Vol.8 No.3 (2024): Journal Scientific MQRInvestigar ISSN: 2588–0659
https://doi.org/10.56048/MQR20225.8.3.2024.1311-1323

Digital certification scheme for electronic documents at the Catholic University of Cuenca: An approach based on computer security principles

Esquema de certificación digital de documentos electrónicos en la Universidad Católica de Cuenca: Un enfoque basado en principios de seguridad informática

Autores:

Carrión-Ramírez, Patricio Renán
UNIVERSIDAD CATÓLICA DE CUENCA
Estudiante de la Unidad Académica de Posgrado Maestría en Ciberseguridad
Cuenca – Ecuador

patricio.carrion@ucacue.edu.ec

https://orcid.org/0009-0002-8707-8507

Criollo-Bonilla, Ronald Raúl
UNIVERSIDAD CATÓLICA DE CUENCA
Docente de la Unidad Académica de Posgrado Maestría en Ciberseguridad
Cuenca – Ecuador

ronald.criollo@ucacue.edu.ec

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

Fechas de recepción: 25-JUN-2024 aceptación: 17-JUL-2024 publicación:15-SEP-2024

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

Resumen

La investigación se centró en la implementación de un esquema de certificación digital de documentos electrónicos en la Universidad Católica de Cuenca, adoptando un enfoque basado en los fundamentos de seguridad informática vinculados a la Confidencialidad, Integridad y Disponibilidad (CID). Dada la creciente necesidad de mejorar estos principios en el entorno educativo moderno, la Universidad carecía de un sistema formal de certificación digital para los estudiantes, representando una oportunidad significativa para implementar un marco que garantice acceso exclusivo a personas autorizadas, preservando la integridad y disponibilidad de la documentación electrónica. La implementación de esta propuesta se basó en la adopción de tecnologías avanzadas de firma digital, fundamentadas en la infraestructura de llave pública (PKI) y la autenticación digital, con el objetivo de asegurar la legalidad e inviolabilidad de los documentos electrónicos gestionados por la institución. El uso de algoritmos hash SHA-256 y cifrado RSA (Rivest, Shamir y Adleman) proporcionó una sólida capa de seguridad para evitar la manipulación y alteración de los documentos. El modelo se desarrolló en tres fases, que incluyeron un análisis de la literatura, la selección y ajuste del modelo, y pruebas completas para evaluar posibles vulnerabilidades y escenarios de amenazas del mundo real. Este enfoque metodológico técnico aseguró la solidez del esquema y su potencial para mejorar los procesos electrónicos y la gestión de documentos en la Universidad. Este proyecto contribuye significativamente a la modernización y seguridad de la gestión documental en la Universidad Católica de Cuenca. La implementación exitosa de este plan sentará las bases para un entorno digital más seguro y confiable, alineado con las mejores prácticas para la autenticación digital y la gestión de registros electrónicos en instituciones educativas.

Palabras clave: Certificación digital; seguridad informática; Infraestructura de Llave Pública (PKI); firmas electrónicas; gestión documental

Abstract

The research focused on the implementation of a digital certification scheme for electronic documents at the Universidad Católica de Cuenca, adopting an approach based on the fundamentals of information security linked to Confidentiality, Integrity, and Availability (CIA). Given the growing need to improve these principles in the modern educational environment, the University lacked a formal digital certification system for students, representing a significant opportunity to implement a framework that guarantees exclusive access to authorized persons, preserving the integrity and availability of electronic documentation. The implementation of this proposal was based on the adoption of advanced digital signature technologies, grounded in Public Key Infrastructure (PKI) and digital authentication, with the aim of ensuring the legality and inviolability of the electronic documents managed by the institution. The use of SHA-256 hash algorithms and RSA encryption (Rivest, Shamir, and Adleman) provided a robust security layer to prevent the manipulation and alteration of documents. The model was developed in three phases, which included a literature review, the selection and adjustment of the model, and comprehensive testing to evaluate potential vulnerabilities and real-world threat scenarios. This technical methodological approach ensured the robustness of the scheme and its potential to improve electronic processes and document management at the University. This project significantly contributes to the modernization and security of document management at the Universidad Católica de Cuenca. The successful implementation of this plan will lay the foundation for a safer and more reliable digital environment, aligned with best practices for digital authentication and electronic record management in educational institutions.

