y Derechos Conexos, número 6683 de 14 de octubre de 1982 y sus reformas, publicada en la Gaceta número 226 de 25 de noviembre de 1982; incluyendo el numeral 70 de dicha ley que advierte: artículo 70º: Es permitido citar a un autor transcribiendo los pasajes pertinentes siempre que estos no sean tantos y seguidos, que puedan considerarse como una producción simulada y sustancial, que redunde en perjuicio del autor y de la obra original. Asimismo, quedo advertido que la Universidad San Isidro Labrador se reserva el derecho de protocolizar este documento ante Notario Público. En fe de lo anterior firmo en la ciudad de Alajuela, al ser el 16 del mes de Noviembre del año dos mil veinticinco.

Raúl Armando Barrantes Elizondo
Cédula: 112620997

DEDICATORIA

Deseo expresar mi más profundo y sincero agradecimiento a mi familia, pilar fundamental en mi vida y en mi formación. De manera muy especial, extiendo este reconocimiento a mis padres Nidia Elizondo Granados y Marvin Barrantes Avendaño, quienes, con su ejemplo de dedicación, sacrificio y amor incondicional, han sido la base sobre la cual he construido mi trayectoria académica y profesional. Su constante apoyo, sus palabras de aliento y la confianza que siempre han depositado en mí han sido motores esenciales que me impulsaron a perseverar y avanzar incluso en los momentos más desafiantes.

Agradezco profundamente a Dios, fuente de fortaleza espiritual y guía permanente en mi vida. Su presencia ha sido para mí un refugio y una inspiración, otorgándome la sabiduría, la perseverancia y la tenacidad necesarias para culminar este trabajo final y alcanzar el nivel de Maestría. Reconozco que cada paso dado, cada reto enfrentado y cada meta alcanzada han sido posibles gracias a Su dirección y a Su gracia.

Mi gratitud se extiende también a todos mis amigos y compañeros, quienes han formado parte importante de este recorrido. A mis colegas de trabajo, por su comprensión y respaldo en los momentos en que fue necesario equilibrar las responsabilidades profesionales con las académicas. A mis compañeros de los cursos de maestría, por las discusiones enriquecedoras, el intercambio de ideas y el apoyo mutuo que fortaleció nuestro crecimiento colectivo. Y, por supuesto, a mis amigos de la vida, quienes han celebrado conmigo los logros y me han acompañado en cada etapa de este proceso.

De manera muy especial, deseo expresar un agradecimiento profundo y entrañable a mi esposa Katherine Sandoval Villalobos. Su amor, paciencia, comprensión y apoyo constante han sido determinantes para que pudiera continuar y culminar este camino. Ha sido ella quien, con su presencia y motivación, me ha impulsado a mantenerme firme ante las dificultades y a perseverar con convicción. Su acompañamiento ha marcado una diferencia invaluable en cada época de mi vida y, particularmente, en esta etapa académica que hoy concluye.

AGRADECIMIENTOS

Expreso mi más sincero y profundo agradecimiento a la Universidad Internacional San Isidro Labrador (UISIL) por brindarme la oportunidad de cursar la Maestría en Ciberseguridad, un programa que constituyó un componente esencial en el fortalecimiento de mis capacidades analíticas, técnicas y metodológicas. La sólida formación recibida, fundamentada en principios actualizados de seguridad de la información, gestión de riesgos, arquitectura de ciberseguridad y normativas internacionales, permitió la consolidación de competencias clave para abordar de manera integral los desafíos contemporáneos en esta disciplina. Este proceso formativo se convirtió en un elemento determinante para la estructuración conceptual y el desarrollo metodológico del presente trabajo final de graduación.

Mi más profundo reconocimiento se dirige a mi tutor académico, cuyo acompañamiento riguroso y orientación especializada resultaron fundamentales para la correcta ejecución de cada etapa de esta investigación. Su capacidad para ofrecer retroalimentaciones precisas, su compromiso con el cumplimiento de estándares académicos y su guía en la interpretación y aplicación de marcos teóricos y metodológicos aportaron un insumo invaluable para asegurar la calidad científica y técnica del estudio.

Asimismo, extiendo un agradecimiento especial al personal técnico del Instituto Nacional de Seguros (INS), quienes brindaron un apoyo decisivo durante el proceso de aplicación del instrumento de recolección de datos. Su apertura para participar en la investigación, así como la disposición para compartir experiencias, procedimientos operativos y conocimientos especializados relacionados con controles perimetrales y mecanismos de defensa institucional, constituyeron un aporte significativo para la validación empírica y el análisis detallado de los resultados obtenidos. La información facilitada permitió profundizar en el entendimiento de las prácticas actuales y de los retos asociados a la gestión de la seguridad en entornos organizacionales reales.

Finalmente, manifiesto mi más profundo agradecimiento a mi familia, cuyo apoyo incondicional, paciencia y respaldo emocional fueron indispensables para sostener el ritmo académico y afrontar de manera equilibrada las exigencias de esta etapa.

Su acompañamiento constante, motivación y comprensión contribuyeron de manera determinante a la culminación exitosa de este trabajo y al cumplimiento de esta meta profesional y personal.

CARTA DE AUTORIZACIÓN DEL TUTOR

Pérez Zeledón, 06 de diciembre 2025

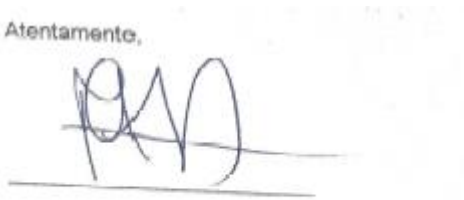
Licenciado
Ruddy Rodríguez Acuña
Coordinador de la Escuela de Informática
Universidad Internacional San Isidro Labrador

Estimado señor Coordinador:

Yo, Randall Mauricio Artavia Delgado, mayor, Ingeniero en informática, con domicilio en la Trinidad de Moravia San José, portador de la cédula de identidad número 205740823, en mi condición de tutor del Proyecto de Graduación titulado Maestría en Ciberseguridad. propuesta por el estudiante Raul Armando Barrantes Elizondo, manifiesto lo siguiente:

1. Que el proceso de trabajo final de graduación culmina satisfactoriamente.
2. Que se ha incorporado en el documento final las sugerencias hechas por el Tribunal Examinador.
3. Que he cumplido con el acompañamiento encomendado por la Universidad en forma y fondo.
4. Que considero que el documento final responde a las exigencias académicas establecidas por la Universidad.

Atentamente,



MATI Randall Mauricio Artavia Delgado
Tutor

CARTA DE APROBACIÓN DEL LECTOR

Pérez Zeledón, 06 de diciembre 2025

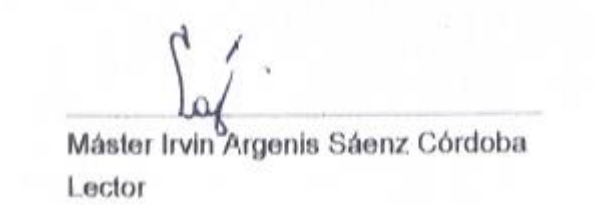
Licenciado
Ruddy Rodríguez Acuña
Coordinador de la Escuela de Informática
Universidad Internacional San Isidro Labrador

Estimado señor Coordinador:

Yo, Irvin Argenis Sáenz Córdoba, mayor, Casado, Máster Ciberseguridad , vecino de Guapiles, portador de la cédula de identidad número 7-0197-0839, en mi condición de lector del Proyecto de Graduación titulado Maestría de Ciberseguridad propuesta por el estudiante Raúl Armando Barrantes Elizondo, manifiesto lo siguiente:

1. Que la lectura del trabajo final de graduación concluye satisfactoriamente.
2. Que he leído el documento final y he hecho mis observaciones en el mismo.
3. Que he cumplido con las labores de lector encomendadas por la Universidad en forma y fondo.
4. Que considero que el documento final responde a las exigencias académicas establecidas por la Universidad.

Atentamente,



Máster Irvin Argenis Sáenz Córdoba
Lector

TABLA DE CONTENIDOS

ÍNDICE DE TABLAS Y CUADROS

ÍNDICE DE GRÁFICOS, FIGURAS E ILUSTRACIONES

LISTA DE PALABRAS CLAVES

Identidad digital

Blockchain

Identidad autosoberana (SSI)

Credenciales verificables (VC)

Identificadores descentralizados (DID)

Seguridad de la información

ISO/IEC 27001

Gestión del riesgo

Trazabilidad

Autenticación multifactor

Aplicación móvil institucional

Tarjetas NFC

Ciberseguridad

Gobernanza digital

Transformación digital

Infraestructura institucional

Protección de datos

Criptografía

Acceso seguro

Auditoría tecnológica

Descentralización

Modelo de identidad

Continuidad operativa

Interoperabilidad

Arquitectura digital

Resiliencia tecnológica

RESUMEN EJECUTIVO

El presente Trabajo Final de Graduación propone el diseño de un sistema de identidad digital descentralizada basado en tecnología blockchain para reemplazar el mecanismo tradicional de acceso físico mediante tarjetas NFC utilizado en el Instituto Nacional de Seguros (INS). La propuesta surge a partir de la identificación de brechas operativas y de seguridad que afectan la eficacia del modelo actual de autenticación, así como de la necesidad institucional de modernizar sus procesos en concordancia con marcos internacionales como ISO/IEC 27001.

El estudio inicia con un diagnóstico de la situación actual mediante la aplicación de un cuestionario estructurado dirigido al personal técnico de TI, Seguridad Informática, Auditoría y Recursos Humanos. Los resultados cuantitativos evidencian que el 100% de los funcionarios utiliza tarjetas NFC, mientras que más del 75% ha experimentado fallos operativos, duplicaciones o inconsistencias en su funcionamiento. Asimismo, el 87.5% manifiesta interés en migrar hacia un sistema más moderno basado en una aplicación móvil institucional. A nivel tecnológico, el 75% afirma conocer la tecnología blockchain y el 87.5% apoya su incorporación en los procesos de autenticación y control de acceso.

Complementariamente, se realizaron entrevistas semiestructuradas que permitieron profundizar en los principales riesgos asociados al modelo actual, entre ellos: pérdida o clonación de tarjetas, lentitud en la revocación de credenciales, falta de trazabilidad robusta y ausencia de mecanismos avanzados de auditoría. La revisión documental corroboró estas debilidades y evidenció la necesidad de un sistema alineado con buenas prácticas internacionales de seguridad.

El análisis de riesgos permitió clasificar amenazas, vulnerabilidades y controles, confirmando que el sistema NFC representa un punto crítico dentro del ecosistema de acceso institucional. Entre los hallazgos más relevantes destacan la insuficiente trazabilidad de eventos, el riesgo de suplantación de identidad y la dependencia de un sistema centralizado susceptible a fallos.

Con base en los resultados, se desarrolló una propuesta técnica que consiste en un sistema de identidad digital descentralizada, fundamentado en Identificadores Descentralizados (DID) y Credenciales Verificables (VC), sostenido en una

blockchain permisionada. Este modelo sustituye el uso de tarjetas físicas por una aplicación móvil institucional capaz de generar autenticación mediante QR dinámicos, Bluetooth o NFC digital, además de ofrecer mecanismos avanzados de auditoría, revocación y trazabilidad inmutable.

La propuesta busca fortalecer la gobernanza digital del INS, mejorar la eficiencia operativa, reducir riesgos asociados a la pérdida o clonación de tarjetas, y alinear la gestión de identidades con estándares internacionales como ISO/IEC 27001 e ISO/IEC 27555. Adicionalmente, prepara a la institución para una futura interoperabilidad con plataformas estatales de identidad digital.

Los resultados del estudio demuestran que el INS se encuentra en condiciones técnicas y organizacionales para realizar esta transición, contando con recursos humanos capacitados, infraestructura tecnológica apta y una alta disposición al cambio por parte del personal. El modelo propuesto constituye un avance significativo en la modernización institucional y posiciona al INS como una entidad pionera en la adopción de identidad digital soberana dentro del sector público costarricense.

CAPITULO I. INTRODUCCIÓN

1.1 Planteamiento del tema de estudio

La presente propuesta tiene como finalidad plantear una solución tecnológica innovadora para el manejo de identidades digitales en el Instituto Nacional de Seguros (INS), utilizando tecnología blockchain [1] como pilar fundamental. La iniciativa se enmarca en los esfuerzos de transformación digital del sector público, promoviendo sistemas más seguros, auditables y eficientes. La propuesta se basa en la implementación de un sistema alineado con la norma Sistema de Gestión de Seguridad de Información SGSI (ISO 27001), garantizando así el cumplimiento de estándares internacionales en gestión de la seguridad de la información.

El interés por este tema ha surgido a partir de múltiples referencias bibliográficas y experiencias internacionales que evidencian el potencial de la tecnología blockchain para transformar la forma en que se gestionan las identidades digitales. Países como Estonia, Suiza, Corea del Sur y Argentina han demostrado que es posible descentralizar el control de credenciales personales mediante esquemas de identidad soberana (SSI), mejorando la seguridad, la privacidad y la eficiencia operativa (Vassil, 2015; IDB, 2023; Blockchain Labs, 2021).

En el contexto nacional, Costa Rica cuenta con avances importantes en materia de identidad digital, como el Sistema Nacional de Certificación Digital operado por el MICITT, así como proyectos en desarrollo liderados por el Tribunal Supremo de Elecciones. Sin embargo, estas soluciones aún dependen de modelos centralizados y dispositivos físicos, lo cual limita su alcance y escalabilidad (MICITT, 2023; TSE, 2024). Dentro del INS, la gestión actual de identidad se encuentra fragmentada, con mecanismos basados en usuarios y contraseñas que carecen de validación distribuida, trazabilidad robusta y control sobre el ciclo de vida de las credenciales.

---

1. Blockchain es una tecnología de registro distribuido que permite almacenar datos de manera descentralizada, segura e inmutable. Cada bloque contiene un conjunto de transacciones y está vinculado criptográficamente al bloque anterior, formando una cadena inalterable. Su diseño evita la necesidad de intermediarios, favoreciendo la confianza entre las partes (Narayanan et al., 2016).

Por lo tanto, esta propuesta se enfoca en diseñar un sistema de identidad digital que permita al INS garantizar una autenticación segura, verificable y auditable, con base en una arquitectura blockchain privada o permisionada. El enfoque adoptado busca integrar los principios de identidad descentralizada (DID), credenciales verificables (VC) y control criptográfico de accesos, todo ello bajo un modelo alineado con los controles de la norma ISO/IEC 27001. De esta forma, se espera establecer un referente técnico y normativo que fortalezca la seguridad institucional, la gobernanza digital y la confianza organizacional.

La propuesta nace, entonces, como respuesta a una necesidad institucional evidente, documentada en experiencias internacionales exitosas y sustentada en principios normativos reconocidos, y conduce directamente al problema identificado: la ausencia de un modelo moderno y descentralizado para la gestión de identidad funcional en el INS, alineado con los estándares globales de seguridad de la información.

1.2 Antecedentes del tema

En los últimos años, el Instituto Nacional de Seguros (INS) ha avanzado en la digitalización de diversos procesos administrativos. Sin embargo, uno de los desafíos persistentes en la organización es la gestión de identidades digitales de sus funcionarios, la cual se realiza actualmente mediante mecanismos centralizados, dependientes de credenciales estáticas, sin trazabilidad robusta ni validación distribuida. Esta situación representa una vulnerabilidad crítica para la seguridad institucional, especialmente en contextos donde el acceso remoto, el teletrabajo y la interoperabilidad con otros sistemas del Estado se han vuelto comunes.

Varios estudios han advertido que los esquemas de autenticación tradicionales están expuestos a suplantación de identidad, reutilización de contraseñas, y acceso no autorizado, factores que comprometen la integridad y disponibilidad de los sistemas institucionales (Zhou, Zhang, & Xie, 2020). En consecuencia, se requiere un enfoque que trascienda la simple provisión de herramientas tecnológicas y que

se centre en el tratamiento integral de la identidad como un activo crítico de seguridad de la información.

