Vol.8 No.3 (2024): Journal Scientific MQRInvestigar ISSN: 2588–0659
https://doi.org/10.56048/MQR20225.8.3.2024.1372-1387

Validation model for digital signatures and certificates embedded in electronic documents generated by students at the Catholic University of Cuenca

Modelo de validación de firmas y certificados digitales embebidos en documentos electrónicos generados por estudiantes de la Universidad Católica de Cuenca

Autores:

Galarza-Pauta, Kléber Fernando
UNIVERSIDAD CATÓLICA DE CUENCA
Ingeniero de sistemas
Maestría en ciberseguridad
Cuenca – Ecuador

kgalarza@ucacue.edu.ec

https://orcid.org/0009-0007-6038-1860

Criollo-Bonilla, Ronald Raúl
ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL
Magíster en Sistemas de Información Gerencial
Docente Tutor de la maestría en ciberseguridad
Cuenca – Ecuador

ronald.criollo@ucacue.edu.ec

https://orcid.org/0000-0001-7103-6869

Fechas de recepción: 25-JUN-2024 aceptación: 18-JUL-2024 publicación:15-SEP-2024

https://orcid.org/0000-0002-8695-5005
http://mqrinvestigar.com/

Resumen

Este artículo examina la importancia y los métodos de verificación de firmas digitales embebidas en documentos electrónicos generados por los estudiantes de la Universidad Católica de Cuenca, enfatizando su rol crucial en asegurar la autenticidad, integridad y no repudio de los documentos. Con el creciente desarrollo de soluciones basadas en tecnologías de la información en instituciones educativas, la firma digital se ha convertido en una herramienta esencial para la validación de documentos electrónicos. La investigación se estructura en tres fases metodológicas: (i) una revisión del estado del arte mediante un enfoque deductivo – inductivo en bases de datos científicas, (ii) un análisis situacional actual utilizando métodos analítico – sintético e histórico para explorar problemas y variables en la gestión documental, y finalmente (iii) la aplicación de métodos hipotéticos y experimentales para proponer una solución innovadora. Dentro de la propuesta, se realiza un análisis detallado de técnicas y algoritmos como RSA (Rivest-Shamir-Adleman) y ECDSA (Elliptic Curve Digital Signature Algorithm), evaluando su seguridad y eficiencia. Se destaca la importancia de una infraestructura de clave pública (PKI) robusta para respaldar los procesos de verificación de firmas digitales. Los resultados de la investigación proporcionan un marco sólido para implementar un modelo de verificación de firmas digitales en la universidad, promoviendo la confianza y seguridad en los trámites administrativos y académicos. Este enfoque no solo optimiza la gestión documental, sino que también sienta las bases para futuras investigaciones y desarrollos en el campo de la ciberseguridad educativa.

Palabras clave: Firma digital; criptografía asimétrica; documentos electrónicos; seguridad informática; infraestructura de clave pública (PKI)

Abstract

This article examines the importance and methods of verifying digital signatures embedded in electronic documents generated by students at the Universidad Católica de Cuenca, emphasizing their crucial role in ensuring document authenticity, integrity, and non-repudiation. With the growing development of information technology solutions in educational institutions, digital signatures have become an essential tool for validating electronic documents. The research is structured into three methodological phases: (i) a review of the state of the art using a deductive-inductive approach in scientific databases, (ii) a current situational analysis using analytical-synthetic and historical methods to explore issues and variables in document management, and finally (iii) the application of hypothetical and experimental methods to propose an innovative solution. Within the proposal, a detailed analysis of techniques and algorithms such as RSA (Rivest-Shamir-Adleman) and ECDSA (Elliptic Curve Digital Signature Algorithm) is conducted, evaluating their security and efficiency. The importance of a robust Public Key Infrastructure (PKI) to support digital signature verification processes is highlighted. The research findings provide a solid framework for implementing a digital signature verification model at the university, enhancing trust and security in administrative and academic procedures. This approach not only optimizes document management but also lays the groundwork for future research and developments in educational cybersecurity.

