REVISTA CUBANA
DE TRANSFORMACIÓN DIGITAL

RNPS 2487 • ISSN 2708-3411
Vol. 5 • Nro. 1 • ene-mar 2024 • e247

ESTUDIO DE CASO

Experiencias de firma digital en la Empresa de Tecnologías de la Información para la Defensa

Digital signature experiences in the Defense Information Technology Company

Jessica Ruiz Hernández
jessica.ruiz@uic.cu • https://orcid.org/0000-0002-4475-0474

EMPRESA DE TECNOLOGÍAS DE LA INFORMACIÓN PARA LA DEFENSA

Recibido: 2023-11-11 • Aceptado: 2024-02-20

RESUMEN

En esta investigación se explora la utilización de la firma digital, la cual constituye una solución tecnológica que utiliza técnicas matemáticas para validar la autenticidad e integridad de un mensaje, software o documento digital. Es una tecnología novedosa aún para el país, aunque en los últimos años ha crecido su uso sobre todo en el sector de la economía y el Gobierno. Sin embargo, a pesar del auge que ha tenido se debe crear una cultura alrededor del tema. Existe desconocimiento de su uso por parte de los usuarios, así como la seguridad que aporta y la importancia que representa para garantizar la validez de un documento digital. En este trabajo se caracterizó el proceso de gestión de la firma digital, tomando como ejemplo el Prestador de Servicios Criptográficos de Certificación, de la empresa XETID. Se realizaron entrevistas a directivos y expertos del tema, y encuestas a usuarios que solicitan el servicio de emisión de certificados digitales, obteniendo determinados elementos que ayudarán a mejorar el servicio y fomentar la cultura sobre firma digital en el país. Para impulsar el uso de esta tecnología se hace necesario trazar acciones que permitan incentivar su utilización y resalten su importancia para garantizar la seguridad de la información que se comparte en las plataformas digitales.

Palabras clave: acciones, capacitación, desconocimiento, firma digital, seguridad.

ABSTRACT

In this research, the use of the digital signature is explored, which constitutes a technological solution that uses mathematical techniques to validate the authenticity and integrity of a message, software or digital document. It is still a new technology for the country, although in recent years its use has grown, especially in the economy and government sector. However, despite the boom it has had, a culture must be created around the subject. There is ignorance on the part of the users, of its use, the security it provides and the importance it represents to

guarantee the validity of a digital document. In the work, the digital signature management process was characterized, taking as an example the Cryptographic Certification Services Provider of the company XETID. Interviews were conducted with managers and experts on the subject; and surveys of users who request the digital certificate issuance service, obtaining certain elements that will help improve the service and promote the culture of digital signatures in the country. To promote the use of this technology, it is necessary to draw up actions that encourage its use and highlight its importance to guarantee the security of the information that is shared on digital platforms.

Keywords: actions, training, ignorance, digital signature, security.

INTRODUCCIÓN

Los certificados digitales desempeñan un papel fundamental en la gestión de la seguridad de la información en la era digital. Feghhi et al. (1999), Fritscher (1999), Rao et al. (2017) y Sensuse et al. (2020) señalan en estudios relacionados con los certificados digitales, que estos son un componente esencial para garantizar la autenticidad de las transacciones electrónicas, establecer relaciones de confianza en entornos en línea y proteger la integridad de los datos. Los certificados digitales permiten verificar la identidad de los participantes en una comunicación electrónica, verificar la autenticidad de los sitios web y asegurar que la información trasmitida no haya sido alterada durante el proceso. Permiten cifrar esa información, garantizando su confidencialidad.

El tema de la investigación requiere que se traten inicialmente algunos conceptos fundamentales para llegar a una completa comprensión, de manera que se abordarán las definiciones de firma digital, certificado digital y Prestador de Servicios Criptográficos de Certificación.

El Ministerio del Interior (Minint), en la Resolución 2 de 2016, define la firma digital como un valor numérico que se adhiere a un mensaje o documento y que se obtiene mediante un procedimiento matemático conocido, vinculado a la llave privada del suscriptor iniciador de una comunicación y al texto del mensaje, para permitir determinar que este valor se ha obtenido exclusivamente con esa llave privada (secreta) del iniciador, y que el mensaje inicial no ha sido modificado después de efectuada la transformación (Minint, 2016).