Por otro lado, el uso de tecnologías emergentes como blockchain ha sido propuesto en diferentes sectores como un medio eficaz para la gestión de identidades digitales seguras y descentralizadas. Estas soluciones permiten a las instituciones garantizar el control distribuido, la trazabilidad de accesos y la autonomía de los usuarios sobre su información personal (Zyskind, Nathan, & Pentland, 2015). No obstante, en el caso del INS, aún no se ha adoptado un sistema que incorpore estos principios ni que se encuentre alineado con estándares internacionales como la norma ISO/IEC 27001, la cual provee un marco sólido para el manejo seguro de la información (ISO, 2013).

Este vacío tecnológico y normativo se ve agravado por la creciente necesidad de cumplir con las regulaciones sobre protección de datos personales y seguridad de la información, lo que demanda un sistema moderno, auditado y alineado con buenas prácticas. A nivel organizacional, la ausencia de una solución de identidad digital robusta limita la capacidad del INS para controlar eficazmente los accesos a sistemas críticos, exponer menos superficie a ataques internos y externos, y establecer una gobernanza clara de la identidad digital.

En términos de alcance, el presente trabajo se enfocará exclusivamente en la propuesta de un sistema de identidad digital descentralizada para funcionarios activos del INS, sin abordar aún clientes o usuarios externos. El análisis se delimita al entorno organizacional del INS en el contexto postpandemia (2020–2025), periodo en el que se ha intensificado el uso de plataformas digitales y se ha hecho evidente la necesidad de modernizar la infraestructura de seguridad.

Por tanto, el problema central identificado es la ausencia de un modelo de identidad digital descentralizada y alineada con estándares internacionales, que permita al INS garantizar el control seguro, verificable y autónomo de las identidades funcionales de sus colaboradores, lo cual genera una necesidad urgente de revisar y modernizar el enfoque actual de gestión de identidades digitales institucionales.

1.3 Justificación

La implementación de un sistema de identidad digital basado en tecnología blockchain para los funcionarios del Instituto Nacional de Seguros (INS), alineado con las mejores prácticas de la norma ISO/IEC 27001, responde a una necesidad urgente de fortalecer la seguridad, eficiencia y autonomía en la gestión de identidades dentro de la institución. Esta propuesta adquiere relevancia en el marco de la transformación digital del sector público costarricense, donde las entidades enfrentan crecientes desafíos relacionados con la protección de datos, la ciberseguridad y la interoperabilidad de sistemas.

En la era digital, la gestión de identidades se ha consolidado como un componente esencial de los sistemas de seguridad de la información. Un fallo en este proceso puede generar consecuencias críticas, como accesos indebidos a información sensible, interrupciones operativas o incidentes de fraude institucional. Según Narayanan et al. (2016), los métodos tradicionales de autenticación basados en credenciales centralizadas y contraseñas son vulnerables a amenazas como el phishing, la reutilización de claves y el robo de identidad.

Estas limitaciones técnicas tienen implicaciones directas para organizaciones como el INS, que maneja información sensible de carácter personal, financiero, legal y médico. La protección de esta información debe garantizarse no solo por cumplimiento normativo, sino también para preservar la confianza de los usuarios internos y externos.

En este contexto, las tecnologías emergentes como blockchain permiten rediseñar el paradigma de gestión de identidades. Al tratarse de un sistema descentralizado, cada identidad puede ser validada de manera segura, verificable e inmutable, eliminando los riesgos asociados a puntos únicos de falla (Zyskind, Nathan, & Pentland, 2015). Además, el uso de blockchain facilita la implementación de mecanismos de control de acceso basados en atributos, el registro de auditoría distribuido y la gestión de credenciales reutilizables sin exponer datos personales a terceros.

Por su parte, la norma ISO/IEC 27001 establece las bases para un Sistema de Gestión de Seguridad de la Información (SGSI) robusto. Integrar este marco en el diseño del sistema de identidad digital garantiza que se consideren principios como el análisis de riesgos, la gestión de activos de información, la seguridad de los recursos humanos, el control de accesos, la criptografía y la continuidad del negocio (ISO, 2013). De esta manera, la propuesta no solo es técnicamente sólida, sino también alineada con las buenas prácticas reconocidas a nivel internacional.

Utilidad, Beneficios y Alcance del Trabajo

Este trabajo se propone diseñar una solución que transforme estructuralmente la manera en que se autentican los funcionarios del INS, con implicaciones positivas en las siguientes áreas:

- **Seguridad de la información**: Reducción significativa del riesgo de accesos no autorizados y pérdida de integridad de datos sensibles.
- **Trazabilidad y cumplimiento**: Auditoría completa y automática de los accesos e identidades, facilitando el cumplimiento con regulaciones locales como la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales (Ley N.º 8968).
- **Autonomía del usuario**: Permite a cada funcionario controlar su identidad digital mediante mecanismos descentralizados, sin depender de intermediarios.
- **Reducción de costos operativos**: Al automatizar procesos de verificación y acceso, se reduce la carga administrativa de gestión de usuarios y soporte técnico.
- **Reputación institucional**: Posiciona al INS como líder en innovación dentro del aparato estatal costarricense, promoviendo una cultura de seguridad avanzada y orientada a resultados.

Beneficiarios del Proyecto

- **Funcionarios del INS**: Accederán a un sistema de identidad más eficiente, confiable y respetuoso de su privacidad digital.
- **Dirección de Tecnología de la Información**: Contará con un marco de control más robusto, moderno y automatizado para la administración de identidades.
- **Gestores de cumplimiento y auditoría**: Dispondrán de trazabilidad verificable para sustentar procesos de revisión interna y externa.

El Estado costarricense: Obtendrá un caso de referencia para la integración de blockchain y estándares internacionales en la gestión pública.

1.4 Objetivos

1.4.1 Objetivo general

Diseñar una propuesta para un sistema de identidad digital descentralizada, utilizando tecnología blockchain y cumpliendo con los lineamientos de la norma ISO/IEC 27001, para mejorar la seguridad, trazabilidad y control de las credenciales digitales de los funcionarios del Instituto Nacional de Seguros (INS), durante el periodo 2025–2026, en el marco de su estrategia institucional de transformación digital.

1.4.2 Objetivos específicos

Diagnosticar la situación actual, para determinar posibles brechas en la identidad digital que puedan estar afectando al Instituto Nacional de Seguros.

Elaborar un análisis de riesgos, que permita evaluar el impacto y la probabilidad de los riesgos asociados a la identidad digital, que pueden afectar a la organización.

Diseñar una propuesta para solución tecnológica clara y adaptada a la realidad del INS, que aproveche las ventajas de la tecnología blockchain para garantizar que cada funcionario pueda acceder de forma segura.

1.5 Alcances

El alcance se centrará en el diseño de una propuesta para un sistema de identidad digital descentralizada orientado exclusivamente a los funcionarios activos del Instituto Nacional de Seguros (INS). La propuesta se desarrollará con base en los principios de la tecnología blockchain y los lineamientos establecidos por la norma internacional ISO/IEC 27001, que rige los sistemas de gestión de seguridad de la información (SGSI).

El alcance de esta propuesta comprende:

- El análisis del contexto institucional del INS en relación con la gestión de identidades digitales, esto implica revisar cómo el Instituto Nacional de Seguros (INS) actualmente administra las identidades digitales de sus funcionarios.
- La identificación de brechas y riesgos en el sistema actual de autenticación; realizar un diagnóstico técnico y normativo que permita detectar vulnerabilidades, amenazas y debilidades en el sistema actual de autenticación
- El diseño de una solución técnica que integre mecanismos como Identificadores Descentralizados (DID), Credenciales Verificables (VC), trazabilidad criptográfica y control de acceso basado en blockchain privada o permisionada.
- La alineación del diseño propuesto con los requisitos y controles de la norma ISO/IEC 27001, incluyendo aspectos como control de accesos, criptografía, análisis de riesgos y continuidad del negocio.

No se abordarán en esta investigación elementos como:

- La inclusión de clientes externos o asegurados del INS.
- La implementación técnica del sistema (fase de desarrollo o programación).
- El análisis financiero o de adquisición de infraestructura tecnológica.

1.6 Limitaciones

Limitaciones en el tratamiento de la formulación del tema.

A pesar del enfoque innovador de la propuesta, existen diversas limitaciones inherentes tanto a la tecnología blockchain como al contexto institucional del INS:

- **Madurez tecnológica**: Blockchain es una tecnología emergente cuya adopción aún está en proceso en el sector público costarricense, lo que implica desafíos regulatorios y técnicos (Zyskind et al., 2015).
- **Falta de estandarización**: No existe un estándar único para la implementación de identidades digitales basadas en blockchain, lo que puede generar barreras de interoperabilidad y escalabilidad (ISO, 2013).
- **Limitado conocimiento institucional**: La adopción de nuevas tecnologías enfrenta resistencia al cambio y requerimientos de capacitación para el personal institucional (Narayanan et al., 2016).
- **Costos asociados**: La implementación de blockchain implica inversión inicial considerable en infraestructura tecnológica, desarrollo y mantenimiento, lo cual puede no ser viable en el corto plazo sin estudios de factibilidad financiera (Blockchain Labs, 2021).
- **Escalabilidad**: Las soluciones blockchain deben estar diseñadas para soportar crecimiento en usuarios y volumen de transacciones, lo que representa un reto técnico en entornos complejos como el del INS (Vassil, 2015).
- **Privacidad y protección de datos**: Aunque blockchain ofrece mecanismos de seguridad avanzados, se deben tomar precauciones para cumplir con la normativa local de protección de datos (Ley 8968) y evitar la exposición indebida de información personal (IDB, 2023).

1.7 Cronograma de actividades

NOMBRE DE LA TAREA	DURACIÓN	INICIO	FINAL
Planeación del trabajo	3 semanas	06-05-2025	24-05-2025
- Definición del título	1 semana	06-05-2025	12-05-2025
- Definición de objetivos	1 semana	06-05-2025	12-05-2025
- Creación del cronograma	1 semana	13-05-2025	19-05-2025
- Creación bitácora de trabajo	1 semana	13-05-2025	19-05-2025
- Entrega del plan de trabajo al tutor	1 semana	02-10-2025	08-10-2025
Desarrollo del Capítulo I	3 semanas	27-05-2025	14-06-2025
- Creación de estructura del TFG	1 semana	27-05-2025	02-06-2025
- Planteamiento del tema	1 semana	27-05-2025	02-06-2025
- Justificación del trabajo	1 semana	03-06-2025	09-06-2025
- Definición de alcances	1 semana	03-06-2025	09-06-2025
- Definición de limitaciones	1 semana	10-06-2025	14-06-2025
- Definición producto esperado	1 semana	10-06-2025	14-06-2025
- Envío Capítulo I al tutor	1 día	14-06-2025	14-06-2025
Desarrollo del Capítulo II	4 semanas	17-06-2025	14-07-2025
- Desarrollo de marco teórico	4 semanas	17-06-2025	14-07-2025
- Envío Capítulo II al tutor	1 día	14-07-2025	14-07-2025
Desarrollo del Capítulo III	4 semanas	15-07-2025	11-08-2025
- Tipo de Investigación	1 semana	15-07-2025	21-07-2025
- Administración y abordaje	1 semana	15-07-2025	21-07-2025
- Sujetos y fuentes	1 semana	22-07-2025	28-07-2025
- Diseño de técnicas e instrumentos	1 semana	29-07-2025	04-08-2025
- Envío Capítulo III al tutor	1 día	11-08-2025	11-08-2025
Desarrollo del Capítulo IV	3 semanas	12-08-2025	01-09-2025
- Introducción a la propuesta	1 semana	12-08-2025	18-08-2025
- Propuesta	2 semanas	19-08-2025	01-09-2025
- Envío Capítulo IV al tutor	1 día	01-09-2025	01-09-2025
Desarrollo del Capítulo V	4 semanas	09-10-2025	05-11-2025
- Desarrollo conclusiones	2 semanas	02-09-2025	15-09-2025
- Desarrollo recomendaciones	1 semana	16-09-2025	22-09-2025
- Resumen ejecutivo	1 semana	23-09-2025	29-09-2025
- Anexos	1 semana	23-09-2025	29-09-2025
- Envío Capítulo V al tutor	1 día	06-11-2025	06-11-2025

1.8 Producto esperado del TFG

Objetivos específicos	Entregables	Formato
Diagnosticar la situación actual, para determinar posibles brechas en la identidad digital que puedan estar afectando al Instituto Nacional de Seguros.	Informe de diagnóstico institucional de identidad digital, incluyendoanálisis de situación actual, herramientas usadas, métodos de autenticación, deficiencias y análisis comparativo con modelos internacionales.	Documento Word / PDF
Elaborar un análisis de riesgos, que permita evaluar el impacto y la probabilidad de los riesgos asociados a la identidad digital, que pueden afectar a la organización.	Matriz de riesgos con probabilidad e impacto, categorización de amenazas, controles actuales, controles necesarios y recomendaciones priorizadas.	Hoja de Cálculo / Word
Diseñar una propuesta para solución tecnológica clara y adaptada a la realidad del INS, que aproveche las ventajas de la tecnología blockchain para garantizar que cada funcionario pueda acceder de forma segura.	Documento técnico con la arquitectura propuesta del sistema de identidad digital descentralizada, componentes tecnológicos, alineamiento con ISO/IEC 27001, y esquema de implementación futura.	Documento técnico con la arquitectura propuesta del sistema de identidad digital descentralizada, componentes tecnológicos, alineamiento con ISO/IEC 27001, y esquema de

		implementación futura.

CAPÍTULO II. MARCO TEÓRICO

El presente marco teórico tiene como objetivo contextualizar y sustentar el diseño de un sistema de identidad digital descentralizada basado en tecnología blockchain, alineado con los lineamientos de la norma ISO/IEC 27001. Se explorarán los fundamentos de la identidad digital, los modelos actuales de gestión, la integración de blockchain en este ámbito, los principios de la norma ISO/IEC 27001 y el contexto normativo costarricense, además de casos de uso internacionales y tendencias emergentes.

2.1 Fundamentos de la identidad digital

Definición

La identidad digital puede definirse como el conjunto de atributos, credenciales y representaciones electrónicas que identifican de manera única a un individuo, organización o dispositivo en entornos digitales (Zhou, Zhang & Xie, 2020). A diferencia de la identidad física, que se basa en documentos oficiales y procesos presenciales, la identidad digital se autentica a través de datos electrónicos como nombres de usuario, contraseñas, certificados digitales, biometría o claves criptográficas.

Según Allen (2016), la identidad digital “es la base sobre la cual se construyen las relaciones de confianza en el mundo digital”, lo que la convierte en un activo estratégico para gobiernos, empresas y ciudadanos. Una gestión inadecuada de este activo puede derivar en accesos no autorizados, fraude y vulneración de datos personales, impactando directamente en la seguridad de las organizaciones y en los derechos de los usuarios.

Tipos de identidad digital

Existen tres modelos principales de gestión de identidad digital, cada uno con ventajas y limitaciones:

- **Modelo centralizado:**

En este modelo, una autoridad única (como una institución estatal o empresa tecnológica) administra la creación, almacenamiento y verificación de identidades. Aunque es el sistema más común y sencillo de implementar, concentra riesgos al centralizar toda la información en un único repositorio, haciéndolo susceptible a ciberataques y violaciones de privacidad (Narayanan et al., 2016).

- **Modelo federado:**

  Este modelo permite que múltiples organizaciones validen identidades de forma compartida. Ejemplos son los accesos con cuentas de Google o Facebook. Aunque mejora la interoperabilidad, los usuarios siguen sin tener control sobre sus datos, delegando la gestión a grandes proveedores (Sporny et al., 2022).