Keywords: Digital signature; asymmetric cryptography; electronic documents; computer security; Public Key Infrastructure (PKI)

Introducción

El creciente desarrollo de la tecnología y la necesidad de realizar la digitalización de transacciones han impulsado el desarrollo de sistemas seguros y eficientes para la verificación de identidad (Taleb y Vergnaud, 2021; Barbón Pérez y Fernández Pino, 2018). Según Marissa (2013), la correcta diferenciación entre método y metodología es un problema frecuente en soluciones tecnológicas, y debe ser considerada dentro del proceso de firmas y certificados digitales. Estos mecanismos ayudan a disminuir riesgos de adulteración de documentos digitales, asegurando al usuario la autenticidad, integridad y no repudio en sus transacciones (Lizano Martinez et al., 2014; Palmer, 2008).

A medida que la utilización de firmas y certificados digitales se extiende en diferentes sectores, se presenta la necesidad imperante de mejorar la eficiencia y robustez de los sistemas de verificación. Esto se observa con la certificación FIDO2 y en el campo de las billeteras de hardware en rápida expansión, incluyendo diseños validados en SoC FPGA (Aggarwal y Kumar, 2021; Mašek y Novotný, 2022). Según Zuhua (2009) y Hsu et al. (2014), una firma digital proporciona la autenticidad de un mensaje firmado con respecto a una clave pública, mientras que la autenticidad de la clave pública con respecto a un firmante reside en un certificado proporcionado por una autoridad certificadora.

Sin embargo, los criptosistemas de clave pública que no requieren certificados digitales son muy atractivos en las comunicaciones inalámbricas debido a las limitaciones impuestas por el ancho de banda y los recursos computacionales de los dispositivos de comunicación inalámbricos móviles. Para eliminar el certificado digital de clave pública, Shamir introdujo el concepto de criptosistema basado en identidad (ID) (Harn, Ren, y Lin, 2009).

Para resolver el problema de la custodia de claves del criptosistema basado en identidad, Girault introdujo la noción de una clave pública auto-certificada, la cual no solo elimina la necesidad de autenticar una clave pública, sino que también resuelve el problema de la custodia de claves (Zhang et al., 2012; Irigoitia, 2016).

Este artículo ha realizado una investigación basada en diversas fuentes bibliográficas para analizar el concepto de verificación de firmas y certificados digitales, incluyendo algoritmos criptográficos, estándares tecnológicos, procedimientos y herramientas de seguridad disponibles en el mercado.

Además, se ha considerado la ciberseguridad, la criptografía, la infraestructura de clave pública (PKI), métodos de autenticación y nuevas técnicas de verificación de firmas en línea basadas en modelos matemáticos como la transformada de coseno discreta (DCT) y la representación dispersa (Kim, Cho, y Cha, 2005; Vergara da Silva y Santana de Freitas, 2002; Liu, Yang, y Yang, 2015).

La firma de documentos digitales se realiza mediante el uso del paradigma de criptografía de llave pública, donde a cada ciudadano se le genera un par de llaves pública/privada y un certificado digital. Este certificado digital es distribuido para el conocimiento de todos los

usuarios del sistema, permitiendo que el signatario firme cualquier documento digital utilizando su llave privada. Una vez que los documentos firmados son recibidos por alguna entidad, esta puede comprobar la validez de la firma utilizando la llave pública del firmante (Dominguez Perez et al., 2019).

La Universidad Católica de Cuenca está experimentando actualmente una transformación digital al implementar la política de cero papeles, con el objetivo de potenciar la gestión de documentos y mejorar la seguridad de los trámites estudiantiles realizados de manera virtual. Aunque la infraestructura informática de la institución cuenta con distintos servicios disponibles para los estudiantes, no existe una aplicación que permita la creación y verificación de firmas y certificados digitales. Esto proporcionaría la certeza de que la documentación sea íntegra, permitiendo así dar el trámite correspondiente.