Keywords: Digital certification; IT security; Public Key Infrastructure (PKI); electronic signatures; document management

Introducción

La llegada del COVID-19 ha cambiado profundamente diversas facetas de la vida cotidiana. Desde el 11 de marzo de 2019, cuando la Organización Mundial de la Salud (OMS) declaró al COVID-19 como pandemia, se ha observado un notable incremento en la adopción de herramientas tecnológicas (Cárdenas, 2023). Este fenómeno ha transformado significativamente el desarrollo de las actividades diarias, especialmente en el ámbito educativo.

La Universidad Católica de Cuenca, al igual que otras instituciones educativas, enfrenta el desafío de gestionar y almacenar documentos electrónicos de manera segura y confiable. En este contexto, la certificación digital de documentos electrónicos se presenta como un elemento crucial para asegurar la integridad y autenticidad de dichos archivos. La implementación de un certificado digital, un documento electrónico emitido por una entidad de servicios de certificación que permite identificar oficialmente al firmante del documento, es esencial para proteger datos y establecer conexiones de red seguras (López y Orozco, 2018).

La integridad de los datos es un aspecto fundamental para la confiabilidad de los sistemas informáticos. Es imperativo implementar medidas de seguridad que protejan los datos y prevengan cualquier alteración no autorizada. Además, la disponibilidad de los datos es crucial para el correcto funcionamiento de estos sistemas (de la Mata Barranco, 2016). Paralelamente, la confidencialidad, definida por la Organización Internacional de Estandarización (ISO) en la norma ISO/IEC 27002, se refiere a "garantizar que la información sea accesible solo para aquellos autorizados a tener acceso" (Gil Yacobazzo et al., 2018). Finalmente, la disponibilidad implica la capacidad de acceder a la información, sistemas o recursos cuando sea necesario (Polanco Puerta y Presencial, 2023).

En este contexto, la propuesta de un esquema de firmas digitales para la certificación y dictamen de información electrónica podría ser una solución efectiva. Actualmente, la información que circula por internet está sujeta a diversas vulnerabilidades, lo que genera desconfianza en el uso de medios electrónicos para la gestión de documentos (Flórez y Gutiérrez, 2012). La Universidad Católica carece de un esquema de certificación digital de documentos electrónicos, lo que ocasiona problemas de credibilidad, confiabilidad, seguridad y privacidad. La ausencia de estándares y procesos de control rigurosos contribuye a la ineficiencia de los procesos manuales.

El objetivo principal de este trabajo investigativo es establecer un marco de referencia para prevenir el fraude y asegurar la integridad de la información mediante la implementación de

un esquema de certificación que permita emitir firmas digitales para los estudiantes. El uso de códigos QR en certificados digitales puede mejorar significativamente la seguridad y facilidad de verificación (Curo, 2022). Además, la integración de firmas electrónicas avanzadas, el empleo de Infraestructura de Clave Pública (PKI) y la adherencia a estándares como el X.509 para la generación de certificados, serán componentes clave del esquema de certificación propuesto.

Desde una perspectiva operativa, se propone desarrollar un sistema de autenticación digital en un sistema de gestión documental, con vistas a integrarlo en el futuro a la plataforma web de la Universidad. No obstante, se anticipan desafíos relacionados con la usabilidad y la capacitación de los usuarios, que serán cruciales para la adopción exitosa del modelo planteado.

