Instituto Tecnológico y de Estudios Superiores de Monterrey

Campus Monterrey

Uso de álgebras modernas para seguridad y criptografía
MA2006B.601

Reto: Fase 1

Equipo 1:
Sebastián Miramontes Soto - A01285296
Adrián Mateos Garza - A01722496
Miguel Ángel González Gutiérrez - A01198604
Antonio Pena Lozano - A01722688
Roberto Priego Bautista - A01285539

Docentes:
Luis Miguel Méndez Díaz
Daniel Otero Fadul
Raúl Gómez Muñoz
Sadam Hussain

Fecha:
07/03/2025

To-Do List

2. Índice

3. Resumen (en español e inglés de 100 a 150 palabras).

4. Introducción: tema y nicho del objeto de estudio (máximo 250 palabras).

5. Marco referencial que incluye el marco teórico, contextual y estado del arte

6. Metodología que incluya una descripción detallada de los métodos utilizados para obtener la solución del reto.

7. Resultados: presentación de los procedimientos de los métodos usados y resultados obtenidos

8. Conclusiones finales

9. Recomendaciones para el socio formador (máximo 1000 palabras).

10. Referencias en formato APA.

Indice:

####

Resumen:

####

Palabras clave: ###

Abstract:

####

Kew Words: ####

Introducción:

La seguridad digital es de gran importancia para los documentos electrónicos, ya que entre los elementos más importantes de estos se encuentran la confidencialidad y la autenticidad. Para lograr esto —es decir, que el documento electrónico sea accesible solo para una lista de individuos autorizados y que estas mismas personas se comprometan con su contenido—, se suele utilizar el concepto de autenticación digital y la firma electrónica o autógrafa (Marrero, 2003). La motivación principal de este proyecto es garantizar la autenticidad e integridad de los documentos emitidos por organizaciones que apoyan migrantes, evitando fraudes, falsificaciones y pérdidas de confianza, ya que la migración es un es un fenómeno global que afecta a millones de personas, los cuales suelen acudir a casa migrantes, los cuales les brindan asesoría legal, asistencia humanitaria, orientación laboral y educación, generando una gran cantidad de documentos o información, los cuales pueden ser falsificados, alterados o utilizados de manera fraudulenta, en caso de no ser manejados de una forma correcta. Dentro de los objetivos mas especificos del reto se encuentra el desarrollar un sistema de firma digital adaptado a la organización socio formadora (Casa Monarca), que funcione de la mejor manera y pueda garantizar el cumplimiento de normativas y principios éticos.

Marco referencial:

Caso 1. IMPLEMENTACIÓN DE UN SISTEMA WEB CON FIRMA DIGITAL PARA MEJORAR EL PROCESO DE TRÁMITE DOCUMENTARIO INTERNO EN EL INSTITUTO GEOGRÁFICO NACIONAL

El siguiente informe fue un trabajo hecho por la Facultad de Ingeniería y Arquitectura de la Universidad Autónoma del Perú con el objetivo de mejorar procesos dentro de una institución gubernamental. Consideramos que este documento cuenta con una gran referencia el cual podria ser implementada en Casa Monarca ya que las tecnologias presentadas no son las mas nuevas que hay, pero no representan que sean obsoletas o vulnerables, al contrario, cuentan con la documentación suficiente para poder desarrollar un producto parecido.

Marco Teorico.

El estudio parte de la idea de la creacion de un sistema web con una arquitectura de cliente/servidor que se ejecuta desde el navegador y se comunica mediante puertos y protocolos estandarizados. Se explica de igual manera como estos sistemas permiten la gestion de información de manera remota. Ademas de que abarcan el uso de firmas digitales para garantizar la autenticidad e integridad de los documentos mandados. Una de las tecnologias las cuales se nota demasiado que se estan usando es Java y multiples extenciones de Java como lo son JSP (JavaSever Pages), lo cual sirve para el desarrollo de una interfaz de usuario (UI) y Apache Tomcat, el cual es un servidor web que permite ejecutar aplicaciones webs escritas en Java. Se describen ademas arquitecturas de software como lo son el patron de Modelo-Vista-Controlador para la organización de codigo y metodologias como la Srum con un enfoque de trabajo iterativa e incremental, asignando roles, gestionado un backlog del producto y planificando el desarrollo a través de 'sprints', lo cual optimiza la productividad de todo el equipo.