El objetivo principal de este artículo es contribuir al avance de la verificación de firmas y certificados digitales embebidos en los documentos electrónicos a través de la aplicación de algoritmos y métodos criptográficos, garantizando la autenticidad, integridad y no repudio de los documentos electrónicos. Se pretende lograr esto mediante una revisión exhaustiva de métodos existentes, la identificación de áreas de mejora y la implementación de soluciones innovadoras

Metodología

Para desarrollar un modelo de verificación de firmas digitales embebidas en documentos electrónicos dentro la institución, se siguieron tres fases claramente definidas. En primer lugar, se inició con la revisión del estado del arte en bases de datos científicas. Mediante el modelo analítico-sintético, se planteó una ecuación de búsqueda que contempló la revisión de artículos científicos y memorias de congresos con un máximo de cinco años de antigüedad, en idioma inglés y español. Se descargaron los archivos CSV de los resultados para posteriormente clasificarlos y analizarlos, identificando así los desarrollos más recientes y relevantes en el campo de la verificación de firmas digitales.

En la segunda etapa, se caracterizaron las variables relacionadas con la legalización de documentos utilizando los métodos histórico, de campo y analítico. Este análisis se enfocó en entender cómo se manejaban actualmente las firmas y certificados digitales dentro de la institución y en identificar las prácticas y normativas vigentes. La recopilación de datos se realizó a través de entrevistas, encuestas y revisión documental, lo que permitió obtener una visión clara de la situación actual.

En la etapa final, se propuso un modelo de verificación de firmas digitales utilizando los métodos hipotético, analítico y experimental. Se clasificaron las variables previamente identificadas para garantizar un alto grado de seguridad, eficiencia y usabilidad del sistema. Las variables dependientes e independientes incluyeron la clave pública del firmante, el algoritmo de firma, el hash de los datos firmados, el certificado digital, la cadena de certificados, la fecha y hora de la firma, las políticas de firma, el formato de los datos firmados, la revocación de certificados, la entropía y calidad de las claves, el entorno de ejecución, y las normativas y estándares aplicables.

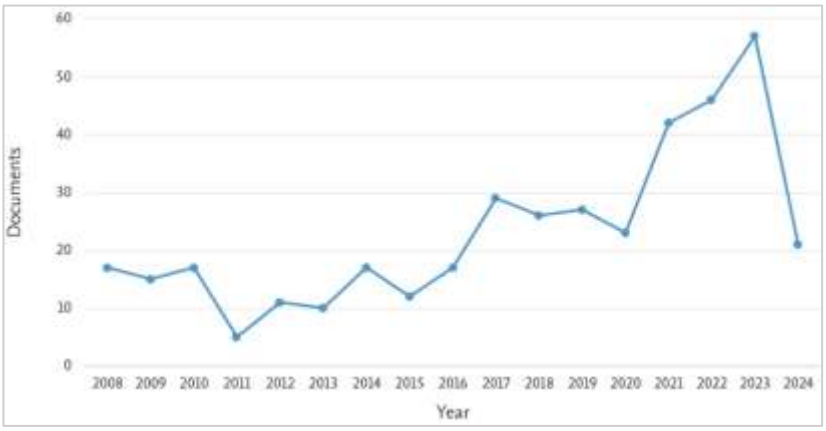
Este enfoque metodológico permitió desarrollar un modelo robusto y fiable para la verificación de firmas digitales embebidas en documentos electrónicos. De esta manera, se aseguró la autenticidad, integridad y no repudio de los documentos generados por los estudiantes de la Universidad Católica de Cuenca, contribuyendo significativamente a la transformación digital y a la seguridad de los trámites estudiantiles realizados de manera virtual.

Resultados

En la primera fase de la revisión de las bases de datos, planteamos la siguiente ecuación de búsqueda avanzada: verification AND digital AND signatures AND embedded AND electronic AND documents AND (LIMIT-TO (DOCTYPE , "ar") OR LIMIT-TO (DOCTYPE , "cp")) AND (LIMIT-TO (LANGUAGE , "English")). Con esta ecuación, se obtuvieron 458 artículos. Al realizar un análisis detallado de estos artículos, se observó una pendiente positiva del 1.42% en los trabajos investigados dentro de la temática, tal como se muestra en la Figura 1. Este incremento refleja la creciente importancia y relevancia de la investigación en el campo de la verificación de firmas digitales embebidas en documentos electrónicos.