Metodología

La investigación surgió a través de la metodología de Infraestructura de Llave Pública (PKI), la cual se basa en la gestión y distribución de claves públicas por parte de una Autoridad Certificadora (AC). Este enfoque funciona bajo un modelo de confianza, donde los usuarios confían en que las claves públicas administradas por la PKI son auténticas y pertenecen a las entidades correctas. La metodología se dividió en tres fases, siguiendo las normas ISO/IEC 27001, para llevar un control riguroso del comportamiento del modelo.

En la primera fase, se contempló un análisis de la literatura, utilizando como base fundamental los algoritmos hash SHA-256. Este algoritmo funciona dividiendo los datos de entrada en bloques de 512 bits, cada uno procesado en 64 rondas de operaciones. Estas operaciones incluyeron funciones lógicas bitwise como AND, OR, XOR, así como adición y rotación bitwise. El resultado fue un valor hash único que representó los datos originales.

Asimismo, se analizaron métodos de encriptación RSA, un método asimétrico que emplea dos claves diferentes para cifrar y descifrar. La llave pública se compartió para la encriptación mientras que la llave privada se utilizó para la desencriptación. Este estudio permitió la vinculación de mejores prácticas y proporcionó una perspectiva técnica eficaz para la implementación.

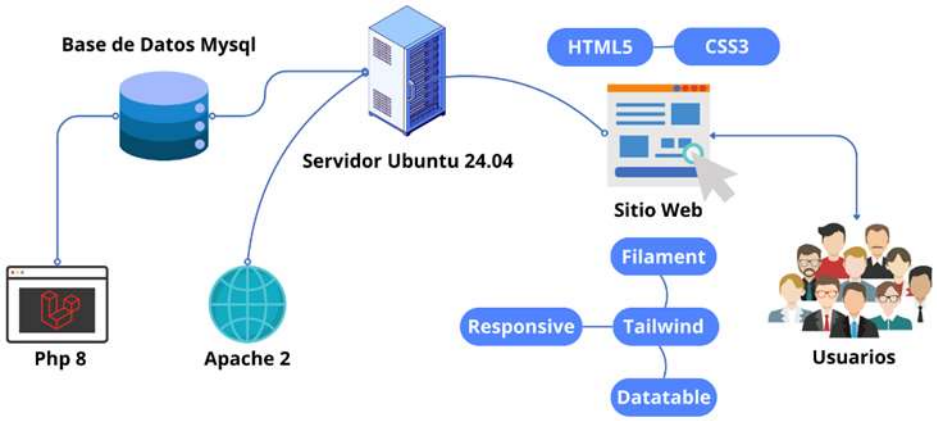
En la segunda fase del proyecto, el objetivo principal fue la selección y ajuste del modelo para la generación de los certificados digitales para los estudiantes de la institución y para la CA (entidad certificadora). Se obtuvieron los archivos ca.crt (certificado de la CA) y private.key (llave privada de la CA). Esto comprendió la evaluación del método RSA 4096

de encriptación utilizando la herramienta OpenSSL, la cual crea la llave pública y privada para autenticar y cifrar la comunicación.

Luego, se diseñó y desarrolló un prototipo funcional del esquema de generación de certificados utilizando el sistema operativo Ubuntu 24.04 LTS. Para el frontend, se empleó Filament PHP y sus componentes como Datatables y Tailwind, mientras que para el backend se implementaron Apache 2, PHP 8 y MySQL 8, como se observa en la Figura 1.

Figura 1

Prototipo propuesto del esquema.



Nota: La figura muestra el prototipo propuesto para el esquema del proyecto. Fuente: Elaboración propia.

Incorporamos las pruebas de la firma digital en documentos electrónicos con el software Adobe PDF Reader en un entorno controlado para garantizar la integridad del proceso. Se escogieron estas plataformas de desarrollo porque sus licencias permiten generar código abierto y no están sujetas a ninguna obligación con terceros.