Marco Contextual.

La situación en la que nos enmarca es el contexto del Instituto Geográfico Nacional del Perú, donde los procesos de tramites de documentos se realiza de forma física. Esto implica que la generación y manejos de archivos se efectua mediante imprimiendo documentos y haciendo entregas manuales lo cual puede generar:

- Demoras en la atención de documentos.
- Aumento en el consumo de papel y otros materiales y/o servicios (tintas, mantenimiento de imprentas, servicio de envio)
- Dificultades de seguimiento de documentación interna

Ante esta situación se llego a la conclusion de atacar este problema con la creacion de una solución digutal que les permitiera:

- Reducir los tiempos de atención de documentos.
- Optimizar el uso de recursos al disminuir el gasto en papeleria.

- Dificultades en el control y seguimiento de la docuentación interna.

Estado del Arte

La revisión dada por sus antecedentes muestran que han habido problematicas relativamente parecidas. Las cuales incluyen estudios que demuestran que la implementación de estos sistemas de gestión de documentos mejora la eficiencia en la búsqueda y control de la información y reduce significativamente tiempos, costos y mejora la satisfacción del personal encargado. En cuanto al enfoque criptografico decidieron conformarlo con la implementación de uso de Documento Nacional de Identidad (DNI) digitales, el cual contiene un certificado digital unico que permite encriptar y firmar electronicamente documentos. Esta tecnologia de igual manera es utilizada en México en sistemas como el SAT, el cual te proporcionan con una E-FIRMA para garantizar ciertos procesos legales con respecto a la contribución de impuestos.

Caso 2. La implementación de la firma digital en el sector público : Mejoras en la gestión y en los procesos para lograr óptimos resultados

El presente estudio se basa en la investigación realizada por De Luca (2015) sobre la implementación de la firma digital en el sector público y sus beneficios en la gestión documental. Este caso es una referencia valiosa para la aplicación en Casa Monarca, ya que presenta un marco teórico sólido, ejemplos de implementación y el impacto positivo en la eficiencia administrativa.

Marco Teórico

El estudio se basa de la necesidad de poder garantizar autenticidad, integridad y no repudio de documentos electrónicos a través de firmas digitales que se basaron en criptografía de clave pública o PKI, en donde se hicieron análisis de los algoritmos más utilizados, como lo son Rivest-Shamir-Adleman (RSA), Digital Signature Algorithm (DSA) y Elliptic Curve Digital Signature Algorithm (ECDSA), como también los mecanismos de hashing tipo SHA-256, que aseguran la no alteración de documentos.

La firma digital ha tenido relevancia como una herramienta importante para la optimización de procesos administrativos dentro del sector público. Y existen evidencias los cuales destacan en su función de reducir la utilización de papel y tener transparencia gubernamental, por lo que existen marcos normativos que proporcionan una base legal para su aplicación.

Marco Contextual

Hemos aprendido que Casa Monarca es una organización 100% dedicada al apoyo de migrantes, por lo que manejan una cantidad grande de documentos legales y administrativos. Sin embargo, actualmente, muchos de estos documentos están almacenados de forma tradicional, lo que incrementa el riesgo de falsificación, pérdida de información e ineficiencia en el control de documentos.

En Latinoamérica, la implementación de la firma digital ha ido creciendo cada vez más en sectores gubernamentales y empresariales. Países como Argentina, México y Brasil se han actualizado desarrollando infraestructuras de clave pública para la validación de documentos. En el contexto del problema, para Casa Monarca, adoptar una solución de firma digital permitiría optimizar la gestión documental, lo cual mejora la

seguridad, alineándose con las mejores prácticas de protección de datos.

Estado del Arte

En el estudio de Juan Carlos De Luca (2015), se hace un análisis sobre la aplicación de la forma digital dentro de la Administración Pública Argentina, la cual resalta en tener mejoras en eficiencia, reducción de costos y aumento en la transparencia.