Figura 1

Número de documentos por año, en base al tema de investigación.

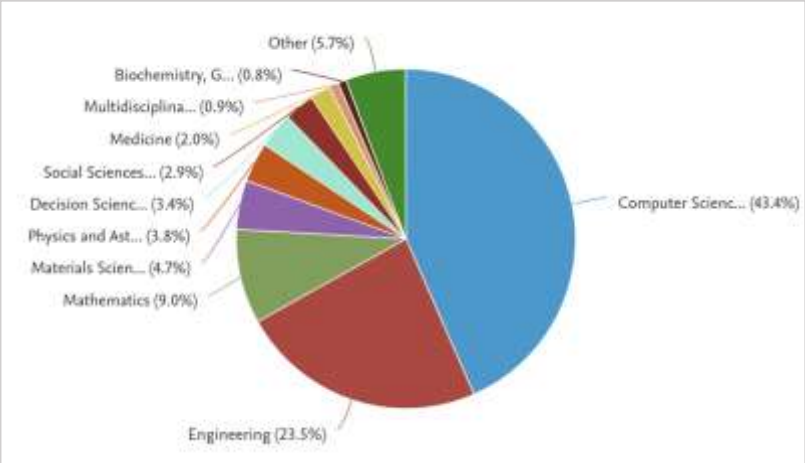


Además, al analizar los artículos desde el punto de vista del área de conocimiento, se encontró que el 43.4% de los artículos están en el ámbito de las Ciencias de la Computación, seguido por un 23.5% en el área de ingenierías. El restante porcentaje se distribuye entre otras áreas de conocimiento, lo que indica un soporte multidisciplinario para esta temática de

investigación, como se ilustra en la Figura 2. Este análisis muestra que, aunque la mayoría de las investigaciones se concentran en Ciencias de la Computación e ingenierías, hay un interés creciente en otras disciplinas que también contribuyen a este campo.

Figura 2

Documentos por área de conocimiento.



Actualmente, entre los principales problemas identificados en la Universidad Católica de Cuenca se encuentran la falsificación de documentos presentados en diferentes departamentos y trámites. Además, debido a la imposibilidad de algunos estudiantes de estar físicamente en la ciudad, a menudo solicitan a amigos que realicen los trámites por ellos, lo que genera errores.

Históricamente, se evidencia que se tramitan aproximadamente 110 trámites al día, considerando un valor promedio basado en la actividad de cada departamento distribuido en la Universidad. Esto se traduce en un total de 2,200 trámites por mes y 26,400 trámites al año, convirtiéndose en un problema técnico y de investigación, además de afectar la seguridad, tiempos y calidad de los procesos. Además, para desarrollar la propuesta de un modelo de verificación de firmas digitales embebidas, se planteó un listado de requisitos. Mediante un análisis de expertos, se levantó información sobre la prioridad de estos requisitos, como se presenta en la Tabla 1.

Los expertos consultados fueron los secretarios de cada una de las facultades de la Universidad, quienes cuentan con un mínimo de cinco años de experiencia en la gestión documental. Esta consulta permitió establecer una jerarquía de prioridades que guiará el desarrollo y la implementación del modelo propuesto, asegurando que responda adecuadamente a las necesidades específicas de la Universidad.

Tabla 1

Variables de la verificación de firmas digitales.

Criterio	Criterio
C1. Verificación de firmas	C10. Mejora la competitividad
C2. Gestión de claves	C11. Evita las filas y los desplazamientos
C3. Almacenamiento seguro	C12. Agiliza y disminuye el papeleo
C4. Seguridad	C13. Protege suplantación de identidad
C5. Usabilidad	C14. Contribuye con el medio ambiente
C6. Compatibilidad	C15. Mejor utilización del espacio físico
C7. Base de datos	C16. Protección jurídica
C8. Interfaz de usuario	C17. Agilizar la tramitología
C9. Ahorro de dinero y tiempo	C18. Proteger la integridad de documentos

Con los valores de la Tabla 1, se aplica el cálculo de la varianza (Ec.1) y el Alpha de Cronbach (Ec.2) para determinar la importancia de las variables.