En la tercera fase, se realizaron pruebas completas del primer modelo planteado. Se abordó el análisis de posibles vulnerabilidades utilizando la herramienta Kali Linux. Se efectuaron ataques de denegación de servicios que afectaron la disponibilidad del sitio web, ataques de phishing que perjudicaron la confidencialidad, y ataques de fuerza bruta para acceder a las credenciales de un usuario que comprometieron la integridad de la base de datos. Esto permitió analizar la fortaleza del diseño ante ciberataques.

Este enfoque metodológico técnico aseguró la solidez del esquema formulado y su capacidad para fortalecer la seguridad en los procesos electrónicos, potenciando la gestión de documentos digitales en la Universidad Católica de Cuenca. El tipo de investigación fue

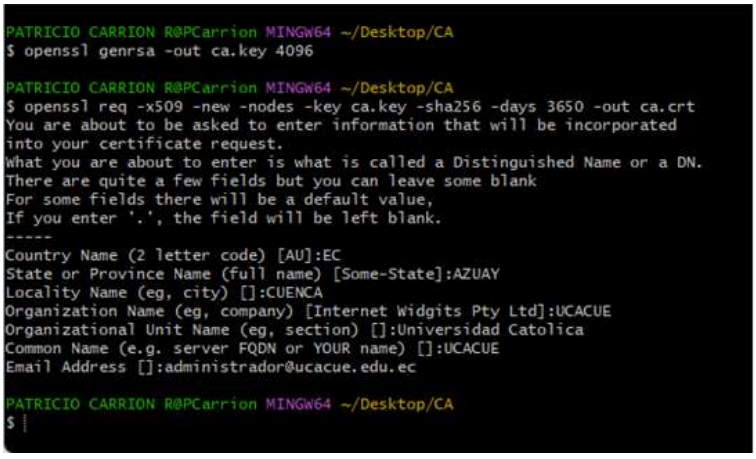
descriptivo, centrándose en una descripción detallada y completa del esquema de generación de certificados y su impacto en la confidencialidad, integridad y disponibilidad de la información.

Resultados

Lo primero que se realizó fue generar, con la herramienta OpenSSL previamente instalada en la máquina Ubuntu donde está implementado el sitio web, el certificado auto-firmada raíz de la Autoridad Certificadora (CA), cuya validez es de diez años. Una vez que expire, todos los certificados firmados por la CA dejarán de ser válidos, ver Figura 2.

Figura 2

Generación del certificado raíz de la CA.



Nota: La figura muestra la generación del certificado raíz de la Autoridad Certificadora. Fuente: Elaboración propia.

Los comandos utilizados para generar la llave privada y el certificado raíz auto-firmado de la CA fueron los siguientes:

```
openssl genrsa -out ca.key 4096
openssl req -x509 -new -nodes -key ca.key -sha256 -days 3650 -out ca.crt
```

Una vez obtenidos los dos archivos, ca.crt (certificado) y ca.key (clave privada) de la CA, el siguiente paso fue trasladarlos al directorio en donde está desplegado el servidor web y de base de datos encargado de la aplicación. Estos archivos deben ser almacenados cuidadosamente. El ingreso a la aplicación se realiza a través de la dirección http://localhost:8000/dashboard/login, donde el estudiante debe autenticarse o registrarse para poder acceder, como se observa en la Figura 3.