- **Modelo descentralizado:**

  En este enfoque, los usuarios son los principales custodios de sus credenciales, que se almacenan en billeteras digitales. Gracias al uso de tecnologías como blockchain y estándares de Identificadores Descentralizados (DID), las personas pueden decidir qué datos comparten y con quién, reduciendo la dependencia de intermediarios (Allen, 2016). Este es el paradigma que sustenta el concepto de identidad soberana.

Problemas comunes en los modelos tradicionales

Los modelos centralizados y federados, aunque dominantes, presentan desafíos significativos:

- **Riesgo de ciberataques masivos:** Una vulneración puede comprometer millones de identidades (Narayanan et al., 2016).
- **Falta de control individual:** Los usuarios no deciden cómo, cuándo y con quién comparten sus datos.
- **Déficit de transparencia:** Dificultades para auditar accesos y usos de las credenciales.

- **Dependencia de terceros:** Lo que puede limitar la soberanía digital, especialmente en contextos gubernamentales.

Estos problemas explican por qué las tendencias actuales apuntan hacia modelos descentralizados, que priorizan la autonomía del usuario, el uso de mecanismos criptográficos avanzados y la eliminación de intermediarios.

Modelo	Características	Ventajas	Desventajas	Ejemplos reales
Centralizado	Administrado por una única autoridad (gobierno, empresa).	- Implementación simple.- Control total por la entidad emisora.	- Punto único de falla.- Alta vulnerabilidad a ciberataques.- Sin control del usuario.	Sistema Nacional de Certificación Digital (Costa Rica).
Federado	Identidad compartida entre múltiples organizaciones confiables.	- Interoperabilidad entre plataformas.- Reducción de credenciales múltiples.	- Dependencia de grandes proveedores.- Complejidad en la gobernanza de datos.	Autenticación con cuentas Google/Facebook para servicios estatales.
Descentralizado	Basado en blockchain y estándares como DID (Identificadores Descentralizados).	- Control del usuario sobre sus datos.- Mayor seguridad y trazabilidad.- Reducción de intermediarios.	- Complejidad técnica.- Necesidad de infraestructura avanzada.- Curva de adopción.	QuarkID (Argentina), COOV (Corea del Sur).

Tabla 1. Comparación modelos de gestión de identidad digital

Esta tabla ilustra claramente las diferencias fundamentales entre los modelos, ayudando a visualizar por qué el modelo descentralizado es el más adecuado para entornos como el del Instituto Nacional de Seguros (INS), que necesita combinar seguridad, trazabilidad y autonomía.

2.2 Norma ISO/IEC 27001 en la Gestión de Identidad

La ISO/IEC 27001:2013 es el estándar internacional más reconocido para implementar un Sistema de Gestión de Seguridad de la Información (SGSI). Este marco establece los requisitos para identificar, evaluar y mitigar riesgos relacionados con la seguridad de los datos, con el fin de garantizar la

confidencialidad, integridad y disponibilidad de la información (International Organization for Standardization [ISO], 2013).

En el contexto de la identidad digital, esta norma adquiere un papel crítico, pues establece directrices claras para el control de accesos (A.9), la gestión de credenciales y privilegios, el uso seguro de criptografía (A.10), la protección de datos personales y el registro y monitoreo de actividades (A.12). En otras palabras, ISO 27001 define los controles necesarios para evitar accesos no autorizados, fugas de datos y usos indebidos de las credenciales.

Principales controles aplicables a la identidad digital

A continuación, se destacan los controles más relevantes para un sistema de identidad digital descentralizada:

1. **A.9 Control de acceso:**
    - Establece políticas para asignar y revocar permisos de acceso a los usuarios.
    - Implementación de mecanismos robustos de autenticación (por ejemplo, multifactor).
    - Segregación de funciones y gestión segura de cuentas con privilegios elevados.
2. **A.10 Criptografía:**
    - Uso de algoritmos y claves robustas para proteger datos sensibles.
    - Aplicación de técnicas de cifrado para el almacenamiento y la transmisión de credenciales digitales.
3. **A.12 Registro y monitoreo:**
    - Registro de eventos de seguridad relacionados con la gestión de identidades.
    - Detección temprana de accesos indebidos y análisis forense ante incidentes.

4. **A.18 Cumplimiento legal:**
    - Asegura que el tratamiento de identidades respete las normativas de protección de datos, como la Ley 8968 en Costa Rica o el GDPR en Europa.

Ejemplos prácticos

- **Gobiernos europeos:** Integran ISO 27001 en sus plataformas nacionales de identidad (como en Estonia) para garantizar la seguridad de las credenciales electrónicas y proteger los servicios digitales gubernamentales.
- **Sector bancario:** Las entidades financieras usan estos controles para autenticar clientes y empleados, con registros auditables que facilitan la detección de fraudes.
- **Empresas aseguradoras:** Implementan políticas de control de acceso basadas en ISO 27001 para limitar privilegios según el rol del colaborador, alineando el modelo con los requisitos regulatorios.

Control ISO 27001	Aplicación en identidad digital	Beneficio principal
A.9 Control de acceso	Asignación y revocación segura de credenciales; autenticación multifactor.	Prevención de accesos indebidos.
A.10 Criptografía	Cifrado de credenciales y datos sensibles.	Protección ante filtraciones y ataques.
A.12 Registro de eventos	Monitoreo continuo y trazabilidad de accesos.	Detección temprana de incidentes.
A.18 Cumplimiento	Alineación con leyes de protección de datos.	Evitar sanciones y fortalecer la confianza.

Tabla 2 Controles ISO/IEC 27001 aplicados a la identidad digital

2.3 Contexto Normativo en Costa Rica

Costa Rica ha avanzado en el ámbito de la identidad digital con iniciativas como el Sistema Nacional de Certificación Digital (MICITT, 2023) y el proyecto del Tribunal Supremo de Elecciones (TSE) sobre identidad digital nacional. La Ley 8968 sobre protección de datos personales refuerza la necesidad de sistemas que aseguren la privacidad y el control de la información de los usuarios.

El punto de partida relevante es el Sistema Nacional de Certificación Digital, operado por el Banco Central de Costa Rica y supervisado por el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT), que habilita el uso de firmas electrónicas avanzadas para autenticar documentos y trámites en línea (MICITT, 2023).

Sistema Nacional de Certificación Digital

Este sistema se basa en una infraestructura de clave pública (PKI) que permite a los ciudadanos firmar electrónicamente documentos con validez legal. Entre sus características destacan:

- **Emitido por el Banco Central:** lo que garantiza un nivel alto de confianza institucional.
- **Basado en tokens físicos:** certificados almacenados en dispositivos USB o tarjetas inteligentes.
- **Reconocimiento legal:** en concordancia con la Ley 8454 sobre certificados, firmas digitales y documentos electrónicos.

Si bien ha sido un avance significativo, su adopción ha sido limitada, debido a barreras como:

- **Requisitos técnicos complejos:** necesidad de lectores y software especializado.
- **Desconocimiento por parte de la población:** baja alfabetización digital.
- **Enfoque centralizado:** que limita la interoperabilidad con sistemas descentralizados y modelos más modernos como SSI (Self-Sovereign Identity).

Proyecto del Tribunal Supremo de Elecciones (TSE): identidad digital nacional

En 2024, el TSE anunció un ambicioso proyecto para lanzar la cédula de identidad digital, disponible inicialmente en dispositivos móviles (TSE, 2024). Este proyecto busca:

- Facilitar la autenticación en plataformas públicas y privadas.
- Ampliar el acceso a trámites sin necesidad de interacción presencial.
- Fortalecer los controles biométricos asociados a la identidad nacional.

Sin embargo, aún persiste el desafío de definir si esta solución adoptará un modelo descentralizado o si continuará con un enfoque centralizado tradicional, lo cual condicionará su potencial de interoperabilidad y empoderamiento del ciudadano sobre sus datos.

Marco normativo: Ley 8968 sobre protección de datos

La Ley 8968, conocida como la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales, establece principios como:

- **Consentimiento informado:** los datos solo pueden tratarse con autorización del titular.
- **Finalidad legítima:** uso restringido al propósito declarado.
- **Minimización de datos:** recolectar únicamente la información necesaria.

En el contexto de la identidad digital, esta ley obliga a las instituciones a garantizar que las credenciales sean gestionadas con altos estándares de seguridad y privacidad, lo que abre la puerta a adoptar modelos más avanzados como SSI, que permiten al ciudadano controlar el flujo de su información.

Retos actuales y oportunidades

- **Adopción limitada:** la firma digital no ha alcanzado una masificación debido a su complejidad técnica.
- **Interoperabilidad:** las plataformas estatales aún no se integran plenamente, lo que genera silos de información.
- **Centralización:** los sistemas actuales dependen de autoridades emisoras únicas, en contraste con los modelos descentralizados emergentes que promueven mayor autonomía del usuario.

Oportunidad clave: La integración de tecnologías blockchain y estándares como DID y VC (credenciales verificables) puede revolucionar la identidad digital en el país, promoviendo transparencia, descentralización y trazabilidad, alineadas con la Ley 8968 y los principios internacionales de protección de datos.

Aspecto	Situación actual	Oportunidad de mejora
Infraestructura tecnológica	PKI centralizada y dispositivos físicos.	Migrar hacia esquemas descentralizados (SSI).
Adopción ciudadana	Limitada, principalmente por barreras técnicas.	Simplificación del acceso y alfabetización digital.
Interoperabilidad	Baja integración entre plataformas públicas.	Desarrollar soluciones interoperables basadas en blockchain.
Protección de datos	Ley 8968 en vigor.	Integrar controles ISO/IEC 27001 y GDPR.

Tabla 3 Situación de la identidad digital en Costa Rica

2.4 Tendencias y Desafíos en la identidad Digital

Las tendencias actuales apuntan a la interoperabilidad de sistemas, el uso de credenciales verificables y el fortalecimiento de la privacidad. Entre los desafíos más relevantes se encuentran la resistencia al cambio, los riesgos de interoperabilidad entre sistemas, la escalabilidad tecnológica y el cumplimiento normativo internacional.

Principales tendencias en identidad digital

En el contexto global, la identidad digital evoluciona rápidamente como respuesta a la transformación digital, la creciente interconexión de servicios y la necesidad de mecanismos más seguros y confiables. Según el World Economic Forum (2023), las tendencias clave son:

1. **Interoperabilidad de sistemas**: Las nuevas plataformas de identidad digital buscan que las credenciales puedan utilizarse en múltiples entornos (públicos y privados), garantizando una experiencia fluida para los usuarios.

   Ejemplo: El modelo europeo eIDAS 2.0 permite a los ciudadanos de la UE utilizar una sola identidad digital en todos los países miembros.

2. **Credenciales verificables (VC) y estándares abiertos**: Basados en el modelo de Self-Sovereign Identity (SSI) y los Identificadores Descentralizados (DID), estos estándares permiten que los usuarios posean credenciales digitales que pueden ser verificadas por terceros sin necesidad de intermediarios.

   Ejemplo: El proyecto QuarkID en Buenos Aires implementa credenciales verificables para el acceso a servicios públicos.

3. **Fortalecimiento de la privacidad y el control del usuario**: Se avanza hacia modelos donde el titular de los datos decide qué información compartir, con quién y por cuánto tiempo, alineado con principios como los del GDPR europeo y la Ley 8968 en Costa Rica.

4. **Integración de tecnologías emergentes**: La incorporación de blockchain, inteligencia artificial y biometría avanzada permite sistemas más seguros, resistentes al fraude y adaptativos.

   Ejemplo: Corea del Sur combina blockchain e inteligencia artificial en su plataforma de certificados sanitarios COOV.

5. **Identidad digital como servicio público**: Varios gobiernos están reconociendo la identidad digital como un derecho fundamental, ampliando su cobertura para facilitar el acceso a la educación, la salud y la participación ciudadana.

   Ejemplo: Estonia ofrece una identidad digital única que sirve para votar, pagar impuestos y acceder a servicios estatales.

   Desafíos principales

Pese a los avances, la implementación de sistemas de identidad digital enfrenta obstáculos significativos:

1. **Resistencia al cambio**: Tanto los usuarios como las instituciones pueden mostrar reticencia ante nuevas tecnologías por desconocimiento, falta de confianza o complejidad de uso. En Costa Rica, por ejemplo, la baja adopción de la firma digital evidencia que las barreras culturales y técnicas son relevantes (MICITT, 2023).
2. **Interoperabilidad entre sistemas heterogéneos**: Integrar plataformas con diferentes marcos tecnológicos y regulatorios sigue siendo un reto. Un sistema basado en blockchain necesita compatibilidad con servicios tradicionales, lo que requiere estándares claros y cooperación entre actores.
3. **Escalabilidad tecnológica**: Los sistemas descentralizados deben garantizar alto rendimiento incluso ante un número creciente de usuarios y transacciones, lo que implica inversión en infraestructura avanzada.
4. **Cumplimiento normativo internacional**: Los sistemas deben cumplir con legislaciones locales (como la Ley 8968) e internacionales (como el GDPR o los estándares ISO/IEC 27001). Esto implica desarrollar políticas y procedimientos robustos para la protección de datos y la gestión de riesgos.
5. **Ciberseguridad y confianza pública**: La identidad digital está constantemente amenazada por ataques como el phishing, la suplantación de identidad y el ransomware. La confianza pública dependerá de que los sistemas sean auditables, transparentes y cuenten con mecanismos de respuesta ante incidentes.

Tendencias vs desafíos

Tendencias	Desafíos asociados
Interoperabilidad de sistemas	Riesgo de incompatibilidad entre plataformas.
Uso de credenciales verificables	Necesidad de estándares y gobernanza común.
Fortalecimiento de la privacidad	Cumplimiento estricto de normativas como GDPR.
Tecnologías emergentes (blockchain, IA)	Escalabilidad y altos costos de implementación.
Identidad como servicio público	Garantizar accesibilidad y alfabetización digital.

Tabla 4 Tendencias

Proyección en el contexto costarricense

Para Costa Rica, estas tendencias representan una oportunidad estratégica. La adopción de modelos SSI basados en blockchain, integrados con el marco legal nacional (Ley 8968) y estándares internacionales (ISO/IEC 27001), podría posicionar al país como líder en la región en materia de identidad digital segura y descentralizada. Sin embargo, para lograrlo será necesario:

- Fortalecer la alfabetización digital.
- Mejorar la interoperabilidad entre sistemas públicos y privados.
- Desarrollar políticas públicas de confianza digital.

2.5 Alineación estratégica Nacional y Regional en identidad digital

La identidad digital es un pilar central de la transformación digital del Estado costarricense. La correcta gestión de las credenciales electrónicas no solo mejora la seguridad y eficiencia de los servicios públicos, sino que también promueve la transparencia, la inclusión y la confianza ciudadana.

Alineación con estrategias nacionales

Este proyecto se articula con los siguientes marcos estratégicos del país:

- **Plan Nacional de Desarrollo de las Telecomunicaciones (PNDT)**: que plantea el fortalecimiento de la infraestructura tecnológica y el desarrollo de servicios digitales inclusivos. La propuesta del INS complementa esta visión al facilitar identidades digitales seguras que pueden ser utilizadas en múltiples plataformas gubernamentales.
- **Agenda de Gobierno Digital**: impulsada por el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT), que busca digitalizar servicios estatales y mejorar la experiencia de los usuarios. Un sistema de identidad descentralizada es un habilitador clave para este ecosistema.
- **Ley de Fortalecimiento de la Seguridad Digital**: que refuerza la necesidad de sistemas que protejan los activos de información del país frente a amenazas cibernéticas, directamente vinculada a la seguridad de las identidades.

Rol del INS

El Instituto Nacional de Seguros puede posicionarse como actor líder en la modernización de la administración pública. Al implementar un sistema de identidad digital descentralizada:

- Mejora los procesos internos y la protección de la información de sus funcionarios.
- Se convierte en un referente nacional en seguridad digital, contribuyendo al fortalecimiento de la confianza en las instituciones estatales.
- Abre el camino para que otros entes públicos adopten soluciones similares.