$$S^2 = \frac{\sum(X_i - \bar{x})^2}{n-1} \qquad (1)$$

Donde:

$S^2 = varianza$

$X_i = término\ de\ conjunto\ de\ datos$

$\bar{x} = medida\ de\ la\ muestra$

$\sum = sumatoria$

$n = tamaño\ de\ la\ muestra$

$$\alpha = \frac{K}{K-1}\left[1 - \frac{\sum V_i}{V_t}\right] \qquad (2)$$

Donde:

$\alpha = Coeficiente\ del\ alfa\ de\ Cronbach$

$K = número\ de$ ítems

$V_i = varianzas\ de\ cada$ ítems

$V_t = varianza\ del\ total$

En cuanto al análisis de las variables, se utilizó el coeficiente Alfa de Cronbach como medida de consistencia interna. Los valores obtenidos, cercanos a 1 para todas las variables según se muestra en la Tabla 2, indican una buena fiabilidad en la medición de la misma construcción teórica. Las variables se clasificaron en dos grupos: Grupo 1 (C4, C5, C8, C9, C12, C15, C17) y otro grupo adicional, considerándolas para integrar el algoritmo de validación de firmas y certificados digitales embebidos en documentos electrónicos.

Tabla 1

Cálculo de Varianza y del Alfa de Cronbach

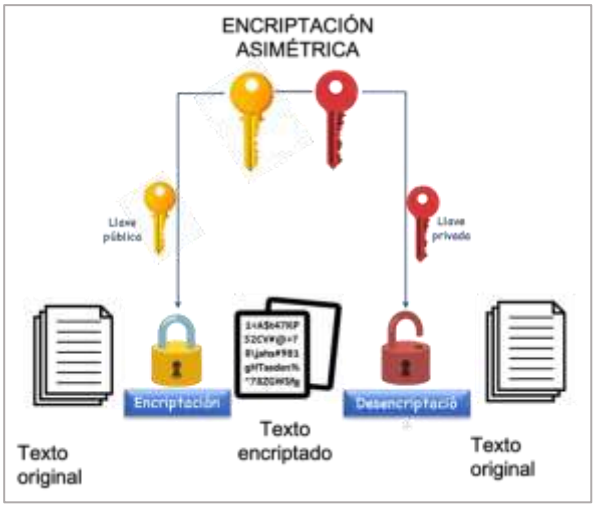
Criterio	Varianza	Alfa de Cronbach
C1. Verificación de firmas	0,538353721	0,955997956
C2. Gestión de claves	0,474133537	0,968264012
C3. Almacenamiento seguro	0,357925586	0,990459734
C4. Seguridad	0,281472987	1,005062182

C5. Usabilidad	0,003185525	1,058215094
C6. Compatibilidad	0,571992864	0,949572878
C7. Base de datos	0,385448522	0,985202852
C8. Interfaz de usuario	0,079638124	1,043612646
C9. Ahorro de dinero y tiempo	0,156090724	1,029010197
C10. Mejora la competitividad	0,385448522	0,985202852
C11. Evita las filas y los desplazamientos	0,357925586	0,990459734
C12. Agiliza y disminuye el papeleo	0,000127421	1,058799192
C13. Protege suplantación de identidad	0,538353721	0,955997956
C14. Contribuye con el medio ambiente	0,474133537	0,968264012
C15. Mejor utilización del espacio físico	0,305937819	1,000389399
C16. Protección jurídica	0,538353721	0,955997956
C17. Agilizar la tramitología	0,079638124	1,043612646
C18. Proteger la integridad de documentos	0,015417941	1,055878702

Para la fase de implementación del modelo propuesto, se basó en la encriptación asimétrica para establecer un canal de comunicación seguro entre las partes involucradas. Tanto el emisor como el receptor deben utilizar criptografía asimétrica con el mismo algoritmo definido, lo que garantiza la creación de un juego de claves único e irrepetible para cada transacción, como se muestra en la Figura 3. Este enfoque asegura la autenticidad e integridad de los documentos electrónicos generados por los estudiantes de la Universidad Católica de Cuenca, optimizando la seguridad y eficiencia de los procesos administrativos y académicos.