De igual forma, plantea que el Certificado Digital de Llave Pública Reconocido es un archivo o documento electrónico, mediante el cual una autoridad de certificación garantiza el vínculo entre la identidad de un sujeto o entidad y una llave criptográfica pública. Se expide y firma digitalmente por una autoridad de certificación, aprobada para operar en la infraestructura, cuyo certificado digital (el de la autoridad) está firmado por la Autoridad Raíz (Minint, 2016). En 2018, el Decreto-Ley 370, en su artículo 31, reconoce la validez del empleo de los certificados digitales para firmar documentos legales, con plena eficacia por las autoridades y funcionarios públicos a todos los efectos procedentes (Minjus, 2019).

El Prestador de Servicios Criptográficos de Certificación (PSCC) se define como la persona jurídica que presta servicios criptográficos y expide certificados digitales para su utilización en la creación y verificación de la firma digital y el establecimiento de canales de comunicaciones seguros (Minint, 2016).

La base legal es explícita en cuanto a los principales conceptos, disposiciones y orientaciones necesarias, para garantizar la distribución de los certificados digitales de forma segura. Sin embargo, es una documentación extensa y abarcadora, y a pesar de ser los ministerios de Comunicaciones y del Interior los encargados de la preparación de un Plan de Divulgación Y Capacitación sobre la firma digital en Cuba (Minjus, 2022), también recae en los PSCC la tarea de capacitar al personal que solicita el servicio y crear estrategias para que la información llegue de forma clara y precisa. En el país existen varias entidades reconocidas por el Ministerio del Interior, que están autorizadas a brindar el servicio de emisión de certificados digitales (Rodríguez, 2023). Este trabajo se apoyó en la empresa XETID, para caracterizar el servicio de emisión de certificados digitales (ACX, 2022), ver las principales limitaciones que existen para generalizar el uso de la firma digital a todos los ciudadanos, proponer acciones que permitan incentivar su utilización y resaltar su importancia para garantizar la seguridad de la información que se comparte en las plataformas digitales.

METODOLOGÍA

En la realización de este caso de estudio se revisaron leyes, decretos, acuerdos y normas, que se establecen en el país para el uso de los certificados digitales. Se analizó detalladamente el proceso de gestión del certificado digital que realiza la empresa XETID para sus clientes. Se realizaron entrevistas a directivos y especialistas en la Infraestructura de Llave Pública y encuestas a usuarios que solicitan el servicio.

Análisis de documentos

Se empleó el método de revisión bibliográfica centrado en el impulso que se le desea dar al empleo de la firma digital en el país; además, se consultaron artículos de sitios oficiales donde se ofrece una información más clara y concreta de los avances que ha tenido esta tecnología en Cuba, sus principales usos y usuarios. El estudio de la base legal permite centrarse en los objetivos del país, con respecto a la firma digital y la informatización de la sociedad, y trazar medidas concretas acordes a las necesidades existentes y las proyecciones futuras, las cuales representan una guía para informarnos e informar a los clientes sobre estos temas.

Proceso de gestión de certificados digitales en la empresa XETID

Se utilizó el método de observación en las fases del proceso de gestión de certificados digitales en la empresa XETID. Se analizó el proceso de contratación del servicio de emisión de certificados digitales; se examinó el correo de ACX como fuente principal de recepción de solicitudes; se observó el tratamiento que se le da a cada solicitud y se analizaron los principales problemas que enfrentan los usuarios al descargar los certificados. La caracterización de este proceso permite concretar dónde se encuentran las debilidades y fortalezas del servicio, posibilitando que se tracen acciones para mejorarlo.

Entrevistas y encuestas

Se realizaron entrevistas a directivos y especialistas que trabajan en el desarrollo y la administración de ACX. Se realizaron encuestas a algunos usuarios; se mantuvo el anonimato del encuestado para garantizar la confidencialidad de la respuesta y se utilizó una escala tipo Likert con cinco opciones de respuesta: Siempre (5), La mayoría del tiempo (4), A veces (3), Casi nunca (2), Nunca (1).