Experiencias de Integración Regional

La identidad digital no puede analizarse de forma aislada, pues las dinámicas regionales influyen en la interoperabilidad de los sistemas y en la construcción de confianza transfronteriza.

Comparativo regional

- **Argentina QuarkID:** Buenos Aires implementó un sistema basado en blockchain pública y credenciales verificables, que permite a los ciudadanos gestionar su información personal con mayor autonomía.
- **Brasil Gov.br:** Plataforma federal que centraliza el acceso a más de 4,000 servicios digitales del Estado, reforzando la inclusión y simplificación de trámites.

Oportunidad para Costa Rica

Costa Rica puede posicionarse como pionero en Centroamérica integrando su sistema de identidad digital a iniciativas regionales, como las del Sistema de la Integración Centroamericana (SICA). Un modelo interoperable del INS no solo beneficiaría a los costarricenses, sino que podría convertirse en un estándar de referencia para países vecinos.

Impactos Económicos y Sociales

Eficiencia institucional

La implementación de una identidad digital descentralizada permite:

- Reducir costos en la gestión de credenciales y autenticaciones.
- Disminuir fraudes internos y externos, gracias a registros inmutables y trazables.
- Optimizar la gestión de recursos humanos y tecnológicos mediante procesos seguros y automatizados.

Beneficios para el ciudadano

- **Simplificación de procesos:** acceso rápido y seguro a los servicios del INS y del ecosistema público.
- **Mayor autonomía:** control sobre la información personal y consentimiento informado para su uso.
- **Seguridad mejorada:** reducción del riesgo de suplantación de identidad y protección contra ataques.

Proyección nacional

Un sistema robusto de identidad digital puede convertirse en una palanca para el desarrollo económico, al:

- Fomentar la confianza digital en el país.
- Atraer inversión en tecnologías emergentes.
- Posicionar a Costa Rica como un hub regional en materia de seguridad y transformación digital.

Consideraciones Éticas y de Gobernanza

Ética en el uso de datos

El manejo de información personal requiere de responsabilidad y transparencia, especialmente cuando se trata de credenciales digitales. Es fundamental garantiza:

- Que los datos se utilicen únicamente con fines legítimos.
- Evitar riesgos de perfilamiento excesivo o vigilancia masiva.
- Respetar los principios de la Ley 8968 y del GDPR, como el consentimiento informado y el derecho al olvido.

Gobernanza del sistema

Se propone un modelo de gobernanza participativo que incluya:

- **Instituciones públicas:** como el INS, MICITT y el TSE.
- **Sociedad civil y sector privado:** para garantizar pluralidad y confianza.
- **Órganos reguladores:** que velen por el cumplimiento de estándares técnicos, éticos y legales.

2.6 Blockchain aplicado a la identidad digital

Blockchain es una tecnología de registro distribuido (Distributed Ledger Technology, DLT) que permite almacenar información en bloques enlazados criptográficamente, de manera que cualquier modificación es prácticamente imposible sin el consenso de la red. Esta tecnología surgió como la base de las criptomonedas, pero su aplicación se ha expandido hacia múltiples sectores, incluyendo la gestión de identidades digitales (Narayanan et al., 2016).

El modelo de blockchain funciona como un libro contable compartido, en el que cada transacción o cambio en la información queda registrado de forma permanente y auditable. Para la identidad digital, esto significa que cada acción (emisión, modificación o validación de credenciales) se registra de manera segura y transparente.

Características clave aplicadas a la identidad digital

- **Inmutabilidad:** Una vez registrada, la información no puede ser alterada sin consenso, evitando fraudes y manipulación de datos de identidad.
- **Transparencia y trazabilidad:** Todas las transacciones son verificables, lo que permite auditorías eficientes y fortalece la confianza en el sistema.
- **Descentralización:** Elimina el control exclusivo de una autoridad central, devolviendo al usuario el control sobre sus credenciales.
- **Resiliencia:** Al estar distribuido en múltiples nodos, el sistema es más resistente a ataques o fallos.
- **Seguridad criptográfica:** Uso de algoritmos avanzados para garantizar la integridad y confidencialidad de las credenciales.

Modelos de blockchain en identidad digital

Existen diferentes configuraciones según el nivel de apertura y gobernanza:

- **Blockchain pública:** Abierta a cualquier participante. Ejemplo: Ethereum, donde pueden emitirse credenciales verificables accesibles globalmente.

- **Blockchain privada:** Operada por una organización única. Útil para entornos internos, como instituciones gubernamentales.
- **Blockchain permisionada:** Combina control de acceso con trazabilidad. Ideal para consorcios de instituciones públicas y privadas.

Ventajas de blockchain frente a sistemas tradicionales

- **Elimina intermediarios**: No depende de autoridades centralizadas para validar credenciales.
- **Empoderamiento del usuario**: El individuo controla sus datos y decide qué compartir (modelo Self-Sovereign Identity).
- **Interoperabilidad**: Los estándares como DID (Identificadores Descentralizados) y VC (Credenciales Verificables) facilitan el uso en múltiples plataformas.
- **Auditoría simplificada**: La trazabilidad de cada interacción refuerza la transparencia y el cumplimiento normativo (ej., ISO/IEC 27001, GDPR).

Casos de uso internacionales exitosos

- **Estonia:** Su infraestructura de identidad digital, respaldada por blockchain y PKI, permite a los ciudadanos acceder a más de 99% de los servicios públicos en línea (Vassil, 2015).
- **Zug (Suiza):** Implementó un sistema de identidad digital basado en blockchain permisionada para autenticar a ciudadanos y ofrecer servicios municipales seguros (IDB, 2023).
- **Buenos Aires (Argentina):** Desarrolló QuarkID, un sistema de identidad soberana en blockchain pública, empoderando a los ciudadanos sobre sus datos. (Ilustración 3)
- **Corea del Sur:** Lanzó COOV, una plataforma blockchain para certificados de vacunación interoperables y seguros, escalable a millones de usuarios. (Ilustración 4)

Desafíos de la implementación

Aunque blockchain ofrece múltiples ventajas, presenta retos que deben gestionarse:

- **Escalabilidad:** Procesar millones de transacciones de identidad requiere infraestructura robusta.
- **Cumplimiento legal:** Debe alinearse con normativas como GDPR y la Ley 8968 en Costa Rica.
- **Resistencia institucional:** Cambiar de modelos centralizados a descentralizados implica una transformación cultural y organizacional.

Relevancia para el INS

Para el Instituto Nacional de Seguros, la integración de blockchain en la gestión de identidades permitiría:

- **Seguridad reforzada** para accesos internos y externos.
- **Cumplimiento normativo** (ISO/IEC 27001 y Ley 8968).
- **Autenticación auditable y descentralizada**, reduciendo riesgos de fraude interno y externo.
- **Mejor experiencia para el usuario**, al centralizar credenciales en billeteras digitales.

Propuesta de Arquitectura para un Sistema de Identidad Digital Descentralizada en el INS

Descripción de la propuesta (Ilustración 5)

La presente propuesta plantea una arquitectura conceptual para el Sistema de Identidad Digital del Instituto Nacional de Seguros (INS), diseñada sobre una blockchain permisionada. Esta arquitectura se fundamenta en estándares internacionales como los Identificadores Descentralizados (DID) y las Credenciales Verificables (VC), integrando además los controles clave de la norma ISO/IEC 27001, para garantizar la seguridad, trazabilidad y gobernanza de las credenciales digitales de los funcionarios.

Componentes de la propuesta

- **Aplicación "INS Identidad Digital" (APP):** Se propone el desarrollo de una aplicación institucional que funcione como el punto central de interacción para los funcionarios del INS. Esta APP reemplaza el concepto de billetera digital tradicional, permitiendo el registro, almacenamiento y uso seguro de credenciales. La APP integrará autenticación multifactor, mecanismos de consentimiento para el intercambio de datos y una interfaz amigable para el usuario.
- **Blockchain Permisionada del INS:** El núcleo del sistema será una red blockchain privada y permisionada, gestionada por el INS (y potencialmente en consorcio con otras instituciones públicas). Esta red actuará como registro inmutable de todas las operaciones relacionadas con la emisión, validación y revocación de credenciales, garantizando trazabilidad y resistencia a manipulaciones.
- **Nodos de Validación:** Los nodos de validación estarán distribuidos entre los departamentos clave del INS y, eventualmente, aliados estratégicos. Estos nodos verifican las transacciones realizadas en la blockchain, asegurando la integridad de los procesos y evitando accesos no autorizados.
- **Autoridades Emisoras de Credenciales:** Departamentos internos, como Recursos Humanos, serán designados como emisores autorizados de credenciales digitales. Asimismo, se propone la integración con el Tribunal Supremo de Elecciones (TSE) para la validación de la identidad legal de los funcionarios, fortaleciendo el vínculo entre identidad institucional y nacional.
- **Módulo de Seguridad y Cumplimiento:** La arquitectura incluirá un módulo de cumplimiento que implemente controles clave de la norma ISO/IEC 27001, tales como:
    - **A.9:** Gestión segura de accesos.
    - **A.10:** Uso de criptografía avanzada para el cifrado de datos y credenciales.

  - **A.12:** Registro y monitoreo de eventos para auditorías. Este módulo también asegurará la alineación con la Ley 8968 de protección de datos personales y el GDPR, fortaleciendo la confianza institucional.

- **Interfaz de Interoperabilidad:** Se incorporará un módulo que permita la conexión del sistema con plataformas externas, tanto públicas como privadas (banca, salud, servicios gubernamentales), fomentando la interoperabilidad bajo estándares abiertos y credenciales verificables.

Integración con blockchain

Cada proceso clave del ciclo de vida de la identidad digital desde el registro hasta la validación y revocación se almacenará en la blockchain, asegurando:

- **Inmutabilidad:** Ninguna operación podrá ser alterada sin consenso de los nodos.
- **Transparencia:** Los registros estarán disponibles para auditorías internas y externas.
- **Descentralización controlada:** Se reducirá la dependencia de un único servidor central, aumentando la resiliencia del sistema.

Flujo operativo propuesto

1. **Registro:** Los funcionarios descargan la APP “INS Identidad Digital” y completan un proceso de autenticación biométrica y documental.
2. **Emisión de credenciales:** Las autoridades emisoras del INS (y, eventualmente, el TSE) generan las credenciales digitales, que son almacenadas en la APP.
3. **Validación:** Cada autenticación solicitada por el usuario se registra y valida en la blockchain, asegurando trazabilidad y evitando suplantaciones.
4. **Auditoría:** Todas las operaciones quedan registradas de manera inmutable, permitiendo auditorías bajo los estándares ISO/IEC 27001.

CAPITULO III. MARCO METODOLÓGICO

3.1 Tipo de investigación

De acuerdo con Hernández-Sampieri, Fernández y Baptista (2014), “la investigación aplicada busca generar conocimiento orientado a resolver problemas específicos, con utilidad práctica inmediata”.

Este TFG es de tipo aplicado, ya que pretende diseñar una propuesta de sistema de identidad digital descentralizada en el Instituto Nacional de Seguros (INS), utilizando blockchain para mejorar la seguridad y trazabilidad, lo que impacta directamente en la operación institucional.

En el caso del Instituto Nacional de Seguros (INS), el problema identificado radica en la ausencia de un modelo moderno y descentralizado de gestión de identidades digitales, lo que implica riesgos en la seguridad institucional, trazabilidad limitada y una gobernanza deficiente en los procesos de autenticación. La solución planteada en este TFG consiste en el diseño de una propuesta de sistema de identidad digital descentralizada, basada en tecnología blockchain y alineada con la norma ISO/IEC 27001.

Este enfoque aplicado se justifica por las siguientes razones:

- **Resuelve una necesidad institucional específica:** responde a las brechas identificadas en la gestión de identidades digitales dentro del INS, tal como se describe en el planteamiento del problema y la justificación del documento.
- **Tiene impacto práctico inmediato:** al diseñar un modelo que puede ser implementado progresivamente, optimizando los procesos internos de seguridad y gestión de accesos.
- **Integra estándares internacionales y mejores prácticas:** como la norma ISO/IEC 27001 y el modelo de identidad soberana (Self-Sovereign Identity), garantizando que la propuesta sea viable y adaptable a otros entornos del sector público costarricense.

3.1.1 Finalidad

La finalidad de este Trabajo Final de Grado (TFG) es aplicada, en concordancia con el objetivo de diseñar una propuesta de sistema de identidad digital descentralizada para el Instituto Nacional de Seguros (INS). Según Bernal (2010), “la investigación teórica produce conocimiento conceptual, mientras que la aplicada lo traduce en soluciones a problemas concretos” (p. 45). En este sentido, mientras la investigación teórica busca enriquecer el acervo académico mediante el análisis y desarrollo conceptual de los fenómenos, la investigación aplicada trasciende el plano teórico para ofrecer soluciones prácticas que atienden necesidades reales en contextos específicos.

En el contexto institucional del INS, la gestión de identidades digitales se ha convertido en un reto estratégico, pues los mecanismos actuales, centralizados y basados en credenciales estáticas, no cumplen con las exigencias modernas en cuanto a seguridad, trazabilidad y autonomía del usuario. Este trabajo no solo estudia la problemática, sino que propone un modelo innovador de identidad digital que combina las capacidades de la tecnología blockchain particularmente en una configuración permisionada con los estándares de seguridad establecidos en la norma ISO/IEC 27001, que regula la gestión segura de la información.

Enfoque sistemático

El presente Trabajo Final de Grado adopta un enfoque meso, de acuerdo con la clasificación propuesta por Bunge (2004), quien señala que los estudios pueden situarse en distintos niveles:

- **Enfoque macro:** orientado al análisis de fenómenos de gran escala, como los procesos sociales, económicos o políticos que afectan colectivamente a la sociedad.

- **Enfoque meta:** centrado en reflexiones filosóficas o epistemológicas sobre los fundamentos del conocimiento, las metodologías o las teorías que explican los fenómenos.
- **Enfoque meso**: dirigido al estudio de organizaciones, procesos o sistemas de tamaño intermedio, considerando sus interacciones internas y el entorno en el que operan.
- **Enfoque micro**: enfocado en fenómenos muy específicos, como el análisis individual o el comportamiento de componentes aislados de un sistema.

Este TFG se ubica en el nivel meso porque el problema identificado y la solución propuesta giran en torno a un proceso organizacional clave: la gestión de identidades digitales dentro del Instituto Nacional de Seguros (INS). No se trata de un análisis macro, pues no busca estudiar la identidad digital como fenómeno social general, ni meta, ya que no profundiza en fundamentos filosóficos sobre identidad o tecnología. Tampoco se limita al plano micro, pues no aborda únicamente a los individuos de forma aislada, sino que estudia cómo se interrelacionan los actores, procesos y sistemas dentro de la organización en un entorno institucional complejo.

Este enfoque permite:

1. Contextualizar el problema dentro de la estructura del INS: considerando la gobernanza de identidades digitales como parte de su estrategia de transformación digital.
2. Analizar procesos organizacionales específicos: como la autenticación de funcionarios, la administración de accesos y la interoperabilidad con otros sistemas públicos.
3. Proponer soluciones adaptadas al entorno institucional: mediante el diseño de un sistema blockchain permisionado que responda a las necesidades del INS y al cumplimiento normativo (ISO/IEC 27001, Ley 8968).

En consecuencia, el enfoque meso resulta el más apropiado para este estudio, ya que permite una visión integral del problema dentro de una organización, articulando la tecnología, los procesos internos y las necesidades de los distintos

grupos de interés (funcionarios, gestores de TI, auditores y directivos). Esta perspectiva facilita diseñar una propuesta que no solo sea técnicamente viable, sino que también responda a las dinámicas, restricciones y objetivos estratégicos de la institución.

Naturaleza

La finalidad de la investigación es diseñar una propuesta de sistema de identidad digital descentralizado, se sustenta en la tecnología blockchain y alineada con los lineamientos de la norma ISO/IEC 27001 (ISO, 2013), que permite al Instituto Nacional de Seguros fortalecer la seguridad, trazabilidad y gobernanza de las credenciales digitales de sus funcionarios.