Figura 3

Proceso de encriptación asimétrica.



Para llevar a cabo la verificación de firmas digitales embebidas en documentos electrónicos, se establecieron seis fases en el proceso de comprobación, como se detalla en la Figura 4: (i)

extracción del documento firmado, (ii) extracción de la firma y certificado, (iii) verificación del certificado, (iv) recálculo del hash del documento original, (v) descifrado del hash cifrado utilizando la clave pública y (vi) verificación de la firma.

Figura 4

Algoritmo para la verificación de firmas y certificados digitales.

```
Inicio
    documento_firmado = cargar_documento("ruta_al_documento_firmado.pdf")
    firma_electronica = extraer_firma(documento_firmado)
    certificado_digital = extraer_certificado(documento_firmado)
    es_certificado_valido = verificar_certificado(certificado_digital)
    if not es_certificado_valido {
                                print("Certificado no válido")
                                exit()
                                }
    documento_original = extraer_contenido(documento_firmado)
    hash_recalculado = calcular_hash(documento_original)
    hash_descifrado = descifrar_con_clave_publica(firma_electronica, certificado_digital)
    if hash_recalculado == hash_descifrado {
            print ("Firma válida: el documento no ha sido alterado y la firma es auténtica.")
        else {
            print ("Firma inválida: el documento ha sido alterado o la firma no es auténtica.")
          }
end
```

Este proceso asegura la autenticidad e integridad de los documentos digitales, proporcionando un marco robusto para la validación de firmas dentro del entorno universitario.

Discusión

La implementación de firmas y certificados digitales en la Universidad Católica de Cuenca presenta varios beneficios y desafíos. Este artículo ha permitido identificar y analizar estos aspectos desde una perspectiva técnica y organizacional, demostrando que dicha implementación mejora significativamente la seguridad y autenticidad de los documentos administrativos y académicos.

Los resultados sugieren que las firmas digitales proporcionan una garantía robusta contra la alteración de documentos, mientras que los certificados digitales validan la identidad del firmante de manera efectiva. Esto confirma nuestra hipótesis de que estas tecnologías pueden aumentar la confianza en los procesos documentales de la institución.

Artículos han demostrado la eficacia de las firmas digitales para garantizar la autenticidad de los documentos, pues brinda máxima seguridad ante un intento de falsificación, además de incorporar otra característica como el no repudio, la cual asegura que el autor no puede negar que ha elaborado un documento que contenga su firma electrónica (Estudillo, 2022).

Los resultados son consistentes con artículos previos como indica Ortega Gamez J., (2024), al señalar que las actividades más recurrentes en una institución de educación superior tienen que ver con la gestión documental. Por ello surge la necesidad de buscar soluciones tecnológicas, entre las que destacan las firmas digitales.

La implementación de un modelo de validación de firmas y certificados digitales dentro de la institución tiene varias implicaciones prácticas que pueden transformar significativamente los procesos administrativos y académicos. Proporciona una capa adicional de seguridad que asegura la autenticidad e integridad de los documentos electrónicos, para prevenir la falsificación y el fraude, lo que conlleva a fortalecer la confianza en los procesos administrativos y académicos de la institución. De la misma manera, se genera una eficiencia administrativa al validar documentos de manera automática, reduciendo el tiempo y los recursos necesarios para su procesamiento. Esto puede resultar en una mayor eficiencia operativa.

A pesar de los beneficios, la implementación de un modelo para la verificación de firmas y certificados digitales, también presenta desafíos. La adopción de firmas y certificados digitales requiere de una infraestructura tecnológica robusta y segura, lo que indicaría que la institución debe invertir en sistemas de gestión de certificados (PKI), hardware adecuado y soluciones de software que garantice la adaptabilidad del modelo propuesto. Además, la compatibilidad e interoperabilidad con sistemas y plataformas existentes en la institución.

La efectividad de estas tecnologías depende en gran medida de la capacitación del personal administrativo y estudiantes en el uso adecuado de firmas y certificados digitales. Además, es importante concienciar a todos los usuarios sobre la importancia y el correcto manejo de estos sistemas para evitar errores y malos entendidos.