RESULTADOS Y DISCUSIÓN

Análisis de documentos

En la Resolución 2 de 2016, del Ministerio del Interior (Minint), se consultaron los principales conceptos referentes a la firma digital y se revisó el procedimiento establecido para la solicitud y el otorgamiento de los certificados digitales de llave pública. En la Resolución se establecen las reglas y obligaciones que deben seguir usuarios, PSCC y autoridades de Registro y Certificación (Minint, 2016).

En el Decreto-Ley 370 de 2018 se promueve el uso de las TIC a todos los niveles, incentivando su desarrollo y estableciendo las competencias del Ministerio de Comunicaciones (Mincom) y de los órganos, organismos y entidades nacionales del Estado y del Gobierno, en el proceso de informatización de la sociedad. Además, en él se reconoce la validez de documentos en formato digital firmados electrónicamente con el empleo de certificados digitales de la Infraestructura Nacional de Llave Pública (Minjus, 2019).

El Decreto N° 360 de 2019 establece las premisas de la seguridad de las TIC para la informatización de la sociedad y la defensa del ciberespacio nacional, y define la estrategia y planificación del sistema de seguridad de las TIC, los organismos responsables, los requerimientos para el empleo seguro de las TIC y las entidades encargadas de la capacitación y divulgación sobre la seguridad de las TIC (Consejo de Ministros, 2019).

La Declaración de Prácticas de Certificación de la ACX «[…] detalla las normas y condiciones generales de los servicios de certificación que presta ACX […], constituye el compendio general de normas aplicables a toda actividad de ACX como Prestador de Servicios de Certificación» (XETID, 2020).

La Resolución 23 de 2022 establece reglas generales para el establecimiento y empleo de los servicios de firma digital de documentos electrónicos basados en dispositivos y técnicas criptográficas, y declara los responsables de la calidad y efectividad del despliegue, el uso, el perfeccionamiento y la seguridad de los servicios de firma digital de documentos electrónicos (Minjus, 2022).

Proceso de gestión de certificados digitales en la empresa XETID

Tomando en cuenta las normativas y los documentos rectores de la firma digital en Cuba, que definen cómo debe estar conformada la autoridad certificadora y las obligaciones que tiene, y la experiencia de la autora en el trabajo en ACX, a continuación, se muestra el proceso de gestión de certificados en la empresa XETID, a partir del cual se definen las debilidades y fortalezas del servicio.

Antes de enviar la solicitud, el cliente debe tener firmado un contrato de prestación de servicios con la empresa XETID, donde se establece la relación contractual con el prestador (ACX) (XETID, 2022). En el contrato se establecen las características del servicio. Es importante establecer en el Anexo 1 los Representantes Legales (RL) que serán los autorizados a solicitar la emisión, renovación o revocación de los certificados digitales. Una vez firmado el contrato, el usuario podrá enviar la solicitud al correo: acxetid@xetid.cu donde será analizada la solicitud.

El proceso de emisión concluye con el envío a los usuarios de un correo de notificación con las credenciales (usuario y contraseña) para descargar el certificado digital en la página de ACX (XETID, s.f.). En la tabla 1 se recogen fases, fortalezas y debilidades del proceso de gestión de solicitud de emisión de certificados digitales.

Tabla 1. Fases, fortalezas y debilidades del proceso de gestión de solicitud de emisión de certificados digitales