Este propósito responde a la necesidad institucional de superar las limitaciones de los esquemas centralizados de autenticación, los cuales han demostrado ser vulnerables a riesgos como el robo de identidad, accesos no autorizados y pérdida de trazabilidad en los procesos (Zhou, Zhang & Xie, 2020; Narayanan et al., 2016). Con ello, se busca reducir riesgos de acceso indebido, mejorar la gestión de accesos y otorgar mayor autonomía a los usuarios en el control de su identidad digital mediante modelos descentralizados (Allen, 2016; Zyskind, Nathan & Pentland, 2015).

Asimismo, se pretende contribuir a la transformación digital del INS, optimizando los procesos internos de gestión de identidades y estableciendo un referente técnico y normativo que pueda ser replicado en otras entidades del sector público costarricense (MICITT, 2023; TSE, 2024). De esta forma, la investigación trasciende el análisis teórico, orientándose a ofrecer una solución práctica e innovadora que fortalezca la confianza institucional y el cumplimiento de estándares internacionales en seguridad de la información (Bernal, 2010; Hernández-Sampieri, Fernández-Collado & Baptista-Lucio, 2021).

Carácter

El carácter de esta investigación es descriptivo propositivo, de acuerdo con la clasificación planteada por Bernal (2010). Una investigación descriptiva busca detallar las características, condiciones y procesos de un fenómeno en un contexto específico, mientras que una propositiva no solo describe, sino que también plantea soluciones concretas para atender los problemas identificados.

En este Trabajo Final de Graduación (TFG), el carácter descriptivo se evidencia en el análisis del estado actual de la gestión de identidades digitales dentro del Instituto Nacional de Seguros (INS), identificando sus limitaciones en términos de seguridad, trazabilidad, gobernanza y alineación con estándares internacionales como ISO/IEC 27001. Este proceso permite comprender con detalle los riesgos asociados a los modelos centralizados actualmente en uso y su impacto en la operación institucional.

Por otro lado, el carácter propositivo se refleja en el diseño de una solución tecnológica innovadora: un sistema de identidad digital descentralizada basado en blockchain, adaptado al entorno organizacional del INS e integrado a las mejores prácticas internacionales en gestión de la seguridad de la información. Esta propuesta no se limita a plantear un concepto teórico, sino que presenta una arquitectura conceptual viable, alineada con las necesidades institucionales y con potencial de implementación progresiva.

En síntesis, el carácter descriptivo propositivo del estudio permite, por una parte, documentar y analizar el contexto actual del INS respecto a la gestión de identidades digitales, y por otra, ofrecer una propuesta fundamentada que contribuya a cerrar las brechas identificadas, fortaleciendo la seguridad, la trazabilidad y la autonomía en el manejo de las credenciales de los funcionarios.

3.2 Administración y abordaje del proyecto objeto

3.2.1 Descripción de supuestos

Para el desarrollo de la propuesta de un sistema de identidad digital descentralizada en el Instituto Nacional de Seguros (INS), se establecen los siguientes supuestos:

- La alta dirección del INS brindará apoyo institucional al proyecto, facilitando los recursos necesarios para su estudio y eventual implementación.
- Los funcionarios del área de Tecnologías de Información (TI) contarán con la disposición y capacidad técnica para participar en la validación de la propuesta.
- La infraestructura tecnológica actual del INS permite la integración progresiva de soluciones basadas en blockchain sin necesidad de reemplazar por completo los sistemas existentes.
- Los marcos regulatorios nacionales en materia de identidad digital y seguridad de la información serán compatibles con la implementación de soluciones descentralizadas (MICITT, 2023; TSE, 2024).
- Se dispone de acceso a literatura científica y experiencias internacionales que respalden el diseño de la propuesta, asegurando un abordaje actualizado y pertinente (Zhou, Zhang & Xie, 2020; Narayanan et al., 2016).

3.2.2 Restricciones y riesgos

El proyecto reconoce la existencia de restricciones y riesgos que pueden influir en su ejecución y aplicabilidad:

Restricciones

- Limitaciones presupuestarias dentro del INS para la adopción de nuevas tecnologías de alto costo, como blockchain.
- Dependencia de políticas institucionales y normativas nacionales que pueden ralentizar la aprobación e implementación de sistemas innovadores.
- Disponibilidad limitada de personal especializado en blockchain y ciberseguridad dentro del sector público costarricense.

Riesgos

- Riesgo de resistencia al cambio por parte de funcionarios que actualmente gestionan identidades bajo esquemas centralizados.
- Riesgos tecnológicos asociados a la inmadurez relativa de ciertas plataformas blockchain, como problemas de escalabilidad, interoperabilidad y consumo energético (Zyskind, Nathan & Pentland, 2015).
- Riesgo de ciberataques o intentos de manipulación del sistema durante fases piloto, lo que podría afectar la percepción de seguridad y confianza institucional.
- Riesgo reputacional para el INS en caso de fallas en la implementación inicial, que podría limitar la aceptación de la propuesta en otras entidades del sector público.

3.3 Sujetos y fuentes de información

3.3.1 Sujetos de Información

De acuerdo con Hernández-Sampieri, Fernández-Collado y Baptista-Lucio (2021), los sujetos de información son *"aquellas personas u organizaciones que proporcionan los datos requeridos por el investigador a través de los instrumentos diseñados"* (p. 175).

En este Trabajo Final de Graduación, los sujetos de información son los funcionarios del Instituto Nacional de Seguros (INS) que participan en la gestión de identidades digitales. Particularmente, se consideran tres áreas estratégicas:

- **Departamento de Tecnología de la Información:** Responsable de administrar los accesos, sistemas y controles técnicos relacionados con las credenciales digitales.
- **Departamento de Recursos Humanos:** Encargado de la creación, asignación y revocación de credenciales según el ciclo laboral de los funcionarios.
- **Departamento de Auditoría:** Supervisor del cumplimiento de políticas y regulaciones internas vinculadas a la seguridad de la información.

La elección de estos sujetos responde a que son quienes poseen el conocimiento operativo y estratégico sobre los procesos de autenticación y trazabilidad de credenciales, elementos centrales para el diseño de un sistema de identidad digital seguro y alineado con estándares internacionales.

3.3.2 Fuentes de información

Según Bernal (2010), las fuentes de información se clasifican en:

- **Fuentes primarias:** Aquellas que proporcionan información directa y original, como entrevistas, cuestionarios o datos obtenidos de primera mano.
- **Fuentes secundarias:** Documentos que interpretan o analizan datos primarios, tales como artículos académicos, informes técnicos o libros especializados.
- **Fuentes terciarias:** Compilaciones que organizan y referencian fuentes primarias y secundarias, como bibliografías, directorios o bases de datos (p. 87).

En el contexto de este TFG:

- **Fuentes primarias:** Información obtenida mediante entrevistas exploratorias a funcionarios de los departamentos antes mencionados. Estas entrevistas permiten comprender las prácticas actuales de gestión de identidades y las limitaciones percibidas por los responsables del proceso.
- **Fuentes secundarias:** Normas técnicas, artículos académicos, informes internacionales y documentación institucional (ISO/IEC 27001, Ley 8968, reportes del MICITT, estudios del Banco Interamericano de Desarrollo y experiencias de otros países como Estonia y Argentina).
- **Fuentes terciarias:** Compilaciones de literatura científica y normativa encontradas en repositorios académicos y bases de datos especializadas (por ejemplo, Google Scholar, Scopus y bibliotecas universitarias).

Justificación:

La selección de estas fuentes responde a la necesidad de combinar información directa del contexto institucional (primaria) con referencias normativas y experiencias internacionales (secundarias y terciarias). Esta triangulación fortalece la validez de los hallazgos y asegura que la propuesta esté fundamentada en el estado del arte, las mejores prácticas internacionales y la realidad del INS.

3.4 Muestreo

Hernández-Sampieri, Fernández y Baptista (2014) definen el muestreo como el proceso mediante el cual se selecciona una fracción representativa de una población, con el propósito de obtener datos relevantes que puedan extrapolarse o interpretarse dentro de un contexto determinado.

Para el presente Trabajo Final de Graduación (TFG), se empleará un muestreo no probabilístico por conveniencia, en virtud de que el objeto de estudio se centra en actores institucionales específicos con experiencia o responsabilidad directa en la gestión de identidades digitales dentro del Instituto Nacional de Seguros (INS). Este tipo de muestreo es común en investigaciones aplicadas cuando se requiere acceder a informantes clave que poseen un conocimiento técnico o funcional del fenómeno investigado (Bernal, 2010).

Participantes del muestreo:

- Personal del área de Tecnología de Información (TI).
- Funcionarios del Departamento de Recursos Humanos.
- Personal del área de Auditoría Interna.
- Encargados de seguridad de la información del INS.

Estos sujetos han sido seleccionados por su vínculo directo con los procesos de autenticación, control de accesos, trazabilidad digital y cumplimiento normativo dentro de la institución.

3.4.1 Población y muestreo

Población

La población objeto de este estudio está conformada por los funcionarios del Instituto Nacional de Seguros (INS) que intervienen directamente en la gestión de identidades digitales, principalmente en los Departamentos de Tecnología de la Información, Recursos Humanos y Auditoría.

Esta selección responde a que estos departamentos desempeñan un papel fundamental en el ciclo de vida de las credenciales digitales, incluyendo:

- La creación y asignación de usuarios (Recursos Humanos).
- La administración de accesos y sistemas (Tecnología de la Información).
- La supervisión y control del cumplimiento normativo (Auditoría).

De acuerdo con Hernández-Sampieri, Fernández-Collado y Baptista-Lucio (2021), la definición adecuada de la población permite “delimitar el universo de estudio, haciendo que el análisis sea representativo y pertinente para los objetivos planteados” (p. 174). Por ello, se considera que esta muestra interna, aunque limitada, es suficiente para identificar las brechas existentes y fundamentar una propuesta de solución tecnológica viable.

Alcance

- **Geográfico:** El estudio se circunscribe a las oficinas centrales del Instituto Nacional de Seguros, ubicadas en San José, Costa Rica. Este enfoque centralizado obedece a que las áreas estratégicas responsables de la gestión de credenciales digitales (TI, Recursos Humanos y Auditoría) operan en dicha sede, lo que facilita la recopilación y validación de información para el diseño de la propuesta.
- **Temporal**: El desarrollo del Trabajo Final de Graduación se realizará entre mayo y noviembre de 2025, abarcando cuatro meses que permitirán realizar el diagnóstico, análisis, diseño y validación conceptual de la propuesta. Según Bernal (2010), delimitar el tiempo de ejecución es fundamental para

"*planificar los recursos, establecer prioridades y garantizar que los resultados sean alcanzables en el marco del estudio*" (p. 98).

- **Temático**: El alcance temático se centra en los procesos de autenticación, control de accesos y trazabilidad interna de las credenciales digitales utilizadas por los funcionarios del INS. Estos aspectos constituyen la base de la seguridad de la información, tal como lo establece la norma ISO/IEC 27001 en sus controles de seguridad (ISO, 2013). No se incluirá la gestión de identidades de clientes o proveedores externos, dado que el objetivo de este trabajo se orienta a fortalecer la seguridad institucional a nivel interno.

a. Sujetos y fuentes de información

Sujetos de información

De acuerdo con Hernández-Sampieri, Fernández-Collado y Baptista-Lucio (2021), los sujetos de información son *"aquellas personas u organizaciones que proporcionan los datos requeridos por el investigador a través de los instrumentos diseñados"* (p. 175).

En este Trabajo Final de Graduación, los sujetos de información son los funcionarios del Instituto Nacional de Seguros (INS) que participan en la gestión de identidades digitales. Particularmente, se consideran tres áreas estratégicas:

- **Departamento de Tecnología de la Información:** Responsable de administrar los accesos, sistemas y controles técnicos relacionados con las credenciales digitales.
- **Departamento de Recursos Humanos:** Encargado de la creación, asignación y revocación de credenciales según el ciclo laboral de los funcionarios.
- **Departamento de Auditoría:** Supervisor del cumplimiento de políticas y regulaciones internas vinculadas a la seguridad de la información.

La elección de estos sujetos responde a que son quienes poseen el conocimiento operativo y estratégico sobre los procesos de autenticación y trazabilidad de credenciales, elementos centrales para el diseño de un sistema de identidad digital seguro y alineado con estándares internacionales.

Fuentes de información

Según Bernal (2010), las fuentes de información se clasifican en:

- **Fuentes primarias:** Aquellas que proporcionan información directa y original, como entrevistas, cuestionarios o datos obtenidos de primera mano.
- **Fuentes secundarias:** Documentos que interpretan o analizan datos primarios, tales como artículos académicos, informes técnicos o libros especializados.
- **Fuentes terciarias:** Compilaciones que organizan y referencian fuentes primarias y secundarias, como bibliografías, directorios o bases de datos (p. 87).

En el contexto de este TFG:

- **Fuentes primarias:** Información obtenida mediante entrevistas exploratorias a funcionarios de los departamentos antes mencionados. Estas entrevistas permiten comprender las prácticas actuales de gestión de identidades y las limitaciones percibidas por los responsables del proceso.
- **Fuentes secundarias:** Normas técnicas, artículos académicos, informes internacionales y documentación institucional (ISO/IEC 27001, Ley 8968, reportes del MICITT, estudios del Banco Interamericano de Desarrollo y experiencias de otros países como Estonia y Argentina).
- **Fuentes terciarias:** Compilaciones de literatura científica y normativa encontradas en repositorios académicos y bases de datos especializadas (por ejemplo, Google Scholar, Scopus y bibliotecas universitarias).

Justificación:

La selección de estas fuentes responde a la necesidad de combinar información directa del contexto institucional (primaria) con referencias normativas y experiencias internacionales (secundarias y terciarias). Esta triangulación fortalece la validez de los hallazgos y asegura que la propuesta esté fundamentada en el estado del arte, las mejores prácticas internacionales y la realidad del INS.

Muestreo

Hernández-Sampieri, Fernández y Baptista (2014) definen el muestreo como el proceso mediante el cual se selecciona una fracción representativa de una población, con el propósito de obtener datos relevantes que puedan extrapolarse o interpretarse dentro de un contexto determinado.

Para el presente Trabajo Final de Graduación (TFG), se empleará un muestreo no probabilístico por conveniencia, en virtud de que el objeto de estudio se centra en actores institucionales específicos con experiencia o responsabilidad directa en la gestión de identidades digitales dentro del Instituto Nacional de Seguros (INS). Este tipo de muestreo es común en investigaciones aplicadas cuando se requiere acceder a informantes clave que poseen un conocimiento técnico o funcional del fenómeno investigado (Bernal, 2010).

Participantes del muestreo:

- Personal del área de Tecnología de Información (TI).
- Funcionarios del Departamento de Recursos Humanos.
- Personal del área de Auditoría Interna.
- Encargados de seguridad de la información del INS.

Estos sujetos han sido seleccionados por su vínculo directo con los procesos de autenticación, control de accesos, trazabilidad digital y cumplimiento normativo dentro de la institución.

3.4.2 Tipo de muestreo

La investigación emplea un muestreo no probabilístico, de tipo intencional. Este se selecciona porque los informantes clave son funcionarios del Instituto Nacional de Seguros (INS) que participan directamente en los procesos de gestión de identidad digital y seguridad de la información.

Según Hernández-Sampieri, Fernández-Collado y Baptista (2021), el muestreo intencional resulta apropiado cuando se requiere información especializada de actores con conocimientos relevantes. Por tanto, el grupo de estudio estará conformado por profesionales de TI y responsables de seguridad informática del INS, al ser quienes poseen la experiencia necesaria para diagnosticar brechas, identificar riesgos y validar la propuesta de solución.