Figura 3

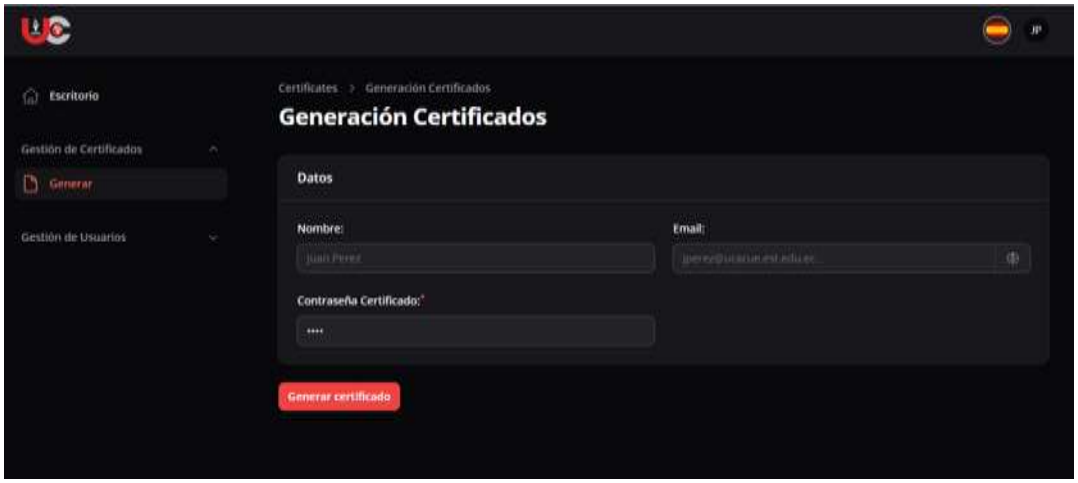
Formulario login.

Fuente: Elaboración propia.

Una vez autenticado en el sitio web, el usuario puede generar su certificado digital. Si aún no lo ha hecho, se le solicita una clave y puede descargar el certificado, el cual le permitirá firmar documentos electrónicos. La duración de su firma digital dependerá de la duración de su carrera académica. Este proceso de obtención del certificado puede realizarse una sola vez mientras dure su vigencia. Si necesita generarlo nuevamente, debe solicitar la baja del certificado anterior a la CA, como se observa en la Figura 4.

Figura 4

Generación de certificados para los estudiantes.



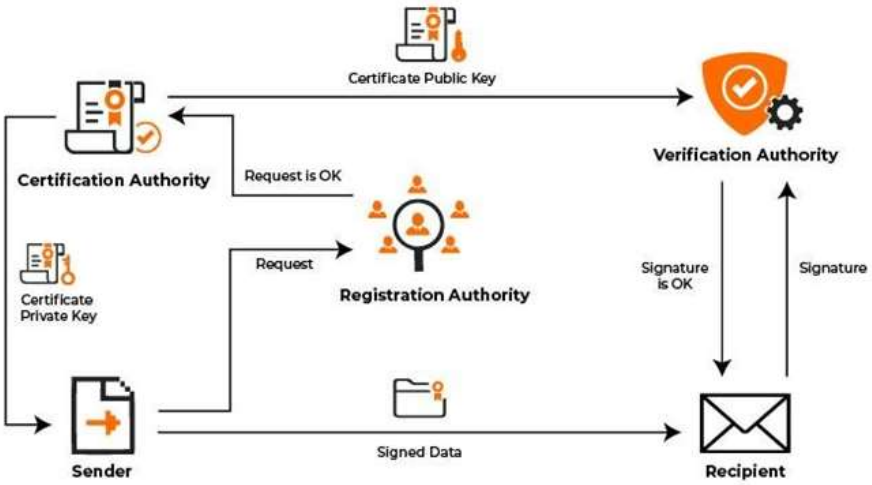
Fuente: Elaboración propia.

La importancia de una PKI radica en los algoritmos criptográficos que utiliza para asegurar que la información esté protegida ante cualquier amenaza externa. Además, provee

certificados digitales que otorgan identidad a personas naturales u organizaciones (Ramos Rafael, 2018). La infraestructura de la llave pública se presenta en la Figura 5.

Figura 5

Infraestructura de llave pública PKI.



Fuente: https://www.iebschool.com/blog/herramientas-ciberseguridad-digital-business/.

Discusión

La investigación realizada reveló hallazgos significativos, entre los cuales destaca que la firma electrónica mediante la generación de certificados digitales garantiza la identidad de una persona. Esto se logra al vincular la clave pública con los datos que ratifican al dueño del certificado. El esquema PKI, que asegura las comunicaciones y protege los datos de accesos no autorizados, es fundamental para evitar el repudio.