Fases	Fortalezas	Debilidades
Contratación	• El contrato se encuentra disponible en la página certificados.xetid.cu. • En el contrato puede definir tantos RL como desee. • Especialistas comerciales con total disposición y preparación para asesorar este proceso.	• Los clientes no definen los RL en el Anexo 1. • No se gestiona el Suplemento de los contratos cuando hay cambios en los RL. • Demora en la gestión de Suplementos.
Solicitud	• La solicitud puede ser enviada por correo electrónico. • Correo acxetid@xetid.cu puede recibir solicitudes desde cualquier dominio. • La planilla de solicitud es un PDF modificable (cuestionario).	• Datos del representante legal incorrecto. • Tiempo de validez no definido. • Datos de los usuarios incorrectos. • Usuarios con el mismo correo. • Planilla de solicitud sin firmar. • No se precisa el número de contrato.
Procesamiento de la solicitud	• Menos de 72 horas. • Se les da seguimiento a las solicitudes hasta lograr procesarlas. • Se le notifica al representante legal en caso de haber rebotado algún correo de notificación de sus usuarios. • En caso de algún error por parte del personal que procesa las solicitudes se corrige inmediatamente. • El correo acxetid@xetid.cu tiene alcance internacional.	• En caso de fallas eléctricas se detiene el servicio. • Si el servidor de correo tiene problemas, no le llegan las notificaciones al usuario. • Los usuarios envían una dirección de correo incorrecta (correo rebotado). • El correo del usuario está lleno (correo rebotado). • Errores al transcribir datos.
Descarga del certificado digital	• La descarga y validación a través de Internet. • Las credenciales para descargar el certificado digital se envían por correo electrónico. • La contraseña enviada es única y la genera automáticamente el servidor, solo el usuario tiene acceso a ella. • En el sitio certificados.xetid.cu está disponible una herramienta para cambiar la contraseña del certificado una vez descargado.	• El usuario intenta descargar más de una vez el certificado con las mismas credenciales • Problemas de conexión con el servidor, cambia el estado del certificado, pero no devuelve el fichero PKCS#12. • El usuario utiliza una contraseña incorrecta para descargar el certificado.

(**Fuente**: elaboración propia)

De los problemas encontrados en las fases de contratación y solicitud se deriva que se debe reforzar la asesoría a los clientes que deseen el servicio, para que el llenado del contrato y la planilla de solicitud tengan la menor cantidad de errores. Además, deben leerse los términos del contrato y la Declaración de Prácticas de Certificación de ACX para conocer las particularidades del servicio y las condiciones que deben cumplir para llenar correctamente la planilla de solicitud.

En la fase de procesamiento de la solicitud, los problemas encontrados están dirigidos a que el usuario no recibe el correo de notificación, ya sea por problemas de conexión en el servidor o por errores en el correo de los usuarios y en pocos casos por errores cometidos por la autoridad de registro en el momento de transcribir los datos de los usuarios, de modo que para evitar estos errores, el prestador debe asegurarse de contar con la conexión óptima antes de emitir los certificados digitales y el cliente debe cerciorarse de estar mandando los datos correctos para que sean procesados.

En la fase de descarga del certificado, el error más común es una consecuencia del incorrecto manejo y cuidado del certificado digital: el usuario no custodia correctamente el contenedor criptográfico y cuando necesita firmar algún documento vuelve a intentar descargarlo, lo cual no es posible. En ese punto, el representante legal debe solicitar la renovación de este certificado. Por ello, es de vital importancia que el usuario proteja su certificado digital y la contraseña para su utilización.

Entrevistas

Las entrevistas estuvieron dirigidas a los directivos y el personal que administra la autoridad de certificación ACX. Se entrevistaron cinco compañeros, dos de ellos con más de 5 años de experiencia como administradores de la autoridad de certificación. El resultado de las entrevistas se resume así:

- Desconocimiento del uso de la firma digital. No existe una cultura fomentada en el tema.
- Se desconoce la seguridad que aporta a los documentos digitales.
- Poca protección del PKCS#12, y en ocasiones se comparte la contraseña.
- Existen aún procesos en las empresas que obligan a tener documentos impresos guardados (una vez impreso el documento firmado digitalmente, la firma pierde totalmente su sentido).
- Desconfianza en un documento si no ven plasmada la imagen de la firma digital.
- Existe poco personal capacitado para llevar a cabo un uso masivo de la firma digital.
- Se debe elevar la propaganda del tema, para incentivar su uso y mostrar las ventajas.
- Se deben crear los procesos que exijan a las personas naturales el uso de la firma digital.
- Es necesario que cada usuario posea un correo electrónico.
- Se debe garantizar la capacitación de los usuarios y las autoridades de registro.
- Los administradores de la AC deben estar en constante actualización y desarrollo.
- Se debe trabajar en la automatización de algunos de los procesos para mejorar en eficiencia al procesar las solicitudes.