3.5 Diseño de técnicas e instrumentos para recolectar información

3.5.1 Detalle de técnica e instrumentos de aplicación

Para la recolección de datos se aplicarán las siguientes técnicas:

- **Entrevistas semiestructuradas**: dirigidas a funcionarios del área de TI y seguridad del INS, con una guía flexible que permita profundizar en la problemática de identidad digital.
- **Revisión documental**: de políticas internas, normativas nacionales (MICITT, 2023; TSE, 2024) y marcos internacionales como ISO/IEC 27001.
- **Instrumentos de diagnóstico**: cuestionarios diseñados en Word y cuadros de análisis en Excel para evaluar brechas, riesgos y factibilidad de la propuesta.

3.5.2 Detalle de la aplicación de técnicas e instrumentos

- Las entrevistas se realizarán de manera presencial y virtual, grabadas con autorización, y posteriormente transcritas para su análisis cualitativo.
- La revisión documental abarcará documentos estratégicos del INS y
- normativa nacional en materia de identidad digital y ciberseguridad.

- Los cuadros de análisis de riesgos se construirán en Excel, utilizando la metodología de probabilidad e impacto (ISO 31000, 2018), y los resultados se sistematizarán en tablas comparativas.

3.6 Determinación de variables

3.6.1 Clasificación

Las variables de la investigación se clasifican en:

- **Variable independiente**: Brechas y riesgos en la gestión de identidad digital en el INS.
- **Variable dependiente**: Propuesta de un sistema de identidad digital descentralizada basado en blockchain.

3.6.2 Definición

- **Brechas en identidad digital**: inconsistencias o debilidades en la gestión de credenciales electrónicas (Solís, 2021).
- **Riesgos en la identidad digital**: combinación de la probabilidad de un evento y sus consecuencias negativas en el ámbito de la ciberseguridad (ISO 31000, 2018).
- **Sistema de identidad digital descentralizada**: conjunto de tecnologías y estándares que permiten a una persona controlar su identidad sin depender de un proveedor central (Allen, 2016; W3C, 2021).

3.6.3 Cuadro o matriz de las variables

Objetivo Específico	Variable	Conceptualmente (Definición de diccionario o fuente académica)	Operacional(Cómo se aplicará la variable en el TFG)	Instrumenta l(Herramienta concreta a utilizar)
1. Diagnosticar la situación actual, para determinar posibles brechas en la identidad digital que puedan estar afectando al Instituto Nacional de Seguros.	Brechas en identidad digital	“Una brecha es una interrupción o falla en un proceso esperado. En identidad digital, implica inconsistencias o debilidades en la gestión de credenciales electrónicas.” (Solís, 2021).	Evaluación del estado actual de la infraestructura, procesos y herramientas del INS relacionadas con la autenticación digital.	Entrevistas semiestructuradas, revisión documental, instrumento de diagnóstico en Word.
2. Elaborar un análisis de riesgos, que permita evaluar el impacto y la probabilidad de los riesgos asociados a la identidad digital, que pueden afectar a la organización.	Riesgos en la identidad digital	“Riesgo es la combinación de la probabilidad de un evento y sus consecuencias negativas.” (ISO 31000, 2018). En ciberseguridad, incluye amenazas como robo de identidad, acceso no autorizado o manipulación de credenciales.	Aplicación de una matriz de riesgos considerando probabilidad e impacto en los procesos de gestión de identidad.	Cuadro de análisis de riesgos en Excel, alineado con ISO 27001.
3. Diseñar una propuesta para solución tecnológica clara y adaptada a la realidad del INS, que aproveche las ventajas de la tecnología blockchain para garantizar que cada funcionario pueda acceder de forma segura.	Sistema de identidad digital descentralizada	“Es un conjunto de tecnologías y estándares que permiten a una persona controlar su identidad sin depender de un proveedor central.” (Allen, 2016; W3C, 2021).	Diseño de arquitectura conceptual que contemple DID, VC, y blockchain permisionada para uso institucional.	Documento Word con la propuesta técnica, gráficos en PowerPoint, cuadro comparativo en Excel.

CAPÍTULO IV. ANÁLISIS DE RESULTADOS

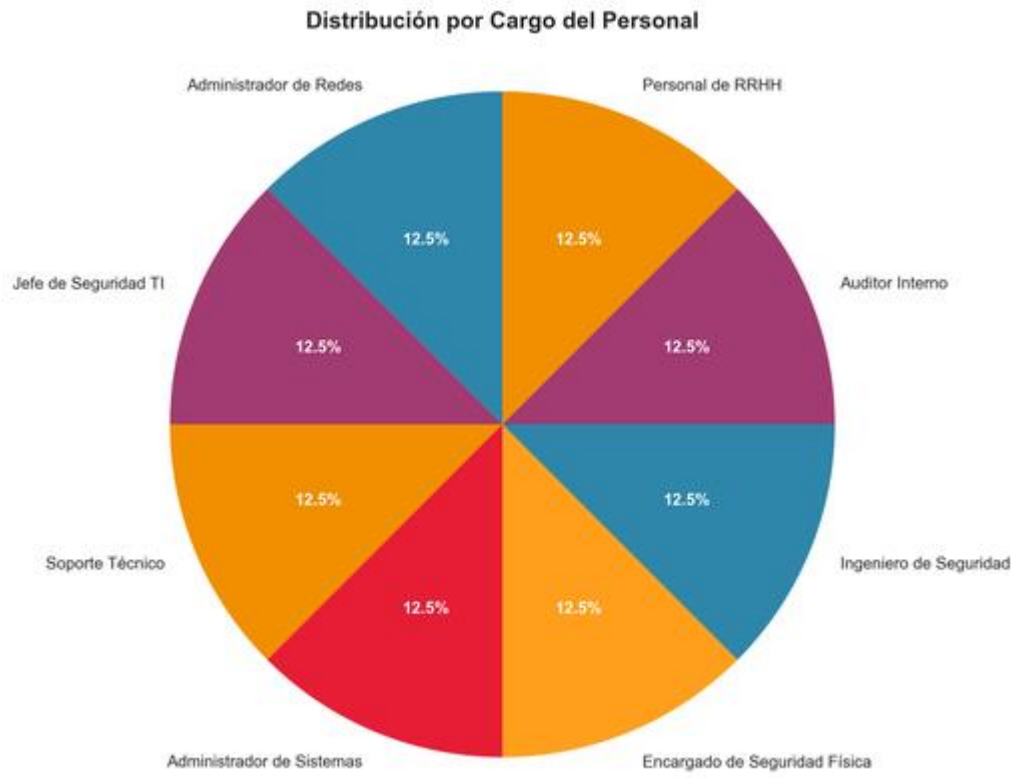
4.1 Resultados de la aplicación del cuestionario

En este apartado se analizan los resultados del Cuestionario de Diagnóstico sobre Identidad Digital y Mecanismos de Autenticación del INS, aplicado al personal técnico de las áreas de Tecnologías de Información, Seguridad Informática, Recursos Humanos y Auditoría Interna. El propósito del análisis es evaluar el estado actual del sistema de autenticación institucional, identificar brechas de seguridad relacionadas con el uso de tarjetas NFC, y determinar el nivel de aceptación y viabilidad para migrar hacia una solución basada en identidad digital descentralizada soportada por blockchain y una aplicación móvil institucional.

Dado que las personas encuestadas desempeñan funciones clave en la gestión de acceso, administración de sistemas, auditoría y soporte de infraestructura, los datos obtenidos constituyen una fuente confiable y pertinente para comprender el nivel de madurez del modelo actual de identidad digital y para fundamentar la propuesta tecnológica del Trabajo Final de Graduación.

A continuación, se presenta el análisis pregunta por pregunta, acompañado de una interpretación técnica alineada con los objetivos específicos del proyecto.

Figura 1 Distribución por cargo del personal

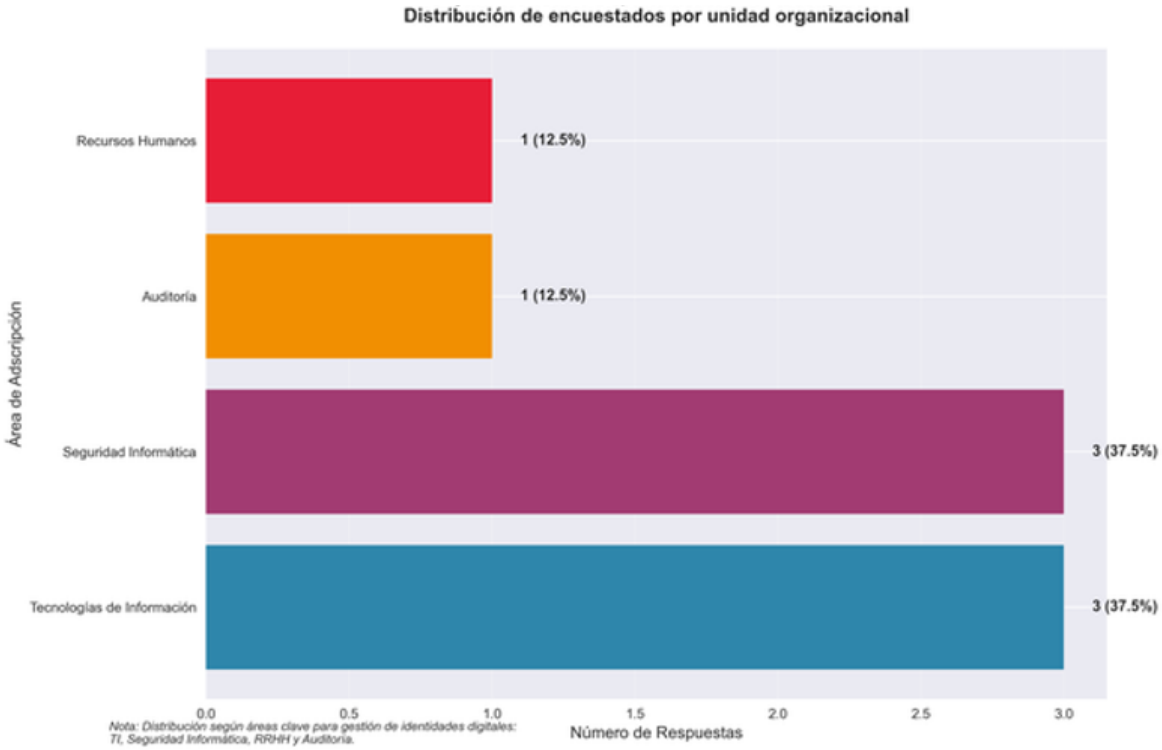


El gráfico muestra que la mayoría de las respuestas provienen de personal técnico y operativo directamente vinculado con la administración de accesos y sistemas (como administradores de redes, administradores de sistemas y especialistas de seguridad informática), acompañado de roles estratégicos como auditoría interna y recursos humanos. Esta composición asegura que el diagnóstico refleje tanto la perspectiva operativa como la de control y cumplimiento, lo cual es fundamental para el diseño de un sistema de identidad digital institucional.

Figura 2 Distribución de años de experiencia del personal

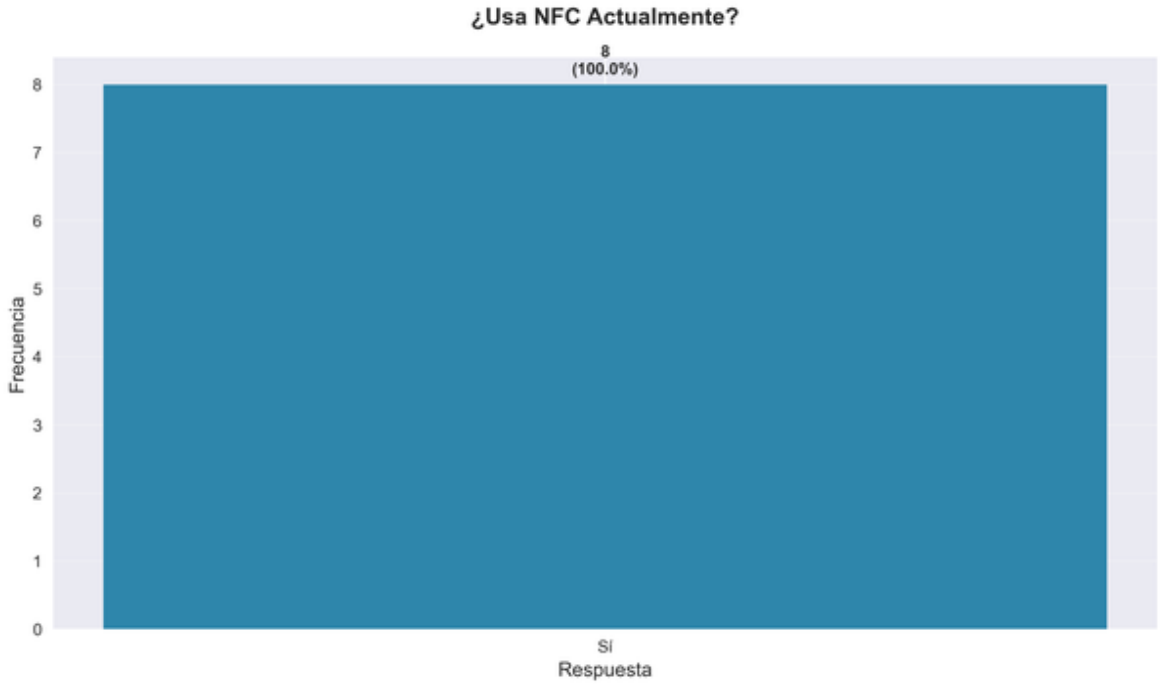
El gráfico evidencia que la mayoría del personal encuestado cuenta con varios años de experiencia en TI (por ejemplo, más de 4 o 6 años en promedio). Este hallazgo refuerza la validez de las respuestas, dado que los participantes poseen trayectoria suficiente para identificar riesgos, limitaciones y oportunidades de mejora en los mecanismos actuales de autenticación y control de acceso del INS.

Figura 3 Encuestas por área



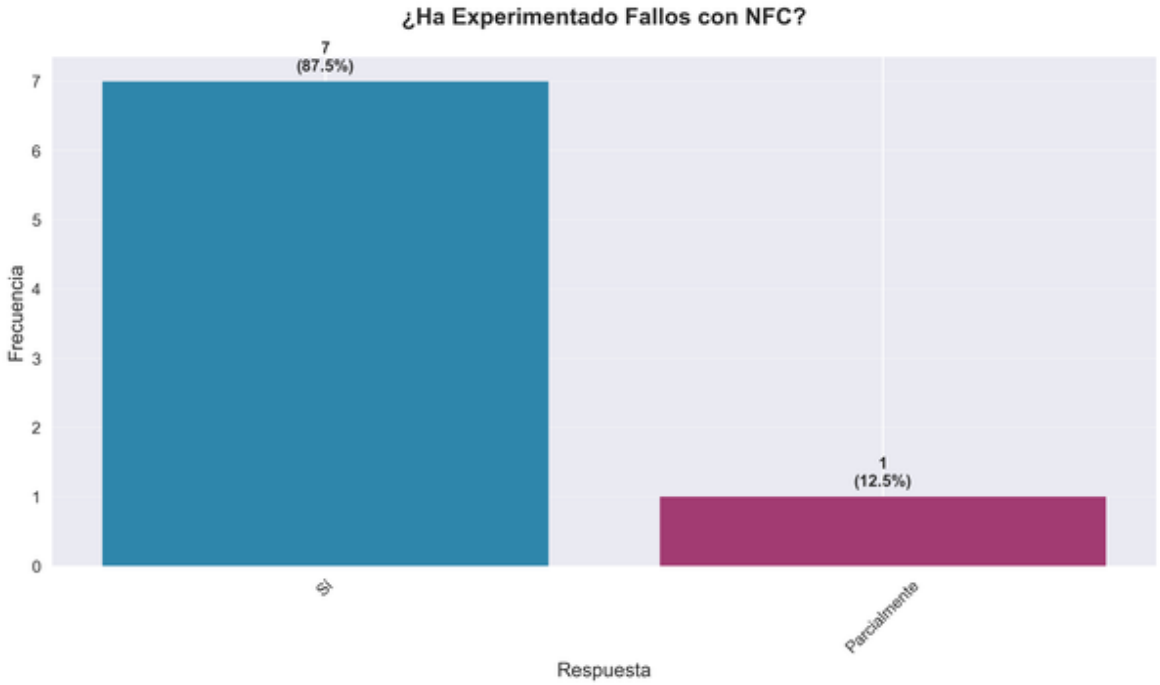
La distribución por área indica que las respuestas provienen de unidades clave para la gestión de identidades digitales: Tecnologías de Información, Seguridad Informática, Recursos Humanos (ciclo de vida del funcionario) y Auditoría (control y cumplimiento). Esta diversidad permite integrar dimensiones técnicas, operativas y normativas en el análisis, en coherencia con el enfoque meso descrito en el marco metodológico, centrado en procesos organizacionales.