Este artículo se ha centrado principalmente en los aspectos técnicos y administrativos de la implementación de firmas y certificados digitales. Sin embargo, no se han abordado en profundidad las posibles implicaciones legales y regulatorias que también son cruciales para una implementación exitosa. Así mismo, la investigación se ha llevado a cabo en un contexto específico, por lo que los resultados pueden variar en función de las particularidades de otras instituciones.

Para fortalecer los resultados obtenidos y abordar las limitaciones identificadas, se recomienda realizar artículos adicionales que exploren las implicaciones legales y regulatorias de la implementación de firmas y certificados digitales. También sería beneficioso explorar y evaluar algoritmos avanzados de seguridad para la validación de firmas y certificados digitales. Algoritmos como RSA, ECC y algoritmos post-cuánticos

pueden ofrecer diferentes niveles de seguridad y eficiencia. Artículos futuros podrían explorar la integración de técnicas de inteligencia artificial y aprendizaje automático para detectar patrones sospechosos y aumentar la seguridad de los documentos electrónicos.

La tecnología blockchain ofrece un alto nivel de seguridad y transparencia debido a su naturaleza descentralizada y su capacidad para registrar transacciones de manera inmutable. Próximas investigaciones podrían explorar la integración de blockchain en la gestión de firmas digitales, evaluando como esta tecnología puede mejorar la seguridad, la trazabilidad y la confianza en los documentos electrónicos.

Es fundamental llevar a cabo artículos comparativos que evalúen la implementación de la validación de firmas digitales en diferentes tipos de instituciones educativas, tales como universidades públicas, privadas, colegios técnicos y escuelas secundarias. Estos artículos pueden identificar factores contextuales que influyen en el éxito de la implementación y proporcionar recomendaciones adaptadas a las necesidades específicas de cada tipo de institución.

La adopción de firmas digitales contribuye a la transparencia institucional al garantizar que todos los documentos emitidos por los estudiantes de la universidad son auténticos y no han sido manipulados. Esto mejora la confianza de docentes, padres y público en general en la validez de los documentos académicos, fortaleciendo la reputación de la institución.

El uso de firmas digitales desincentiva la falsificación de documentos y otros tipos de fraude académico, promoviendo un entorno de integridad y honestidad. La garantía de autenticidad y la trazabilidad de los documentos firmados digitalmente refuerzan la responsabilidad y la ética en la creación y manejo de documentos académicos. Estos aspectos contribuyen al bienestar general de la comunidad universitaria y la sociedad, posicionando a la institucion educativa como líder en la adopción de tecnologías innovadoras, en la promoción de prácticas éticas y contribuyendo con el medio ambiente.

Conclusiones

En este artículo, hemos estudiado, resumido y discutido varios esquemas y soluciones de seguridad, en base a la revisión del estado del arte en bases de datos científicas con preferencia en esquemas de autenticación, métodos de criptografía matemática, análisis de infraestructura de firma digital, algoritmos y estándares tecnológicos. De igual manera, se ha investigado la implementación de un modelo de validación de firmas y certificados digitales embebidos en documentos electrónicos generados por los estudiantes de la Universidad Católica de Cuenca, destacando sus beneficios, desafíos y el avance significativo hacia la modernización de los procesos administrativos y académicos. A través de un análisis detallado, se ha demostrado que la propuesta del modelo garantiza la autenticidad y seguridad de los documentos estudiantiles. Este sistema fortalece la confianza en la integridad de los

documentos emitidos, asegurando su validez y reduciendo riesgos de falsificación o manipulación. Además, la implementación de estas tecnologías ha demostrado mejorar la eficiencia administrativa, reducir costos operativos, contribuir a la sostenibilidad ambiental y fomentar prácticas más responsables y éticas en la gestión documental.

No obstante, para una implementación exitosa y sostenible, es importante que la institución invierta en la capacitación del personal, así como en la actualización y mantenimiento continuo de la infraestructura tecnológica. Así mismo, es recomendable seguir explorando estándares internacionales y mejores prácticas en el ámbito de la seguridad digital para asegurar la interoperabilidad y la adaptabilidad del sistema a futuros avances tecnológicos.