Las entrevistas evidencian que la capacitación es un elemento fundamental para lograr un uso correcto de la firma digital en el país. El desconocimiento, las violaciones de las políticas de seguridad y el arraigo a viejas costumbres, son de los principales problemas que debemos enfrentar y corregir para que la firma digital se posicione como el elemento esencial para garantizar la autenticación, integridad y no repudio de los documentos que se comparten en el entorno digital.

Encuesta

Para la elaboración de la encuesta, se fijó el objetivo de valorar cómo se manifiesta la variable «uso de la firma digital» en una muestra de los usuarios de la autoridad certificadora ACX. En la construcción de este instrumento se hizo énfasis en que las preguntas exploraran la calidad del servicio que ofrece ACX, la asesoría que se les da a los usuarios ante dudas, problemas o reclamaciones y la capacitación que deben recibir tanto los usuarios como el prestador.

Valoración del instrumento

El contenido del instrumento se basó en la incorporación de enunciados enfocados en la valoración del uso de la firma en los usuarios del prestador de servicios de certificación ACX. En el momento de la percepción, se encontraban junto a los usuarios el personal perteneciente a la empresa XETID que realiza la asesoría y el acompañamiento durante el despliegue de la firma digital. Se les aplicó la encuesta a treinta usuarios. Se empleó el análisis de promedio para exponer los resultados. El correcto uso de los certificados digitales está influenciado por múltiples factores, entre los que se destacan la preparación que posee el personal que capacita y orienta sobre la utilización de la firma digital durante la implementación de esta tecnología en las diferentes entidades. En este sentido, influyen las cualidades del capacitador y otros trabajadores conocedores del tema con los que interactúa el usuario a diario. La aplicación del instrumento «Valoración del uso de la firma digital» a los usuarios seleccionados, permitió recolectar datos referentes a la percepción (criterios de satisfacción) que tienen los usuarios sobre el servicio de emisión de certificados digitales de la empresa XETID. En la tabla 2 y la figura 1 se presentan los resultados.

Tabla 2. Percepción de los usuarios acerca del uso de la firma digital

N°	Dimensiones	Indicadores	Evaluación promedio por indicadores	Evaluación promedio de la dimensión
1.	**Calidad del Servicio**	¿Con qué frecuencia está disponible el servicio?	4.1	3.78
2.		¿Le llega sin errores el certificado emitido?	4.5	
3.		¿Puede descargar el certificado satisfactoriamente?	3.2	
4.		¿Puede validar el certificado satisfactoriamente?	4	
5.		¿Es atendida su solicitud inmediatamente?	3.1	
6.	**Asesoría**	¿Recibe correcta atención ante dudas?	4.5	4.05
7.		¿Recibe correcta atención ante reclamaciones?	3.4	
8.		¿Recibe atención ante problemas con la descarga de los certificados digitales?	4	
9.		¿Recibe atención ante problemas con la configuración de los lectores PDF o sistemas donde gestiona la firma de documentos?	4.3	
10.	**Capacitación**	¿Recibe un curso previo al uso de la firma digital?	2.5	2.97
11.		¿Considera que debe recibir una capacitación sobre el uso de la firma digital?	3	
12.		¿Reconoce la importancia de la firma digital?	3.2	
13.		¿Con que frecuencia configura usted solo la firma digital?	2	
14.		¿Está preparado para la configuración y utilización de la firma digital?	3.1	

N°	Dimensiones	Indicadores	Evaluación promedio por indicadores	Evaluación promedio de la dimensión
15.		¿Considera que el personal de XETID está preparado para orientar sobre la configuración y utilización de la firma digital?	4	
16.	**Protección del certificado digital**	¿Reconoce los riesgos de violar las políticas de seguridad sobre el cuidado de la firma digital?	2.9	2.3
17.		¿Resguarda la contraseña de su certificado digital de forma segura?	2	
18.		¿Mantiene en secreto su contraseña?	3	
19.		¿Cambia la contraseña de su certificado digital una vez lo descarga?	1.2	
20.		¿Comprueba la validez de la firma digital en los documentos que recibe?	2.3	
21.		¿Reconoce cuándo un documento está firmado digitalmente?	2.4	

(Fuente: elaboración propia)