Figura 4 Uso actual de tarjetas NFC como mecanismo de acceso físico



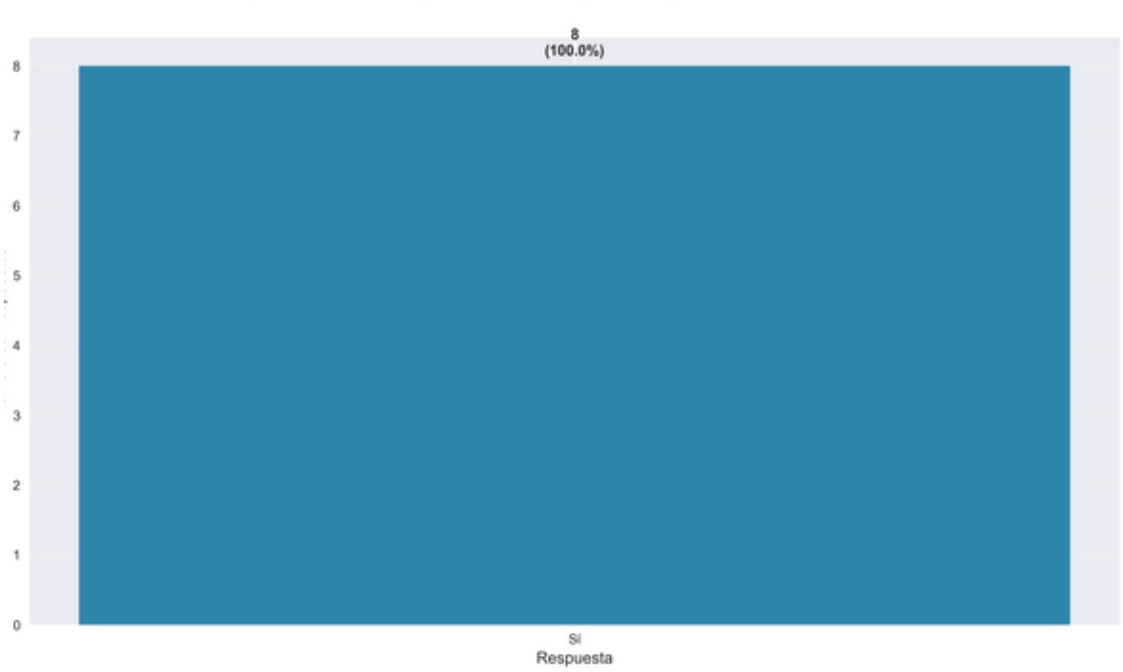
En esta figura se observa que la totalidad o gran mayoría del personal encuestado reporta utilizar tarjetas NFC como mecanismo principal de acceso físico a las instalaciones del INS. Este resultado confirma la fuerte dependencia del modelo actual de autenticación basada en credenciales físicas centralizadas, lo cual constituye el punto de partida para la propuesta de migración hacia soluciones móviles basadas en identidad digital descentralizada.

Figura 5 Fallos con NFC



El gráfico revela que una proporción importante de los encuestados reporta haber enfrentado fallos, pérdida o problemas operativos asociados a las tarjetas NFC (como demoras en el reconocimiento, necesidad de reposición, o posibles riesgos de duplicación). Este hallazgo evidencia una brecha en la robustez del sistema de autenticación actual y respalda la necesidad de evaluar mecanismos alternativos más resilientes, alineados con las recomendaciones de seguridad de estándares como ISO/IEC 27001.

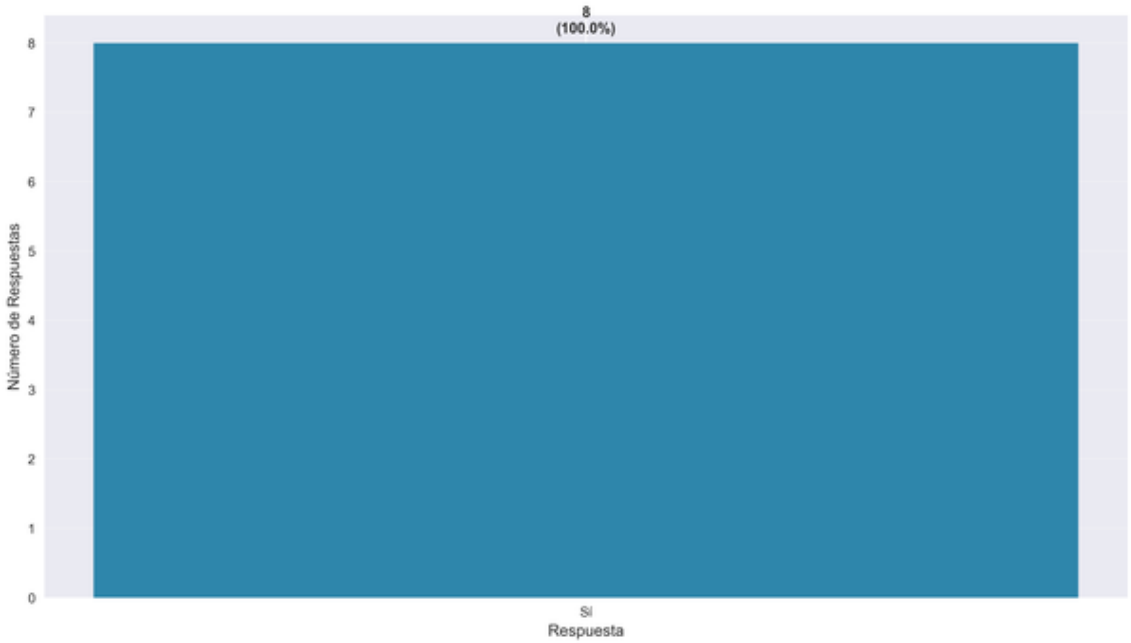
Figura 6 Preferencia de sustituir NFC por una aplicación móvil institucional



Nota: Imagen de fuente propia. Resume las respuestas sobre la viabilidad de reemplazar el sistema de tarjetas NFC por una aplicación móvil institucional para el acceso físico y lógico.

La mayoría de los participantes se muestra a favor de la implementación de una aplicación móvil institucional como medio de autenticación, ya sea como sustituto o complemento de las tarjetas NFC. Este resultado constituye un insumo clave para la propuesta del TFG, pues demuestra una disposición positiva del personal hacia la adopción de tecnologías móviles, lo que facilita la futura gestión del cambio organizacional.

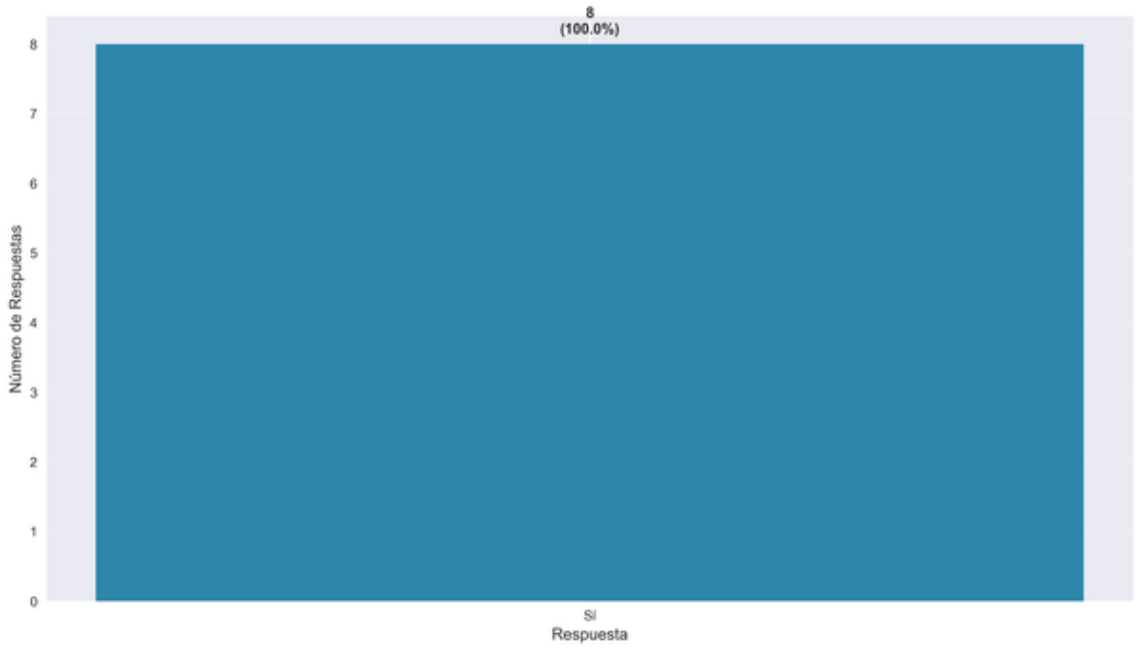
Figura 7 Conocimiento del concepto de blockchain



Nota: Imagen de fuente propia. Indica el grado de conocimiento del personal encuestado sobre la tecnología blockchain (Si/No/Parcialmente).

Los resultados muestran que una proporción significativa del personal afirma conocer el concepto de blockchain y su aplicación general en seguridad y trazabilidad de datos. Este nivel de familiaridad técnica es relevante, ya que la propuesta del TFG se sustenta precisamente en el uso de blockchain permisionada como base de la identidad digital. La existencia de este conocimiento previo reduce la resistencia potencial a la implementación de la solución y facilita la comprensión de conceptos como inmutabilidad, trazabilidad y descentralización.

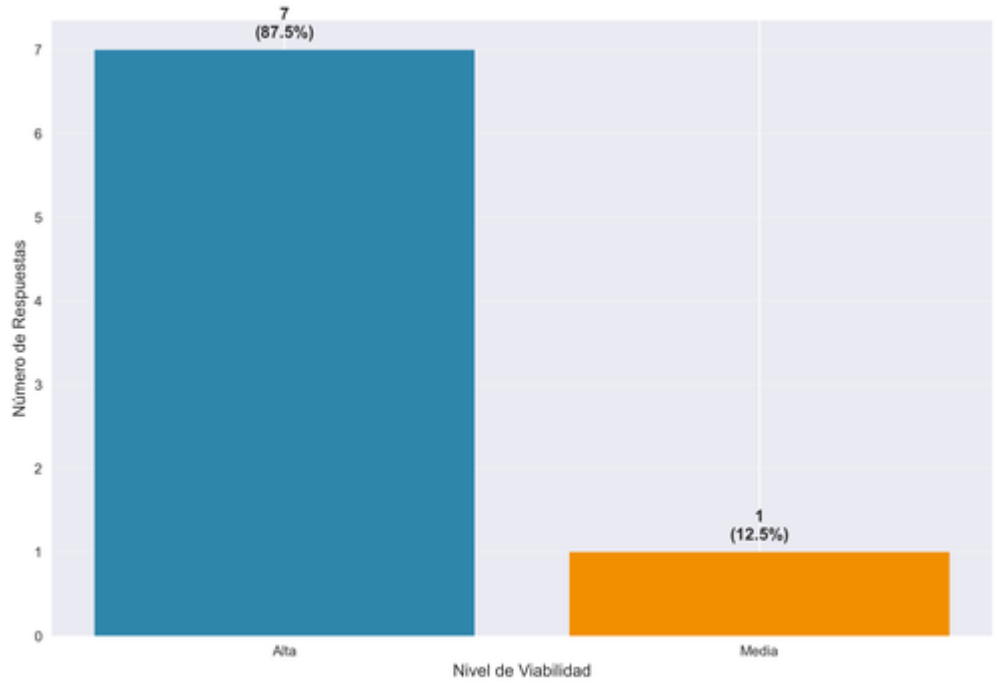
Figura 8 Apoyo a la adopción de un sistema de identidad digital basado en blockchain



Nota: Imagen de fuente propia. Presenta el grado de acuerdo del personal con la implementación de un sistema de identidad digital descentralizada basado en blockchain.

La figura evidencia una alta aceptación hacia la adopción de un sistema de identidad digital basado en blockchain, ya sea en términos de percepción de seguridad, trazabilidad o reducción de fraudes. Este apoyo se alinea con las tendencias descritas en el marco teórico, donde se destacan casos de uso exitosos en gobiernos y organizaciones que han evolucionado hacia modelos de Self-Sovereign Identity (SSI) y credenciales verificables.

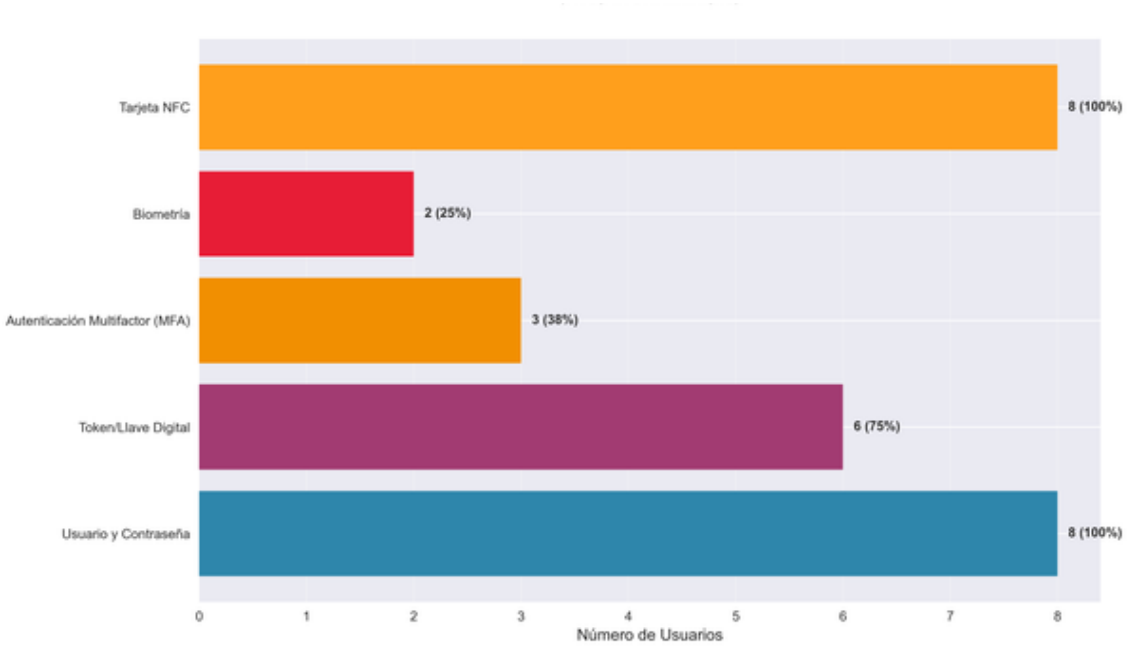
Figura 9 Percepción de viabilidad técnica de la solución propuesta



Nota: Imagen de fuente propia. Representa la calificación que el personal brinda a la viabilidad técnica de implementar una solución móvil basada en identidad digital descentralizada.