Existen casos específicos analizados como la implementación dentro de la Bolsa de Cereales de Rosario, donde la firma digital tuvo un impacto positivo al permitir agilizar procesos y reducir tiempos de administración. Esto respalda la idea de que las firmas digitales para optimizar desarrollos, eliminando procedimientos de estilos burocráticos los cuales no son realmente necesarios.

De manera internacional, existen marcos como eIDAS en la Unión Europea y el NIST SP 800-63B en Estados Unidos los cuales establecen ciertas regulaciones para la firma digital y el tipo de aplicación que tenga en documentos oficiales, teniendo como aliados a tecnologías como OpenSSL, como también bibliotecas para la criptografía en distintos lenguajes de programación como Python o R que han tenido peso en facilitar la implementación de este tipo de sistemas en numerosas organizaciones.

Caso 3. Aplicación de la plataforma de firma digital en la emisión de los documentos académicos de una Universidad Pública

Esta investigación tenía como propósito inicial introducir una plataforma que incorporara la firma digital para mejorar la eficiencia en la emisión de documentos académicos, optimizando tanto el proceso como la satisfacción estudiantil. La firma digital se presenta como una herramienta esencial para agilizar y garantizar la seguridad en la emisión de estos documentos, lo que está alineado con el propósito principal del estudio.

Marco Teórico

Para desarrollar una plataforma de firma digital es necesario familiarizarse con diversos conceptos:

- Documentos académicos: son toda aquella papelería oficial detallada en el Reglamento Académico, que los estudiantes pueden solicitar para diferentes fines.
- Firmas electrónicas: cualquier símbolo creado electrónicamente que se utiliza para autenticar o vincular al firmante con un documento o archivo.
- Firma digital: un tipo de firma electrónica basada en criptografía asimétrica, caracterizada por su autenticidad, integridad y no repudio del suscriptor.
- Certificado digital: documento electrónico generado y firmado digitalmente por una entidad certificadora, el cual vincula un par de claves con una persona determinada.
- Software de firma digital: aplicación que facilita el uso de la firma digital en un entorno electrónico con el debido valor legal.

Marco Contextual

La Universidad Nacional de Barranca (UNAB) se caracteriza por su necesidad de modernizar los procesos administrativos, especialmente en la emisión de documentos académicos. Uno de los mayores problemas es la

demora en la entrega de dichos documentos, lo que genera ineficiencia administrativa y quejas por parte de la comunidad universitaria.

La adopción de nuevas tecnologías ha sido un factor clave en la optimización de procesos dentro de las instituciones educativas de nivel superior. Se han encontrado diversas estadísticas e información relacionada con la temática, tanto en el contexto local como en el internacional.

En Perú, país de procedencia de esta investigación, el proceso de digitalización mediante firmas digitales sigue en desarrollo. No obstante, el mercado global de firmas digitales fue valorado en aproximadamente 2.8 mil millones de dólares en 2022, y se espera que alcance los 12.7 mil millones para 2027. En 2021, solo el 35% de las universidades peruanas contaban con un sistema digital para emitir documentos oficiales, aunque este proceso se aceleró debido a la pandemia de COVID-19.

Estado del Arte

Esta problemática ha sido abordada en distintos escenarios previos, lo que indica que la implementación de una plataforma de firma digital podría optimizar significativamente el proceso de emisión de documentos académicos en la Universidad Nacional de Barranca.

Entre los estudios relacionados, se encuentra "Análisis del sistema de facturación electrónica y su aplicación en las empresas cartoneras en Guayaquil", cuyo objetivo era demostrar los beneficios de la facturación electrónica y su impacto en la recaudación tributaria. Los resultados mostraron cambios significativos en los procesos, con beneficios tanto económicos como productivos.

Asimismo, en Perú se realizó el estudio "Implementación de Firmas Digitales para el Control de la Integridad de Certificados de Estudios", el cual evidenció que la firma digital contribuye efectivamente a un mejor control y gestión de los certificados de estudio en el ámbito universitario.