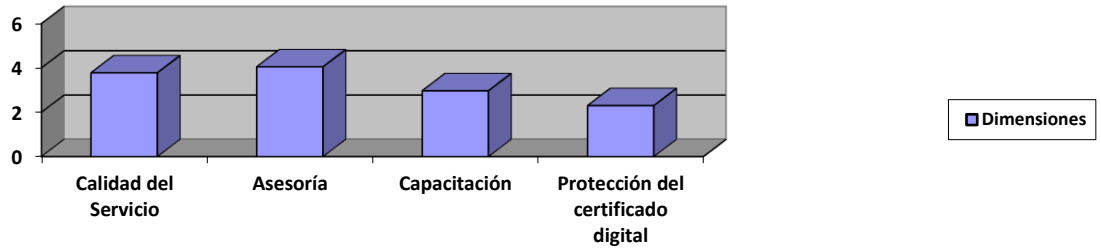

Fig. 1 Resultados de la encuesta (Fuente: elaboración propia).

La encuesta muestra que la asesoría es la dimensión mejor valorada entre los usuarios y se refiere a la atención por parte del prestador. En segundo lugar, se encuentra la calidad del servicio, seguida de la capacitación. Con respecto a esta última, es importante destacar que la idea de capacitación que tienen los usuarios se limita a explicar cómo descargar el certificado y su posterior configuración en los lectores PDF o en sistemas de gestión de documentos digitales. No se profundiza en temas más técnicos referentes a la firma digital, lo cual trae como consecuencia que no se cree una conciencia en el usuario para el cuidado del certificado digital una vez descargado. Esto se evidencia en los resultados de la última dimensión: la protección del certificado digital se muestra como la más crítica, comprobando que en los usuarios no existe la noción del peligro que trae la violación de las medidas de seguridad para proteger el certificado digital.

Los resultados de la revisión de documentos, del análisis del proceso de gestión de emisión de certificados digitales, la entrevista y la encuesta tienen relación en cuanto a la correspondencia que existe entre la capacitación y un correcto uso de la firma digital, evidenciando que el desconocimiento y las violaciones de las políticas de seguridad constituyen el problema fundamental en el uso de la firma digital en los usuarios de la empresa XETID. Este el punto de partida para llevar a cabo una estrategia que permita perfeccionar el desempeño y preparación de los capacitadores, mejorar los conocimientos de los usuarios y por consecuencia la calidad del servicio.

Resultados integrados del estudio diagnóstico

Los resultados se sometieron a una triangulación, lo que posibilitó el contraste de la información obtenida mediante diversas fuentes de procedencia, a partir de los criterios emitidos por los usuarios y los especialistas, así como con el análisis del proceso de gestión de los certificados digitales y el estudio de normativas, leyes y resoluciones, identificándose las siguientes regularidades:

- Los documentos normativos a nivel de país, reconocen la validez de la firma y definen las condiciones que deben establecerse para su correcto uso y divulgación; sin embargo, no se declara una alternativa científicamente fundamentada que establezca las pautas que se deben seguir para la capacitación y el perfeccionamiento de las autoridades de certificación.

- A pesar de existir la voluntad para desarrollar una capacitación con vistas al mejoramiento del uso de la firma digital por parte de los usuarios, aún persiste falta de motivación de estos para recibir este tipo de capacitación, debido a que es un contenido técnico y en ocasiones difícil de comprender para algunos usuarios.

- La autoridad de certificación no cuenta con gran número de especialistas en el tema que puedan cubrir toda la demanda existente; sin embargo, se deberá impartir capacitación a los trabajadores que participan en el despliegue de la firma digital en las entidades, para de esta forma poder cubrir la mayor cantidad de clientes.

- Todos los especialistas consideran necesario desarrollar una capacitación y mantenerse actualizados de forma permanente; sin embargo, debe llevarse a cabo un proceso de innovación que no solo desarrolle actividades teóricas, sino que permita que el usuario se presente como un investigador de su propia práctica, para lograr una mayor motivación por este tipo de capacitación.