Referencias bibliográficas

Aggarwal, S., & Kumar, N. (2021). Digital signatures. *Advances in Computers*, *121*, 95-107. Obtenido de https://www.sciencedirect.com/science/article/abs/pii/S0065245820300590#fn9000

Aguilera Hintelholher, R. M. (2013). Identidad y diferenciación entre Método y Metodología. *Artículos Políticos*, 81-103.

Barbón Pérez, O. G., & Fernández Pino, J. W. (2018). The role of strategic educational management in knowledge management, science, technology, and innovation in higher education. *Educación médica*, *19*(1), 51-55. Obtenido de https://www.sciencedirect.com/science/article/pii/S1575181317300013

Estudillo, M. (2022, 4 de diciembre). ¿Qué es la firma electrónica avanzada y para qué sirve? Signaturit Blog. https://blog.signaturit.com/es/que-es-la-firma-electronica-avanzada

Harn, L., Ren, J., & Lin, C. (2009). Design of DL-based certificateless digital signatures. *Journal of Systems and Software*, 789-793. doi:https://doi.org/10.1016/j.jss.2008.11.844

Hsu, C. L., Chuang, Y. H., Tsai, P. L., Almari, A., & Mizanur Rahman, S. M. (2014). Design of Pairing-Based Proxy Signcryption System Model for Online Proxy Auctions. *Information Technology and Control*, 4-37. doi:http://dx.doi.org/10.5755/j01.itc.43.4.6348

Kim, J. W., Cho, H. G., & Cha, E. Y. (2005). A Study on Enhanced Dynamic Signature Verification for the Embedded System. *Brain, Vision, and Artificial Intelligence. BVAI*. Berlín: Springer. doi:https://doi.org/10.1007/11565123_42

Liu, Y., Yang, Z., & Yang, L. (2015). Online Signature Verification Based on DCT and Sparse Representation. *IEEE Transactions on Cybernetics,*, 2498-2511. doi:10.1109/TCYB.2014.2375959

Mašek, V., & Novotný, M. (2022). Versatile Hardware Framework for Elliptic Curve Cryptography. *2022 25th International Symposium on Design and Diagnostics of Electronic Circuits and Systems (DDECS)*, 80-83. doi:10.1109/DDECS54261.2022.9770143

Ortega Gamez, J., De la Cruz Maldonado, J., & Abrego Almazán, D. (2024). Aplicación de la firma digital en una institución de educación superior. *RECAI Revista De Artículos En ContaduríA, AdministracióN E InformáTica*, *13*(37), 15 - 28. doi:10.36677/recai.v13i37.22367

Palmer, A. J. (2008). Criteria to evaluate Automated Personal Identification Mechanisms. *Computers & Security*, *27*(7-8), 260-284. Obtenido de https://www.sciencedirect.com/science/article/abs/pii/S016740480800045X

Taleb, A. R., & Vergnaud, D. (2021). Speeding-up verification of digital signatures. *Journal of Computer and System Sciences*, 22-39.

Vergara da Silva, A., & Santana de Freitas, D. (2002). Wavelet-based compared to function-based on-line signature verification. *Proceedings. XV Brazilian Symposium on Computer Graphics and Image Processing* (págs. 218-225). Brazil: IEEE.

Zhang, S., Tang, F., Lin, C., & Ke, P. (2012). Provably secure Self-Certified Signature schemes with message recovery. *China Communications*, 112-119. Obtenido de https://www.scopus.com/record/display.uri?eid=2-s2.0-84872478146&origin=inward&txGid=b9ca243a1c8da18888a248624073cda2

Zuhua, S. (2009). Security of self-certified signatures. *Information Processing Letters*, 1147 1150. doi:https://doi.org/10.1016/j.ipl.2009.07.020

Conflicto de intereses:

Los autores declaran que no existe conflicto de interés posible.

Financiamiento:

No existió asistencia financiera de partes externas al presente artículo.

Nota:

El artículo no es producto de una publicación anterior.