Caso 4. Decreto 743/2024: Reforma de Ley de Firma Digital en Argentina

En la actualidad, la digitalización de documentos y trámites administrativos ha ganado gran relevancia a nivel global, especialmente en el area gubernamental. Las firmas digitales se ha convertido en una herramienta clave para garantizar autenticidad, integridad y validez legal de documentos electrónicos, a su vez facilitando los procesos de trámites de manera segura y eficiente. Bajo este contexto, Argentina recientemente ha implementado regulaciones específicas para propiciar el uso de las firmas digitales tanto en el sector público como en el sector privado.

Marco Teorico

Los principales tipos de firma digital que existen actualmente para tramites gubernamentales son 2: Firma Digital y la Firma Electronica; Una firma electronica es cualquier método de firma electrónica que se realice con datos de identidad mediante un certificado digital simple, por otro lado, la firma digital se fundamenta en técnicas de criptografía asimétrica, en las cuales se utilizan claves públicas y privadas para generar un valor numérico (huella digital) único a partir del contenido del documento. Este valor o huella se añade al documento para garantizar su autenticidad, integridad y no repudio, es decir, avalar que el documento no ha sido alterado y que

proviene del titular legítimo. La Ley Argentina Nº 25.506 establece que, mediante la aplicación de operaciones matemáticas y el uso de certificados digitales avanzados, la firma digital adquiere validez legal, diferenciándose de la firma electrónica simple que utiliza métodos menos rigurosos de autenticación.

Marco Contextual

En Argentina, el uso de la firma digital ha sido potenciado para modernizar la tramitación de procedimientos administrativos y mejorar la accesibilidad a servicios digitales. El reciente Decreto 743/2024, publicado el 19 de agosto del 2024, introduce cambios significativos al permitir la verificación de identidad de forma remota, eliminando la obligatoriedad de la presencialidad para la emisión, renovación o revocación de certificados. Asimismo, este decreto autoriza a los certificadores licenciados a delegar la validación de identidad en autoridades de registro, lo que simplifica y agiliza bastante los trámites. La creación de la Infraestructura de Firma Digital de la República Argentina (IFDRA) respalda este sistema, administrando el registro público de firmas digitales y supervisando a los certificadores, lo que aumenta la confianza en el uso de esta tecnología tanto en el sector público como privado.

Estado del Arte

La implementación de la firma digital en Argentina se suma a un esfuerzo global en el que numerosos países han estado adoptando soluciones tecnológicas para garantizar la autenticidad y seguridad de documentos electrónicos. Experiencias en Argentina, como las de la adopción de la Ley Nº 25.506 y sus modificaciones recientes, demuestran cómo la digitalización de los trámites administrativos contribuye a una mayor eficiencia y seguridad jurídica. A nivel internacional, existen trabajos y aplicaciones en áreas como el comercio electrónico, la administración pública y las transacciones financieras que le han dado validez y respaldo a la utilizacion de las firmas digital. Además, diversas herramientas y bibliotecas de criptografía (por ejemplo, OpenSSL, Bouncy Castle o librerías específicas de lenguajes de programación como Java y Python) proporcionan recursos fundamentales para el desarrollo e implementación de firmas digitales. Estas soluciones se han convertido en el estándar alrededor del mundo, permitiendo que la tecnología evolucione en sintonía con las necesidades de seguridad, accesibilidad y legalidad que exige la transformación digital de los servicios.

Caso 5. Firmas digitales en México: conceptos, oportunidades y desafíos

La pandemia de COVID-19 evidenció la necesidad de contar con herramientas tecnológicas que automatizan las tareas asociadas al uso de firmas digitales. Sin embargo, a pesar de los enormes beneficios que conllevan, las firmas digitales han experimentado un proceso de adopción lento, por lo que es de gran importancia analizar y potenciar su uso en cualquier proceso.

Marco teórico

Las firmas digitales son el equivalente digital de las firmas autógrafas, las cuales se han utilizado ampliamente para garantizar la autenticidad de un documento y su contenido. Dentro de los retos que enfrentan las

firmas autógrafas y que deben ser asegurados en las firmas digitales, se encuentran:
- Autenticidad: Identificar inequívocamente al firmante.
- No repudio: Garantizar que el firmante no pueda negar haber realizado la firma.
- Integridad: Asegurar que el documento no haya sido modificado después de haber sido firmado.