CONCLUSIONES

Los resultados del estudio descriptivo diagnóstico realizado mediante la triangulación de tres fuentes: entrevista y encuesta a especialistas y a usuarios, el análisis del proceso de gestión de solicitudes de emisión de certificados digitales y el estudio de documentos rectores, permitió desde diferentes perspectivas, caracterizar el servicio de emisión de certificados que brinda la empresa XETID y determinar las regularidades fundamentales que definen el uso de los certificados digitales por parte de los usuarios y la necesidad de la capacitación para que este uso sea acorde a la política que establecen el país y el Minint. Garantizar una gestión eficiente permite brindar un servicio de calidad a los usuarios. Generalizar la firma digital para todos los ciudadanos en el país es un reto que se debe asumir con seriedad, por lo que hacer un diagnóstico de los problemas que presenta hoy el servicio es el primer paso para para su perfeccionamiento. En el trabajo se muestran las herramientas para que se valore el servicio de emisión de certificados y a partir de los resultados que arroje la investigación se trace un camino que se deba seguir para su mejoramiento continuo. En investigaciones futuras se propone elaborar una estrategia de mejoras para mitigar los principales problemas que se evidencian en este trabajo.

REFERENCIAS

Antón Rodriguez, S. (2023, enero 31). Firma digital, más que un garabato escaneado. Granma - Órgano oficial del PCC. https://www.granma.cu/doble-click/2023-01-31/firma-digital-mas-que-un-garabato-escaneado-31-01-2023-20-01-53

Consejo de Ministros (2019). Decreto N° 360 [Sobre la seguridad de las tecnologías de la información y la comunicación y la defensa del ciberespacio nacional]. https://www.mincom.gob.cu/sites/default/files/marcoregulatorio/d_360-2019_seguridad_tic_y_ciberespacio_nacional.pdf

Feghhi, J., Williams, P., & Feghhi, J. (1999). Digital Certificates: Applied internet security. Addison-Wesley.

Fritscher, M. (1999). Towards A Unique World-wide Digital Certificate. AMCIS 1999 Proceedings. https://aisel.aisnet.org/amcis1999/150

Minint (2016, septiembre 1). Resolución 2 de 2016 de Ministerio del Interior [Text]. Gaceta Oficial. https://www.gacetaoficial.gob.cu/es/resolucion-2-de-2016-de-ministerio-del-interior

Minjus (2019, septiembre 15). Decreto-Ley 370 de 2018 [Sobre la Informatización de la Sociedad en Cuba. GOC-2019-547-O45]. Gaceta Oficial. https://www.gacetaoficial.gob.cu/es/decreto-ley-370-de-2018-de-consejo-de-estado

Minjus (2022, noviembre 10). Resolución 23 de 2022 [Reglas generales para el establecimiento y empleo de los servicios de firma digital de documentos electrónicos basados en dispositivos y técnicas criptográficas. GOC-2022-1034-EX70]. Gaceta Oficial. https://www.gacetaoficial.gob.cu/sites/default/files/goc-2022-ex70_0.pdf

Rao, N., Srivastava, S., & K. S., S. (2017). PKI Deployment Challenges and Recommendations for ICS Networks. International Journal of Information Security and Privacy (IJISP), 11(2): 38-48. https://doi.org/10.4018/IJISP.2017040104

Sensuse, D. I., Syahrizal, A., Aditya, F., & Nazri, M. (2020). Information Security Risk Management Planning of Digital Certificate Management Case Study: Balai Sertifikasi Elektronik. 2020 Fifth International Conference on Informatics and Computing (ICIC), 1-7. https://doi.org/10.1109/ICIC50835.2020.9288593

XETID (s. f.). Prestador de Servicios de Certificación ACXETID. Recuperado 9 de abril de 2023, de https://certificados.xetid.cu/externalra-gui/descarga.xhtml

XETID (2020, junio 5). Declaración de Prácticas de certificación de la ACXETID. Prestador de Servicios de Certificación ACXETID. https://certificados.xetid.cu/externalra-gui/documentos/Declaracion_de_Practicas_Certificacion_de_la_ACXETID.pdf

XETID (2022). Contrato General de Certificación entre XETID y otras entidades. https://certificados.xetid.cu/externalra-gui/documentos/Contrato_del_PSC_General.pdf