Uno de los beneficios principales observados fue la reducción significativa de tiempo para acceder a servicios, eliminando la necesidad de traslados e interacción con personal administrativo. Este sistema en línea permite a los estudiantes obtener sus credenciales digitales válidas para trámites universitarios, garantizando la confidencialidad, disponibilidad e integridad de la información.

La firma digital, como técnica segura de firma electrónica, permite identificar fehacientemente al firmante del documento electrónico, garantizando la autenticación, integridad y no repudio del documento firmado. Este método proporciona una forma segura y verificable de manifestar la voluntad mediante medios electrónicos (Irigoitia, 2016).
Un certificado digital es un documento identificativo que vincula a una persona o equipo con una clave pública, la cual está matemáticamente relacionada con una clave privada. La clave

pública se utiliza para el cifrado de información y la verificación de la firma digital, mientras que la clave privada realiza las operaciones opuestas (Francisco Javier Castro Martínez Supervisor y René Fuentes Cortez, 2015).

La infraestructura de clave pública (PKI) se define como el conjunto de hardware, software, personas, políticas y procedimientos necesarios para crear, administrar, almacenar, distribuir y revocar certificados de clave pública basados en criptografía de clave pública. Es un conjunto de protocolos, servicios y estándares que soportan aplicaciones basadas en criptografía de clave pública (Francisco Javier Castro Martínez Supervisor y René Fuentes Cortez, 2015).
La integración del algoritmo SHA-256 en el esquema fue uno de los pilares fundamentales, ya que aumenta la seguridad de la comunicación. El cifrado de dos claves es un método que utiliza un par de claves para enviar mensajes; una clave es pública y puede ser entregada a cualquier persona, mientras que la otra es privada y debe ser conservada por el propietario para evitar accesos no autorizados (Arévalo Rodríguez et al., 2022).

El cifrado RSA, basado en la dificultad para factorizar grandes números, también fue crucial. Las claves pública y privada se calculan a partir de un número producto de dos primos grandes, lo que complica significativamente los intentos de recuperación del texto claro a partir del criptograma y la clave pública, enfrentando al atacante a un problema de factorización o a la resolución de un logaritmo discreto (Cabrera Jara, 2018).

Estos hallazgos y aplicaciones metodológicas demuestran la solidez y efectividad del esquema de certificación digital implementado, contribuyendo significativamente a la modernización y seguridad de la gestión documental en la Universidad Católica de Cuenca. La implementación exitosa de este sistema sentará las bases para un entorno digital más seguro y confiable, alineado con las mejores prácticas para la autenticación digital y la gestión de registros electrónicos en instituciones educativas.

Conclusiones

La implementación de un esquema de certificación digital de documentos electrónicos que se basa en los principios de Confidencialidad, Integridad y Disponibilidad (CID) ha demostrado ser un avance significativo en la modernización y seguridad de la gestión documental de la Universidad Católica de Cuenca. El proyecto ha asegurado la inviolabilidad y autenticidad de los documentos electrónicos mediante el uso de algoritmos de hash SHA-256 y cifrado RSA, utilizando tecnologías avanzadas de firma digital e infraestructura de llave pública (PKI).

Un enfoque metodológico riguroso que permitió identificar y mitigar posibles vulnerabilidades y amenazas fue garantizado por el desarrollo del modelo en tres fases: análisis de la literatura, selección y ajuste del modelo, y pruebas completas. La implementación exitosa de este esquema no solo mejora los procedimientos electrónicos de la universidad, sino que también establece un precedente para la adopción de mejores prácticas de autenticación digital y gestión de registros electrónicos en la educación.

Finalmente, este proyecto ayuda a la Universidad Católica de Cuenca a crear un entorno digital más seguro y confiable. Esto se ajusta a las demandas de la era digital y las expectativas de seguridad contemporáneas.