Dentro de los conceptos relacionados con las firmas electrónicas y la criptografía, se mencionan la criptografía de clave pública (Public Key Cryptography, PKC), las infraestructuras de clave pública (Public Key Infrastructure, PKI) y la Infraestructura Extendida de Seguridad (IES), los cuales son fundamentales para el desarrollo del proceso de firmas.

Marco contextual

La implementación oficial de firmas digitales en México data del año 2000; sin embargo, fue hasta el 11 de enero de 2011 cuando se publicó en el Diario Oficial de la Federación el decreto por el que se expide la Ley de Firma Electrónica Avanzada. Mediante esta ley, se reconoce la equivalencia entre la firma autógrafa y la firma digital, y se definen las características de los certificados digitales y de la PKI.

El uso de firmas digitales en México aún está en sus primeras etapas, ya que persiste una falta de confianza y conocimiento sobre su aplicación. No obstante, en prácticamente todos los estados de la República Mexicana existe legislación relacionada con su uso. Además, instituciones como el Banco de México, la Secretaría de Economía y el Servicio de Administración Tributaria (SAT) emplean recursos similares.

Estado del arte

En México, la investigación y el desarrollo en el tema de firmas digitales son escasos, debido a la existencia de pocos grupos de investigación en el área de criptografía. No obstante, en el Cinvestav Tamaulipas se ha trabajado en la formación de recursos humanos en materia de firma electrónica, particularmente a nivel licenciatura, y también se han realizado aportaciones en el desarrollo de soluciones de criptografía poscuántica (Post-Quantum Cryptography, PQC) para el entorno del Internet de las Cosas (IoT).

A pesar de las barreras culturales que dificultan la adopción de las firmas digitales, existen múltiples ventajas que deberían aprovecharse, como una mayor seguridad, la automatización de procesos y el ahorro de recursos. Además, este tipo de tecnología impulsa diversas líneas de investigación orientadas hacia los avances tecnológicos.

De Luca, J. C. (2015). La implementación de la firma digital en el sector público : Mejoras en la gestión y en los procesos para lograr óptimos resultados . (Trabajo Final de Posgrado. Universidad de Buenos Aires.) http://bibliotecadigital.econ.uba.ar/download/tpos/1502-0390_DeLucaJC.pdf

Edicom. (2024, 12 de septiembre). Decreto 743/2024: Reforma de Ley de Firma Digital en Argentina. https://edicom.mx/blog/firma-digital-argentina#:~:text=Validez%20legal%20de%20la%20firma,privadas%20utilizando%20la%20firma% 20digital.

Herrera, R. M. A. (2024). Aplicación de la plataforma de firma digital en la emisión de los documentos académicos de una Universidad Pública. Alpha Centauri, 5(3), 24-33. http://www.journalalphacentauri.com/index.php/revista/article/view/176

Sandoval, M. M. (2022). Firmas digitales en México: conceptos, oportunidades y desafíos. https://ccc.inaoep.mx/~mmorales/divulg/JD05.pdf

Zavaleta Antón, J. A. (2022). Implementación de un sistema web con firma digital para mejorar el proceso de trámite documentario interno en el Instituto Geográfico Nacional, 2021. https://repositorio.autonoma.edu.pe/handle/20.500.13067/1946

Metodología:

###

Metodología:

###

Resultados:

###

Conclusiones:

###

Recomendaciones:

###

Referencias:

Argentina.gob. (s.f.). Firma digital. Jefatura de Gabinete de Ministros. https://www.argentina.gob.ar/firma-digital

Edicom. (2024, 12 de septiembre). Decreto 743/2024: Reforma de Ley de Firma Digital en Argentina. https://edicom.mx/blog/firma-digital-argentina#:~:text=Validez%20legal%20de%20la%20firma,privadas%20utilizando%20la%20firma%20digital.

Marrero Travieso, Y. (2003). La Criptografía como elemento de la seguridad informática. Acimed, 11(6), 0-0