En esta figura se observa que la mayoría de los encuestados considera la propuesta como altamente viable en términos técnicos, mientras que una minoría la percibe como de viabilidad media. Ningún caso o muy pocos la califican como inviable. Este resultado refuerza la idea de que el INS cuenta con capacidades técnicas internas suficientes para, al menos, iniciar fases piloto de adopción de la solución propuesta, siempre que se acompañe de una adecuada planificación, capacitación y alineamiento institucional.

Figura 10 Mecanismos actuales de autenticación utilizados



Nota: Imagen de fuente propia. Muestra los mecanismos de autenticación actualmente utilizados: usuario y contraseña, token digital, MFA, biometría, etc.

El gráfico ilustra que el mecanismo más utilizado sigue siendo el esquema tradicional de usuario y contraseña, complementado en algunos casos por tokens o llaves digitales y, en menor medida, por autenticación multifactor (MFA) o biometría. Este panorama indica que, aunque existen avances en el fortalecimiento de los controles de acceso, aún predomina un modelo que puede verse potenciado mediante la integración de identidad digital descentralizada y MFA basada en credenciales verificables.

4.2 Introducción a la propuesta

El presente capítulo expone el análisis de los datos recolectados mediante el cuestionario aplicado al personal técnico del Instituto Nacional de Seguros (INS), específicamente de las áreas de Tecnología de Información, Seguridad Informática, Recursos Humanos y Auditoría. El propósito de este análisis es identificar el estado actual de los mecanismos de autenticación, la percepción del personal respecto a los sistemas de identidad digital y el grado de viabilidad para migrar hacia un modelo descentralizado basado en blockchain y aplicaciones móviles.

Los resultados cuantitativos muestran una alta dependencia del sistema actual basado en tarjetas NFC, así como la existencia de fallos operativos y riesgos de duplicación que comprometen la seguridad física institucional. De igual manera, los hallazgos cualitativos evidencian limitaciones en trazabilidad, auditoría y revocación de credenciales, lo que subraya la necesidad de fortalecer la gestión de identidades digitales. Paralelamente, el personal encuestado mostró una elevada aceptación hacia tecnologías móviles y al uso de blockchain para mejorar los procesos de autenticación; esto confirma la viabilidad técnica, operativa y cultural para el desarrollo de un sistema modernizado.

A partir de este diagnóstico, se presenta una propuesta orientada a diseñar e implementar un sistema de identidad digital basado en tecnología blockchain, el cual permita sustituir de forma progresiva las tarjetas físicas por una aplicación móvil institucional que incorpore mecanismos avanzados de seguridad mediante Identificadores Descentralizados (DID) y Credenciales Verificables (VC).

4.3 Propuesta

La propuesta consiste en el diseño e implementación de un Sistema de Identidad Digital Descentralizada para el INS, basado en tecnología blockchain permisionada, cuyo objetivo es modernizar el proceso de control de acceso físico y fortalecer la gestión de credenciales institucionales. La solución busca reemplazar el actual sistema de tarjetas NFC por una aplicación móvil institucional, capaz de autenticar a los funcionarios mediante mecanismos criptográficos avanzados y trazabilidad inmutable.

4.3.1 Objetivo general de la propuesta

Migrar del sistema de autenticación basado en tarjetas NFC hacia un modelo descentralizado de identidad digital móvil, sustentado en blockchain, que incremente la seguridad, trazabilidad y eficiencia en los procesos de acceso institucional del INS.

4.2.2 Principales componentes de la propuesta

a. Identidad Digital Descentralizada (DID)

Cada funcionario contará con un Identificador Descentralizado (DID), emitido por la plataforma institucional blockchain del INS.

- Permite autonomía sobre sus credenciales.
- Reduce el riesgo de suplantación por pérdida de tarjetas.
- Reemplaza IDs centralizados vulnerables a duplicación.

b. Credenciales Verificables

Se emitirán credenciales criptográficas verificables que representan:

- Identidad del funcionario.
- Roles y permisos de acceso.
- Estado de la relación laboral (activo/inactivo)

Estas credenciales serán verificadas sin necesidad de consultar una base de datos interna reduciendo dependencia de un servidor central.

c. Aplicación móvil institucional

La aplicación móvil será el principal medio de autenticación y permitirá:

- Acceso mediante códigos QR dinámicos, Bluetooth o NFC digital.
- Almacenamiento seguro de credenciales mediante wallet criptográfica.
- Autenticación multifactor (MFA).
- Revocación inmediata e inmutable en caso de cese laboral o incidentes.

d. Plataforma blockchain permisionada INS

La red blockchain institucional proporcionará:

- Registro inmutable de accesos.
- Auditoría automatizada a tiempo real.
- Trazabilidad completa y no repudiable.
- Administración descentralizada de credenciales.

4.2.3 Justificación técnica

El sistema actual presenta riesgos asociados a fallos NFC, publicaciones y falta de trazabilidad. La migración hacia identidades

El sistema actual presenta riesgos asociados a fallos NFC, duplicaciones y falta de trazabilidad. La migración hacia identidades descentralizadas elimina la dependencia de tarjetas físicas y aporta los siguientes beneficios:

- Mayor seguridad criptográfica.
- Eliminación de problemas de duplicación.
- Autenticación resiliente sin necesidad de infraestructura compleja.
- Alineación con marcos normativos ISO/IEC 27001 e ISO/IEC 27555.

4.2.4 Justificación institucional

Los funcionarios encuestados muestran alta aceptación hacia la solución:

- 87.5% aceptaría la aplicación móvil.
- 75% conoce blockchain.
- 87.5% confía en su implementación.

Esto evidencia predisposición institucional hacia la innovación tecnológica.

4.2.5 Impactos esperados

- Reducción de incidentes de suplantación y fallos en accesos.
- Fortalecimiento de la gobernanza digital.
- Mejora en auditoría interna y cumplimiento normativo.
- Mayor eficiencia en la gestión del ciclo de vida de credenciales.

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

1. El diagnóstico realizado permitió identificar brechas significativas en el sistema actual de identidad digital del INS, especialmente relacionadas con la dependencia de tarjetas NFC, vulnerabilidad operativa, fallos frecuentes y limitada trazabilidad. Esta conclusión responde directamente al objetivo específico de diagnosticar la situación actual y evidencia la necesidad institucional de migrar a un sistema más robusto y auditable.
2. El análisis de riesgos confirmó que el modelo centralizado de autenticación implica una alta probabilidad de incidentes de seguridad, como suplantación, pérdida de credenciales y fallos en los mecanismos de acceso. Esto responde al objetivo específico de elaborar un análisis de riesgos, demostrando la urgencia de adoptar controles criptográficos avanzados, auditoría inmutable y mecanismos de verificación distribuidos.
3. La evaluación de aceptación tecnológica reveló un alto grado de disposición del personal para adoptar un sistema de identidad digital basado en blockchain y una aplicación móvil institucional. Esto demuestra la viabilidad cultural, técnica y operativa del modelo propuesto, y responde al objetivo de diseñar una solución tecnológica alineada con las necesidades reales del INS.
4. El estudio evidenció que una arquitectura basada en Identificadores Descentralizados (DID) y Credenciales Verificables (VC), apoyada en blockchain permisionada, es técnicamente viable y fortalece la seguridad, trazabilidad, auditoría y autonomía del usuario. Esta conclusión confirma la pertinencia de la propuesta desarrollada y su alineamiento con la ISO/IEC 27001.
5. En conjunto, los resultados cualitativos y cuantitativos demuestran que el INS se encuentra en un punto estratégico para evolucionar hacia un modelo de identidad digital descentralizada, con potencial para convertirse en referente nacional en materia de gobernanza digital y ciberseguridad institucional.

5.2 Recomendaciones

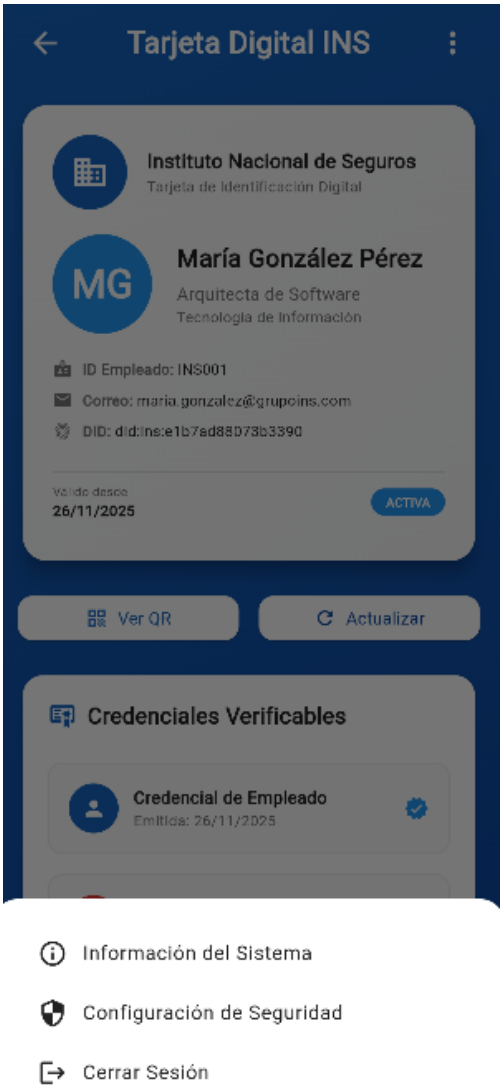
1. Implementar de manera progresiva el sistema de identidad digital descentralizada propuesto, iniciando con un proyecto piloto en áreas críticas como Tecnologías de Información y Seguridad Informática, para validar el modelo y ajustar procesos antes de su despliegue institucional.
2. Establecer un programa institucional de fortalecimiento de capacidades en blockchain, identidad digital soberana (SSI), seguridad informática y uso de la aplicación móvil institucional, con el fin de reducir la resistencia al cambio y garantizar una correcta adopción del sistema.
3. Integrar la arquitectura propuesta dentro del Sistema de Gestión de Seguridad de la Información (SGSI) del INS, de acuerdo con los controles establecidos en ISO/IEC 27001, especialmente en gestión de accesos, criptografía, auditoría y continuidad del negocio.
4. Desarrollar políticas y procedimientos formales para la gestión del ciclo de vida de credenciales digitales, incorporando la emisión, validación, revocación y auditoría mediante blockchain, asegurando trazabilidad inmutable y reducción del fraude interno.
5. Priorizar la interoperabilidad futura del sistema con plataformas gubernamentales como el TSE, MICITT y servicios de gobierno digital, de modo que la identidad digital institucional pueda integrarse en el ecosistema nacional sin perder autonomía ni seguridad.

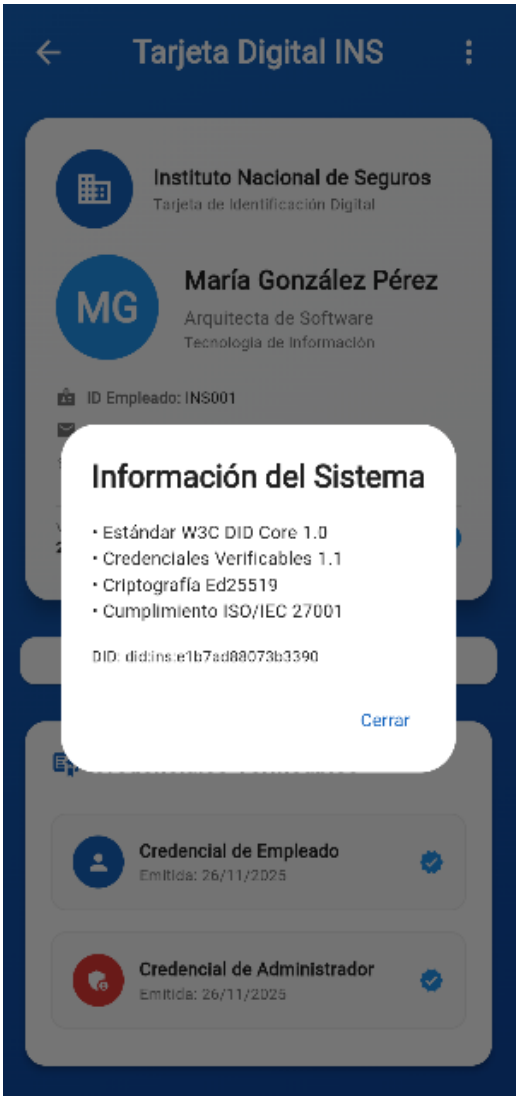
BIBLIOGRAFÍA

- Allen, C. (2016). The path to self-sovereign identity.
- Banco Interamericano de Desarrollo (IDB). (2023). Identidad digital en América Latina. https://publications.iadb.org/es/identidad-digital-en-america-latina-y-el-caribe
- Bernal, C. A. (2010). Metodología de la investigación.
- Blockchain Labs. (2021). Decentralized Identity Systems. https://blockchainlabs.nz
- Hernández-Sampieri, R., Fernández-Collado, C., & Baptista-Lucio, P. (2021). Metodología de la investigación.
- International Organization for Standardization (ISO). (2013). ISO/IEC 27001:2013. Information technology Security techniques Information security management systems Requirements. ISO.
- MICITT. (2023). Certificación Digital. Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones de Costa Rica. https://www.micitt.go.cr
- Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). Bitcoin and Cryptocurrency Technologies. Princeton University Press.
- Tribunal Supremo de Elecciones (TSE). (2024). Avances en identidad digital. https://www.tse.go.cr
- Vassil, K. (2015). Estonia's E-Government Infrastructure: Foundation for Digital Identity. e-Estonia Briefing Centre.
- Zhou, J., Zhang, Z., & Xie, W. (2020). A survey on digital identity management using blockchain. IEEE Access, 8, 168321–168333. https://doi.org/10.1109/ACCESS.2020.3022272
- Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing privacy: Using blockchain to protect personal data. Proceedings - 2015 IEEE Symposium on Security and Privacy Workshops. https://doi.org/10.1109/SPW.2015.27

ANEXOS

Anexo 1. Prototipo


Tarjeta Digital INS
Instituto Nacional de Seguros
Tarjeta de Identificación Digital
MG
María González Pérez
Arquitecta de Software
Tecnología de Información
ID Empleado: INS001
Correo: maria.gonzalez@grupoins.com
DID: did:ins:e1b7ad88073b3390
Válido desde
26/11/2025
ACTIVA
Ver QR
Actualizar
Credenciales Verificables
Credencial de Empleado
Emitida: 26/11/2025
Información del Sistema
Configuración de Seguridad
Cerrar Sesión


Tarjeta Digital INS
Instituto Nacional de Seguros
Tarjeta de Identificación Digital
MG
María González Pérez
Arquitecta de Software
Tecnología de Información
ID Empleado: INS001
Información del Sistema
• Estándar W3C DID Core 1.0
• Credenciales Verificables 1.1
• Criptografía Ed25519
• Cumplimiento ISO/IEC 27001
DID: did:ins:e1b7ad88073b3390
Cerrar
Credencial de Empleado
Emitida: 26/11/2025
Credencial de Administrador
Emitida: 26/11/2025


Tarjeta Digital INS
Instituto Nacional de Seguros
Tarjeta de Identificación Digital
MG
María González Pérez
Arquitecta de Software
Tecnología de Información
Configuración de Seguridad
Autenticación Biométrica
Cifrado de Datos
Auditoría de Acceso
Cerrar
Credencial de Empleado
Emitida: 26/11/2025
Credencial de Administrador
Emitida: 26/11/2025


Tarjeta Digital INS
Instituto Nacional de Seguros
Tarjeta de Identificación Digital
MG
María González Pérez
Arquitecta de Software
Tecnología de Información
ID Empleado: INS001
Correo: maria.gonzalez@grupoins.com
DID: did:ins:e1b7ad88073b3390
Válido desde
26/11/2025
ACTIVA
Ver QR
Actualizar
Credenciales Verificables
Credencial de Empleado
Emitida: 26/11/2025
Credencial de Administrador
Emitida: 26/11/2025
Datos actualizados