Referencias bibliográficas

Arévalo Rodríguez, A. S., Hurtado Gómez, D. M., y Galindo Sierra, G. J. (2022). Algoritmo internacional de cifrado de datos (IDEA) que utiliza la variante de cifrado SHA-256. Revista Vínculos: Ciencia, tecnología y sociedad, ISSN 1794-211X, ISSN-e 2322-939X, Vol. 19, No. 2, 2022, 19(2), 3. https://dialnet.unirioja.es/servlet/articulo?codigo=9020213yinfo=resumenyidioma=SPA

Cabrera Jara, H. J. (2018). Estudio comparativo de los algoritmos de encriptación advanced encryption standard (aes) y rivest, shamir & adleman (rsa). Universidad Nacional Jorge Basadre Grohmann. https://repositorio.unjbg.edu.pe/handle/20.500.12510/1870

Arévalo Rodríguez, A. S., Hurtado Gómez, D. M., y Galindo Sierra, G. J. (2022). Algoritmo internacional de cifrado de datos (IDEA) que utiliza la variante de cifrado SHA-256. Revista Vínculos: Ciencia, tecnología y sociedad, ISSN 1794-211X, ISSN-e 2322-939X, Vol. 19, No. 2, 2022, 19(2), 3. https://dialnet.unirioja.es/servlet/articulo?codigo=9020213yinfo=resumenyidioma=SPA

Cabrera Jara, H. J. (2018). Estudio comparativo de los algoritmos de encriptación advanced encryption standard (aes) y rivest, shamir & adleman (rsa). Universidad *Nacional* Jorge Basadre Grohmann. https://repositorio.unjbg.edu.pe/handle/20.500.12510/1870

Cárdenas, J. S. (2023). La firma electrónica y la seguridad digital en los certificados de vigencia de poder emitidos por la Oficina Registral de Andahuaylas, 2022. https://repositorio.ucv.edu.pe/handle/20.500.12692/115584

Curo, G. G. (2022). Certificación Digital con QR. https://api.semanticscholar.org/CorpusID:252085053

de la Mata Barranco, N. J. (2016). Los delitos contra la integridad y disponibilidad de datos y sistemas informáticos después de la LO 1/2015. https://api.semanticscholar.org/CorpusID:186154510

Flórez, E. E. I., y Gutiérrez, J. L. M. (2012). CERTIFICACIÓN Y DICTAMEN DIGITAL: UNA ALTERNATIVA PARA GENERAR CONFIANZA EN LA INFORMACIÓN CONTABLE ELECTRÓNICA. https://api.semanticscholar.org/CorpusID:170450391

Gil Yacobazzo, J. E., Viega Rodríguez, M. J., Gil Yacobazzo, J. E., y Viega Rodríguez, M. J. (2018). Historia clínica electrónica: confidencialidad y privacidad de los datos clínicos. Revista Médica del Uruguay, 34(4), 102-119. https://doi.org/10.29193/RMU.34.4.6

López, D. S., y Orozco, C. (2018). Digital de documentos PDF en dispositivos con sistema operativo android. https://api.semanticscholar.org/CorpusID:165270767

Polanco Puerta, E. R., y Presencial. (2023). La Relevancia de la Seguridad de la Información y Ciberseguridad en el Gobierno de los Datos. http://repository.unipiloto.edu.co/handle/20.500.12277/13077

Ramos Rafael, E. D. (2018). Propuesta de una infraestructura de clave pública para el uso de cifrado y firma digital en los mensajes de correo electrónico de un servicio basado en Office 365. Universidad Peruana de Ciencias Aplicadas (UPC). https://doi.org/10.19083/tesis/624169

Conflicto de intereses:

Los autores declaran que no existe conflicto de interés posible.

Financiamiento:

No existió asistencia financiera de partes externas al presente artículo.

Agradecimiento:

N/A

Nota:

El artículo no es producto de una publicación anterior.